

Naren Yogarajah

Trussel deteksjon i Microsoft Azure Cloud

Bacheloroppgave i Informatikk, drift av datasystemer

Veileder: Stein Meisingseth

Mai 2019

Naren Yogarajah

Trussel deteksjon i Microsoft Azure Cloud

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Stein Meisingseth
Mai 2019

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

Forord

Informatikk, drift av datasystemer er et praktisk opplagt studie hvor man lærer IT kompetanse rettet mot markedet. Denne kompetansen er fokusert og rettet mot IT driftsteknisk og sikkerhet kunnskap. I drift av datasystemer linjen er det sentralt med teamarbeid og prosjektarbeid er en de hyppige læringsformene som brukes i dette studiet. Hensikten med dette bachelorprosjektet fra et faglig synspunkt er å lære mer om mulighetene som finnes for deteksjon og overvåking i skyplattformen Azure. Dette har jeg som student greid å oppnå og jeg har lært om flere ulike muligheter som finnes for deteksjon i Azure. Vi har i Azure en haug med tjenester og jeg har greid å begrense oppgaven til å hovedsakelig fokusere på arbeidshypotesen som ble satt tidlig i prosjektet.

Takksigelse

I denne anledningen vil jeg takke min veileder Stein Meisingseth fra NTNU og Roger Schage Storløkken, Lars Arne Sand og Johan Fredrik Juell fra DNB. Dere har jeg gitt meg veldig gode tips og nyttig veiledning for hele bachelorprosjektet mitt. Jeg må innrømme at jeg har lært veldig mye fra tilbakemeldingene dere har tatt dere tid til å gi meg og ikke minst ser jeg for meg at disse tilbakemeldingene også vil hjelpe meg videre i livet. Tusen takk for at dere har vært gode og viktige støttespillere gjennom et slikt prosjekt som dette. Når jeg startet dette prosjektet så var det veldig mye informasjon å sette seg inn i. Med gode tips og triks fra deres side har jeg greid å strukturere og lage en god plan for å komme i mål med bachelorprosjektet og dette setter jeg veldig stor pris på. Nok en gang Tusen Takk for hjelpen.

Sammendrag

Cloud Computing er et høyt oppegående tema blant dagens næringsliv og kombinasjonen med IT-sikkerhet blir dermed et viktig utgangspunkt for bedrifter å sette seg inn i. Ettersom IT-sikkerhet har blitt et veldig viktig tema de siste årene og min interesse for å lære mer om sikkerhetsdelen innenfor data har jeg valgt å skrive om IT-sikkerhet i Microsoft Azure Cloud. Bachelorprosjektet tar for seg muligheter som finnes for trussel deteksjon i Microsoft Azure Cloud. Tjenester som Azure Identity Protection, Azure Log Analytics og Azure Security Center er et sentralt utgangspunkt gjennom hele prosjektet. Prosjektet starter med å ta for seg en forstudieanalyse hvor det blir angitt ulike mål, utføring av interessentanalyse og avdekning av ulike risikoer knyttet til prosjektet. Deretter forsetter jeg med en systemkravrapport som tar for seg beskrivelse og funksjonalitet av ulike tjenester i Azure knyttet til sikkerhetsområdet. Videre fortsetter det med et driftsdokument hvor alt av installasjon og konfigurasjon av tjenester beskrevet i systemkravrapporten foregår. Helt tilslutt reflekterer jeg over meg og min gjennomgang av prosjektet i sluttrapporten.

Summary

Cloud Computing is a high rising theme among today's business. Therefore, the combination of cloud and IT security have been an important base of focus for today's businesses. I have always been interested in learning more about IT security and therefore I have chosen to write about Threat detection in Microsoft Azure Cloud which is an upcoming important theme among today's IT industry. In my bachelor's thesis you will learn more about the opportunities for threat detection in Microsoft Azure Cloud. Important services like Azure Identity Protection, Azure Log Analytics and Azure Security Center are central focal points throughout the whole project. The project starts with a pilot study where I focus on defining the goals for the project. I also conduct a stakeholder analysis and chart the various risks associated to the project. Then I continue with a system requirement report that consists of descriptions and functionality of variety of security services associated with threat detection in Azure. Furthermore, I continue with an operation document which consist of installations and configurations. At last I finish off with a reflection on myself and my review of the project in the final report. In this report I will give you an insight into how the project has taken place and how I solved the tasks and goals.

Forstudierapport

Versjon 0.4

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
14.01.19 - 20.01.19	0.1	Opprettelse av forstudierapport og formatering, Interessenter og rammebetingelser, standarder og metoder, prosjektets omfang og avgrensninger, Retningslinjer og standarder, prosjektorganisering, krav til kvalitetsgjennomgang, endringshåndtering, Risikoanalyse, kritiske suksessfaktorer, Prosjektets milepæler og hovedaktiviteter, Introduksjon, bakgrunn, formattering, innholdsfortegnelse	Naren Yogarajah
21.01.19 - 25.01.19	0.2		Naren Yogarajah

		Beskrivelse av problemet, Rammebetingelser og krav, Utføre endringer fra veiledningsmøte #2, Risikoanalyse elementer, interessentanalyse, prosjektmål	
26.01.19 - 28.01.19	0.3	Risikoanalyse, Innholdsfortegnelse, definisjoner og forkortelser	Naren Yogarajah
12.04.19	0.4	Innholdsfortegnelse, struktur, overskrifter	Naren Yogarajah

Innholdsfortegnelse

1. Introduksjon	13
2. Bakgrunn for prosjektet	13
2.1 Beskrivelser av problemer og behov	13
2.1.2 Definisjoner og forkortelser	14
2.2 Kort om dagens systemer og rutiner	15
2.2.1 Dagens systemer	15
2.2.2 Brukerne av skytjenesten	15
2.2.3 Forvaltning og drift	15
2.2.4 Oppgradering av dagens systemer	15
3. Prosjekt mål	16
3.1 Effektmål	16
3.2 Resultatmål	16
3.3 Prosessmål	16
3.4 Prosjektets omfang	17
3.4.1 Prosjektets avgrensninger	17
3.4.2 Prosjektets funksjonelle egenskaper	17
3.4.3 Prosjektets ikke-funksjonelle egenskaper og krav	18
3.5 Prosjektets milepæler og hovedaktiviteter	18
4. Interessenter og rammebetingelser	19
4.1 Interessentanalyse	19
4.2 Rammebetingelser	21
5. Kritiske suksessfaktorer	22
5.1 Suksessfaktorer	22
5.2 Informasjonsbehov	22
6. Risikoanalyse	24
7. Retningslinjer og standarder	27
7.1 Krav til dokumentasjon	27
7.2 Krav til kvalitetsgjennomganger	28
7.3 Krav til standarder og metoder	28
7.4 Endringshåndtering	29
8. Prosjektorganisering	30
9. Anbefaling om videre arbeid	31

Figur 1 Prosjektets milepæler og hovedaktiviteter	18
Figur 2 Interessenter	20
Figur 3 Risikoanalysemodell	26
Figur 4 Prosjektorganisering	30

Tabell 1 Prosjektets funksjonelle egenskaper.....	17
Tabell 2 Informasjonsbehov	22
Tabell 3 Dokumentasjonskrav	27

1. Introduksjon

Hensikten med dokumentet er å finne ut hvordan prosjektet skal struktureres og planlegges. Hensikten ved å utføre en forstudierapport går ut på å gå gjennom prosjektets ulike faser og kartlegge konsekvenser og hindringer som kan oppstå underveis i prosjektet.

Forstudierapporten tar for seg prosjektets mål hvor det inngår ulike type mål som effektmål, resultatmål, prosessmål, videre vil man ta for seg interessenter og rammebetingelser for prosjektet da vil man her inkludere en interessentanalyse. Deretter kartlegges det kritiske suksessfaktorer og videre blir det utført en risikoanalyse for prosjektet. I risikoanalysen vil man ta for seg ulike risikoelementer som kan forekomme i prosjektet. Deretter skal man sette en del retningslinjer og standarder man jobber ut ifra i prosjektet. Videre skal vi se litt mer på hvordan prosjektet er organisert. Tilslutt blir det en kort anbefaling om videre arbeid med dette aktuelle prosjektet.

2. Bakgrunn for prosjektet

Bakgrunn for prosjektet er å finne gode sikkerhetsløsninger for DNB sitt cloud system Azure. Bruk av skytjenester blir mer og mer relevant på bedriftsmarkedet og dermed blir det viktig å finne grundige sikkerhetsløsninger som gir gode tiltak for å beskytte slike skytjenester. I den anledningen har jeg fått i oppgave om å skrive om «Sikkerhet i Azure» med problemstillingen «hvilke muligheter finnes det for trussel deteksjon i Azure ved bruk av tjenester som Azure Active Directory, Azure Log Analytics og Azure Security Center».

2.1 Beskrivelser av problemer og behov

Flere bedrifter på dagens marked migrerer sine fysiske IT løsninger til skyen i dag. En stor problemstilling rundt dette er hvor sikkert skyen egentlig er. Etersom migreringen til clouden foregår så man samtidig ta for seg sikkerheten i den nye cloud plattformen. Det er da man møter utfordringer i bedriften slik som:

- Det blir en økt angrepsflate
- Det blir en økning av antall log kilder som skal overvåkes
- Det blir også en økning av sikkerhetsverktøy man må sette seg inn i.
- Man trenger kompetanse og prosedyrer som man må følge knyttet til det nye miljøet

2.1.2 Definisjoner og forkortelser

- DNB – Den Norske Bank
Den Norske Bank er det største finanskonsernet her i Norge.
- TCS - Tata Consultancy Services
Tata Consultancy Services er en indisk multinasjonal informasjonsteknologi bedrift som har sitt hovedkvarter i Mumbai i India.
- HCL Technologies
HCL Technologies er et indisk multinasjonalt teknologiselskap som har sitt hovedkvarter i Noida, Uttar Pradesh, India. Noen av tjenestene de tilbyr er blant annet Cloud, Cybersikkerhet, infrastruktur, applikasjon og business tjenester.
- DxC Technology
DxC er en bedrift som fokuserer på å levere informasjonsteknologi tjenester som fokuserer på digital transformasjon for større globale organisasjoner.
- Infosys
Infosys er et multinasjonalt selskap som tilbyr tjenester innenfor informasjonsteknologi, business, outsourcing.
- EVRY
EVRY er Nordens største IT Selskap og de tilbyr tjenester innenfor informasjonsteknologi og programvare.

2.2 Kort om dagens systemer og rutiner

2.2.1 Dagens systemer

DNB ønsker ikke å gå direkte inn på akkurat dette og henviser til å fokusere mer på Azure og hvilke muligheter man har i Azure. Microsoft Azure er en cloud computing tjeneste, vi kan også kalle Azure for en skyplattform hvor man blant annet har flere ulike muligheter til å drive med utvikling, testing, distribuering og tjenester. Disse mulighetene går hovedsakelig gjennom Microsoft sine datasentre som er plassert verden rundt.

2.2.2 Brukerne av skytjenesten

Brukerne av cloud systemet Azure er IT-ansatte i DNB. Det brukes også noen tjenester av DNB sine ansatte uten at disse ansatte er nødvendig klar over at de tar i bruk tjenester fra Azure.

2.2.3 Forvaltning og drift

Ansvar for forvaltningen og driften i DNB består av en kombinasjon av forvaltede tjenester og underleverandører. DNB har godt samarbeid med underleverandører som EVRY, HCL, TCS, Infosys og DxC Technology.

2.2.4 Oppgradering av dagens systemer

DNB har for tiden satt i gang med å oppgradere sine systemer til å migreres til skyen. On-Premises datasentre blir migrert opp til ulike skyløsninger.

3. Prosjektmål

Prosjektets mål går ut på å kartlegge og finne ut av hvilke muligheter det finnes for trussel deteksjon i tjenester som Azure Security Center, Azure Log Analytics og Azure Active Directory. Innenfor dette målet innebærer det at man blir kjent med Cloud Computing tjenesten Azure og dens funksjoner. Det vil også bli viktig å forstå de grunnleggende konseptene innenfor Cloud Computing og forstå Azure sin sikkerhetsarkitektur.

3.1 Effektmål

Få en økt bevisstgjøring av muligheter for hvordan man kan avdekke trusler i skytjenesten Azure og hvordan man kan forebygge/hindre slike angrep. Et indirekte effektmål kan også settes til å forbedre sikkerheten i bedriften siden det vil ikke for meg være mulighet til å direkte gjøre fysiske endringer i DNB.

3.2 Resultatmål

Ut ifra dette prosjektet skal det klart fremlegges hvilke muligheter det finnes for å gjenkjenne trusler ved hjelp av tjenester som Azure Security Center, Azure Log Analytics og Azure Active Directory. Forebygging av slike trusler ved hjelp av innebygde forsvarsmekanismer i Azure kan også være et sluttmaal dersom det gjenstår tid i oppgaven.

3.3 Prosessmål

Prosessmål som kan bli satt for dette prosjektet er følgende:

- Å få en god forståelse av Azure og dens funksjoner
- I et slikt prosjekt blir det også viktig for meg å fokusere på å øke min kompetanse innenfor digital samhandling.
- Å få en god karakter på oppgaven og gi mitt beste slik at jeg kan prøve å få en toppkarakter.
- Bli bedre kjent med hvordan DNB arbeider med datasikkerhet i deres bedrift.

3.4 Prosjektets omfang

Prosjektets omfang skal hovedsakelig utgangspunkt i følgende punkter for videre arbeid i oppgaven:

- Cloud trusler og sikkerhet i Azure - alt skal handle om Azure
- Azure Sikkerhetsinfrastruktur
- Azure Security Center
 - Detektere angrep
 - Vise angrep som blir utført og hvordan de merkes i sikkerhetssenteret
 - Forebygge angrep
 - Analysere trusler
- Azure Active Directory
- Azure Log Analytics
- Andre tjenester for trussel deteksjon (Dersom du har tid)

3.4.1 Prosjektets avgrensninger

Prosjektet skal ikke sammenligne Azure med andre skytjenester.

Azure har en haug med funksjoner, så prosjektet skal ikke ta for seg alle funksjonene i Azure. Dermed blir det her viktig å avgrense det viktigste relatert til den aktuelle problemstillingen.

3.4.2 Prosjektets funksjonelle egenskaper

Tabell 1 Prosjektets funksjonelle egenskaper

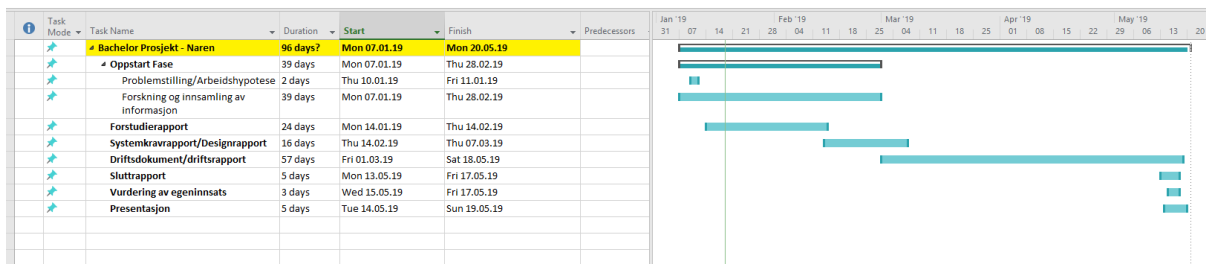
Produkt	Funksjon
Microsoft Azure	Skal tilby virtuelle maskiner, et virtuelt nettverk, sikkerhetssenter, muligheter for log analyser, Active directory
Microsoft Windows 10 Education (i Azure)	Skal være tilknyttet domene fra Windows Server 2016
Windows Server 2016 Standard (i Azure)	Skal ha en fungerende domenekontroller

Ubuntu 18.04 (i Azure)	Skal ha SSH installert
Kali Linux 2018.1 (i Azure)	Skal ha SSH installert, ulike angrepsmåter skal demonstreres

3.4.3 Prosjektets ikke-funksjonelle egenskaper og krav

- Azure må være tilgjengelig under prosjektet.
- Det er viktig at prosjektet innleveres til sluttdatoen som er satt for dette aktuelle prosjektet.

3.5 Prosjektets milepæler og hovedaktiviteter



Figur 1 Prosjektets milepæler og hovedaktiviteter

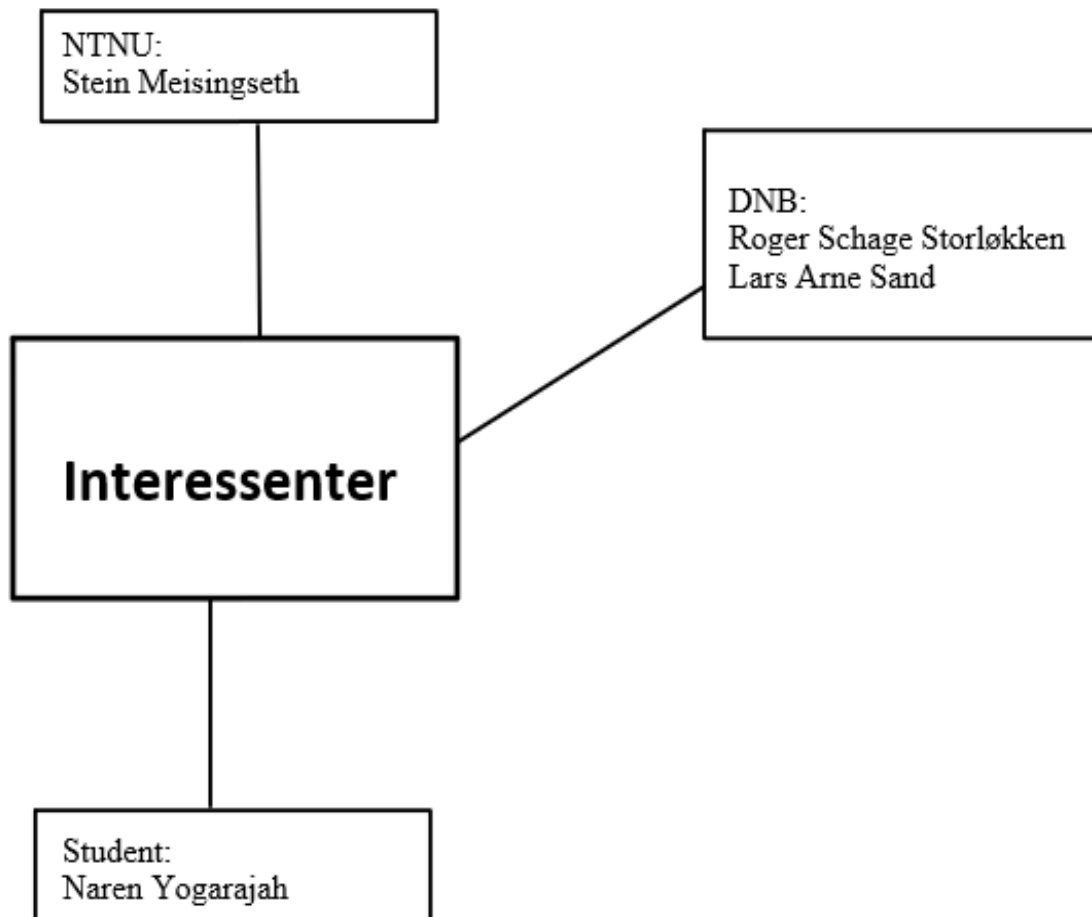
Prosjektets milepælsplan og hovedaktiviteter har blitt vedlagt som et Microsoft Project 2016 dokument i forstudierapporten.

4. Interessenter og rammebetingelser

4.1 Interessentanalyse

- **Oppgavestiller:**
Oppgavestiller i prosjektet er DNB i samarbeid med NTNU.
- **Brukere:**
Brukerne som kommer til å bruke denne løsningen er IT-ansatte i datasikkerhet avdelingen til DNB.
- **Godkjenning av resultat:**
Godkjenning av resultat blir utført av oppgave stillere fra DNB: Roger Schage Storløyken og Lars Arne Sand i samarbeid med hovedveileder Stein Meisingseth fra NTNU.
- **Det daglige livet:**
Det er ingen som direkte blir berørt av prosjektet.
- **Vite mer om produktet:**
Naren Yogarajah som skriver bacheloroppgaven trenger å vite mer om produktet. I dette tilfellet er det ikke et spesifikt produkt, men det er ulike tjenester som man bør sette seg inn i løpet av prosjektet.
- **Prosjektforløpet:**
Den som trenger å vite noe om prosjektforløpet er de tre interessenter partene som involvert i prosjektet: DNB (Roger Schage Storløyken og Lars Arne Sand), NTNU (Stein Meisingseth), Naren Yogarajah.
- **Utføring av arbeidet:**
Naren Yogarajah utfører arbeidet med veiledning fra følgende parter: DNB (Roger Schage Storløyken og Lars Arne Sand) og NTNU (Stein Meisingseth)
- **Bidrag og leveranse:**
Bidrag og leveranse av prosjektet blir utført av NTNU student Naren Yogarajah

(3.årstrinn, Informatikk med spesialisering i drift av datasystemer).



Figur 2 Interessenter

Interessenter	Suksesskriterium	Bidrag til prosjektet
DNB: Roger Schage Storløkken, Lars Arne Sand	Får ny kunnskap om sikkerhet innenfor Azure.	Hovedansvar for å gi veiledning til leverandør. Utdeling av nødvendig materiell for prosjektet.
NTNU: Stein Meisingseth	Får ny kunnskap om sikkerhet innenfor Azure.	Hovedansvar for å gi veiledning til leverandør.
Leverandør: Naren Yogarajah	Får en grundig og dyp forståelse innenfor Azure og hvordan dens sikkerhet fungerer	Ansvar for å utføre prosjektet med dokumentasjon underveis.

4.2 Rammebetingelser

- **Absolutte krav til ferdigdato:**

Prosjektet skal være ferdig levert til 20 mai 2019.

- **Absolutte krav til kostnadsramme:**

Absolutte krav til kostnadsrammen for dette prosjektet er 10000,- NOK , referert fra veileder i DNB Lars Arne Sand.

- **Myndighetskrav:**

Prosjektet skal være utført i henhold til norske lover.

- **Drifts og utviklingsmiljø:**

Drifts og utviklingsmiljø skal foregå i Windows 10 Education/Home/Enterprise, Ubuntu 16.04/18.04, Windows Server 2012/2016 og Microsoft Azure.

5. Kritiske suksessfaktorer

5.1 Suksessfaktorer

- Det er viktig at oppdragstaker bruker god tid til å forstå hvordan skyplattformen Azure fungerer og dens funksjoner.
- Løsningen som legges frem bør være et grundig og vel analysert resultat som viser gode muligheter for sikkerhetsmekanismer som kan tas bruk i Azure

5.2 Informasjonsbehov

Tabell 2 Informasjonsbehov

Mottakelse av informasjon	Form av informasjon	Tidspunkt for levering	Formål
DNB (Roger Schage Storløkken og Lars Arne Sand), NTNU (Stein Meisingseth)	Forstudierapport	15.02.2019	Tilbakemelding fra veilederne og bruk for revisjon basert på tilbakemeldingene
DNB (Roger Schage Storløkken og Lars Arne Sand), NTNU (Stein Meisingseth)	Systemkrav Rapport	08.03.2019	Tilbakemelding fra veilederne og bruk for revisjon basert på tilbakemeldingene
DNB (Roger Schage Storløkken og Lars Arne Sand), NTNU (Stein Meisingseth)	Driftsdokument	10.05.2019	Tilbakemelding fra veilederne og bruk for revisjon basert på tilbakemeldingene
DNB (Roger Schage Storløkken og Lars	Sluttrapport	15.05.2019	Tilbakemelding fra veilederne og bruk

Arne Sand), NTNU (Stein Meisingseth)			for revisjon basert på tilbakemeldingene
DNB (Roger Schage Storløkken og Lars Arne Sand), NTNU (Stein Meisingseth)	Tidsskjema	Ukentlig revisjon	Informasjon om status for prosjekt
DNB (Roger Schage Storløkken og Lars Arne Sand), NTNU (Stein Meisingseth)	Prosjektplan	Ukentlig revisjon	Informasjon om status for prosjekt
DNB (Roger Schage Storløkken og Lars Arne Sand), NTNU (Stein Meisingseth)	Prosjekthåndbok	15.05.2019	Tilbakemelding fra veilederne og bruk for revisjon basert på tilbakemeldingene
DNB (Roger Schage Storløkken og Lars Arne Sand), NTNU (Stein Meisingseth)	Presentasjon	Ca. 20 mai	Presentasjon av prosjektet

Tidspunktene for levering er satt som absolutt siste dato for frist, men det er mulig at man leverer litt tidligere også.

6. Risikoanalyse

- **1. Problemer som kommer på bakgrunn av maskinvare og dens funksjonalitet**

Konsekvens:

Et av marerittene vi oppdragstakere står ovenfor er dersom flere ukers/måneders arbeid plutselig forsvinner og at det ikke er mulighet for gjenopprettelse av arbeidet.

Konsekvensen av dette er at prosjektet ikke blir utført til den aktuelle sluttdatoen som er satt og eventuelt kan bli avbrutt av prosjekt stiller.

Tiltak:

Det er viktig at man tar regelmessige sikkerhetskopier av alle dokumenter liggende både på datamaskinen fysisk, ta i bruk en skylagringstjeneste som OneDrive eller Google Drive og ikke minst blir det veldig viktig å ha prosjektet lagret og oppdatert på en ekstern disk som USB, Ekstern Harddisk eller SSD. Man kan også etter å ha utført hvert arbeid, sende en kopi på e-post, slik at man har dokumentasjonen også liggende på e-posten.

Kommentar:

Konsekvensene dersom man mister veldig mye dokumentasjon er ganske stor i slike prosjekter. Jeg velger å ta regelmessig backup på forskjellige plattformer, slik at sannsynligheten for at dette skal skje er veldig liten. Men, det er mulighet for at det kan oppstå problemer med maskinvare og dette kan bli beregnet som en større risiko i et slikt prosjekt. Faren for at dette skal foregå er veldig liten og sannsynligheten for at det oppstår av seg selv er også ganske liten.

- **2. Sykdom som oppstår underveis under utføring av oppdraget**

Konsekvens:

Konsekvensen av at sykdom oppstår underveis i prosjektet vil føre til at man vil miste mange arbeidstimer og det vil igjen føre til at man ikke får levert prosjekt til tide.

Tiltak:

Når eventuelle sykdommer oppstår underveis i prosjektet er det viktig at man

informerer så raskt så mulig veileder og oppgavestiller og prøver å komme til en løsning i samarbeid med alle parter.

Kommentar:

Sannsynligheten for eventuelle sykdom som skal oppstå under prosjektet er middels lav, og dersom det oppstår er jeg som oppdragstaker klar over at jeg er nødt til å jobbe uansett siden jeg jobber individuelt og jeg vil komme i mål med prosjektet.

- **3. Prosjektgruppen som utfører oppdraget mangler kompetanse og ressurser**

Konsekvens:

Konsekvensen av at prosjektgruppen har mangel på kompetanse og ressurser vil føre til at man ikke får oppfylt kravene som er satt for prosjektet, det vil også være at man utfører prosjektet på en uønsket måte som også kan dra med seg kritiske og alvorlige feil og komplikasjoner.

Tiltak:

Hovedtiltaket her er å ta i bruk internett og man kan også spørre fagansvarlige/veiledere for prosjektet. Internett har i utgangspunktet de fleste ressursene som man trenger for å utføre prosjektet.

Kommentar:

Hvis vi beregner konsekvensene av dette utfallet så kan man si at konsekvensene ikke er så store som de andre risikoelementene i og med at man har Internett som en hovedressurs og i tillegg så finnes det ganske mye gode og hensiktsmessige videoer på nettet.

