

Helleik Rabba Rise
Stian Engen

Windows Server 2019/2022 and Azure Cloud security systems

A general recommendation

Bachelor's thesis in Digital Infrastruktur og Cybersikkerhet
(BDIGSEC)

Supervisor: Erik Hjelmås

May 2022

Helleik Rabba Rise
Stian Engen

Windows Server 2019/2022 and Azure Cloud security systems

A general recommendation

Bachelor's thesis in Digital Infrastruktur og Cybersikkerhet (BDIGSEC)
Supervisor: Erik Hjelmås
May 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Sammendrag

Tittel: Windows Server 2019/2022 and Azure Cloud security systems - a general recommendation

Deltagere: Helleik Rabba Rise, Stian Engen

Veileder: Erik Hjelmås

Oppdragsgiver: Norwegian University of Science and Technology (NTNU) Security Operations Center (SOC)

Kontaktperson: Christoffer Vargtass Hallstensen

Nøkkelord: Windows Server, Informasjonssikkerhet, Sikkerhetsfunksjoner, Microsoft Azure

Antall sider: 65

Antall vedlegg: 11

Tilgjengelighet: Åpen

Studiepoeng: 22,5

Sammendrag:

Organisasjoner i dag har mange cybertrusler som de bør være oppmerksomme på og som de bør aktivt beskyttes imot. Det er mange sikkerhetsfunksjoner som er viktige å bruke for å aktivt beskytte seg imot disse sikkerhetstruslene. Målet med denne oppgaven var å kartlegge forskjellige sikkerhetsfunksjoner og hvilke trusler disse sikkerhetsfunksjonene beskytter imot. For å nå dette målet har gruppen kartlagt flere av de viktigste sikkerhetsfunksjonene i Windows Server 2022, Windows Server 2019 og i Microsoft Azure Cloud. Det er gjennomført ytelsestester som kartlegger hvor mye disse sikkerhetsfunksjonene påvirker ytelsen i Windows Server 2022 og Windows Server 2019. Sluttproduktet er en anbefaling over hvilke sikkerhetsfunksjoner som er nyttig å bruke. Dette er beskrevet gjennom rapporten, og hvordan disse sikkerhetsfunksjonene hjelper med å oppfylle krav rundt standarder og rammeverk.

Abstract

Title: Windows Server 2019/2022 and Azure Cloud security systems - a general recommendation

Participants: Helleik Rabba Rise, Stian Engen

Supervisor: Erik Hjelmås

Employer: Norwegian University of Science and Technology (NTNU), Security Operations Center (SOC)

Contact person: Christoffer Vargtass Hallstensen

Keywords: Windows Server, Information security, Security features, Microsoft Azure

Pages: 65

Attachments: 11

Availability: Open

Study points: 22,5

Abstract:

Organizations today have many cybersecurity threats that they need to be aware of and actively mitigate. There are many security features that is important to use to actively mitigate these security threats. The goal of this thesis is to map out various security features and what kind of threats these features protect against. To achieve this goal the group has mapped out some of the most important security features in Windows Server 2022, Windows Server 2019 and Microsoft Azure Cloud. There has also been done performance tests on how the security features effects the system performance in Windows Server 2022 and Windows Server 2019. The end product is a recommendation of which security features discussed in this thesis that should be implemented, including some of the standards and frameworks these security features help to fulfill.

Preface

This thesis is developed by Helleik Rabba Rise and Stian Engen, and is the final project of our three years while studying Digital infrastruktur and Cybersecurity at NTNU Gjøvik. Through the study we have acquired knowledge about many different aspects of IT systems. From how to configure a network with many end nodes, to how to set up a big cloud environment using docker Swarm. We have also learned about different operating systems and how they work, with some insights in programming and hacking. Despite the Corona pandemic affecting most of our time during our degree, we have acquired a lot of knowledge.

We would like to thank all the contributors who have helped out during the work on this thesis. These contributors are Erik Hjelmås with guidance and advice, NTNU SOC represented by Christoffer Vargtass Hallstensen for providing us with this assignment and Janne Cathrin Hetle Aspheim for helping out with the performance tests. The group would also like to thank Thomas Engen and Kristina Eraker Ødegård for the help on the document structure and proofreading.

Table of Contents

Sammendrag	i
Abstract	ii
Preface	iii
Table of Contents	vii
List of Figures	viii
Acronyms	x
Glossary	xii
1 Introduction	1
1.1 Background	1
1.2 Thesis question	2
1.3 Project description	2
1.3.1 Project Goals	2
1.3.2 Restrictions and constraints	3
1.4 Target audience	3
1.5 Group division	4
1.6 Own background and competence	4
1.7 What the group had to learn	4
1.7.1 Roles	4
1.8 Project management process	5
1.8.1 Tools	5
1.8.2 Method and approach	6
1.9 Methodology	7
1.9.1 Source evaluation	7
2 Theory	8
2.1 Definitions	8
2.1.1 ISMS	8
2.1.2 SOC	8
2.2 Rootkits	8
2.3 Windows	9
2.3.1 Server Core	9
2.3.2 Secured-Core	9
2.3.3 Root of Trust for Measurement	9
2.3.4 DMA protection	9
2.3.5 BitLocker Drive Encryption	10
2.3.6 Hyper-V	10
2.3.7 Hypervisor Code Integrity (HVCI)	10
2.4 Azure	11

2.4.1	Microsoft Azure	11
2.4.2	Azure Automanage - Hotpatch	11
2.5	Framework	11
2.5.1	ISO27001	11
2.5.2	ISO27002	12
2.5.3	Helsenormen for informasjonssikkerhet og personvern i helse- og omsorgssektoren	12
2.5.4	NSM Grunnprinsipper for IKT-sikkerhet 2.0	13
3	Windows security mechanisms	14
3.1	TPM 2.0	14
3.2	Static Root of Trust for Measurement (SRTM)	15
3.3	Dynamic Root of Trust Measurement (DRTM)	15
3.4	The boot process	16
3.4.1	Secure Boot	16
3.4.2	Trusted Boot	17
3.4.3	Early-launch antimalware drivers (ELAM)	17
3.4.4	Measured boot	17
3.5	System Guard	18
3.6	Virtualization-Based Security (VBS)	18
3.7	Secure connectivity	18
3.7.1	QUIC	19
3.8	Secure-core server	22
3.9	System monitor (sysmon)	23
3.10	Process Monitor (Procmon)	24
3.11	Tamper Protection	25
3.12	Reputation-based protection	26
3.13	Windows Defender Application Control	26
3.14	Applocker	26
3.15	Microsoft Defender for Endpoint	27
3.16	Differences between Server 2022 and Server 2019	28
3.17	Frameworks	29
3.17.1	Helsenormen for informasjonssikkerhet i omsorg- og helsesektor	29
3.17.2	ISO/IEC 27002:2022	30
3.17.3	NSM Grunnprinsipper for IKT-sikkerhet 2.0	31
4	Azure security features	32
4.1	Azure Sentinel	32
4.2	Azure AD Identity Protection	32
4.3	Azure AD Privileged Identity Management	33
4.4	Microsoft Defender for Cloud	33
4.5	Multi-factor Authentication (MFA)	34
4.6	Key Vault	34
4.7	Frameworks	35

4.7.1	Helsenormen for informasjonssikkerhet i omsorg- og helsesektor	35
4.7.2	ISO/IEC 27002:2022	36
4.7.3	NSM Grunnprinsipper for IKT-sikkerhet 2.0	36
5	Testing and Demonstration	37
5.1	Setting up test environment Azure	37
5.1.1	Sysmon configuration file	40
5.2	Windows Testing and Demonstration	40
5.2.1	Sysmon testing and demonstration	40
5.2.2	Tamper Protection testing	44
5.2.3	Credential Guard	46
5.3	Azure Testing and Demonstration	48
5.3.1	Sentinel Testing	48
5.4	Performance test	55
5.4.1	Windows Server 2022	56
5.4.2	Windows Server 2019	59
6	Reflection and Discussion	62
6.1	Results	62
6.2	Further work	63
6.2.1	Active directory	63
6.2.2	Policies	63
6.2.3	Network security	63
6.3	Work Evaluation	64
6.3.1	Group work	64
6.3.2	Project work	64
6.3.3	What could be done different	64
7	Conclusion	65
	Bibliography	66
A	Project Plan	71
B	Useful PowerShell commands for Microsoft Defender Antivirus	81
C	Setting up test environment skyhigh	84
D	YAML file for SkyHigh setup	85
E	Sysmon config file	88
F	Defender for cloud Demonstration	126
G	Key Vault Demonstration	130

H Meetings 134

I Time tracking Stian Engen 140

J Time tracking Helleik Rabba Rise 141

K Contracts 142

List of Figures

1	How the boot process is secured, inspired by [44]	16
2	Initial connections TCP+TLS 1.3 vs QUIC, inspired by [38] . . .	20
3	Resumed connections TCP+TLS 1.3 vs QUIC, inspired by [38] .	20
4	SMB client configuration (Source: own material)	21
5	ForceSMBEncryptionOverQuic set to True (Source: own material)	22
6	Snippet from SMB server configuration (Source: own material) .	22
7	Process monitor event log (Source: own material)	25
8	Resource group is made (Source: own material)	37
9	VM is made inside the resource group (Source: own material) . .	38
10	Checking TPM status (Source: own material)	39
11	Secured-core overview (Source: own material)	39
12	Sysmon setup (Source: own material)	40
13	Event Viewer (Source: own material)	41
14	Filtering options for Microsoft Event Viewer (Source: own material)	41
15	Information about an event(Source: own material)	42
16	Friendly View (Source: own material)	43
17	XML View (Source: own material)	43
18	Check to see if Tamper Protection is on (Source: own material) .	44
19	DisableRealtimeMonitoring is set to False (Source: own material)	45
20	DisableRealtimeMonitoring is still set to False (Source: own ma- terial)	46
21	Turning on Credential Guard (Source: own material)	47
22	Check if it is active (Source: own material)	47
23	Create a new workspace (Source: own material)	48
24	Create Log Analytics workspace (Source: own material)	49
25	Enable Microsoft Sentinel (Own material)	50
26	Connect the VM server to the Log Analytics workspace (Source: own material)	50
27	Successfully connected VM (Source: own material)	51
28	Data connectors (Source: own material)	51
29	Search Defender for Cloud (Source: own material)	51
30	Open connector page (Source: own material)	52
31	Configuring connection (Source: own material)	52
32	Security alerts (Source: own material)	53
33	Sample alerts (Source: own material)	53
34	Sample alerts (Source: own material)	54
35	Overview over incidents (Source: own material)	55
36	Windows Server 2022 with default security configuration (Source: own material)	56
37	Windows Server 2022 with improved security configuration (Source: own material)	57
38	Windows Server 2022 with improved security configuration (without Sysmon) (Source: own material)	58

39	Windows Server 2019 with default security configuration (Source: own material)	59
40	Windows Server 2019 with improved security configuration (Source: own material)	60
41	Windows Server 2019 with improved security configuration(without Sysmon) (Source: own material)	61
42	Organization chart	73
43	Waterfall model	75
44	Gantt chart	79
45	Checking Microsoft Defender Antivirus status	81
46	New instance created	84
47	Install agents on VM's	126
48	Security posture and Regulatory compliance	127
49	Workload protections and Firewall manager	127
50	Inventory and Information protection	128
51	Recommendations tab	128
52	Security recommendations	129
53	Creating a new Key Vault	130
54	Enabling disk encryption	131
55	Set access policy	132
56	Making a secret	132
57	List secrets	133

Acronyms

CLI	command line interface.	4
CPU	central processing unit.	19
CSPM	Cloud security posture management.	33
CWP	Cloud Workload Protection.	34
DCSG1002	Cyber security and teamwork.	4
DCSG1005	Infrastructure: secure core services.	4
DCSG2005	Risk Management.	4
DDoS	distributed denial-of-service.	1
DLP	Data Loss Prevention.	27
DMA	Direct Memory Access.	9, 10, 23, 39, 62
DNS	Domain Name System.	18, 23
DRM	Digital Rights Management.	14
DRTM	Dynamic Root of Trust for Measurement.	9, 23
EDR	Endpoint detection and response.	27
ELAM	Early-launch antimalware.	17
GUI	graphical user interface.	9, 24
HVCI	Hypervisor Code Integrity.	9, 10, 18, 23, 26, 47, 62
IaaS	infrastructure as a Service.	6, 11
IDATG2202	Operating systems.	4
IEC	International Electrotechnical Commission.	14
IOMMU	Input/Output Memory Management Unit.	9
IP	Internet protocol.	32, 33
ISMS	information security management systems.	4, 8, 12
ISO	International Organization for Standardization.	4, 11, 12, 14
IT	information technology.	13, 63

MFA multi-factor authentication. 34

NTNU Norwegian University of Science and Technology. i, ii, 1–4, 6, 7, 71–73, 76, 77

OEM Original equipment manufacturer. 22

OS operating system. 3, 10, 11, 15–18, 26, 82

PaaS platform as a Service. 6, 11

PC personal computer. 15, 16

PCI Peripheral Component Interconnect. 9

PIM Privileged Identity Management. 33

Procmon process monitor. 24

QUIC Quic UDP Internet Connections. 19, 21

RDMA Remote Direct Memory Access. 19

RTM Root of Trust for Measurement. 9

SaaS software as a service. 6, 11

SIEM security information and event management. 23, 24, 32, 33, 40, 42, 62

SMB server message block. 18, 19, 21, 22

SOAR Security orchestration, automation and response. 32, 62

SOC Security Operations Center. i, ii, 1–3, 7, 8, 71, 76

SRTM Static Root of Trust for Measurement. 9, 15–17

Sysmon System Monitor. 23, 24

TCP transmission control protocol. 19

TLS transport layer security. 18, 19, 21, 34

TPM Trusted platform module. 3, 9, 14–17, 23, 37, 38, 57, 59, 62, 135

UDP user datagram protocol. 19

UEFI Unified Extensible Firmware Interface. 15–17

VBS Virtualization-Based Security. 9, 10, 18, 23, 62

VM virtual machine. 4, 10, 11, 37–39, 50, 55–57

VPN virtual private network. 21, 32, 33

WDAC Windows Defender Application Control. 26, 62

Wmi Windows Management Instrumentation. 23

Glossary

boot kit A boot kit is a type of root kit that tries to attack in the boot process of the machine. 15, 16

cyber Involving computers or computer networks. ii, 1, 4, 8, 11, 25

Kanban A Kanban board is a agile project-management tool that is designed to help visualize work and maximize efficiency. 2, 5–7, 64, 72, 75, 76

LaTeX LaTeX is a typesetting system that includes many features for production of technical and scientific documents. 4, 5

Microsoft Microsoft is a large vendor of computer software. 6, 18, 27

Microsoft Azure Microsoft Azure is a cloud platform. i, ii, 3, 4, 6, 11, 37, 38, 62–65

OpenStack OpenStack is an open source cloud computing infrastructure software. 3, 6

Overleaf Overleaf is a online LaTeX editor. 5

phishing A type of social engineering where the attacker tries to get the victim to revealing sensitive information or download malicious software. 1

ransomware Malicious software that often encrypts the victims computer and requests money to decrypt it, or threatens to publish the victims personal data. 1

SkyHiGh NTNU's Openstack cloud service. 3, 6, 7

Toggl track Toggl track is a online time tracker that is easy to use for group projects. 5, 7

Chapter 1

1 Introduction

1.1 Background

The project owner NTNU Security Operations Center (SOC) is the one defining the requirements for this thesis. NTNU is a university with a main profile in science and technology with an international focus, and has its headquarters in Trondheim as well as campuses in Ålesund and Gjøvik [47]. SOC is the Digital Security department at NTNU. Their task is to detect, analyze and respond to digital security threats aimed at NTNU's systems, as well as reduce vulnerabilities in NTNU's digital infrastructure.

To evaluate which security mechanisms that are essential to provide NTNU with the best possible security coverage on all areas, it is important to have a good understanding of the cybersecurity threat landscape. This includes knowledge of what the biggest threats are currently and what might become important in the future.

Companies today have a plethora of cyber threats that they should be aware of and actively mitigate. Some of the most common security threats that the world face today is Phishing, Ransomware, distributed denial-of-service (DDoS), and compromised passwords [5]. These threats have become especially more prevalent today considering how working from home has become the new normal for many employees around the world.

All though this expansion of remote and hybrid workplaces has brought new opportunities and made productivity a lot easier for the workforce, it has also brought with it a set of new cybersecurity challenges. According to data from the Microsoft commissioned security signals report: *«75% of security decision-makers at the vice-president level and above feel that the move to hybrid work leaves their organization more vulnerable to security threats»* [46].

The group have selected the task to map out the different built-in security features in Windows Server 2019/2022 and various security services in Azure Cloud. This will help NTNU SOC to know what security features they should implement to defend against current and new security threats in an ever changing environment. This will provide some guidance for NTNU to transition into newer Windows Server operating systems and illustrate what the security possibilities are in Azure Cloud.

1.2 Thesis question

"Which security features are crucial for hardening the security of a Windows Server 2019/2022 and Microsoft Azure Cloud environment?"

1.3 Project description

The NTNU SOC is a part of the digital security department at NTNU. Their task is detecting, analyzing and responding to digital security threats aimed at NTNU's systems. The group has received this project from the NTNU SOC with Christoffer Vargtass Hallstensen as the contact person.

The goal for this project is to examine the different security functions of the newer versions of Windows Server and Microsoft Azure, as well as identify the specific types of threats that these security functions eliminates. This information will then be used to create a recommendation for a collection of security mechanisms that NTNU should implement to have a well-rounded and complete protection against most cybersecurity threats.

1.3.1 Project Goals

The end product will be an analysis of different security mechanisms in Windows server 2019/2022 and Microsoft Azure. The main goal of this thesis is to map out the most important security mechanisms and what kind of attacks they protect against, as well as finding out how these security mechanisms help to fulfill relevant frameworks. How the different security configurations affect the system performance is also a part of the project.

Learning goals

- **L1:** Obtain new knowledge about important security features in Windows server 2019/2022.
- **L2:** Learn how to use Microsoft Azure Cloud platform.
- **L3:** Get a better understanding of how to implement the various security mechanisms.
- **L4:** Learn how to organize a larger project and how to use a Kanban board in practice.
- **L5:** Obtain more knowledge about different international and national security standards.
- **L6:** Learn what is best practice when it comes to Windows Server security.

Effect goals

- **E1:** Make a recommendation of what security features that should be used in Windows server 2019/2022.
- **E2:** Make a recommendation of what security mechanisms and features to use in Microsoft Azure.
- **E3:** Find a good balance between security and performance in Windows Server 2019/2022 and Microsoft Azure.

Result goals

- **R1:** The end product should be a helpful guidance on which security features to implement on Windows Server and in Azure Cloud.
- **R2:** Measurements from tests that show difference before- and after turning on the various security features.
- **R3:** Show how to implement some of the security features included in this thesis.
- **R4:** Provide a good overview of which sections in the various frameworks the different security features helps to fulfill.

1.3.2 Restrictions and constraints

The plan was to use SkyHiGh for testing the operating system because the group was familiar with OpenStack, but SkyHiGh did not support Trusted platform module (TPM) 2.0 yet. TPM is a new requirement for Windows server 2022. The Trusted platform module was needed for multiple security features [11], therefore these features could not be tested in SkyHiGh. That is why most of the testing was preformed in Microsoft Azure.

The group had not worked with Microsoft Azure before, and because of this there was used more time then planned getting familiar with how to use the Microsoft Azure portal and its functions.

1.4 Target audience

The targeted audience is NTNU SOC, but this thesis is relevant for many other businesses who plan on using Windows Server 2019/2022 or using Microsoft Azure as a public cloud provider. It is also relevant for people who just want to get a better understanding of the security features in Windows Server and the security features that Microsoft Azure provides.

1.5 Group division

The group initially consisted of four members, but 16.02.2022 there was made a decision to split the group into two different groups where one group would write about Windows Server 2019/2022 and Microsoft Azure. The other group about Windows 10/11 and Microsoft Office. The reason why the group decided to split up was because the collaboration did not work out as well as wished.

1.6 Own background and competence

The group consists of two bachelor degree students who study infrastructure and cybersecurity at NTNU Gjøvik. Both of the group members have completed the course Operating systems (IDATG2202) [37], which provided useful insight in how the Windows operating system is structured. In Cyber security and teamwork (DCSG1002) [57] the students learned how to work in teams and how to identify and mitigate known security threats. Risk Management (DCSG2005) [55] where the group acquired knowledge about information security management systems (ISMS) frameworks for security, International Organization for Standardization (ISO) standards such as 27001, 27002, 27005, security policy and security culture. In the course Infrastructure: secure core services (DCSG1005) [36] the group learned to set up and work with a cloud system, this was needed for the testing phase of this project.

1.7 What the group had to learn

For this project the group had to learn how to write in LaTeX and how to set up the document structure. The group also had to learn how to use Microsoft Azure to set up test VMs and how to manage them. Then the group had to learn about the Microsoft Azure command center and how to use multiple of the security features Microsoft Azure has to offer, to test what combination the group would recommend. To deploy the test VMs and set up the environment with the CLI, the group had to learn how to use the Microsoft Azure cloud shell.

1.7.1 Roles

Group Roles

Group leader: Helleik Rabba Rise

Secretary: Stian Engen

Project Roles

Stian Engen: Responsibility for quality assurance of the report.

Helleik Rabba Rise: Responsibility for the thesis structure and presentation.

Administrative responsibilities

- Book rooms: Helleik Rabba Rise
- Time keeping in Toggl track: Stian Engen
- Gantt-scheme compliance: Stian Engen
- Overleaf structure: Helleik Rabba Rise
- Kanban board: Stian Engen

1.8 Project management process

1.8.1 Tools

Toggl

Toggl track is used to track the time used by both group members while working on the thesis. Toggl track might motivate the group members to work more, because you can see how much the rest of the group worked. It can also be a reminder to work more if the set work time is not met. The whole group have all the logged work of the rest of the members, this is great for balancing the work load.

Overleaf

The thesis is written in Overleaf, because it offers a platform where the group can collaborate both at once. It is written in LaTeX because it provides good customisation opportunities, and is widely used on scientific documents.

Microsoft Teams

Microsoft Teams is used for file sharing, communication and meetings during the development of this project. The Kanban board that is used is also in Teams, which is where the group members will log different tasks that needs to be done and how the progress is going with the different tasks.

Microsoft Azure

Microsoft Azure is a public cloud service offering infrastructure as a Service (IaaS), software as a service (SaaS) and platform as a Service (PaaS). Microsoft Azure supports many Microsoft-specific tools and software, but also supports many third-party options. This is where the testing environment for Windows server 2019 and 2022 will find place, as well as the testing of the different security features Microsoft Azure provides.

SkyHiGh

SkyHiGh is a private cloud service which is hosted by NTNU. SkyHiGh is running OpenStack as their computing platform. OpenStack is usually used as an infrastructure as a Service[48]. This is where some the vulnerability tests on Windows server 2019 and 2022 will be performed.

Draw.io

Draw.io is a free online tool for making sketches, diagrams or charts. It provides many types of figures that is easy to implement to your illustrations to make them look better and easier to understand. It is easy to use with drag and drop functionality and snap on functionality.

1.8.2 Method and approach

Microsoft Teams provides an built in Kanban board feature. The Kanban board will be the group's main tool to organize the different tasks that needs to be done. The Kanban board is an agile project management tool that will help the group to visualize work and maximize efficiency and work flow. There is 5 different columns on the board: Backlog, In progress, Testing, Review and Completed.

Backlog: This is where all the different tasks that needs to be done is put, so whenever a group member comes up with a new task it is placed under the "backlog" column.

In progress: When a group member starts working on a task from "backlog" the task is then moved to "in progress". In this column the group member can specify the status of the task as well as make some notes that is relevant to the specific task.

Testing: The "testing" column is where all the tasks that requires testing in SkyHiGh or Microsoft Azure will be placed.

Review: All the tasks a group member is finished with will be placed under this column. When a task is placed under "review", another group member will oversee the task and approve it or give feedback on what is missing or should be done different.

Complete: After a group member has approved a task in "review" the task will be placed under complete.

By using this agile work method the group will easily be able to prioritize the different tasks that will come up during the work on this project. The Kanban board will also allow the group to assign the different tasks to individual members as well as setting deadlines for the specific tasks.

Toggl track is another tool that will be used to keep a record of how much each group member works in hours. This is where group members individually registers work hours and what they have done throughout the project.

1.9 Methodology

The information that this report is being based on will primarily come from Microsoft's own documentation with supplements of information from other sources that are good and reliable. Two different test environments is used for testing, the primary test environment is Azure Cloud, but some test will take place in SkyHiGh. In these environments different security features will be configured and enabled. These test will include both security and performance.

To make sure the requirements from NTNU SOC is met, the group will have meetings with Christoffer Vargtass Hallstensen when needed, and have regular meetings with supervisor Erik Hjelmås every week. Since there are only two group members, meetings are planned every day on weekdays where the group members work together.

1.9.1 Source evaluation

Multiple sources and articles were used to understand how the different security features and functions, described in this thesis, work. When collecting the information needed, sources from the official sites and well known companies were preferred, to ensure the information was reliable. This was important to maintain the integrity of the thesis. Most of the information is collected from Microsoft's official sites (Microsoft docs). When obtaining information from other sites it was important to ensure the author had a relevant background from the IT security industry.

Chapter 2

2 Theory

This chapter consists of several sections, where each part describes a type of theory that is relevant to the thesis. Definitions are clearly described in this chapter to make sure there is a common understanding of the different terms and to avoid misunderstandings. The various frameworks that is in this thesis will also be described in this chapter.

2.1 Definitions

2.1.1 ISMS

information security management systems (ISMS) is a documented management system that consists of a set of security controls that protect the integrity, confidentiality and availability of assets from vulnerabilities and threats. Organizations can protect their sensitive, confidential and personal data from being compromised by designing, implementing, managing and maintaining an ISMS[40].

2.1.2 SOC

Security Operations Center (SOC) is a central part within an organization who is responsible for continuously monitoring and improving an organization's security. While also detect, analyze, prevent and respond to cybersecurity incidents.

2.2 Rootkits

Rootkits is a collective name for a type of software that is usually classified as malware, this malware usually grants access to a computer or privileges to software that is not usually allowed. The different types of rootkits provides different types of privileges to the attacker. There are rootkits that can hide and disguise as other processes, then there are more serious rootkits that run on kernel level and even on hardware level. When the rootkit is running on kernel or hardware level it can be hard to detect, but there are different security measures for this like "Device Guard" and other security features that removes multiple ways the attacker is able to infect a system with a kernel level rootkit [56].

2.3 Windows

2.3.1 Server Core

Windows Server Core is an optional server version to the full installation. The Server Core is a smaller installation and does not contain all the server roles that the usual installation provides, while installing, it is possible to choose which roles to install. This makes the server more secure because it has a smaller disk footprint and therefore less code for potential attackers to attack or exploit. The Server Core does not have a GUI, because it only includes the essential services to do its task, which usually only needs to be done through PowerShell or other GUI tools [30].

2.3.2 Secured-Core

This is a concept that combines firmware, hardware and driver capabilities to protect the operating environment. For the system to be classified as a Secure-Core server it must meet some requirements. The system has to use the Trusted platform module 2.0, Secure Boot with Dynamic Root of Trust for Measurement has to be enabled, System Guard with Direct Memory Access protection must be activated and Virtualization-Based Security and Hypervisor Code Integrity needs to be enabled. These security features will defend many pathways attackers might want to use, from the boot process to protecting data in memory.

2.3.3 Root of Trust for Measurement

Root of Trust for Measurement (RTM) is a software capability that TPM helps out with, but it does not solely live inside the TPM chip. RTM works by making sure the environment that is booting, is verified and not tampered with. There are several different processes that can happen during the boot chain, these processes can change over time and change the order in which they load. Dynamic Root of Trust for Measurement (DRTM) and Static Root of Trust for Measurement (SRTM) are two different RTM methods.

2.3.4 DMA protection

Kernel Direct Memory Access (DMA) protection protects the device by using the Input/Output Memory Management Unit (IOMMU) to block PCI devices unless the device has drivers that support memory isolation like DMA remapping. DMA remapping works by restricting the device to a specific memory location. By restricting the device to a specific memory location the device is allocated a clear space of memory where it can perform its functions. This

ensures that the device does not have access to any other information stored in the system memory. If a device driver do not support DMA remapping, it will not be able to run on a device with DMA protection enabled [15].

2.3.5 BitLocker Drive Encryption

BitLocker Drive Encryption provides full-volume encryption to protect data at rest. The most used configuration splits the hard drive into multiple volumes. User data and the operating system (OS) on one volume that contains confidential information. The other volumes hold public information such as system information, recovery tools and boot components. Bitlocker encrypts the volume that contains the operating system. So if the hard disk/computer is stolen or lost when powered off, the data that is on the volume remains confidential [10].

2.3.6 Hyper-V

Hyper-V is a virtualization service that uses Windows hypervisor, Hyper-V enables the creation of one or many virtualized computing environments. These environments are separated and will not affect each other. In these environments it is possible to create and manage multiple VMs. These VMs can use many different operating systems and do different tasks. This will provide the ability to host multiple services on the same machine without any of the services affecting each other, even if some of the hosted services gets errors and shuts down. Hyper-V offers multiple useful features like disaster recovery and backups where it is possible to save the current state of the virtual machines in another geographical location [39].

2.3.7 Hypervisor Code Integrity (HVCI)

Hypervisor Code Integrity is also called Memory integrity in Windows. It is named Memory integrity because it uses Virtualization-Based Security to perform code integrity checks. These checks the drivers and programs that try to run in kernel-mode, if the code comes from a trusted source. If the code comes from a source that is not trusted HVCI will prevent the code from running kernel-mode privileges. HVCI protects other Windows processes from being tampered with by ensuring that these processes have a valid certificate [14].

2.4 Azure

2.4.1 Microsoft Azure

Microsoft Azure is a cloud computing service operated by Microsoft that mainly offers three services, IaaS, PaaS and SaaS. Microsoft Azure supports various different programming languages, frameworks and tools. This includes both Microsoft and third party systems and software.

2.4.2 Azure Automanage - Hotpatch

Hotpatching is a new feature for the Windows server 2022 Datacenter: Azure Edition. This feature enables the ability to update the VM without needing to reboot the machine after installation. This feature is not available on the standard Windows server 2022 OS [12]. The hotpatching feature should enable faster deployment of updates and therefore lower the workload and ensure the VM is running the latest version of the OS. This ensures that the latest security patches is deployed as soon as possible. The hotpaching feature will not ensure that the VM never is rebooted, when a new baseline is released by Microsoft the VM will have to reboot to start using the the new baseline, the hotpatches will only add or modify the current baseline. These baselines is released periodically with three month intervals in the beginning. When an unplanned baseline is released the VM is required to reboot and install the new baseline [7].

2.5 Framework

A cybersecurity framework is a system of guidelines, best practices and standards to manage risks that occur in the digital world. By using these guidelines and frameworks, organizations will be more attractive to other possible customers, because it fulfills the recommended standards. This ensures good practices within the organization and is then going to be seen as an more serious company. Some businesses require that their partners follows certain standards and frameworks.

2.5.1 ISO27001

International Organization for Standardization (ISO) is a international organization that has developed different standards for various sectors. ISO27001 is an international standard that has been developed to set requirements for establishment, implementation, maintenance and continuous improvement of management systems in the information security sector. The main aim of ISO27001

is to help organizations keep the information assets they own more secure. Following ISO27001 have several benefits that include helping to maintain confidentiality, integrity and accessibility of information through a risk management process. ISO27001 also provides the compliance requirements that is needed to become certified.

2.5.2 ISO27002

ISO27002 is a set of guidelines that is made to help organizations to introduce and implement information security management systems (ISMS) best practices based on ISO27001. This will help organizations to meet the requirements to be ISO27001 certified. There are many guidelines in ISO27002 that is not needed to get the ISO27001 certification, but the guidelines are recommended best practices to make the organization more secure and robust against any possible incidents or attacks.

2.5.3 Helsenormen for informasjonssikkerhet og personvern i helse- og omsorgssektoren

(Health norm for information security and privacy in the healthcare sector)

Helsenormen is a rule set of norms that is created for privacy and information security. Helsenormen applies to all businesses that has committed to following it. These norms are developed for organisations and businesses within the health sector, but is used by other sectors like science and innovation. Helsenormen does not contain all the legal requirements to information security and handling personal information. Helsenormen is rather a supplementation to the current regulations. Helsenormen distinguishes between "must" and "should" requirements, if the organization handles much personal information from many people, the requirements are higher then for smaller organizations, but Helsenormen is required to cover most of the aspects within information security and privacy: humans, processes and technology [33].

2.5.4 NSM Grunnprinsipper for IKT-sikkerhet 2.0

(National security authority Basic principles for IT-security 2.0)

NSM's grunnprinsipper is a set of recommendations for companies on how to secure their information systems. Which recommendations that should be implemented varies from how big the company is and what information they collect from their users. If the company is large they should implement more recommendations than a small business. NSM's grunnprinsipper is divided into four sections. First is "Identifying and mapping" this section provides guidelines and principles on how to get a view on what IT systems is being used by the company and what kind of service or products they provide. This will then be used to prioritize which security measures they should implement and how, to meet the businesses needs. The second section is "Protect and maintain", the principle here is to secure and maintain a secure IT system over time and after revisions. The third section is "Detect", this implies to detect and eliminate known security threats. There should also be implemented a monitoring system that can find irregularities that can imply that something is wrong and if it should be further investigated. There should be done regular vulnerability mapping of the IT systems, these will help remove vulnerabilities and find deviations from the preferred security standards. The last section is "Handling and recovery". This covers how to handle security incidents effectively. It also includes restoring the IT systems to their normal state [52].

Chapter 3

3 Windows security mechanisms

3.1 TPM 2.0

Trusted platform module (TPM), also known as ISO/IEC 11889 is an international standard for a secure cryptoprocessor. A secure cryptoprocessor is a chip or microprocessor that carry out cryptographic operations and is for the most part ingrained with different physical security measures, and is providing a degree of tamper resistance. The term TPM is also used to refer to a chip that is conforming to the ISO/IEC 11889 standard. Some of the things TPM is used for is Windows Defender, enforcement and protection of software licenses and Digital Rights Management (DRM) [24].

Some of the data that is transmitted is sent unencrypted, TPM chips use both software and hardware to protect passwords or encryption keys when they are sent in an unencrypted form. TPM chips provide a safe storage to store encryption keys, passwords and certificates that is used to log in to online services. This is safer than storing this type of information on the hard drive.

There are different things you can do with a TPM, the most basic use of a TPM is to set a login password for the system. The TPM chip automatically protect the data, by not storing it on the hard drive. One of the reasons many people decide to use TPM, is to enable the Windows BitLocker Drive encryption. When a system have both TPM and BitLocker the TPM chip runs a sequence of conditional tests to check if it is safe to boot up the system. If the TPM notice that the hard disk was moved it locks down the system.

TPM adds additional hardware based security to Windows. Some of TPM's biggest features is Platform Crypto Provider, Virtual Smart Card, Windows Hello for Business, BitLocker Drive Encryption, Device Encryption, Measured Boot, Health Attestation and Credential Guard.

Some concerning parts about TPM for the future is that manufactures might use it to prevent you from making sensitive modifications to your system. The TPM will only obey its owner by default. If the owner tell the TPM that the current state of the system is known-good, the TPM will always make sure the system is in that state. The problem is if a manufacturer sets the TPM to believe that a known-good state is where hostile Digital rights management or other rights restricting software is enabled.

Another element that can be criticised is that a TPM may be used to prove to remote websites that the machine is running software that they want the machine to run, or that the machine is using a device that is not fully under your

control. A TPM can prove to a remote server that the firmware in the system has not been tampered with. If the system firmware is designed to restrict rights, then the TPM is proving that the rights are adequately curtailed. TPMs are currently not being used to do this, but the technology to do it is available [34].

3.2 Static Root of Trust for Measurement (SRTM)

SRTM ensures that no unauthorized firmware or device drivers starts before the Windows bootloader. This is to prevent malicious software such as boot kits to access privileges it should not have. SRTM is part of the Secure Boot feature which is providing hardware-based root of trust, this is important, to have a secure platform for the OS to run on.

SRTM uses TPM to do measurements of all the firmware and device drivers. These measurements are then checked up against different lists. There are two types of SRTM lists, both with their own drawbacks. One of the lists is a "blocklist". This list contains known-bad Static Root of Trust for Measurements. This type has the weakness where if someone changes a few bits of a "bad" SRTM it have to be listed on the "bad" list and blocked, and therefore a small change of a "bad" SRTM can make it go through, because one minor change will create a new SRTM hash that is not on the "blocklist". This will then enable someone to start the operating system on untrusted firmware or software which makes the OS vulnerable. The other list is a list of "good" SRTMs, this list does not have the same weakness as the "bad" list, but there are many Bios/PC combination measurements that have to be added to this list. This is a slow process and developing UEFI code can be time consuming. The main drawback with SRTM is that it needs to keep measurements of all the UEFI components and this contains a big amount of code. Every time the system changes it needs to make new measurements[1]. If the firmware fails the measurement, the UEFI firmware will try to recover a trusted firmware version [32].

3.3 Dynamic Root of Trust Measurement (DRTM)

This is a newer solution to mitigate the problems with SRTM and to try and provide a safe environment for the operating system. This is done by different technologies depending on the hardware of the system, but the concept is the same. It lets the system boot freely even if the system uses code that is not trusted[32]. Then the system is launched into a trusted state by taking control of all the CPUs and the chipset, and telling it to perform specific tasks that ensures that nothing else than specific code can run. Then everything that is currently running gets stopped or blocked. This to create a clean state of the system where no untrusted code is running, or at this point only specific code

is running on the system. When this process is over the state of the system is measured with the TPM[2], and is then verified.

3.4 The boot process

In the boot process of a machine there is many processes happening that the user do not see. There is many security features who work together to ensure the system's integrity, this process is illustrated in Fig. 1.

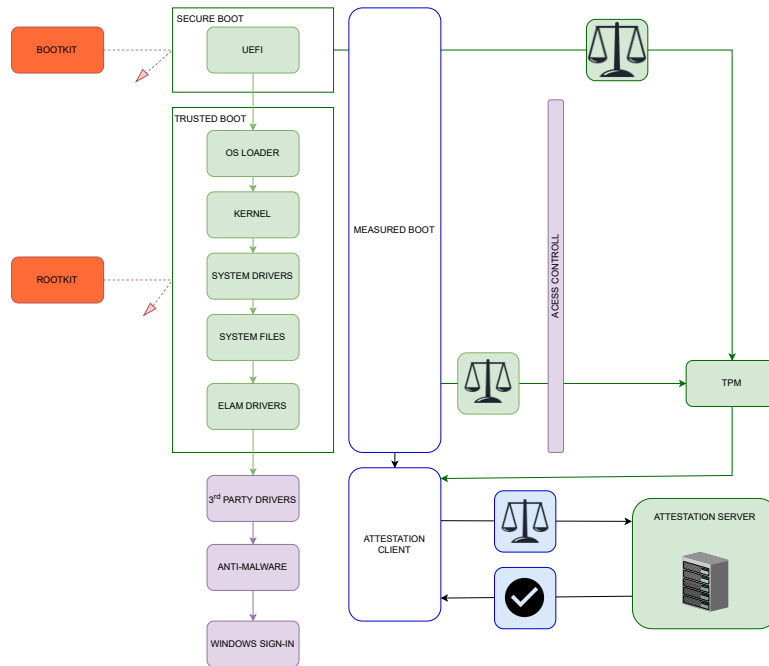


Figure 1: How the boot process is secured, inspired by [44]

3.4.1 Secure Boot

Secure Boot is a security standard which is developed by multiple different actors in the PC industry. This was created to protect the operating system's bootloader from being tampered with, by boot kits. This protection is done by the UEFI firmware[21]. The UEFI checks every piece of the boot software with a signature database, this technique is called Static Root of Trust for Measurement. This can be drivers on a memory stick or expansion card, graphical applications and the Operating system[44]. If everything is in the signature database and not in the revoked database (this depends on the list type the

SRTM uses) the system continues the boot process, and the operating system starts managing the hardware.

3.4.2 Trusted Boot

Trusted Boot continues the process from Secure Boot. The Windows bootloader that was checked by the UEFI in the Secure Boot process is now verifying the digital signature of the Windows kernel. If the signature is within the database the kernel now verifies all the remaining components of the Windows startup process. This again includes all the Option ROMs (drivers on expansion cards etc. also known as UEFI firmware drivers)[22]. This is illustrated in Fig. 1. The Windows kernel then verifies boot drivers, system files and Early-launch antimalware (ELAM) drivers. If any of the signatures do not match, it means that the software have been tampered with, or something is wrong with it. Then the bootloader will not load the current component. When corruptions occur in parts of the Windows OS, it can often repair the corrupted component automatically, but it can not fix UEFI drivers if there is something wrong with them.