- **4. Naturkatastrofer som ødelegger datasentre**

Konsekvens:

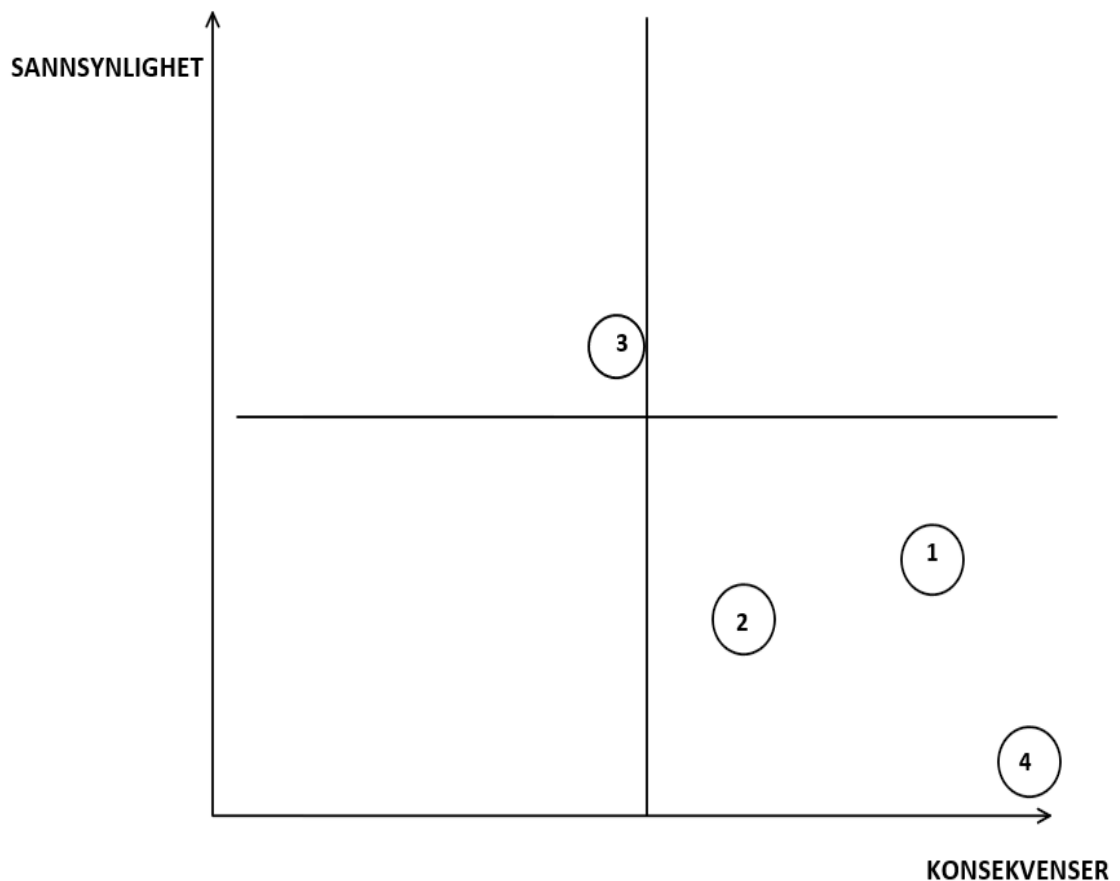
Konsekvenser av naturkatastrofer som ødelegger datasentre vil påvirke prosjektet enormt, dersom alle datasentre som fungerer som hoved maskinvare til prosjektet går ned, er det mye data og prosjektarbeid som vil gå tapt.

Tiltak:

Datasentre er i dag beskyttet mot nesten alle type katastrofehendelser. Man har blant annet eget sikret rom for å opprettholde alle disse datasentrene. Datasentre har ofte fysiske sikringer som er godt rustet for ulike type naturkatastrofer som f.eks egne sikringsmekanismer og isolasjonslag.

Kommentar:

Faren for naturkatastrofe er liten, men samtidig er sannsynligheten for at dette blir til realitet på en skala fra lav til høy så vil denne risikoen ligge midt imellom. Da blir konsekvensene veldig stort. Man vet aldri hva som skjer i framtiden og dermed vet man heller ikke om en slik naturkatastrofe vil inntreffe.



Figur 3 Risikoanalysemodell

7. Retningslinjer og standarder

7.1 Krav til dokumentasjon

Tabell 3 Dokumentasjonskrav

Navn	Dato	Type	Kommentar
Forstudierapport	14.02.2019	Elektronisk (Microsoft Word)	Skal inkludere prosjektets milepælsplan og hovedaktivitet i MS Project form.
Systemkrav/Designrapport	07.03.2019	Elektronisk (Microsoft Word)	
Driftsdokument/Driftsrapport	18.05.2019	Elektronisk (Microsoft Word)	
Sluttrapport	17.05.2019	Elektronisk (Microsoft Word)	
Individuelt refleksjonsnotat	16.05.2019	Elektronisk (Microsoft Word)	
Framdriftsplan	Skal revideres ukentlig	Elektronisk (Microsoft Project 2016)	
Tidsskjema	Skal revideres ukentlig	Elektronisk (Microsoft Word)	
Prosjekthåndbok	15.05.2019	Elektronisk (Microsoft Word)	
Presentasjon	Ca. 20 mai	Elektronisk (Microsoft	

		PowerPoint, Skype for Business)	
--	--	---------------------------------------	--

7.2 Krav til kvalitetsgjennomganger

Vedlagte dokumenter i tabellen ovenfor skal bli levert til oppdragsgiver og veilederne for dette prosjektet. Deretter skal tilbakemelding fra veilederne bli brukt som et utgangspunkt for revidering, kvalitetssjekk og forbedring på de ulike dokumentene.

7.3 Krav til standarder og metoder

Prosjektet skal ta i bruk følgende standarder og metoder:

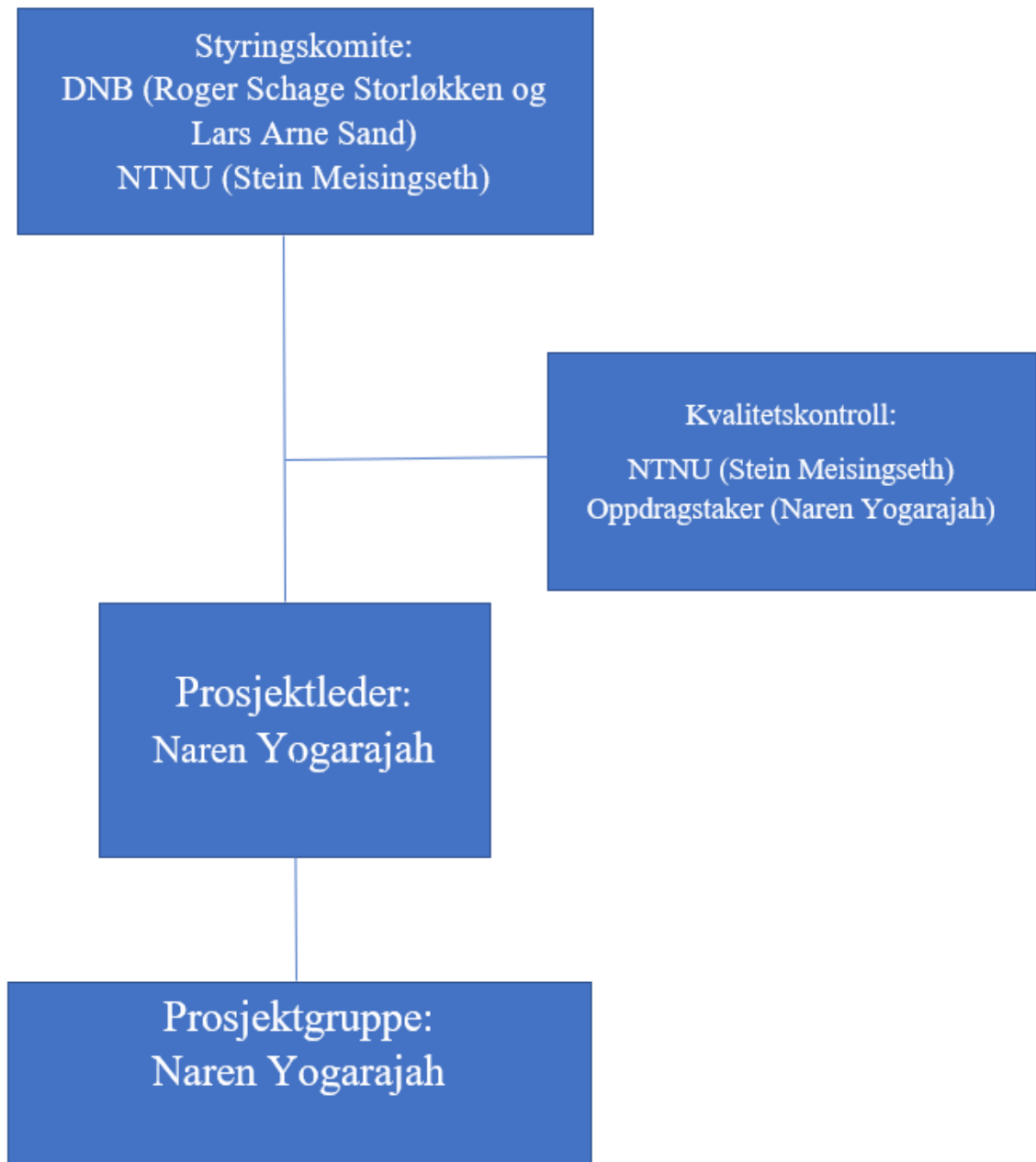
- Databaseverktøy
 - Microsoft Azure Cloud SQL Database
- Digital Samhandling
 - Skype for Business
 - Office 365
 - Google Drive
 - Blackboard Learn+
- Dokumentmaler
 - Forstudierapport Mal
 - Designdokument Mal
 - Driftsdokument Mal
 - Sluttrapport Mal
- Utviklingsverktøy
 - Windows 10 Education/Home/Enterprise
 - Ubuntu 16.04/18.04
 - Windows Server 2012/2016/2019

- Debian 9.2 (Stretch)
- Kali Linux 2018.1
- Microsoft Azure
- Windows PowerShell
- Visual Studio Code

7.4 Endringshåndtering

Dersom det foreligger ønsker for å forandre allerede avtalte planer fra prosjektet kreves dette at det utføres i samarbeid med følgende parter: DNB (Roger Schage Storløkken og Lars Arne Sand), NTNU (Stein Meisingseth) og oppdragstaker (Naren Yogarajah). Da vil det være helt normalt å følge en formell prosedyre som krever at man dokumenterer endringens innhold, deretter analyserer hva som blir konsekvensene av endringene for prosjektet, deretter må man beregne eventuelle kost og nytte kostnader, videre kreves det at prosjektet godkjennes og avtales på nytt fra inkluderende parter. Det blir også viktig å skrive logg samtidig som endringen trår til, videre så må man justere planene som allerede er satt opp. Videre skal man gi beskjed til interessentene i prosjektet og deretter utføre de avtalte endringene til rett tidspunkt. Det vil bli viktig å forstå at oppdragstaker vil innkalle til et møte og de forandringene vil bli et godt utgangspunkt for videre diskusjon før man tar en grundig og gjennomtenkt avgjørelse.

8. Prosjektorganisering



Figur 4 Prosjektorganisering

I og med at oppdraget blir utført av en person individuelt er det ikke nødvendighet for arbeidsfordeling i prosjektet. Men, det kreves at studenten greier å strukturere hver del av prosjektet slik at studenten får nok tid til å jobbe med hver ulike del.

9. Anbefaling om videre arbeid

Prosjektet anbefales at det blir tatt videre, men forutsetning er at siden prosjektet blir utført av kun en person vil det kreve hardt arbeid, struktur og disiplin gjennom prosjektperioden for å komme i mål og oppnå gode resultater. Ikke minst blir det større mengder med arbeidsoppgaver som må deles jevnt og hensiktsmessig utover prosjektperioden. Videre arbeid bør også fokusere på integrasjon av andre tredjepartstjenester som er i samme kategori som prosjektets tjenester. Det blir her veldig sentralt å se på hvordan samspillet foregår mellom Azure og tredjeparts tjenestene. Eksempelvis er det flere bedrifter som tar i bruk Splunk og dette er noe Azure har mulighet til å integrere. For å forstå samspillet mellom f.eks disse to tjenestene er det sentralt å lese seg opp på hva Splunk er, hvilke funksjonalitet den har og konfigurasjon av denne tjenesten samtidig som man har Azure og dens funksjonalitet i bakhode.

Systemkrav-rapport

Versjon 0.3

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
23.01.19 - 23.02.19	0.1	Oppsett, formatering, Nettverkstopologi, definisjoner og forkortelser, Azure Identity Protection, figur for IDP, Azure Security Center - varsler, deteksjon, Use case, eksempler, just in time vm, deteksjonsmetoder	Naren Yogarajah
24.02.19 – 25.03.19	0.2	Use case, threat detection, Log Analytics, log analytics deteksjon, grammatikk +språk, Azure ATP, ad connect, security center deteksjon, Shared Responsibility Model, se gjennom før innsending til 1.utkast, Microsoft antimalware, Behavioral Analysis, anomali deteksjon, Endring av norske	Naren Yogarajah

		<p>begreper til engelske, 1.utkast systemkrav tilbakemelding, Struktur, omgjøring, Azure Sentinel, Detection & Security Monitoring, stavekontroll</p>	
26.03.19 - 24.04.19	0.3	<p>Endring av Begrunnelse for valg av løsning, Brukere, domain og passord, Endring av kildehenvisning, passord til global azure administrator endret, Gjenkjenn angrep på Docker løsning, Deteksjon av trusler i kontainer løsning, Firewall Traffic anomalies</p>	Naren Yogarajah

Innholdsfortegnelse

1. Innledning	41
1.1 Dokumentets hensikt	41
1.2 Oversikt over innholdet.....	41
1.3 Referanser.....	41
2. Prosjektets omfang	42
2.1 Kort om kunden og deres behov.....	42
2.2 Definisjoner og forkortelser.....	42
2.3 Avgrensning av prosjektet.....	43
3. Begrunnelse for valg av løsning	43
4. Teori.....	44
4.1 Cloud Computing.....	44
4.1.1 Public Cloud	44
4.1.2 Private Cloud	44
4.1.3 Hybrid Cloud	45
4.1.4 Infrastructure as a service (IaaS)	45
4.1.5 Platform as a service (PaaS)	45
4.1.6 Serverless computing	45
4.1.7 Software as a service (SaaS).....	45
4.1.8 Trusler og sikkerhet i skyen	46
4.1.8.1 Cloud Weaponization.....	46
4.1.8.2 Feilkonfigurasjon.....	46
4.1.8.3 Usikre API.....	47
4.2 Microsoft Azure.....	47
4.2.1 Hvordan fungerer Azure	48
4.3 Shared Responsibility Model.....	49
4.4 Detection & Security Monitoring	51
4.5 The Cyber Kill Chain	52
5. Use-cases	54
5.1 Beskrivelse av Use-cases	54
6. Azure.....	56
6.1 Tjenester i Azure.....	56
6.1.1 Azure Active Directory.....	56
6.1.1.1 Azure Active Directory Connect.....	56

6.1.1.2 Azure Identity Protection	57
6.1.1.3 Azure AD Privileged Identity Management.....	57
6.1.1.4 Azure Advanced Threat Protection	57
6.1.2 Azure Log Analytics	58
6.1.3 Azure Security Center	59
6.1.3.1 Just In Time VM Access.....	61
6.1.3.2 Network Security Groups	62
6.1.3.3 Security Alerts Map	62
6.1.3.4 Security Policy	63
6.1.4 Azure Sentinel.....	63
6.1.5 Implementasjon av jump servere.....	64
6.2 Beskrivelse av hvordan tjenestene kan oppdage trusler	65
6.2.1 Hvordan beskyttes identitet i dag i Identity Protection	65
6.2.1.1 Azure Multi Factor Authentication.....	69
6.2.1.2 Uhåndtert Cloud Programvare	69
6.2.2 Hvordan kan man bruke Log Analytics til å oppdage trusler.....	70
6.2.2.1 Firewall Traffic anomalies	73
6.2.3 Metoder for trussel deteksjon i Security Center.....	74
6.2.3.1 Atomic Detection.....	75
6.2.3.2 Threat Intelligence	76
6.2.3.3 Behavioral Analysis	77
6.2.3.4 Anomaly Detection	78
6.2.3.5 Detection Fusion	79
6.2.3.6 Microsoft Antimalware	81
6.2.3.7 Strengthen Security Posture	82
6.2.3.8 File Integrity Monitoring (FIM).....	83
6.2.3.9 Security Alerts	83
6.2.4 Hvordan fungerer trussel deteksjon i Azure Security Center	83
6.2.4.1 Gjenkjenn angrep på kontainerløsninger i Azure.....	85
6.2.5 Hvordan kan man ta i bruk Azure Sentinel for trussel deteksjon.....	87
6.2.5.1 Advanced Alert Rules	88
6.2.5.2 GitHub Threat Detection Library	88
6.2.5.3 Hunting-tool	88
6.2.5.4 Automated Threat Response.....	88
6.2.6 Advanced Threat Protection for Azure SQL Databaser	89
6.2.6.1 Vulnerability to SQL injection	89

6.2.6.2 Potential SQL injection	90
6.2.6.3 Access from unusual location	90
6.2.6.4 Access from a potentially harmful application	90
7. Use-case tilnærming i Azure	91
8. Nettverkstopologi	95
9. Kilder	98

Figur 1	49
Figur 2	51
Figur 3	59
Figur 4	60
Figur 5	65
Figur 6	74
Figur 7	80
Figur 8	86
Figur 9	87
Figur 10	95

Tabell 1	52
Tabell 2	71
Tabell 3	72
Tabell 4	73
Tabell 5	73
Tabell 6	81
Tabell 7	91
Tabell 8	96
Tabell 9	96
Tabell 10	96
Tabell 11	97

1. Innledning

1.1 Dokumentets hensikt

Hensikten med systemkravrapporten er å gi et helhetlig bilde som er med på å vise hvilke funksjoner som skal tas med videre i prosjektet. Systemkravrapporten skal også gi en konseptuell beskrivelse av de ulike punktene som skal utføres i prosjektet og det skal være tilrettelagt et godt bilde for videre utføring av prosjektet. Systemkravrapporten er utformet i bacheloroppgave sammenheng der det skrives om "Sikkerhet i Azure" i samarbeid med DNB og NTNU.

1.2 Oversikt over innholdet

Systemkravrapporten tar for seg flere ulike deler. Rapporten starter med å forklare dokumentets hensikt, videre får man en oversikt over hva systemkravrapporten tar for seg. Deretter får man en oversikt over tilgjengelige referanser fra andre dokumenter i systemkravrapporten. Videre så blir det en liten kort innledning med informasjon om kunden og deres behov for dette prosjektet. Deretter fortsetter dokumentet videre med å ta for seg aktuelle definisjoner og forkortelser som har blitt nevnt i systemkravrapporten. Under avgrensning av prosjektet vil det sies noe om hvor grensen går for prosjektet og hvilke punkter som man ikke skal ta for seg som utgangspunkt i prosjektet. Derpå fortsettes det med tekniske løsningsbeskrivelser som vil ta for seg viktige punkter og innhold som er relevant og tilknyttet de ulike funksjonalitetene som Azure Active Directory, Azure Log Analytics og Azure Security Center som skal videre utforskes på i Azure. Det følges også med et nettverkstopologi-diagram som viser et nettverksoppsett for prosjektet. Til slutt avsluttes det med å si noe om hvorfor man akkurat har valgt denne teknologi løsningen for prosjektet og kildene som har blitt brukt for dette dokumentet.

1.3 Referanser

Referanser fra andre rapporter som er tatt med i systemkravrapporten er forstudierapporten som er utarbeidet i tidligere fase i dette bachelorprosjektet.

2. Prosjektets omfang

2.1 Kort om kunden og deres behov

Den norske bank (DNB) er det største finanskonsernet i Norge og har sitt hovedkvarter i Oslo. DNB er som flere andre bedrifter på dagens marked i gang med å migrere sine fysiske maskiner til skyløsninger. I den sammenhengen så blir sikkerhet og hvordan man håndterer sikkerheten i slike skyløsninger et godt tema. I den anledning har DNB i samarbeid med NTNU gitt ut en oppgave om "Sikkerhet i Azure". Videre spesifikt så skal man i bachelorprosjektet jobbe ut ifra problemstillingen "Hvilke muligheter finnes det for trussel deteksjon i Azure ved bruk av tjenester som Azure Active Directory, Azure Log Analytics og Azure Security Center.

2.2 Definisjoner og forkortelser

Active Directory - Active Directory (AD) er en katalogtjeneste som tilbys av Microsoft.

Azure Active Directory (Azure AD) - Azure Active Directory tilhører cloud og er en skybasert tilgang og identitet tjeneste.

Azure Log Analytics - Med Azure Log Analytics har man mulighet til å analysere innsamlede data fra Azure Monitor.

Azure Security Center - Azure Security Center er en sikkerhetstjeneste senter som inneholder flere ulike tjenester som er med på å avdekke og forebygge trusler i Azure.

Exploit - definisjonen av Exploit innenfor dataverden, er at en programvare, kode eller kommandoer utnytter en sårbarhet eller Bug til å utføre ulovlige aktiviteter på en datamaskin eller en nettside.

Orkestrering - definisjonen av orkestrering innenfor dataverden er at det foregår en automatisert konfigurasjon, koordinering og administrasjon av datasystemer eller også programvare.

Payload - I cyberangrep sammenheng kan man definere Payload som en komponent i angrepet som fører til at det forårsaker skade til offeret som blir angrepet.

SaaS - Software as a Service

IaaS - Infrastructure as a Service

PaaS – Platform as a Service

On-Prem - On-Premises

2.3 Avgrensning av prosjektet

Prosjektet skal i hovedsak ta for seg hvilke muligheter det finnes for trussel deteksjon i Azure sine tjenester som i denne sammenheng vil inkludere Azure Active Directory, Azure Log Analytics og Azure Security Center. Det vil bli viktige å avgrense prosjektet siden Azure har flere ulike funksjonaliteter og tjenester i clouden, men man skal ikke ta for seg alle disse funksjonene. Man skal ta med det som er konkret for problemstillingen og fokusere på de aktuelle tjenestene for prosjektet. Det er også fornuftig å ta med annen viktig informasjon som er essensielt for å forstå de ulike sentrale tjenestene som man fokuserer på i oppgaven. Det vil også bli viktig å ikke ha for mye fokus på andre skyløsninger og å ha hovedfokuset på Azure gjennom hele oppgaven blir sentralt. Dette vil si at man ikke skal sammenligne f.eks andre cloud tjenester mot Azure i prosjektet.

3. Begrunnelse for valg av løsning

En god begrunnelse for at jeg har valgt å løse prosjektet med valg av akkurat disse tjenestene er at tjenester som Azure Security Center, Azure Log Analytics og Azure Active Directory er et sentralt utgangspunkt man kan jobbe ut ifra når man tenker på temaet "Sikkerhet" på Azure plattformen. Microsoft har greid å utvikle et veldig moderne Workspace i Azure, som også er rustet for større angrep som utføres i fremtiden. Enkelte av funksjonalitetene i Azure Portal er fortsatt under preview noe som viser at Microsoft stadig er fokuserte på forbedring av sine tjenester som ligger i Azure. Azure Security Center har massevis av funksjoner man må sette seg inn i, flere og flere av tjenestene Microsoft utvikler gir en god tilknytning og samhandling til hverandre noe som også er noe av grunnen til valg av de nevnte tjenestene. Microsoft har klart å utvikle en oversiktlig og strukturert form for analyser, sikkerhetsvarsler og deteksjon som får meg som forbruker et ønske om å sette meg inn og lære grundig om enhver løsning. Dette vil ikke kun være lærerikt for meg, men dette er informasjon og kunnskap jeg får tatt

med meg videre i arbeidslivet og satt i bruk på arbeidsplassen også. Ikke minst tenker jeg på å studere videre med en master i informasjonssikkerhet, dermed vil slike funksjonaliteter også hjelpe meg med å forstå og få et helhetsbilde av hva man jobber med innen IT sikkerhet og hvilke områder som er mest utsatt, og hvilke utfordringer cloud tar for seg i dag. Å forstå hvilke utfordringer cloud tar for seg i dag i 2019 er en sentral del man bør ha i bakhode før man jobber med sikkerheten i cloud.

4. Teori

4.1 Cloud Computing

Cloud Computing er skyløsninger som leverer data tjenester som servere, lagringskapasitet, databaser, nettverk, programvare, analyser, intelligens og flere andre tjenester over internett. Det samme som at de tjenestene som leveres blir gjort over internett kan også defineres til å bli levert over «the cloud». Det finnes 3 ulike modeller innenfor cloud computing:

4.1.1 Public Cloud

Når det kommer til Public Cloud blir dette eid og administrert av tredjeparts cloud service parter. Et typisk eksempel innenfor denne kategorien er Microsoft Azure. I et slik tilfelle, blir all hardware, programvare og annen tilhørende infrastruktur eid og administrert av den som tilbyr cloud tjenesten, nemlig Microsoft Azure i dette tilfelle hvis vi tar for oss den cloud tjenesten.

4.1.2 Private Cloud

I dette tilfelle er en Private Cloud, Cloud computing tjenester som blir brukt av en organisasjon eller også en fungerende business. Private Clouden befinner seg ofte på bedriftens lokasjon, eller så pleier også bedrifter å betale tredjeparts leverandører for bruk av cloud tjenester som f.eks Azure eller AWS. I det tilfelle med Private Cloud blir dens tjenester

og infrastruktur administrert over på et privat nettverk.

4.1.3 Hybrid Cloud

Når det kommer til Hybrid Cloud, er dette en Cloud type som kombinerer både Public Cloud og Private Cloud. Dette vil igjen si at man har mulighet til å dele data og programvare mellom både Public Cloud og Private Cloud. Fordelen ved bruk av Hybrid Cloud type er at man får større fleksibilitet og det åpner også for større muligheter.

Det finnes 4 cloud computing service modeller:

4.1.4 Infrastructure as a service (IaaS)

Med bruk av IaaS så er det vanlig at man leier IT infrastruktur som igjen vil innebære tilgang til servere, virtuelle maskiner, lagring, nettverk og operativsystemer. Disse blir igjen betalt på en Subscription, f.eks i Azure er det typisk å ta i bruk pay-as-you-go Subscription for betaling av det du bruker i Azure. IaaS tilbyr tilgang til fysiske maskiner, virtuelle maskiner, virtuell lagringskapasitet.

4.1.5 Platform as a service (PaaS)

PaaS blir typisk tatt i bruk for utvikling, testing, levering og administrasjon av programvare. Så her i dette tilfelle vil det si at det blir tilbudt et miljø for å utføre de nevnte tjenestene ovenfor.

4.1.6 Serverless computing

Innenfor dette område er hovedfokuset å ikke bruke mye tid på administrasjon av servere og infrastruktur når man skal utvikle app/programvare funksjonalitet. Når det kommer til Serverless computing er målet å la deg utvikle og kjøre applikasjoner, tjenester uten at man bryr seg/tenker på serverne.

4.1.7 Software as a service (SaaS)

Innenfor dette område handler det om levering av applikasjoner over internett. Her blir da programvare distribuert på en host tjeneste og den blir videre tilgjengelig via Internet for sluttbrukerne.

4.1.8 Trusler og sikkerhet i skyen

Ut ifra [Microsoft Security Intelligence report](#) kan vi se at de angrepene som kommer til Azure sine tjenester kommer fra IP adresser som stammer fra Kina med en utbredelse på 35.1 %, USA med en utbredelse på 32.5 % og Korea med en utbredelse på 3.1 %. Disse angrepene ble målt det første kvartalet i året 2017.

4.1.8.1 Cloud Weaponization

Hvis vi ser på det generelle trusselbildet som ligger i skyen kan vi si at en av truslene er følgende. En angriper tar kontroll over en eller flere virtuelle maskiner som ligger i skyen. Når angriperen har fått kontrollen og maskinene er kompromittert kan angriperen igjen kjøre nye angrep mot enten andre skytjenester, skyleverandører eller også maskiner som ligger på on-premises. Dette kalles for Cloud Weaponization. Her kan man blant annet inkludere Brute-force angrep og phishing angrep. Når angriperen først er inne og har kontroll over en eller flere virtuelle maskiner, blir det enkelt for han/hun å utføre port skanning og se etter flere åpne hull som kan utnyttes for ulovlig aktivitet.

Når en angriper har først kontroll på en virtuell maskin og er inne på den virtuelle maskinen i skyen blir det lettere tilgjengelig for angriperen å utføre videre utforskning av miljøet som angriperen er allerede er inne på. Dette vil blant annet innebære at angriperen kan stjele informasjon, utnytte tilgangen til on-premises ressursene, angripe andre, ta i bruk den aktuelle virtuelle maskinen til å utføre større angrep som f.eks å bli med i et større botnet eller også misbruke informasjon angriper finner på systemet. Dette er kun noen av flere aktiviteter en angriper kan utføre når han/hun er inne i systemet.

4.1.8.2 Feilkonfigurasjon

En annen trussel kan være det å ha utført noe feil under en konfigurasjon eller også under DevOps. Dette kan kategoriseres innenfor menneskelig feil som oppstår. Deling av Public key i public cloud er en av truslene som kan inkluderes i dette område.

4.1.8.3 Usikre API

Usikre Application Programming Interface (API) er også noe som forekommer frekvent som en sky trussel i det siste. API blir misbrukt gjennom å utnytte sårbarheter som ligger i deres grensesnitt. Gjennom disse "hullene" i grensesnittet kan potensielle angripere utføre angrep og ta kontroll over applikasjonene som ligger i skyen. Det er viktig at API er sikret siden, de fungerer som en offentlig dør inn til selve applikasjonen. Når vi sier en offentlig dør inn til applikasjonen, kan vi også videre relatere dette til at man kommer seg inn i skyen gjennom denne applikasjonen. Et meget godt eksempel på usikker API som har blitt misbrukt er [hendelsen som skjedde hos Moonpig](#). I Moonpig eksemplet har det blitt funnet ut at APIen til Android Applikasjonen til Moonpig har tatt i bruk statiske legitimasjonsopplysninger som er uavhengig av kundekontoer. Forskjellen på de forskjellige brukerne og innkommende forespørsler var kun en kunde ID.

4.2 Microsoft Azure

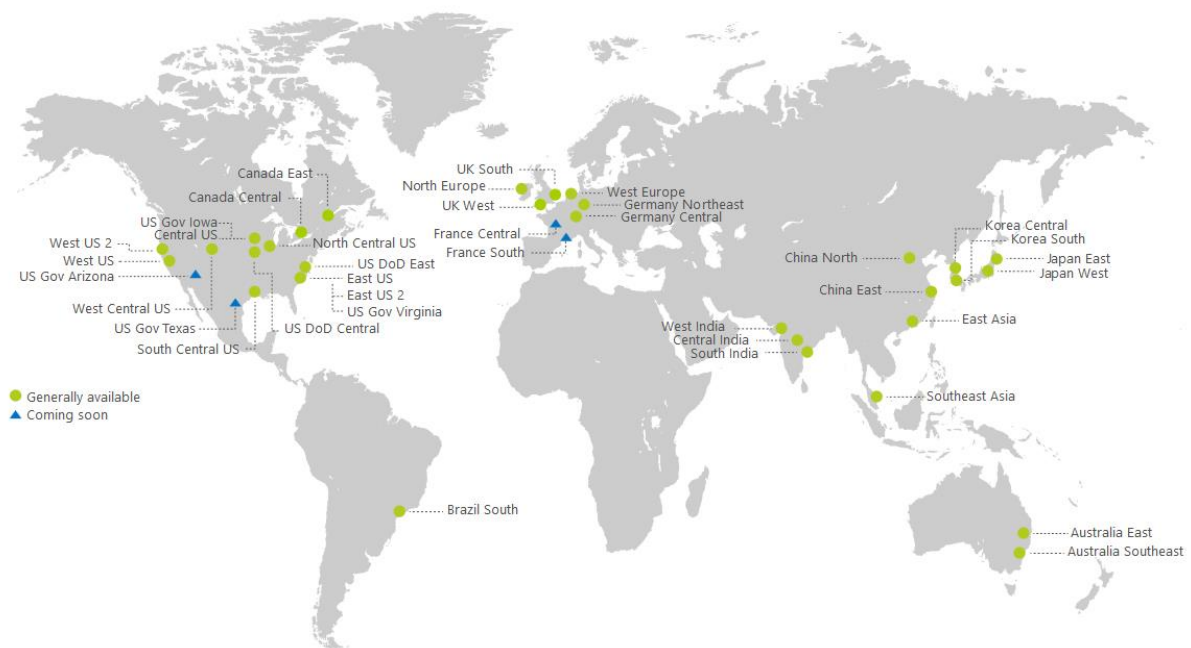
Microsoft Azure er en privat og offentlig skyplattform. Azure tar i bruk teknologi som tar for seg virtualisering. I Azure har vi mulighet til å bygge, distribuere og administrere både applikasjoner og tjenester. Dette fungerer gjennom et globalt nettverk med utplassering av ulike datasentre på flere ulike lokasjoner spredt rundt i verden. Azure tilbyr også tjenester innenfor On-Premises, Infrastructure as a Service (IAAS), Software as a Service (SAAS), Platform as a Service (PAAS). I tillegg til dette tilbyr Azure støtte for flere ulike programmeringsspråk, rammeverk og verktøy. Azure tilbyr også støtte både for Microsoft baserte systemer og programvare, og tredjeparts leverandører sine systemer og programvare. I Azure får man både kjørt Windows baserte og Linux baserte maskiner.

4.2.1 Hvordan fungerer Azure

Vi kan hovedsakelig definere skyen som et sett med fysiske servere i enten en eller flere datasentre. Disse kjører virtualisert maskinvare på vegne av deres kunder som har behov for dette. I hvert av datasentrene som tilhører Microsoft har man en samling av servere som befinner seg i en egen server rack. Server Racken inneholder mange Server Blades. I tillegg til dette har den en Network Switch, som gir nettverkstilkobling. Server Rack har også en power supply som gir strøm. I slike tilfeller blir også server racken gruppert i større enheter som også blir kalt for cluster. Innenfor disse så er det slik at de fleste serverne er utviklet for å kunne kjøre disse virtuelle maskinvarene på vegne av sin bruker. Men, her er det også noen av serverne som kjører programvare som inneholder sky administrasjon, denne blir også kjent som Fabric Controller. Fabric Controller har mange ansvarsområder og tildeler blant annet tjenester som skal overvåke Server Health og de ulike tjenestene som blir kjørt på server. Ikke minst når serverne feiler eller får en feilmelding har Fabric Controller ansvar for å ordne opp i den aktuelle feilen.

Azure er et større sett med servere og maskinvare innenfor et nettverk. I tillegg har Azure distribuerte applikasjoner som er ansvarlig for driften av delen som orkestrerer den virtualiserte maskinvaren og programvare på de ulike serverne. Det som menes med orkestrering i denne sammenheng er at det foregår en automatisert konfigurering, koordinering og administrasjon av både datasystemer og programvare i server racken. Hvorfor er Azure egentlig så kraftig? Det er nemlig orkestreringen som nevnt tidligere som gjør at Azure er så kraftig slik at brukere ikke trenger å tenke på drift, oppgradering og oppdatering av maskinvare. Alt dette blir utført av Azure i bakgrunnen, slik at brukerne ikke får sett hvordan dette fungerer direkte på systemene sine.

Azure har datasentre som befinner seg over hele verden. Disse datasentrene blir kombinert utplassert i ulike regioner. I disse regionene har Microsoft flere ulike datasentre som er plassert omkring slik at dersom man opplever at noe data går tapt så har man en effektiv fungerende backup løsning for gjenopprettelse som vil være tilgjengelig for brukeren. Nå i 2019 finnes det 38 regioner hvor vi har Microsoft sine ulike datasentre.



Figur 5

Bildet ovenfor viser en oversikt over hvor Microsoft sine ulike datasentrene befinner seg. Som vi ser har Microsoft et globalt nettverk med datasentre for bruk til Azure.

Kilde: Microsoft Global Datacenters [Digital Image]. (n.d.). Hentet 24. Februar 2019, fra <https://www.znetlive.com/images/microsoft-global-datacenters.jpg>

4.3 Shared Responsibility Model

En av de viktigste områdene man bør sette seg inn i og forstå når man tenker på sikkerhet, er Shared Responsibility modellen. Azure blir administrert og kjørt under denne Shared Responsibility modellen. Det er viktig å forstå at når man tar i bruk Azure, at Azure har ansvar for sikkerheten rundt infrastrukturen sin og plattform sikkerheten. Men dette betyr ikke at brukeren/kundene ikke har noen ansvarsområder, de må blant annet selv ta ansvar og initiativ til å sikre miljøet i Azure. I tillegg til dette har brukerne også ansvar for å ikke dele data rundt til ukjente eller andre personer som ikke skal ha tilgang til aktuell data. Det blir like viktig for brukerne av Azure å identifisere de brukerne som prøver å misbruke tjenester i

Azure og ikke minst legge inn gode policyer som passer inn etter deres behov i Azure. Share Responsibility Model er en modell som brukes for å bestemme hvilke roller for både de som tilbyr cloud tjenesten og forbrukerne av cloud har innenfor cloud sikkerhet. Det vil dermed bli veldig sentralt og viktig at de som tilbyr cloud tjenesten i dette tilfelle Azure og forbrukerne av Azure samarbeider om å møte sikkerhetskravene.

Shared Responsibility Model tar for seg hvilke parter som har ansvar for hvilke områder og er hovedsakelig knyttet til sikkerhetsområdet. Hver av disse områdene er knyttet til hver av tjenestene Azure tilbyr On-premises, IaaS, PaaS og SaaS. Det blir like viktig å holde seg oppdatert på de seneste sårbarhetene som finnes på markedet ved å ta i bruk forskjellige nettsider som f.eks National Vulnerability Database(<https://nvd.nist.gov>) og SecurityFocus(<https://securityfocus.com>). Uansett hvilken type deployment som er satt og foregår har du som forbruker ansvaret for områdene Data, Endpoint, User og Access management. Det er like viktig å forstå at cloud er et delt ansvarsområde for alle parter.

Under er det vedlagt en figur som forteller hvordan Share Responsibility Modellen fungerer på tvers av de ulike cloud tjeneste modellene.

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Shared
Identity & access management	Cloud Customer	Cloud Customer	Shared	Shared
Application level controls	Cloud Customer	Cloud Customer	Shared	Cloud Provider
Network controls	Cloud Customer	Shared	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Shared	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend: Cloud Customer (Blue), Cloud Provider (Grey)

Figur 6

Kilde: *What Does Shared Responsibility in the Cloud Mean [Digital Bilde]*. (n.d.). Hentet 11 mars 2019, fra <https://msdnshared.blob.core.windows.net/media/2016/04/image745.png>

4.4 Detection & Security Monitoring

Når vi snakker om deteksjon innenfor cyber security verden er det viktig å ha gode rutiner og verktøy for deteksjon av trusler. Dette må foregå på en effektiv, rask og troverdig måte som igjen kan føre til man får eliminert den aktuelle trusselen eller trusselene. Dette er viktig både i mindre og større bedrifter. Et godt samarbeid mellom ulike kilder fra deteksjon vil føre til at man får et bredere bilde av trusselen som foreligger. Forståelse for The Cyber Kill Chain modellen vil gjøre at du får et helhetlig bilde og detaljert forståelse av hvordan angrepet tar

sted. Dette kan du igjen ta til din nytte for videre planlegging av hvordan du kan eliminere angrepet allerede i tidlig fase før det har mulighet til å spre seg i bredere tilstand. For å utføre slik trussel deteksjonen har vi flere ulike metodikk som kan brukes som blant annet:

- Threat Intelligence
- User Analyze og Behavioral Analytics of an Attacker.
- Security Event Threat Detection
- Anomaly Detection
- Network Threat Detection
- Endpoint Threat Detection
- Logg Analyser

4.5 The Cyber Kill Chain

The Cyber Kill Chain er en trussel modell. Denne modellen er utviklet med tanke på IT sikkerhetspersonell og forskere. Bakgrunnen for dette er at de skal få organisert tankene og få et bilde rundt både deteksjon og trussel respons ut ifra modellens prinsipper. Det vil bli viktig å forstå hvordan Cyber Kill Chain prosessen foregår før man tar for seg den videre prosessen av hvordan Security Center jobber med å gjenkjenne angrep og trusler mot Azure. The Cyber Kill Chain deles inn i følgende faser:

Tabell 4

Fasene i Cyber Kill Chain	Hva som blir utført i de ulike fasene
1. Rekognosering (Reconnaissance)	Identifikasjon av ofre fra angrippers side
2. Våpenisering (Weaponization)	Filer er samlet som våpen mot et målrettet system. Deretter blir dette brukt for installasjon av ondsinnet kode/programvare.
3. Leveranse (Delivery)	Plassering av skadevare fra våpenisering

	delen.
4. Utnyttelse (Exploitation)	Den ondsinnede programvaren blir kjørt på offerets system.
5. Installasjon (Installation)	En bakdør bli installert på maskinen til offeret.
6. Kommandere og kontroll (Command and Control(C&C))	I denne fasen kommuniserer den ondsinnede programvaren med C&C systemet. Dette vil igjen føre til at angriper kan hente ut sitt mål fra offerets maskin.
7. Tiltak på mål (Actions on objectives)	I denne fasen henter angriperen ut informasjon og filer etter sitt ønske fra offerets maskin. Dette ønske kan være basert på mål angriperen har som spesifikke filer og informasjon. Det kan også være basert på det en angriper ser på offerets maskin.

Cyber Kill Chain skal gi deg som sikkerhetspersonell en indikasjon på at noe er på gang, men det blir opptil deg selv å finne ut og sette ulike punkter fra Kill Chain i sammenheng for å finne ut om det foreligger en aktuell trussel mot Azure eller ikke. Det er ofte slik at, dersom det skal foregå sikkerhetstester og penetrasjonstesting på Azure plattformen, blir dette ofte informert på forhånd til personale slik at man da på forhånd vet at det i slike tilfeller ikke foreligger en reel trussel.

5. Use-cases

5.1 Beskrivelse av Use-cases

Case 1: Deteksjon av Spam aktivitet

I et slikt tilfelle som dette kan vi ta for oss en angriper som har tatt over en virtuell maskin i Azure. Denne virtuelle maskinen blir brukt til utsending av spam e-poster. Security Center tar i bruk maskinlæring som nevnt tidligere. Dermed kan de basert på data fra maskinlæring oppdage mistenkeligheter i Simple Mail Transfer Protokoll (SMTP) trafikken. Deretter blir det kjørt spørringer opp mot andre dataressurser og kilder for å dobbeltsjekke om dette er en kilde som kan knyttes til mistenkelig aktivitet. Helt til slutt blir denne dataen korrelert i samarbeid med Office 365 sin spam database.

Et resultat av denne korrelasjonen skal bestemme om denne trafikken skal slippes gjennom SMTP protokollen eller ikke. Dersom det i tilfelle registreres at trafikken er mistenkelig får Security Center satt i gang et varsel som tilsier at det er oppdaget mistenkelig aktivitet fra den aktuelle virtuelle maskinen. I dette caset bruker Security Center maskinlæring, trussel intelligens og innebygde analyser fra Office 365. Basert på denne dataen fra 3 ulike parter har man en god forståelse og et godt grunnlag for tillit og et godt grunnlag for å jobbe ut ifra aktuelle varsler som fremkommer.

Case 2: Krasj Dump Analyser

I dette caset kan vi ta for oss en angriper som har kompromittert en virtuell maskin i Azure. Angriperen installerer Malware på denne virtuelle maskinen. Denne blir ikke gjenkjent av antiviruset som er satt opp på den aktuelle virtuelle maskinen. Denne Malware som er blitt installert fører til krasj i et program som er legitim på det virtuelle miljøet i Azure. Når en slik krasj oppstår er det vanlig at Windows Error Reporting (WER) genererer en brukermodus minne krasj fil. Dette er en filtype av ".dmp". Denne er lokalisert under følgende sti: *%LOCALAPPDATA%\CrashDumps*. Det Security Center i dette tilfelle gjør er at, det blir samlet en kopi av en slik dump fil. Etter dette skanner Security Center denne filen for kompromittering og exploits.

Dersom det forekommer spor av kompromittering og exploits vil Security Center trigge et varsel. Dette varslet vil gå ut på at denne krasj dump filen har blitt analysert til å oppdage kjørbare kode som blir mistenkeliggjort med bakgrunn av atferden filen utgjør. Denne atferden viser seg vanligvis å bli utført av skadelige Payload. Slik data blir igjen sjekket opp mot eksisterende intelligens informasjon før man får slike sikkerhetsvarsler.

Ulike varsler som kan forekomme i Security Center på bakgrunn av krasj dump analyse kan være følgende:

Kode Injeksjon som er oppdaget:

Dette feltet handler om kode injeksjon som tar for seg innsetting av kjørbare moduler. Dette kan foregå både i prosesser eller også i tråder. Denne prosessen er ofte tatt i bruk av Malware for å få tilgang til data. Den blir også brukt for å enten gjemme den ondsinnede programvaren eller også for å forhindre at man får fjernet den ondsinnede programvaren. Denne type sikkerhetsvarsel indikerer at det finnes en modul som allerede er injisert i krasj dumpen. En slik modul blir sjekket av Security Center for å sjekke om den har en mistenkelig atferd eller ikke. Basert på dette kan man vite om det er tegn på noe mistenkelig aktivitet som er på gang eller ikke. Etter å ha fått resultat fra Security Center blir dette indikert av SIGNATURE feltet i selve varslet.

Case 3: Brute-force angrep

Brute-force angrep er en metode som hovedsakelig tar for seg angripere som kontinuerlig prøver ut flere kombinasjoner av brukernavn og passord til de får det til å stemme. Det er slik at et menneske ikke greier å komme opp med millioner av forslag med brukernavn og passord helt til man får en riktig kombinasjon. Dermed tas det i bruk verktøy som gjør dette for de aktuelle angriperne. Dette verktøyet vil gjette de korrekte innloggingsdetaljene og når det er suksessfullt får man en beskjed om at innloggingen er suksessfull. Ved bruk av maskinlæring blir det opprettet en baselinje med historikk som har pågått over en tidsperiode som inneholder fjern tilkoblinger (RDP). Ved hjelp av dette har man også mulighet til å gjenkjenne Brute-force angrep mot Secure Shell (SSH), Remote Desktop Protocol (RDP) og SQL porter.

Forutsetning for å utføre følgende Use Case, er at Windows Firewall og Windows Defender Security er slått av på den aktuelle virtuelle maskinen test angrepet foregår på.

6. Azure

6.1 Tjenester i Azure

6.1.1 Azure Active Directory

Azure Active Directory Domain Services er en tjeneste i Azure som tilbyr domene tjenester som tilknytning av domener, Group policy, LDAP, Kerberos/NTLM. Disse tjenestene er fullt kompatibel med Windows Server sin Active Directory tjeneste. En veldig nyttig funksjon som har kommet frem i Azure Active Directory Domain Services er at man har mulighet til å tilknytte domene som er på on-premises maskin med Azure Active Directory. I dette prosjektet blir det tatt i bruk Active Directory Premium P2 som har funksjoner som Identity Protection, Privileged Identity Management og Access Reviews.

6.1.1.1 Azure Active Directory Connect

Synkronisering av identiteter fra Azure Active Directory til on-premises maskiner og virtuelle maskiner er en funksjonalitet man kan oppnå ved bruk av Azure Active Directory Connect. En annen mulighet AD Connect tilbyr er at man får installert hele Identity Bridge, med dette menes at man får installert Active Directory Federations Services (AD FS). AD FS tilbyr brukerne muligheter som single sign-on tilgang til systemer og programvare som befinner seg utenfor organisasjonens lokasjon.

6.1.1.2 Azure Identity Protection

Azure Identity Protection er en av mange funksjoner som finnes i Azure. Azure Identity Protection er med på å hjelpe oss å gjenkjenne og forhindre ulike identitetsangrep. I Azure Active Directory Identity Protection har man mulighet til å overvåke mistenkelige hendelser og sette i gang tiltak for å bli kvitt disse. Azure Active Directory tar i bruk moderne teknologi som maskinlæring algoritmer for gjenkjenning av mistenkelig aktivitet. Maskinlæring blir brukt direkte opp mot identiteter, når en bruker logger seg inn mot Azure så blir punkter som IP-adresse, lokasjon, user agent, Login patterns i det siste tidspunktet gjenkjent. Basert på dette kan man avgjøre om det er en god eller ond bruker som vil logge seg inn i systemet. Basert på denne dataen så kan Identity Protection opprette rapporter og varsler som vil gi deg informasjon som kan brukes til evaluering av den mistenkelige aktiviteten slik at du igjen kan sette i gang nødvendige tiltak for den aktuelle trusselen som er gjenkjent.

6.1.1.3 Azure AD Privileged Identity Management

Ved bruk av Azure AD Privileged Identity Management (PID) får man mulighet til å administrere, kontrollere og overvåke Privileged Identities. Ved bruk av PID får man tilgang til kataloginformasjon som befinner seg i Azure og andre ressurser i portalen. En av hovedårsakene til å ta i bruk Privileged Identity Management er å begrense angrep overflaten. Ikke minst er målet med PID å få satt i gang bruk av tjenesten Just-In-Time. Ved bruk av Azure Active Directory Privileged Identity Management har man mulighet til å redusere, unngå sikkerhetsbrudd og risiko knyttet til Azure. Ved bruk av tjenesten har man mulighet til å sette en start og slutt dato på ressursene som befinner seg i Azure. Dette krever at man får tilgang til å aktivere Privileged roles. Dersom man har tenkt å ta i bruk Azure AD Privileged Identity Management trenger man å ha Azure AD Premium P2 lisens.

6.1.1.4 Azure Advanced Threat Protection

Azure Advanced Threat Protection er en tjeneste som brukes hovedsakelig til å gjenkjenne kompromitterte identiteter, avansert angrepsmetodikk og ikke minst interne trusler som kommer frem. Gjennom bruk av Azure ATP sin attack timeline får man frem viktig

informasjon. Det er veldig enkelt å jobbe med Azure ATP i og med at det kun er en sensor som skal lastes ned, denne har som oppgave å overvåke lokal trafikk. Denne skal installeres på din egen Domain Controller. Azure ATP tar i bruk sikkerhetsrapporter og analyser.

Gjennom disse prøver Azure ATP å få til en reduksjon av kompromitterte brukerkontoer og stoppe avanserte angrep mot Azure.

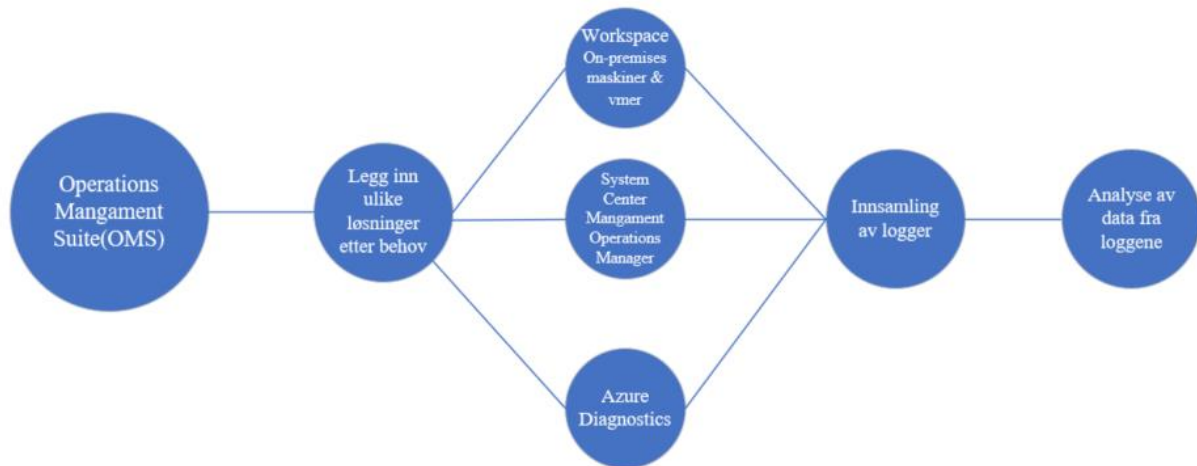
6.1.2 Azure Log Analytics

Azure Log Analytics er en tjeneste som tilbyr kolleksjon av loggdata som kommer fra Azure Monitor. Disse logg dataene blir lagret i Log Analytics Workspace. Log Analytics tilbyr sentralisert behandling av logger. En annen ting Log Analytics er god på er generering av både innsikt og varsler av de ulike loggene som forekommer i Log Analytics Workspace. Blant disse loggene snakker vi da om aktivitetslogger, event logger, diagnostikk logger, applikasjonslogger og egne tilpassede logger. Ved bruk av slike logger kan man generere en innsikt i hva disse loggene innebærer og dersom det er behov for tiltak er dette også tilgjengelig for utføring. En av fordelene ved å ta i bruk Azure Log Analytics er at man får alle detaljer og informasjon samlet i et sted både for dine virtuelle maskiner og on-premises maskiner. Her blir også Amazons AWS Open Stack løsninger inkludert. Azure Log Analytics bruker et spørrespråk kalt The Kusto Query Language (KQL) for innsamling og utforsking av logger. Azure Log Analytics har byttet navnet til Azure Monitor Logs.

Azure Log Analytics kan bli distribuert i tre modeller som er følgende:

- Agenter som er direkte installert på maskinen.
I dette tilfelle kan man nedlaste OMS agenten på klientmaskinen. OMS står for Operations Management Suite. Videre opplastes logger til ditt OMS Workspace.
- OMS Gateway
I dette tilfelle blir det satt opp en gateway som har i oppgave å opptre som en Proxy. Her har gateway ansvaret for å samle inn logger fra agentene. Videre skal de sendes til Azure Log Analytics.
- Integrasjon av OMS med System Center Operations Manager (SCOM)
I dette tilfelle har du mulighet til å tilkoble agenten med SCOM. Da vil SCOM opptre som en slags OMS gateway og vil videresende logger til Azure Log Analytics.

Bildet under viser hvordan Log Analytics fungerer og hvilke muligheter man har i Log Analytics.



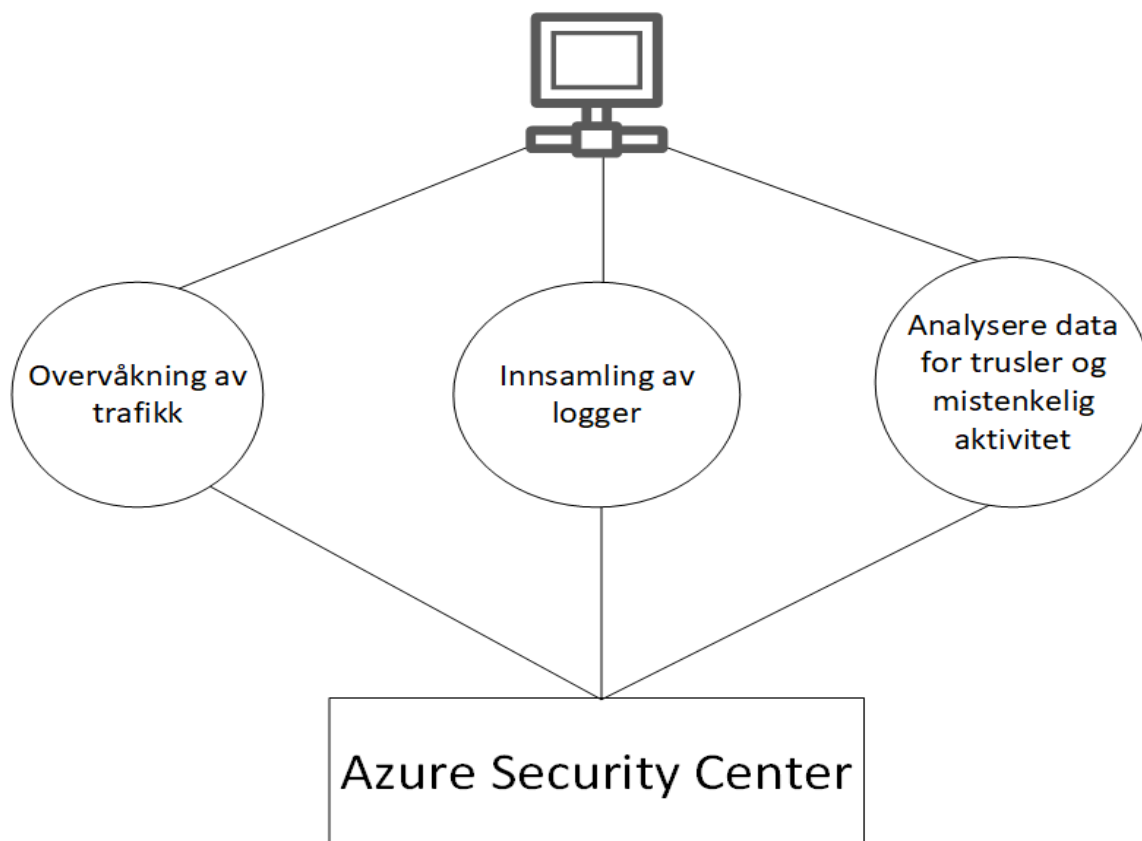
Figur 7

6.1.3 Azure Security Center

Azure Security Center er en skybasert tjeneste på Azure plattformen. Azure Security Center tilbyr tjenester som Intrusion detection og Intrusion prevention for den virtuelle infrastrukturen som er oppbygd i Azure. Informasjonen som er tatt i bruk i Azure Security Center er hentet fra Microsoft sine ledende samarbeidspartnere som Microsoft Digital Crimes Unit, Microsoft Security Response Center og andre parter som er i samarbeid med Microsoft. Dersom du er registrert som en Azure kunde, får du tatt i bruk Azure Security Center helt gratis. Hvis du tar i bruk Azure som trial har du fortsatt tilgang på Security Center. Azure Security Center er innebygd i Azure Portal.