3.4.3 Early-launch antimalware drivers (ELAM)

After Trusted Boot, there are loaded many third party drivers. To ensure that there is not loaded any malicious boot drivers ELAM checks all the boot drivers if they can be trusted before they are loaded[19]. This is important because most anti-malware systems does not start before the boot drivers are loaded[44].

3.4.4 Measured boot

Rootkits have the ability to hide their presence in an infected machine, if a machine is infected the anti-malware software is not able to detect this. When the infected machine is done booting and the user sign in on the machine, the malware will have full access to all the data in the system and the organization if the machine is connected to an enterprise network. Measured boot mitigates this problem by using TPM, UEFI and third party software[16]. The PC's UEFI firmware stores a hash from everything that will be loaded before the anti-malware application. Before the boot process is done Windows starts a non-Microsoft remote attestation client. This client communicates with the attestation server, and receives a unique key[17]. This key is then used to digitally sign the log that was recorded by the UEFI, this is signed with the Trusted platform module. The signed log file can contain more information depending on the configuration, this is then sent to the attestation server. The attestation server then determines if the machine is healthy or not. If the machine is determined infected it will not be able to connect to the enterprise

network and can be set in quarantine, this is managed by the organization and their policies.

3.5 System Guard

System Guard is a part of Microsoft Windows Defender, it includes both VBS and HVCI technologies. The job of System Guard is to maintain the integrity of the system during the boot process and run time. It also validates that the system integrity has not been changed through remote or local attestation. VBS use a part of a system memory that is separate from the OS in a virtual secure mode. This is to prevent malware from being able to execute code or getting access to platform secrets. HVCI is used as an additional check, it uses VBS to check the kernel mode drivers and binaries before they are started. System Guard helps with defending against the types of bootkits and rootkits that frequently affected Windows 7 systems. The reason System Guard protects against these kind of threats is because it prevents any kind of unauthorized software or firmware from launching before the Windows boot loader.

3.6 Virtualization-Based Security (VBS)

Virtualization-Based Security separates multiple security features from the operating system by using Windows hypervisor. This is done by isolating a secure part of memory from the OS itself. This part of the memory creates a safe environment for the security features, this environment increases the protection of the security features from vulnerabilities in the OS[25]. This will limit the abilities malware have, even if the malware have access to the OS kernel.

3.7 Secure connectivity

Secure connectivity is a concept that is implemented by using newer internet protocols which is more secure. These protocols have been set as default on Windows Server 2022. Encrypted DNS name resolution is done by using the HTTPS protocol to encrypt the DNS query. This helps keeping the traffic more private and protects against people eavesdropping, or a man in the middle manipulating the DNS data. HTTPS and TLS 1.3 is enabled as default on Windows server 2022. This provides a more secure communication channel between servers and nodes. TLS 1.3 is the newest version of TLS. The protocol is improved by using a minimum of clear text protocol bits[53].

Server message block (SMB) is now a Windows-based network, where users that is connected can share, create, modify and delete shared files and folders, devices like printers and scanners are also available here. SMB now supports AES-256

encryption. What type of encryption which is going to be used is determined between the machines when they connect to each other, but it will always try to use the highest level of encryption available if nothing else is specified[3]. Windows server 2022 supports SMB encryption within the server clusters, this means that the SMB traffic between the servers within the same data center can be encrypted. This makes the communication between the servers more secure. SMB Direct is a feature that is made for transporting a big amount of data, with low latency and low CPU utilization. To use SMB Direct the network adapter of the machine must support Remote Direct Memory Access (RDMA) capabilities. This is usually usefull for servers running an SQL Server or Hyper-V and require a lot of data and high speeds. SMB Direct supports encryption in Windows Server 2022. In previous versions of Windows Server you were able to toggle on encryption, but this disabled direct data placement. Doing so made RDMA perform like TCP.

3.7.1 QUIC

QUIC is in this context an encrypted connection-oriented protocol. The protocol operates on the transport layer and is built on UDP. Because of this, QUIC have reduced connection times, recovering faster when packets is lost and less round trips compared to TCP, but it is not as reliable as TCP and is not as suitable as TCP in many situations yet. Some monitoring systems and security systems might not be able to work with QUIC. In Fig. 2 there is an illustration of an initial connection to a server where one is using TCP with TLS 1.3 and the other example uses QUIC. In Fig. 3 it is illustrated how a machine using TCP with TLS 1.3 re-establishes connection with a server and how QUIC does it. These illustrations shows the speed improvements in QUIC compared to TCP by looking at the numbers of handshakes.

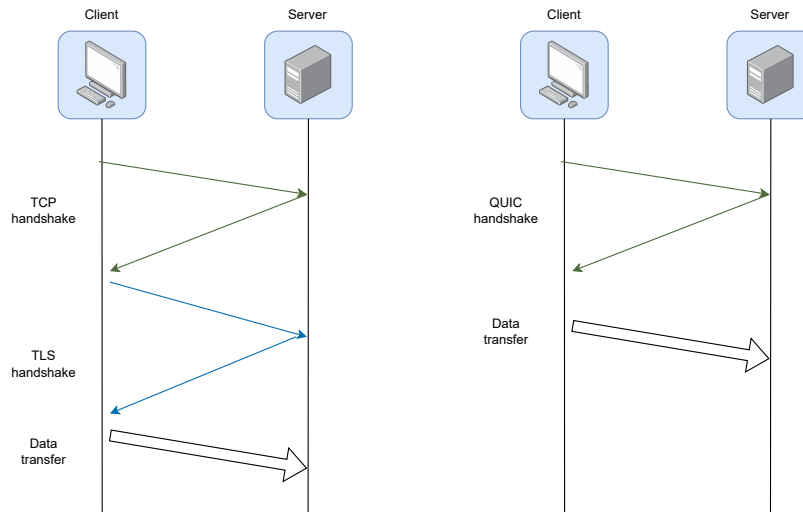


Figure 2: Initial connections TCP+TLS 1.3 vs QUIC, inspired by [38]

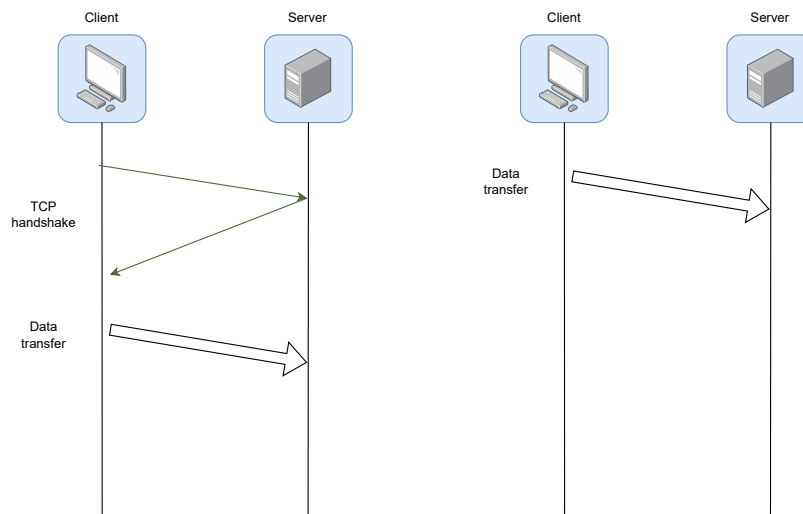


Figure 3: Resumed connections TCP+TLS 1.3 vs QUIC, inspired by [38]

SMB over QUIC is only available on Windows Server Azure Edition at the moment. QUIC can act like a "SMB VPN" for organizations, where the traffic is encrypted with TLS 1.3, and can further be encrypted with SMB encryption [23]. SMB over QUIC enables the user to access the organizations file servers without needing a VPN, and is then able to work from anyplace where there is internet. All the data transmitted with QUIC is encrypted and this protects the data from anyone, even on an insecure internet, but the data not transmitted with QUIC is not secure.

To look at the SMB client configuration one can run the following command:

```
Get-SmbClientConfiguration
```

The output from this command can be seen in Fig. 4.

```
PS C:\> Get-SmbClientConfiguration

SkipCertificateCheck           : False
ConnectionCountPerRssNetworkInterface : 4
DirectoryCacheEntriesMax      : 16
DirectoryCacheEntrySizeMax    : 65536
DirectoryCacheLifetime        : 10
DormantFileLimit              : 1023
EnableBandwidthThrottling     : True
EnableByteRangeLockingOnReadOnlyFiles : True
EnableInsecureGuestLogons     : True
EnableLargeMtu                : True
EnableLoadBalanceScaleOut     : True
EnableMultiChannel            : True
EnableSecuritySignature       : True
ExtendedSessionTimeout        : 1000
FileInfoCacheEntriesMax       : 64
FileInfoCacheLifetime         : 10
FileNotFoundCacheEntriesMax    : 128
FileNotFoundCacheLifetime     : 5
ForceSMBEncryptionOverQuic    : False
KeepConn                      : 600
MaxCmds                       : 50
MaximumConnectionCountPerServer : 32
OplocksDisabled               : False
RequireSecuritySignature      : False
SessionTimeout                : 60
UseOpportunisticLocking       : True
WindowSizeThreshold           : 1
```

Figure 4: SMB client configuration (Source: own material)

TLS 1.3 provides encryption for SMB over QUIC, so there is usually no need for SMB encryption. But if you need to enable it you can run the following command:

```
Set-SmbClientConfiguration -ForceSMBEncryptionOverQuic $True
```

In Fig. 5 "ForceSMBEncryptionOverQuic" has been set to True.

```
FileNotFoundCacheEntriesMax : 128
FileNotFoundCacheLifetime   : 5
ForceSMBEncryptionOverQuic  : True
KeepConn                     : 600
MaxCmds                      : 50
```

Figure 5: ForceSMBEncryptionOverQuic set to True (Source: own material)

To look at the SMB server configuration you can run the following command:

```
Get-SmbServerConfiguration
```

In Fig. 6 both "RestrictNamedpipeAccessViaQuic" and "EnableSMBQUIC" is true by default.

```
ValidateAliasNotCircular : True
ValidateShareScope       : True
ValidateShareScopeNotAliased : True
ValidateTargetName       : True
RestrictNamedpipeAccessViaQuic : True
EnableSMBQUIC            : True
```

Figure 6: Snippet from SMB server configuration (Source: own material)

3.8 Secure-core server

Secure-core server is a classification. If a server fulfill the requirements to be classified as a Secure-core server the costumer knows that the OEM has provided a set of hardware, firmware and drivers that meet the Secure-core requirements. The Secure-core server is built on three key elements:

- Simplified security
- Advanced protection
- Preventative defense

These elements ensures that the system have all the new security features and should be a secure platform for user data and critical applications. Simplified security is implemented by ensuring the customer that the hardware and firmware is trusted and the security features on the server is easily configured in

Windows Admin Center. The Advanced protection is implemented with some key security features. These are: Trusted platform module, Secure Boot with Dynamic Root of Trust for Measurement, System Guard with Kernel Direct Memory Access protection, Virtualization-Based Security and Hypervisor Code Integrity. The Preventative defence part is fulfilled with the Advanced protection, many of these features will protect against multiple exploits a potential attacker would try to use[29].

3.9 System monitor (sysmon)

Sysmon is a system monitor for Windows. It is a system service and a device driver. It is made for Windows client 8.1 and higher, and Windows Server 2012 and higher. When Sysmon is installed it will continuously monitor and log system activity to the Windows event log. Sysmon will not stop monitoring and will continue logging after a reboot. It will continue to monitor until it is disabled. Sysmon will provide detailed information about processes, drivers, file modification, Windows Management Instrumentation (Wmi) events, DNS events and errors. The information and events that Sysmon provides can be collected with Windows Event Collection or an SIEM agent for further investigation. Sysmon does not provide an analysis of the events it collects, this has to be done with other services[51]. It does not hide from attackers, but it should create an alert when Sysmon changes state, starts or stops. Sysmon should be configured to provide the monitoring and logging that the current system requires, it is possible to configure event filtering to only get the events that is needed.

Sysmon needs a configuration file to be able to work. It is the configuration file that tells Sysmon what events to collect. There are many good pre-defined configuration files for Sysmon, but if these is going to be used they should be tailored for the current machine and system it is going to be running on. When a configuration file is ready to be tested, it should not be applied to the entire system, but rather on a test environment or a small part of the system. This is important to see if the current configuration works with the environment and antivirus that is being used.

In this report the group have used SwiftOnSecurity's Sysmon file [54], because this file is a great preset of configurations that can be customized to the needs of the current system. Everything in the file is followed up with comments referring to different attacking vectors on Mitre Att&ck that the current part of the configuration will create an alert for. There is other options like sysmon-modular [35] which might be easier to modify to the system it is going to run on, but the group did not have any specific system. That is why the group went with the SwiftOnSecurity's file.

3.10 Process Monitor (Procmon)

Procmon is a free, downloadable utility for Microsoft Windows Client and Server. It is compatible with Windows Vista or Windows Server 2008 and newer. It is an advanced monitoring tool that shows file system, Registry and process/thread activity in real-time. It provides the features of two older Sysinternals utilities, Filemon and Regmon with other improvements. [50] All the information that is being logged can be written to a file, this can then be used later to troubleshoot and hunting for malware. There are many options for filtering events, you are also able to save all events or just the ones that pass through the filter. When setting up Procmon on a system it is important to note that Procmon can run via PowerShell and it runs on administrator access and privileges. It is important to make sure it is protected from unauthorised users. This can be done by using Applocker and block unauthorised users from running Procmon.

Procmon provides an GUI where all processes is logged depending on the applied filters. In contrast to sysmon which only provides events that can be viewed in Windows Event Viewer or an SIEM agent. Procmon provides the ability to see the process tree, here it is possible to see all the processes run by each application or program, this can be helpful when debugging. Sysmon is best suited for logging continuously, but for debugging and for a fast and easy visualization of the running processes it is a great tool. Running the following command will run Procmon, the location of the "Procmon.exe" file must be specified for the current system.

```
Procmon.exe `
/Quiet /AcceptEula /Backingfile `
C:\Users\Administrator\Desktop\ProcmonLog.PLM
```

Procmon was included in the SysteminternalsSuite folder along with Sysmon. To run Procmon you have to accept the license to run the utility, this is done with "/AcceptEula" option. Using "/Backingfile" enables you to set a destination to save the output from Procmon [42]. When Procmon is running it will display many processes depending on the present filters, this can be seen in Fig. 7.

Process Monitor - C:\Users\Administrator\Desktop\ProcmonLog.PLM.PML

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:40:...	MsMpEng.exe	2604	CreateFile	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	Desired Access: R...
11:40:...	MsMpEng.exe	2604	FileSystemControl	C:\Users\Administrator\Desktop\Procmon...	OPLOCK HANDLE...	Control: FSCTL_R...
11:40:...	MsMpEng.exe	2604	CreateFile	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	Desired Access: G...
11:40:...	MsMpEng.exe	2604	QueryStandardI...	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	AllocationSize: 4.1...
11:40:...	MsMpEng.exe	2604	QueryBasicInfor...	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	CreationTime: 4/7/...
11:40:...	MsMpEng.exe	2604	FileSystemControl	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	Control: FSCTL_R...
11:40:...	MsMpEng.exe	2604	QueryBasicInfor...	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	CreationTime: 4/7/...
11:40:...	MsMpEng.exe	2604	ReadFile	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	Offset: 0. Length: 4...
11:40:...	MsMpEng.exe	2604	ReadFile	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	Offset: 4,190,208, ...
11:40:...	MsMpEng.exe	2604	ReadFile	C:\Users\Administrator\Desktop\Procmon...	SUCCESS	Offset: 4,190,208, ...
11:40:...	Idle	0	Process Profiling		SUCCESS	User Time: 0.0000...
11:40:...	Secure System	104	Process Profiling		SUCCESS	User Time: 0.0000...
11:40:...	Registry	180	Process Profiling		SUCCESS	User Time: 0.0000...
11:40:...	smss.exe	424	Process Profiling		SUCCESS	User Time: 0.1875...
11:40:...	csrss.exe	544	Process Profiling		SUCCESS	User Time: 131.35...
11:40:...	wininit.exe	616	Process Profiling		SUCCESS	User Time: 0.5781...
11:40:...	services.exe	760	Process Profiling		SUCCESS	User Time: 4980.8...
11:40:...	lsass.exe	780	Process Profiling		SUCCESS	User Time: 507.57...
11:40:...	svchost.exe	908	Process Profiling		SUCCESS	User Time: 737.15...
11:40:...	fontdrvhost.exe	928	Process Profiling		SUCCESS	User Time: 1.9843...
11:40:...	svchost.exe	392	Process Profiling		SUCCESS	User Time: 1081.9...
11:40:...	svchost.exe	536	Process Profiling		SUCCESS	User Time: 141.42...
11:40:...	svchost.exe	1088	Process Profiling		SUCCESS	User Time: 340.75...
11:40:...	svchost.exe	1104	Process Profiling		SUCCESS	User Time: 4.9375...
11:40:...	svchost.exe	1140	Process Profiling		SUCCESS	User Time: 2.3593...
11:40:...	svchost.exe	1160	Process Profiling		SUCCESS	User Time: 68.937...
11:40:...	svchost.exe	1172	Process Profiling		SUCCESS	User Time: 2.5937...
11:40:...	svchost.exe	1180	Process Profiling		SUCCESS	User Time: 9.5937...
11:40:...	svchost.exe	1312	Process Profiling		SUCCESS	User Time: 3335.0...
11:40:...	svchost.exe	1400	Process Profiling		SUCCESS	User Time: 70.562...
11:40:...	svchost.exe	1428	Process Profiling		SUCCESS	User Time: 293.82...
11:40:...	svchost.exe	1516	Process Profiling		SUCCESS	User Time: 104.73...
11:40:...	svchost.exe	1536	Process Profiling		SUCCESS	User Time: 5.6093...
11:40:...	svchost.exe	1580	Process Profiling		SUCCESS	User Time: 22.671...
11:40:...	svchost.exe	1588	Process Profiling		SUCCESS	User Time: 9.9062...
11:40:...	svchost.exe	1596	Process Profiling		SUCCESS	User Time: 14.156...
11:40:...	svchost.exe	1744	Process Profiling		SUCCESS	User Time: 418.43...
11:40:...	svchost.exe	1768	Process Profiling		SUCCESS	User Time: 1.4218...
11:40:...	svchost.exe	1840	Process Profiling		SUCCESS	User Time: 195.96...
11:40:...	svchost.exe	1860	Process Profiling		SUCCESS	User Time: 10.453...
11:40:...	svchost.exe	1892	Process Profiling		SUCCESS	User Time: 8.2812...

Showing 93,140 of 274,326 events (33%) Backed by C:\Users\Administrator\Desktop\ProcmonLog.PLM.PML

Figure 7: Process monitor event log (Source: own material)

3.11 Tamper Protection

Tamper Protection works by locking the Microsoft Defender Antivirus to its secure, default values. This prevents security settings from being changed through methods like, changing settings through PowerShell, Configuring settings in the Registry Editor and editing or removing security settings through the use of Group Policy. The reason it is advised to use Tamper Protection is because in the case of a cyber attack the bad actors may try to disable security features,

such as for example antivirus protection. When Tamper Protection is on, malicious apps are prevented from disabling security features such as virus and threat protection, real-time protection, behavior monitoring, antivirus, cloud-delivered protection, security intelligence updates and automatic actions on detected threats [20].

3.12 Reputation-based protection

Reputation-based protection helps to protect against potentially unwanted applications, which is software that can make your machine run slower or install other harmful software. In the Windows Security settings you can choose to block either apps, downloads or both. "Block downloads" search for potentially unwanted applications as they are being downloaded, this feature only works in the Microsoft Edge browser. "Block apps" help detect potentially unwanted applications that has already been installed or downloaded [4].

3.13 Windows Defender Application Control

WDAC is used by enterprises to have the ability to restrict the apps users are able to use. The user are only able to run approved apps, this functionality works great with the combination of HVCI. WDAC is available on Windows 10, 11, Server 2016 and newer. HVCI will ensure that only approved processes get privileges in memory, and WDAC will restrict which applications are allowed to run. WDAC policies is enforced by the Windows kernel[31]. The policies is applied early in the boot process, before any other third party applications and much of the OS code. While using WDAC you are able to set application control policies for code that run in user mode and kernel mode, including hardware and software drivers. This includes some code that run as part of the Windows OS.

3.14 Applocker

Applocker have much in common with WDAC, it prevents end-users running unapproved software on the Windows machines in their organization. Applocker does not get any new features anymore, that is why it is recommended to use WDAC instead. But in some cases it is best to use Applocker. For example if it is needed to apply policies to older Windows OSs, apply different policies to different groups or users that is going to share the same computers[6]. Applocker is not supported on Server Core. Applocker can be used in parallel with WDAC to have the ability to apply group specific rules for shared devices. It is recommended to only use Applocker as an compliment to WDAC.

3.15 Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is an enterprise security tool designed to detect, investigate, prevent and respond to advanced threats. There are multiple security features in Defender for Endpoint. These security features are antivirus, anti-malware, threat protection, cloud access security broker, identity and access management and information protection including Data Loss Prevention (DLP).

Microsoft Defender Antivirus is built into Windows and works together with Defender for Endpoint to administer protection in the cloud and on your device. Microsoft Defender Antivirus has three different modes, active mode, passive mode and disabled/uninstalled. When it is in active mode Microsoft Defender Antivirus is being used as the main antivirus application on the endpoint. When in active mode it will scan files, remediate threats and detect threats that is listed in the organizations security reports. When Microsoft Defender Antivirus is in passive mode the files are scanned, but threats are only detected and reported. If threats are found in passive mode they will not be remediated by Microsoft Defender Antivirus.

Data Loss Prevention (DLP) helps to prevent accidental or unintentional sharing of sensitive data. DLP can examine both files and email messages for sensitive data like for example a credit card number. When using DLP it can detect sensitive data and take various actions like logging the event for auditing purposes, blocking the file sharing or the email from taking place or give a warning to the end user that is sharing the file or sending the email.

Microsoft Defender Antivirus has some compatibility with other non-Microsoft antivirus/antimalware products, Microsoft Defender Antivirus can then run in passive mode. Whether it is compatible with other non-Microsoft antivirus/antimalware will depend on what kind of operating system is used and if the device is onboarded to Defender for Endpoint.

Some negative sides with Microsoft Defender for Endpoint is that if it is installed with the default configurations by Microsoft it will disable other anti-malware and Endpoint detection and response (EDR) software that is present on the endpoint. Another negative thing is that DLP and automatic label classification which is some of Defender for Endpoint's most attractive features only work on Microsoft documents.

3.16 Differences between Server 2022 and Server 2019

The differences in the two operating systems was greater when Server 2022 was released, but Server 2019 have had many updates and now contain much of the same features as Server 2022.

Server type → Security feature ↓	2019	2022
HVCI	Available	Available
VBS	Available	Available
Tamper protection	Available	Available
DMA protection	Available	Available
TPM 2.0	Not required	Required*
Hardware-enforced Stack Protection	Not available	Available
UEFI secure boot	Available	Available
Secure Launch	Available	Available
Reputation based protection	Can be configured	Available
SMB over QUIC	Not available	Only Datacenter Azure edition
TLS 1.3	Can be configured	Configured by default

3.17 Frameworks

This section contains the various security features mentioned earlier and what section they help to fulfill in the frameworks below [33],[41],[52]. These frameworks were requested by the client.

3.17.1 Helsenormen for informasjonssikkerhet i omsorg- og helsesektor

Secure Boot:

4.2.1, 5.4.1

Trusted Boot:

4.2.1, 5.4.1

Early-launch antimalware drivers:

4.2.1, 5.4.1

Measured boot:

4.2.1, 5.4.1

System Guard:

4.2.1, 5.4.1

Virtualization-Based Security:

4.2.1, 5.4.1

SMB over QUIC:

5.4.1, 5.5.1

Sysmon:

3.2, 4.2.1, 5.4.1, 5.4.4, 5.5.5, 5.8.1

Tamper Protection:

3.2, 4.2.1, 5.4.1

Reputation-based protection:

4.2.1, 5.4.1

Windows Defender Application Control and Applocker:

3.2, 4.2.1, 5.4.1

Microsoft Defender For Endpoint:

4.2.1, 5.4.1

3.17.2 ISO/IEC 27002:2022

Secure Boot:

5.7, 8.1, 8.7, 8.8

Trusted Boot:

5.7, 8.1, 8.7, 8.8

Early-launch antimalware drivers:

5.7, 8.1, 8.7, 8.8

Measured boot:

5.7, 8.1, 8.7, 8.8

System Guard:

5.7, 8.1, 8.7, 8.8

Virtualization-Based Security:

5.7, 8.1, 8.7, 8.8

SMB over QUIC:

5.7, 5.14, 8.1, 8.11, 8.12, 8.20, 8.24

Sysmon:

5.7, 5.10, 5.15, 5.16, 5.24, 5.26, 5.28, 8.3, 8.4, 8.5, 8.8, 8.9, 8.15, 8.16, 8.18, 8.21

Tamper Protection:

5.2, 5.3, 5.7, 5.15, 8.1, 8.7, 8.8, 8.9

Reputation-based protection:

5.3, 5.7, 5.15, 8.1, 8.7, 8.8, 8.18, 8.19

Windows Defender Application Control and Applocker:

5.2, 5.3, 5.7, 5.10, 5.12, 5.15, 5.18, 5.31, 5.33, 8.1, 8.3, 8.5, 8.7, 8.8, 8.9, 8.12, 8.18, 8.19, 8.23

Microsoft Defender For Endpoint:

5.7, 5.26, 5.28, 8.1, 8.7, 8.8, 8.15, 8.16, 8.19

3.17.3 NSM Grunnprinsipper for IKT-sikkerhet 2.0

Secure Boot:

2.3.4

Trusted Boot:

2.3.4

Early-launch antimalware drivers:

2.3.4

Measured boot:

2.3.4

System Guard:

2.3.4

Virtualization-Based Security:

2.3.4

SMB over QUIC:

2.3.4, 2.4.2, 2.7.1, 2.7.2, 2.7.4

Sysmon:

2.3.4, 2.3.10, 3.1.3, 3.2.1, 4.2.1, 4.2.2, 4.3.3

Tamper Protection:

2.3.4, 2.6.4

Reputation-based protection:

2.1.3, 2.3.2, 2.3.4

Windows Defender Application Control and Applocker:

2.1.4, 2.3.2, 2.3.4, 2.6.1, 2.6.4, 2.6.5, 3.2.6

Microsoft Defender For Endpoint:

2.3.2, 2.3.4, 3.1.1, 3.1.3, 3.2.1

Chapter 4

4 Azure security features

4.1 Azure Sentinel

Azure Sentinel is a cloud native security information and event management (SIEM), and Security orchestration, automation and response (SOAR) solution. Azure Sentinel is automatically scaling with the number of nodes it is collecting data from. Azure Sentinel is able to collect data from on premise as well as in the cloud. The data collected in Azure Sentinel is configured by the organizations preferences, usually it collects telemetry from Linux and Windows machines, and it can collect data from firewall systems, files and other apps. There is many built-in analytic rules and it is possible to create more and manage them.

Azure Sentinel is able to learn from the system, and alert if irregularities appear. There are many possibilities for automation in Azure Sentinel with the use of playbooks. Playbooks is where the automation in Azure Sentinel is created and managed. This can be made with Azure Logic Apps Designer or using JSON programming language. There is also many predefined playbook templates which can be configured.

When rules are triggered or anomalies appear, an incident is created. These incidents must be investigated by an administrator. Azure Sentinel can visualize these incidents in the whole system. This will help determine the scope and impact of the incident if there are multiple nodes impacted or multiple related incidents. [9]

4.2 Azure AD Identity Protection

Azure Active Directory Identity Protection collects information from a user when the user sign in. The information is then analyzed and a risk score is calculated. This risk score is based on the probability that the sign-in was performed by someone else than the user. Some of the risks Identity Protection processes to calculate the risk score, is unfamiliar sign-ins, this is compared to earlier logins. The risk score will increase if for example the user connects from an anonymous IP address, this can be from the Tor network or using an anonymous VPN. If the user has known leaked login credentials, or if the user has tried many password combinations, the risk score will also increase. Some of the risks are detected real time (within 5-10 min) and others are detected "offline" and reported within 48 hours.

Identity Protection categorizes the different risks in three tiers: low, medium and high. These risks are then reported in to three separate reports, the first is

Risky users, this can be users that have a risk history. It can also be a user that have accessed many sensitive files that is new to the user. The administrators will then be provided with information regarding the risky user and possible actions to take. Second is Risky sign-ins, this can be a sign-in using a VPN or from another country. The administrators will be provided with information from the device that signed in, this can be information regarding the device, application, location and more. The administrator is able to confirm the sign-in as safe or compromised. The last category is Risk detection this can be sign-in attempts and from what IP address and location the sign-in attempt was from. This category can be triggered at the same time as the others, depending on what the incident was. The administrator can then return to the user's risk or sign-ins report to take actions, as this category mainly contain more information about risks regarding the other categories [13].

The risk data from Identity Protection can be exported to other tools for logging or to the organizations SIEM. Using their preferred SIEM solution, they are able to further investigate the incident and take further actions[27].

4.3 Azure AD Privileged Identity Management

Privileged Identity Management (PIM) is a feature in Azure AD that makes it possible to monitor, control and manage access to important resources/data that is within organization. The reason to use PIM is because it will reduce the likelihood of an authorized user unintentionally impacting a sensitive resource or malicious actor getting access. PIM mitigate these risks by providing time-based and approval-based role activation. By using time-based and approval-based role activation it will reduce the risk of unnecessary, excessive or misused access permissions on important resources [26].

4.4 Microsoft Defender for Cloud

Microsoft Defender for Cloud is a tool for threat protection and posture management. It will help strengthen the security posture of cloud resources. Defender for Cloud will help with protecting workloads in Azure, hybrid and other cloud platforms [28].

Defender for Cloud fulfill three important security requirements, these are Continuous vulnerability assessment, Security hardening and defending workloads and resources. This will help with the Cloud security posture management (CSPM) by providing better visibility and hardening guidance to help improve the security effectively and efficiently. Defender for Cloud identifies the risk level based on a secure score, higher secure score means lower identified risk level. The secure score is a score that is calculated by continually assessing the resources, subscriptions and organization for security issues. Another import-

ant part of cloud security is Cloud Workload Protection (CWP), CWP works by helping detect, analyze and resolve threats [18].

4.5 Multi-factor Authentication (MFA)

multi-factor authentication adds another level of security while signing in to an account, this is important because if an attacker gets access to an account severe damage can be done to the organization. When enabled MFA will require the user to be authenticated with at least two of the following methods:

- Something only the user knows, often a password or passphrase.
- Something the user have, often another device like phone or a key.
- Something user specific, biometrics often fingerprint or facial recognition.

Microsoft Azure provides multiple options to each of the authentication methods, the users is able to edit or add the preferred authentication methods. The administrators are able to set password requirements for the passwords the user chooses. This is important because simple passwords can be easily brute-forced, but with MFA the attacker is not able to get access with only a password.

4.6 Key Vault

Azure Key Vault is a service for securely storing and accessing keys, secrets and certificates. Key Vault supports two types of containers. One is software and hardware security module backed keys, certificates and secrets. The other is vaults and managed hardware security module pools. Key Vault uses transport layer security (TLS) protocol to protect the data when traveling between Key Vault and clients. Key Vault also uses "Perfect Forward Secrecy" to protect connections between customers client systems and Microsoft cloud services by unique keys. The connections also use RSA-based 2048-bit encryption key length. The combination of "Perfect Forward Secrecy" and RSA-based 2048-bit encryption keys makes it very difficult for someone to intercept or access the data in transit[8].

4.7 Frameworks

This section contains the various security features mentioned earlier and what section they help to fulfill, in the frameworks below [33],[41],[52]. These frameworks was requested by the client.

4.7.1 Helsenormen for informasjonssikkerhet i omsorg- og helsesektor

Microsoft Sentinel:

3.3, 4.2.1, 5.4.1, 5.4.4, 5.8.1

Azure AD Identity Protection:

3.2, 4.2.1, 5.2.1, 5.2.2, 5.2.3, 5.3.3, 5.4.1, 5.4.4

Azure AD Privileged Identity Management:

3.2, 4.2.1, 5.2.1, 5.1.3, 5.2.2, 5.2.3, 5.3.3, 5.4.1, 5.4.4

Microsoft Defender for Cloud:

4.2.1, 5.4.1, 5.4.4, 5.8.1

Multi-factor Authentication (MFA):

3.2, 4.2.1, 5.2.1, 5.2.2, 5.2.3, 5.3.3, 5.4.1, 5.4.4

Key Vault:

4.2.1, 5.3.3, 5.3.5, 5.4.1, 5.4.4

4.7.2 ISO/IEC 27002:2022

Microsoft Sentinel:

5.3, 5.7, 5.10, 5.15, 5.24, 5.26, 5.28, 5.37, 8.1, 8.7, 8.8, 8.9, 8.12, 8.15, 8.16, 8.19

Azure AD Identity Protection:

5.2, 5.3, 5.7, 5.10, 5.12, 5.15, 5.16, 5.17, 5.18, 5.26, 5.28, 5.33, 8.1, 8.2, 8.3, 8.5, 8.10, 8.15, 8.16

Azure AD Privileged Identity Management:

5.2, 5.3, 5.7, 5.10, 5.12, 5.15, 5.16, 5.17, 5.18, 5.33, 8.1, 8.2, 8.3, 8.4, 8.5, 8.9, 8.10, 8.32

Microsoft Defender for Cloud:

5.3, 5.7, 5.15, 5.24, 5.26, 5.28, 8.1, 8.7, 8.8, 8.9, 8.12, 8.15, 8.16, 8.19, 8.20, 8.27

Multi-factor Authentication (MFA):

5.3, 5.7, 5.12, 5.15, 5.16, 5.17, 5.18, 8.1, 8.2, 8.3, 8.5

Key Vault:

5.7, 5.14, 5.17, 5.18, 5.31, 8.1, 8.3, 8.5, 8.10, 8.11, 8.24

4.7.3 NSM Grunnprinsipper for IKT-sikkerhet 2.0

Microsoft Sentinel:

2.3.4, 2.3.10, 3.1.1, 3.1.2, 3.1.3, 3.2.1, 3.3, 4.2.1, 4.2.2, 4.3.1, 4.3.3, 4.4.2

Azure AD Identity Protection:

2.3.4, 2.6.1, 2.6.2, 3.2.1, 3.2.6

Azure AD Privileged Identity Management:

1.3.1, 1.3.2, 1.3.3, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 3.2.6

Microsoft Defender for Cloud:

2.3.1, 2.3.3, 2.3.4, 2.3.10, 2.4, 2.7.2, 3.1.1, 3.1.2, 3.1.3, 3.2.1, 4.2.1, 4.2.2, 4.3.1

Multi-factor Authentication (MFA):

2.3.4, 2.3.7, 2.6.7

Key Vault:

2.3.4, 2.3.6, 2.3.7, 2.6.6, 2.7.1, 2.7.2

Chapter 5

5 Testing and Demonstration

In this chapter it is shown how the group have set up the test environment in Microsoft Azure cloud. As well as some test that demonstrates how the different security features is configured and set up. There is also some tests that checks if the security features are working properly. At last there is some performance tests that compare different security configurations on Windows Server 2022 and Windows Server 2019.

5.1 Setting up test environment Azure

Cloud Shell was used to set up the Microsoft Azure Cloud test environment because of the opportunities for automation.

A Resource group is required to be able to create a VM in Microsoft Azure. The following command creates a new resource group named "Gruppe124" in the "norwayeast" location, this can be viewed in Fig. 8.

```
az group create -l norwayeast -n Gruppe124
```

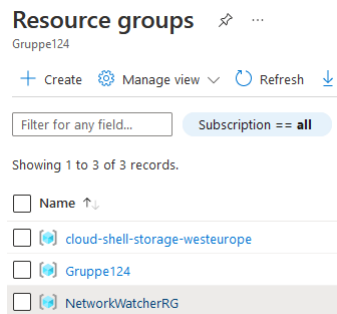


Figure 8: Resource group is made (Source: own material)

To create the VM used in the tests, the following command was used. This command created a VM with Trusted launch, Secure Boot and TPM enabled. The VM was created in the previously created Resource group "Gruppe124" and can then be seen in this Resource group in the cloud portal as seen in Fig. 9.

```

az vm create --resource-group Gruppe124 `
--name WS2022 `
--image MicrosoftWindowsServer:WindowsServer:2022... `
--public-ip-sku Standard `
--security-type TrustedLaunch `
--enable-secure-boot true `
--enable-vtpm true `
--admin-username gruppe124

```

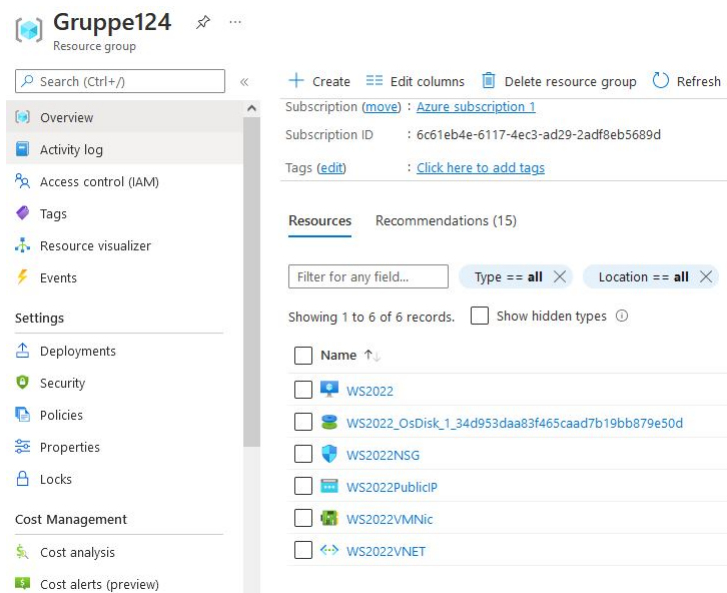


Figure 9: VM is made inside the resource group (Source: own material)

After the VM was created, Remote Desktop was used to turn on the remaining security features that was not doable from the Microsoft Azure portal.

The following command was used to enable Controlled Folder Access.

```
Set-MpPreference -EnableControlledFolderAccess Enabled
```

The following command will display information about the TPM of the current machine, including if it is enabled.

```
Get-TPM
```

Fig. 10 shows that TPM is both present and enabled.

```

Administrator: Windows PowerShell
PS C:\Users\gruppe124> Get-TPM

TpmPresent           : True
TpmReady             : True
TpmEnabled           : True
TpmActivated         : True
TpmOwned             : True
RestartPending      : False
ManufacturerId       : 1297303124
ManufacturerIdTxt    : MSFT
ManufacturerVersion  : 8224.786.18.0
ManufacturerVersionFull120 : 8224.786.18.0

ManagedAuthLevel    : Full
OwnerAuth            : p21esEaHOS11fmYajPj3baGrfMU=
OwnerClearDisabled   : False
AutoProvisioning     : Enabled
LockedOut            : False
LockoutHealTime      : 10 minutes
LockoutCount         : 0
LockoutMax           : 31
SelfTest             : {}

PS C:\Users\gruppe124>

```


Figure 10: Checking TPM status (Source: own material)

Boot DMA protection and System guard is not supported on VMs in Azure. The requirements for Secured-core is viewable in the security section of Windows Admin Center on the server, here it is possible to see what requirements are met for Secure-core server certification. In Fig. 11 it can be seen that all possible requirements for Secure-core in a Azure Cloud hosted VM is met.

Security PREVIEW

Summary Protection history **Secured-core**

[What is Secured-core server?](#)

 Your device meets only 4 of 6 requirements for Secured-core Server.

Enable Disable







Security Feature	Status
Hypervisor Enforced Code Integrity (HVCI)	 On
Boot DMA Protection	 Not supported
System Guard	 Not supported
Secure Boot	 On
Virtualization-based Security (VBS)	 On
Trusted Platform Module 2.0 (TPM 2.0)	 On

Figure 11: Secured-core overview (Source: own material)

5.1.1 Sysmon configuration file

SwiftOnSecurity's configuration file was used to set up Sysmon. The configuration file is listed in the appendix. To enable Sysmon the following command was ran inside the SysinternalsSuite folder. The SysinternalsSuite folder can be downloaded from Microsoft [45].

```
Sysmon.exe -accepteula -i "PATH TO CONFIGURATION FILE"
```

When the previous command is ran successfully the output should look like Fig. 12.

```
C:\Users\Administrator\Downloads\SysinternalsSuite>Sysmon.exe -accepteula -i C:\Users\Administrator\Downloads\sysmon-config-master\sysmonconfig-export.xml

System Monitor v13.33 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved
.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.81
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.

C:\Users\Administrator\Downloads\SysinternalsSuite>
```

Figure 12: Sysmon setup (Source: own material)

5.2 Windows Testing and Demonstration

5.2.1 Sysmon testing and demonstration

The Sysmon logs is viewable in the Event Viewer Applications and is located in Service Log → Microsoft → Windows → Sysmon → Operational. Sysmon logs will look like Fig. 13 in Event Viewer. If Sysmon is configured with a SIEM these events can be found there as well.

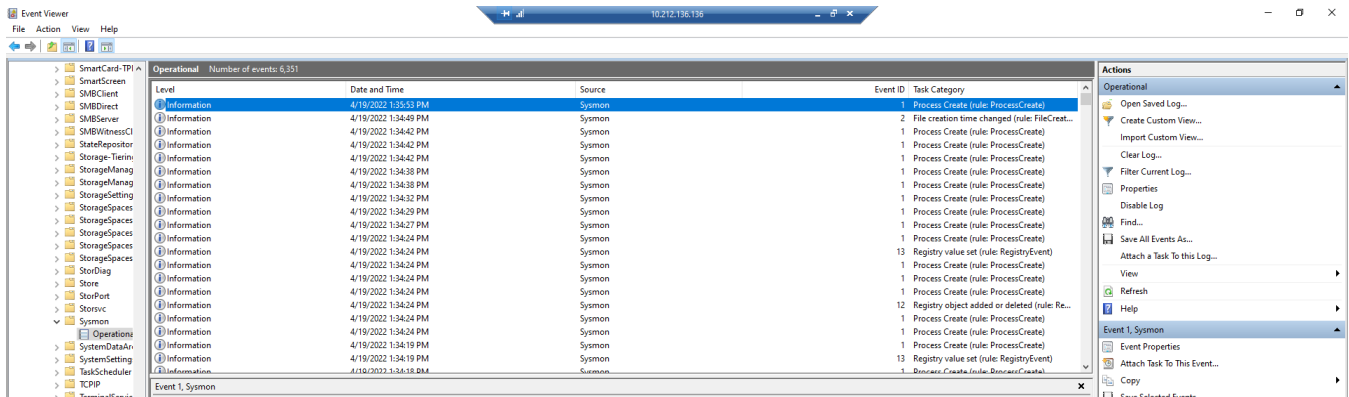


Figure 13: Event Viewer (Source: own material)

Depending on the system and the configuration of Sysmon it can be many events in Event Viewer, but by using the filtering feature in Event Viewer only the events corresponding to the present filter is visible. The filter feature in Event Viewer provides many filtering options, these can be seen in Fig. 14.

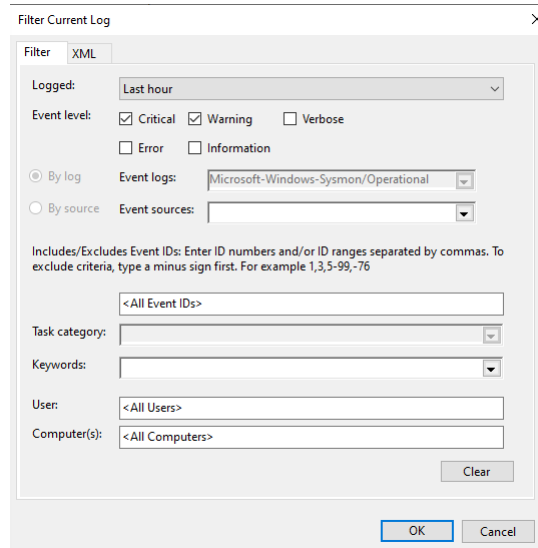


Figure 14: Filtering options for Microsoft Event Viewer (Source: own material)

To test if Sysmon logged events properly, the test user was used to create a process by starting the calculator application. This was then logged by Sysmon, this event can be seen in Fig. 15.

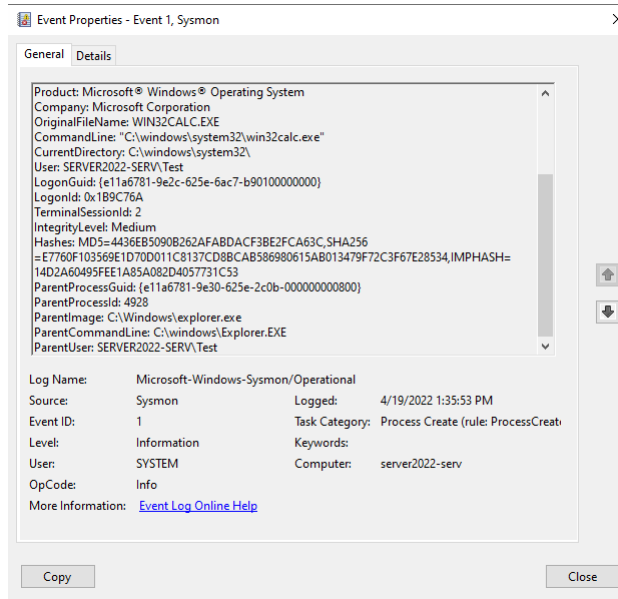


Figure 15: Information about an event(Source: own material)

The event can then be inspected to view all the information provided, it is advised to use a SIEM for this to be able to further investigate and take measures. There is two options for viewing the event in Event Viewer. The first option is Friendly view, it provides all the information in plain text and is easy to read. This is seen in Fig. 16. The second option is XML View, this option provides all the information in XML format and is best suited for exporting to other applications or a SIEM. XML view can be seen in Fig. 17.

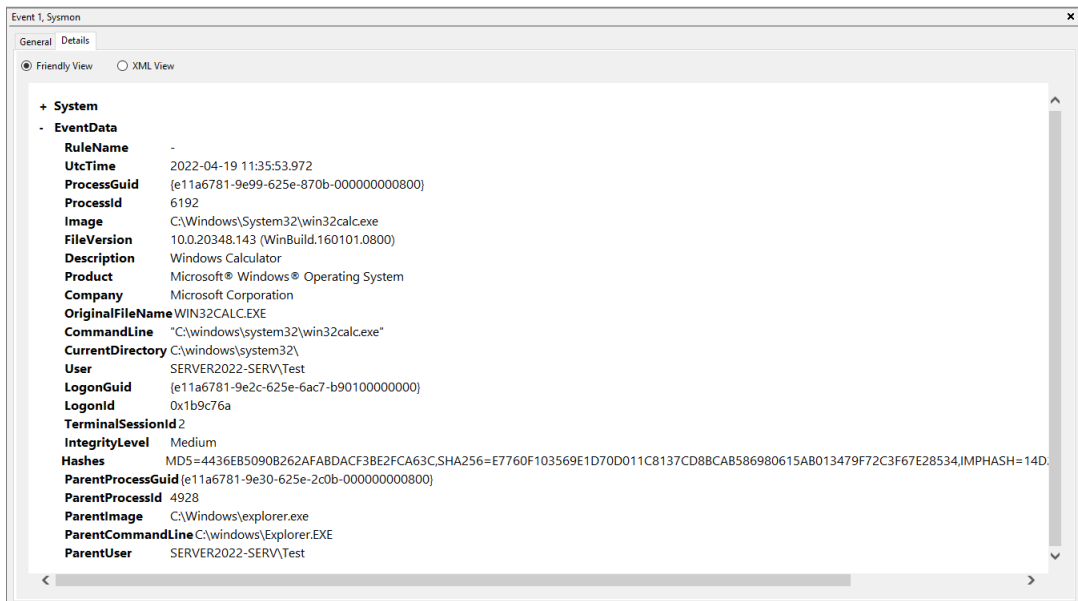
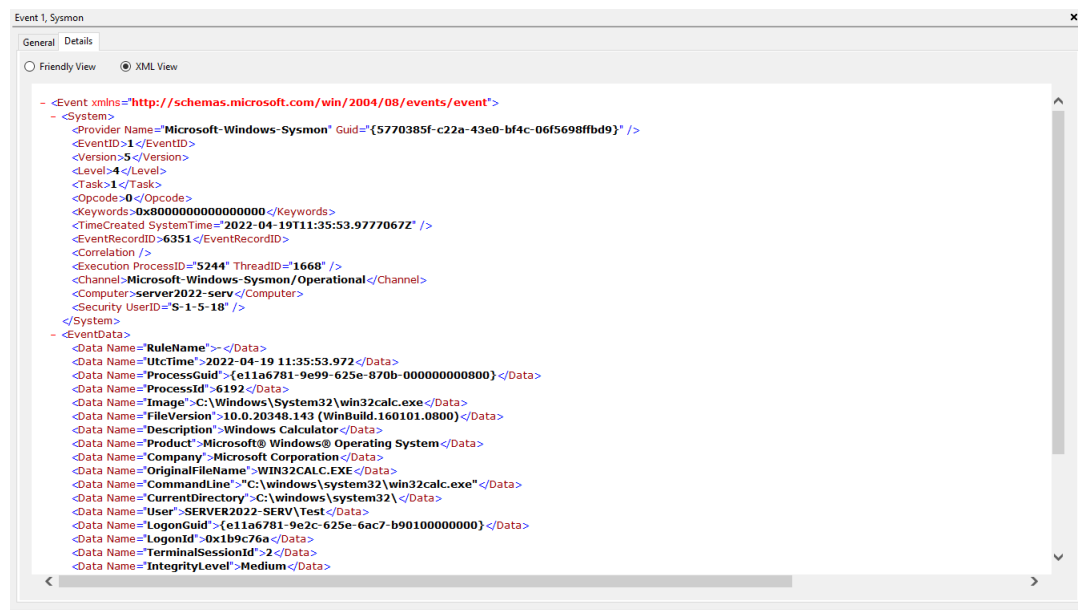


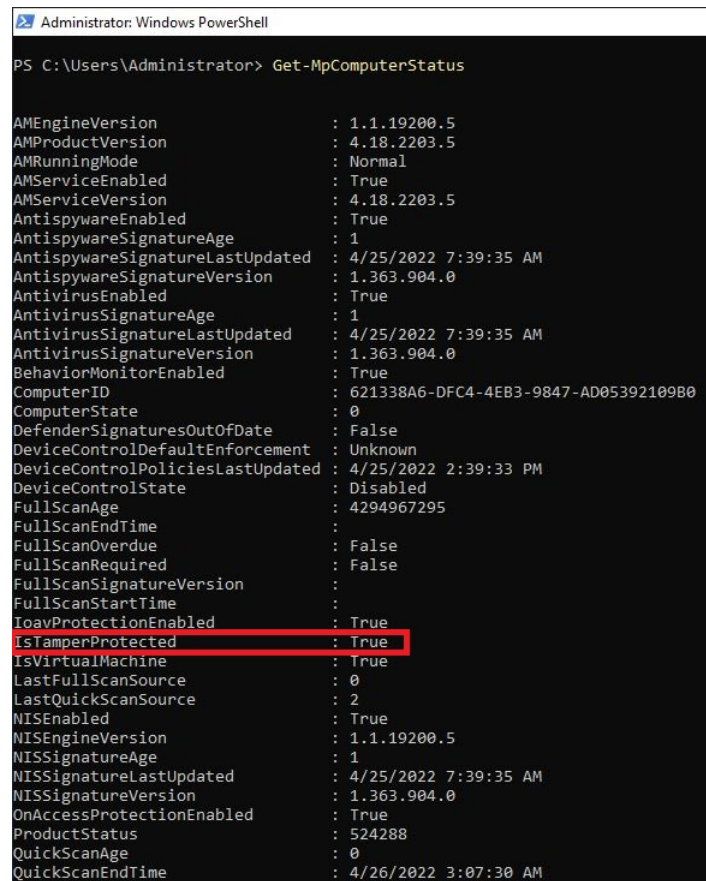
Figure 16: Friendly View (Source: own material)



5.2.2 Tamper Protection testing

To check if Tamper Protection is enabled on the current machine the following command was ran. The output from this command can be viewed in Fig. 18. Tamper protection is on because "IsTamperProtected" is "True".

```
Get-MpComputerStatus
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-MpComputerStatus

AMEngineVersion           : 1.1.19200.5
AMProductVersion          : 4.18.2203.5
AMRunningMode              : Normal
AMServiceEnabled          : True
AMServiceVersion          : 4.18.2203.5
AntispywareEnabled        : True
AntispywareSignatureAge   : 1
AntispywareSignatureLastUpdated : 4/25/2022 7:39:35 AM
AntispywareSignatureVersion : 1.363.904.0
AntivirusEnabled          : True
AntivirusSignatureAge     : 1
AntivirusSignatureLastUpdated : 4/25/2022 7:39:35 AM
AntivirusSignatureVersion : 1.363.904.0
BehaviorMonitorEnabled    : True
ComputerID                : 621338A6-DFC4-4EB3-9847-AD05392109B0
ComputerState              : 0
DefenderSignaturesOutOfDate : False
DeviceControlDefaultEnforcement : Unknown
DeviceControlPoliciesLastUpdated : 4/25/2022 2:39:33 PM
DeviceControlState        : Disabled
FullScanAge                : 4294967295
FullScanEndTime           :
FullScanOverdue            : False
FullScanRequired           : False
FullScanSignatureVersion   :
FullScanStartTime         :
IoavProtectionEnabled      : True
IsTamperProtected         : True
IsVirtualMachine           : True
LastFullScanSource         : 0
LastQuickScanSource        : 2
NISEnabled                 : True
NISEngineVersion           : 1.1.19200.5
NISSignatureAge           : 1
NISSignatureLastUpdated   : 4/25/2022 7:39:35 AM
NISSignatureVersion        : 1.363.904.0
OnAccessProtectionEnabled  : True
ProductStatus              : 524288
QuickScanAge               : 0
QuickScanEndTime          : 4/26/2022 3:07:30 AM
```

Figure 18: Check to see if Tamper Protection is on (Source: own material)

Real-time Monitoring was attempted turned off to test if Tamper Protection was working properly. First the state of Real-time Monitoring was checked using the following command, the output can be viewed in Fig. 19.

Get-mppreference

```

Select Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-mppreference

AllowDatagramProcessingOnWinServer      : False
AllowNetworkProtectionDownLevel        : False
AllowNetworkProtectionOnWinServer      : False
AllowSwitchToAsyncInspection           : False
AttackSurfaceReductionOnlyExclusions   :
AttackSurfaceReductionRules_Actions    :
AttackSurfaceReductionRules_Ids       :
CheckForSignaturesBeforeRunningScan   : False
CloudBlockLevel                        : 0
CloudExtendedTimeout                   : 0
ComputerID                             : 621338A6-DFC4-4EB3-9847-AD05392109B0
ControlledFolderAccessAllowedApplications :
ControlledFolderAccessProtectedFolders :
DefinitionUpdatesChannel              : 0
DisableArchiveScanning                 : False
DisableAutoExclusions                  : False
DisableBehaviorMonitoring               : False
DisableBlockAtFirstSeen                 : False
DisableCatchupFullScan                  : True
DisableCatchupQuickScan                 : True
DisableCpuThrottleOnIdleScans          : True
DisableDatagramProcessing               : False
DisableDnsOverTcpParsing                : False
DisableDnsParsing                       : False
DisableEmailScanning                   : True
DisableFtpParsing                       : False
DisableGradualRelease                   : False
DisableHttpParsing                      : False
DisableInboundConnectionFiltering      : False
DisableIOAVProtection                  : False
DisableNetworkProtectionPerfTelemetry  : False
DisablePrivacyMode                      : False
DisableRdpParsing                       : False
DisableRealtimeMonitoring               : False
DisableRemovableDrivesScanning         : True
DisableRestorePoint                     : True
DisableScanningMappedNetworkDrivesForFullScan : True
DisableScanningNetworkFiles             : False
DisableScriptScanning                  : False
DisableSshParsing                       : False
DisableTDTFeature                       : False

```

Figure 19: DisableRealtimeMonitoring is set to False (Source: own material)

PowerShell was then ran in Administrator, and the following command was used to try and change the state of "DisableRealtimeMonitoring" to "True".

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

After running the command "DisableRealtimeMonitoring" should be set to "True", but because Tamper Protection is turned on it is still set to "False". This can be seen in Fig. 20.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-mp preference

AllowDatagramProcessingOnWinServer      : False
AllowNetworkProtectionDownLevel        : False
AllowNetworkProtectionOnWinServer      : False
AllowSwitchToAsyncInspection           : False
AttackSurfaceReductionOnlyExclusions    :
AttackSurfaceReductionRules_Actions    :
AttackSurfaceReductionRules_Ids        :
CheckForSignaturesBeforeRunningScan    : False
CloudBlockLevel                         : 0
CloudExtendedTimeout                   : 0
ComputerID                              : 621338A6-DFC4-4EB3-9847-AD05392109B0
ControlledFolderAccessAllowedApplications :
ControlledFolderAccessProtectedFolders :
DefinitionUpdatesChannel               : 0
DisableArchiveScanning                 : False
DisableAutoExclusions                  : False
DisableBehaviorMonitoring               : False
DisableBlockAtFirstSeen                : False
DisableCatchupFullScan                 : True
DisableCatchupQuickScan                : True
DisableCpuThrottleOnIdleScans          : True
DisableDatagramProcessing               : False
DisableDnsOverTcpParsing                : False
DisableDnsParsing                      : False
DisableEmailScanning                   : True
DisableFtpParsing                      : False
DisableGradualRelease                  : False
DisableHttpParsing                     : False
DisableInboundConnectionFiltering      : False
DisableIOAVProtection                  : False
DisableNetworkProtectionPerfTelemetry   : False
DisablePrivacyMode                     : False
DisableRdpParsing                      : False
DisableRealtimeMonitoring              : False
DisableRemovableDriveScanning          : True
DisableRestorePoint                    : True
DisableScanningMappedNetworkDrivesForFullScan : True
DisableScanningNetworkFiles            : False
DisableScriptScanning                  : False
DisableSshParsing                      : False
DisableTDTFeature                      : False
```

Figure 20: DisableRealtimeMonitoring is still set to False (Source: own material)

5.2.3 Credential Guard

”Device Guard and Credential Guard hardware readiness tool” was used to enable Credential Guard, it can be downloaded from [43]. The following command was used to enable Credential Guard, the output of this command can be viewed in Fig. 21.

```
.\DG_Readiness_Tool_v3.6.ps1 -enable -CG
```

```

Administrator: Windows PowerShell
PS C:\Users\gruppe124\Downloads\dgreadiness_v3.6\dgreadiness_v3.6> .\DG_Readiness_Tool_v3.6.ps1 -enable -CG
#####
Readiness Tool Version 3.4 Release.
Tool to check if your device is capable to run Device Guard and Credential Guard.
#####
Running on a Virtual Machine. DG/CG is supported only if both guest VM and host machine are running with windows 10, ver
sion 1703 or later with English localization.
#####
OS and Hardware requirements for enabling Device Guard and Credential Guard
 1. OS SKUs: Available only on these OS Skus - Enterprise, Server, Education, Enterprise IoT, Pro, and Home
 2. Hardware: Recent hardware that supports virtualization extension with SLAT
To learn more please visit: https://aka.ms/dgwhcr
#####
Enabling Device Guard and Credential Guard
Setting RegKeys to enable DG/CG
Enabling Hyper-V and IOMMU
Enabling Hyper-V and IOMMU successful
Please reboot the machine, for settings to be applied.

```

Figure 21: Turning on Credential Guard (Source: own material)

The following command can be used to check if Credential Guard is turned on. Fig. 22 show the output from the previous command. It can be seen that "RequiredSecurityProperties" and "SecurityServicesConfigured" is set to "1" and "2". "1" means that HVCI is configured and running. "2" means that Credential Guard is configured and running.

```
Get-CimInstance -ClassName Win32_DeviceGuard -Namespace '
root\Microsoft\Windows\DeviceGuard
```

```

PS C:\Users\gruppe124\Downloads\dgreadiness_v3.6\dgreadiness_v3.6> Get-CimInstance -ClassName Win32_DeviceGuard -Namespace
root\Microsoft\Windows\DeviceGuard

AvailableSecurityProperties           : {1, 2, 5, 7}
CodeIntegrityPolicyEnforcementStatus : 2
InstanceIdentifier                   : 4ff40742-2649-41b8-bdd1-e80fad1cce80
RequiredSecurityProperties           : {1, 2}
SecurityServicesConfigured           : {1, 2}
SecurityServicesRunning              : {2}
UsermodeCodeIntegrityPolicyEnforcementStatus : 0
Version                              : 1.0
VirtualizationBasedSecurityStatus    : 2
VirtualMachineIsolation              : False
VirtualMachineIsolationProperties    : {0}
PSComputerName                       :

```

Figure 22: Check if it is active (Source: own material)

5.3 Azure Testing and Demonstration

5.3.1 Sentinel Testing

The first task needed to set up Microsoft Sentinel was to create a workspace. The workspace was created by navigating to "Home → Microsoft Sentinel", this is shown in Fig. 23.



Figure 23: Create a new workspace (Source: own material)

To create a new Log Analytics workspace it is necessary to specify which resource group the workspace should be included in, and the name of the workspace. It should also be specified which region the workspace should be created. This can be seen in Fig. 24.

[Home](#) > [Microsoft Sentinel](#) > [Add Microsoft Sentinel to a workspace](#) >

Create Log Analytics workspace ...

[Basics](#) [Tags](#) [Review + Create](#)

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) ×

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ	<input type="text" value="Azure subscription 1"/>
Resource group * ⓘ	<input type="text" value="Gruppe124"/>

[Create new](#)

Instance details

Name * ⓘ	<input type="text" value="Gruppe124Workspace"/>
Region * ⓘ	<input type="text" value="Norway East"/>

[Review + Create](#)

[« Previous](#)

[Next : Tags >](#)

Figure 24: Create Log Analytics workspace (Source: own material)

To enable Microsoft Sentinel it was needed to select the Log Analytics workspace location, Log Analytics workspace, Automation account subscription and Automation account. This can be seen in Fig. 25

Desired State Configuration Management

Enable consistent control and compliance of this VM with Desired State Configuration.

This service is included with Azure virtual machines and Azure Arc machines. You only pay for logs stored in Log Analytics.

This service requires a Log Analytics workspace and an Automation account. You can use your existing workspace and account or let us configure the nearest workspace and account for use.

Log Analytics workspace location ⓘ
 Norway East

Log Analytics workspace ⓘ
 Gruppe124Workspace

Automation account subscription ⓘ
 Azure subscription 1

Automation account ⓘ
 Create Automation account...

[Enable](#)

Figure 25: Enable Microsoft Sentinel (Own material)

The next step was to connect the VM to the Log Analytics workspace so that Microsoft Sentinel is able to detect the VM, This can be seen in Fig. 26 and Fig. 27.

WS2022 ...
 Virtual machine

[Connect](#) [Disconnect](#) [Refresh](#)

i Not connected

Status
 Not connected

Workspace Name
 None

Message
 VM is not connected to Log Analytics.

Figure 26: Connect the VM server to the Log Analytics workspace (Source: own material)

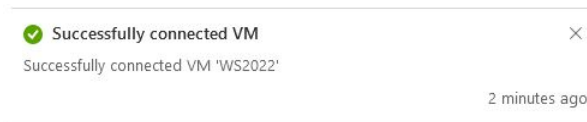


Figure 27: Successfully connected VM (Source: own material)

The next task was to connect Microsoft Sentinel and Microsoft Defender for cloud, to do this the first step was to navigate to "Data connectors" and search for Microsoft Defender for Cloud. This can be seen in Fig. 28 and Fig. 29.

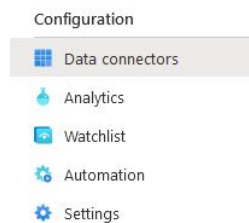


Figure 28: Data connectors (Source: own material)

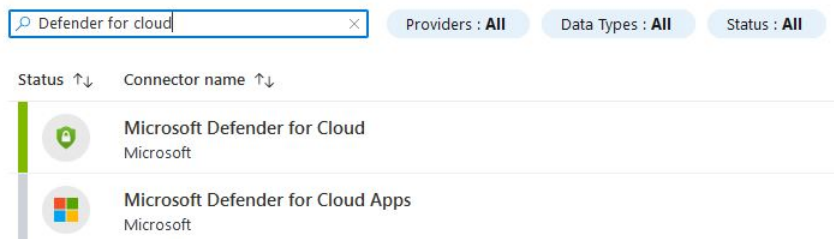


Figure 29: Search Defender for Cloud (Source: own material)

After finding Microsoft Defender for Cloud in the connector page, the next objective was to connect and enable Bi-directional sync. This allows different security alerts in Microsoft Defender for Cloud to appear as incidents in Microsoft Sentinel. How to open the connector page and enable Bi-directional sync can be seen in Fig. 30 and Fig. 31.

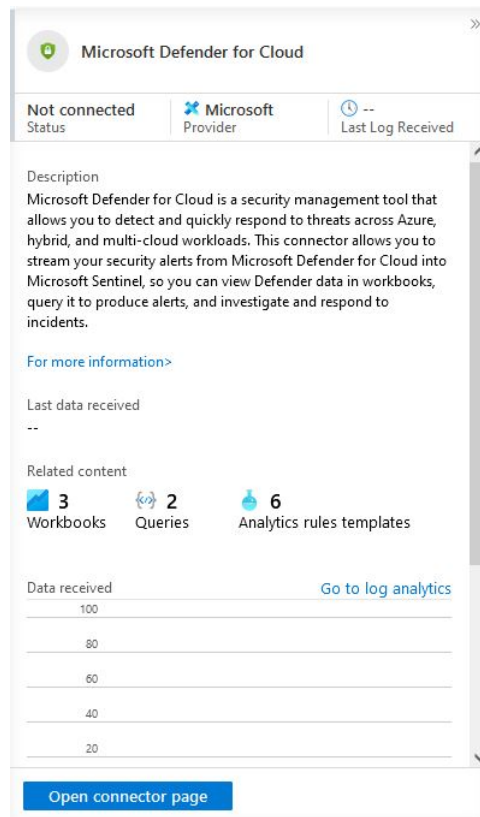


Figure 30: Open connector page (Source: own material)



Configuration

Connect Microsoft Defender for Cloud to Microsoft Sentinel

Mark the check box of each Azure subscription whose alerts you want to import into Microsoft Sentinel, then select **Connect** above

The connector can be enabled only on subscriptions that have at least one Microsoft Defender plan enabled in Microsoft Defender subscription.

[Connect](#) | [Disconnect](#) | [Enable bi-directional sync](#) | [Disable bi-directional sync](#) | [Enable Microsoft Defender](#)

<input checked="" type="checkbox"/> Subscription ↑↓	Status	Bi-directional sync
<input checked="" type="checkbox"/> Azure subscription 1	<input checked="" type="checkbox"/> Connected	<input checked="" type="checkbox"/> Enabled

Figure 31: Configuring connection (Source: own material)

The next task was to test if the connection between Microsoft Sentinel and Microsoft Defender for Cloud was working like it was supposed to. To test this one can run the "Sample alerts" in Microsoft Defender for cloud and see if these alerts appear as incidents in Microsoft Sentinel. The "Sample alerts" can be found under the "Security alerts" tab in Microsoft Defender for Cloud. This can be seen in Fig. 32 and Fig. 33.

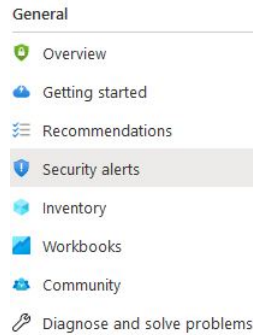


Figure 32: Security alerts (Source: own material)



Figure 33: Sample alerts (Source: own material)

After the "Sample alerts" was used the alerts showed up in Microsoft Defender for cloud, this is shown in Fig. 34. The alerts show Severity, Alert title, Affected resource, Activity start time and MITRE ATT&CK tactics.

<input type="checkbox"/> Severity ↑↓	Alert title ↑↓	Affected resource ↑↓	Activity start time (UTC+2) ↑↓	MITRE ATT&CK® tactics
<input type="checkbox"/> High	Suspicious WordPress theme invoc... Sample alert	Sample-App	04/27/22, 12:17 PM	
<input type="checkbox"/> High	Phishing content hosted on Azure ... Sample alert	Sample-App	04/27/22, 12:17 PM	Collection
<input type="checkbox"/> High	Potential SQL Brute Force attempt Sample alert	Sample-DB	04/27/22, 12:16 PM	Pre-attack
<input type="checkbox"/> High	Attempted logon by a potentially h... Sample alert	Sample-DB	04/27/22, 12:16 PM	Pre-attack
<input type="checkbox"/> High	Potential SQL Injection Sample alert	Sample-DB	04/27/22, 12:16 PM	
<input type="checkbox"/> High	Unusual export location Sample alert	Sample-DB	04/27/22, 12:16 PM	Exfiltration
<input type="checkbox"/> High	Access from a Tor exit node to a st... Sample alert	Sample-Storage	04/27/22, 12:16 PM	Pre-attack
<input type="checkbox"/> High	Unusual amount of data extracted f... Sample alert	Sample-Storage	04/27/22, 12:16 PM	Exfiltration
<input type="checkbox"/> High	Digital currency mining related beh... Sample alert	Sample-VM	04/27/22, 12:16 PM	Execution
<input type="checkbox"/> High	Detected suspicious file cleanup co... Sample alert	Sample-VM	04/27/22, 12:16 PM	Defense Evasion
<input type="checkbox"/> High	Detected Petya ransomware indicat... Sample alert	Sample-VM	04/27/22, 12:16 PM	Execution

Figure 34: Sample alerts (Source: own material)

The last thing that was necessary to check was if the Bi-directional sync was working. Then see if the alerts appeared as incidents in Microsoft Sentinel. The incidents appeared like they where supposed to, this can be seen in Fig. 35.

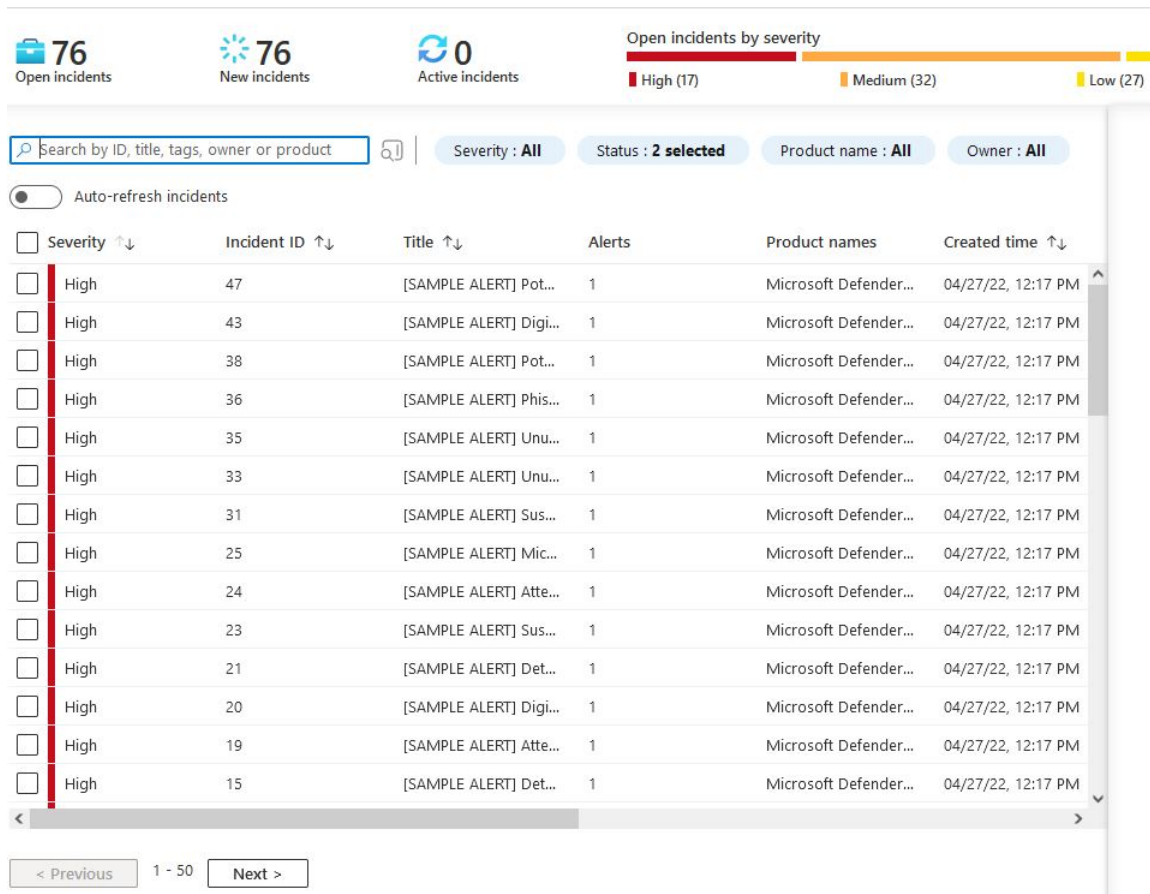


Figure 35: Overview over incidents (Source: own material)

5.4 Performance test

The performance test that was used wrote one million files of 100kb each to the disk. The client requested a performance test that wrote files to the disk, this is why this type of performance test was used [49]. The script was ran through "PSScriptAnalyzer" to make sure it was optimized. The same VM size configuration was used on all tests: Standard D4ads v5 (4 vcpus, 16 GiB memory).