Security Center samler inn informasjon i forbindelse med nettverksdata og feeds. Dette kommer fra de tilknyttede partnerne hos Microsoft. Basert på denne informasjonen bruker Microsoft å oppdage trusler og andre mistenkelige aktiviteter på Azure plattformen. Security

Center analyserer informasjonen som kommer fra de tilknyttede partnere ved å korrelere data fra kildene til å identifisere trusler og mistenkelige aktivitet som foregår på Azure. Med korrelering i denne sammenheng vil man si at driver en samvariasjon mellom to mål. I Azure Security Center blir det samlet inn data fra flere ulike datakilder. Her inkluderer man Endpoint logger, nettverkstrafikk, cloud aktivitet. Deretter basert på dette blir det satt i gang maskinlæring og atferd baserte logikk metodikk til å gjenkjenne trusler og mistenkelig aktivitet. I tillegg til dette har vi mulighet til å utvikle egne tilpassede varsler med et sterkt og effektivt søkespråk som The Kusto Query Language. Azure Security Center tilbyr sikkerhetsanbefalinger som bør iverksettes. Eksempel på sikkerhetsanbefalinger Security Center tilbyr kan være nettverksbeskyttelse, Endpoint Protection, kryptering av data, disk, Access control lists, hvitlisting av innkommende forespørsler som virker truende og blokkering av forespørsler som er uautoriserte.



Figur 8

Figuren ovenfor viser 3 steg for trussel deteksjon i Azure Security Center. Etter å ha vært gjennom de 3 steg blir resultatet fremstilt på dashbordet i Azure Security Center.

Når man tar i bruk Security Center for første gang og aktiverer dette blir en overvåkingsagent automatisk distribuert og installert til de virtuelle maskinene dine i Azure. Dersom man vil tilkoble sine on-premises maskiner til Azure Security Center gjøres dette manuelt. Security Center begynner deretter å gjøre en helhetsvurdering av den aktuelle sikkerhetsstatusen på maskinene, nettverket, applikasjonene og data som er knyttet til Security Center. Deretter begynner Azure sin analytics engine å analysere dataene som er kommet inn i Security Center. Videre går disse dataene gjennom maskinlæring. Basert på dette kommer Security Center med anbefalinger og vurderinger tilknyttet sikkerhetsvarsler og trusselnivået i miljøet på Azure. En god og smart fordel ved bruk av Azure Security Center er at man med en gang får varsel dersom noe ondsinnet/anomali er på vei eller også angrep som har utprøvd seg i miljøet eller angrepet som har foregått suksessfullt.

For å få flere avanserte muligheter i Security Center må det legges inn Standard Tier Subscription i Azure. Standard Tier er en versjon som tilbyr brukerne avanserte funksjonaliteter i Azure Security Center. Standard Tier blir satt opp av DNB i Azure Portal. Funksjonalitet som følger med i Standard Tier versjonen er følgende:

- Threat Intelligence
- Built-in og custom alerts
- Adaptive Application Controller
- Just-in-time VM Access
- Security Event Collection og Advanced Search

6.1.3.1 Just In Time VM Access

Azure Security Center har også funksjoner som hjelper Azure å forebygge angrep. En av funksjonene her er Just in time VM Access. Ifølge [Microsoft](#) er det mest vanlige angrepet som er i bruk mot IAAS sine virtuelle maskiner RDP Brute Force angrep. Disse angriperne angriper vanligvis administrasjonporter. RDP og SSH porter er veldig vanlig blant disse angriperne. Ved bruk av Just in time VM Access kan man sette begrensninger på disse portene. Dermed har man mulighet til å utføre arbeidet som krever de portene åpen. Deretter kan portene bli satt opp til å bli stengt. Just In Time VM Access lar deg kontrollere hvem som kan få tilgang til portene på den virtuelle maskinen, når og for hvor lenge man får tilgang til

de ulike portene. Ved bruk av Just in time VM Access kan man sette en tidsbegrensning på bruk av portene. Dette gjør man under Security Center, deretter undergruppe Just In Time VM Access, også videre på Recommended fanen. Just in time VM Access er en nettverkskontroll mekanisme som er anbefalt å bruke i Azure. Just in time VM Access fungerer både på Linux og Windows plattformen. Dette er en nettverkskontroll mekanisme og dermed vil ikke nettverkslaget spille noen rolle for hvilken plattform man skal ta i bruk for å aktivere disse funksjonene.

Just In Time VM Access (JIT) fungerer slik som at en bruker sender en forespørsel for bruk av JIT tilgang. Da sjekker Azure Security Center dette opp mot deres tilgangsrettigheter som er knyttet opp mot Role-based Access control (RBAC). I dette tilfelle vil da brukeren få tilgang til JIT dersom brukeren har skrivetilgang til den virtuelle maskinen bruker ønsker å sette opp JIT på. Just In Time VM Access har tilgang til både de standard portene som kan brukes til å gi andre tilgang, og man kan også opprette nye porter og i tillegg fjerne ulike porter som også allerede befinner seg på systemet. En fordel med å ta i bruk JIT er at man kan også ordne konfigurasjonen av selve JIT policy gjennom bruk av Powershell.

6.1.3.2 Network Security Groups

Ved bruk av Network Security Groups (NSG) har man i Azure mulighet til å enten tillate eller blokkere tilgang basert på portene, hvor IP-adressene originalt stammer fra, og hvilken destinasjons IP man tilkobler seg mot. NSG vurderer både innkommende og utgående forespørsler fra Azure. Det er basert på disse vurderingene man enten tillater tilgang eller nekter tilgang mot Azure.

6.1.3.3 Security Alerts Map

Azure Security Center tilbyr brukerne et kart som har mulighet til å identifisere ulike sikkerhetstrusler. Security Center henter denne dataen basert på intel fra deres kilder internt i Microsoft. Her kan man blant annet f.eks gjenkjenne om din datamaskin er en del av et botnet. Det er mulighet til å få tilgang til informasjon som kan hente inn hvor de ulike truslene stammer fra i dette kartet. Eksempel på informasjon som man kan hente ut fra Security Alert

Map er trussel type, hvilket land trusselen kommer fra, trussel lokasjon som viser til eksakt lokasjon av hvor angrepet tar sted fra og trussel detaljer blir lagt fram på kartet.

6.1.3.4 Security Policy

Security Policy er policy regler som settes for å opprettholde et sikkerhetsbehov. Ulike sensitiv data vil kreve ulike policy regler, disse vil hjelpe til å opprettholde en god sikkerhet i en organisasjon eller også i en myndighet. Security Policy er innebygd i Azure Security Center. I den anledning er det mulighet til å konfigurere eller også endre ulike policyregler som er satt opp i Security Center. Gjennom bruk av Security Policy kan man definere ulike retningslinjer som er tilpasset behovet til organisasjonen. Basert på sikkerhetsvurderingene som gjøres i Azure Security Center får man en ide om hvilken type policyer som bør konfigureres og i hvilken sammenheng man bør ta i bruk de ulike policyene.

6.1.4 Azure Sentinel

Azure Sentinel er et Security Information and Event Management (SIEM) system. Azure Sentinel er også en Security Orchestration Automated Response (SOAR) løsning. Med Azure Sentinel har man mulighet til å få gode og effektive data fra sikkerhetsanalyser og threat Intelligence. Azure Sentinel tilbyr flere ulike gode muligheter som:

- Innsamling av data fra cloud basis som vil si at man har mulighet til å samle inn data fra alle brukere, enheter, infrastruktur, programvare som befinner seg både på ulike cloud løsninger som f.eks Azure, AWS, Google Cloud og on-premises maskiner.
- Man har mulighet til å oppdage trusler som ikke har blitt tidligere oppdaget. Man har i tillegg til dette muligheten til å ta i bruk Microsoft sine analyser til å redusere utfallet av de falske truslene som blir gjenkjent som positive.
- Noe som stadig blir populært i dagens samfunn i 2019 er kunstig intelligens. Ved bruk av kunstig intelligens har man mulighet til å etterforske trusler.
- Ved bruk av innebygd Orchestration og automatisering av oppgavene har man med Azure Sentinel mulighet til å respondere effektivt til trusler som er oppdaget og andre alvorlige hendelser.

Azure Sentinel har også en integrasjonsløsning som integrer Azure Sentinel med Azure Advanced Threat Protection. Dermed har du mulighet til å utføre analyser av brukeratferd. I tillegg har du muligheten til å utføre prioritert analyse av hvilke brukere som skal gå til etterforskning i ønsket rekkefølge. Dette kan igjen utføres basert på graden av varsel og hendelsesnivå. Her kan man også inkludere at det baserer seg også på patterns som kjøres gjennom Microsoft 365 og Azure Sentinel.

Ved bruk av Azure Sentinel har man også mulighet til å ta i bruk funksjonaliteten «Hunting». Dette er et veldig nyttig verktøy for dette bachelorprosjektet og tar for seg muligheten til å jakte på sikkerhetstrusler som går gjennom tilknyttede Data Sources i Azure. Alt dette vil foregå før et aktuelt sikkerhetsvarsel aktiveres. Denne funksjonaliteten er basert på [MITRE Framework](#).

6.1.5 Implementasjon av jump servere

For sikkerhets skyld er det alltid en god ide å ha fjernet Internett tilgang fra virtuelle maskiner slik at det virtuelle miljøet er mer sikker enn det det er dersom internet er tilkoblet. Når en virtuell maskin er tilkoblet til internett er det større farer for bakdører som blir installert og andre ondsinnede programmer som blir lastet ned på maskinen. I tillegg til dette er det en veldig god ide å ha fjernet tilgangen til Remote Desktop Protocol på de virtuelle maskinene. Når man tenker på å utføre dette her i praksis, er det veldig lite sannsynlighet for at man gjør disse tingene.

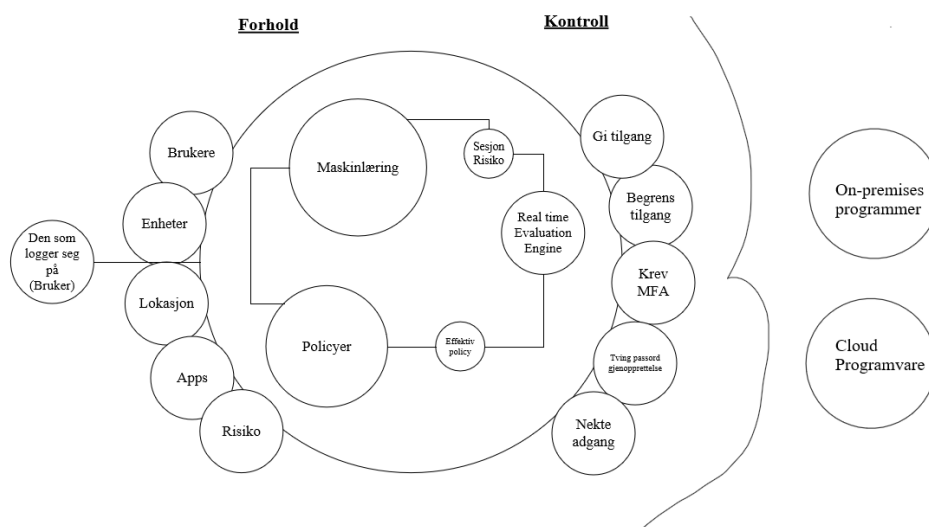
I den anledning er det heller bedre å implementere "jump servere". Disse serverne er installert og vedlikeholdt i den demilitariserte sonen (DMZ). Det som menes med DMZ er at man er et separert nettverk eller også subnet. Bakgrunnen for å ta i bruk disse jump serverne er at de kan bli brukt til å ta imot RDP tilkoblingene som kommer mot de virtuelle maskinene fra brukerne og videre assistere dem til å få logget seg inn. Dermed kan man fra denne jump serveren, få logget seg videre inn ved bruk av RDP til de ulike virtuelle maskinene fra brukerens side. Jump servere har et nettverk som har tilkobling til resterende verden og et nettverk som er koblet internt i organisasjonen. Denne type server har også alle de nødvendige

sikkerhetsrestriksjonene som trengs for en server. Videre tilbyr den sikker tilgang fra bruker side til andre servere.

6.2 Beskrivelse av hvordan tjenestene kan oppdage trusler

6.2.1 Hvordan beskyttes identitet i dag i Identity Protection

Microsoft tar i bruk en kombinasjon av Conditional Access og Identity Protection. Når en bruker logger inn så skal det settes regler rundt brukeren, enheten, lokasjonen den kommer fra og hvilke apper som er i bruk på deres vegne og hvilken risiko som er der med den aktuelle innloggingen. Deretter skal denne dataen bli kjørt gjennom maskinlæring, og videre gjennom en real time evaluation engine og de aktuelle policyene som allerede er satt for brukeren for å gjennomgå risikonivået. Dette skal videre føre deg til å ta konkrete valg basert på tilbakemeldingen du får fra øvrige parter. Under dette punktet kan du velge å sette valg som å gi tilgang, eller å begrense tilgang, du kan også kreve at det blir satt Multi Factor Authentication (MFA), eller kan du også kreve at passordet gjenopprettes. I verste tilfeller som du opplever kan du også nekte tilgang i Identity Protection. Dette kan gjøres både på skyplattform programvare og på on-premises programvare.



Figur 9

I Identity Protection har vi 2 risikotyper. Microsoft tar for seg hovedsakelig disse 2 risikotypene. **User risk** tar for seg sannsynligheten for at en ond aktør har kompromittert en gitt identitet. **Sign-in risk** tar for seg sannsynligheten for at en gitt innlogging ikke er autorisert av den egentlige eieren. Vi har også mulighet til å ta i bruk Security Policy her iblant risk policyen i Azure slik at man automatisk gir respons for mistenkelige trusler. Vi har to hovedtyper deteksjonsmetoder i Identity Protection:

- Real-Time

Real-Time vil kjøre samtidig som man logger inn. Denne deteksjonsmetoden vil hjelpe oss med å finne risiko i real-time sign-in metoden og er også med på kartlegging av risiko knyttet til brukerne i Azure Active Directory.

- Near Real-time

Den andre metoden er Near Real-time som vil kjøre med en gang man har innlogget seg med brukerne i AD, som også er med på å kartleggingen av bruker risikoen.

Med Identity Protection kan man sende varsler for ulike risiko hendelser som oppstår i Azure. Det er også ganske enkelt å utføre tilbakestilling av passord med Identity Protection. Man har blant annet mulighet til å sette opp policy for å blokkere mistenkelige innlogginger. Her har man også mulighet til å tilby MFA som er Multi Factor Authentication som vil si at du må ta i bruk to trinns verifikasjon før du logger inn på den aktuelle tjenesten. Dersom man logger seg inn på brukeren sin fra ukjente lokasjoner vil MFA bli satt i gang. Microsoft ser på flere ulike funksjoner i innloggingen. De får blant annet veldig mye informasjon om lokasjonen, IP-adressen og enhetstype. Microsoft evaluerer alle disse nøkkelpunktene for å fortelle brukeren om dette er en innlogging som kommer fra en kjent part eller om den kommer fra en ukjent part. Microsoft utfører dette ved hjelp av å opprettholde en profil av brukerne og den aktuelle tennant sine kjente funksjonaliteter i deres backend. Azure AD Identity Protection kan bli lagt inn på Marketplace i Microsoft Azure.

I Identity Protection kan vi automatisere prosessen til å sette i gang tiltak for å eliminere trusler med risk policy. Ved å sette opp risk policy så har man flere valg som å velge når man vil sette i gang nødvendige tiltak for en aktuell trussel. Dette kan man gjøre enten når bruker risikoen er lav eller høyere, medium eller høyere eller også når den er høy. Da kan man f.eks

sette i gang tiltak som å kreve at man endrer passord, eller at man krever en Azure MFA registrering, eller også at man krever en MFA-autentisering. I verste fall kan man også blokkere tilgangen til den aktuelle brukeren.

Microsoft samarbeider med IT-sikkerhet forskere, sikkerhetspartnere og politiet. Dermed kan brukere og passord som blir lekket på Dark Web, paste sites og andre lignende sider som blir tilgjengelig for handel på nett, sammenlignet av Microsoft med data som allerede ligger i Azure Active Directory. Microsoft sammenligner passord Hash som f.eks blir tradet online på Dark Web med passordene som befinner seg i Azure Active Directory. Dersom man ser at det blir en match i dette, så vet Microsoft automatisk at brukeren har blitt kompromittert. Dersom du har satt opp risk policyen, vil den gjøre at de aktuelle brukerne som er utsatt for sikkerhetslekkasje må gjennom en Multi Factor Authentication og passord endring. Etter dette vil ikke de aktuelle brukerne være en del av den lekkede informasjon på nettet, siden da vil disse brukerkontoene være gjenopprettet og være tilbake i normal tilstand. Ulike andre eksempler på Risk Event Typer som kan bli oppdaget i Identity Protection er innlogginger fra anonyme IP adresser som f.eks ved bruk av tjenesten TOR og anonyme VPN. Her har Microsoft tatt i bruk Real-Time deteksjon metoden og da blir man også i dette tilfelle utfordret av Multi Factor Authentication.

Et eksempel fra Near real-time detection kan være når to påfølgende sign-ins kommer fra lokasjoner langt unna innen en veldig kort tidsramme. En bruker logger inn fra New York i USA, samme bruker logger seg inn fra Chennai i India kort tid etter. Dette kan enten være VPN eller kontoopplysningene som er stjålet eller også at kontoopplysningene er for enkle å knekke seg inn på. Microsoft ser på tidsrammen og distanse rammen for de to ulike innloggingene og kan ut ifra dette se at det ganske uvanlig at noen på så kort tid logger seg inn på 2 forskjellige steder. Identity Protection har en innebygd VPN, mobilnettverk og lokasjon og omdømme intelligens som baserer seg på intel. Så det er ikke uvanlig at man f.eks jobber fra New York, men at hovedkvarteret kan ligge i Chennai, India som fører til at de som jobber fra New York blir sendt videre gjennom VPN til India. Basert på lokasjons intel fra Microsoft sin side vil de greiere å minimere de falske varslene fra f.eks VPN.

Innlogginger fra skadelige enheter som har skadevare på seg vil også bli gjenkjent i Identity Protection. Sign-in fra IP-adresser som er infisert med Malware kommer under Near real-time deteksjoner. Dersom denne IP-adressen kommer under et Botnet, så har Microsoft Digital Crimes Unit ansvar for å ta ned botnet i hele verden, og dermed vil de fortelle hvilke IP som er infisert av de ulike botnettene og dermed igjen kan Identity Protection gjenkjenne og varsle om disse IP-adressene til Microsoft Digital Crimes Unit.

Identity Protection har en funksjon som kalles for Identity Secure Score. Denne tilbyr informasjon om hvordan din identitet sikkerhet ligger ann og gir en poengscore basert på dette. Hvordan sikkerheten kan bli forbedret er også noe Identity Secure Score tar for seg. Typiske eksempler på dette kan f.eks være at man må slå på MFA tilgang, self-service passord gjenopprettelse, slå på sign-in og bruker risk policyer eller det å deaktivere kontoer som ikke har vært brukt på over tretti dager. Et annet eksempel kan være å ikke ta i bruk mer enn fem globale administratorer.

En liste med anbefalinger som bør følges når du tenker på identitet og sikkerhet i Azure er følgende:

- Bruk MFA for administrator kontoer
- Bruk PIM for alle kontoer
- Overvåk dine Risiko Rapporter
- Ta i bruk Identity Security Score
- Ta gjerne å test passwordless sign-in med Microsoft Authenticator
- Slå på Password Hash Sync
- Ta i bruk SIEM systemer som tar ut data fra Azure AD logger
- Blokkering av mistenkelige IP-adresser bør være et viktig steg for å sikre deg
- Blokkering av Legacy Auth
- Moderniser gjerne password policy som er satt opp i Azure.
- Ta i bruk user risk policy
- Ta i bruk sign-in risk policy
- Gå gjennom apper som trenger spesifikke tilgangsrettigheter og ta gjerne i bruk Microsoft Cloud App Security(MCAS)

6.2.1.1 Azure Multi Factor Authentication

Azure tar i bruk 2 stegs verifikasjon med bruk av Multi Factor Authentication. Da vil brukeren få flere valg for autentisering av sin identitet som følgende:

- Tekstmelding
- Telefonoppringning
- Microsoft tar også i bruk Authentication appen, ved bruk av denne appen får man en kode fra datamaskin og flere alternativer med kode forslag i appen. Videre skal du som bruker velge det riktige alternativet i appen som matcher koden på datamaskinen.

Azure MFA har mulighet til integrasjon med on-premises løsninger som Active Directory Federation Services (AD FS) med versjon 2016 eller høyere og Network Policy Server (NPS). Det finnes tre metoder å sette MFA på i Azure. Den ene går ut på å ta i bruk Conditional Access policyen, her må man spesifisere bruk av MFA tilgang ved å sette hvilke metoder for verifikasjon som er ønsket gjennom Conditional Access policyen. Den andre går ut på å ta i bruk risk policyen som er brukt av Azure Active Directory Identity Protection. Ved å ta i bruk denne kan man sette 2 steg verifikasjon. Ellers går den siste metoden på å endre user mode til å bli satt til 2 steg verifikasjon.

6.2.1.2 Uhåndtert Cloud Programvare

Det er veldig typisk at man overser programvare som ikke blir håndtert i en større bedrift, da det er flere arbeidsoppgaver som må utføres. I den sammenheng, kan det utgjøre en sårbarhet å ikke ha håndtert all programvare som finnes i clouden. I dette tilfelle bør man ta i bruk Cloud Discovery for å finne ut hvilke applikasjoner som står uhåndtert. Videre kan man administrere disse ved hjelp av Azure Active Directory. Arbeidsoppgaven til Cloud Discovery er å analysere trafikk mot Microsoft Cloud App Security sin cloud app katalog. Her finnes det over 16000 cloud applikasjoner. Videre blir applikasjonene her rangert. De får også en poengscore som er basert på over 70 risiko faktorer.

6.2.2 Hvordan kan man bruke Log Analytics til å oppdage trusler

Det å kun ha trussel deteksjon med Log Analytics vil ikke fungere effektivt. Når man tar i bruk Log Analytics i kombinasjon med Azure Security Center vil man få en større nytte av Log Analytics til å hente ut logger som peker ut til å ha trusler eller mistenkelig aktivitet i seg. Azure Security Center er utformet til at du som forbruker kan få sette i gang mottiltak for trusler som er oppdaget i Azure. Mens, Azure Log Analytics kan brukes til å vise sammenhengen av relasjonen mellom de ulike attributtene som er involvert i selve angrepet eller den mistenkelige aktiviteten som foregår. Log Analytics har en Operations Management Suite (OMS). Det OMSet i Log Analytics gjør er å samle inn informasjon. Basert på denne informasjonen blir det videre utført analyser av systemene til Microsoft. Her vil det komme frem informasjon om virtuelle maskiner som er lagt inn og tilkoblet Log Analytics sin OMS. Videre blir det samlet inn informasjon fra OMS agenten som kan installeres på Windows servere, her vil man da inkludere også on-premises servere og AWS. OMS samler også informasjon om lagringskontoer og andre varierte tjenester innenfor Microsoft sine cloud tjenester og Azure. Denne informasjonen kan man hente ut med logger ved å ta i bruk spørrespråket KQL i Log Analytics.

Ved bruk av Log Analytics, kan en metode for å oppdage trusler og mistenkelig aktivitet være å se på prosesser, brukerkontoer og datamaskiner. Gjennom dette kan man se når ulike prosesser og brukerkontoer oppfører seg unormalt og anomale og hvor man får en indikasjon av at ondsinnet aktivitet er på gang. Når typiske sentrale system prosesser blir kjørt eller avbrutt og annen viktig programvare som antivirus og brannmur blir deaktivert kan man raskt fatte en mistanke, hvis man ikke selv utfører denne prosessen. Ved hjelp av KQL kan man spesifisere en spesifikk prosess som man ønsker å se nærmere på gjennom å definere hvilke eventID selve prosessen har. Gjennom Kusto Query Language kan man spesifisere spesifikke attributter man vil fokusere på når man kjører spørringer mot ulike logger som f.eks Commandline, Project, Account og SubjectLogonId er noen av dem. Ved bruk av Log Analytics kan man finne ut av som har skjedd i en aktuell innloggingssesjon. Videre her kan man se hvilken bruker som har logget seg inn på den aktuelle innloggingssesjonen. Under denne tidsperioden er det også mulighet til å se hvilke IP-adresser som ble tilkoblet til maskinen. Det er også mulighet til å se hvilke IP adresser den aktuelle maskinen tilkoblet seg

mot i en spesifisert tidsperiode. Alt dette vil hjelpe til å gjøre jakten på trusler og mistenkelig aktivitet mye enklere.

Uten å vite prosess navnet til en aktuell prosess er det mulighet til å etterforske ondsinnet aktivitet ved bruk av følgende parametere i Log Analytics:

Tabell 5

```
SecurityEvent  
| where TimeGenerated >= ago(4d)  
| search CommandLine: "/stext " and CommandLine : "/scomma "  
| project NewProcessName , CommandLine
```

Her vil det da komme opp ondsinnet aktivitet som har foregått i en periode på mindre eller lik 4 dager i Log Analytics.

Det hender veldig ofte at angripere tar i bruk integrerte Windows prosesser til å skrive sine ondsinnede koder. Angriperne prøver mest mulig å integrere deres løsninger opp mot prosessene som allerede finnes på Windows. Ondsinnet programvare altså Malware prøver å ta ofte prosessen Svchost.exe i bruk for å skjule sin ondsinnede aktivitet, i den tilnærmingen slik at et offer skal tro at man egentlig tar i bruk innebygd verktøy som er sikker på Windows operativsystemet. I dette tilfelle er det veldig lett for en kompetent sikkerhetsanalytiker å se forskjell på mellom de eksisterende prosessene på operativsystemet og de ondsinnede prosessene.

Prosessene "Svchost.exe" er en av dem, dette er en stor og sentral systemprosess som er vert for flere av tjenestene som kjører på Windows. "Svchost.exe" er en generisk prosess som opptrer som vert for tjenester som blir kjørt fra ulike dynamiske koblingsbibliotek. "Svchost.exe" prosessen kjører fast fra følgende sti: %windir%/system32 eller også på %windir%/SysWOW64. Denne prosessen blir kjørt under disse tjenestene: NT AUTHORITY\SYSTEM, LOCAL SERVICE, NETWORK SERVICE kontoer. Dermed kan man

kjøre en spørring mot prosessen "Svchost.exe" med KQL for å sjekke opp om denne prosessen er kompromittert/forstyrret av andre prosesser som har ond hensikt.

Typiske metoder som angriper tar i bruk for å utnytte prosessen "Svchost.exe" er blant annet at angriperen angir navnet på prosessen helt likt men erstatter bokstaven o med 0 istedenfor så det blir følgende: "Svch0st.exe", her er det lett å overse slike navn endringer, så det gjelder å være kritisk til enhver prosess man ser på som en analytiker. En annen metode er også at angriperer navner prosessen SVCHost.exe også legger dette i en annen katalog enn standard Windows32 katalogen.