```
Param(  
    [string]$fileName,  
    $fileCount = 1000000  
)  
$fileSize = 102400  
for ($i = 1; $i -le $fileCount; $i++) {  
    $outputFileName = "C:\Users\Gruppe124\test\$fileName.$i"  
    $file = [System.IO.File]::Create($outputFileName)  
    $file.SetLength($fileSize)  
    $file.Close()  
}
```

5.4.1 Windows Server 2022

The first test that was ran used the default windows server 2022 configuration. There was not done any changes to the security configuration. In Fig. 36 is the results of the test.

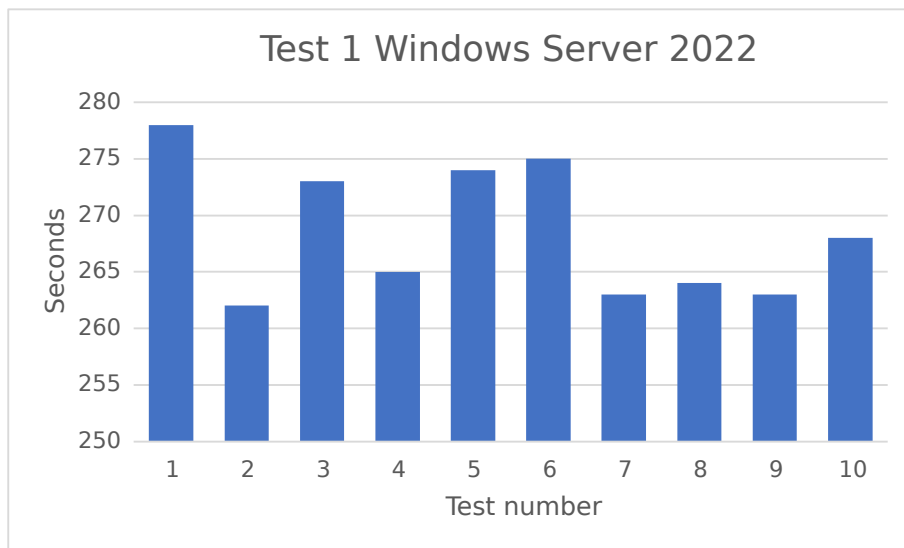


Figure 36: Windows Server 2022 with default security configuration (Source: own material)

Mean value = 268.5 seconds

Standard deviation: $\sigma = 5.64$ seconds

The same test was used again but the VM security configuration was changed.

The new VM had TPM, Tamper Protection, Controlled folder access, Reputation-based protection (Potentially unwanted app blocking) and Core isolation (Memory integrity) enabled. This VM had Sysmon enabled as well, with the configuration file from SwiftOnSecurity that is listed in the appendix. The results of the test can be studied in Fig. 37.

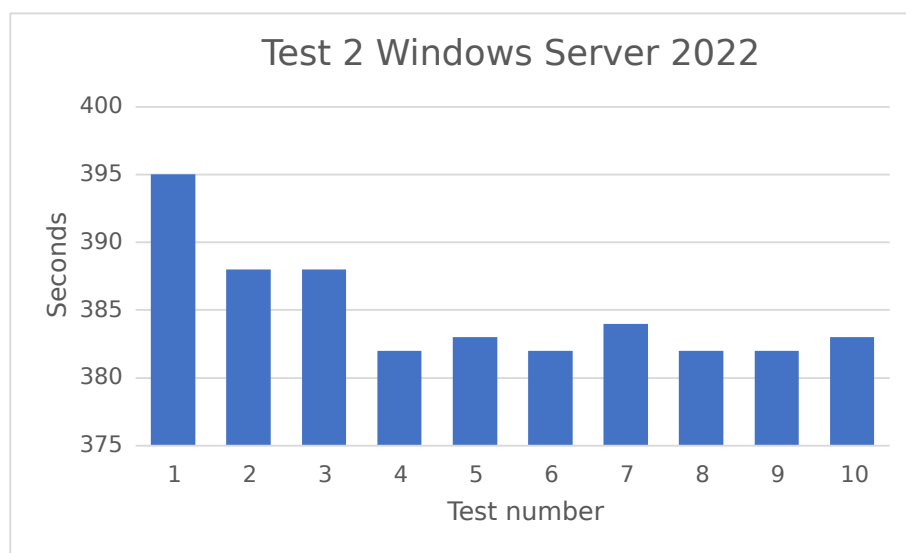


Figure 37: Windows Server 2022 with improved security configuration (Source: own material)

Mean value = 384.9 seconds

Standard deviation: $\sigma = 4.04$ seconds

The results from the tests show that there was a time increase of 43.4% after the security configuration was changed. The main reason for the time increase was Sysmon. With the same security functions as Fig. 37, but without Sysmon there was only a time increase of 2.2%. This can be seen in Fig. 38.

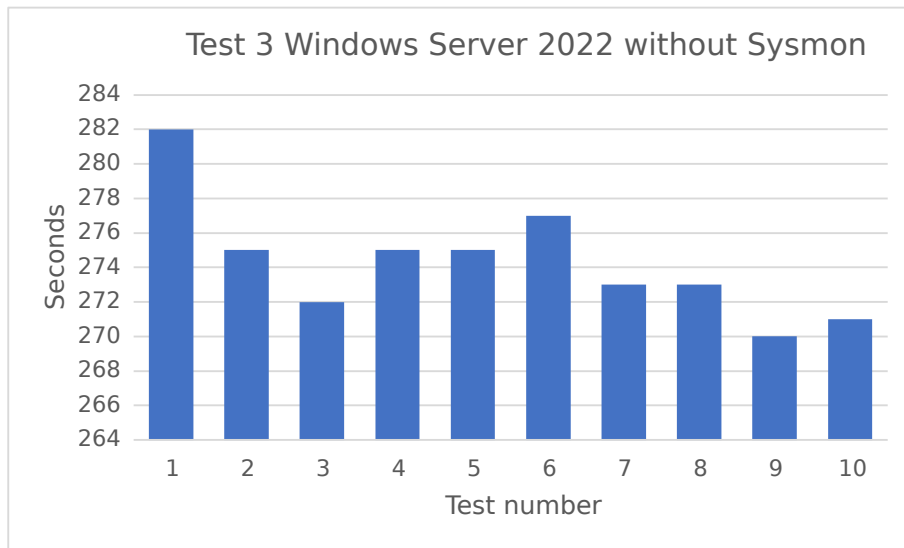


Figure 38: Windows Server 2022 with improved security configuration (without Sysmon) (Source: own material)

Mean value = 274.3 seconds

Standard deviation: $\sigma = 3.26$ seconds

5.4.2 Windows Server 2019

The same test that was used on the Windows Server 2022 was also used on the Windows Server 2019. In Fig. 39 is test results of test 4.

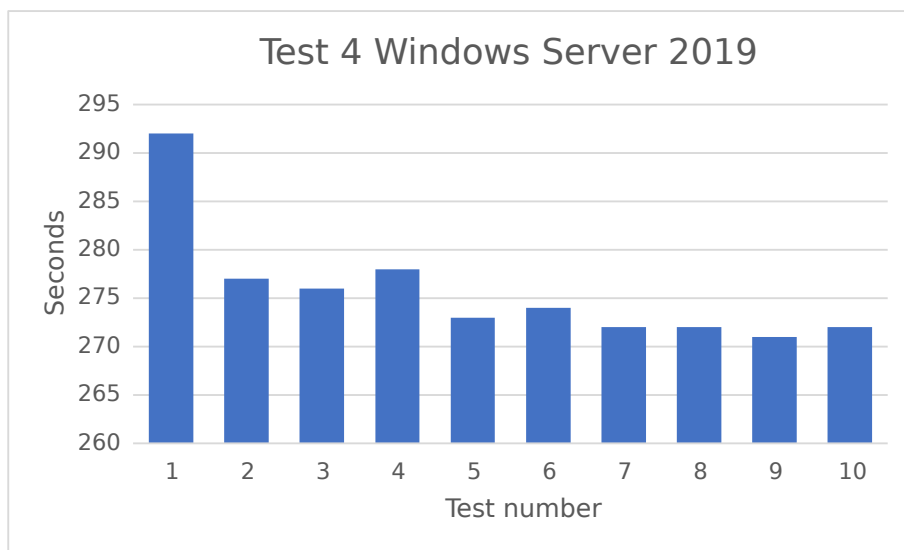


Figure 39: Windows Server 2019 with default security configuration (Source: own material)

Mean value = 275.7 seconds

Standard deviation: $\sigma = 5.88$ seconds

The same test was ran again on the Windows Server 2019, but with Controlled folder access, Memory integrity and Sysmon with the configuration file from SwiftOnSecurity. "Check apps and files" was set to Block and the VM that was used had TPM. In Fig. 40 is the results of the test.

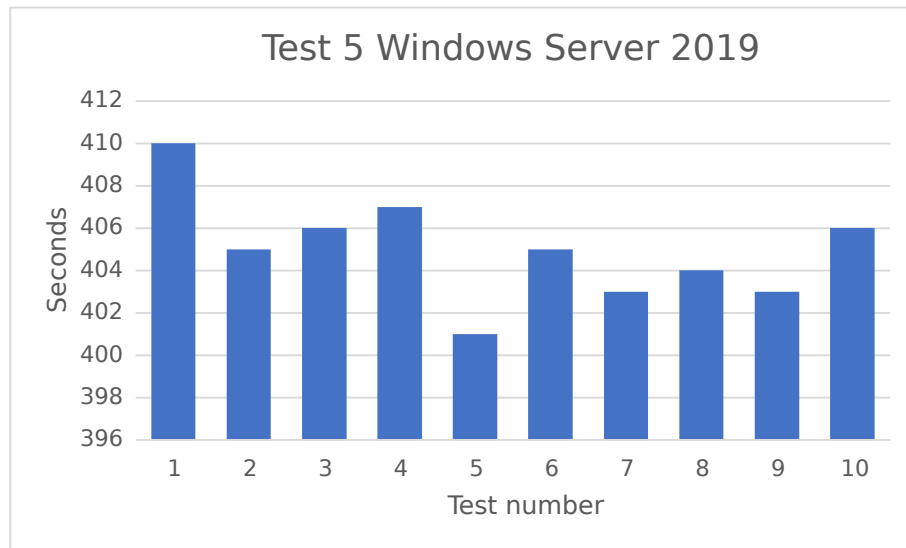


Figure 40: Windows Server 2019 with improved security configuration (Source: own material)

Mean value = 405.0 seconds

Standard deviation: $\sigma = 2.37$ seconds

The results from the tests show that there was a time increase of 46.9% after the security configuration was changed. The main reason for the time increase was Sysmon. With the same security functions as Fig. 40, but without Sysmon there was only a time increase of 3.3%. This can be seen in Fig. 41.

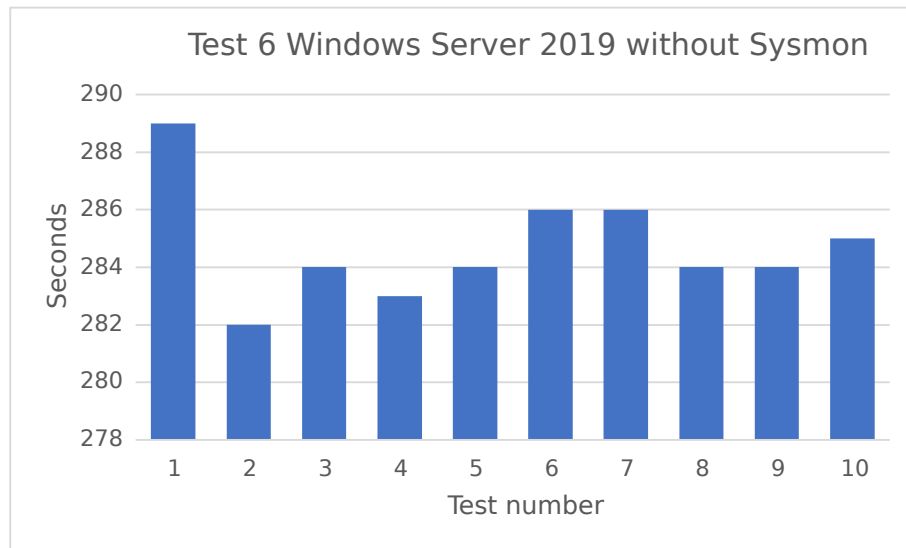


Figure 41: Windows Server 2019 with improved security configuration(without Sysmon) (Source: own material)

Mean value = 284.7 seconds

Standard deviation: $\sigma = 1.85$ seconds

Chapter 6

6 Reflection and Discussion

6.1 Results

Throughout working on this thesis the group learned that the best practice for Windows Server 2019/2022 security configuration was to use all the built in security features such as Tamper Protection, Secure Boot, Trusted Boot, Measured Boot, Reputation-based Protection, WDAC, Applocker, as well as using all this security features needed for the Windows Server to meet all the Secure-Core requirements. The Secure-Core requirements are HVCI, Boot DMA Protection, System Guard, Virtualization-Based Security (VBS) and TPM 2.0. The positive effects on the security by using these features outweigh the effects they have on the performance of the Server. It is also recommended to use Sysmon to monitor events and processes. The security configuration of Sysmon that is used in chapter 5.4 has a lot of impact on the system performance because it monitors many activities. It is strongly advised to make configurations to Sysmon file, to meet the requirements for the specific system. By making the Sysmon configuration file shorter and more specific to the Windows Server being used, it can significantly improve the system performance. When it comes to Microsoft Defender for Endpoint it can be used as a good antivirus, but there are other antivirus solutions that should be considered.

Microsoft Azure Cloud provides many security features to ensure that the customer's cloud environment is safe. Some of these features is costly, but the customer needs to assess the security criteria of the system. If the customer have many users and much personal data about these users, the security requirements is significantly higher if following the frameworks. Microsoft Sentinel is a SIEM and provide SOAR possibilities in Microsoft Azure cloud, using a SIEM it can greatly reduce the response time for events and can provide a simplified overview of the current system, which can help the system administrators. This is some of the reasons why it is recommended to use a SIEM solution.

Azure AD Identity Protection is a great solution for Azure AD, for both small and big organizations, which will help the organization to identify abnormal logins. This is a good tool because it can stop potential attackers. Microsoft Defender for Cloud provides suggestions for security improvements and can work with Microsoft Sentinel and other third party SIEMs. Microsoft Defender for Cloud have its own security alert system, which can be useful for a quick overview in case of a security threat. This tool should be used if the organization is using Microsoft Azure cloud. Azure AD Privileged Identity Management helps the organization by providing an organized overview of the users with higher privileges, this can help the organization to keep a good security practice. For

big organizations this can be a great tool, but for small organizations with a smaller IT-team, it might not be necessary. Multi-factor Authentication is recommended to implement, because of the extra layer of security it provides. Key Vault is a resource that is recommended to use in Microsoft Azure that provides a safe environment to store and use keys, secrets and certificates.

6.2 Further work

This thesis has covered some parts of the Cyber landscape organizations provide to protect and actively monitor. There are many other parts of a Windows Server- or Azure Cloud environment that can be further analysed and worked with, the parts this group would suggest is listed below.

6.2.1 Active directory

Working on this thesis it was not looked in to what the best practices are when it comes to the different Active Directory solutions. Since Active Directory is used by many organizations and there is many policies that can be implemented to make the system more secure, it is something that can be looked further into in the future.

6.2.2 Policies

It is many different policies that is relevant for making a windows server as secure as possible, in this project the group decided not to focus on the different policies. Some policies that is useful to make the system as secure as possible is Exploit Guard policy and different Windows Firewall policies. There is also much more work to be done when it comes to group policies and what the best practises are, but using the official Security Baseline is a good starting point, but needs further customization for the specific system.

6.2.3 Network security

The group did not prioritize different network security services and what the best practices are for these services. So there is further work that can be done to find out what the best network security configuration is also.

6.3 Work Evaluation

6.3.1 Group work

At the start of the project the group did not function optimally, and this reflected on to the work hours. After the group was divided this was not an issue anymore, the group worked together almost every day and were able to catch up on the lost hours. When the group worked together it was mostly communication with voice chat on Microsoft Teams and had fixed working hours from 09:30 to 15:30 almost every day. The group used the Kanban board to keep a nice and clear structure of the different tasks that needed to be completed.

6.3.2 Project work

The group did not get to specify the project to the client's needs as much as hoped for, because it was difficult to get in touch with the client. This resulted in few meetings and the group was left to decide what to include in the thesis.

It was difficult to find reliable information about the newer Microsoft Azure and Windows Server security features other places than from Microsoft's own documentation. This was unfortunate, because the group would like to provide information about possible drawbacks and experiences with the different features.

Something that could be done if there was more time was to configure Sysmon and Microsoft Sentinel to work together, and check if the Sysmon configuration file from SwiftOnSecurity could be optimized for a specific Windows Server. There could also be performed an comparison between Microsoft Defender for Endpoint vs other antivirus solutions.

6.3.3 What could be done different

If there was anything the group would do differently it would be to contact Microsoft Norway and try to get a meeting with a security professional. It could also be beneficial for the thesis to try to interview other security specialists, this was not done because there was much information to be found on the internet and due to the time limit.

7 Conclusion

The thesis question for this project was "*Which security features are crucial for hardening the security of a Windows Server 2019/2022 and Microsoft Azure Cloud environment?*". The assignment was to create a recommendation for which security features to implement on the newer versions of Windows Server 2019 and 2022 including security features in Microsoft Azure. When considering how well this project answers to the assignment, it is important to first look at the thesis question and how well the group have managed to answer it.

Through out the project the group have consciously mapped out the different features that are crucial for hardening a Windows Server and Microsoft Azure Cloud environment. Although the project ended up with clear recommendations there are a lot of further work to do, to provide a complete guide.

When considering how well the result goals of this thesis is answered, it is essential to look at the whole process. Goal 1 (1.3.1) have clearly been answered thoroughly throughout the thesis. It was also desirable that the performance impact the various security features had on the system was tested, this was done in 5.4 and the group is satisfied with how the testing was performed. That means result goal 2 has been accomplished (1.3.1). Result goal 3 is fulfilled in the testing part of the thesis, by showing how the security features is enabled and verified that they work as intended. The group has also made a overview over how the different security functions affect the various frameworks that was requested by the client, which fulfills result goal 4(1.3.1).

To view this in its eternity, the group have answered the thesis question and the result goals to the best of the groups ability, considering the thesis scope and challenging theme. It provides a great foundation for further work.

Bibliography

- [1] Danny Fullerton (northox). *Dynamic vs Static root of trust*. URL: <https://security.stackexchange.com/questions/53258/dynamic-vs-static-root-of-trust/54001#54001> (visited on 23/04/2022).
- [2] Danny Fullerton (northox). *How does the TPM perform integrity measurements on a system?* URL: <https://security.stackexchange.com/questions/39329/how-does-the-tpm-perform-integrity-measurements-on-a-system> (visited on 23/04/2022).
- [3] Ashwin Baliga. *Enable secured-core and secure connectivity with Windows Server 2022*. URL: <https://docs.microsoft.com/en-us/shows/inside-azure-for-it/enable-secured-core-and-secure-connectivity-with-windows-server-2022> (visited on 05/02/2022).
- [4] Shawn Brink. *How to Enable or Disable Microsoft Defender Antivirus Potential Unwanted App (PUA) Protection in Windows 10*. URL: <https://www.tenforums.com/tutorials/32236-enable-disable-microsoft-defender-pua-protection-windows-10-a.html> (visited on 04/04/2022).
- [5] Cisco. *What Is a Cyberattack?* URL: <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html> (visited on 12/04/2022).
- [6] Microsoft Security Community. *AppLocker*. URL: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview> (visited on 08/02/2022).
- [7] Microsoft Security Community. *Automatic VM guest patching for Azure VMs*. URL: <https://docs.microsoft.com/en-us/azure/virtual-machines/automatic-vm-guest-patching> (visited on 13/03/2022).
- [8] Microsoft Security Community. *Azure Key Vault basic concepts*. URL: <https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts> (visited on 26/04/2022).
- [9] Microsoft Security Community. *Azure Sentinel webinar: Understanding Azure Sentinel features and functionality deep dive*. URL: <https://www.youtube.com/watch?v=7An7BB-CcQI> (visited on 26/03/2022).
- [10] Microsoft Security Community. *BitLocker*. URL: <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview> (visited on 12/03/2022).
- [11] Microsoft Security Community. *Hardware requirements for Windows Server*. URL: <https://docs.microsoft.com/en-us/windows-server/get-started/hardware-requirements> (visited on 25/01/2022).
- [12] Microsoft Security Community. *Hotpatch for new virtual machines*. URL: <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-hvci-enablement> (visited on 13/03/2022).

-
- [13] Microsoft Security Community. *How To: Investigate risk*. URL: <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk> (visited on 13/03/2022).
- [14] Microsoft Security Community. *Hypervisor-protected Code Integrity enablement*. URL: <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-hvci-enablement> (visited on 13/03/2022).
- [15] Microsoft Security Community. *Kernel DMA Protection*. URL: <https://docs.microsoft.com/en-us/windows/security/information-protection/kernel-dma-protection-for-thunderbolt> (visited on 14/03/2022).
- [16] Microsoft Security Community. *Measured Boot*. URL: <https://docs.microsoft.com/en-us/windows/win32/w8cookbook/measured-boot> (visited on 11/02/2022).
- [17] Microsoft Security Community. *Measured boot and host attestation*. URL: <https://docs.microsoft.com/en-us/azure/security/fundamentals/measured-boot-host-attestation> (visited on 11/02/2022).
- [18] Microsoft Security Community. *Microsoft Defender for Cloud's enhanced security features*. URL: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/enhanced-security-features-overview> (visited on 14/03/2022).
- [19] Microsoft Security Community. *Overview of Early Launch AntiMalware*. URL: <https://docs.microsoft.com/en-us/windows-hardware/drivers/install/early-launch-antimalware> (visited on 11/02/2022).
- [20] Microsoft Security Community. *Protect security settings with tamper protection*. URL: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection?view=o365-worldwide> (visited on 10/05/2022).
- [21] Microsoft Security Community. *Secure boot*. URL: <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot> (visited on 08/02/2022).
- [22] Microsoft Security Community. *Secure Boot and Trusted Boot*. URL: <https://docs.microsoft.com/en-us/windows/security/trusted-boot> (visited on 08/02/2022).
- [23] Microsoft Security Community. *SMB over QUIC*. URL: <https://docs.microsoft.com/en-us/windows-server/storage/file-server/smb-over-quic> (visited on 05/04/2022).
- [24] Microsoft Security Community. *Trusted Platform Module 2.0*. URL: <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-tpm> (visited on 15/03/2022).
- [25] Microsoft Security Community. *Virtualization-based Security (VBS)*. URL: <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs> (visited on 02/02/2022).

-
- [26] Microsoft Security Community. *What is Azure AD Privileged Identity Management?* URL: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure> (visited on 21/03/2022).
- [27] Microsoft Security Community. *What is Identity Protection?* URL: <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection> (visited on 13/03/2022).
- [28] Microsoft Security Community. *What is Microsoft Defender for Cloud?* URL: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction> (visited on 14/03/2022).
- [29] Microsoft Security Community. *What is Secured-core server?* URL: <https://docs.microsoft.com/en-us/windows-server/security/secured-core-server> (visited on 04/02/2022).
- [30] Microsoft Security Community. *What is the Server Core installation option in Windows Server?* URL: <https://docs.microsoft.com/en-us/windows-server/administration/server-core/what-is-server-core> (visited on 12/03/2022).
- [31] Microsoft Security Community. *Windows Defender Application Control and AppLocker Overview.* URL: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview> (visited on 04/02/2022).
- [32] Microsoft Security Community. *Windows Defender System Guard: How a hardware-based root of trust helps protect Windows 10.* URL: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-system-guard/how-hardware-based-root-of-trust-helps-protect-windows> (visited on 23/04/2022).
- [33] Direktoratet for e-helse. *Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.* URL: <https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren> (visited on 10/03/2022).
- [34] forest. *Do a TPM's benefits outweigh the risks.* URL: <https://security.stackexchange.com/questions/187820/do-a-tpms-benefits-outweigh-the-risks> (visited on 12/04/2022).
- [35] Olaf Hargton. *sysmon-modular — A Sysmon configuration repository for everybody to customise.* URL: <https://github.com/olafhartong/sysmon-modular> (visited on 28/02/2022).
- [36] Erik Hjelmås. *DCSG1005 - Infrastruktur: sikre grunntjenester.* URL: <https://www.ntnu.no/studier/emner/DCSG1005#tab=omEmnet> (visited on 21/02/2022).
- [37] Erik Hjelmås. *IDATG2202 - Operativsystemer.* URL: <https://www.ntnu.no/studier/emner/IDATG2202#tab=omEmnet> (visited on 21/02/2022).
- [38] Didier Van Hoye. *QUIC, HURRY UP!* URL: <https://www.starwindsoftware.com/blog/smb-over-quic> (visited on 05/04/2022).

-
- [39] *Hyper-V Technology Overview*. URL: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview> (visited on 10/03/2022).
- [40] isms.online. *What is an Information Security Management System (ISMS)?* URL: <https://www.isms.online/information-security-management-system-isms/> (visited on 10/03/2022).
- [41] ISO. *Information security, cybersecurity and privacy protection — Information security controls*. Tech. rep. ISO/IEC 27002:2022. Geneva, Switzerland: International Organization for Standardization, 2022.
- [42] Vickie Li. *Process Monitor v3.89*. URL: <https://medium.com/swlh/what-is-process-monitor-8cca0167faaf> (visited on 07/04/2022).
- [43] Microsoft. *Device Guard and Credential Guard hardware readiness tool*. URL: <https://www.microsoft.com/en-us/download/details.aspx?id=53337> (visited on 27/04/2022).
- [44] Microsoft. *Secure the Windows boot process*. URL: <https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process> (visited on 23/03/2022).
- [45] Microsoft. *Sysinternals Suite*. URL: <https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite> (visited on 04/05/2022).
- [46] Microsoft. *Windows 11 Security Book: Powerful security from chip to cloud*. URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMyFE> (visited on 10/02/2022).
- [47] NTNU. *About NTNU – Norwegian University of Science and Technology*. URL: <https://www.ntnu.edu/about> (visited on 18/02/2022).
- [48] Openstack. *Vision for OpenStack Clouds*. URL: <https://governance.openstack.org/tc/reference/technical-vision.html> (visited on 25/01/2022).
- [49] Ophir Oren. *Windows PowerShell: creating large files on disk — fast!* URL: <https://medium.com/@developer82/windows-powershell-creating-large-files-on-disk-fast-306d8df9d116> (visited on 07/05/2022).
- [50] Mark Russinovich. *Process Monitor v3.89*. URL: <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon> (visited on 06/04/2022).
- [51] Mark Russinovich and Thomas Garnier. *Process Monitor v3.89*. URL: <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon> (visited on 03/04/2022).
- [52] Nasjonal sikkerhetsmyndighet. *Grunnprinsipper for IKT-sikkerhet 2.0*. URL: <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/> (visited on 11/03/2022).
- [53] Andrei Popov Sunny Zankharia. *Enable secured-core and secure connectivity with Windows Server 2022*. URL: <https://www.microsoft.com/security/blog/2020/08/20/taking-transport-layer-security-tls-to-the-next-level-with-tls-1-3/> (visited on 05/02/2022).
-

- [54] SwiftOnSecurity. *sysmon-config* — *A Sysmon configuration file for everybody to fork*. URL: <https://github.com/SwiftOnSecurity/sysmon-config> (visited on 22/02/2022).
- [55] Gaute Bjørklund Wangen. *DCSG2005 - Risikostyring*. URL: <https://www.ntnu.no/studier/emner/DCSG2005#tab=omEmnet> (visited on 21/02/2022).
- [56] Wikipedia contributors. *Rootkit* — *Wikipedia, The Free Encyclopedia*. URL: <https://en.wikipedia.org/w/index.php?title=Rootkit&oldid=1084738119> (visited on 17/02/2022).
- [57] Erjon Zoto. *DCSG1002 - Cybersikkerhet og teamarbeid*. URL: <https://www.ntnu.no/studier/emner/DCSG1002#tab=omEmnet> (visited on 21/02/2022).

A Project Plan

Goals and framework

Background

The SOC at NTNU (Norwegian University of Science and Technology) is part of the Digital Security department at NTNU. They have the function of detecting, analyzing and responding to digital security threats aimed at NTNU's systems. Our group has received this project from the NTNU SOC with Christoffer Vargtass Hallstensen as our contact person at the NTNU SOC.

Our task for this project is to examine the different security functions of the newer versions of Microsoft Windows and Microsoft Office, as well as identify the specific types of threats these security functions eliminates. This information will then be used to create a recommendation for a collection of security mechanisms that NTNU should implement to have a well-rounded and complete protection against most IT-security threats.

Project goals

Learning goals:

- Get a good understanding of the different security aspects in different versions of Windows and Microsoft Office.
- Learn to develop a best practice-plan in bigger systems based on gathered information.

Effect goals:

- Map out the various security features in Windows and Microsoft Office in depth.
- Map out the various threats in Windows and Microsoft Office.
- Use this overview and analysis to come up with a recommendation of what security mechanisms and controls NTNU should incorporate in their systems to provide well rounded security against the most relevant threats.

Result goals:

- Look at the differences in performance between the different versions of Windows when it comes to security features.

Framework

- The test environment will be in NTNU's internal cloud service SkyHigh.
- There will not be bought any licenses.
- There is no need to automate the setup of the test environment.
- The report will be written in English because it's a universal language that is commonly used to describe IT concepts and definitions.

Tools

Tool	Description
PowerShell	Scripting
SkuHigh/Openstack	Cloud infrastructure for developing test environment
Toggl	Time tracking and planning
Overleaf	Collaboration on the assignment
Discord	Communication
Microsoft Teams	Meetings, documents, file sharing, Kanban board
Teamgantt	Gantt chart

Scope

Restriction

The project will focus on the built-in security features of Windows 10, 11, Server 2019 and 2022. We will not look at other versions of Windows due to the task specifications. If we at some point must prioritize which version of the operating system to analyze, we will focus on Windows 11 and Windows server 2022 due to the future-oriented nature of the task. We will always focus on the newest version of Microsoft Office.

Situation

NTNU's systems have thousands of users every day together with much personal data. Due to this, upgrading to newer operating systems can prove to be a hard but necessary task to provide the best possible security. NTNU will need much testing and analyzing before they safely can upgrade to the new systems, since the newer operating systems might have bugs and new threats that need to be mitigated. Scalability and performance are also something that needs to be ensured to keep the up-time high.

Due to this, a part of our task is to analyze the possible threats and attack vectors, so NTNU can transfer gradually and safely to these newer operating systems.

Case

The task is to investigate different security features built into newer versions of Microsoft Windows (10, 11, Server 2019, Server 2022) and Microsoft Office. The task also includes mapping which threats, and attack vectors can provide effective risk-reducing measures. In addition to investigating how attacks can be detected. The Client also wants us to look at available safety controls for NTNU's management system for information security, and thus make an assessment and recommendation about which security controls NTNU should introduce to increase information security and the ability to detect digital threats on the Windows platform.

Project organizing

Organization chart

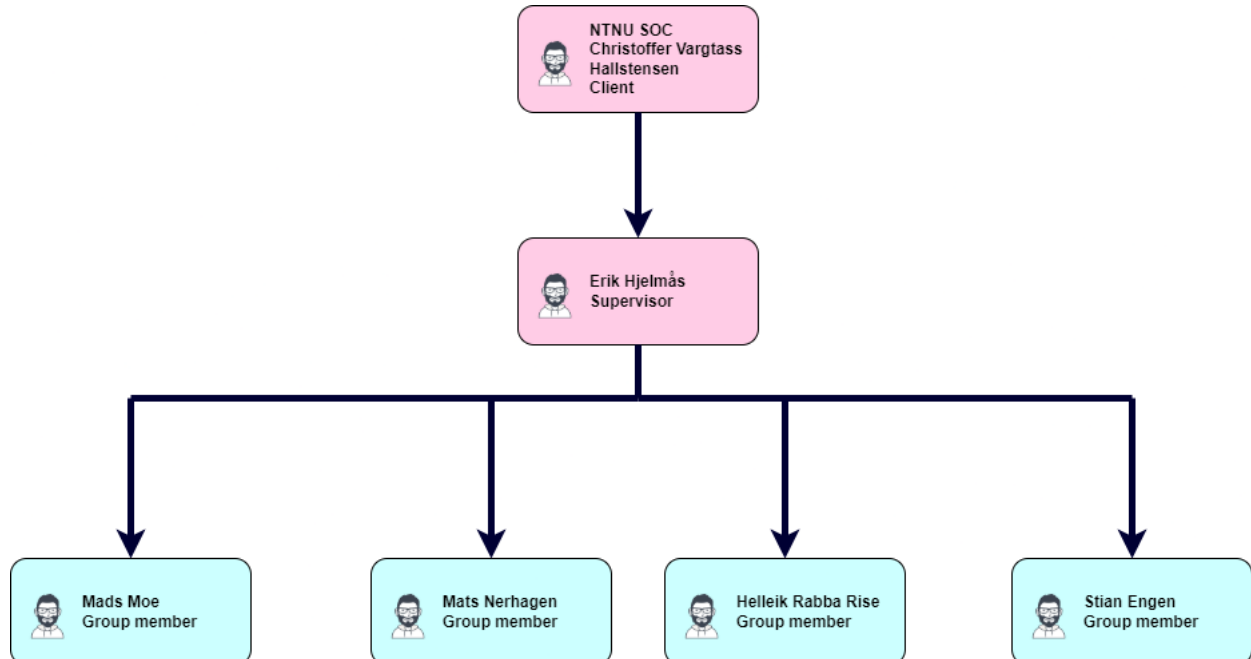


Figure 42: Organization chart

Responsibilities and roles

Roles:

Group leader – Mads Reneflot Moe

Secretary – Mats Nerhagen

Group member – Helleik Rabba Rise

Group member – Stian Engen

Responsibilities:

Book rooms – Helleik Rabba Rise

Overseeing Gantt-scheme compliance – Mats Nerhagen

Overseeing Overleaf structure – Mads Reneflot Moe

Overseeing Toggl Track – Stian Engen

Group rules

1. Work hours each week should be around 30 hours per person. You are allowed to work more than this if you have an upcoming absence that you know of.
2. Missed work hours must be compensated for in the two following weeks.
3. Work hours must be logged by Toggl Track by everyone each day.
4. Should a group member get sick they have to notify the rest of the group if this prevents them from attending meetings or completing tasks with a set deadline.
5. It is important that group members notify the group of any planned absence they might have so this will not affect the planning of any future meetings or deadlines.
6. If any group member breaks the rules, a meeting with the other members should take place to decide further actions. See next rule.
7. If any group member makes commits serious infractions on the rules, a meeting with the advisor should take place to decide if the member will get dismissed from the group.

Routines

- Every group member must meet for group meetings over internet every Monday 10:00, unless something else is specified.

- Every group member must meet for status meetings over the internet every Friday at 10:00, unless something else is specified.
- Physical group meetings should take place every Wednesday both before and after the guidance meeting (09:30) when the situation allows it.
- Workdays are from Monday to Friday every week. Working hours are primarily between 09:00 and 16:00.
- We will use the built in Kanban board in Microsoft Teams (called “planner/tasks”). All tasks should be logged using that Kanban board.

Planning, follow up and reporting

Project structuring - Development model

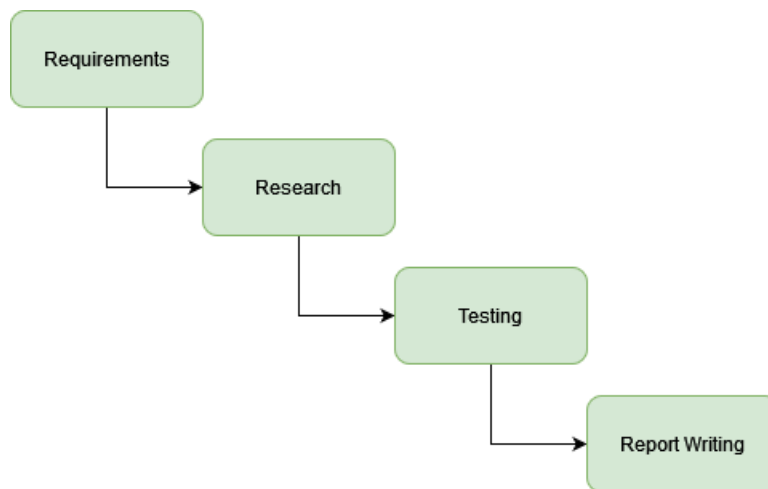


Figure 43: Waterfall model

Method and approach

We will use the app “Tasks delivered by Planner and To do” as a Kanban board in Teams to organize our work. The Kanban board is implemented to enable better collaboration, and to reduce the need for status meetings since the status information of each task will be available through the card information and position. The Kanban board will visualize the workflow from start to finish with the five different columns Backlog, In progress, Testing, Review and Completed.

All tasks the group decides on will be put under the Backlog column. When a group member starts to work on a task the task will be moved from Backlog

to In progress. If there is something regarding the task that needs to be tested the task will be moved to Testing. When a group member is done with a task the task will be moved to Review where all the finished tasks will be put. After another group member has gone through the task and approved it the task will be moved to Complete. Complete is where all the approved tasks will be put.

Each individual task will be assigned to different group members, and you will be able to set dates for deadlines, how urgent the task is and how much progress has been made. Using a Kanban board will therefore help us prioritize our work and get a good overview of all our tasks.

Plan for meetings

We plan to have status meetings with all group members every Monday and Friday at 10:00 where we talk about our progression on the different tasks. We will plan additional meetings if we feel the need to.

Meetings with Erik Hjelmås (advisor) will take place every Wednesday at 09:30 and will require physical attendance (when possible) after week 4. These meetings will have an associated report written.

Meetings with NTNU-SOC will take place when needed, primarily after a new milestone is reached to plan further work. These meetings will have an associated report written.

Organizing

Documentation, standards, and source code

The report will be written in a Latex document, where all the members will be able to edit and update the report simultaneously. Overleaf, an online editor, will be used for this.

We will use Microsoft Teams to share documents as a standard.

Risk assessment

In our risk assessment we have mapped out and identified different risks based on likelihood and consequence. We have also added countermeasures to reduce the likelihood and consequences of each risk.

Nr.	Risk	Description	Countermeasures
1	Difficulties with setup of test environment.	Too complex test environment.	Good research and planning.
2	Downtime OpenStack.	Server downtime for the test environment due to NTNU servers.	Planning according to scheduled downtime.
3	Accidental loss of documents.	Accidental loss of documents or files Due to human error.	Saving often and usage of backup often.
4	Malicious software.	Installation of malicious software onto the test environment due to human error.	Check the files hash values before and after downloading.

Table 1: Technical risk

Nr.	Risk	Description	Countermeasures
5	Requirements not met	The groups focus diverges too far away from the original task description, and therefore does not meet the requirements.	Reading the case and assignment again together with status meetings with advisor.
6	Loss of gathered information.	Not filling in the source list as it should, making it hard to find later.	Be consistent with good source notation.

Table 2: Business risk

Nr.	Risk	Description	Countermeasures
7	Sick group member.	A member of the group is unable to work due to sickness.	Explain what has been done to the group member, so he or she catches up.
8	Uncoordinated work.	Uncoordinated work due to bad workflow and communication.	Using Tasks to know what we should work on and when we should work on it. And regular meetings to coordinate.

Table 3: Project group risk

Consequence→ Likelihood↓	1-Low	2-Medium	3-High	4-Critical
4-Highly likely				
3-Likely	7			
2-Less likely		1	5, 8	
1-Unlikely	2	6	4	3

Table 4: Risk matrix before countermeasures

Consequence→ Likelihood↓	1-Low	2-Medium	3-High	4-Critical
4-Highly likely				
3-Likely	7			
2-Less likely		1		
1-Unlikely	2	3, 5, 6, 8	4	

Table 5: Risk matrix after countermeasures

Implementation plan

Milestones

26.01.2022 Project plan completed
 23.02.2022 Setup of test environment completed
 13.05.2022 Report completed
 16.05.2022 Presentation completed

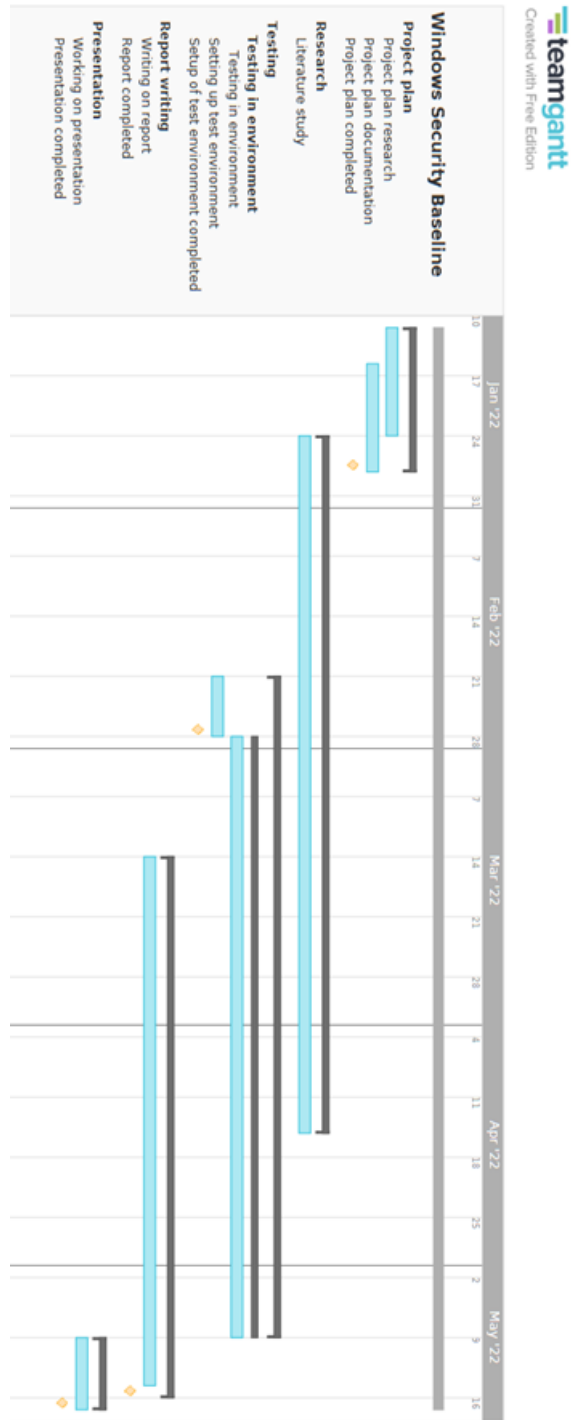


Figure 44: Gantt chart

Research

The research phase will last from 27.01 to 18.04. This research phase will focus on researching different threats that exist, together with the built-in security mechanisms in Windows and Microsoft Office. This research phase will go in parallel with writing the report and doing

B Useful PowerShell commands for Microsoft Defender Antivirus

To check the status of Microsoft Defender Antivirus you can run the command below. If `AMRunningMode` is "Normal" that means Microsoft Defender Antivirus is running in active mode.

```
Get-MpComputerStatus
```

```
PS C:\> Get-MpComputerStatus
RunspaceId           : 20ec3341-69ae-4709-ba05-73b587afb4c7
AMEngineVersion      : 1.1.19000.8
AMProductVersion     : 4.18.2202.4
AMRunningMode        : Normal
AMServiceEnabled    : True
AMServiceVersion     : 4.18.2202.4
AntispywareEnabled   : True
AntispywareSignatureAge : 1
AntispywareSignatureLastUpdated : 4/3/2022 5:47:09 AM
AntispywareSignatureVersion : 1.361.1231.0
AntivirusEnabled     : True
AntivirusSignatureAge : 1
AntivirusSignatureLastUpdated : 4/3/2022 5:47:09 AM
AntivirusSignatureVersion : 1.361.1231.0
BehaviorMonitorEnabled : True
ComputerID           : 2C4FA5C1-9C75-4591-9975-8C38F93098BD
ComputerState        : 0
DefenderSignaturesOutOfDate : False
DeviceControlDefaultEnforcement : Unknown
DeviceControlPoliciesLastUpdated : 4/3/2022 4:54:37 PM
DeviceControlState   : Disabled
FullScanAge          : 4294967295
FullScanEndTime      :
FullScanOverdue      : False
FullScanRequired     : False
FullScanSignatureVersion :
FullScanStartTime    :
IoavProtectionEnabled : True
IsTamperProtected    : True
IsVirtualMachine     : False
LastFullScanSource   : 0
LastQuickScanSource  : 2
NISEnabled           : True
NISEngineVersion     : 1.1.19000.8
NISSignatureAge      : 1
NISSignatureLastUpdated : 4/3/2022 5:47:09 AM
NISSignatureVersion  : 1.361.1231.0
OnAccessProtectionEnabled : True
ProductStatus        : 524288
QuickScanAge         : 0
QuickScanEndTime     : 4/4/2022 3:54:18 AM
```

Figure 45: Checking Microsoft Defender Antivirus status

Command to check for Microsoft Defender Antivirus updates:

```
Update-MpSignature
```

To run a quick scan you could use this command:

```
Start-MpScan -ScanType QuickScan
```

To run a full virus scan you can use this command:

```
Start-MpScan -ScanType FullScan
```

You can also run a custom virus scan on a specific path with this command:

```
Start-MpScan -ScanType CustomScan -ScanPath PATH\TO\FOLDER
```

There is also a option to perform a offline virus scan, this could be useful if unwanted malware infect a device and the antivirus is not able to remove it when the OS is fully loaded. This command can be used to run a offline virus scan:

```
Start-MpWDOScan
```

When this command is ran the device will automatically restart and boot into the recovery environment. Then it will perform a full scan to remove viruses that would not be possible to detect during the normal operation of the OS. When the scan is done the device automatically restarts. After the restart you can go to "Windows Security ; Virus & threat protection ; Protection history" to view the scan report.

To delete a active threat you can run this command:

```
Remove-MpThreat
```

You can use this command to schedule a daily malware quick scan:

```
Set-MpPreference -ScanScheduleQuickScanTime SCAN-TIME
```

If you want to schedule a full scan you can use the following commands:

```
Set-MpPreference -ScanParameters 2
```

The 2 parameter specify a full scan.

```
Set-MpPreference -RemediationScheduleDay SCAN-DAY
```

In the command above you just need to change SCAN-DAY for the day number you want to run the full scan. "0"=everyday, "1"=Sunday, "2"=Monday, "3"=Tuesday, "4"= Wednesday, "5"= Thursday, "6"= Friday, "7"= Saturday, "8"= never. So if you want to scedual the full scan for Saturdays you run the following command:

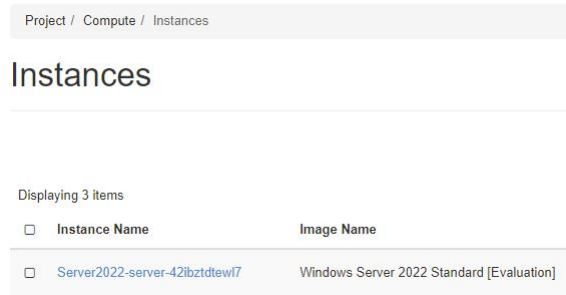
```
Set-MpPreference -RemediationScheduleDay 7
```

If you want to allow Microsoft Defender Antivirus to scan network drives use the following command:

```
Set-MpPreference -DisableScanningMappedNetworkDrivesForFullScan $false
```

C Setting up test environment skyhigh

```
openstack stack create -t single_windows_server.yaml server2022
```



The screenshot shows the OpenStack dashboard interface. At the top, there is a breadcrumb trail: "Project / Compute / Instances". Below this, the heading "Instances" is displayed. Underneath, it says "Displaying 3 items". A table lists the instances with columns for "Instance Name" and "Image Name". One instance is listed: "Server2022-server-42ibztdewi7" with the image "Windows Server 2022 Standard [Evaluation]".

<input type="checkbox"/>	Instance Name	Image Name
<input type="checkbox"/>	Server2022-server-42ibztdewi7	Windows Server 2022 Standard [Evaluation]

Figure 46: New instance created

The following command was used to installing PowerShell 7:

```
iex "& { $(irm https://aka.ms/install-powershell.ps1) } -UseMSI"
```

D YAML file for SkyHigh setup

YAML file provided by Erik Hjelmås

```
heat_template_version: 2013-05-23

description: >
  HOT template to create a new neutron network plus a router to the public
  network, and for deploying a single instance (most recent Windows Server)
  with a floating ip.

parameters:
  key_name:
    type: string
    description: Name of keypair to assign to servers

resources:
  private_net:
    type: OS::Neutron::Net

  private_subnet:
    type: OS::Neutron::Subnet
    properties:
      network_id: { get_resource: private_net }
      cidr: 192.168.111.0/24
      gateway_ip: 192.168.111.1
      allocation_pools:
        - start: 192.168.111.101
          end: 192.168.111.200

  router:
    type: OS::Neutron::Router
    properties:
      external_gateway_info:
        network: ntnu-internal

  router_interface:
    type: OS::Neutron::RouterInterface
    properties:
      router_id: { get_resource: router }
      subnet_id: { get_resource: private_subnet }

  server:
    type: OS::Nova::Server
    properties:
      image: 'Windows Server 2022 Standard [Evaluation]'
      flavor: m1.small
      key_name: { get_param: key_name }
      networks:
        - port: { get_resource: server_port }

  server_port:
    type: OS::Neutron::Port
    properties:
      network_id: { get_resource: private_net }
      security_groups:
        - { get_resource: server_security_group }
      fixed_ips:
        - subnet_id: { get_resource: private_subnet }

  server_floating_ip:
    type: OS::Neutron::FloatingIP
    properties:
      floating_network: ntnu-internal
```

```
61     port_id: { get_resource: server_port }
62
63 server_security_group:
64   type: OS::Neutron::SecurityGroup
65   properties:
66     description: Add security group rules for server
67     rules:
68       - remote_ip_prefix: 0.0.0.0/0
69         protocol: icmp
70       - remote_ip_prefix: 0.0.0.0/0
71         protocol: tcp
72         port_range_min: 22
73         port_range_max: 22
74       - remote_ip_prefix: 0.0.0.0/0
75         protocol: tcp
76         port_range_min: 80
77         port_range_max: 80
78       - remote_ip_prefix: 0.0.0.0/0
79         protocol: tcp
80         port_range_min: 443
81         port_range_max: 443
82       - remote_ip_prefix: 0.0.0.0/0
83         protocol: tcp
84         port_range_min: 3389
85         port_range_max: 3389
86
87 outputs:
88   server_private_ip:
89     description: IP address of server in private network
90     value: { get_attr: [ server, first_address ] }
91   server_public_ip:
92     description: Floating IP address of server in public network
93     value: { get_attr: [ server_floating_ip, floating_ip_address ] }
~.
```

E Sysmon config file


```
<!--
  sysmon-config | A Sysmon configuration focused on default high-quality event tracing
  and easy customization by the community
  Source version: 74 | Date: 2021-07-08
  Source project: https://github.com/SwiftOnSecurity/sysmon-config
  Source license: Creative Commons Attribution 4.0 | You may privatize, fork, edit,
  teach, publish, or deploy for commercial use - with attribution in the text.

  Fork version: <N/A>
  Fork author: <N/A>
  Fork project: <N/A>
  Fork license: <N/A>

  REQUIRED: Sysmon version 13 or higher (due to changes in syntax and bug-fixes)
  https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

  NOTE: To collect Sysmon logs centrally for free, see https://aka.ms/WEF | Command to
  allow log access to the Network Service:
  wevtutil.exe sl Microsoft-Windows-Sysmon/Operational /ca:0:BAG:SYD:(A;;0xf0005;;;SY
  (A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)

  NOTE: Do not let the size and complexity of this configuration discourage you from
  customizing it or building your own.
  This configuration is based around known, high-signal event tracing, and thus
  appears complicated, but it is only very
  detailed. Significant effort over years has been invested in front-loading as much
  filtering as possible onto the
  client. This is to make analysis of intrusions possible by hand, and to try to
  surface anomalous activity as quickly
  as possible to technicians armed only with Event Viewer. Its purpose is to
  democratize system monitoring for all organizations.

  NOTE: Sysmon is NOT a whitelist solution or HIDS correlation engine, it is a
  computer change logging tool.
  Do NOT ignore everything possible. Sysmon's purpose is providing context during a
  threat or problem investigation. Legitimate
  processes are routinely used by threats - do not blindly exclude them. Additionally
  be mindful of process-hollowing / imitation.

  NOTE: By default this monitors DNS, which is extremely noisy. If you are starting
  out on your monitoring journey, just remove that section.
  You can remove DNS events from Event Viewer screen by applying a 'Filter Current
  View' for event IDs of: -22
  Additionally, if you want to monitor DNS, you should deploy client-side adblocking
  to reduce lookups. See the DNS section for info.

  NOTE: This configuration is designed for PER-MACHINE installs of Chrome and
  OneDrive. That moves their binaries out of user-controlled folders.
  Otherwise, attackers could imitate these common applications, and bypass your
  logging. Below are silent upgrades you can do, no user impact:
  - https://docs.microsoft.com/en-us/onedrive/per-machine-installation
  - https://cloud.google.com/chrome-enterprise/browser/download/
  - As of 2021-02-16 there is no machine-level version of Microsoft Teams. The one
  provided copies itself to the user profile.

  NOTE: Sysmon is not hardened against an attacker with admin rights. Additionally,
  this configuration offers an attacker, willing
  to study it, limited ways to evade some of the logging. If you are in a very high-
  threat environment, you should consider a broader,
  log-most approach. However, in the vast majority of cases, an attacker will bumble
```

```
through multiple behavioral traps which
41  this configuration monitors, especially in the first minutes.
42
43  NOTE: If you encounter unexplainable event inclusion/exclusion, you may have a
second Sysmon instance installed under a different exe filename.
44  To clear this, try downloading the latest version and uninstalling with -u force. I
it hangs, kill the processes and run it again to cleanup.
45
46  TECHNICAL:
47  - Run sysmon.exe -? for a briefing on Sysmon configuration.
48  - Sysmon XML cannot use the AMPERSAND sign. Replace it with this: &amp;
49  - Sysmon 8+ can track which rule caused an event to be logged through the "RuleName
field.
50  - If you only specify exclude for a filtering subsection, everything in that
subsection is logged by default.
51  - Some Sysmon monitoring abilities are not meant for widely deployed general-purpos
use due to performance impact. Depends on environment.
52  - Duplicate or overlapping "Include" rules do not result in duplicate events being
logged.
53  - All characters enclosed by XML tags are always interpreted literally. Sysmon does
not support wildcards (*), alternate characters, or RegEx.
54  - In registry events, the value name is appended to the full key path with a "\"
delimiter. Default key values are named "\\(Default)"
55  - "Image" is a technical term for a compiled binary file like an EXE or DLL. Also,
it can match just the filename, or entire path.
56  - "ProcessGuid" and "LoginGuid" are not random, they contain some embedded
information. https://gist.github.com/mattifestation/0102042160c9a60b2b847378c0ef70b4
57
58  FILTERING: Filter conditions available for use are: is,is not,contains,contains
any,contains all,excludes,excludes any,excludes all,begin with,end with,less than,mor
than,image
59  - The "image" filter is usable on any field. Same as "is" but can either match
entire string, or only the text after last "\". Credit: @mattifestation
60
61 -->
62
63 <Sysmon schemaversion="4.50">
64   <!--SYSMON META CONFIG-->
65   <HashAlgorithms>md5,sha256,IMPHASH</HashAlgorithms> <!-- Both MD5 and SHA256 are th
industry-standard algorithms. Remove IMPHASH if you do not use DLL import
fingerprinting. -->
66   <CheckRevocation/> <!-- Check loaded drivers, log if their code-signing certificate
has been revoked, in case malware stole one to sign a kernel driver -->
67
68   <!-- <ImageLoad/> --> <!-- Would manually force-on ImageLoad monitoring, even
without configuration below. Included only documentation. -->
69   <!-- <ProcessAccessConfig/> --> <!-- Would manually force-on ProcessAccess
monitoring, even without configuration below. Included only documentation. -->
70   <!-- <PipeMonitoringConfig/> --> <!-- Would manually force-on PipeCreated /
PipeConnected events, even without configuration below. Included only documentation.
-->
71   <!-- <ArchiveDirectory> -->
72
73   <EventFiltering>
74
75   <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
76   <!--COMMENT: All processes launched will be logged, except for what matches a
rule below. It's best to be as specific as possible,
77   to avoid user-mode executables imitating other process names to avoid logging,
or if malware drops files in an existing directory.
```

```
78     Ultimately, you must weigh CPU time checking many detailed rules, against the
79     risk of malware exploiting the blindness created.
80     Beware of Masquerading, where attackers imitate the names and paths of
81     legitimate tools. Ideally, you'd use both file path and
82     code signatures to validate, but Sysmon does not support that. Look into
83     AppLocker/WindowsDeviceGuard for whitelisting support. -->
84     <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description,
85     Product, Company, CommandLine, CurrentDirectory, User, LogonGuid, LogonId,
86     TerminalSessionId, IntegrityLevel, Hashes, ParentProcessGuid, ParentProcessId,
87     ParentImage, ParentCommandLine, RuleName-->
88     <RuleGroup name="" groupRelation="or">
89     <ProcessCreate onmatch="exclude">
90     <!--SECTION: Microsoft Windows-->
91     <CommandLine condition="begin with"> "C:\Windows\system32\wermgr.exe"
92     "-queuereporting_svc" </CommandLine> <!--Windows:Windows error reporting/telemetry-->
93     <CommandLine condition="begin with">C:\Windows\system32\DllHost.exe
94     /Processid</CommandLine> <!--Windows-->
95     <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe
96     -Embedding</CommandLine> <!--Windows: WMI provider host-->
97     <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe
98     -secured -Embedding</CommandLine> <!--Windows: WMI provider host-->
99     <CommandLine condition="is">C:\Windows\system32\wermgr.exe -upload</CommandLine
100     <!--Windows:Windows error reporting/telemetry-->
101     <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe
102     /Embedding</CommandLine> <!--Windows: Search Indexer-->
103     <CommandLine condition="is">C:\windows\system32\wermgr.exe
104     -queuereporting</CommandLine> <!--Windows:Windows error reporting/telemetry-->
105     <CommandLine condition="is">\\?\C:\Windows\system32\autochk.exe *</CommandLine>
106     <!--Microsoft:Bootup: Auto Check Utility-->
107     <CommandLine condition="is">\SystemRoot\System32\smss.exe</CommandLine> <!--
108     Microsoft:Bootup: Windows Session Manager-->
109     <CommandLine condition="is">C:\Windows\System32\RuntimeBroker.exe
110     -Embedding</CommandLine> <!--Windows:Apps permissions [ https://fossbytes.com/runtime
111     broker-process-windows-10/ ] -->
112     <Image condition="is">C:\Program Files (x86)\Common Files\microsoft shared\ink
113     \TabTip32.exe</Image> <!--Windows: Touch Keyboard and Handwriting Panel Helper-->
114     <Image condition="is">C:\Windows\System32\TokenBrokerCookies.exe</Image> <!--
115     Windows: SSO sign-in assistant for MicrosoftOnline.com-->
116     <Image condition="is">C:\Windows\System32\plasrv.exe</Image> <!--Windows:
117     Performance Logs and Alerts DCOM Server-->
118     <Image condition="is">C:\Windows\System32\wifitask.exe</Image> <!--Windows:
119     Wireless Background Task-->
120     <Image condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--
121     Windows: Customer Experience Improvement-->
122     <Image condition="is">C:\Windows\system32\PrintIsolationHost.exe</Image> <!--
123     Windows: Printing-->
124     <Image condition="is">C:\Windows\system32\SppExtComObj.Exe</Image> <!--Windows:
125     KMS activation-->
126     <Image condition="is">C:\Windows\system32\audiodg.exe</Image> <!--Windows:
127     Launched constantly-->
128     <Image condition="is">C:\Windows\system32\conhost.exe</Image> <!--Windows:
129     Command line interface host process-->
130     <Image condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Windows:
131     Network file syncing-->
132     <Image condition="is">C:\Windows\system32\musNotification.exe</Image> <!--
133     Windows: Update pop-ups-->
134     <Image condition="is">C:\Windows\system32\musNotificationUx.exe</Image> <!--
135     Windows: Update pop-ups-->
136     <Image condition="is">C:\Windows\system32\powercfg.exe</Image> <!--
```

```
Microsoft:Power configuration management-->
109 <Image condition="is">C:\Windows\system32\sndVol.exe</Image> <!--Windows: Volur
control-->
110 <Image condition="is">C:\Windows\system32\sppsvc.exe</Image> <!--Windows:
Software Protection Service-->
111 <Image condition="is">C:\Windows\system32\wbem\WmiApSrv.exe</Image> <!--Windows
WMI performance adapter host process-->
112 <IntegrityLevel condition="is">AppContainer</IntegrityLevel> <!--Windows: Don't
care about sandboxed processes right now. Will need to revisit this decision.-->
113 <ParentCommandLine condition="begin with">%%SystemRoot%\system32\csrss.exe
ObjectDirectory=\Windows</ParentCommandLine> <!--Windows:CommandShell: Triggered when
programs use the command shell, but doesn't provide attribution for what caused it-->
114 <ParentCommandLine condition="is">C:\windows\system32\wormgr.exe
-queuereporting</ParentCommandLine> <!--Windows:Windows error reporting/telemetry-->
115 <CommandLine condition="is">C:\WINDOWS\system32\devicecensus.exe
UserCxt</CommandLine>
116 <CommandLine condition="is">C:\Windows\System32\usocoreworker.exe
-Embedding</CommandLine>
117 <ParentImage condition="is">C:\Windows\system32\SearchIndexer.exe</ParentImage>
<!--Windows:Search: Launches many uninteresting sub-processes-->
118 <!--SECTION: Windows:svchost-->
119 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -s
StateRepository</CommandLine>
120 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -p -s
camsvc</CommandLine>
121 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
appmodel</CommandLine> <!--Windows 10-->
122 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k appmodel -p -s
tiledatamodelsvc</CommandLine>
123 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k camera -s
FrameServer</CommandLine>
124 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k dcomlaunch -s
LSM</CommandLine>
125 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k dcomlaunch -s
PlugPlay</CommandLine>
126 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
defragsvc</CommandLine> <!--Windows defragmentation-->
127 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k devicesflow -s
DevicesFlowUserSvc</CommandLine>
128 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
imgsvc</CommandLine> <!--Microsoft:The Windows Image Acquisition Service-->
129 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService -s
EventSystem</CommandLine>
130 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService -s
bthserv</CommandLine>
131 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k LocalService -p
-s BthAvctpSvc</CommandLine>
132 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService -s
nsi</CommandLine>
133 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k localService -s
w32Time</CommandLine>
134 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceAndNoImpersonation</CommandLine> <!--Windows: Network services-->
135 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceAndNoImpersonation -p</CommandLine> <!--Windows: Network services-->
136 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted -s Dhcp</CommandLine> <!--Windows: Network services-->
137 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted -s EventLog</CommandLine>
138 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
```

```
localServiceNetworkRestricted -s TimeBrokerSvc</CommandLine>
139 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted -s WFDSConMgrSvc</CommandLine>
140 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
LocalServiceNetworkRestricted -s BTAGService</CommandLine>
141 <CommandLine condition="is">C:\Windows\System32\svchost.exe -k
LocalSystemNetworkRestricted -p -s NcbService</CommandLine> <!--Win10:1903:Network
Connection Broker-->
142 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted</CommandLine> <!--Windows: Network services-->
143 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceAndNoImpersonation -s SensrSvc</CommandLine>
144 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceAndNoImpersonation -p -s SSDPSRV</CommandLine> <!--Windows:SSDP [
https://en.wikipedia.org/wiki/Simple\_Service\_Discovery\_Protocol ] -->
145 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceNoNetwork</CommandLine>
146 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -p -s WPDBusEnum</CommandLine>
147 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -p -s fhsvc</CommandLine>
148 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -s DeviceAssociationService</CommandLine>
149 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -s NcbService</CommandLine>
150 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -s SensorService</CommandLine>
151 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -s TabletInputService</CommandLine>
152 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -s UmRdpService</CommandLine>
153 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -s WPDBusEnum</CommandLine>
154 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -p -s NgcSvc</CommandLine> <!--Microsoft:Passport-->
155 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceNetworkRestricted -p -s NgcCtrSvc</CommandLine> <!--Microsoft:Passport
Container-->
156 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localServiceAndNoImpersonation -s SCardSvr</CommandLine>
157 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
wuauerv</CommandLine>
158 <CommandLine condition="is">C:\Windows\System32\svchost.exe -k netsvcs -p -s
SessionEnv</CommandLine> <!--Windows:Remote desktop configuration-->
159 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted -s WdiSystemHost</CommandLine> <!--Windows: Diagnostic
System Host [ http://www.blackviper.com/windows-services/diagnostic-system-host/ ] --
160 <CommandLine condition="is">C:\Windows\System32\svchost.exe -k
localSystemNetworkRestricted -p -s WdiSystemHost</CommandLine> <!--Windows: Diagnosti
System Host [ http://www.blackviper.com/windows-services/diagnostic-system-host/ ] --
161 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted</CommandLine> <!--Windows-->
162 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
wldisvc</CommandLine> <!--Windows: Windows Live Sign-In Assistant [
https://www.howtogeek.com/howto/30348/what-are-wldisvc.exe-and-wldisvc.exe-and-why-are-they-running/ ] -->
163 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
ncaSvc</CommandLine> <!--Windows: Network Connectivity Assistant [
http://www.blackviper.com/windows-services/network-connectivity-assistant/ ] -->
164 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
```

```
BDESVCS</CommandLine> <!--Windows:Network: BitLocker Drive Encryption-->
165 <CommandLine condition="is">C:\Windows\System32\svchost.exe -k netsvcs -p -s
BDESVCS</CommandLine> <!--Microsoft:Win10:1903:Network: BitLocker Drive Encryption-->
166 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
BITS</CommandLine> <!--Windows:Network: Background Intelligent File Transfer (BITS)
-->
167 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
BITS</CommandLine> <!--Windows:Network: Background Intelligent File Transfer (BITS)
-->
168 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
CertPropSvc</CommandLine>
169 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
DsmSvc</CommandLine>
170 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -p -s
Appinfo</CommandLine>
171 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
Gpsvc</CommandLine> <!--Windows:Network: Group Policy -->
172 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
ProfSvc</CommandLine> <!--Windows: Network services-->
173 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
SENS</CommandLine> <!--Windows: Network services-->
174 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
SessionEnv</CommandLine> <!--Windows: Network services-->
175 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
Themes</CommandLine> <!--Windows: Network services-->
176 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k netsvcs -s
Winmgmt</CommandLine> <!--Windows: Windows Management Instrumentation (WMI) -->
177 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
netsvcs</CommandLine> <!--Windows: Network services-->
178 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k networkService -
-s DoSvc</CommandLine>
179 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k networkService -
Dnscache</CommandLine> <!--Windows:Network: DNS caching, other uses -->
180 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k networkService -
LanmanWorkstation</CommandLine> <!--Windows:Network: "Workstation" service, used for
SMB file-sharing connections and RDP-->
181 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k networkService -
NlaSvc</CommandLine> <!--Windows:Network: Network Location Awareness-->
182 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k networkService -
TermService</CommandLine> <!--Windows:Network: Terminal Services (RDP)-->
183 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
networkService</CommandLine> <!--Windows: Network services-->
184 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k networkService
-p</CommandLine> <!--Windows: Network services-->
185 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
networkServiceNetworkRestricted</CommandLine> <!--Windows: Network services-->
186 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
rPCSS</CommandLine> <!--Windows Services-->
187 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
secsvcs</CommandLine>
188 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
swprv</CommandLine> <!--Microsoft:Software Shadow Copy Provider-->
189 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
unistackSvcGroup</CommandLine> <!--Windows 10-->
190 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
utcsvc</CommandLine> <!--Windows Services-->
191 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
wbioSvcGroup</CommandLine> <!--Windows Services-->
192 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
werSvcGroup</CommandLine> <!--Windows: ErrorReporting-->
```

```
193 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k wusvcs -p -s
WaaSMedicSvc</CommandLine> <!--Windows: Update Medic Service [
https://www.thewindowsclub.com/windows-update-medic-service ] -->
194 <CommandLine condition="is">C:\Windows\System32\svchost.exe -k wsappx -p -s
ClipSVC</CommandLine> <!--Windows:Apps: Client License Service-->
195 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k wsappx -p -s
AppXSvc</CommandLine> <!--Windows:Apps: AppX Deployment Service-->
196 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k wsappx -s
ClipSVC</CommandLine> <!--Windows:Apps: Client License Service-->
197 <CommandLine condition="is">C:\Windows\system32\svchost.exe -k
wsappx</CommandLine> <!--Windows:Apps [ https://www.howtogeek.com/320261/what-is-
wsappx-and-why-is-it-running-on-my-pc/ ] -->
198 <ParentCommandLine condition="is">C:\Windows\system32\svchost.exe -k
netsvcs</ParentCommandLine> <!--Windows: Network services: Spawns Consent.exe-->
199 <ParentCommandLine condition="is">C:\Windows\system32\svchost.exe -k
localSystemNetworkRestricted</ParentCommandLine> <!--Windows-->
200 <CommandLine condition="is">C:\Windows\system32\deviceenroller.exe /c
/AutoEnrollMDM</CommandLine> <!--Windows: AzureAD device enrollment agent-->
201 <!--SECTION: Microsoft:Edge-->
202 <CommandLine condition="begin with">"C:\Program Files (x86)\Microsoft\Edge
Dev\Application\msedge.exe" --type=</CommandLine>
203 <!--SECTION: Microsoft:dotNet-->
204 <CommandLine condition="begin with">C:\Windows\Microsoft.NET\Framework
\v4.0.30319\ngen.exe</CommandLine> <!--Microsoft:DotNet-->
205 <CommandLine condition="begin with">C:\WINDOWS\Microsoft.NET\Framework64
\v4.0.30319\ngen.exe</CommandLine> <!--Microsoft:DotNet-->
206 <CommandLine condition="begin with">C:\Windows\Microsoft.NET\Framework
\v4.0.30319\ngentask.exe</CommandLine> <!--Microsoft:DotNet-->
207 <CommandLine condition="begin with">C:\WINDOWS\Microsoft.NET\Framework64
\v4.0.30319\ngentask.exe</CommandLine> <!--Microsoft:DotNet-->
208 <Image condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319
\mscorsvw.exe</Image> <!--Microsoft:DotNet-->
209 <Image condition="is">C:\Windows\Microsoft.NET\Framework\v4.0.30319
\mscorsvw.exe</Image> <!--Microsoft:DotNet-->
210 <Image condition="is">C:\Windows\Microsoft.Net\Framework64\v3.0\WPF
\PresentationFontCache.exe</Image> <!--Windows: Font cache service-->
211 <ParentCommandLine condition="begin with">C:\Windows\Microsoft.NET\Framework64
\v4.0.30319\ngentask.exe</ParentCommandLine>
212 <ParentImage condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319
\mscorsvw.exe</ParentImage> <!--Microsoft:DotNet-->
213 <ParentImage condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319
\ngentask.exe</ParentImage> <!--Microsoft:DotNet-->
214 <ParentImage condition="is">C:\Windows\Microsoft.NET\Framework\v4.0.30319
\mscorsvw.exe</ParentImage> <!--Microsoft:DotNet-->
215 <ParentImage condition="is">C:\Windows\Microsoft.NET\Framework\v4.0.30319
\ngentask.exe</ParentImage> <!--Microsoft:DotNet: Spawns thousands of ngen.exe
processes-->
216 <!--SECTION: Microsoft:Office-->
217 <Image condition="is">C:\Program Files\Microsoft Office\Office16
\MSOSYNC.EXE</Image> <!--Microsoft:Office: Background process for SharePoint/Office36
connectivity-->
218 <Image condition="is">C:\Program Files (x86)\Microsoft Office\Office16
\MSOSYNC.EXE</Image> <!--Microsoft:Office: Background process for SharePoint/Office36
connectivity-->
219 <Image condition="is">C:\Program Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE</Image> <!--Microsoft:Office:
Licensing service-->
220 <Image condition="is">C:\Program Files\Microsoft Office\Office16
\mssoia.exe</Image> <!--Microsoft:Office: Telemetry collector-->
221 <Image condition="is">C:\Program Files (x86)\Microsoft Office\root\Office16
```

```
\officebackgroundtaskhandler.exe</Image>
222 <!--SECTION: Microsoft:Office:Click2Run-->
223 <Image condition="is">C:\Program Files\Common Files\Microsoft Shared\ClickToRun
\OfficeC2RClient.exe</Image> <!--Microsoft:Office: Background process-->
224 <ParentImage condition="is">C:\Program Files\Common Files\Microsoft
Shared\ClickToRun\OfficeClickToRun.exe</ParentImage> <!--Microsoft:Office: Background
process-->
225 <ParentImage condition="is">C:\Program Files\Common Files\Microsoft
Shared\ClickToRun\OfficeC2RClient.exe</ParentImage> <!--Microsoft:Office: Background
process-->
226 <!--SECTION: Windows: Media player-->
227 <Image condition="is">C:\Program Files\Windows Media Player\wmpnscfg.exe</Image>
<!--Windows: Media Player Network Sharing Service Configuration Application-->
228 <!--SECTION: Google-->
229 <CommandLine condition="begin with">"C:\Program Files (x86)\Google\Chrome
\Application\chrome.exe" --type=</CommandLine> <!--Google:Chrome: massive command-lin
arguments-->
230 <CommandLine condition="begin with">"C:\Program Files\Google\Chrome\Application
\chrome.exe" --type=</CommandLine> <!--Google:Chrome: massive command-line
arguments-->
231 </ProcessCreate>
232 </RuleGroup>
233
234 <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM
[FileCreateTime]-->
235 <!--COMMENT: [ https://attack.mitre.org/wiki/Technique/T1099 ] -->
236
237 <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, CreationUtcTime
PreviousCreationUtcTime-->
238 <RuleGroup name="" groupRelation="or">
239 <FileCreateTime onmatch="include">
240 <Image name="T1099" condition="begin with">C:\Users</Image> <!--Look for
timestomping in user area, usually nothing should be doing that here-->
241 <TargetFilename name="T1099" condition="end with">.exe</TargetFilename> <!--Loc
for backdated executables anywhere-->
242 <Image name="T1099" condition="begin with">\Device
\HarddiskVolumeShadowCopy</Image> <!--Nothing should be written here | Credit:
@SBousseaden [ https://twitter.com/SBousseaden/status/1133030955407630336 ] -->
243 </FileCreateTime>
244 </RuleGroup>
245
246 <RuleGroup name="" groupRelation="or">
247 <FileCreateTime onmatch="exclude">
248 <Image condition="image">OneDrive.exe</Image> <!--OneDrive constantly changes
file times-->
249 <Image condition="image">C:\Windows\system32\backgroundTaskHost.exe</Image>
250 <Image condition="contains">setup</Image> <!--Ignore setups-->
251 <Image condition="contains">install</Image> <!--Ignore setups-->
252 <Image condition="contains">Update</Image> <!--Ignore setups-->
253 <Image condition="end with">redist.exe</Image> <!--Ignore setups-->
254 <Image condition="is">msiexec.exe</Image> <!--Ignore setups-->
255 <Image condition="is">TrustedInstaller.exe</Image> <!--Ignore setups-->
256 <TargetFilename condition="contains">\NVIDIA\NvBackend\ApplicationOntology
</TargetFilename> <!--NVIDIA GeForce Experience Application Ontology, 1000's of
events in user profile-->
257 </FileCreateTime>
258 </RuleGroup>
259
260 <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
261 <!--COMMENT: By default this configuration takes a very conservative approach to
```



```
network logging, limited to only extremely high-signal events.-->
262 <!--COMMENT: [ https://attack.mitre.org/wiki/Command_and_Control ] [
https://attack.mitre.org/wiki/Exfiltration ] [ https://attack.mitre.org
/wiki/Lateral_Movement ] -->
263 <!--TECHNICAL: For the DestinationHostname, Sysmon uses the GetNameInfo API,
which will often not have any information, and may just be a CDN. This is NOT reliabl
for filtering.-->
264 <!--TECHNICAL: For the DestinationPortName, Sysmon uses the GetNameInfo API for
the friendly name of ports you see in logs.-->
265 <!--TECHNICAL: These exe do not initiate their connections, and thus includes do
not work in this section: BITSADMIN NLTEST-->
266
267 <!-- https://www.first.org/resources/papers/conf2017/APT-Log-Analysis-Tracking-
Attack-Tools-by-Audit-Policy-and-Sysmon.pdf -->
268
269 <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, User, Protocol, Initiated,
SourceIsIpv6, SourceIp, SourceHostname, SourcePort, SourcePortName, DestinationIsIpv6
DestinationIp, DestinationHostname, DestinationPort, DestinationPortName-->
270 <RuleGroup name="" groupRelation="or">
271 <NetworkConnect onmatch="include">
272 <!--Suspicious sources for network-connecting binaries-->
273 <Image name="Usermode" condition="begin with">C:\Users</Image> <!--Tools
downloaded by users can use other processes for networking, but this is a very
valuable indicator.-->
274 <Image name="Caution" condition="begin with">C:\Recycle</Image> <!--Nothing
should operate from the RecycleBin locations.-->
275 <Image condition="begin with">C:\ProgramData</Image> <!--Normally, network
communications should be sourced from "Program Files" not from ProgramData, something
to look at-->
276 <Image condition="begin with">C:\Windows\Temp</Image> <!--Suspicious anything
would communicate from the system-level temp directory-->
277 <Image name="Caution" condition="begin with">\</Image> <!--Devices and VSC
shouldn't be executing changes | Credit: @SBousseaden @ionstorm @neu5ron
@PerchedSystems [ https://twitter.com/SwiftOnSecurity/status/1133167323991486464 ] --
278 <Image name="Caution" condition="begin with">C:\perflogs</Image> <!-- Credit
@blu3_team [ https://blu3-team.blogspot.com/2019/05/netconn-from-suspicious-
directories.html ] -->
279 <Image name="Caution" condition="begin with">C:\intel</Image> <!-- Credit
@blu3_team [ https://blu3-team.blogspot.com/2019/05/netconn-from-suspicious-
directories.html ] -->
280 <Image name="Caution" condition="begin with">C:\Windows\fonts</Image> <!--
Credit @blu3_team [ https://blu3-team.blogspot.com/2019/05/netconn-from-suspicious-
directories.html ] -->
281 <Image name="Caution" condition="begin with">C:\Windows\system32\config</Image>
<!-- Credit @blu3_team [ https://blu3-team.blogspot.com/2019/05/netconn-from-
suspicious-directories.html ] -->
282 <!--Suspicious Windows tools-->
283 <Image condition="image">at.exe</Image> <!--Windows: Remote task scheduling,
removed in Win10 | Credit @ion-storm -->
284 <Image condition="image">certutil.exe</Image> <!--Windows: Certificate tool can
contact outbound | Credit @ion-storm @FVT [ https://twitter.com/FVT/status
/834433734602530817 ] -->
285 <Image condition="image">cmd.exe</Image> <!--Windows: Remote command prompt-->
286 <Image condition="image">cmstp.exe</Image> <!--Windows: Connection manager
profiles can launch executables from WebDAV [ https://twitter.com/NickTyrer/status
/958450014111633408 ] | Credit @NickTyrer @Oddvarmoe @KyleHanslovan @subTee -->
287 <Image condition="image">cscript.exe</Image> <!--WindowsScriptingHost: | Credit
@Cyb3rOps [ https://gist.github.com/Neo23x0/a4b4af9481e01e749409 ] -->
288 <Image condition="image">driverquery.exe</Image> <!--Windows: Remote
recognisance of system configuration, oudated/vulnerable drivers -->
```

```
289     <Image condition="image">dsquery.exe</Image> <!--Microsoft: Query Active
Directory -->
290     <Image condition="image">hh.exe</Image> <!--Windows: HTML Help Executable, open
CHM files -->
291     <Image condition="image">infDefaultInstall.exe</Image> <!--Microsoft: [
https://github.com/huntresslabs/evading-autoruns ] | Credit @KyleHanslovan -->
292     <Image condition="image">java.exe</Image> <!--Java: Monitor usage of vulnerable
application and init from JAR files | Credit @ion-storm -->
293     <Image condition="image">javaw.exe</Image> <!--Java: Monitor usage of vulnerabl
application and init from JAR files -->
294     <Image condition="image">javaws.exe</Image> <!--Java: Monitor usage of
vulnerable application and init from JAR files -->
295     <Image condition="image">mmc.exe</Image> <!--Windows: -->
296     <Image condition="image">msbuild.exe</Image> <!--Windows: [ https://www.hybrid-
analysis.com/sample
/a314f6106633fba4b70f9d6ddbbee452e8f8f44a72117749c21243dc93c7ed3ac?environmentId=100 ]
-->
297     <Image condition="image">mshta.exe</Image> <!--Windows: HTML application
executes scripts without IE protections | Credit @ion-storm [ https://en.wikipedia.or
/wiki/HTML_Application ] -->
298     <Image condition="image">msiexec.exe</Image> <!--Windows: Can install from
http:// paths | Credit @vector-sec -->
299     <Image condition="image">nbtstat.exe</Image> <!--Windows: NetBIOS statistics,
attackers use to enumerate local network -->
300     <Image condition="image">net.exe</Image> <!--Windows: Note - May not detect
anything, net.exe is a front-end to lower APIs | Credit @ion-storm -->
301     <Image condition="image">net1.exe</Image> <!--Windows: Launched by "net.exe",
but it may not detect connections either -->
302     <Image condition="image">notepad.exe</Image> <!--Windows: [ https://secreary.com
/ReversingMalware/CoinMiner/ ] [ https://blog.cobaltstrike.com/2013/08/08/why-is-
notepad-exe-connecting-to-the-internet/ ] -->
303     <Image condition="image">nslookup.exe</Image> <!--Windows: Retrieve data over
DNS -->
304     <Image condition="image">powershell.exe</Image> <!--Windows: PowerShell
interface-->
305     <Image condition="image">powershell_ise.exe</Image> <!--Windows: PowerShell
interface-->
306     <Image condition="image">qprocess.exe</Image> <!--Windows: [
https://www.first.org/resources/papers/conf2017/APT-Log-Analysis-Tracking-Attack-
Tools-by-Audit-Policy-and-Sysmon.pdf ] -->
307     <Image condition="image">qwinsta.exe</Image> <!--Windows: Query remote sessions
| Credit @ion-storm -->
308     <Image condition="image">qwinsta.exe</Image> <!--Windows: Remotely query login
sessions on a server or workstation | Credit @ion-storm -->
309     <Image condition="image">reg.exe</Image> <!--Windows: Remote Registry editing
ability | Credit @ion-storm -->
310     <Image condition="image">regsvcs.exe</Image> <!--Windows: [ https://www.hybrid-
analysis.com/sample
/3f94d7080e6c5b8f59eecc3d44f7e817b31562caeba21d02ad705a0bfc63d67?environmentId=100 ]
-->
311     <Image condition="image">regsvr32.exe</Image> <!--Windows: [
https://subt0x10.blogspot.com/2016/04/bypass-application-whitelisting-script.html ]
-->
312     <Image condition="image">rundll32.exe</Image> <!--Windows: [
https://blog.cobaltstrike.com/2016/07/22/why-is-rundll32-exe-connecting-to-the-
internet/ ] -->
313     <Image condition="image">rwinsta.exe</Image> <!--Windows: Disconnect remote
sessions | Credit @ion-storm -->
314     <Image condition="image">sc.exe</Image> <!--Windows: Remotely change Windows
service settings | Credit @ion-storm -->
```

```
315     <Image condition="image">schtasks.exe</Image> <!--Windows: Command-line
interface to local and remote tasks -->
316     <Image condition="image">taskkill.exe</Image> <!--Windows: Kill processes, has
remote ability -->
317     <Image condition="image">tasklist.exe</Image> <!--Windows: List processes, has
remote ability -->
318     <Image condition="image">wmic.exe</Image> <!--WindowsManagementInstrumentation:
Credit @Cyb3r0ps [ https://gist.github.com/Neo23x0/a4b4af9481e01e749409 ] -->
319     <Image condition="image">wscript.exe</Image> <!--WindowsScriptingHost: | Credit
@arekfurt -->
320     <!--Live of the Land Binaries and scripts (LOLBAS) -->
321     <Image condition="image">bitsadmin.exe</Image> <!-- Windows: Background
Intelligent Transfer Service - Can download from URLs -->
322     <Image condition="image">esentutl.exe</Image> <!-- Windows: Database utilities
for the ESE - Can fetch from UNC paths -->
323     <Image condition="image">expand.exe</Image> <!-- Windows: Expands one or more
compressed files - Can fetch from UNC paths -->
324     <Image condition="image">extrac32.exe</Image> <!--Windows: Uncompress .cab file
- Can fetch from UNC paths -->
325     <Image condition="image">findstr.exe</Image> <!-- Windows: Search for strings -
Can fetch from UNC paths -->
326     <Image condition="image">GfxDownloadWrapper.exe</Image> <!-- Intel Graphics
Control Panel: Remote file download -->
327     <Image condition="image">ieexec.exe</Image> <!-- Windows: Microsoft .NET
Framework application - Download and execute from URLs -->
328     <Image condition="image">makecab.exe</Image> <!-- Windows: Packages existing
files into a .cab - Can fetch from UNC paths -->
329     <Image condition="image">replace.exe</Image> <!-- Windows: Used to replace file
with another file - Can fetch from UNC paths -->
330     <Image condition="image">Excel.exe</Image> <!-- Windows Office: Excel - Can
download from URLs -->
331     <Image condition="image">Powerpnt.exe</Image> <!-- Windows Office: PowerPoint -
Can download from URLs -->
332     <Image condition="image">Winword.exe</Image> <!-- Windows Office: Word - Can
download from URLs -->
333     <Image condition="image">squirrel.exe</Image> <!-- Windows: Update the
Nugget/Squirrel packages. Part of Teams. - Can download from URLs -->
334     <!--Relevant 3rd Party Tools-->
335     <Image condition="image">nc.exe</Image> <!-- Nmap's modern version of netcat [
https://nmap.org/ncat/guide/index.html#ncat-overview ] [ https://securityblog.gr
/1517/create-backdoor-in-windows-with-ncat/ ] -->
336     <Image condition="image">ncat.exe</Image> <!-- Nmap's modern version of netcat
https://nmap.org/ncat/guide/index.html#ncat-overview ] [ https://securityblog.gr
/1517/create-backdoor-in-windows-with-ncat/ ] -->
337     <Image condition="image">psexec.exe</Image> <!--Sysinternals:PsExec client side
| Credit @Cyb3r0ps -->
338     <Image condition="image">psexesvc.exe</Image> <!--Sysinternals:PsExec server
side | Credit @Cyb3r0ps -->
339     <Image condition="image">tor.exe</Image> <!--Tor [ https://www.hybrid-
analysis.com/sample
/800bf028a23440134fc834efc5c1e02cc70f05b2e800bbc285d7c92a4b126b1c?environmentId=100 ]
-->
340     <Image condition="image">vnc.exe</Image> <!-- VNC client | Credit @Cyb3r0ps -->
341     <Image condition="image">vncservice.exe</Image> <!-- VNC server | Credit
@Cyb3r0ps -->
342     <Image condition="image">vncviewer.exe</Image> <!-- VNC client | Credit
@Cyb3r0ps -->
343     <Image condition="image">winexesvc.exe</Image> <!-- Winexe service executable |
Credit @Cyb3r0ps -->
344     <Image condition="image">nmap.exe</Image>
```