Under er det vedlagt en typisk spørring som sjekker prosesser som inneholder prosessen "Svchost.exe".

Tabell 6

```
SecurityEvent
| where TimeGenerated >= ago(4d)
| where ProcessName contains "svchost.exe"
| where NewProcessName !contains "C:\\Windows\\System32"
| where NewProcessName !contains "C:\\Windows\\Syswow64"
```

I resultatet som kommer opp i Log Analytics kan man sjekke om prosessen "Svchost.exe" er en underprosess av "services.exe" eller om den blir kjørt fra andre steder som f.eks CommandLine. Ut ifra dette kan man videre etterforske om prosessen er en del av et angrep eller kompromittert maskin/nettverk, eller om maskinen blir kjørt på riktige og normale premisser.

Et annet typisk angrep kan være Brute-force angrep. Når angriperne har kompromittert en maskin er det typiske at det neste steget blir å samle så mye informasjon de kan fra den kompromitterte maskinen. Det er typisk at det her inkluderes sensitiv data og bruker og passord informasjon til ulike kontoer. I slike tilfeller blir det også oppdaget høyt antall innloggingsforsøk på ulike kontoer som kommer fra en maskin. Så dersom vi oppdager at innloggingsforsøk som foregår mer enn vanlig antall og at det er et utallig mange forsøk som feiler, kan vi sjekke det opp med en Kusto Query Language spørring i Log Analytics som

følger:

Tabell 7

```
SecurityEvent
| where EventID == "her skrives prosessIDen inn."
| where AccountType = "User"
| where TimeGenerated >= ago(3d)
| summarize IndividualAccounts = dcount(Account) by Computer
| where IndividualAccounts > 4
```

Vedlagt KQL spørring hentet fra: Prakash, A.(Ed.). (2018, September 12). How Security Center and Log Analytics can be used for Threat Hunting. Hentet 01 Mars, 2019 fra <https://azure.microsoft.com/en-us/blog/ways-to-use-azure-security-center-log-analytics-for-threat-hunting/>

6.2.2.1 Firewall Traffic anomalies

En annen potensiell indikator for angrep i både organisasjon og privat sammenheng er Firewall trafikk. En smart ting å utføre for å analysere Firewall trafikk er å opprette en baselinje som viser og representerer den vanlige Firewall trafikken i Azure. Ved å opprette en slik baselinje har man mulighet til å se og velge ut deler av trafikken som peker mot anormalitet. Dette kan bli gjort med Log Analytics og spørrespråket KQL:

Tabell 8

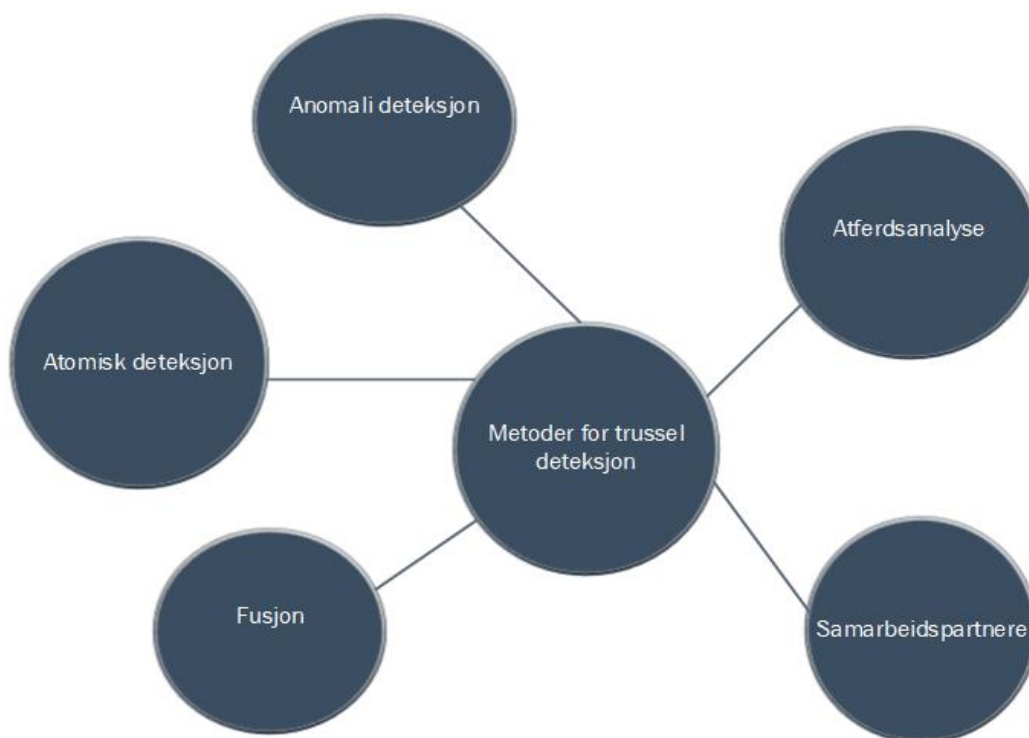
```
CommonSecurityLog
| summarize count() by bin(TimeGenerated, 100h)
```

Etter du har kjørt spørringen i ditt Log Analytics Workspace og dersom du får ut data: Kan du videre klikke på Charts for å se en baselinje over Firewall trafikk i foregående valgt tidsperiode.

6.2.3 Metoder for trussel deteksjon i Security Center

Azure Security Center tar i bruk flere ulike metoder for trussel deteksjon. De blir vedlagt nedenfor:

- Atomic Detection
- Threat Intelligence Feed og innkommende data fra tilhørende samarbeidspartnere innenfor sikkerhet
- Behavioral Analysis
- Anomaly Detection
- Detection Fusion



Figur 10

6.2.3.1 Atomic Detection

Det finnes to typer atomiske deteksjoner. Den ene typen er hovedsakelig basert på signaturbasert deteksjon. Den andre går ut på deteksjon av atferd som er utvetydig.

Signature-based Atomic Detection

Atomisk deteksjon er en veldig spesifikk deteksjonstype. Atomisk deteksjon tar i bruk Hash verdier også kalt signaturer. Dette brukes for skanning av ondsinnede kode bilder. Dersom det blir skannet for et bilde på enten disken eller i minne, og dette bilde blir matchet med Hash verdien. Da vil det bli registrert at mistenkelig aktivitet er på gang og angriperen blir fjernet umiddelbart. Atomisk deteksjon er en veldig effektiv måte for deteksjon av trusler og den måles til å være presis og perfekt i omtrent hver situasjons den møter på seg, hovedsakelig på grunn av at hashverdien garanterer et unikt funn i hver situasjon. Hver hashverdi er unik. Ulemper med atomisk deteksjonsskanning er at det er veldig lett for en angriper å utføre en endring. Denne endringen kan være å endre en liten del i selve kodebilde. Dette vil igjen få konsekvenser for Hash verdien, siden når en bit er endret i selve kodebildet, så blir automatisk Hash verdien også endret. Dermed blir det også nødvendig for en ny kalkulasjon av den nye Hash verdien. På bakgrunn av dette blir systemenes kjøretid også påvirket og det ender med at de kjører på ganske sakte kjøretid.

Single-finding Atomic Detection

Den andre typen av atomisk deteksjon er basert på single-finding i en loggoppføring i en virtuell maskin. Dette kan være alt fra en enkelt pakke som er logget i en brannmur, eller andre enkle event hendelser som er gjenkjent i systemet. Single-finding er en deteksjonstype som er mer effektiv enn signaturbasert deteksjon på bakgrunn av følgende punkter:

- Single-finding atomisk deteksjon baserer seg ikke på bilde Hash verdier. Dette betyr igjen at dersom en bit eller mer endrer seg så vil ikke det påvirke det aktuelle mønstret.
- Single-finding tar i hovedfokus på ondsinnede eller også utvetydige atferd under deteksjon.

Hvis vi f.eks tar for oss Security Identifier (SID) på en brukerkonto. SID er et nummer som blir brukt for identifikasjon av brukere, grupper og datamaskiner på Windows plattformen. Det er mest sannsynlig ingen grunn for at dette SID-nummeret skal endres av noen. Dermed kan endring av SID nummeret være en kjent og ondsinnet handling. Dette vil igjen forekomme i event loggen på Windows. Via Single-finding deteksjonsmetoden vil man kunne ha mulighet til å skanne denne event loggen for slike endringer. Basert på slike endringer som utføres, kan man igjen oppdage dette ved bruk av Single-finding atomisk deteksjonsmetoden. En ulempe som kan noteres i forbindelse med Single-finding metoden er at den kan omgå av en angriper som gjør en liten endring i den ondsinnede eller dårlige delen.

6.2.3.2 Threat Intelligence

En fordel som bør noteres med offentlige skyløsninger er at man har tilgang til trussel intelligens fra flere hundre/tusen/millioner maskiner. Basert på slik data kan man prøve å øke beskyttelsen for disse maskinene og andre tjenester. Trussel intelligens feed er en rapport som inneholder IP adresser av internet noder. Disse adressene er mistenkt for å ha vært innblandet i ondsinnet atferd/aktivitet. For å gi et par eksempler kan man nevne typiske hendelser:

- Utsending av Spam.
- Utføring av Brute-force angrep
- Utsending av trafikk som er en del av DDOS(Distributed Denial-of-service Network) nettverk(også kalt botnet)
- Å opptre som vert for et ondsinnet nettsted med mye skadevare
- Å opptre som verk for opphavsrettighet beskyttet materiale(eks. fildeling, ulovlig film distribusjon)
- Å opptre som vert for farlige sider(eks. terrororganisasjoner)

Microsoft dobbeltsjekker deres egen trussel intelligens feed med andre feeds som befinner seg på markedet. Azure Security Center har et godt samarbeid med Azure, Office 365, Microsoft CRM online, Microsoft Dynamics AX, Outlook, MSN, Microsoft Digital Crimes Unit og Microsoft Security Response Center (MSRC). Dermed henter de også en del god informasjon fra de ulike samarbeidspartnerne. Azure Security Center kan også hente ut eventlogs fra flere andre typer kilder som følgende:

Integrasjon av brannmurløsning med Azure Security Center vil føre til at sikkerhets eventlogs

informasjon som forekommer i brannmur sine logger vil komme som varsler i Azure Security Center sitt konsoll. Ikke minst gjelder det samme for tjenester som Azure Active Directory, Azure antimalware, andre Azure tjenester og deres samarbeidspartneres integrerte tjenester.

6.2.3.3 Behavioral Analysis

Når vi snakker om Behavioral Analysis kan vi sette det i sammenheng med atomisk deteksjon og trussel intelligens. Disse to metodene er ganske brukbare for deteksjon av trusler og mistenkelig aktivitet, men vi må også tenke på hva slags atferd som blir utøvet før et angrep trår til. Dermed blir det viktig i denne sammenheng å definere deteksjonsparametere som trengs for å oppdage og forstå atferd. Når man tar i bruk Behavioral Analysis legger man hovedvekten på angriperens atferd. Dermed i denne sammenheng har det lite relevans å ta for seg hvordan angriperen setter angrepet i gang, men heller ha fokuset på atferden til angriperen. En utfordring med Behavioral Analysis som vi kan ta for oss er om spørsmålet om det virkelig foregår mistenkelig aktivitet eller ikke. Eksempelvis så ser vi at det har vært 4 innloggingsforsøk på kun 90 -120 sekunder. Dette blir klassifisert som mistenkelig aktivitet som foregår på den aktuelle kontoen. En mulighet her er at det egentlig er sant at det foregår mistenkelig aktivitet på kontoen, men det kan også være sant at bruker f.eks har skrevet passordet sitt med stavefeil eller brukeren har glemt passordet sitt, og dermed prøvd de alternativene han/hun husker. Dermed blir det viktig og hensiktsmessig lurt å få inn mer informasjon før man sender ut en eventuell sikkerhetsadvarsel i Azure Security Center. Behavioral Analysis analyserer og sammenligner data mot en samling med allerede kjente parametere. Disse parameterne blir valgt gjennom høyt nivå maskinlæring teknologier og algoritmer. Disse algoritmene er igjen tilknyttet avanserte og høynivå datasett. Security Center kan ta i bruk Behavioral Analysis til å analysere kompromitterte ressurser. Disse er basert på gjennomføring av analyser av virtuelle maskiner sine logger, virtuelle nettverk enheter sine logger, fabrikk logger og krasj dumper. Det er slik at parameterne ofte samarbeider med andre signaler fra Azure til å sjekke om andre bevismateriale for pågående mistenkelige eller ondsinnet aktivitet er på gang.

Eksempler på dette kan være:

- Mistenkelige prosesser som kjøres:

Det er slik at flere og flere angripere tar i bruk metodikk som går ut på å kjøre ondsinnet programvare uten at det skal gjenkjennes i systemet. Det kan ofte hende at angriperen navngir en ondsinnet programvare lik en viktig systemfil som allerede finnes på systemet, men at denne ondsinnede filen blir plassert på et annet sted i systemet. Security Center prøver alltid å gjenkjenne slike avvik som dette ved å behandle atferden og ikke minst foreta seg overvåkning av de mistenkelige prosessene som settes i gang.

- Ondsinnede PowerShell scripts:

Ved bruk av PowerShell kan angripere kjøre ondsinnet kode på ulike virtuelle maskiner som befinner seg i Azure. Ved bruk av scriptet kan angriper tilpasse sitt utvalgte formål når man kjører det aktuelle scriptet mot offeret. Det er veldig vanlig at Security Center overvåker og etterforsker PowerShell aktivitet som foregår for mistenkelig eller skadelig aktivitet i Azure miljøet.

- Lateral Movement & Intern Reconnaissance:

Det er ofte slik at angripere beveger seg sideveis fra en kompromittert maskin til andre i samme nettverk. Dette kalles for Lateral Movement. Security Center har gode rutiner for dette og overvåker prosesser og innloggingsforsøk til å gjenkjenne forsøk som angriper utfører for å prøve å holde seg inne i nettverket. Dette kan være alt fra metoder som kommando kjøring gjennom fjernstyring, nettverk undersøkelse og konto opptelling.

6.2.3.4 Anomaly Detection

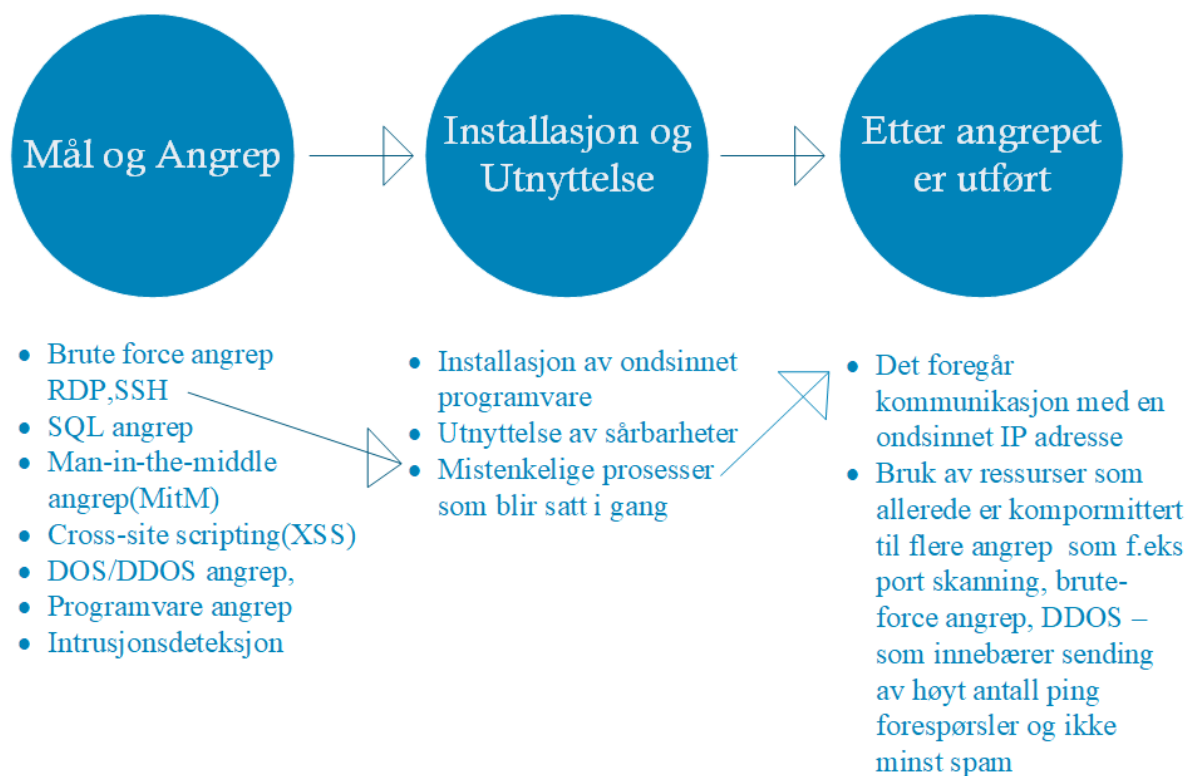
Det som menes med anomali er at det er et mønster som avviker fra et forventet eller normalt resultat. Det anomali deteksjon går ut på er deteksjon av mønstre som ikke oppfører seg som vanlig eller forventet i den aktuelle situasjonen. Her blir det blant annet sammenlignet flere ulike attributter for å oppdage og gjenkjenne unormale mønstre. Spesielt i IT situasjoner blir det viktig for IT sikkerhetspersonell å forstå den normale slik at man også har forståelsen til å forstå hva som ikke kan være normalt, det er i hovedsak det som handler om anomali og dens deteksjonsmetoder. Dermed blir det viktig å skape en baselinje med det som inneholder det

"normale atferd og oppførsel". På denne baselinjen kan man blant annet ta for seg tidsbruk for valg av baselinjes verdier og faktorene som er nødvendig å ha med på baselinjen.

Så det Azure Security Center gjør er å opprette baselinjer for VMer. Disse går på tvers av en matrise med flere parametere som også er brukbare for bestemmelse av det aktuelle sikkerhetsnivået i Azure. Perioden på baselinjene pleier å variere, men ofte er de på 30 dager. Denne baselinjen kan man ta i bruk i ulike algoritmer med fokus på statistikk, slik at du kan få en bestemmelse av hva som er normalt/ikke normalt. I denne sammenheng kan vi definere "normal" som det som er forventet og har vært konsistent med det tidligere funnene, mens det "unormale" kan defineres til å være det som er uforventet, overraskende, og ikke minst det som ikke er konsistent med de tidligere funnene. I dette tilfelle kan vi dermed definere konsistent som å det å være fast og sammenhengende. Hvis vi tar for oss innkommende RDP og SSH Brute-force angrep og setter dette i anomali deteksjonsperspektiv: Her kan Azure Security Center bestemme baselinjen for innloggingsaktivitet for de ulike virtuelle maskinene som befinner seg i Azure. Deretter kan Security Center ta i bruk maskinlæring for å vurdere de normale innloggingsaktivitetene. Dersom man videre ser at det er avvik eller forskjeller på baselinjen for innloggingsaktivitet vil det bli generert et varsel. Alt dette vil være basert på valgene maskinlæringen tar i dette tilfelle.

6.2.3.5 Detection Fusion

Security Incident er en type varsel som forekommer i Azure Security Center. Denne forekommer i situasjoner når flere ulike varsler blir knyttet sammen hverandre. Da får man en indikasjon av det pågår et aktivt angrep mot Azure. I denne sammenheng blir også Security Incident i flere tilfeller referert til å være fusion alert siden i et slikt tilfelle blir det flere ulike varsler som blir representert i en sammenheng.



Figur 11

Figuren ovenfor viser hvilke typer varsler som kan f.eks vises i de ulike stegene til Cyber Kill Chain prosessen. Vi kan se at f.eks de punktene med pil som linker til hverandre har en viss sammenheng og har en mulighet til å utløse flere varsler som er i tilknytning til hverandre.

Ut ifra figuren ovenfor kan vi sette det i sammenheng med Cyber Kill Chain modellen slik:

Tabell 9

Mål og angrep	Security Center gjenkjenner et Brute-force-angrep som går imot RDP og SSH protokollen på en VM i Azure. Dette blir avgjort ved å sammenligne baselinjen for RDP & SSH tilkoblinger til selve virtuelle maskinen og RDP innloggingsforsøk.
Installasjon og utnyttelse	Deretter så gjenkjenner Security Center oppstart av en mistenkelig prosess på selve VMen. Her kan man jobbe ut ifra flere tilfeller og muligheter. Det blir dermed veldig viktig å sette de ulike tilfellene i sammenheng til andre hendelser for å finne ut om det er et angrep som tar sted eller ikke.
Etter angrepet er utført	Her i dette tilfelle så gjenkjenner Security Center kommunikasjonen mellom den ondsinnede IP adressen og den virtuelle maskinen. Fortsatt her kan det være flere ulike muligheter og utgangspunkt. Det kan hende en person fra red team utfører noen testinger mot VMer (blir ofte informert om slikt på forhånd) eller kan det også hende at VMen er kompromittert av en angriper.

6.2.3.6 Microsoft Antimalware

Microsoft Antimalware er en agent løsning for programvare og tennant miljøet som befinner seg på Azure. Ved bruk av Microsoft Antimalware har man mulighet til å ta i bruk beskyttelse

basert på dine behov av programvare og dens arbeidsområde. Her kan ta i bruk "Basic Secure-by-default" valget eller også "Advanced custom configuration". Videre her inkluderer man da antimalware overvåkning. Microsoft Antimalware løsningen er en sikkerhetsløsning som kan tilbys til bruk for de virtuelle maskinene i Azure. De er også allerede installert automatisk på alle Azure sine Platform as a Service virtuelle maskiner. Det som er spesielt med Microsoft Antimalware er at det kjøres i bakgrunnen og at det ikke krever noen menneskelige inngrep. Dersom man velger å ta i bruk denne løsningen på en virtuell maskin, er det kun det å installere vi mennesker må utføre, resten konfigureres automatisk av Microsoft Antimalware.

Noen av mulighetene man har ved å ta i bruk Microsoft Antimalware er Real-time Protection som vil si at Antimalware overvåker aktivitet som foregår i Azure og på de virtuelle maskinene, ved å gjøre dette kan Microsoft Antimalware oppdage og blokkere ondsinnet og skadelig programvare som prøver å kjøre i Azure. Man får også utført periodisk skanning etter faste tidspunkt for å gjenkjenne ondsinnet kode og programvare. En annen god fordel ved å ta i bruk Microsoft Antimalware er at den tar aktivt grep på funnet ondsinnet og skadelig programvare eller kode ved å slette dette eller sette disse filene i karantene. Den utfører også rydding i skadelige registeroppføringer.

6.2.3.7 Strengthen Security Posture

En god funksjonalitet Azure Security Center har er at Security Center utfører analyserer periodevis. Disse analysene går ut på å analysere den aktuelle sikkerhet statusen for dine ressurser i Azure. Dersom det forekommer potensielle sårbarheter blir det satt opp anbefalinger som bør utføres eller følges. På Security Center sitt dashboard har vi en kategori som kalles for Resource security hygiene. Her finner vi anbefalingene som bør settes i gang så snart så mulig. Det er et hjul som vises frem i dashboardet og i det hjulet befinner det seg antall anbefalinger du bør gjøre for å styrke sikkerheten i Azure.

6.2.3.8 File Integrity Monitoring (FIM)

Ved bruk av File Integrity Monitoring får man gjort et dybdesøk og utforsket videre i filer og registry keys som befinner seg i operativsystemer, programvare. Ved å se på dette får man et bilde og kan se på indikasjoner av angrep som tar sted eller også prøver å ta sted. Azure Security Center kan ta i bruk File Integrity Monitoring for å se og oppdage endringer i kataloger som indikerer tegn på skadelig og ondsinnet aktivitet. Når man tar i bruk FIM blir det blant annet utført sammenligning for å bestemme om den aktuelle statusen til en fil er annerledes fra den siste skanningen av den samme filen. Slik kan man se differanser som har foregått i den nærmeste tiden og indikasjoner på at filen enten er kompromittert eller endret. Denne File Integrity Monitoring funksjonaliteten fungerer både på Windows og Linux operativsystem. Den er tilgjengelig via Standard Tier Subscription i Security Center.

6.2.3.9 Security Alerts

Azure Security Center får opp en liste med security alerts som er prioritert i Security Center Dashboard (Overview undermeny). Her vil man også få opp viktig informasjon som er nødvendig for å etterforske den aktuelle trussel situasjonen og informasjon om hvordan du reduserer eller også fjerner angrepet. Security Alerts befinner seg under Threat Protection, hvor man har et hjul med ulike farger som symboliserer alvorlighetsgraden for aktuelle Security Alerts.

6.2.4 Hvordan fungerer trussel deteksjon i Azure Security Center

Når en trussel blir gjenkjent i Azure Security Center, går den gjennom følgende steg:

- Trusselen blir sammenlignet med trussel intelligens feeden som ligger i Security Center.
- Det blir brukt en Secure Score og et resonnement system (definisjon av resonnement er at det skal være en tankerekke som logisk skal føre til at man får en konklusjon/sluttvalg).

- Trusselen går gjennom Advanced engine som korrelerer varslene til aktuelle hendelser.

Azure Security Center tar i bruk avansert incident-response verktøy for å hjelpe kundene til å utføre etterforskning av trussel omfanget. Deretter får kundene også mulighet til å legge inn de tilpassede endringene for å redusere truslene.

Ut ifra sikkerhetsvarslene får vi informasjon om følgende:

- Om hva som er bakgrunnen for utløsningen av sikkerhetsvarslet
- Hvilke ressurser som er målrettet for angrep
- Kilden som stammer fra angrepet
- Forslag for å redusere den aktuelle trusselen

Sikkerhetsvarsler blir delt inn i 4 kategorier:

- **Virtual Machine Behavioral Analysis (VMBA)**

VMBA tar i bruk Behavioral Analysis til identifikasjon av komprimerte ressurser.

Dette baserer seg på analyser fra event logs til virtuelle maskiner. Eksempler på informasjon som det blir jobbet ut ifra er innloggingshendelser og prosessopprettelser.

- **Network Analysis**

Network Analysis fokuserer på å samle inn trafikk fra tjenesten Azure Internet Protocol Flow Information Export (IPFIX). Deretter blir denne dataen som innsamles analysert for ulike trusler. Eksempel på en slik trussel kan være mistenkelig aktivitet fra RDP Nettverk aktivitet fra flere ulike ukjente kilder.

- **Resource Analysis**

Resource Analysis tar for seg analyse av PAAS som står for Platform as a Service.

Her blir tjenester som Azure SQL analysert. Basert på analyser fra PAAS blir det utløst varsler dersom det forekommer trusler og mistenkelig aktivitet. Et godt eksempel på en trussel som kan forekomme under ressursanalyse kan være en typisk SQL Injeksjon varsel.

- **Kontekstuell informasjon**

I denne kategorien av kontekstuell informasjon så får man mulighet til å få ekstra informasjon om den aktuelle trusselen og muligheter som ligger for reduksjon av farenivå med hovedfokus på trusselen.

6.2.4.1 Gjenkjenn angrep på kontainerløsninger i Azure

Når man tar i bruk Docker løsning må man ha i baktanke at en veldig aktuell og felles tilgangsvektor for angripere og andre uvedkommende som vil gjøre noe ondsinnet en feilkonfigurert daemon. Docker har som standard satt opp slik at deres «engine» er kun tilgjengelig via en UNIX socket og dermed så har man automatisk ikke tilgang til Docker engine gjennom fjernkobling. Men, det er slik at når man jobber med Docker kan man også i enkelte tilfeller ønske/kreve å bruke fjerntilkobling til Docker engine. Her i dette tilfelle kan man da nevne at Docker har støtte for TCP sockets. Her kommer problemet. Dersom man kjører daemon med TCP socket uten å spesifisere flagget «tlsverify» i daemonkjøringen så har hvem som helst i nettverket tilgang på selve Docker Hosten. Da har man videre mulighet til å kjøre uautentisert API forespørsler til selve Docker engine. Da er det slik at en slik Docker daemon som står eksponert fritt i nettverket ofte blir kompromittert veldig raskt av angripere og andre uvedkommende. Slik Docker daemon kan gjenkjennes i Azure Security Center og man har muligheter til å få varsler på slik type angrep.