```
345     <Image condition="image">psinfo.exe</Image>
346     <!--Ports: Suspicious-->
347     <DestinationPort name="SSH" condition="is">22</DestinationPort> <!--SSH
protocol, monitor admin connections-->
348     <DestinationPort name="Telnet" condition="is">23</DestinationPort> <!--Telnet
protocol, monitor admin connections, insecure-->
349     <DestinationPort name="SMTP" condition="is">25</DestinationPort> <!--SMTP mail
protocol port, insecure, used by threats-->
350     <DestinationPort name="IMAP" condition="is">143</DestinationPort> <!--IMAP mail
protocol port, insecure, used by threats-->
351     <DestinationPort name="RDP" condition="is">3389</DestinationPort> <!--
Windows:RDP: Monitor admin connections-->
352     <DestinationPort name="VNC" condition="is">5800</DestinationPort> <!--VNC
protocol: Monitor admin connections, often insecure, using hard-coded admin
password-->
353     <DestinationPort name="VNC" condition="is">5900</DestinationPort> <!--VNC
protocol Monitor admin connections, often insecure, using hard-coded admin password--
354     <DestinationPort name="Alert,Metasploit" condition="is">4444</DestinationPort>
355     <!--Ports: Proxy-->
356     <DestinationPort name="Proxy" condition="is">1080</DestinationPort> <!--Socks
proxy port | Credit @ion-storm-->
357     <DestinationPort name="Proxy" condition="is">3128</DestinationPort> <!--Socks
proxy port | Credit @ion-storm-->
358     <DestinationPort name="Proxy" condition="is">8080</DestinationPort> <!--Socks
proxy port | Credit @ion-storm-->
359     <!--Ports: Tor-->
360     <DestinationPort name="Tor" condition="is">1723</DestinationPort> <!--Tor
protocol [ https://attack.mitre.org/wiki/Technique/T1090 ] | Credit @ion-storm-->
361     <DestinationPort name="Tor" condition="is">9001</DestinationPort> <!--Tor
protocol [ http://www.computerworlduk.com/tutorial/security/tor-enterprise-2016-
blocking-malware-darknet-use-rogue-nodes-3633907/ ] -->
362     <DestinationPort name="Tor" condition="is">9030</DestinationPort> <!--Tor
protocol [ http://www.computerworlduk.com/tutorial/security/tor-enterprise-2016-
blocking-malware-darknet-use-rogue-nodes-3633907/ ] -->
363     </NetworkConnect>
364     </RuleGroup>
365
366     <RuleGroup name="" groupRelation="or">
367     <NetworkConnect onmatch="exclude">
368     <!--SECTION: Microsoft-->
369     <Image condition="begin with">C:\ProgramData\Microsoft\Windows Defender\Platfor
</Image>
370     <Image condition="end with">AppData\Local\Microsoft\Teams\current
\Teams.exe</Image> <!--Microsoft: Teams-->
371     <DestinationHostname condition="end with">.microsoft.com</DestinationHostname>
<!--Microsoft:Update delivery-->
372     <DestinationHostname condition="end
with">microsoft.com.akadns.net</DestinationHostname> <!--Microsoft:Update delivery-->
373     <DestinationHostname condition="end
with">microsoft.com.nsatc.net</DestinationHostname> <!--Microsoft:Update delivery-->
374     <!--OCSP known addresses-->
375     <DestinationIp condition="is">23.4.43.27</DestinationIp> <!--Digicert [
https://otx.alienvault.com/indicator/ip/23.4.43.27 ] -->
376     <DestinationIp condition="is">72.21.91.29</DestinationIp> <!--Digicert [
https://otx.alienvault.com/indicator/ip/72.21.91.29 ] -->
377     <!--Section: Loopback Addresses-->
378     <DestinationIp condition="is">127.0.0.1</DestinationIp> <!--Credit @ITProPaul--
379     <DestinationIp condition="begin with">fe80:0:0:0</DestinationIp> <!--Credit
@ITProPaul-->
380     </NetworkConnect>
```

```
381 </RuleGroup>
382
383 <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
384
385 <!--DATA: UtcTime, State, Version, SchemaVersion-->
386 <!--Cannot be filtered.-->
387
388 <!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
389 <!--COMMENT: Useful data in building infection timelines.-->
390
391 <!--DATA: UtcTime, ProcessGuid, ProcessId, Image-->
392 <RuleGroup name="" groupRelation="or">
393 <ProcessTerminate onmatch="include">
394 <Image condition="begin with">C:\Users</Image> <!--Process terminations by user
binaries-->
395 <Image condition="begin with">\</Image> <!--Devices and VSC shouldn't be
executing changes | Credit: @SBousseaden @ionstorm @neu5ron @PerchedSystems [
https://twitter.com/SwiftOnSecurity/status/1133167323991486464 ] -->
396 </ProcessTerminate>
397 </RuleGroup>
398
399 <RuleGroup name="" groupRelation="or">
400 <ProcessTerminate onmatch="exclude">
401 </ProcessTerminate>
402 </RuleGroup>
403
404 <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
405 <!--COMMENT: Because drivers with bugs can be used to escalate to kernel
permissions, be extremely selective
406 about what you exclude from monitoring. Low event volume, little incentive to
exclude.
407 [ https://attack.mitre.org/wiki/Technique/T1014 ] -->
408 <!--TECHNICAL: Sysmon will check the signing certificate revocation status of an
driver you don't exclude.-->
409
410 <!--DATA: UtcTime, ImageLoaded, Hashes, Signed, Signature, SignatureStatus-->
411 <RuleGroup name="" groupRelation="or">
412 <DriverLoad onmatch="exclude">
413 <Signature condition="contains">microsoft</Signature> <!--Exclude signed
Microsoft drivers-->
414 <Signature condition="contains">windows</Signature> <!--Exclude signed Microsof
drivers-->
415 <Signature condition="begin with">Intel </Signature> <!--Exclude signed Intel
drivers-->
416 </DriverLoad>
417 </RuleGroup>
418
419 <!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
420 <!--COMMENT: Can cause high system load, disabled by default.-->
421 <!--COMMENT: [ https://attack.mitre.org/wiki/Technique/T1073 ] [
https://attack.mitre.org/wiki/Technique/T1038 ] [ https://attack.mitre.org
/wiki/Technique/T1034 ] -->
422
423 <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, ImageLoaded, Hashes, Signed,
Signature, SignatureStatus-->
424 <RuleGroup name="" groupRelation="or">
425 <ImageLoad onmatch="include">
426 <!--NOTE: Using "include" with no rules means nothing in this section will be
logged-->
427 </ImageLoad>
```

```
428 </RuleGroup>
429
430 <!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
431 <!--COMMENT: Monitor for processes injecting code into other processes. Often
432 used by malware to cloak their actions. Also when Firefox loads Flash.
433 [ https://attack.mitre.org/wiki/Technique/T1055 ] -->
434 <!--DATA: UtcTime, SourceProcessGuid, SourceProcessId, SourceImage,
435 TargetProcessId, TargetImage, NewThreadId, StartAddress, StartModule, StartFunction-->
436 <RuleGroup name="" groupRelation="or">
437 <CreateRemoteThread onmatch="exclude">
438 <!--COMMENT: Exclude mostly-safe sources and log anything else.-->
439 <SourceImage condition="is">C:\Windows\system32\wbem\WmiPrvSE.exe</SourceImage>
440 <SourceImage condition="is">C:\Windows\system32\svchost.exe</SourceImage>
441 <SourceImage condition="is">C:\Windows\system32\wininit.exe</SourceImage>
442 <SourceImage condition="is">C:\Windows\system32\csrss.exe</SourceImage>
443 <SourceImage condition="is">C:\Windows\system32\services.exe</SourceImage>
444 <SourceImage condition="is">C:\Windows\system32\winlogon.exe</SourceImage>
445 <SourceImage condition="is">C:\Windows\system32\audiodg.exe</SourceImage>
446 <StartModule condition="is">C:\Windows\system32\kernel32.dll</StartModule>
447 <TargetImage condition="is">C:\Program Files (x86)\Google\Chrome\Application
448 \chrome.exe</TargetImage>
449 </CreateRemoteThread>
450 </RuleGroup>
451
452 <!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
453 <!--EVENT 9: "RawAccessRead detected"-->
454 <!--COMMENT: Can cause high system load, disabled by default.-->
455 <!--COMMENT: Monitor for raw sector-level access to the disk, often used to
456 bypass access control lists or access locked files.
457 Disabled by default since including even one entry here activates this
458 component. Reward/performance/rule maintenance decision.
459 Encourage you to experiment with this feature yourself. [
460 https://attack.mitre.org/wiki/Technique/T1067 ] -->
461 <!--COMMENT: You will likely want to set this to a full capture on domain
462 controllers, where no process should be doing raw reads.-->
463 <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, Device-->
464 <RuleGroup name="" groupRelation="or">
465 <RawAccessRead onmatch="include">
466 <!--NOTE: Using "include" with no rules means nothing in this section will be
467 logged-->
468 </RawAccessRead>
469 </RuleGroup>
470
471 <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
472 <!--EVENT 10: "Process accessed"-->
473 <!--COMMENT: Can cause high system load, disabled by default.-->
474 <!--COMMENT: Monitor for processes accessing other process' memory.-->
475 <!--DATA: UtcTime, SourceProcessGuid, SourceProcessId, SourceThreadId,
476 SourceImage, TargetProcessGuid, TargetProcessId, TargetImage, GrantedAccess,
477 CallTrace-->
478 <RuleGroup name="" groupRelation="or">
479 <ProcessAccess onmatch="include">
480 <!--NOTE: Using "include" with no rules means nothing in this section will be
481 logged-->
482 </ProcessAccess>
483 </RuleGroup>
484
```

```
477 <!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
478 <!--EVENT 11: "File created"-->
479 <!--NOTE: Other filesystem "minifilters" can make it appear to Sysmon that some
files are being written twice. This is not a Sysmon issue, per Mark Russinovich.-->
480 <!--NOTE: You may not see files detected by antivirus. Other filesystem
minifilters, like antivirus, can act before Sysmon receives the alert a file was
written.-->
481
482 <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename,
CreationUtcTime-->
483 <RuleGroup name="" groupRelation="or">
484 <FileCreate onmatch="include">
485 <TargetFilename name="T1023" condition="contains">\Start Menu</TargetFilename>
<!--Windows: Startup links and shortcut modification [ https://attack.mitre.org
/wiki/Technique/T1023 ] -->
486 <TargetFilename name="T1165" condition="contains">\Startup</TargetFilename>
<!--Microsoft:Changes to user's auto-launched files and shortcuts-->
487 <TargetFilename name="OutlookAttachment" condition="contains">\Content.Outlook
</TargetFilename> <!--Microsoft:Outlook: attachments-->
488 <TargetFilename name="Downloads" condition="contains">\Downloads
</TargetFilename> <!--Downloaded files. Does not include "Run" files in IE-->
489 <TargetFilename condition="end with">.application</TargetFilename> <!--
Microsoft:ClickOnce: [ https://blog.netspi.com/all-you-need-is-one-a-clickonce-love-
story/ ] -->
490 <TargetFilename condition="end with">.appref-ms</TargetFilename> <!--
Microsoft:ClickOnce application | Credit @ion-storm -->
491 <TargetFilename condition="end with">.bat</TargetFilename> <!--Batch
scripting-->
492 <TargetFilename condition="end with">.chm</TargetFilename>
493 <TargetFilename condition="end with">.cmd</TargetFilename> <!--Batch scripting:
Batch scripts can also use the .cmd extension | Credit: @mmazanec -->
494 <TargetFilename condition="end with">.cmdline</TargetFilename> <!--
Microsoft:dotNet: Executed by cvtres.exe-->
495 <TargetFilename name="T1176" condition="end with">.crx</TargetFilename> <!--
Chrome extension-->
496 <TargetFilename condition="end with">.dmp</TargetFilename> <!--Process dumps [
(fr) http://blog.gentilkiwi.com/securite/mimikatz/minidump ] -->
497 <TargetFilename condition="end with">.docm</TargetFilename> <!--
Microsoft:Office:Word: Macro-->
498 <TargetFilename name="DLL" condition="end with">.dll</TargetFilename> <!--
Microsoft:Office:Word: Macro-->
499 <TargetFilename name="EXE" condition="end with">.exe</TargetFilename> <!--
Executable-->
500 <TargetFilename name="ProcessHostingdotNETCode" condition="end
with">.exe.log</TargetFilename> <!-- [ https://github.com/bitsadmin/nopowershell ] |
Credit: @SBousseaden [ https://twitter.com/SBousseaden/status/1137493597769687040 ]
-->
501 <TargetFilename condition="end with">.jar</TargetFilename> <!--Java applets-->
502 <TargetFilename condition="end with">.jnlp</TargetFilename> <!--Java applets-->
503 <TargetFilename condition="end with">.jse</TargetFilename> <!--Scripting [
Example: https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-
spyware/Mal~Phires-C/detailed-analysis.aspx ] -->
504 <TargetFilename condition="end with">.hta</TargetFilename> <!--Scripting-->
505 <TargetFilename condition="end with">.job</TargetFilename> <!--Scheduled task--
506 <TargetFilename condition="end with">.pptm</TargetFilename> <!--
Microsoft:Office:Word: Macro-->
507 <TargetFilename condition="end with">.ps1</TargetFilename> <!--PowerShell [ Mor
information: http://www.hexacorn.com/blog/2014/08/27/beyond-good-ol-run-key-part-16/
-->
508 <TargetFilename condition="end with">.sct</TargetFilename> <!--Scripting |
```

```
Credit @bartblaze -->
509     <TargetFilename condition="end with">.sys</TargetFilename> <!--System driver
files-->
510     <TargetFilename condition="end with">.scr</TargetFilename> <!--System driver
files-->
511     <TargetFilename condition="end with">.vbe</TargetFilename> <!--
VisualBasicScripting-->
512     <TargetFilename condition="end with">.vbs</TargetFilename> <!--
VisualBasicScripting-->
513     <TargetFilename condition="end with">.wsc</TargetFilename> <!--Scripting |
Credit @bartblaze -->
514     <TargetFilename condition="end with">.wsf</TargetFilename> <!--Scripting |
Credit @bartblaze -->
515     <TargetFilename condition="end with">.xlsm</TargetFilename> <!--
Microsoft:Office:Word: Macro-->
516     <TargetFilename condition="end with">.ocx</TargetFilename> <!--
Microsoft:ActiveX-->
517     <TargetFilename condition="end with">proj</TargetFilename><!--
Microsoft:MSBuild:Script: [ https://twitter.com/subTee/status/885919612969394177 ] --
518     <TargetFilename condition="end with">.sln</TargetFilename><!--
Microsoft:MSBuild:Script: [ https://twitter.com/subTee/status/885919612969394177 ] --
519     <TargetFilename condition="end with">.xls</TargetFilename><!--Microsoft [
https://medium.com/@threathuntingteam/msxml-exe-and-wmic-exe-a-way-to-proxy-code-
execution-8d524f642b75 ] -->
520     <TargetFilename name="DefaultUserModified" condition="begin with">C:\Users
\Default</TargetFilename> <!--Windows: Changes to default user profile-->
521     <TargetFilename condition="begin with">C:\Windows\system32
\Drivers</TargetFilename> <!--Microsoft: Drivers dropped here-->
522     <TargetFilename condition="begin with">C:\Windows\SysWOW64
\Drivers</TargetFilename> <!--Microsoft: Drivers dropped here-->
523     <TargetFilename name="T1037,T1484" condition="begin with">C:\Windows\system32
\GroupPolicy\Machine\Scripts</TargetFilename> <!--Group policy [ More information:
http://www.hexacorn.com/blog/2017/01/07/beyond-good-ol-run-key-part-52/ ] -->
524     <TargetFilename name="T1037,T1484" condition="begin with">C:\Windows\system32
\GroupPolicy\User\Scripts</TargetFilename> <!--Group policy [ More information:
http://www.hexacorn.com/blog/2017/01/07/beyond-good-ol-run-key-part-52/ ] -->
525     <TargetFilename condition="begin with">C:\Windows\system32\Wbem</TargetFilename>
<!--Microsoft:WMI: [ More information: http://2014.hacktoergosum.org/slides
/day1_WMI_Shell_Andrei_Dumitrescu.pdf ] -->
526     <TargetFilename condition="begin with">C:\Windows\SysWOW64\Wbem</TargetFilename>
<!--Microsoft:WMI: [ More information: http://2014.hacktoergosum.org/slides
/day1_WMI_Shell_Andrei_Dumitrescu.pdf ] -->
527     <TargetFilename condition="begin with">C:\Windows\system32
\WindowsPowerShell</TargetFilename> <!--Microsoft:Powershell: Look for modifications
for persistence [ https://www.malwarearchaeology.com/cheat-sheets ] -->
528     <TargetFilename condition="begin with">C:\Windows\SysWOW64
\WindowsPowerShell</TargetFilename> <!--Microsoft:Powershell: Look for modifications
for persistence [ https://www.malwarearchaeology.com/cheat-sheets ] -->
529     <TargetFilename name="T1053" condition="begin with">C:\Windows\Tasks
\</TargetFilename> <!--Microsoft:ScheduledTasks [ https://attack.mitre.org
/wiki/Technique/T1053 ] -->
530     <TargetFilename name="T1053" condition="begin with">C:\Windows\system32
\Tasks</TargetFilename> <!--Microsoft:ScheduledTasks [ https://attack.mitre.org
/wiki/Technique/T1053 ] -->
531     <TargetFilename name="T1053" condition="begin with">C:\Windows\SysWOW64
\Tasks</TargetFilename> <!--Microsoft:ScheduledTasks [ https://attack.mitre.org
/wiki/Technique/T1053 ] -->
532     <Image condition="begin with">\Device\HarddiskVolumeShadowCopy</Image> <!--
Nothing should be executing from VSC | Credit: @SBousseaden [ https://twitter.com
/SBousseaden/status/1133030955407630336 ] -->
```



```
533     <!--Windows application compatibility-->
534     <TargetFilename condition="begin with">C:\Windows\AppPatch
\Custom</TargetFilename> <!--Windows: Application compatibility shims [
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-
persistence.html ] -->
535     <TargetFilename condition="contains">VirtualStore</TargetFilename> <!--Windows:
UAC virtualization [ https://blogs.msdn.microsoft.com/oldnewthing/20150902-00/?p=9168
] -->
536     <!--Exploitable file names-->
537     <TargetFilename condition="end with">.xls</TargetFilename> <!--Legacy Office
files are often used for attacks-->
538     <TargetFilename condition="end with">.ppt</TargetFilename> <!--Legacy Office
files are often used for attacks-->
539     <TargetFilename condition="end with">.rtf</TargetFilename> <!--RTF files often
0day malware vectors when opened by Office-->
540     </FileCreate>
541     </RuleGroup>
542
543     <RuleGroup name="" groupRelation="or">
544     <FileCreate onmatch="exclude">
545     <!--SECTION: Microsoft-->
546     <Image condition="is">C:\Program Files (x86)\EMET 5.5\EMET_Service.exe</Image>
<!--Microsoft:EMET: Writes to C:\Windows\AppPatch\-->
547     <!--SECTION: Microsoft:Office:Click2Run-->
548     <Image condition="is">C:\Program Files\Common Files\Microsoft Shared\ClickToRun
\OfficeC2RClient.exe</Image> <!-- Microsoft:Office Click2Run-->
549     <!--SECTION: Windows-->
550     <Image condition="is">C:\Windows\system32\smss.exe</Image> <!-- Windows: Sessio
Manager SubSystem: Creates swapfile.sys,pagefile.sys,hiberfile.sys-->
551     <Image condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--
Windows: Windows 10 app, creates tons of cache files-->
552     <Image condition="is">\\?\C:\Windows\system32\wbem\WMIADAP.EXE</Image> <!--
Windows: WMI Performance updates-->
553     <Image condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Windows:
Network file syncing-->
554     <TargetFilename condition="begin with">C:\Windows\system32\DriverStore\Temp\
</TargetFilename> <!-- Windows: Temp files by DrvInst.exe-->
555     <TargetFilename condition="begin with">C:\Windows\system32\wbem\Performance
\</TargetFilename> <!-- Windows: Created in wbem by WMIADAP.exe-->
556     <TargetFilename condition="begin with">C:\Windows\Installer\</TargetFilename>
<!--Windows:Installer: Ignore MSI installer files caching-->
557     <!--SECTION: Windows:Updates-->
558     <TargetFilename condition="begin with">C:\$WINDOWS.~BT\Sources\</TargetFilename
<!-- Windows: Feature updates containing lots of .exe and .sys-->
559     <Image condition="begin with">C:\Windows\winsxs\amd64_microsoft-windows</Image>
<!-- Windows: Windows update-->
560     </FileCreate>
561     </RuleGroup>
562
563     <!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
564     <!--EVENT 12: "Registry object added or deleted"-->
565     <!--EVENT 13: "Registry value set"-->
566     <!--EVENT 14: "Registry objected renamed"-->
567
568     <!--NOTE: Windows writes hundreds or thousands of registry keys a minute, so just
because you're not changing things, doesn't mean these rules aren't being run.-->
569     <!--NOTE: You do not have to spend a lot of time worrying about performance, CPUs
are fast, but it's something to consider. Every rule and condition type has a small
cost.-->
570     <!--NOTE: "contains" works by finding the first letter, then matching the second,
```

```
etc, so the first letters should be as low-occurrence as possible.-->
571 <!--NOTE: [ https://attack.mitre.org/wiki/Technique/T1112 ] -->
572
573 <!--TECHNICAL: You cannot filter on the "Details" attribute, due to performance
issues when very large keys are written, and variety of data formats-->
574 <!--TECHNICAL: Possible prefixes are HKLM, HKCR, and HKU-->
575 <!--CRITICAL: Schema version 3.30 and higher change HKLM forequals(REGISTRY\MACHINE\ an
HKU forequals(REGISTRY\USER\ and HKCR forequals(REGISTRY\MACHINE\SOFTWARE\Classes\ and
CurrentControlSet="ControlSet001"-->
576 <!--CRITICAL: Due to a bug, Sysmon versions BEFORE 7.01 may not properly log with
the new prefix style for registry keys that was originally introduced in schema
version 3.30-->
577 <!--NOTE: Because Sysmon runs as a service, it has no filtering ability for, or
concept of, HKCU or HKEY_CURRENT_USER. Use "contains" or "end with" to get around thi
limitation-->
578
579 <!-- ! CRITICAL NOTE !: It may appear this section is MISSING important entries,
but SOME RULES MONITOR MANY KEYS, so look VERY CAREFULLY to see if something is
already covered.
580 Sysmon's wildcard monitoring along with highly-tuned generic strings
cuts the rulesets down immensely, compared to doing this in other tools.
581 For example, most COM hijacking in CLSID's across the registry is
covered by a single rule monitoring a InProcServer32 wildcard-->
582
583 <!--DATA: EventType, UtcTime, ProcessGuid, ProcessId, Image, TargetObject, Detail
(can't filter on), NewName (can't filter on)-->
584 <RuleGroup name="" groupRelation="or">
585 <RegistryEvent onmatch="include">
586 <!--Autorun or Startups-->
587 <!--ADDITIONAL REFERENCE: [ http://www.ghacks.net/2016/06/04/windows-
automatic-startup-locations/ ] -->
588 <!--ADDITIONAL REFERENCE: [ https://view.officeapps.live.com
/op/view.aspx?src=https://arsenalrecon.com/downloads/resources
/Registry\_Keys\_Related\_to\_Autorun.ods ] -->
589 <!--ADDITIONAL REFERENCE: [ http://www.silentrunners.org/launchpoints.html ]
-->
590 <!--ADDITIONAL REFERENCE: [ https://www.microsoftpressstore.com/articles
/article.aspx?p=2762082&seqNum=2 ] -->
591 <!--ADDITIONAL REFERENCE: [ https://web.archive.org/web/20200116001643/http:
//scholarworks.rit.edu/cgi/viewcontent.cgi?article=1533&context=theses | Understandin
malware autostart techniques - Matthew Gottlieb ] -->
592 <TargetObject name="T1060,RunKey"
condition="contains">CurrentVersion\Run</TargetObject> <!--Windows: Wildcard for Run
keys, including RunOnce, RunOnceEx, RunServices, RunServicesOnce [Also covers termina
server] -->
593 <TargetObject name="T1060,RunPolicy" condition="contains">Policies\Explorer
\Run</TargetObject> <!--Windows: Alternate runs keys | Credit @ion-storm-->
594 <TargetObject name="T1484" condition="contains">Group
Policy\Scripts</TargetObject> <!--Windows: Group policy scripts-->
595 <TargetObject name="T1484" condition="contains">Windows\System
\Scripts</TargetObject> <!--Windows: Wildcard for Logon, Loggoff, Shutdown-->
596 <TargetObject name="T1060" condition="contains">CurrentVersion\Windows
\Load</TargetObject> <!--Windows: [ https://msdn.microsoft.com/en-us/library
/jj874148.aspx ] -->
597 <TargetObject name="T1060" condition="contains">CurrentVersion\Windows
\Run</TargetObject> <!--Windows: [ https://msdn.microsoft.com/en-us/library
/jj874148.aspx ] -->
598 <TargetObject name="T1060" condition="contains">CurrentVersion\Winlogon
\Shell</TargetObject> <!--Windows: [ https://msdn.microsoft.com/en-us/library
/ms838576\(v=winembedded.5\).aspx ] -->
```

```
599     <TargetObject name="T1060" condition="contains">CurrentVersion\Winlogon
\System</TargetObject> <!--Windows [ https://www.exterminate-it.com/malpedia/regvals
/zlob-dns-changer/118 ] -->
600     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\Notify</TargetObject> <!--Windows: Autorun location [
https://attack.mitre.org/wiki/Technique/T1004 ] [ https://www.cylance.com/windows-
registry-persistence-part-2-the-run-keys-and-search-order ] -->
601     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\Shell</TargetObject> <!--Windows: [
https://technet.microsoft.com/en-us/library/ee851671.aspx ] -->
602     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\Userinit</TargetObject> <!--Windows: Autorun location [
https://www.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-
order ] -->
603     <TargetObject condition="begin with">HKLM\Software\WOW6432Node\Microsoft\Window
NT\CurrentVersion\Drivers32</TargetObject> <!--Windows: Legacy driver loading | Credi
@ion-storm -->
604     <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Control
\Session Manager\BootExecute</TargetObject> <!--Windows: Autorun | Credit @ion-storm
[ https://www.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search
order ] -->
605     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\AeDebug</TargetObject> <!--Windows: Automatic program crash debug
program [ https://www.symantec.com/security_response
/writeup.jsp?docid=2007-050712-5453-99&tabid=2 ] -->
606     <TargetObject condition="contains">UserInitMprLogonScript</TargetObject> <!--
Windows: Legacy logon script environment variable [ http://www.hexacorn.com/blog/2014
/11/14/beyond-good-ol-run-key-part-18/ ] -->
607     <TargetObject name="T1112,ChangeStartupFolderPath" condition="end with">user
shell folders\startup</TargetObject> <!--Monitor changes to Startup folder location
for monitoring evasion | Credit @SBousseaden-->
608     <!--Services-->
609     <TargetObject name="T1031,T1050" condition="end with">\ServiceDll</TargetObject
<!--Windows: Points to a service's DLL [ https://blog.cylance.com/windows-registry-
persistence-part-1-introduction-attack-phases-and-windows-services ] -->
610     <TargetObject name="T1031,T1050" condition="end
with">\ServiceManifest</TargetObject> <!--Windows: Manifest pointing to service's DLL
[ https://www.geoffchappell.com/studies/windows/win32/services/svchost/index.htm ] --
611     <TargetObject name="T1031,T1050" condition="end with">\ImagePath</TargetObject>
<!--Windows: Points to a service's EXE [ https://attack.mitre.org/wiki/Technique/T105
] -->
612     <TargetObject name="T1031,T1050" condition="end with">\Start</TargetObject> <!--
Windows: Services start mode changes (Disabled, Automatically, Manual)-->
613     <!--RDP-->
614     <TargetObject name="RDP port change" condition="end with">Control\Terminal
Server\WinStations\RDP-Tcp\PortNumber</TargetObject> <!--Windows: RDP port change
under Control [ https://blog.menasec.net/2019/02/of-rdp-hijacking-part1-remote-
desktop.html ]-->
615     <TargetObject name="RDP port change" condition="end with">Control\Terminal
Server\fsingleSessionPerUser</TargetObject> <!--Windows: Allow same user to have
mutliple RDP sessions, to hide from admin being impersonated-->
616     <TargetObject name="ModifyRemoteDesktopState" condition="end
with">fDenyTSConnections</TargetObject> <!--Windows: Attacker turning on RDP-->
617     <TargetObject condition="end with">LastLoggedOnUser</TargetObject> <!--Windows:
Changing last-logged in user-->
618     <TargetObject name="ModifyRemoteDesktopPort" condition="end with">RDP-
tcp\PortNumber</TargetObject> <!--Windows: Changing RDP port to evade IDS-->
619     <TargetObject condition="end with">Services\PortProxy\v4tov4</TargetObject> <!--
Windows: Changing RDP port to evade IDS-->
620     <!--CLSID launch commands and Default File Association changes-->
```

```
621     <TargetObject name="T1042" condition="contains">\command\</TargetObject> <!--
Windows: Sensitive sub-key under file associations and CLSID that map to launch
command-->
622     <TargetObject name="T1122" condition="contains">\ddeexec\</TargetObject> <!--
Windows: Sensitive sub-key under file associations and CLSID that map to launch
command-->
623     <TargetObject name="T1122" condition="contains">{86C86720-42A0-1069-
A2E8-08002B30309D}\</TargetObject> <!--Windows: Tooltip handler-->
624     <TargetObject name="T1042" condition="contains">exefile\</TargetObject> <!--
Windows Executable handler, to log any changes not already monitored-->
625     <!--Windows COM-->
626     <TargetObject name="T1122" condition="end with">\InprocServer32\(\Default)
</TargetObject> <!--Windows:COM Object Hijacking [ https://blog.gdatasoftware.com
/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence ] | Credit @ion-
storm -->
627     <!--Windows shell visual modifications used by malware-->
628     <TargetObject name="T1158" condition="end with">\Hidden</TargetObject> <!--
Windows:Explorer: Some types of malware try to hide their hidden system files from th
user, good signal event -->
629     <TargetObject name="T1158" condition="end with">\ShowSuperHidden</TargetObject>
<!--Windows:Explorer: Some types of malware try to hide their hidden system files fro
the user, good signal event [ Example: https://www.symantec.com/security_response
/writeup.jsp?docid=2007-061811-4341-99&tabid=2 ] -->
630     <TargetObject name="T1158" condition="end with">\HideFileExt</TargetObject> <!--
Windows:Explorer: Some malware hides file extensions to make diagnosis/disinfection
more daunting to novice users -->
631     <!--Windows shell hijack and modifications-->
632     <TargetObject condition="contains">Classes\*\</TargetObject> <!--
Windows:Explorer: [ http://www.silentrunners.org/launchpoints.html ] -->
633     <TargetObject condition="contains">Classes\AllFilesystemObjects\</TargetObject>
<!--Windows:Explorer: [ http://www.silentrunners.org/launchpoints.html ] -->
634     <TargetObject condition="contains">Classes\Directory\</TargetObject> <!--
Windows:Explorer: [ https://stackoverflow.com/questions/1323663/windows-shell-context
menu-option ] -->
635     <TargetObject condition="contains">Classes\Drive\</TargetObject> <!--
Windows:Explorer: [ https://stackoverflow.com/questions/1323663/windows-shell-context
menu-option ] -->
636     <TargetObject condition="contains">Classes\Folder\</TargetObject> <!--
Windows:Explorer: ContextMenuHandlers, DragDropHandlers, CopyHookHandlers, [
https://stackoverflow.com/questions/1323663/windows-shell-context-menu-option ] -->
637     <TargetObject condition="contains">Classes\PROTOCOLS\</TargetObject> <!--
Windows:Explorer: Protocol handlers-->
638     <TargetObject condition="contains">ContextMenuHandlers\</TargetObject> <!--
Windows: [ http://oalabs.openanalysis.net/2015/06/04/malware-persistence-
hkey_current_user-shell-extension-handlers/ ] -->
639     <TargetObject condition="contains">CurrentVersion\Shell</TargetObject> <!--
Windows: Shell Folders, ShellExecuteHooks, ShellIconOverloadIdentifiers,
ShellServiceObjects, ShellServiceObjectDelayLoad [ http://oalabs.openanalysis.net
/2015/06/04/malware-persistence-hkey_current_user-shell-extension-handlers/ ] -->
640     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
\CurrentVersion\explorer\ShellExecuteHooks</TargetObject> <!--Windows:
ShellExecuteHooks-->
641     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
\CurrentVersion\explorer\ShellServiceObjectDelayLoad</TargetObject> <!--Windows:
ShellExecuteHooks-->
642     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
\CurrentVersion\explorer\ShellIconOverlayIdentifiers</TargetObject> <!--Windows:
ShellExecuteHooks-->
643     <!--AppPaths hijacking-->
644     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
```

```
\CurrentVersion\App Paths\</TargetObject> <!--Windows: Credit to @Hexacorn [
http://www.hexacorn.com/blog/2013/01/19/beyond-good-ol-run-key-part-3/ ] -->
645 <!--Terminal service boobytrap-->
646 <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Control
\Terminal Server\WinStations\RDP-Tcp\InitialProgram</TargetObject> <!--Windows:RDP:
Note other Terminal Server run keys are handled by another wildcard already-->
647 <!--Group Policy integrity-->
648 <TargetObject name="T1484" condition="begin with">HKLM\Software\Microsoft
\Windows NT\CurrentVersion\Winlogon\GPExtensions\</TargetObject> <!--Windows: Group
Policy internally uses a plug-in architecture that nothing should be modifying-->
649 <!--Winsock and Winsock2-->
650 <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Services
\WinSock</TargetObject> <!--Windows: Wildcard, includes Winsock and Winsock2-->
651 <TargetObject condition="end with">\ProxyServer</TargetObject> <!--Windows:
System and user proxy server-->
652 <!--Credential providers-->
653 <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
\CurrentVersion\Authentication\Credential Provider</TargetObject> <!--Wildcard,
includes Credential Providers and Credential Provider Filters-->
654 <TargetObject name="T1101" condition="begin with">HKLM\SYSTEM\CurrentControlSet
\Control\Lsa\</TargetObject> <!-- [ https://attack.mitre.org/wiki/Technique/T1131 ] [
https://attack.mitre.org/wiki/Technique/T1101 ] -->
655 <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Control
\SecurityProviders</TargetObject> <!--Windows: Changes to WDigest-UseLogonCredential
for password scraping [ https://www.trustedsec.com/april-2015/dumping-wdigest-creds-
with-meterpreter-mimikatzkiwi-in-windows-8-1/ ] -->
656 <TargetObject condition="begin with">HKLM\Software\Microsoft
\Netsh</TargetObject> <!--Windows: Netsh helper DLL [ https://attack.mitre.org
/wiki/Technique/T1128 ] -->
657 <TargetObject condition="contains">Software\Microsoft\Windows\CurrentVersion
\Internet Settings\ProxyEnable</TargetObject> <!--Windows: Malware often disables a
web proxy for 2nd stage downloads -->
658 <!--Networking-->
659 <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Control
\NetworkProvider\Order\</TargetObject> <!--Windows: Order of network providers that
are checked to connect to destination [ https://www.malwarearchaeology.com/cheat-
sheets ] -->
660 <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
NT\CurrentVersion\NetworkList\Profiles</TargetObject> <!--Windows: | Credit @ion-stor
-->
661 <TargetObject name="T1089" condition="end with">\EnableFirewall</TargetObject>
<!--Windows: Monitor for firewall disablement, all firewall profiles [
https://attack.mitre.org/wiki/Technique/T1089 ] -->
662 <TargetObject name="T1089" condition="end
with">\DoNotAllowExceptions</TargetObject> <!--Windows: Monitor for firewall
disablement, all firewall profiles [ https://attack.mitre.org/wiki/Technique/T1089 ]
-->
663 <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Services
\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications
\List</TargetObject> <!--Windows Firewall authorized applications for all networks|
Credit @ion-storm -->
664 <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Services
\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications
\List</TargetObject> <!--Windows Firewall authorized applications for domain networks
-->
665 <!--DLLs that get injected into every process at launch-->
666 <TargetObject name="T1103" condition="begin with">HKLM\Software\Microsoft
\Windows NT\CurrentVersion\Windows\Appinit_Dlls\</TargetObject> <!--Windows: Feature
disabled by default [ https://attack.mitre.org/wiki/Technique/T1103 ] -->
667 <TargetObject name="T1103" condition="begin with">HKLM\Software\Wow6432Node
```

```
\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls\</TargetObject> <!--Windows
Feature disabled by default [ https://attack.mitre.org/wiki/Technique/T1103 ] -->
668   <TargetObject condition="begin with">HKLM\SYSTEM\CurrentControlSet\Control
\Session Manager\AppCertDlls\</TargetObject> <!--Windows: Credit to @Hexacorn [
http://www.hexacorn.com/blog/2013/01/19/beyond-good-ol-run-key-part-3/ ] [
https://blog.comodo.com/malware/trojware-win32-trojanspy-volisk-a/ ] -->
669   <!--Office-->
670   <TargetObject name="T1137" condition="contains">Microsoft\Office\Outlook\Addins
\</TargetObject> <!--Microsoft:Office: Outlook add-ins, access to sensitive data and
often cause issues-->
671   <TargetObject name="T1137" condition="contains">Office Test\</TargetObject> <!--
Microsoft:Office: Persistence method [ http://www.hexacorn.com/blog/2014/04/16/beyond
good-ol-run-key-part-10/ ] | Credit @Hexacorn -->
672   <TargetObject name="Context,ProtectedModeExitOrMacrosUsed"
condition="contains">Security\Trusted Documents\TrustRecords</TargetObject> <!--
Microsoft:Office: Monitor when "Enable editing" or "Enable macros" is used | Credit
@OutflankNL | [ https://outflank.nl/blog/2018/01/16/hunting-for-evil-detect-macros-
being-executed/ ] -->
673   <TargetObject name="Context,ContactedDomain" condition="end
with">\EnableBHO</TargetObject> <!--Microsoft:Office: Contacted domains stored here
'HKEY_CURRENT_USER\<SID>\SOFTWARE\Microsoft\Office\16.0\Common\Internet\Server Cache\
<domain>\EnableBHO' -->
674   <!--IE-->
675   <TargetObject name="T1176" condition="contains">Internet Explorer\Toolbar
\</TargetObject> <!--Microsoft:InternetExplorer: Machine and user [ Example:
https://www.exterminate-it.com/malpedia/remove-mywebsearch ] -->
676   <TargetObject name="T1176" condition="contains">Internet Explorer\Extensions
\</TargetObject> <!--Microsoft:InternetExplorer: Machine and user [ Example:
https://www.exterminate-it.com/malpedia/remove-mywebsearch ] -->
677   <TargetObject name="T1176" condition="contains">Browser Helper Objects\
</TargetObject> <!--Microsoft:InternetExplorer: Machine and user [
https://msdn.microsoft.com/en-us/library/bb250436(v=vs.85).aspx ] -->
678   <TargetObject condition="end with">\DisableSecuritySettingsCheck</TargetObject>
679   <TargetObject condition="end with">\3\1206</TargetObject> <!--
Microsoft:InternetExplorer: Malware sometimes assures scripting is on in Internet Zone
[ https://support.microsoft.com/en-us/help/182569/internet-explorer-security-zones-
registry-entries-for-advanced-users ] -->
680   <TargetObject condition="end with">\3\2500</TargetObject> <!--
Microsoft:InternetExplorer: Malware sometimes disables Protected Mode in Internet Zone
[ https://blog.avast.com/2013/08/12/your-documents-are-corrupted-from-image-to-an-
information-stealing-trojan/ ] -->
681   <TargetObject condition="end with">\3\1809</TargetObject> <!--
Microsoft:InternetExplorer: Malware sometimes disables Pop-up Blocker in Internet Zone
[ https://support.microsoft.com/en-us/help/182569/internet-explorer-security-zones-
registry-entries-for-advanced-users ] -->
682   <!--Magic registry keys-->
683   <TargetObject condition="begin with">HKLM\Software\Classes\CLSID\{AB8902B4-09CA
4BB6-B78D-A8F59079A8D5}\</TargetObject> <!--Windows: Thumbnail cache autostart [
http://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-levels-up-with-
new-autostart-mechanism/ ] -->
684   <TargetObject condition="begin with">HKLM\Software\Classes\WOW6432Node\CLSID
\{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}\</TargetObject> <!--Windows: Thumbnail cache
autostart [ http://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-
levels-up-with-new-autostart-mechanism/ ] -->
685   <TargetObject condition="begin with">HKLM\Software\Classes\CLSID\{083863F1-70DE
11d0-BD40-00A0C911CE86}\</TargetObject> <!--Windows: DirectX instances-->
686   <TargetObject condition="begin with">HKLM\Software\Classes\WOW6432Node\CLSID
\{083863F1-70DE-11d0-BD40-00A0C911CE86}\</TargetObject> <!--Windows: DirectX
instances-->
687   <!--Install/Run artifacts-->
```

```
688     <TargetObject condition="end with">\UrlUpdateInfo</TargetObject> <!--
Microsoft:ClickOnce: Source URL is stored in this value [
https://subt0x10.blogspot.com/2016/12/mimikatz-delivery-via-clickonce-with.html ] -->
689     <TargetObject condition="end with">\InstallSource</TargetObject> <!--Windows:
Source folder for certain program and component installations-->
690     <TargetObject name="Alert,Sysinternals Tool Used" condition="end
with">\EulaAccepted</TargetObject> <!--Sysinternals tool launched. Lots of useful
abilities for attackers -->
691     <!--Antivirus tampering-->
692     <TargetObject name="T1089,Tamper-Defender" condition="end
with">\DisableAntiSpyware</TargetObject> <!--Windows:Defender: State modified via
registry-->
693     <TargetObject name="T1089,Tamper-Defender" condition="end
with">\DisableAntiVirus</TargetObject> <!--Windows:Defender: State modified via
registry-->
694     <TargetObject name="T1089,Tamper-Defender" condition="end
with">\SpynetReporting</TargetObject> <!--Windows:Defender: State modified via
registry-->
695     <TargetObject name="T1089,Tamper-Defender" condition="end
with">DisableRealtimeMonitoring</TargetObject> <!--Windows:Defender: State modified
via registry-->
696     <TargetObject name="T1089,Tamper-Defender" condition="end
with">\SubmitSamplesConsent</TargetObject> <!--Windows:Defender: State modified via
registry-->
697     <TargetObject name="T1562,Tamper-Defender" condition="begin with">HKLM\SOFTWARE
\Policies\Microsoft\Windows Defender\Exclusions\</TargetObject> <!--Windows:Defender:
Exclusions in policy key-->
698     <!--Windows UAC tampering-->
699     <TargetObject name="T1088" condition="end with">HKLM\Software\Microsoft\Windows
\CurrentVersion\Policies\System\EnableLUA</TargetObject> <!--Detect: UAC Tampering |
Credit @ion-storm -->
700     <TargetObject name="T1088" condition="end with">HKLM\Software\Microsoft\Windows
\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy</TargetObject> <!--
Detect: UAC Tampering | Credit @ion-storm -->
701     <!--Microsoft Security Center tampering | Credit @ion-storm -->
702     <TargetObject name="T1089,Tamper-SecCenter" condition="end with">HKLM\Software
\Microsoft\Security Center\</TargetObject> <!-- [ https://attack.mitre.org
/wiki/Technique/T1089 ] -->
703     <TargetObject name="T1089,Tamper-SecCenter" condition="end
with">SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
\HideSCAHealth</TargetObject> <!--Windows:Security Center: Malware sometimes disables
[ https://blog.avast.com/2013/08/12/your-documents-are-corrupted-from-image-to-an-
information-stealing-trojan/ ] -->
704     <!--Windows application compatibility-->
705     <TargetObject name="T1138,AppCompatShim" condition="begin with">HKLM\Software
\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom</TargetObject> <!--Windows
AppCompat [ https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-
persistence.html ] -->
706     <TargetObject name="T1138,AppCompatShim" condition="begin with">HKLM\Software
\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB</TargetObject> <!--
Windows: AppCompat [ https://attack.mitre.org/wiki/Technique/T1138 ] -->
707     <TargetObject condition="contains">VirtualStore</TargetObject> <!--Windows:
Registry virtualization, something's wrong if it's in use [ https://msdn.microsoft.co
/en-us/library/windows/desktop/aa965884(v=vs.85).aspx ] -->
708     <!--Windows internals integrity monitoring-->
709     <TargetObject name="T1183,IFE0" condition="begin with">HKLM\Software\Microsoft
\Windows NT\CurrentVersion\Image File Execution Options\</TargetObject> <!--Windows:
Malware likes changing IFE0, like adding Debugger to disable antivirus EXE-->
710     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
\CurrentVersion\WINEVT\</TargetObject> <!--Windows: Event log system integrity and
```

```
ACLs-->
711     <TargetObject name="Tamper-Safemode" condition="begin with">HKLM\SYSTEM
\CurrentControlSet\Control\Safeboot\</TargetObject> <!--Windows: Services approved to
load in safe mode. Almost nothing should ever modify this.-->
712     <TargetObject name="Tamper-Winlogon" condition="begin with">HKLM\SYSTEM
\CurrentControlSet\Control\Winlogon\</TargetObject> <!--Windows: Providers notified b
WinLogon-->
713     <TargetObject name="Context,DeviceConnectedOrUpdated" condition="end
with">\FriendlyName</TargetObject> <!--Windows: New devices connected and
remembered-->
714     <TargetObject name="Context,MsiInstallerStarted" condition="is">HKLM\Software
\Microsoft\Windows\CurrentVersion\Installer\InProgress\Default</TargetObject> <!--
Windows: See when WindowsInstaller is engaged, useful for timeline matching with othe
events-->
715     <TargetObject name="Tamper-Tracing" condition="begin with">HKLM\Software
\Microsoft\Tracing\RASAPI32</TargetObject> <!--Windows: Malware sometimes disables
tracing to obfuscate tracks-->
716     <TargetObject name="Context,ProcessAccessedPrivateResource" condition="begin
with">HKLM\Software\Microsoft\Windows\CurrentVersion\CapabilityAccessManager
\ConsentStore\</TargetObject> <!-- Windows: Win10 tracks when and what process uses
webcam/microphone/location etc [ https://medium.com/@7a616368/can-you-track-processes
accessing-the-camera-and-microphone-7e6885b37072 ] -->
717     <TargetObject condition="contains">\Keyboard Layout\Preload</TargetObject> <!--
Microsoft:Windows: Keyboard layout loaded into user session [
https://renenyffenegger.ch/notes/Windows/registry/tree/HKEY_CURRENT_USER/Keyboard-
Layout/Preload/index ] | Credit @cyb3rops -->
718     <TargetObject condition="contains">\Keyboard Layout\Substitutes</TargetObject>
<!--Microsoft:Windows: Keyboard layout loaded into user session [
https://renenyffenegger.ch/notes/Windows/registry/tree/HKEY_CURRENT_USER/Keyboard-
Layout/Preload/index ] | Credit @cyb3rops -->
719     <!--Windows inventory events-->
720     <TargetObject name="InvDB-Path" condition="end
with">\LowerCaseLongPath</TargetObject> <!-- [ https://binaryforay.blogspot.com
/2017/10/amcache-still-rules-everything-around.html ] -->
721     <TargetObject name="InvDB-Pub" condition="end with">\Publisher</TargetObject>
<!-- [ https://binaryforay.blogspot.com/2017/10/amcache-still-rules-everything-
around.html ] -->
722     <TargetObject name="InvDB-Ver" condition="end
with">\BinProductVersion</TargetObject> <!-- [ https://docs.microsoft.com/en-
us/windows/privacy/basic-level-windows-diagnostic-events-and-fields-1709 ] -->
723     <TargetObject name="InvDB-DriverVer" condition="end
with">\DriverVersion</TargetObject> <!-- [ https://df-stream.com/2015/02/leveraging-
devicecontainers-key/ ] -->
724     <TargetObject name="InvDB-DriverVer" condition="end
with">\DriverVerVersion</TargetObject> <!-- [ https://df-stream.com/2015/02
/leveraging-devicecontainers-key/ ] -->
725     <TargetObject name="InvDB-CompileTimeClaim" condition="end
with">\LinkDate</TargetObject> <!-- Compile time of EXE, may not be reliable [
https://en.wikipedia.org/wiki/Link_time ] -->
726     <TargetObject name="InvDB" condition="contains">Compatibility Assistant\Store
\</TargetObject> <!-- Inventory -->
727     <!--Suspicious sources-->
728     <Image name="Suspicious,ImageBeginWithBackslash" condition="end
with">regedit.exe</Image> <!--Users and helpdesk staff making system modifications --
729     <Image name="Suspicious,ImageBeginWithBackslash" condition="begin with">\
</Image> <!--Devices and VSC shouldn't be executing changes | Credit: @SBousseaden
@ionstorm @neu5ron @PerchedSystems [ https://twitter.com/SwiftOnSecurity/status
/1133167323991486464 ] -->
730     </RegistryEvent>
731 </RuleGroup>
```



```
732
733 <RuleGroup name="" groupRelation="or">
734   <RegistryEvent onmatch="exclude">
735     <!--COMMENT: Remove low-information noise. Often these hide a process recreatin
an empty key and do not hide the values created subsequently.-->
736     <!--NOTE: A lot of noise can be removed by excluding CreateKey events, which are
largely innocuous-->
737     <TargetObject condition="contains">\\{CAFEEFAC-</TargetObject>
738     <EventType condition="is">CreateKey</EventType>
739     <TargetObject condition="begin with">HKLM\COMPONENTS</TargetObject>
740     <!--Inventory noise-->
741     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
\CurrentVersion\AppModel\StateRepository\Cache</TargetObject>
742     <!--Misc-->
743     <TargetObject condition="end with">Toolbar\WebBrowser</TargetObject> <!--
Microsoft:IE: Extraneous activity-->
744     <TargetObject condition="end with">Browser\ITBar7Height</TargetObject> <!--
Microsoft:IE: Extraneous activity, covers ShellBrowser and WebBrowser-->
745     <TargetObject condition="end with">Browser\ITBar7Layout</TargetObject> <!--
Microsoft:IE: Extraneous activity-->
746     <TargetObject condition="end with">Internet Explorer\Toolbar
\Locked</TargetObject> <!--Windows:Explorer: Extraneous activity-->
747     <TargetObject condition="end with">Toolbar\WebBrowser\{47833539-
D0C5-4125-9FA8-0819E2EAAC93}</TargetObject> <!--Windows:Explorer: Extraneous
activity-->
748     <TargetObject condition="end with">}\PreviousPolicyAreas</TargetObject> <!--
Windows: Remove noise from \Winlogon\GPEExtensions by svchost.exe-->
749     <TargetObject condition="contains">\Control\WMI\Autologger\</TargetObject> <!--
Windows: Remove noise from monitoring "\Start"-->
750     <TargetObject condition="end with">HKLM\SYSTEM\CurrentControlSet\Services\Usosv
\Start</TargetObject> <!--Windows: Remove noise from monitoring "\Start"-->
751     <TargetObject condition="end with">\Lsa\OfflineJoin\CurrentValue</TargetObject>
<!--Windows: Sensitive value during domain join-->
752     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
\CurrentVersion\Installer\UserData\S-1-5-18\</TargetObject> <!--Windows: Remove noise
monitoring installations run as system-->
753     <TargetObject condition="contains">_Classes\AppX</TargetObject> <!--Windows:
Remove noise monitoring "Shell\open\command"--> <!--Win8+-->
754     <TargetObject condition="begin with">HKLM\Software\Microsoft\Windows
\CurrentVersion\WINEVT\Publishers\</TargetObject> <!--Windows: SvcHost Noise-->
755     <!--Bootup Control noise-->
756     <TargetObject condition="end with">HKLM\SYSTEM\CurrentControlSet\Control
\Lsa\LsaPid</TargetObject> <!--Windows:lsass.exe: Boot noise-->
757     <TargetObject condition="end with">HKLM\SYSTEM\CurrentControlSet\Control
\Lsa\SspiCache</TargetObject> <!--Windows:lsass.exe: Boot noise--> <!--Win8+-->
758     <TargetObject condition="end with">HKLM\SYSTEM\CurrentControlSet\Control
\Lsa\Kerberos\Domains</TargetObject> <!--Windows:lsass.exe: Boot noise--> <!--Win8+-->
759     <!--Services startup settings noise, some low-risk services routinely change it
and this can be ignored-->
760     <TargetObject condition="end with">\Services\BITS\Start</TargetObject> <!--
Windows: Remove noise from monitoring "\Start"-->
761     <TargetObject condition="end with">\services\clr_optimization_v2.0.50727_32
\Start</TargetObject> <!--Microsoft:dotNet: Windows 7-->
762     <TargetObject condition="end with">\services\clr_optimization_v2.0.50727_64
\Start</TargetObject> <!--Microsoft:dotNet: Windows 7-->
763     <TargetObject condition="end with">\services\clr_optimization_v4.0.30319_32
\Start</TargetObject> <!--Microsoft:dotNet: Windows 10-->
764     <TargetObject condition="end with">\services\clr_optimization_v4.0.30319_64
\Start</TargetObject> <!--Microsoft:dotNet: Windows 10-->
765     <TargetObject condition="end with">\services\deviceAssociationService
```

```
\Start</TargetObject> <!--Windows: Remove noise from monitoring "\Start"-->
766 <TargetObject condition="end with">\services\fhsvc\Start</TargetObject> <!--
Windows: File History Service-->
767 <TargetObject condition="end with">\services\nal\Start</TargetObject> <!--Intel
Network adapter diagnostic driver-->
768 <TargetObject condition="end with">\services\trustedInstaller
\Start</TargetObject> <!--Windows: Remove noise from monitoring "\Start"-->
769 <TargetObject condition="end with">\services\tunnel\Start</TargetObject> <!--
Windows: Remove noise from monitoring "\Start"-->
770 <TargetObject condition="end with">\services\usoSvc\Start</TargetObject> <!--
Windows: Remove noise from monitoring "\Start"-->
771 <!--FileExts noise filtering-->
772 <TargetObject condition="end with">\UserChoice\ProgId</TargetObject> <!--
Windows: Remove noise from monitoring "FileExts"--> <!--Win8+-->
773 <TargetObject condition="end with">\UserChoice\Hash</TargetObject> <!--Windows:
Remove noise from monitoring "FileExts"--> <!--Win8+-->
774 <TargetObject condition="end with">\OpenWithList\MRUList</TargetObject> <!--
Windows: Remove noise from monitoring "FileExts"-->
775 <TargetObject condition="contains">Shell Extentions\Cached</TargetObject> <!--
Windows: Remove noise generated by explorer.exe on monitored ShellCached binary
keys--> <!--Win8+-->
776 <!--Group Policy noise-->
777 <TargetObject condition="end with">HKLM\System\CurrentControlSet\Control
\Lsa\Audit\SpecialGroups</TargetObject> <!--Windows: Routinely set through Group
Policy, not especially important to log-->
778 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Startup\0\PSScriptOrder</TargetObject> <!--Windows:Group Policy
Noise below the actual key while building-->
779 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Startup\0\SOM-ID</TargetObject> <!--Windows:Group Policy: Noise
below the actual key while building-->
780 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Startup\0\GPO-ID</TargetObject> <!--Windows:Group Policy: Noise
below the actual key while building-->
781 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Startup\0\0\IsPowershell</TargetObject> <!--Windows:Group
Policy: Noise below the actual key while building-->
782 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Startup\0\0\ExecTime</TargetObject> <!--Windows:Group Policy:
Noise below the actual key while building-->
783 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Shutdown\0\PSScriptOrder</TargetObject> <!--Windows:Group
Policy: Noise below the actual key while building-->
784 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Shutdown\0\SOM-ID</TargetObject> <!--Windows:Group Policy: Nois
below the actual key while building-->
785 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Shutdown\0\GPO-ID</TargetObject> <!--Windows:Group Policy: Nois
below the actual key while building-->
786 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Shutdown\0\0\IsPowershell</TargetObject> <!--Windows:Group
Policy: Noise below the actual key while building-->
787 <TargetObject condition="end with">SOFTWARE\Microsoft\Windows\CurrentVersion
\Group Policy\Scripts\Shutdown\0\0\ExecTime</TargetObject> <!--Windows:Group Policy:
Noise below the actual key while building-->
788 <TargetObject condition="contains">\safer\codeidentifiers\0\HASHES
\{</TargetObject> <!--Windows: Software Restriction Policies. Can be used to disable
security tools, but very noisy to monitor if you use it-->
789 <!--SECTION: Office C2R-->
790 <TargetObject condition="contains">VirtualStore\MACHINE\SOFTWARE\Microsoft
```

```
\Office\ClickToRun\</TargetObject> <!--Microsoft: SearchProtocolHost writes to
OfficeC2R registry for Outlook, seemingly regarding mail indexing-->
791 <TargetObject condition="begin with">HKLM\SOFTWARE\Microsoft\Office\ClickToRun
\</TargetObject> <!--Microsoft: Virtual registry for Office-->
792 <!--SECTION: 3rd party-->
793 <Image condition="is">C:\Program Files\WIDCOMM\Bluetooth
Software\btwdins.exe</Image> <!--Constantly writes to HKLM-->
794 <TargetObject condition="begin with">HKCR\VLC.</TargetObject> <!--VLC update
noise-->
795 <TargetObject condition="begin with">HKCR\iTunes.</TargetObject> <!--Apple:
iTunes update noise-->
796 <!--WINEVT publishers noise-->
797 <TargetObject condition="is">HKLM\Software\Microsoft\Windows\CurrentVersion
\WINEVT\Publishers\{945a8954-c147-4acd-923f-40c45405a658}</TargetObject> <!--Windows
update-->
798 </RegistryEvent>
799 </RuleGroup>
800
801 <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
802 <!--EVENT 15: "File stream created"-->
803 <!--COMMENT: Any files created with an NTFS Alternate Data Stream which match
these rules will be hashed and logged.
804 [ https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams
in-ntfs/ ]
805 ADS's are used by browsers and email clients to mark files as originating from
the Internet or other foreign sources.
806 [ https://textslashplain.com/2016/04/04/downloads-and-the-mark-of-the-web/ ] --
807 <!--NOTE: Other filesystem minifilters can make it appear to Sysmon that some
files are being written twice. This is not a Sysmon issue, per Mark Russinovich.-->
808
809 <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, CreationUtcTime
Hash-->
810 <FileCreateStreamHash onmatch="include">
811 <TargetFilename condition="contains">Downloads</TargetFilename> <!--Downloaded
files. Does not include "Run" files in IE-->
812 <TargetFilename condition="contains">Temp\7z</TargetFilename> <!--7zip
extractions-->
813 <TargetFilename condition="contains">Startup</TargetFilename> <!--ADS startup |
Example: [ https://www.hybrid-analysis.com/sample
/a314f6106633fba4b70f9d6ddbee452e8f8f44a72117749c21243dc93c7ed3ac?environmentId=100 ]
-->
814 <TargetFilename condition="end with">.bat</TargetFilename> <!--Batch
scripting-->
815 <TargetFilename condition="end with">.cmd</TargetFilename> <!--Batch scripting
Credit @ion-storm -->
816 <TargetFilename condition="end with">.doc</TargetFilename> <!--Office doc
potentially with macro -->
817 <TargetFilename condition="end with">.hta</TargetFilename> <!--Scripting-->
818 <TargetFilename condition="end with">.jse</TargetFilename> <!--Registry File-->
819 <TargetFilename condition="end with">.lnk</TargetFilename> <!--Shortcut file |
Credit @ion-storm -->
820 <TargetFilename condition="end with">.ppt</TargetFilename> <!--Office doc
potentially with macros-->
821 <TargetFilename condition="end with">.ps1</TargetFilename> <!--PowerShell-->
822 <TargetFilename condition="end with">.ps2</TargetFilename> <!--PowerShell-->
823 <TargetFilename condition="end with">.reg</TargetFilename> <!--Registry File-->
824 <TargetFilename condition="end with">.sct</TargetFilename> <!--Scripting |
Credit @bartblaze -->
825 <TargetFilename condition="end with">.vb</TargetFilename> <!--
VisualBasicScripting files-->
```

```
826     <TargetFilename condition="end with">.vbe</TargetFilename> <!--
VisualBasicScripting files-->
827     <TargetFilename condition="end with">.vbs</TargetFilename> <!--
VisualBasicScripting files-->
828     <TargetFilename condition="end with">.wsc</TargetFilename> <!--Scripting |
Credit @bartblaze -->
829     <TargetFilename condition="end with">.wsf</TargetFilename> <!--Scripting |
Credit @bartblaze -->
830   </FileCreateStreamHash>
831
832   <RuleGroup name="" groupRelation="or">
833     <FileCreateStreamHash onmatch="exclude">
834       </FileCreateStreamHash>
835   </RuleGroup>
836
837   <!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
838   <!--EVENT 16: "Sysmon config state changed"-->
839   <!--COMMENT: This ONLY logs if the hash of the configuration changes. Running
"sysmon.exe -c" with the current configuration will not be logged with Event 16-->
840
841   <!--DATA: UtcTime, Configuration, ConfigurationFileHash-->
842   <!--Cannot be filtered.-->
843
844   <!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
845   <!--EVENT 17: "Pipe Created"-->
846   <!--EVENT 18: "Pipe Connected"-->
847
848   <!--ADDITIONAL REFERENCE: [ https://www.cobaltstrike.com/help-smb-beacon ] -->
849   <!--ADDITIONAL REFERENCE: [ https://blog.cobaltstrike.com/2015/10/07/named-pipe-
pivoting/ ] -->
850
851   <!--DATA: UtcTime, ProcessGuid, ProcessId, PipeName, Image-->
852   <RuleGroup name="" groupRelation="or">
853     <PipeEvent onmatch="include">
854       <!-- Remote Command Execution Tools -->
855       <PipeName condition="contains any">paexec;remcom;csexec</PipeName>
856       <!-- Password or Credential Dumpers -->
857       <PipeName condition="contains any">\lsadump;\cachedump;
\wcservicepipe</PipeName>
858       <!-- Malware -->
859       <PipeName condition="contains any">\isapi_http;\isapi_dg;\isapi_dg2;\sdlrpc;
\ahexec;\winsession;\lsassw;\46a676ab7f179e511e30dd2dc41bd388;
\9f81f59bc58452127884ce513865ed20;\e710f28d59aa529d6792ca6ff0ca1b34;\rpchl_p_3;
\NamePipe_MoreWindows;\pcheap_reuse;\gruntsvc;\583da945-62af-10e8-4902-a8f205c72b2e;
\bizkaz;\svcctl;\Posh;\jaccdpqnvbrxlaf;\csexecsvc</PipeName>
860     <PipeName condition="contains any">\atctl;\userpipe;\iehelper;\sdlrpc;
\comnap</PipeName>
861     <!-- Cobalt Strike Pipe Names -->
862     <PipeName condition="contains all">MSSE-;-server</PipeName>
863     <PipeName condition="begin with">\postex_</PipeName>
864     <PipeName condition="begin with">\postex_ssh_</PipeName>
865     <PipeName condition="begin with">\status_</PipeName>
866     <PipeName condition="begin with">\msagent_</PipeName>
867     </PipeEvent>
868   </RuleGroup>
869
870   <!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
871   <!--EVENT 19: "WmiEventFilter activity detected"-->
872   <!--EVENT 20: "WmiEventConsumer activity detected"-->
873   <!--EVENT 21: "WmiEventConsumerToFilter activity detected"-->
```

```
874
875 <!--ADDITIONAL REFERENCE: [ https://www.darkoperator.com/blog/2017/10/15/
/sysinternals-sysmon-610-tracking-of-permanent-wmi-events ] -->
876 <!--ADDITIONAL REFERENCE: [ https://rawsec.lu/blog/posts/2017/Sep/19/sysmon-v610-
vs-wmi-persistence/ ] -->
877
878 <!--DATA: EventType, UtcTime, Operation, User, Name, Type, Destination, Consumer,
Filter-->
879 <RuleGroup name="" groupRelation="or">
880 <WmiEvent onmatch="exclude">
881 <!--NOTE: Using exclude with no rules means everything will be logged-->
882 </WmiEvent>
883 </RuleGroup>
884
885 <!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
886 <!--EVENT 22: "Dns query"-->
887
888 <!--NOTE: Due to the volume of events that DNS queries generate, some orgs may
want to remove this section from their configuration to reduce Sysmon log turnover.
-->
889
890 <!--COMMENT: DNS logging is a very nuanced challenge in monitoring due to event
volume. Legitimate domains can be used to host malware/C2, but lookup itself is not
very informative.
891 It's fine to exclude monitoring these bulk low-value lookups, but at same
time, you would not have a full log of how malware communicated, potentially missing
C2.
892 This section of Sysmon configuration will require your full judgement and
knowledge of your org's priorities. There is no correct answer.-->
893
894 <!--OPERATIONS: Chrome and Firefox prefetch DNS lookups, or use alternate DNS
lookup methods Sysmon won't capture. You need to turn these off.
895 Search for Group Policy for these browsers to configure this.-->
896
897 <!--OPERATIONS: Most DNS traffic is web advertising. To significantly reduce DNS
queries and malware ads, enable client-side advertising filtering via Group Policy.
This is easy.
898 Internet Explorer: https://decentsecurity.com/adblocking-for-internet-
explorer-deployment/
899 Chrome: https://decentsecurity.com/ublock-for-google-chrome-deployment/
900 Firefox: ToDo
901 Also note, this configuration is designed for United States computers.
Your country's users will may need customization to reduce noise.
902 -->
903
904 <!--CONFIG: DNS poisoning is an issue during threat investigations. Try to only
exclude ROUTINE system-level queries you know are strongly validated with HTTPS or
code signing.-->
905 <!--CONFIG: If you exclude microsoft.com, someone could register malware-
microsoft.com and it wouldn't be logged. Use "END WITH" with leading . or "IS"
operators.-->
906 <!--CONFIG: Be very specific in exclusions. Threat actors use legitimate services
too. Dont exclude all of AWS or Azure or Google or CDNs!-->
907 <!--CONFIG: Popularity data: [ http://s3-us-west-1.amazonaws.com/umbrella-static
/index.html ] [ https://better.fyi/trackers/alexa-top-500-news/ ] -->
908
909 <!--CRITICAL: Do NOT exclude "wpad" lookups. This is a MitM vector routinely used
by attackers. Disable WPAD or enforce client-side DNSSEC for AD domain lookups.-->
910 <!--CRITICAL: Do NOT exclude IPv6 lookups.-->
911
```

```
912 <!--DATA: RuleName, UtcTime, ProcessGuid, ProcessId, QueryName, QueryType,
QueryStatus, QueryResults (can't filter on)-->
913
914 <!--BELOW: These domains should not be excluded at the top level. Be specific if
you want to reduce noise under them.-->
915 <!-- Rejected: .cloudapp.net, customer content [
https://blogs.technet.microsoft.com/ptsblog/2012/06/18/security-consideration-when-
using-cloudapp-net-domain-as-production-environment-in-windows-azure/ ] -->
916 <!-- Rejected: .googleapis.com, customer content [ https://www.zdnet.com/article
/this-business-email-scam-spreads-trojans-through-google-cloud-storage/ ] -->
917 <!-- Rejected: .cloudfront.net, customer content -->
918 <!-- Rejected: .windows.net, customer content -->
919 <!-- Rejected: *github.com, customer content, including open-source malware
components -->
920
921 <RuleGroup name="" groupRelation="or">
922 <DnsQuery onmatch="exclude">
923 <!--Network noise-->
924 <QueryName condition="end with">.arpa.</QueryName> <!--Design decision to not
log reverse DNS lookups. You will need to decide.-->
925 <QueryName condition="end with">.arpa.</QueryName> <!--Design decision to not lc
reverse DNS lookups. You will need to decide.-->
926 <QueryName condition="end with">.msftncsi.com</QueryName> <!--Microsoft proxy
detection | Microsoft default exclusion-->
927 <QueryName condition="is">..localmachine</QueryName>
928 <QueryName condition="is">localhost</QueryName>
929 <!--Microsoft-->
930 <QueryName condition="end with">-pushp.svc.ms</QueryName> <!--Microsoft: Doesn'
appear to host customer content or subdomains-->
931 <QueryName condition="end with">.b-msedge.net</QueryName> <!--Microsoft: Doesn'
appear to host customer content or subdomains-->
932 <QueryName condition="end with">.bing.com</QueryName> <!-- Microsoft | Microsof
default exclusion -->
933 <QueryName condition="end with">.hotmail.com</QueryName> <!--Microsoft |
Microsoft default exclusion-->
934 <QueryName condition="end with">.live.com</QueryName> <!--Microsoft | Microsoft
default exclusion-->
935 <QueryName condition="end with">.live.net</QueryName> <!--Microsoft | Microsoft
default exclusion-->
936 <QueryName condition="end with">.s-microsoft.com</QueryName> <!--Microsoft-->
937 <QueryName condition="end with">.microsoft.com</QueryName> <!--Microsoft |
Microsoft default exclusion-->
938 <QueryName condition="end with">.microsoftonline.com</QueryName> <!--Microsoft
Microsoft default exclusion-->
939 <QueryName condition="end with">.microsoftstore.com</QueryName> <!--Microsoft |
Microsoft default exclusion-->
940 <QueryName condition="end with">.ms-acdc.office.com</QueryName> <!--Microsoft:
Doesn't appear to host customer content or subdomains-->
941 <QueryName condition="end with">.msedge.net</QueryName> <!--Microsoft: Doesn't
appear to host customer content or subdomains-->
942 <QueryName condition="end with">.msn.com</QueryName> <!--Microsoft | Microsoft
default exclusion-->
943 <QueryName condition="end with">.msocdn.com</QueryName> <!--Microsoft-->
944 <QueryName condition="end with">.skype.com</QueryName> <!--Microsoft | Microsof
default exclusion-->
945 <QueryName condition="end with">.skype.net</QueryName> <!--Microsoft | Microsof
default exclusion-->
946 <QueryName condition="end with">.windows.com</QueryName> <!--Microsoft-->
947 <QueryName condition="end with">.windows.net.nsatc.net</QueryName> <!--
Microsoft-->
```

```
948 <QueryName condition="end with">.windowsupdate.com</QueryName> <!--Microsoft-->
949 <QueryName condition="end with">.xboxlive.com</QueryName> <!--Microsoft-->
950 <QueryName condition="is">login.windows.net</QueryName> <!--Microsoft-->
951 <Image condition="begin with">C:\ProgramData\Microsoft\Windows Defender\Platfor
</Image> <!--Microsoft: https://docs.microsoft.com/en-us/windows/security/threat-
protection/microsoft-defender-atp/network-protection -->
952 <!--Microsoft:Office365/AzureAD-->
953 <QueryName condition="end with">.activedirectory.windowsazure.com</QueryName>
<!--Microsoft: AzureAD-->
954 <QueryName condition="end with">.aria.microsoft.com</QueryName> <!--Microsoft:
OneDrive/SharePoint-->
955 <QueryName condition="end with">.msauth.net</QueryName>
956 <QueryName condition="end with">.msftauth.net</QueryName>
957 <QueryName condition="end with">.office.net</QueryName> <!--Microsoft: Office--
958 <QueryName condition="end with">.opinsights.azure.com</QueryName> <!--Microsoft
AzureAD/InTune client event monitoring-->
959 <QueryName condition="end with">.res.office365.com</QueryName> <!--Microsoft:
Office-->
960 <QueryName condition="is">acdc-direct.office.com</QueryName> <!--Microsoft:
Office-->
961 <QueryName condition="is">atm-fp-direct.office.com</QueryName> <!--Microsoft:
Office-->
962 <QueryName condition="is">loki.delve.office.com</QueryName> <!--Microsoft:
Office-->
963 <QueryName condition="is">management.azure.com</QueryName> <!--Microsoft:
AzureAD/InTune-->
964 <QueryName condition="is">messaging.office.com</QueryName> <!--Microsoft:
Office-->
965 <QueryName condition="is">outlook.office365.com</QueryName> <!--Microsoft:
Protected by HSTS-->
966 <QueryName condition="is">portal.azure.com</QueryName> <!--Microsoft:
AzureAD/InTune-->
967 <QueryName condition="is">protection.outlook.com</QueryName> <!--Microsoft:
Office-->
968 <QueryName condition="is">substrate.office.com</QueryName> <!--Microsoft:
Office-->
969 <QueryName condition="end with">.measure.office.com</QueryName> <!--Microsoft:
Office-->
970 <!--3rd-party applications-->
971 <QueryName condition="end with">.adobe.com</QueryName> <!--Adobe-->
972 <QueryName condition="end with">.adobe.io</QueryName> <!--Adobe-->
973 <QueryName condition="end with">.mozaws.net</QueryName> <!--Mozilla-->
974 <QueryName condition="end with">.mozilla.com</QueryName> <!--Mozilla-->
975 <QueryName condition="end with">.mozilla.net</QueryName> <!--Mozilla-->
976 <QueryName condition="end with">.mozilla.org</QueryName> <!--Mozilla-->
977 <QueryName condition="end with">.spotify.com</QueryName> <!--Spotify-->
978 <QueryName condition="end with">.spotify.map.fastly.net</QueryName> <!--
Spotify-->
979 <QueryName condition="end with">.wbx2.com</QueryName> <!--Webex-->
980 <QueryName condition="end with">.webex.com</QueryName> <!--Webex-->
981 <QueryName condition="is">clients1.google.com</QueryName> <!--Google-->
982 <QueryName condition="is">clients2.google.com</QueryName> <!--Google-->
983 <QueryName condition="is">clients3.google.com</QueryName> <!--Google-->
984 <QueryName condition="is">clients4.google.com</QueryName> <!--Google-->
985 <QueryName condition="is">clients5.google.com</QueryName> <!--Google-->
986 <QueryName condition="is">clients6.google.com</QueryName> <!--Google-->
987 <QueryName condition="is">safebrowsing.googleapis.com</QueryName> <!--Google-->
988 <!--Goodlist CDN-->
989 <QueryName condition="end with">.akadns.net</QueryName> <!--AkamaiCDN,
extensively used by Microsoft | Microsoft default exclusion-->
```

```
990 <QueryName condition="end with">.netflix.com</QueryName>
991 <QueryName condition="end with">aspnetcdn.com</QueryName> <!--Microsoft [
https://docs.microsoft.com/en-us/aspnet/ajax/cdn/overview ]-->
992 <QueryName condition="is">ajax.googleapis.com</QueryName>
993 <QueryName condition="is">cdnjs.cloudflare.com</QueryName> <!--Cloudflare: Host
popular javascript libraries-->
994 <QueryName condition="is">fonts.googleapis.com</QueryName> <!--Google fonts-->
995 <QueryName condition="end with">.typekit.net</QueryName> <!--Adobe fonts-->
996 <QueryName condition="is">cdnjs.cloudflare.com</QueryName>
997 <QueryName condition="end with">.stackassets.com</QueryName> <!--Stack
Overflow-->
998 <QueryName condition="end with">.steamcontent.com</QueryName>
999 <QueryName condition="is">play.google.com</QueryName>
1000 <QueryName condition="is">content-autofill.googleapis.com</QueryName>
1001 <!--Web resources-->
1002 <QueryName condition="end with">.disqus.com</QueryName> <!--Microsoft default
exclusion-->
1003 <QueryName condition="end with">.fontawesome.com</QueryName>
1004 <QueryName condition="is">disqus.com</QueryName> <!--Microsoft default
exclusion-->
1005 <!--Ads-->
1006 <QueryName condition="end with">.1rx.io</QueryName> <!--Ads-->
1007 <QueryName condition="end with">.2mdn.net</QueryName> <!--Ads: Google |
Microsoft default exclusion-->
1008 <QueryName condition="end with">.3lift.com</QueryName> <!--Ads-->
1009 <QueryName condition="end with">.adadvisor.net</QueryName> <!--Ads: Neustar [
https://better.fyi/trackers/adadvisor.net/ ] -->
1010 <QueryName condition="end with">.adap.tv</QueryName> <!--Ads:AOL | Microsoft
default exclusion [ https://www.crunchbase.com/organization/adap-tv ] -->
1011 <QueryName condition="end with">.addthis.com</QueryName> <!--Ads:Oracle |
Microsoft default exclusion [ https://en.wikipedia.org/wiki/AddThis ] -->
1012 <QueryName condition="end with">.adform.net</QueryName> <!--Ads-->
1013 <QueryName condition="end with">.adnxs.com</QueryName> <!--Ads: AppNexus |
Microsoft default exclusion-->
1014 <QueryName condition="end with">.adroll.com</QueryName> <!--Ads-->
1015 <QueryName condition="end with">.adrta.com</QueryName> <!--Ads-->
1016 <QueryName condition="end with">.adsafeprotected.com</QueryName> <!--Ads-->
1017 <QueryName condition="end with">.adsrvr.org</QueryName> <!--Ads-->
1018 <QueryName condition="end with">.adsymptotic.com</QueryName> <!--Ads-->
1019 <QueryName condition="end with">.advertising.com</QueryName> <!--Ads | Microsof
default exclusion-->
1020 <QueryName condition="end with">.agkn.com</QueryName> <!--Ads | [
https://www.home.neustar/privacy ]-->
1021 <QueryName condition="end with">.amazon-adsystem.com</QueryName> <!--Ads-->
1022 <QueryName condition="end with">.amazon-adsystem.com</QueryName> <!--Ads-->
1023 <QueryName condition="end with">.analytics.yahoo.com</QueryName> <!--
Ads:Yahoo-->
1024 <QueryName condition="end with">.aol.com</QueryName> <!--Ads | Microsoft defaul
exclusion -->
1025 <QueryName condition="end with">.betrad.com</QueryName> <!--Ads | Microsoft
default exclusion-->
1026 <QueryName condition="end with">.bidswitch.net</QueryName> <!--Ads-->
1027 <QueryName condition="end with">.casalemedia.com</QueryName> <!--Ads | Microsof
default exclusion-->
1028 <QueryName condition="end with">.chartbeat.net</QueryName> <!--Ads | Microsoft
default exclusion [ https://better.fyi/trackers/chartbeat.com/ ]-->
1029 <QueryName condition="end with">.cnn.com</QueryName> <!-- Microsoft default
exclusion-->
1030 <QueryName condition="end with">.convertro.com</QueryName> <!--Ads:Verizon-->
1031 <QueryName condition="end with">.criteo.com</QueryName> <!--Ads [
```



```
https://better.fyi/trackers/criteo.com/ ] -->
1032 <QueryName condition="end with">.criteo.net</QueryName> <!--Ads [
https://better.fyi/trackers/criteo.com/ ] -->
1033 <QueryName condition="end with">.crwdcntrl.net</QueryName> <!--Ads: Lotame [
https://better.fyi/trackers/crwdcntrl.net/ ] -->
1034 <QueryName condition="end with">.demdex.net</QueryName> <!--Ads | Microsoft
default exclusion-->
1035 <QueryName condition="end with">.domdex.com</QueryName>
1036 <QueryName condition="end with">.dotomi.com</QueryName> <!--Ads | Microsoft
default exclusion-->
1037 <QueryName condition="end with">.doubleclick.net</QueryName> <!--Ads:Conversant
| Microsoft default exclusion [ https://www.crunchbase.com/organization/dotomi ] -->
1038 <QueryName condition="end with">.doubleverify.com</QueryName> <!--Ads: Google--
1039 <QueryName condition="end with">.emxdgt.com</QueryName> <!--Ads: EMX-->
1040 <QueryName condition="end with">.everesttech.net</QueryName> <!--Ads | [
https://better.fyi/trackers/everesttech.net/ ] -->
1041 <QueryName condition="end with">.exelator.com</QueryName> <!--Ads:Nielson
Marketing Cloud-->
1042 <QueryName condition="end with">.google-analytics.com</QueryName> <!--Ads:Googl
| Microsoft default exclusion-->
1043 <QueryName condition="end with">.googleadservices.com</QueryName> <!--Google-->
1044 <QueryName condition="end with">.googlesyndication.com</QueryName> <!--
Ads:Google, sometimes called during malicious ads, but not directly responsible |
Microsoft default exclusion [ https://www.hackread.com/wp-content/uploads/2018/06
/Bitdefender-Whitepaper-Zacinlo.pdf ]-->
1045 <QueryName condition="end with">.googletagmanager.com</QueryName> <!--Google-->
1046 <QueryName condition="end with">.googlevideo.com</QueryName> <!--Google |
Microsoft default exclusion-->
1047 <QueryName condition="end with">.gstatic.com</QueryName> <!--Google | Microsoft
default exclusion-->
1048 <QueryName condition="end with">.gvt1.com</QueryName> <!--Google-->
1049 <QueryName condition="end with">.gvt2.com</QueryName> <!--Google-->
1050 <QueryName condition="end with">.ib-ibi.com</QueryName> <!--Ads: Offerpath [
https://better.fyi/trackers/ib-ibi.com/ ] -->
1051 <QueryName condition="end with">.jivox.com</QueryName> <!--Ads-->
1052 <QueryName condition="end with">.krxd.net</QueryName> <!--Ads-->
1053 <QueryName condition="end with">.lijit.com</QueryName> <!--Ads-->
1054 <QueryName condition="end with">.mathtag.com</QueryName> <!--Microsoft default
exclusion-->
1055 <QueryName condition="end with">.moatads.com</QueryName> <!--Ads | Microsoft
default exclusion-->
1056 <QueryName condition="end with">.moatpixel.com</QueryName> <!--Ads | Microsoft
default exclusion-->
1057 <QueryName condition="end with">.mookie1.com</QueryName> <!--Ads-->
1058 <QueryName condition="end with">.myvisualiq.net</QueryName> <!--Ads-->
1059 <QueryName condition="end with">.netmng.com</QueryName> <!--Ads-->
1060 <QueryName condition="end with">.nexac.com</QueryName> <!--Ads | Microsoft
default exclusion-->
1061 <QueryName condition="end with">.openx.net</QueryName> <!--Ads-->
1062 <QueryName condition="end with">.optimizely.com</QueryName> <!--Ads-->
1063 <QueryName condition="end with">.outbrain.com</QueryName> <!--Ads-->
1064 <QueryName condition="end with">.pardot.com</QueryName> <!--Ads-->
1065 <QueryName condition="end with">.phx.gbl</QueryName> <!--Ads | Microsoft defaul
exclusion-->
1066 <QueryName condition="end with">.pinterest.com</QueryName> <!--Pinerest-->
1067 <QueryName condition="end with">.pubmatic.com</QueryName> <!--Ads | Microsoft
default exclusion-->
1068 <QueryName condition="end with">.quantcount.com</QueryName>
1069 <QueryName condition="end with">.quantserve.com</QueryName>
1070 <QueryName condition="end with">.revsci.net</QueryName> <!--Ads:Omniture |
```