Exposed Docker daemon detected
 DD458-0000-2
[Learn more](#)

General information

DESCRIPTION	Machine logs indicate that your Docker daemon (dockerd) exposes a TCP socket. By default, Docker configuration, does not use encryption or authentication when a TCP socket is enabled. This enables full access to the Docker daemon, by anyone with access to the relevant port.
ACTIVITY TIME	Thursday, November 29, 2018, 11:01:11 AM
SEVERITY	Medium
STATE	Active
ATTACKED RESOURCE	DOCKER-DEMO-2
SUBSCRIPTION	ASC Demo (00000000-0000-0000-0000-000000000000)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
COMPROMISED HOST	DOCKER-DEMO-2
USER NAME	root
SUSPICIOUS PROCESS	/usr/bin/dockerd
SUSPICIOUS COMMAND LINE	/usr/bin/dockerd -H unix://var/run/docker.sock -H tcp://0.0.0.0:2375
SUSPICIOUS PROCESS ID	0x1205e

Remediation steps

REMEDATION STEPS	<ol style="list-style-type: none"> 1. If possible, remove the TCP socket from the daemon and use only the default UNIX socket to access the daemon. 2. If a TCP socket is required, make sure that TLS is used (see https://docs.docker.com/engine/security/https/).
------------------	---

Figur 12

Kilde: Detecting threats targeting containers with Azure Security Center [Digital Bilde]. (n.d.). Hentet 23 april 2019, fra <https://azurecomcdn.azureedge.net/mediahandler/acomblog/media/Default/blog/b324b5ff-bd9c-47b9-9b95-4f592e2af611.png>

Figur 8 viser en eksponert Docker daemon som er gjenkjent i Azure Security Center.

Et annet scenario når man tar i bruk docker kontainer løsninger er at kontainerne blir kjørt med høyere rettigheter enn det de egentlig trenger for vanlig kjøring. Dermed vil det si at når man har flere rettigheter med høyere tilgangsnivå har mulighet til å få tilgang til hostens ressurser. I dette tilfelle vil dermed en slik kontainer med høyere tilgangsnivå som blir kompromittert føre til at hosten også kan bli kompromittert. Azure Security Center har mulighet til å gjenkjenne og gi ut varsler når man kjører en kontainer løsning med høyere tilgangsnivå med rettigheter. Azure Security Center har også mulighet til å gjenkjenne kontainere hvor det kjøres SSH servere og kontainere med ondsinnede ISO filer.

Dashboard > Security Center - Overview > Security alerts > Privileged Container Detected > Privileged Container Detected

Privileged Container Detected

DOCKER-DEMO-2

[Learn more](#)

General information

DESCRIPTION	Machine logs indicate that a privileged Docker container is running. A privileged container has a full access to the host's resources. If compromised, an attacker can use the privileged container to gain access to the host machine.
ACTIVITY TIME	Monday, October 22, 2018, 2:50:27 PM
SEVERITY	i Low
STATE	Active
ATTACKED RESOURCE	DOCKER-DEMO-2
SUBSCRIPTION	ASC Demo (00000000-0000-0000-0000-000000000000)
DETECTED BY	■ Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	■ Virtual Machine
COMPROMISED HOST	DOCKER-DEMO-2
USER NAME	unknown/root
ACCOUNT SESSION ID	0xde6
SUSPICIOUS PROCESS	/usr/bin/docker
SUSPICIOUS COMMAND LINE	docker run --privileged -it alpine
SUSPICIOUS PROCESS ID	0x1981f

Remediation steps

REMEDIATION STEPS

If the container doesn't need to run in privileged mode, remove the privileges from the container.

Figur 13

Kilde: Detecting threats targeting containers with Azure Security Center [Digital Bilde]. (n.d.). Hentet 24 april 2019, fra <https://azurecomcdn.azureedge.net/mediahandler/acomblog/media/Default/blog/b324b5ff-bd9c-47b9-9b95-4f592e2af611.png>

Figur 9 viser Azure Security Center som har gjenkjent en kontainer med høyere tilgangsnivå av rettigheter.

6.2.5 Hvordan kan man ta i bruk Azure Sentinel for trussel deteksjon

Azure Sentinel tar imot data ved å tilkoble seg til tjenester og programvare i Azure. Du velger selv hvilke tjenester og programvare du vil overvåke med Azure Sentinel. I dette prosjektets tilfelle kan vi tilknytte og ta imot data fra Azure Active Directory, Azure Log Analytics, Azure Security Center og Azure Identity Protection. Ved å tilkoble til disse tjenestene får man inn data knyttet til sikkerhetshendelser inn i Azure Sentinel. Du får en visualisering og dataanalyse av Data Source som er tilknyttet Azure Sentinel.

6.2.5.1 Advanced Alert Rules

Med Azure Sentinel har du mulighet til å opprette Advanced Alert Rules. Ved å gjøre dette kan du generere ulike case scenarioer som du kan ta i bruk. Deretter kan du ta casene i bruk til videre etterforskning for både trusler som foreligger i Azure miljøet og anomalies av hva som er mistenkelig og unormalt. Ved å opprette slike alert rules får man mulighet til å respondere til trusler som forekommer i miljøet. Man har også mulighet til å definere aktuelle valgte trusler slik at man videre kan sette dem til etterforskning. Ved å gjøre dette har du mulighet til å kun fokusere på de valgte truslene etter din interesse.

6.2.5.2 GitHub Threat Detection Library

En annen funksjonalitet som du har i Azure Sentinel er bruk GitHub Threat Detection Library. Her kan man ta i bruk et ganske stort og omfattende bibliotek med innebygde deteksjoner som kan både implementeres og tilpasses. I dette biblioteket er de ulike deteksjonsmetodene skrevet i KQL, noe som igjen betyr at vi kan ta i bruk Log Analytics for å utføre trussel deteksjon med GitHub Threat Detection Library.

6.2.5.3 Hunting-tool

Ved bruk av Hunting-tool verktøyet i Azure Sentinel har man mulighet til å legge inn spesifikke queries for å finne sikkerhetshendelser og trusler i Azure miljøet.

6.2.5.4 Automated Threat Response

Ved bruk av Azure Sentinel har man mulighet til å sette opp Security Playbooks til automatisk respons for forekommende trusler og hendelser. En Security Playbook inneholder en større samling av prosedyrer som tar for seg hva man skal og bør gjøre når en varselsituasjon forekommer. Ved bruk av Security Playbook har man mulighet til å automatisere og orkestrere dine reponsmetoder til varsler som forekommer. Du kan også velge å kjøre dette ved enten gjennom automatisk håndtering eller også manuell håndtering. Et godt eksempel på dette er at du har mulighet til å sette et sikkerhetsvarsel for mistenkelige og ondsinnede IP-

adresser i Azure miljøet. Dette kan du gjøre på generell basis, eller også dersom du mistenker at en eller flere prøver å koble seg inn i ditt Azure miljø.

6.2.6 Advanced Threat Protection for Azure SQL Databaser

Advanced Threat Protection for Azure SQL Databaser gjenkjenner aktivitet som peker mot anormalitet. Dette inkluderer blant annet ondsinnede og skadelige forsøk på utnyttning av exploits eller til å få tilgang til databaser. Advanced Threat Protection fungerer slik som et nytt lag av sikkerhet for databasene. Dette gir flere ulike muligheter for brukere og kunder som å gjenkjenne og respondere til ulike potensielle trusler som forekommer under Azure SQL Databaser området. Et veldig nyttig funksjonalitet med Advanced Threat Protection for Azure SQL Databaser er at den har integrasjon av varsler med Azure Security Center. Dette fører til at man får opp detaljer om mistenkelig aktivitet tillegg til å få informasjon om hvordan man kan etterforske den mistenkelige hendelsen som forekommer og hvordan man kan redusere utfallet av trusselen. Videre skal vi på noen av varslene som kan trigges i Advanced Threat Protection.

6.2.6.1 Vulnerability to SQL injection

Denne type varsel forekommer når det blir generert en feil SQL setning i databasene. Dette er en mulig advarsel om potensielle sårbarheter som har forekommet i tilknytning til SQL injection attacks. To gode grunner til at slik type varsel kan forekomme er at: 1; At det har forekommet en defekt i applikasjonskoden som er med på å bygge SQL setningen som blir påpekt til å være feil. 2; Eller at det er programkode/andre lagrede prosedyrer som ikke tar i bruk user input ved konstruksjonen av selve SQL setningen som blir tatt i bruk for SQL injection.

6.2.6.2 Potential SQL injection

Dette varslet forekommer når en potensiell angriper prøver å legge inn ondsinnet og skadelig SQL setninger ved bruk av skadelige applikasjoner eller prosedyrer som allerede ligger lagret i systemet.

6.2.6.3 Access from unusual location

Dette varslet forekommer når det blir merket en endring til access pattern knyttet til SQL server. I slikt tilfelle har andre uvedkommende logget inn på SQL server fra en helt annen geografisk lokasjon som er veldig ukjent for SQL Server til vanlig.

6.2.6.4 Access from a potentially harmful application

Et slikt varsel som dette forekommer når en potensiell ondsinnet og skadelig applikasjon blir brukt til å få tilgang til selve databasen i Azure. Her har man to typer scenarioer; den ene går ut på potensiell angrep som brukes felles verktøy, eller kan det også være sikkerhetsteam som driver med penetrasjonstesting og dermed kan det forekomme slik varsler som dette.

7. Use-case tilnærming i Azure

Tabell 10

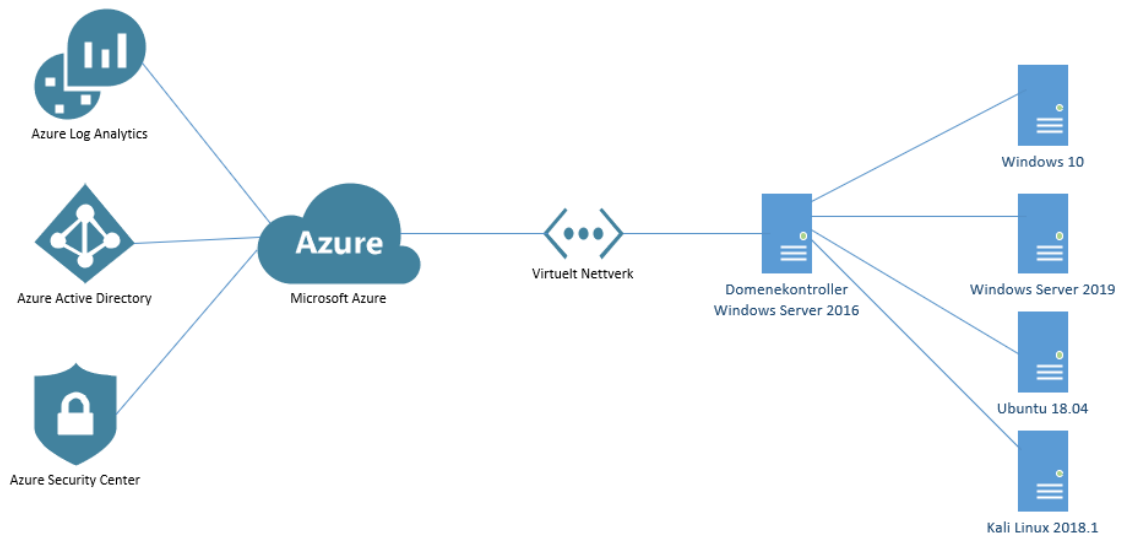
Use Case	Hva vil man oppnå	Tilnærming	Observasjoner	Avvik
Brute-force angrep	Brute-force angrepet fra en virtuell maskin til en annen virtuell maskin blir gjenkjent i Security Alerts. Videre får man også informasjon om hvor angrepet stammer fra.	1.RDP Port 3389 og SSH Port 22 må være åpen på Azure VM. 2. THC Hydra brukes fra Kali Linux til å sette opp test angrep på en virtuell maskin i Azure. 3. En ordliste med passord og en ordliste med brukernavn skal opprettes på Kali. I disse to listene må minst ett av ordene i hver liste inneholde riktig brukernavn og riktig passord.	Brute-force angrepet ble satt i gang. Angrepet fikk ikke tak i brukernavn og passord til tross for ordlister som inneholdt det riktige brukernavnet og passordet. Men Brute-force angrepet gikk igjennom. Dette ble ikke gjenkjent av Security Alerts i Security Center i Azure. Forsøk på Brute-force angrep skal vanligvis komme under deteksjonen i Azure Security	Angrepet ble utprøvd både på lokal IP og offentlig IP adresse.

			Center.	
Varsel validering	Security Center skal oppdage en Security alert for denne varsel validering testen.	<p>1. Kopierer en fil som kan kjøres til desktop (i dette tilfelle calc.exe)</p> <p>2. Endre navnet på calc.exe til ASC.AlertTest_662jfi039N.exe.</p> <p>3. Åpne Command Prompt også kjent som cmd til å skrive inn følgende argument: ASC.AlertTest_662jfi039N.exe -foo.</p> <p>4. Vent i 5-10 minutter før man sjekker Security Alerts i Azure Security Center for endringer.</p>	Etter å ha ventet både i 5 og 10 minutter, ser man ingen tegn på sikkerhetsvarsel for varsel valideringen i Security alerts i Security Center.	Denne metoden ble kjørt 4 ganger for å dobbeltsjekke om denne metoden virkelig fungerer.
eicar_com.zip (virus)	Eicar viruset skal komme opp som et sikkerhetsvarsel	Laster ned Eicar virus fra følgende webside: https://	Etter omtrent 10 timer, får Azure et varsel om at Eicar virus filen	Eicar viruset ble ikke oppdaget med en gang i Azure Security

	i Security Center	www.eicar.org/?page_id=3950 Deretter lagrer man eicar_com.zip filen til skrivebordet. Trenger ikke å åpne opp ZIP filen. Dette gjøres automatisk.	er oppdaget. Videre kommer det beskjed om at Microsoft Antimalware har satt i gang tiltak for å beskytte maskinen fra Malware og annen skadevare. Azure har blokkert tilgangen til Eicar.	Center. Det ser ut til at Security Center tar lenger tid til å registrere Eicar viruset i Security Center.
Metasploit	Metasploit skal oppdages som virus under Security Alerts i Security Center.	Metasploit blir lastet ned fra følgende side: https://www.metasploit.com/	Metasploit ble oppdaget i Security Alerts. Tiltak ble satt i gang for å fjerne trusselen fra Microsoft Antimalware.	Det tar omtrent 1-2 timer eller også lenger tid før Security Center får opp varslene om at Metasploit er oppdaget som trussel i Azure.
Port Skanning	Deteksjon av utførelse av port skanning.	Nmap Security Scanner bli lastet ned fra følgende side: https://nmap.org/download.html	Utførelsen av port skanningen på en virtuell maskin i Azure blir ikke oppdaget som	

			trussel i Security Center og det har heller ikke kommet opp i Security Alerts.	
--	--	--	---	--

8. Nettverkstopologi



Figur 14

Prosjektet vil ta for seg følgende deler:

5 virtuelle maskiner med operativsystem som følger:

Windows Server 2019

Windows Server 2016

Windows 10 Education

Ubuntu 18.04

Kali 2018.1

- 1 Virtuelt nettverk
- Azure Active Directory
- Azure Active Directory Domain Services (Opprettelse av eget domene)
- Azure Security Center
- Brannmur (Microsoft Azure)
- Ruter (Microsoft Azure)

Alt dette vil bli satt opp i sky plattformen Microsoft Azure.

Brukernavn og Passord på de virtuelle maskinene i Azure er vedlagt som følgende:

Tabell 11

Virtuell Maskin	Brukernavn	Passord
Win19	oppgaven	qwerty2019_!
sec	nareny	qwerty2019_!
Pentestmaskin	nareny	qwerty2019_!
win16	nareny	qwerty2019_!
SQL database Azure (SQL Database)	oppgaven	qwerty2019_!

Tabell 12

Azure Global Administrator	Passord
naren@09999.no	bscqwertyoppgave2019_!_?N1

Tabell 13

Azure Demo Bruker	Passord
demobruker@09999.no	abcqwerty2019_!

Tabell 14

Domain	azureatp.local	Qwerty2019_!
Azure Bruker	nareny@09999.no	Bachelor_2019

9. Kilder

- [1] Copeland, M. (2017) Cyber Security on Azure: USA: Apress.
- [2] Diogenes, Y. & W.Shinder, T. (2018) Microsoft Azure Security Center. USA: Pearson Education, Inc.
- [3] Modi, R. Azure for Architects: Implementing cloud design, DevOps, containers, IoT, and serverless solutions on your public cloud. S.1.: PACKT Publishing Limited.
- [4] Wali, M. (2018). Learn Microsoft Azure: Build, manage, and scale cloud applications using the azure ecosystem. PACKT Publishing Limited.
- [5] Nickel, J. (2019). Mastering Identity and Access Management with Microsoft Azure, 2nd edition. S.1.: PACKT Publishing Limited.
- [6] Microsoft. (2018b, 10 april). Azure Security Center | Azure Friday [YouTube]. Lokalisert 10 januar, 2019, fra: <https://www.youtube.com/watch?v=t6gp9k78XEw>
- [7] Microsoft. (2018, 5 juni). Azure Active Directory Identity Protection Detections [YouTube]. Lokalisert 17 januar, 2019, fra: <https://www.youtube.com/watch?v=ZqT9hvJj4r4>
- [8] Microsoft. (2017, 17 mai). Azure Friday | Azure Active Directory Identity Protection [YouTube]. Lokalisert 16 januar, 2019, fra: https://www.youtube.com/watch?v=zI3jn_G0_Ns
- [9] Microsoft. (2018, 2 november). How does Azure work. Lokalisert 28 Februar, 2019 fra: <https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/getting-started/what-is-azure>
- [10] Microsoft Ignite. (2018, 2 oktober). Azure Security Center 101 - THR1068 [YouTube]. Lokalisert 31 januar, 2019, fra: <https://www.youtube.com/watch?v=kfb2O3Nk0Ak>
- [11] Prakash, A. (2018, 16 januar). How Azure Security Center helps analyze attacks using investigation and log search. Lokalisert 20 februar, 2019 fra: <https://azure.microsoft.com/en-us/blog/how-azure-security-center-helps-analyze-attacks-using-investigation-and-log-search/>
- [12] Microsoft Azure. (2018, 17 mai). Detect malicious activity using azure security center and azure log analytics. Lokalisert 22 februar, 2019 fra: <https://azure.microsoft.com/en-us/blog/detect-malicious-activity-using-azure-security-center-and-azure-log-analytics/>

- [13] Kersten, Jenna. "Who's Responsible for Cloud Security - Cloud Service Providers.", KirkpatrickPrice Home, Sarah Morris 17 april 2018. Lokalisert 11 mars, 2019 fra <https://kirkpatrickprice.com/blog/whos-responsible-cloud-security/>
- [14] Dekalb, Leah. "New EBook - Definitive Guide to Azure Security." Skyhigh, Skyhigh Networks, 21 Mars 2018. Lokalisert 11 mars, 2019 fra <https://www.skyhighnetworks.com/cloud-security-blog/new-ebook-definitive-guide-to-azure-security/>
- [15] Martin, Lockheed. "Cyber Kill Chain. " Lockheed Martin. Lokalisert 11 mars, 2019 fra www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- [16] Microsoft. «What Is Cloud Computing? A Beginner's Guide | Microsoft Azure. « A Beginner's Guide | Microsoft Azure. Lokalisert 19 mars, 2019 fra <https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/>
- [17] «MITRE ATT&CK.» MITRE ATT&CK. Lokalisert 28.02.19 fra <https://attack.mitre.org>
- [18] Amazon. «Serverless Computing – Amazon Web Services.» Amazon, Amazon. Lokalisert 19 mars, 2019 fra <https://aws.amazon.com/serverless/>
- [19] Microsoft. «File Integrity Monitoring in Azure Security Center.» Microsoft Docs, 13 Mars, 2019. Lokalisert 20 mars, 2019 fra <https://docs.microsoft.com/en-us/azure/security-center/security-center-file-integrity-monitoring#add-a-new-entity-to-monitor>
- [20] Microsoft. «Managing Security Recommendations in Azure Security Center.» Microsoft Docs, 13 desember, 2018. Lokalisert 20 mars, 2019 fra <https://docs.microsoft.com/en-us/azure/security-center/security-center-recommendations>
- [21] Pliskin, Ram. «How Azure Security Center Helps You Protect Your Environment from New Vulnerabilities.» Blog | Microsoft Azure, 14 februar, 2019. Lokalisert 20 mars, 2019 fra <https://azure.microsoft.com/en-us/blog/how-azure-security-center-helps-you-protect-your-environment-from-new-vulnerabilities/>
- [22] Microsoft. «Deploy Cloud Discovery – Cloud App Security.» Deploy Cloud Discovery – Cloud App Security | Microsoft Docs, 27 januar, 2019. Lokalisert 20 mars, 2019 fra <https://docs.microsoft.com/en-us/cloud-app-security/set-up-cloud-discovery>
- [23] Microsoft. «What Is Azure Sentinel Preview?» Microsoft Docs, 28 februar, 2019. Lokalisert 25 mars, 2019 fra <https://docs.microsoft.com/en-us/azure/sentinel/overview>
- [24] «Threat Detection and Response Techniques: A Deep Dive.» Rapid7. Lokalisert 25 mars, 2019 fra <https://www.rapid7.com/fundamentals/threat-detection/>
- [25] Microsoft. «Run a Playbook in Azure Sentinel Preview.» *Run a Playbook in Azure*

Sentinel Preview / *Microsoft Docs*, 28 februar, 2019. Lokalisert 25 mars, 2019 fra <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

[26] Microsoft. «Investigate Alerts with Azure Sentinel Preview.» *Investigate Alerts with Azure Sentinel Preview* / *Microsoft Docs*, 20 mars, 2019. Lokalisert 25 mars, 2019 fra <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats>

[27] Microsoft. «Advanced Threat Protection – Azure SQL Database.» *Advanced Threat Protection – Azure SQL Database* / *Microsoft Docs*, Microsoft, 31 mars, 2019. Lokalisert 25 april, 2019 fra <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview>

Driftsdokument

Versjon 0.3

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
01.03.19 - 31.03.19	0.1	Oppsett, struktur, Data Collection, Standard Tier, installasjon av vm, hensikt, formål, Azure Sentinel, JIT, struktur, Powershell deteksjon, security alerts, log analytics – Powershell,	Naren Yogarajah
01.04.19 - 30.04.19	0.2	Powershell deteksjon, security alerts, log analytics – Powershell, Svchost prosess, Powershell, struktur, deteksjon, Kilder, struktur, stavekontroll+gramatikk, log analytics, Eicar virus, Identity Protection, log analytics deteksjon TOR Browser Security Alerts Map, Networking – security center, Ad connect, ad Domain services, ATP, MFA registration, User risk policy, Sign-in risk policy, Hunting queries, Brute Force, Azure Sentinel	Naren Yogarajah

		SQL database sikkerhet, Azure SQL Data Warehouse	
01.05.19 – 20.05.19	0.3	<p>Deteksjon og overvåkning, Installasjon, Azure SQL, Azure ATP Identity Protection, Endringer fra 1.utkast driftsdokument – legge inn beskrivelser av viktige tjenester, endring av bildeformat, Azure Sentinel, Azure MFA, 2.utkast endringer – versjonsendringer, beskrivelse, geolokasjon, beskrivelse av hva man ser, hvordan man ser at man har blitt angrepet og faktisk beskrivelse fra Microsoft sin side, geolokasjon – hvilke IP adresser</p>	Naren Yogarajah

Innholdsfortegnelse

1. Introduksjon	109
1.2 Hensikten med dokumentet	109
1.3 Bedriftens krav til systemet	109
1.4 Prosjektets andre dokumenter	109
1.5 Forkortelser	110
1.6 System formål	110
1.7 Systemets ansvarlige	111
1.8 Faser i implementasjon av pilot	111
1.9 Framdriftsplan	111
2. Installasjon og Konfigurasjon	112
2.1 Azure	112
2.1.1 Azure Portal	112
2.1.2 Pay-As-You-Go Subscription	113
2.1.3 Resource Groups	113
2.1.4 Virtuelt nettverk	114
2.1.5 Installasjon av virtuell maskin i Azure	116
2.1.5.1 Remote Desktop Access	125
2.1.5.2 SSH Port	128
2.2 Azure Active Directory	130
2.2.1 Azure AD Premium P2 Edition	130
2.2.2 Azure Active Directory Users	131
2.2.3 Azure Active Directory Identity Protection	133
2.2.3.1 Azure Multi Factor Authentication	136
2.2.3.2 User Risk Policy	140
2.2.3.3 Sign-in risk policy	145
2.2.3.4 Alerts	149
2.2.4 Azure Active Directory Privileged Identity Management	150
2.2.5 Active Directory Domain Services	153
2.2.6 Microsoft Azure Active Directory Connect	164
2.2.7 Azure Advanced Threat Protection	180
2.3 Azure Log Analytics	188
2.3.1 Installasjon av Log Analytics	188
2.3.2 Tilkobling av virtuelle maskiner til Log Analytics	191

2.4 Azure Security Center	193
2.4.1 Installasjon av Azure Security Center	193
2.4.2 Standard Tier Subscription	195
2.4.3 Policy & Compliance	196
2.4.3.1 Data Collection	196
2.4.3.2 Secure Score	199
2.4.4 Resource Security Hygiene	200
2.4.4.1 Recommendations	200
2.4.4.2 Compute & apps	201
2.4.4.3 Networking	204
2.4.5 Advanced Cloud Defense	207
2.4.5.1 Just-in-time VM Access	207
2.4.5.2 File Integrity Monitoring	209
2.4.6 Threat Protection	211
2.4.6.1 Security Alerts	211
2.4.7 Microsoft Antimalware	216
2.5 Azure Sentinel	218
2.5.1 Installasjon av Azure Sentinel	218
2.5.2 Hunting	224
2.6 Azure SQL Databases	226
3. Deteksjon og overvåkning i Azure	227
3.1 Tor Browser	227
3.1.1 Identity Protection	227
3.1.1.2 Vulnerabilities	235
3.1.2 Log Analytics	236
3.1.3 Security Center	237
3.1.3.1 Security Alerts Map	239
3.2 Suspicious Powershell Activity Detected	242
3.2.1 Security Center	242
3.2.2 Log Analytics	244
3.3 Suspicious SVCHOST process executed	248
3.3.1 Security Center	248
3.3.2 Log Analytics	252
3.4 Brute-force angrep	253
3.4.1 Security Center	253
3.4.2 Log Analytics	259

3.5 Eicar Virus.....	260
3.5.1 Security Center.....	260
3.6 Port skanning.....	263
3.6.1 Security Center.....	263
3.7 Traffic from unrecommended IP addresses was detected.....	264
3.7.1 Security Center.....	264
3.8 Trojan: Win32/Powrmry.A! atk	266
3.8.1 Security Center.....	266
3.9 Alert validation.....	268
4.0 SQL Database Vulnerability Assessment	271
5. Kilder	275

1. Introduksjon

1.2 Hensikten med dokumentet

Hensikten med dette driftsdokumentet er at dette dokumentet skal fungere som en installasjonsveiledning av tjenestene som har blitt beskrevet i systemkravrapporten. Her vil man blant annet ta for seg hvordan man går frem steg for steg for å installere tjenester som er nødvendig for prosjektet. Tjenestene som er beskrevet i systemkravrapporten blir tatt i utgangspunkt i dette driftsdokumentet og hovedfokuset blir å se på metoder for trussel deteksjon som foreligger i tjenestene Azure Active Directory, Azure Log Analytics og Azure Security Center. Dokumentets hensikt er også å vekke interesse for leseren om Azure og de mulighetene som foreligger innenfor sikkerhetsområdet av cloud miljøet til Microsoft. Dokumentet er beregnet for de som har en grunnleggende forståelse om cloud og sikkerhet innenfor IT.

1.3 Bedriftens krav til systemet

DNBs krav til systemet vil hovedsakelig være at man får frem de sentrale tjenestene for trussel deteksjon som befinner seg i Azure Active Directory, Azure Log Analytics og Azure Security Center. Sammenhengen mellom tjenestene blir også et sentralt utgangspunkt å ta for seg og få en grundig og god forståelse av hvordan de fungerer sammen blir viktig.

1.4 Prosjektets andre dokumenter

Forstudierapport og systemkravrapport som har blitt utarbeidet tidligere i prosjektet blir brukt som referanse i driftsdokumentet. I forstudierapporten har jeg blant annet utarbeidet en helhetlig plan over prosjektet. Der i blant har jeg fått beskrevet en del målsettinger for prosjektet mer spesifisert er det effektmål, resultatmål og prosessmål som er satt for prosjektet. Etter dette har jeg også tatt for meg en interessentanalyse og redegjort for

suksessfaktorer for prosjektet. I tillegg til dette er risikoanalyse en av de viktigste fasene som er blitt utarbeidet i forstudierapporten, hvor jeg blant annet tar for meg risikofaktorer som er med på å gi et innblikk om hvorvidt prosjektet har mulighet for å mislykkes. I

systemkravrapporten blir det tatt for seg en god og detaljert beskrivelse av de ulike tjenestene som skal fokuseres på i prosjektet og hvordan disse tjenestene har mulighet for å utføre trussel deteksjon i Azure miljøet. I tillegg til dette følger det med en nettverkstopologi diagram og systemkravrapporten blir avsluttet med en begrunnelse for hvorfor jeg har akkurat valgt denne løsningstypen for prosjektet.

1.5 Forkortelser

Navn	Forkortelse
Virtuell maskin	VM
Active Directory	AD
RDP	Remote Desktop Protocol
IT	Informasjonsteknologi
ATP	Advanced Threat Protection
CMD	Command Prompt
SAAS	Software as a service
PAAS	Platform as a service
IAAS	Infrastructure as a service
VPN	Virtual Private Network

1.6 System formål

Formålet med systemet og tjenester vi tar i bruk er hovedsakelig for å kartlegge å finne ut hvilke metoder man kan ta i bruk for trussel deteksjon. I tillegg blir det også viktig å se på hvilke muligheter man har i Azure for å redusere utfallet av angrepet og ikke minst få nok informasjon om angrepet før den forekommer.

1.7 Systemets ansvarlige

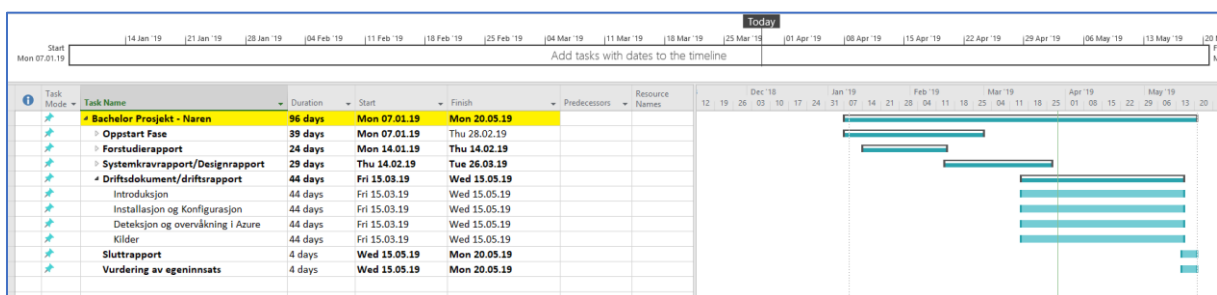
I prosjektets tilfelle kan vi si at systemets ansvarlige er Microsoft, DNB og Naren Yogarajah. Når man definerer systemets ansvarlige innebærer dette ansvaret ovenfor Microsoft Azure som blir tatt i bruk i dette prosjektet.

1.8 Faser i implementasjon av pilot

Fasene i implementasjonen av løsningen er tenkt til å være slik:

- Introduksjon
- Installasjon og Konfigurasjon
Her foregår oppsett av de ulike tjenestene som er utgangspunkt for oppgaven.
- Deteksjon og Overvåkning
Videre under deteksjon og overvåkningsfasen er det tatt for seg mer case scenarioer og hvordan man bruker Azure Active Directory, Azure Log Analytics og Azure Security Center for å gjenkjenne disse case scenarioene.
- Kilder

1.9 Framdriftsplan



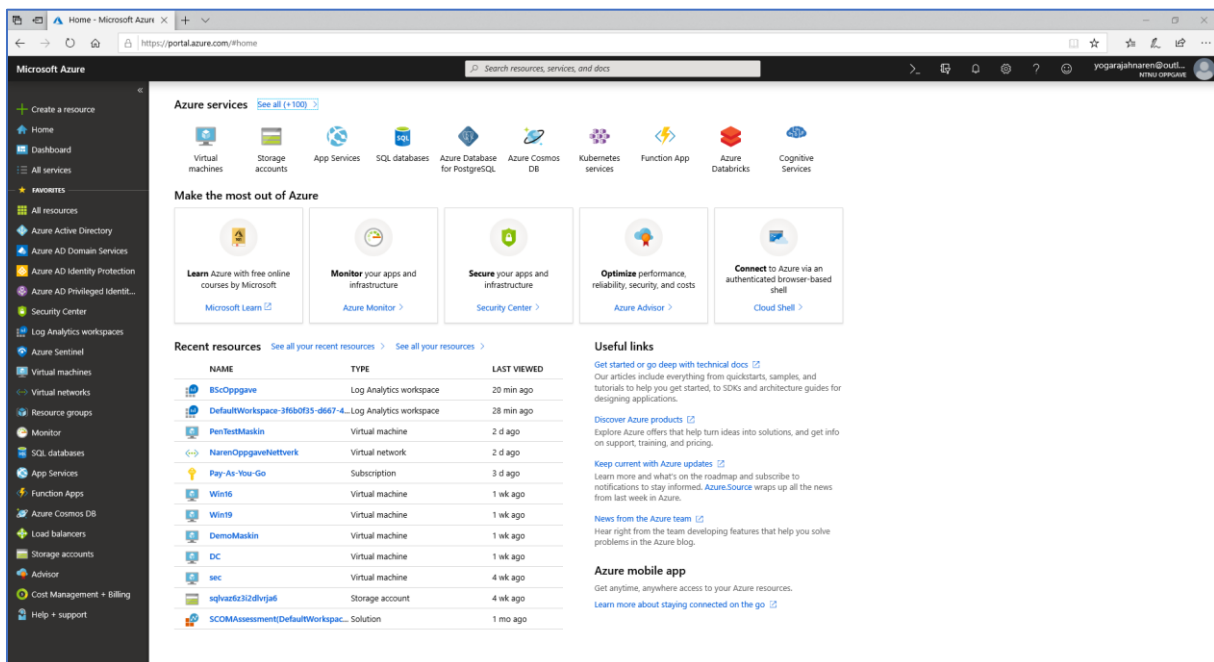
Framdriftsplanen ovenfor viser en foreløpig tenkt plan for utformingen av driftsdokumentet. Denne rapporten skal foregå i perioden 15 mars 2019 til 15 mai 2019. Den kan forekomme endringer underveis i planen, dersom jeg ser behov for dette. Det er lett å stå fast på noen

punkter innenfor installasjonsfasen i driftsdokumentet og da bør man heller komme tilbake til de aktuelle punktene på et senere tidspunkt, i stedet for å gruble på et problem i lenger tid.

2. Installasjon og Konfigurasjon

2.1 Azure

2.1.1 Azure Portal

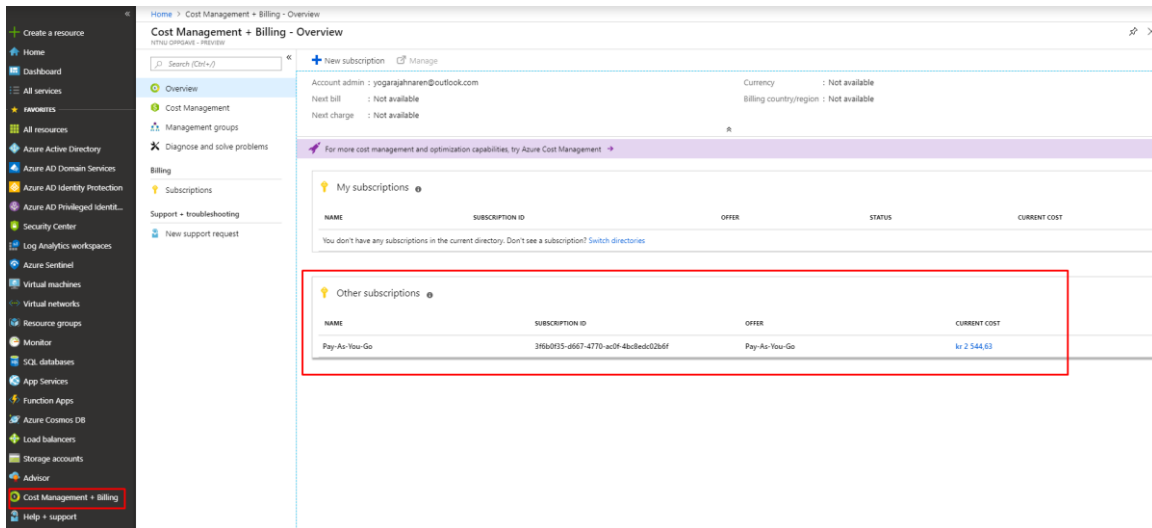


Microsoft Azure er en cloud computing tjeneste som brukes for både utvikling, testing, distribusjon og administrasjon av programvare og tjenester. Dette foregår gjennom Microsoft sine datastentre som ligger spredt verden rundt. Gjennom Microsoft Azure har vi enorme muligheter. SAAS, PAAS, IAAS er noen av mulighetene som Microsoft Azure tilbyr. I tillegg til dette har Microsoft Azure støtte for flere ulike programmeringsspråk, her inkluderer man også annen verktøy og framework.

1. For å komme seg inn på Azure må man navigere seg frem til <https://portal.azure.com>.

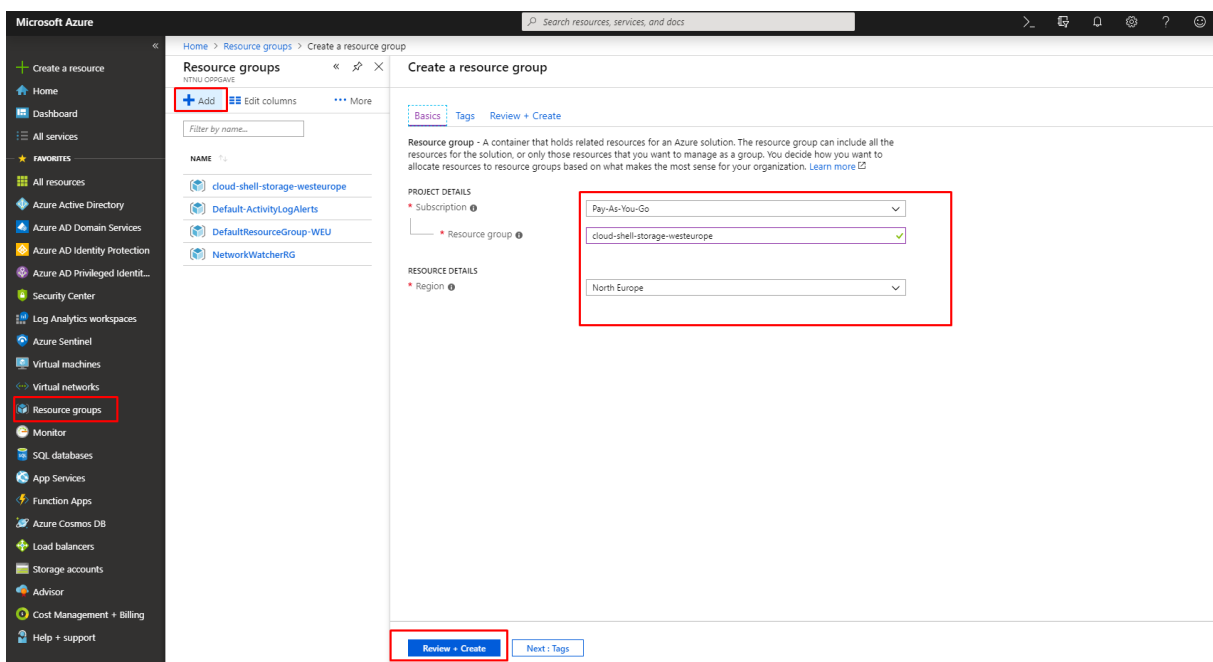
Deretter må man logge seg inn med den tilknyttede brukeren i Azure.

2.1.2 Pay-As-You-Go Subscription



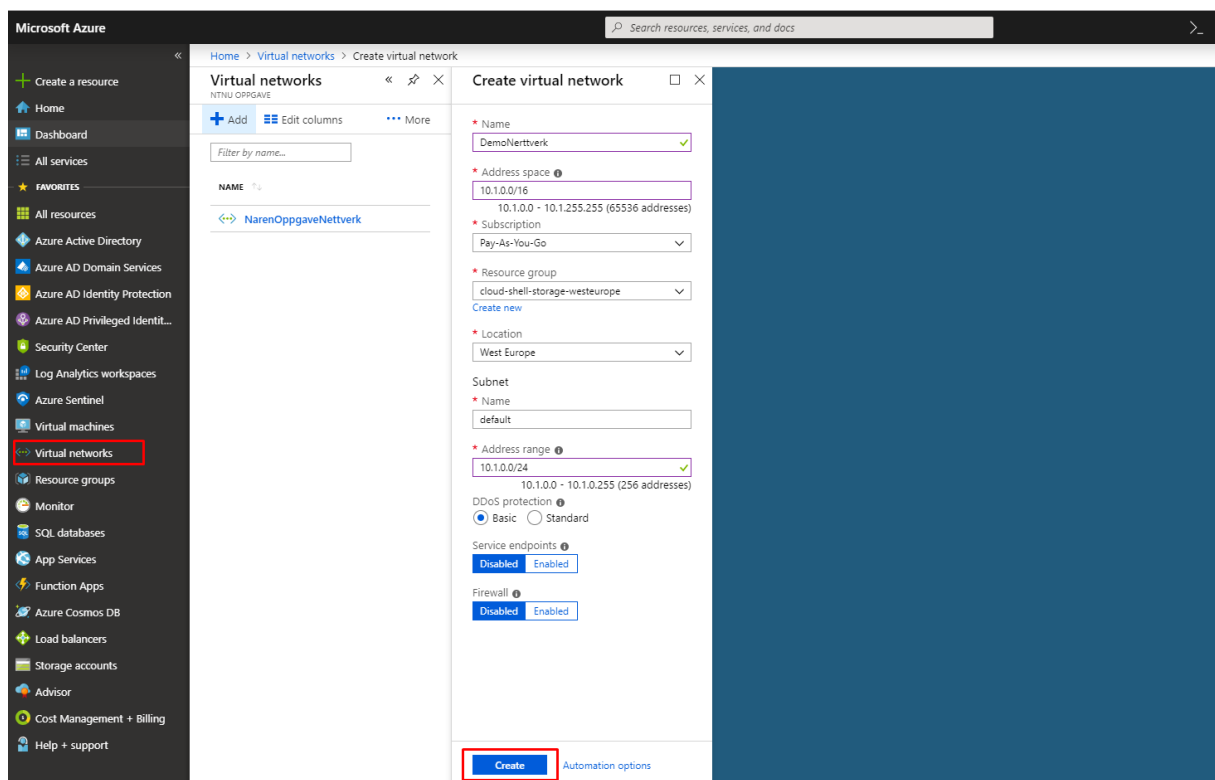
1. For dette prosjektet er det blitt tatt i bruk Pay-As-You-Go Subscription. Dette er allerede satt opp av DNB. Dersom dere vil ta i bruk denne Subscription metoden følg [Microsoft](#) siden.

2.1.3 Resource Groups



1. For å opprette Resource Groups navigerer man seg frem til Resource Groups undermeny under Favorites.
2. Deretter klikker man på Add knappen.
3. Jeg velger videre Pay-As-You-Go Subscription. Deretter setter jeg navnet cloud-shell-storage-westeuropa under Resource group.
4. Region blir satt til North Europe.
5. Deretter klikker jeg på Review + Create knappen.

2.1.4 Virtuelt nettverk



1. For å opprette et virtuelt nettverk i Azure må man navigere seg frem til Virtual Networks under Favorites menyen.
2. Deretter klikker du på Add knappen.
3. Videre legger du inn navn DemoNettverk under Name.
4. Address space blir satt til default: 10.1.0.0/16.
5. Subscription blir satt til Pay-As-You-Go.
6. Resource group blir satt til cloud-shell-storage-westeuropa.

7. Location blir satt til West Europe.
8. Subnet Name er satt til default.
9. Address range under Subnet undermeny blir satt til :10.1.0.0/24.
10. Jeg tikker av for Basic under DDOS Protection.
11. Service Endpoint blir satt til: Disabled.
12. Firewall blir satt til: Disabled.
13. Tilslutt klikker jeg på Create knappen for å opprette nettverket.

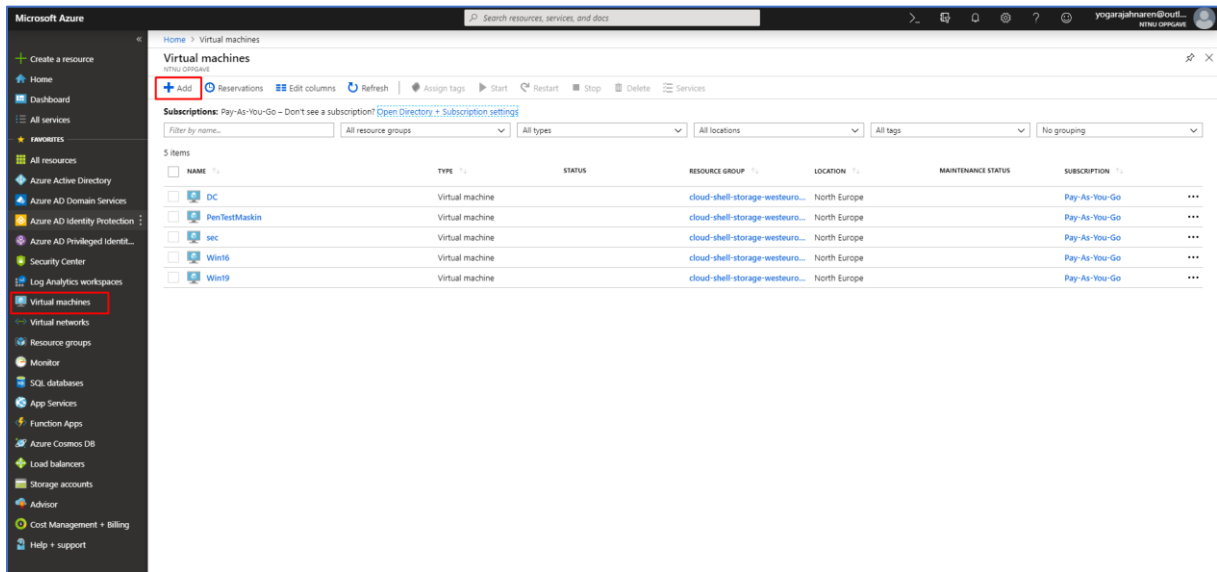
NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
DemoNettverk	cloud-shell-storage-westeuropa	West Europe	Pay-As-You-Go
NarenOppgaveNettverk	cloud-shell-storage-westeuropa	North Europe	Pay-As-You-Go

14. DemoNettverk er nå opprettet og ligger under Virtual Networks menyen.

DEVICE	TYPE	IP ADDRESS	SUBNET
win19550	Network interface	10.0.0.4	default
pentestmaskin944	Network interface	10.0.0.5	default
pentest2linux309	Network interface	10.0.0.6	default
pentest3144	Network interface	10.0.0.7	default
dc694	Network interface	10.0.0.8	default
kali69	Network interface	10.0.0.9	default
sec421	Network interface	10.0.0.10	default
win16317	Network interface	10.0.0.11	default
demomaskin420	Network interface	10.0.0.12	default

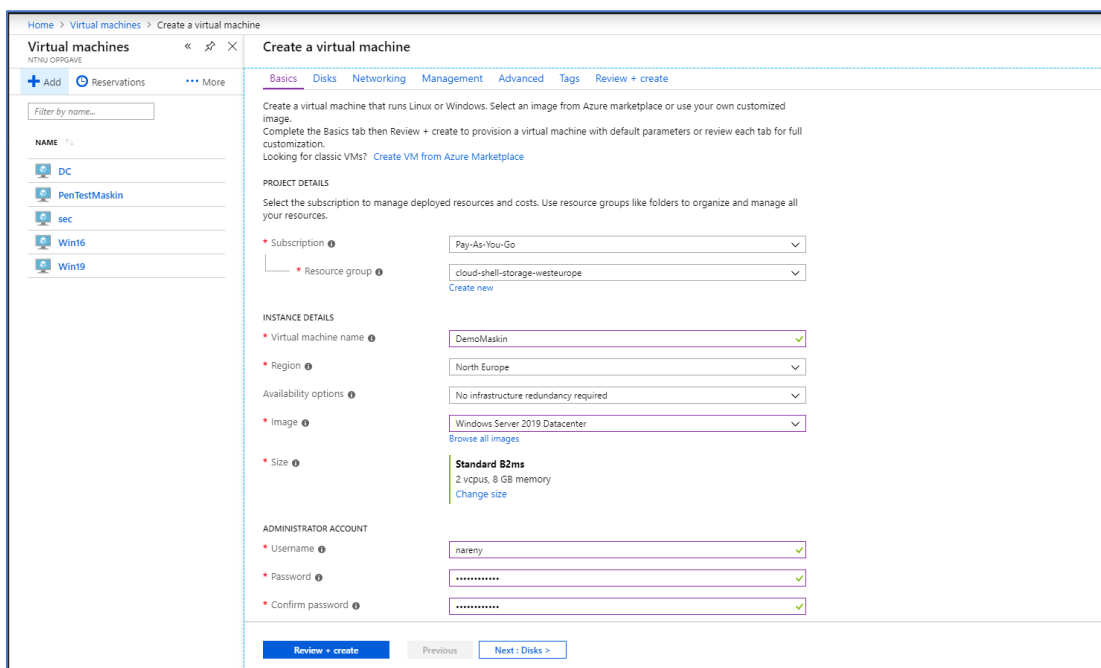
15. Nå er vi inne på dashboardet til nettverket vi har opprettet.

2.1.5 Installasjon av virtuell maskin i Azure



En virtuell maskin kan defineres som en emulering av et datasystem. Her blir det tatt i bruk en ISO fil som fungerer nesten som en ekte datamaskin bare i et eget virtuelt miljø.

1. Når man skal installere en virtuell maskin i Azure, må man gå inn på Virtual machines menyen i Azure. Deretter klikker man på Add for å lage en ny virtuell maskin.



2. Videre får du en meny. Under Basics menyen gjør du følgende. Først velger du riktig

Subscription, i dette tilfelle bruker vi Pay-As-You-Go. Deretter velger du riktig Resource group, som er i dette tilfelle cloud-shell-storage-westeuropa. Deretter skriver du valgt navn på virtuell maskin på Virtual machine name. Videre velger du Region, jeg velger å ta North Europe. Deretter setter du Availability options til No Infrastructure redundancy required. Deretter velger du under Image, ISO filen for den virtuelle maskinen. I dette tilfelle velger jeg å sette denne ISO filen til Windows Server 2019 Datacenter. Deretter klikker jeg på Change Size under size menyen. Videre velger jeg størrelse på 8 GB RAM som er markert i rød boks, deretter klikker jeg på Select knappen. 8GB RAM blir valgt siden, det er en gunstig størrelse for en demo server.

The screenshot shows the 'Create a virtual machine' wizard in the Azure portal. The 'Select a VM size' step is active, displaying a table of available VM sizes. The '82ms' size is highlighted with a red border, indicating it is the selected option. The table provides details for each size, including VCPUS, RAM (GB), DATA DISKS, MAX IOPS, TEMPORARY STORAGE, PREMIUM DISK SUPP., and COST/MONTH (EST.).

VM SIZE	OFFERING	FAMILY	VCPUS	RAM (GB)	DATA DISKS	MAX IOPS	TEMPORARY STORAGE	PREMIUM DISK SUPP.	COST/MONTH (EST.)
B1ts	Standard	General purpose	1	0.5	2	400	1 GB	Yes	Unavailable
B1ms	Standard	General purpose	1	2	2	800	4 GB	Yes	kr 158,17
B1s	Standard	General purpose	1	1	2	400	4 GB	Yes	kr 92,36
82ms	Standard	General purpose	2	8	4	2400	16 GB	Yes	kr 598,86
B2s	Standard	General purpose	2	4	4	1600	8 GB	Yes	kr 323,58
D2s_v3	Standard	General purpose	2	8	4	3200	16 GB	Yes	kr 1 201,34
D4s_v3	Standard	General purpose	4	16	8	6400	32 GB	Yes	kr 2 402,68
D51_v2	Standard	General purpose	1	3.5	4	3200	7 GB	Yes	kr 700,28
D52_v2	Standard	General purpose	2	7	8	6400	14 GB	Yes	kr 1 400,56
D53_v2	Standard	General purpose	4	14	16	12800	28 GB	Yes	kr 2 807,15
B4ms	Standard	General purpose	4	16	8	3600	32 GB	Yes	kr 1 195,30

ADMINISTRATOR ACCOUNT

* Username ⓘ ✓

* Password ⓘ ✓

* Confirm password ⓘ ✓

INBOUND PORT RULES

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports ⓘ None Allow selected ports

Select inbound ports ▾

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

SAVE MONEY

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

* Already have a Windows license? ⓘ Yes No

[Review + create](#) [Previous](#) [Next : Disks >](#)

3. Videre legger jeg inn et brukernavn og sterkt passord under Administrator Account. Deretter under Inbound Port Rules, velger jeg å sette Public Inbound ports til None nå i første omgang. Dette kan vi videre endre senere. Etter dette setter jeg No under Save Money hvor vi har spørsmålet Already have a Windows license. Til slutt klikker jeg på Next: Disks.

Create a virtual machine

[Basics](#)
[Disks](#)
[Networking](#)
[Management](#)
[Advanced](#)
[Tags](#)
[Review + create](#)

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

DISK OPTIONS

* OS disk type

Enable Ultra SSD compatibility (Preview) Yes No
Ultra SSD compatibility is not available for this VM size and location.

DATA DISKS

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	NAME	SIZE (GiB)	DISK TYPE	HOST CACHING
Create and attach a new disk Attach an existing disk				

^ **ADVANCED**

Use managed disks No Yes

Review + create
Previous
Next : Networking >

4. Deretter under Disk Options setter jeg OS disk type til Premium SSD. Under Advanced lar jeg valget ligge på default som er Yes. Deretter klikker jeg på Next: Networking.

Create a virtual machine

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

NETWORK INTERFACE
When creating a virtual machine, a network interface will be created for you.

CONFIGURE VIRTUAL NETWORKS

* Virtual network [Create new](#)

* Subnet [Manage subnet configuration](#)

Public IP [Create new](#)

NIC network security group None Basic Advanced

* Public inbound ports None Allow selected ports

Select inbound ports

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Accelerated networking On Off
The selected VM size does not support accelerated networking.

LOAD BALANCING
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? Yes No

[Review + create](#) [Previous](#) [Next: Management >](#)

5. Under Networking setter jeg Virtual Network til NarenOppgaveNettverk. Deretter setter jeg Subnet til default (10.0.0./24). Videre setter jeg Public IP til valget (new) DemoMaskin-ip. Deretter setter jeg NIC network security group til Basic, som vil være standard valg for NSG. Deretter setter jeg public inbound ports fortsatt til å være None. Videre lar jeg Accelerated networking til å ha valget off. Under Load Balancing blir valget satt til å være No.

Create a virtual machine

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

AZURE SECURITY CENTER
Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
[Learn more](#)

✔ Your subscription is protected by Azure Security Center standard plan.