```
Microsoft default exclusion-->
1071 <QueryName condition="end with">.rfihub.net</QueryName> <!--Ads | Microsoft
default exclusion-->
1072 <QueryName condition="end with">.rlcdn.com</QueryName> <!--Ads: Rapleaf [
https://better.fyi/trackers/rlcdn.com/ ] -->
1073 <QueryName condition="end with">.rubiconproject.com</QueryName> <!--Ads: Rubicc
Project | Microsoft default exclusion [ https://better.fyi/trackers
/rubiconproject.com/ ] -->
1074 <QueryName condition="end with">.scdn.co</QueryName> <!--Spotify-->
1075 <QueryName condition="end with">.scorecardresearch.com</QueryName> <!--Ads:
Comscore | Microsoft default exclusion-->
1076 <QueryName condition="end with">.serving-sys.com</QueryName> <!--Ads | Microsof
default exclusion-->
1077 <QueryName condition="end with">.sharethrough.com</QueryName> <!--Ads-->
1078 <QueryName condition="end with">.simpli.fi</QueryName>
1079 <QueryName condition="end with">.sitescout.com</QueryName> <!--Ads-->
1080 <QueryName condition="end with">.smartadserver.com</QueryName> <!--Ads-->
1081 <QueryName condition="end with">.snapads.com</QueryName> <!--Ads-->
1082 <QueryName condition="end with">.spotxchange.com</QueryName> <!--Ads-->
1083 <QueryName condition="end with">.taboola.com</QueryName> <!--Ads:Taboola-->
1084 <QueryName condition="end with">.taboola.map.fastly.net</QueryName> <!--
Ads:Taboola-->
1085 <QueryName condition="end with">.tapad.com</QueryName>
1086 <QueryName condition="end with">.tidaltv.com</QueryName> <!--Ads: Videology [
https://better.fyi/trackers/tidaltv.com/ ] -->
1087 <QueryName condition="end with">.trafficmanager.net</QueryName> <!--Ads |
Microsoft default exclusion-->
1088 <QueryName condition="end with">.tremorhub.com</QueryName> <!--Ads-->
1089 <QueryName condition="end with">.tribalfusion.com</QueryName> <!--Ads:
Exponential [ https://better.fyi/trackers/tribalfusion.com/ ] -->
1090 <QueryName condition="end with">.turn.com</QueryName> <!--Ads | Microsoft
default exclusion [ https://better.fyi/trackers/turn.com/ ] -->
1091 <QueryName condition="end with">.twimg.com</QueryName> <!--Ads | Microsoft
default exclusion-->
1092 <QueryName condition="end with">.tynt.com</QueryName> <!--Ads-->
1093 <QueryName condition="end with">.w55c.net</QueryName> <!--Ads:dataxu-->
1094 <QueryName condition="end with">.yting.com</QueryName> <!--Google-->
1095 <QueryName condition="end with">.zorosrv.com</QueryName> <!--Ads:Taboola-->
1096 <QueryName condition="is">1rx.io</QueryName> <!--Ads-->
1097 <QueryName condition="is">adservice.google.com</QueryName> <!--Google-->
1098 <QueryName condition="is">ampcid.google.com</QueryName> <!--Google-->
1099 <QueryName condition="is">clientservices.googleapis.com</QueryName> <!--
Google-->
1100 <QueryName condition="is">googleadapis.l.google.com</QueryName> <!--Google-->
1101 <QueryName condition="is">imasdk.googleapis.com</QueryName> <!--Google [
https://developers.google.com/interactive-media-ads/docs/sdks/html5/ ] -->
1102 <QueryName condition="is">l.google.com</QueryName> <!--Google-->
1103 <QueryName condition="is">m1314.com</QueryName> <!--Ads-->
1104 <QueryName condition="is">mtalk.google.com</QueryName> <!--Google-->
1105 <QueryName condition="is">update.googleapis.com</QueryName> <!--Google-->
1106 <QueryName condition="is">www.googletagservices.com</QueryName> <!--Google-->
1107 <!--SocialNet-->
1108 <QueryName condition="end with">.pscp.tv</QueryName> <!--Twitter:Periscope-->
1109 <!--OSCP/CRL Common-->
1110 <QueryName condition="end with">.amazontrust.com</QueryName>
1111 <QueryName condition="end with">.digicert.com</QueryName>
1112 <QueryName condition="end with">.globalsign.com</QueryName>
1113 <QueryName condition="end with">.globalsign.net</QueryName>
1114 <QueryName condition="end with">.intel.com</QueryName>
1115 <QueryName condition="end with">.symcb.com</QueryName> <!--Digicert-->
```

```
1116 <QueryName condition="end with">.symcd.com</QueryName> <!--Digicert-->
1117 <QueryName condition="end with">.thawte.com</QueryName>
1118 <QueryName condition="end with">.usertrust.com</QueryName>
1119 <QueryName condition="end with">.verisign.com</QueryName>
1120 <QueryName condition="end with">ocsp.identrust.com</QueryName>
1121 <QueryName condition="end with">pki.goog</QueryName>
1122 <QueryName condition="is">msocsp.com</QueryName> <!--Microsoft:OCSP-->
1123 <QueryName condition="is">ocsp.comodoca.com</QueryName>
1124 <QueryName condition="is">ocsp.entrust.net</QueryName>
1125 <QueryName condition="is">ocsp.godaddy.com</QueryName>
1126 <QueryName condition="is">ocsp.int-x3.letsencrypt.org</QueryName>
1127 <QueryName condition="is">ocsp.msocsp.com</QueryName> <!--Microsoft:OCSP-->
1128 <QueryName condition="end with">pki.goog</QueryName>
1129 <QueryName condition="is">ocsp.godaddy.com</QueryName>
1130 <QueryName condition="end with">amazontrust.com</QueryName>
1131 <QueryName condition="is">ocsp.sectigo.com</QueryName>
1132 <QueryName condition="is">pki-goog.l.google.com</QueryName>
1133 <QueryName condition="end with">.usertrust.com</QueryName>
1134 <QueryName condition="is">ocsp.comodoca.com</QueryName>
1135 <QueryName condition="is">ocsp.verisign.com</QueryName>
1136 <QueryName condition="is">ocsp.entrust.net</QueryName>
1137 <QueryName condition="end with">ocsp.identrust.com</QueryName>
1138 <QueryName condition="is">status.rapidssl.com</QueryName>
1139 <QueryName condition="is">status.thawte.com</QueryName>
1140 <QueryName condition="is">ocsp.int-x3.letsencrypt.org</QueryName>
1141 </DnsQuery>
1142 </RuleGroup>
1143
1144 <!--SYSMON EVENT ID 23 : FILE DELETE [FileDelete]-->
1145 <!--EVENT 22: "File Delete"-->
1146 <!--COMMENT: Sandbox usage. When a program signals to Windows a file should be
deleted or wiped, Sysmon may be able to capture it.
1147 [ https://isc.sans.edu/forums/diary/Sysmon+and+File+Deletion/26084/ ]
1148 -->
1149
1150 <!--DATA: RuleName, UtcTime, ProcessGuid, ProcessId, User, Image, TargetFilename,
Hashes, IsExecutable, Archived -->
1151
1152 <!--
1153 <RuleGroup name="" groupRelation="or">
1154 <ClipboardChange onmatch="include">
1155 </ClipboardChange>
1156 </RuleGroup>
1157 -->
1158
1159 <!--SYSMON EVENT ID 24 : CLIPBOARD EVENT MONITORING [ClipboardChange]-->
1160 <!--EVENT 24: "Clipboard changed"-->
1161 <!--COMMENT: Sandbox usage. Sysmon can capture the contents of clipboard events
1162 An example of what could be a production usage on restricted desktops is
provided below, but it is commented-out. -->
1163
1164 <!--DATA: EventType, UtcTime, ProcessGuid, ProcessId, Image, Session, ClientInfo,
Hashes, Archived -->
1165
1166 <!--
1167 <RuleGroup name="" groupRelation="or">
1168 <ClipboardChange onmatch="include">
1169 <Image condition="end with">wscript.exe</Image>
1170 <Image condition="end with">cscript.exe</Image>
1171 <Image condition="end with">powershell.exe</Image>
```

```
1172     <Image condition="end with">rdpclip.exe</Image>
1173   </ClipboardChange>
1174 </RuleGroup>
1175 -->
1176
1177 <!--SYSMON EVENT ID 25 : PROCESS TAMPERING [ProcessTampering]-->
1178 <!--EVENT 25: "Process Tampering"-->
1179 <!--COMMENT: This event is generated when a process image is changed from an
external source, such as a different process.
1180 This may or may not provide value in your environment as it requires tuning and
a SIEM to correlate the ProcessGuids.
1181 [ https://medium.com/falconforce/sysmon-13-process-tampering-detection-
820366138a6c ] -->
1182
1183 <!--DATA: EventType, RuleName, UtcTime, ProcessGuid, ProcessId, Image, Type -->
1184
1185 <!--
1186 <RuleGroup name="" groupRelation="or">
1187   <ProcessTampering onmatch="exclude">
1188     <Image condition="begin with">C:\Program Files (x86)\Microsoft\Edge\Application
\</Image>
1189   </ProcessTampering>
1190 </RuleGroup>
1191 -->
1192
1193 <!--SYSMON EVENT ID 255 : ERROR-->
1194 <!--"This event is generated when an error occurred within Sysmon. They can happe
if the system is under heavy load
1195 and certain tasked could not be performed or a bug exists in the Sysmon service
You can report any bugs on the
1196 Sysinternals forum or over Twitter (@markkrussinovich)."-->
1197 <!--Cannot be filtered.-->
1198
1199 </EventFiltering>
1200 </Sysmon>
1201
```


F Defender for cloud Demonstration

When you open Microsoft Defender for cloud the first thing you should do is install agents on your VM's for data collection. This will allow you to receive security alerts and recommendations.

[Install agents](#) [Get started](#)

Make the most of Defender for Cloud by enabling data collection agents

To receive security alerts and recommendations, agents must be installed on your virtual machines for data collection.

[Learn more >](#)

Install agents automatically

The Log Analytics agent will be automatically installed on all the virtual machines in selected subscription.

✓ All set! All of your Azure subscriptions have automatic agent installation enabled

Install agents

Figure 47: Install agents on VM's

In Microsoft Defender for Cloud you will get a overview of different services like security posture, regulatory compliance, workload protections, firewall manager, inventory and Information protection.

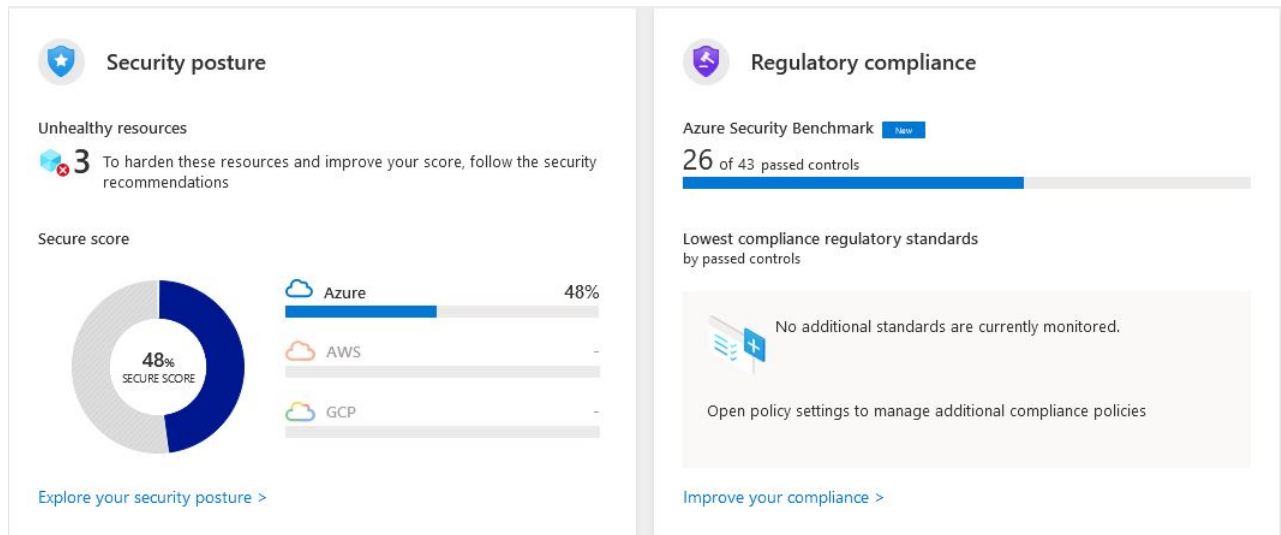


Figure 48: Security posture and Regulatory compliance

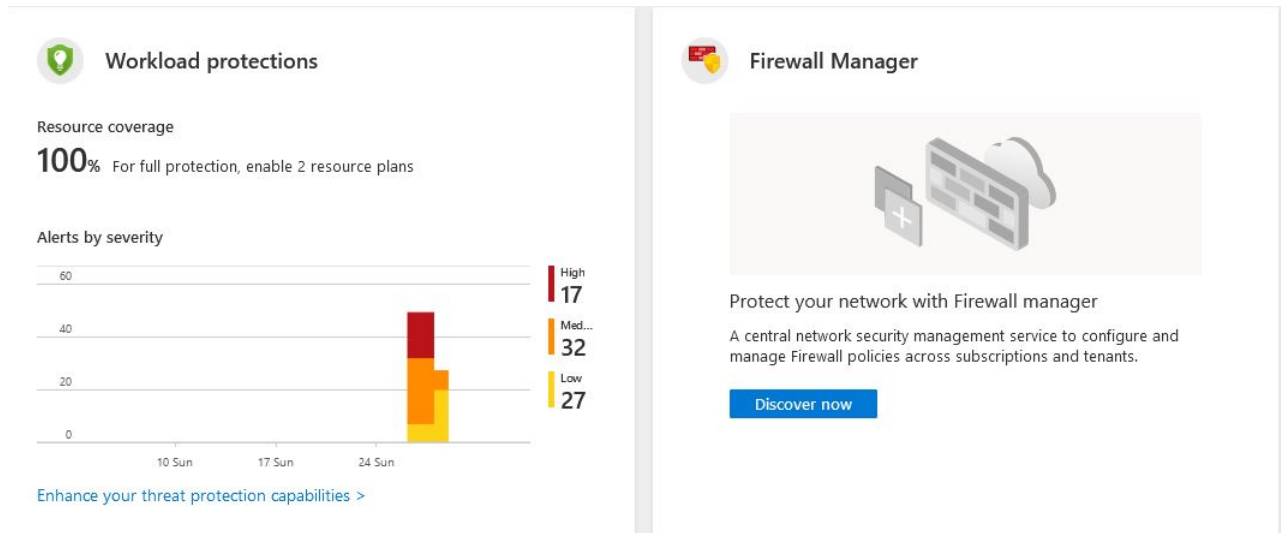


Figure 49: Workload protections and Firewall manager

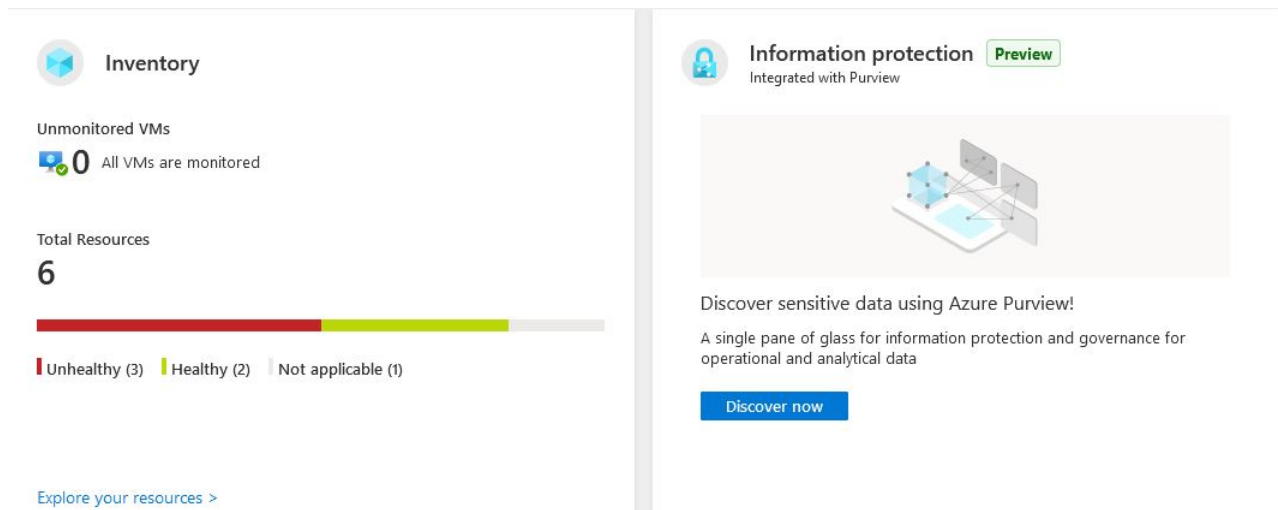


Figure 50: Inventory and Information protection

One of the Key features of Microsoft Defender for cloud is the security Recommendations. To look at the current security recommendations you just need to navigate to the recommendations tab.

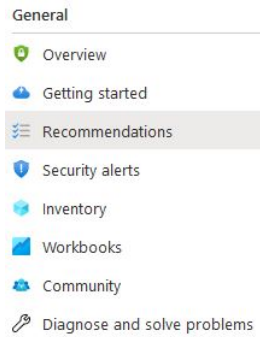


Figure 51: Recommendations tab

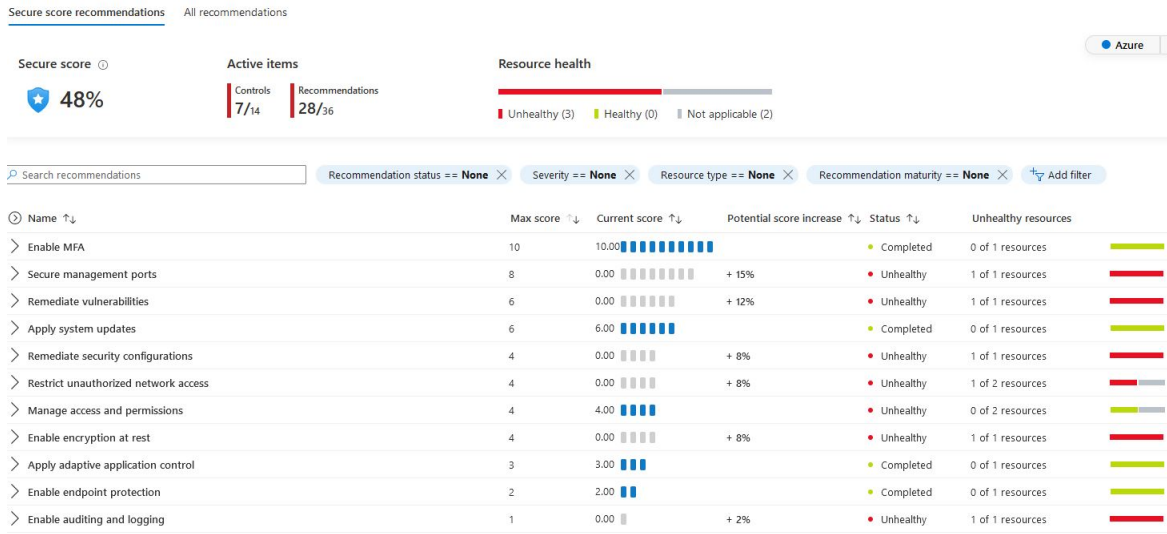


Figure 52: Security recommendations

G Key Vault Demonstration

The following command was used to create a new Key Vault within the existing resource group.

```
New-AzKeyVault -Name "KeyVaultName" `
-ResourceGroupName "ResourceName" -Location "LocationName"
```

In Fig. 53 is the output of the command.

```
PS /home/stian> New-AzKeyVault -Name "Gruppe124KeyVault" -ResourceGroupName "Gruppe124" -Location "West Europe"
WARNING: We have migrated the API calls for this cmdlet from Azure Active Directory Graph to Microsoft Graph.
Visit https://go.microsoft.com/fwlink/?linkid=2181475 for any permission issues.

Vault Name                               : Gruppe124KeyVault
Resource Group Name                       : Gruppe124
Location                                  : West Europe
Resource ID                               : /subscriptions/21b4e6a6-a507-4939-9ec0-3a6ad7fbee5e/resourceGroups/Gruppe124/providers/Microsoft.KeyVault/vaults/Gruppe124KeyVault
Vault URI                                  : https://gruppe124keyvault.vault.azure.net/
Tenant ID                                  : bb29bdd0-de6b-48b5-80df-e9abe378aa55
SKU                                        : Standard
Enabled For Deployment?                   : False
Enabled For Template Deployment?          : False
Enabled For Disk Encryption?              : False
Enabled For RBAC Authorization?          : False
Soft Delete Enabled?                      : True
Soft Delete Retention Period (days)      : 90
Purge Protection Enabled?                 :
Public Network Access                     : Enabled
Access Policies                           :
Network Rule Set                           :
                                           Default Action           : Allow
                                           Bypass                   : AzureServices
                                           IP Rules                  :
                                           Virtual Network Rules    :
Tags                                       :
```

Figure 53: Creating a new Key Vault

After the Key Vault was created, the next objective was to turn on disk encryption. The following command was used to turn on disk encryption.

```
az keyvault update --name "KeyVaultName" `
--resource-group "ResourceName" `
--enabled-for-disk-encryption "true"
```

In Fig. 54 is the output of the command.

```

PS /home/stian> az keyvault update --name "Gruppe124KeyVault" --resource-group "Gruppe124" --enabled-for-disk-encryption "true"
{
  "id": "/subscriptions/21b4e6a6-a507-4939-9ec0-3a6ad7fbee5e/resourceGroups/Gruppe124/providers/Microsoft.KeyVault/vaults/Gruppe124KeyVault",
  "location": "West Europe",
  "name": "Gruppe124KeyVault",
  "properties": {
    "accessPolicies": [],
    "createMode": null,
    "enablePurgeProtection": null,
    "enableRbacAuthorization": false,
    "enableSoftDelete": true,
    "enabledForDeployment": false,
    "enabledForDiskEncryption": true,
    "enabledForTemplateDeployment": false,
    "hsmPoolResourceId": null,
    "networkAcls": null,
    "privateEndpointConnections": null,
    "provisioningState": "Succeeded",
    "publicNetworkAccess": "Enabled",
    "sku": {
      "family": "A",
      "name": "standard"
    },
    "softDeleteRetentionInDays": 90,
    "tenantId": "bb29bdd0-de6b-48b5-80df-e9abe378aa55",
    "vaultUri": "https://gruppe124keyvault.vault.azure.net/"
  }
}

```

Figure 54: Enabling disk encryption

The following command was used to enable so that Microsoft.Compute resource provider can retrieve secrets from the key vault, for example when this key vault is referenced in the creation of a VM.

```

Set-AzKeyVaultAccessPolicy -VaultName "KeyVaultName" `
-ResourceGroupName "ResourceName" -EnabledForDeployment

```

If there is a need for Azure Resource Manager to retrieve secrets from this key vault when referenced in a template deployment, the following command can be used.

```

Set-AzKeyVaultAccessPolicy -VaultName "KeyVaultName" `
-ResourceGroupName "ResourceName" -EnabledForTemplateDeployment

```

The access policy needed to be changed before a new secret, key or certificate could be made, to do this the following command to update the access policy for the current user.

```

Set-AzKeyVaultAccessPolicy -VaultName "KeyVaultName" `
-ObjectId id -PermissionsToSecrets all -PermissionsToKeys all `
PermissionsToCertificates all

```

In Fig. 55 is the output of the command.

```
PS /home/stian> Set-AzKeyVaultAccessPolicy -VaultName Gruppe124KeyVault -ObjectId 4b2d87de-740b-4a7f-8abd-fb5109aa220f `
>> -PermissionsToSecrets all -PermissionsToKeys all -PermissionsToCertificates all
WARNING: We have migrated the API calls for this cmdlet from Azure Active Directory Graph to Microsoft Graph.
Visit https://go.microsoft.com/fwlink/?linkid=2181475 for any permission issues.
PS /home/stian>
```

Figure 55: Set access policy

To make sure everything was set up correctly the following command was used to make a test secret and put it in the key vault.

```
$secret = ConvertTo-SecureString -String 'TEST!' -AsPlainText
```

```
Set-AzKeyVaultSecret -VaultName "KEYVAULTNAME" `
-Name "NAMEOFSECRET" `
-SecretValue $secret
```

In Fig. 56 is this output of the command

```
PS /home/stian> $secret = ConvertTo-SecureString -String 'TEST!' -AsPlainText
PS /home/stian> Set-AzKeyVaultSecret -VaultName Gruppe124KeyVault -Name testSecret -SecretValue $secret

Vault Name : gruppe124keyvault
Name       : testSecret
Version    : ef39d1a1d01d4f568d2a1894d09510cc
Id         : https://gruppe124keyvault.vault.azure.net:443/secrets/testSecret/ef39d1a1d01d4f568d2a1894d09510cc
Enabled    : True
Expires    :
Not Before :
Created    : 5/2/2022 10:01:49 AM
Updated    : 5/2/2022 10:01:49 AM
Content Type :
Tags       :
```

Figure 56: Making a secret

To make sure the secret was made the following command was used to check the key vault secret list.

```
az keyvault secret list --vault-name KeyVaultName
```

```
PS /home/stian> az keyvault secret list --vault-name Gruppe124KeyVault
[
  {
    "attributes": {
      "created": "2022-05-02T10:01:49+00:00",
      "enabled": true,
      "expires": null,
      "notBefore": null,
      "recoveryLevel": "Recoverable+Purgeable",
      "updated": "2022-05-02T10:01:49+00:00"
    },
    "contentType": null,
    "id": "https://gruppe124keyvault.vault.azure.net/secrets/testSecret",
    "managed": null,
    "name": "testSecret",
    "tags": null
  }
]
PS /home/stian> █
```

Figure 57: List secrets

H Meetings

19.01.2022:

Agenda

- Project plan status

We agreed with Erik that we should do physical meeting from 2. February. We discussed the status of our project plan and got some tips on what we should do first. One good suggestion we got was that we should make a progress plan early on.

20.01.2022:

Agenda

- Documentation we could get access to
- Look at NTNU's systems
- Restrictions

In this meeting with the client we discussed and clarified some parts of the assignment. We agreed on that we should not look at NTNU's current solutions and that we should focus on Windows Server 2022 and Windows 11 and make a general best practise on what security features should be used.

26.01.2022:

Agenda

- Project plan
- Group rules and routines

In this meeting we got feedback on how the project plan looked this far. Some of the things we should change was separate group rules and routines and do a proper division of labor.

02.02.2022:

Agenda

- Project plan
- No Windows Server 2022 in SkyHigh

- Goals

We got some feedback on what we needed to change to get our project plan approved. The things we needed to change was effect goals, result goals, learning goals. The rest of the project plan was good. Erik said would ask to get someone to put a Windows Server 2022 image in SkyHigh.

09.02.2022:**Agenda**

- Previous thesis we could look at
- What sources we should use
- SkyHigh do not have TPM

Got some Twitter profiles we could look at for inspiration on what to write about. Erik told us to ask the client about a Solution to the TPM problem. We should use try to use mostly reliable sources even if we look at different forums.

18.02.2022:**Agenda**

- Meeting concerning splitting the group

Discussed which group should do what part of the thesis, we agreed on that we would write about Windows Server and Azure Cloud.

22.02.2022:**Agenda**

- Test environment
- Group division
- Hard to get hold of the client

Erik wanted the test environment to be just one VM. Erik said that the group contract from the original group would suffice. The client have not responded to emails and was hard to get a hold of, this was discussed again with Erik. Erik said we should look at Andy Robbins on Twitter for information.

02.03.2022:**Agenda**

- What should be focused on
- Azure?
- Active Directory and Group policies
- Specific type of server?
- Frameworks

The client would like to prioritize Azure AD over Microsoft AD if it was to be implemented, not to focus on Microsoft 365 Defender any more (change in task description). The client wanted to prioritize a server for monitoring and therefore look at Sysmon. The client wanted "Helsenormen for IKT-sikkerhet", ISO 27001/27002 and "NSM grunprinsipper" as main frameworks to look in to.

08.03.2022:**Agenda**

- What features in Azure Cloud the client wanted

The client wanted to prioritize Microsoft Defender for cloud, Microsoft Sentinel, Azure AD Identity Protection, Azure AD privileged identity management, Multi-factor Authentication and Key Vault (Key Vault was not as important).

09.03.2022:**Agenda**

- What to implement in the thesis and what not
- Performance tests

Since there was not supposed to be created a product in this project "kravspesifikasjoner" was not required. Erik said that PowerShell should be used if possible and group policies should not be prioritized at this point. Erik said that if there was any criticism to the security features it should be in the thesis and wanted performance tests.

23.03.2022:**Agenda**

- Mitre Att&Ck and Mitre D3FEND
- Atomic Red Team git repository

- PowerShell script analyzer

Erik said that Mitre Att&Ck and Mitre D3FEND could provide many tests that could be ran, by Atomic Red Team's git repository. Erik said that there is much information about the different frameworks that should be left out, only use the parts that is touched by the security feature. Erik said that we should not use pictures or figures found on the internet even when referenced to, rather create new and reference to the inspiration.

30.03.2022:**Agenda**

- SwiftOnSecurity Sysmon configuration file
- Send a draft of the thesis soon
- Any people we could contact?

Erik agreed that SwiftOnSecurity's Sysmon configuration file was a good starting point. Agreed on sending in a draft of the thesis. Erik said that we could try and contact Odvar Moe to get some tips.

20.04.2022:**Agenda**

- Should we include different policies?
- Ask if we can run malware in SkyHigh
- How we should document the differences between Windows Server 2019 and Server 2022

We agreed on that we should not focus on policies, this is something we could include if we had any time left after we where done with everything else. Malware could be used in skyhigh as long as we know what they do. Since there is many similarities in Windows Server 2019 and 2022 security we agreed on that it was enough to make a table with which security functions that is available on each server.

25.04.2022:**Agenda**

- Specific tests the client wants us to do

- How we should do the performance test
- Ask if the client have any questions

There was not any specific tests the client wanted us to do so we could decide for our self. The client wanted us to do a performance test where we wrote many files to the disk. The client did not have any questions for us, he wanted us to send him a copy of the next draft.

04.05.2022:
Agenda

- Do we have enough tests and demonstration
- Sysmon configuration file
- When we should send a new draft of the thesis

We agreed on that we have done enough tests, but some of our demonstrations should be put in the appendix. Since it takes a lot of time to customize the Sysmon configuration file, we agreed on that we should only look more into it if we have time. Agreed on sending in a new draft of the thesis 09.05.2022.

11.05.2022:
Agenda

- How the performance test should be documented
- Get some clarifications on the document structure

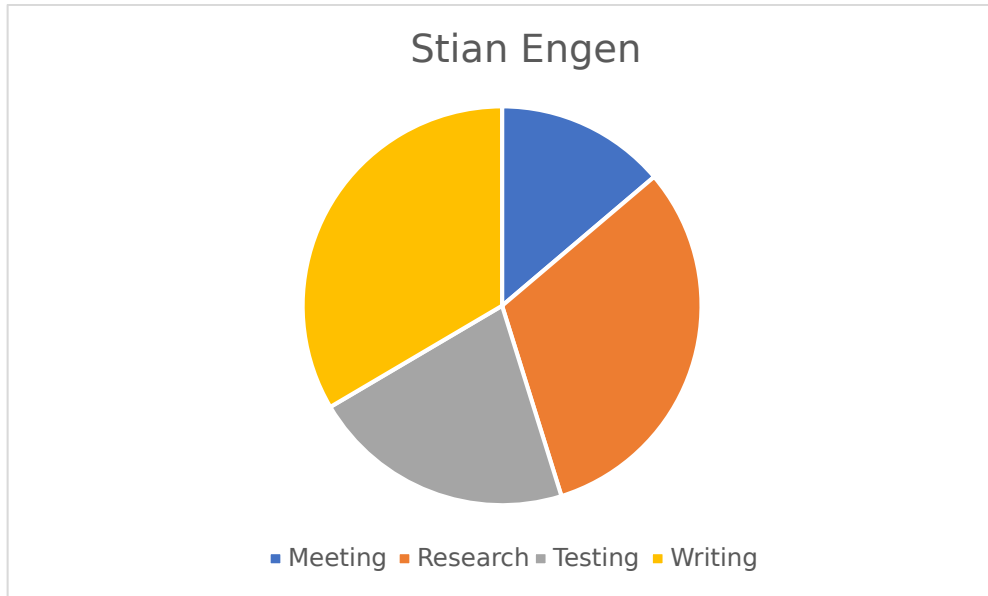
Discussed how the performance test should be documented, Erik suggested that we could get some help by filling out web form "Statistikkhjelpen for bacheloroppgave i ingeniørfag" and plan a meeting. We also got some clarification on what the document structure should look like and what we should include in the appendix.

13.05.2022:
Agenda

- How the performance test should be documented
- Is it enough to run each test 10 times
- What calculations should we include

In the meeting we agreed with Janne that it was enough to run each test 10 times since it was not that much variation in the test and we do not have strict requirements when it comes to accuracy. Janne said we should include a chart, mean value and standard deviation for each test.

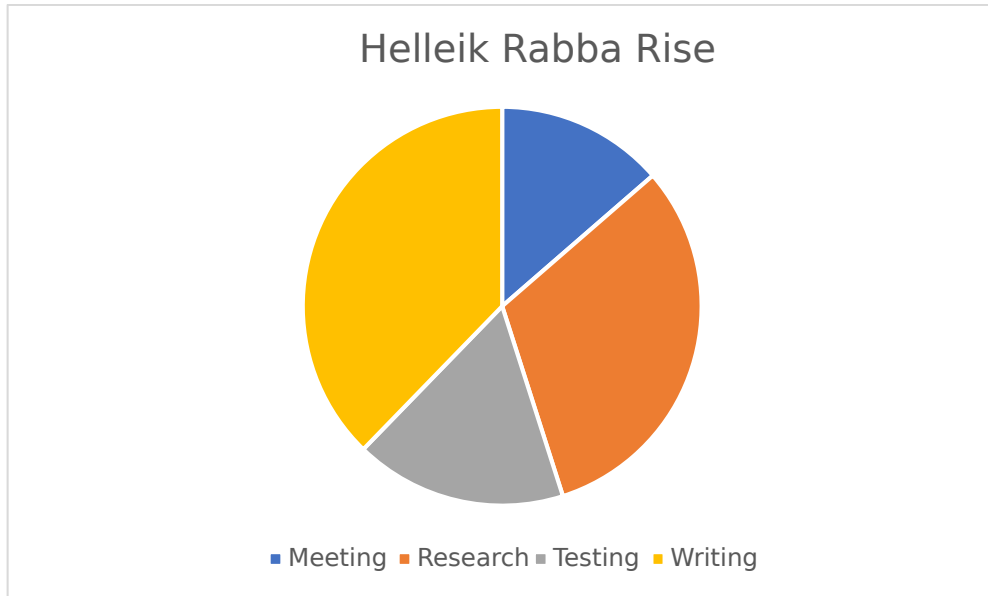
I Time tracking Stian Engen



Meeting: 66 hours
Research: 150 hours
Testing: 102 hours
Writing: 160 hours

Total: 478 hours

J Time tracking Helleik Rabba Rise



Meeting: 65 hours
Research: 150 hours
Testing: 82 hours
Writing: 179 hours

Total: 476 hours

K Contracts



Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett

Er den rett som den som skaper et åndsverk har til å fremstille eksemplarer av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater

Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater

Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn

Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring

Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt: Institutt for Informasjonssikkerhet og Kommunikasjonsteknologi
Veileder ved NTNU: Erik Hjelmås e-post og tlf. erik.hjelmas@ntnu.no , 93034446
Seksjon for Digital sikkerhet, NTNU IT Christoffer Vargrass Hallstensen, Faggruppeteider SOC Epost: Christoffer.hallstensen@ntnu.no Tel: 61135145
Student: Stian Engen Fødselsdato: 18.10.1999
Student: Helleik Rabba Rise Fødselsdato: 19.05.1999
Student: Mads Reneflot Moe Fødselsdato: 16.09.1996
Student: Mats Nerhagen Fødselsdato: 15.02.1999

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	X
Prosjektoppgave	
Annen oppgave	

Startdato: 11.01.2022
Sluttdato: 20.05.2022

Oppgavens arbeidstittel er:
NTNU Windows/Office Security baselines

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven¹. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten

¹ Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

<input type="checkbox"/>	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven
--------------------------	--

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

<input checked="" type="checkbox"/>	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt
-------------------------------------	---

Begrunnelse: Seksjon for Digital sikkerhet beholder eiendomsretten til resultatet for å sikre at ressurser betalt av offentlige midler skal gå til fellesskapets beste etter NTNUs strategi om «Kunnskap for en bedre verden». Seksjon for Digital sikkerhet forplikter seg til å lisensiere kode og rapport som åpen kildekode/creative commons slik at studentene kan ta med seg arbeidet nedlagt i prosjektet videre etter studier, men samtidig ivaretar at fremtidige studenter og andre kan bygge videre på arbeidet.

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

X	Oppgaven skal være offentlig
---	------------------------------

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss

Sett dato

Sett kryss	Sett dato
<input type="checkbox"/>	ett år
<input type="checkbox"/>	to år
<input type="checkbox"/>	tre år

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.





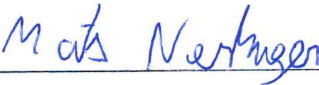
Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder

punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:	
Veileder ved NTNU: Dato:	
Seksjon for Digital sikkerhet, NTNU IT: Dato: 31.01.2022	
Student: Stian Engen Dato: 31.01.2022	 NORGESTEKNISK-NATURVITENSKAPELIGE UNIVERSITET
Student: Helleik Rabba Rise Dato: 31.01.2022	
Student: Mads Reneflot Moe Dato:	
Student: Mats Nerhagen Dato: 01.02.2022	

Signaturer

Student: Stian Engen Dato: 31.01.2022 Stian Engen
Student: Helleik Rabba Rise Dato: 31.01.2022 Helleik R. Rise
Student: Mads Reneflot Moe Dato:
Student: Mats Nerhagen Dato: 01.02.2022 Mats Nerhagen Mats Nerhagen
Seksjon for Digital sikkerhet, NTNU IT: Dato: 31.1.22



NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET



Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDMAL ved avtale om konfidensialitet mellom student og ekstern virksomhet i forbindelse med studentens utførelse av oppgave (master-, bachelor- eller annen oppgave) i samarbeid med ekstern virksomhet, jf. punkt 9 i standardavtale om utføring av oppgave i samarbeid med ekstern virksomhet.

Student ved NTNU: Stian Engen Fødselsdato: 18.10.1999
Student ved NTNU: Helleik Rabba Rise Fødselsdato: 19.05.1999
Student ved NTNU: Mads Reneflot Moe Fødselsdato: 16.09.1996
Student ved NTNU: Mats Nerhagen Fødselsdato: 15.02.1999
Ekstern virksomhet: Seksjon for Digital sikkerhet, NTNU IT

1. Studenten skal utføre oppgave i samarbeid med ekstern virksomhet som ledd i sitt studium ved NTNU.
2. Studenten forplikter seg til å bevare taushet om det han/hun får vite om tekniske innretninger og fremgangsmåter samt drifts- og forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde for den eksterne virksomheten. Det er den eksterne sitt ansvar å sørge for å synliggjøre og tydeliggjøre hvilken informasjon dette omfatter.
3. Studenten er forpliktet til å bevare taushet om dette i 5 år regnet fra sluttdato.
4. Kravet om konfidensialitet gjelder ikke informasjon som:
 - a) var allment tilgjengelig da den ble mottatt
 - b) ble mottatt lovlig fra tredjeperson uten avtale om taushetsplikt
 - c) ble utviklet av studenten uavhengig av mottatt informasjon
 - d) partene er forpliktet til å gi opplysninger om i samsvar med lov eller forskrift eller etter pålegg fra offentlig myndighet.