MONITORING

Boot diagnostics On Off

OS guest diagnostics On Off

IDENTITY

System assigned managed identity On Off

AUTO-SHUTDOWN

Enable auto-shutdown On Off

Shutdown time

Time zone

Notification before shutdown On Off

[Review + create](#) [Previous](#) [Next : Advanced >](#)

6. Under Mangament er kun det som skal endres er Auto-Shutdown. Denne skal settes til On, og Shutdown time skal settes til 19:00:00 med en tidssone Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna. Deretter skal vi sette Notification before shutdown til å være på valget Off. Disse valgene gjøres slik at man får automatisk slått av VMen kl. 19.00 hver eneste dag. Dette blir gjort slik at dersom man glemmer å slå av en virtuell maskin, blir det automatisk gjort til dette tidspunktet noe igjen kan være smart for å spare penger. Resterende øvrige valg blir satt til å være off.

Create a virtual machine


[Basics](#) [Disks](#) [Networking](#) [Management](#) **Advanced** [Tags](#) [Review + create](#)

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

EXTENSIONS
Extensions provide post-deployment configuration and automation.

Extensions ⓘ [Select an extension to install](#)

CLOUD INIT
Cloud init is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files or to configure users and security. [Learn more](#)

 The selected image does not support cloud init.

[Review + create](#) [Previous](#) [Next : Tags >](#)

7. Under Advanced, lar vi alt stå på default og klikker på next: Tags.

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

NAME	VALUE	RESOURCE
<input type="text"/>	:	7 selected

[Review + create](#) [Previous](#) [Next : Review + create >](#)

8. Under Tags, lar vi alt stå på default og klikker på next: Review + create.

Create a virtual machine

✓ Validation passed

Basics Disks Networking Management Advanced Tags **Review + create**

PRODUCT DETAILS

Standard B2ms
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ
0.8049 NOK/hr
[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

BASICS

Subscription Pay-As-You-Go
Resource group cloud-shell-storage-westeuope
Virtual machine name DemoMaskin
Region North Europe
Availability options No infrastructure redundancy required
Username nareny
Public inbound ports None
Already have a Windows license? No

DISKS

OS disk type Premium SSD
Use managed disks Yes

NETWORKING

Virtual network NarenOppgaveNettverk
Subnet default (10.0.0.0/24)

Create Previous Next [Download a template for automation](#)

9. Nå kan du endelig installere din virtuelle maskin ved å klikke på create knappen. Det forutsetter at valideringen blir passert og får en godkjent melding som på dette skjermbilde her.

Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20190323071624 - Overview

CreateVm-MicrosoftWindowsServer.WindowsServer-201-20190323071624 - Overview

Deployment

Search (Ctrl+J)

Delete Cancel Redeploy Refresh

Your deployment is underway

Check the status of your deployment, manage resources, or troubleshoot deployment issues. Pin this page to your dashboard to easily find it next time.

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsServer-201-20190323071624
Subscription: Pay-As-You-Go
Resource group: cloud-shell-storage-westeuope

DEPLOYMENT DETAILS (Download)

Start time: 23-3-2019, 07:25:03
Duration: 21 seconds
Correlation ID: c55d1824-c13f-42e7-bfd7-cda44b5c9147

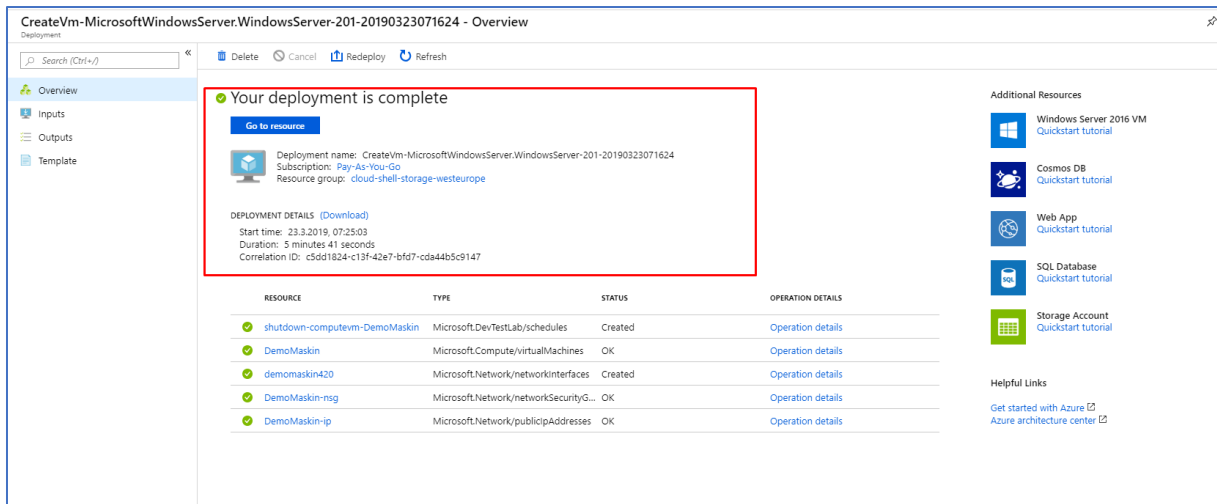
RESOURCE	TYPE	STATUS	OPERATION DETAILS
DemoMaskin	Microsoft.Compute/virtualMachines	Created	Operation details
demomaskin420	Microsoft.Network/networkInterfaces	Created	Operation details
DemoMaskin-nsg	Microsoft.Network/networkSecurityG...	OK	Operation details
DemoMaskin-ip	Microsoft.Network/publicIPAddresses	OK	Operation details

Additional Resources

- Windows Server 2016 VM [Quickstart tutorial](#)
- Cosmos DB [Quickstart tutorial](#)
- Web App [Quickstart tutorial](#)
- SQL Database [Quickstart tutorial](#)
- Storage Account [Quickstart tutorial](#)

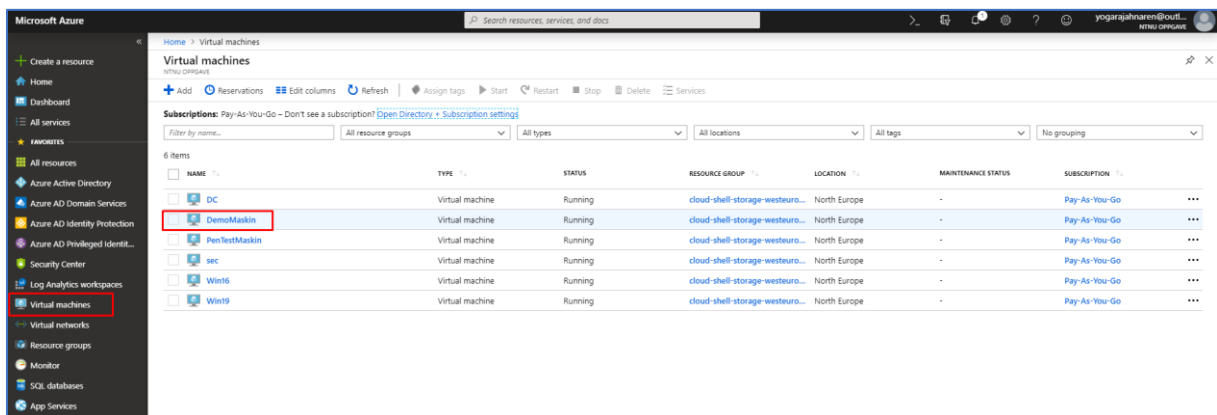
Helpful Links

- [Get started with Azure](#)
- [Azure architecture center](#)

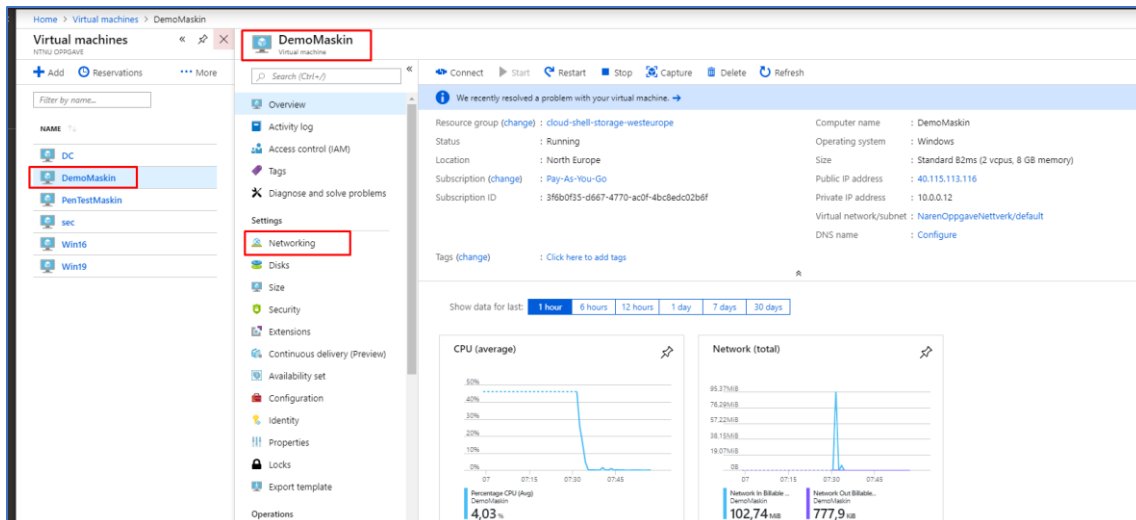


10. Når du klikker på Create blir du videre dirigert til denne siden hvor man har statusen til installasjonen av virtuelle maskinen din. Skjerm bilde ovenfor viser at virtuell maskin er installert.

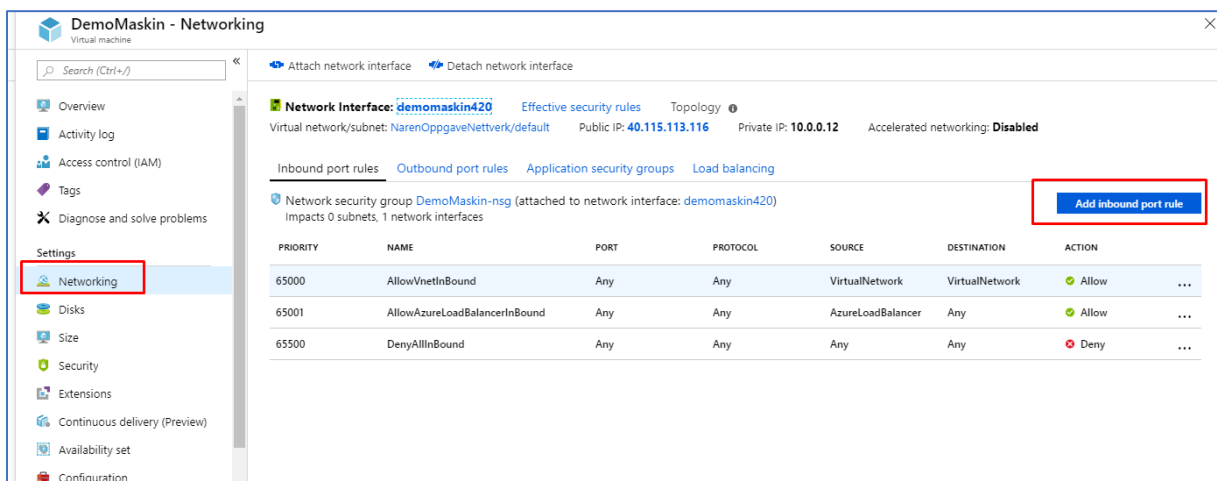
2.1.5.1 Remote Desktop Access



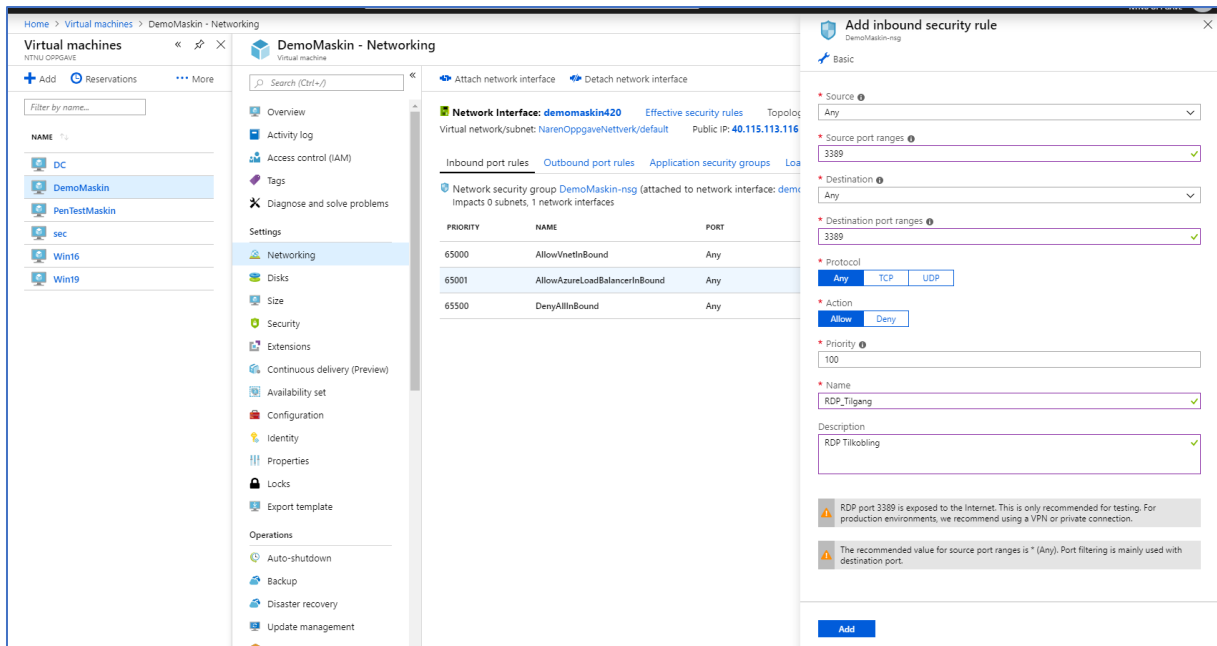
1. Når vi går tilbake til Virtual machines menyen finner vi nå DemoMaskin virtuelle maskinen som vi har opprettet tidligere.



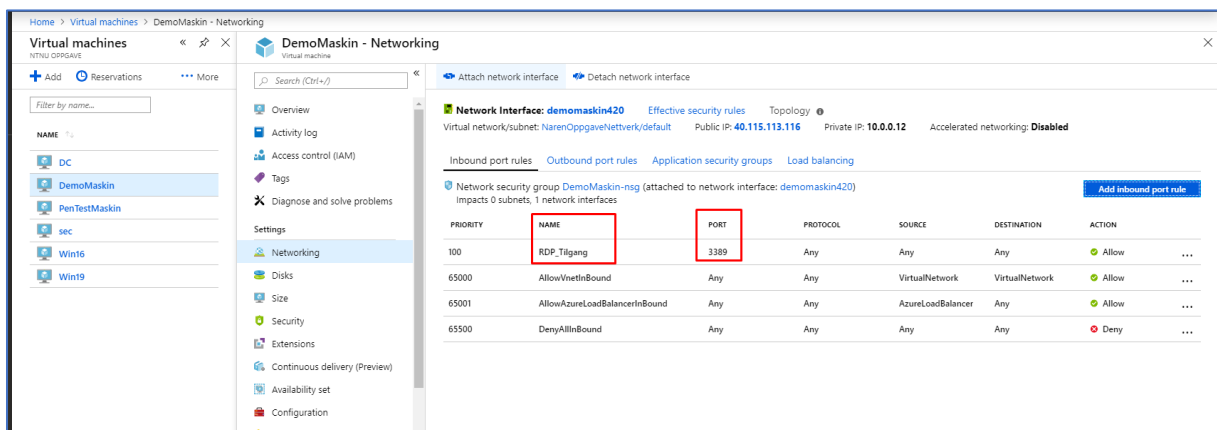
2. Nå skal vi videre åpne opp for RDP tilkobling på DemoMaskin. Dette gjør vi ved å gå inn på Virtual Machines menyen, deretter klikker på DemoMaskin, videre klikker vi på Networking under Settings.



3. Deretter klikker vi på Add Inbound port rule.

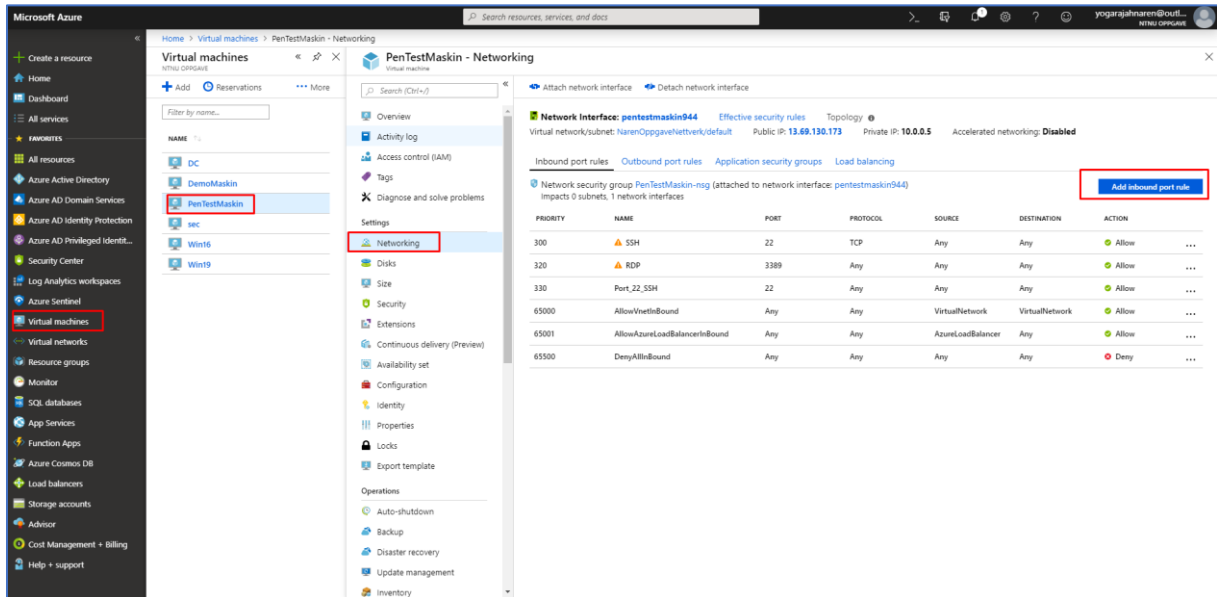


4. Her setter vi Source, til å være Any. Deretter legger vi inn **3389** under Source port ranges. Videre setter vi Destination til Any. Deretter lar vi Destination port ranges til å være på 3389. Videre setter vi Any under Protocol. Deretter setter vi Allow under Action. Priority blir satt til 100. Navnet blir satt til RDP_Tilgang. Tilslutt klikker vi på Add.



5. Nå ser vi at DemoMaskin har blitt åpnet for RDP tilgang på port 3389.

2.1.5.2 SSH Port



1. Videre vil jeg også åpne for SSH port i PenTestMaskin.
2. Dette gjør jeg ved å navigere meg til Virtual machines meny under Favorites.
3. Deretter klikker jeg på PenTestMaskin.
4. Videre klikker jeg på Networking.
5. Deretter klikker jeg på Add inbound port rule.

Add inbound security rule
PenTestMaskin-nsg

Basic

* Source: Any

* Source port ranges: *

* Destination: Any

* Destination port ranges: 22

* Protocol: Any | TCP | UDP

* Action: Allow | Deny

* Priority: 340

* Name: Port_22_SSH_TILGANG

Description:

Add

6. Deretter setter jeg Source til Any.

7. Source port ranges skal stå på default. Dette vil si at man ikke trenger å endre noe her.

8. Destination blir satt til Any.

9. Destination port ranges blir satt til 22.

10. Protocol blir satt til Any.

11. Action blir satt til Allow.

12. Priority skal stå på default.

13. Name blir satt til «Port_22_SSH_TILGANG».

14. Tilslutt klikker jeg på Add knappen.

340	Port_22_SSH_TILGANG	22	Any	Any	Any	Allow	...
-----	---------------------	----	-----	-----	-----	-------	-----

15. Her ser vi at Port 22 er åpnet for tilgang i PentTestMaskin.

2.2 Azure Active Directory

Azure Active Directory er et Identity og access mangament tjeneste som er hovedsakelig cloud basert. Med Azure Active Directory har de ansatte i en organisasjon eller studenter i skolesammenheng mulighet til å få tilgang til eksterne ressurser ved logge seg inn på sine brukere gjennom Microsoft Office 365, eller Azure portal og ikke minst andre SaaS applikasjoner. Man har også mulighet til å ta i bruk Azure AD for å få tilgang til interne ressurser som f.eks programvare på ditt lokale nettverk i bedrift/skole eller også andre utviklede apper som ligger i din egen organisasjon.

2.2.1 Azure AD Premium P2 Edition

The screenshot displays the Azure Active Directory Premium P2 Overview page for the domain '09999.no'. The main heading is 'NTNU OPPGAVE' with a sub-heading 'Azure AD Premium P2'. A line graph titled 'Sign-ins' shows activity from March 3rd to 24th. The 'What's new in Azure AD' section lists 16 services, including 'App Proxy - Access Control' and 'New Federated Apps available in Azure AD app gallery - January 2019'. The right sidebar shows the user's role as 'Global administrator and 27 other roles' and 'Azure AD Connect sync' status as 'Enabled'.

1. Azure AD Premium P2 er blitt satt opp når DNB konfigurerte Azure miljøet til meg. Azure Active Directory Premium P2 kan aktiveres fra [Microsoft](#) sin side til Azure miljøet ditt.

2.2.2 Azure Active Directory Users

The screenshot shows the Azure Active Directory Overview page for the directory 'NTNU OPPGAVE'. The left-hand navigation menu is visible, with the 'Users' option under the 'Manage' section highlighted with a red box. The main content area displays a line graph for 'Sign-ins', a 'What's new in Azure AD' section, and a list of services with checkboxes.

1. For å opprette Active Directory bruker må du gå inn på menyen Active Directory. Deretter går du videre til Users under Manage.

The screenshot shows the 'Users - All users' page in Azure Active Directory. The '+ New user' button is highlighted with a red box. The page displays a list of users with the following columns: NAME, USER NAME, USER TYPE, and SOURCE.

NAME	USER NAME	USER TYPE	SOURCE
Johan Fredrik (local)	johan.fredrik.juell@09999.no	Member	Microsoft Account
johanfj	johanfj@efnet.no	Guest	External Azure Active Directory
naren	naren@09999.no	Member	Azure Active Directory
Naren Y	narenyoga@johanfredrikjuell09999.onmicrosoft.com	Member	Windows Server AD
On-Premises Directory Synchronization Service Ac...	Sync_DCWIN16_57215d934e9d@johanfredrikjuell09999.on...	Member	Windows Server AD
yogarahnaren	yogarahnaren@outlook.com	Guest	Microsoft Account

2. Videre klikker du på New user for å legge til en ny bruker.

Home > NTNU OPPGAVE > Users - All users > User

User

NTNU OPPGAVE

* Name ?
DemoBruker ✓

* User name ?
demobruker@09999.no ✓

Profile ?
Configured >

Properties ?
Default >

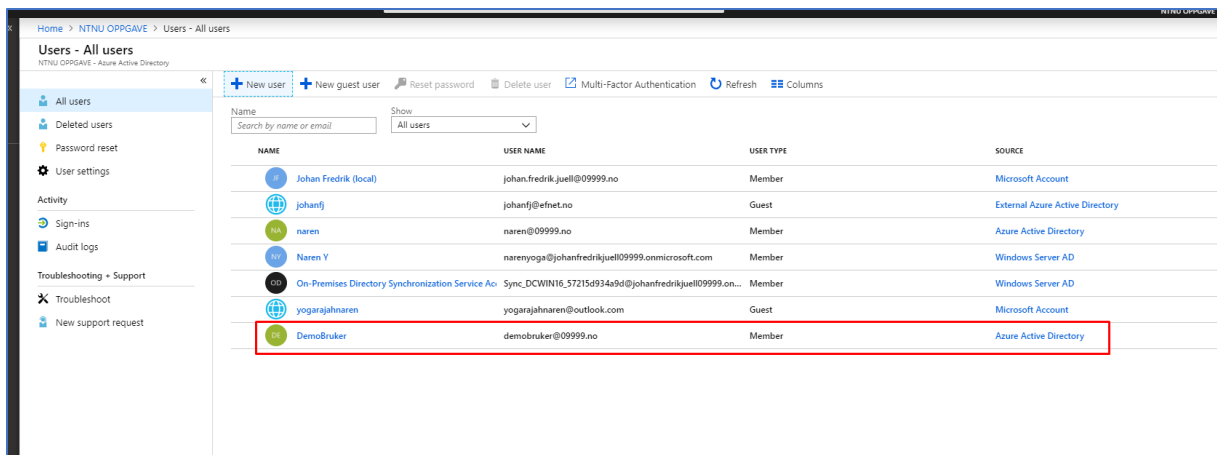
Groups ?
0 groups selected >

Directory role
User >

Password
.....
 Show Password

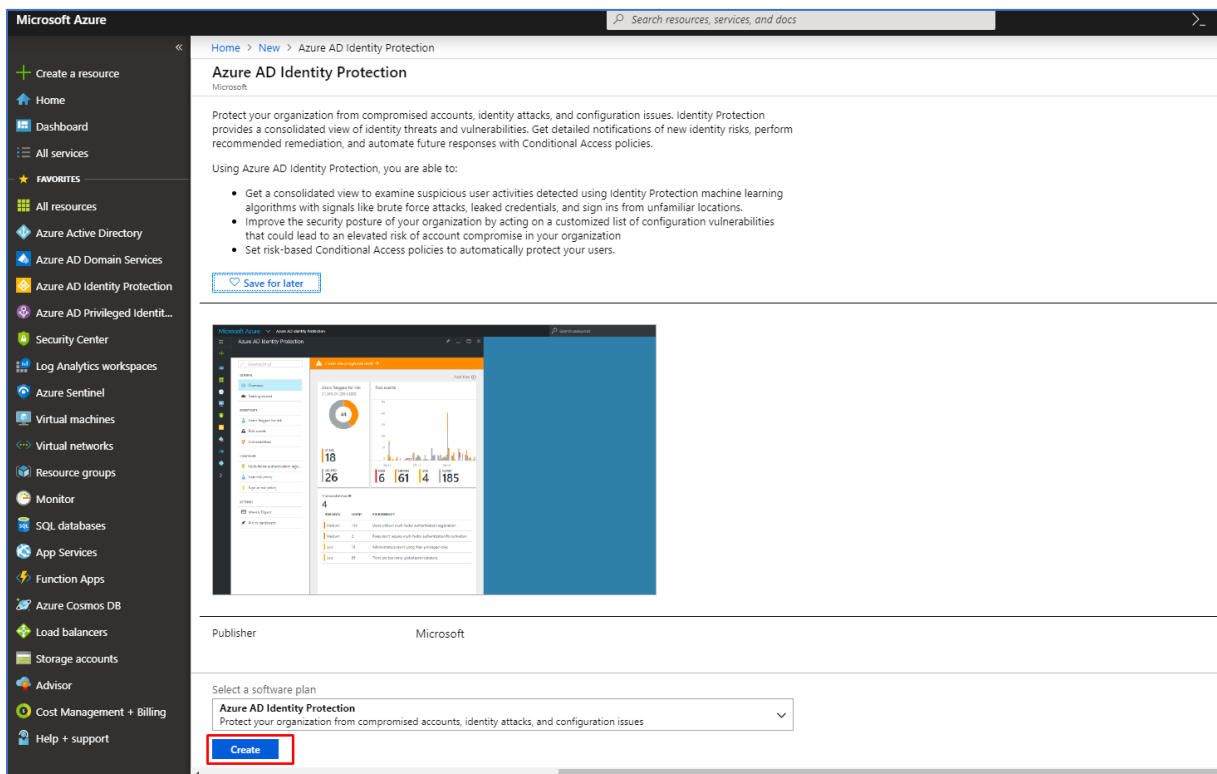
Create

3. Den nye brukeren må være en del av et godkjent domene. Du legger inn både navn og brukernavn og deretter klikker du på create knappen. Passord blir tildelt automatisk. I dette prosjektets tilfelle har DNB allerede opprettet et domene kalt 09999.no til meg.



4. Her ser du at DemoBruker er opprettet og ligger under all users i Azure Active Directory.

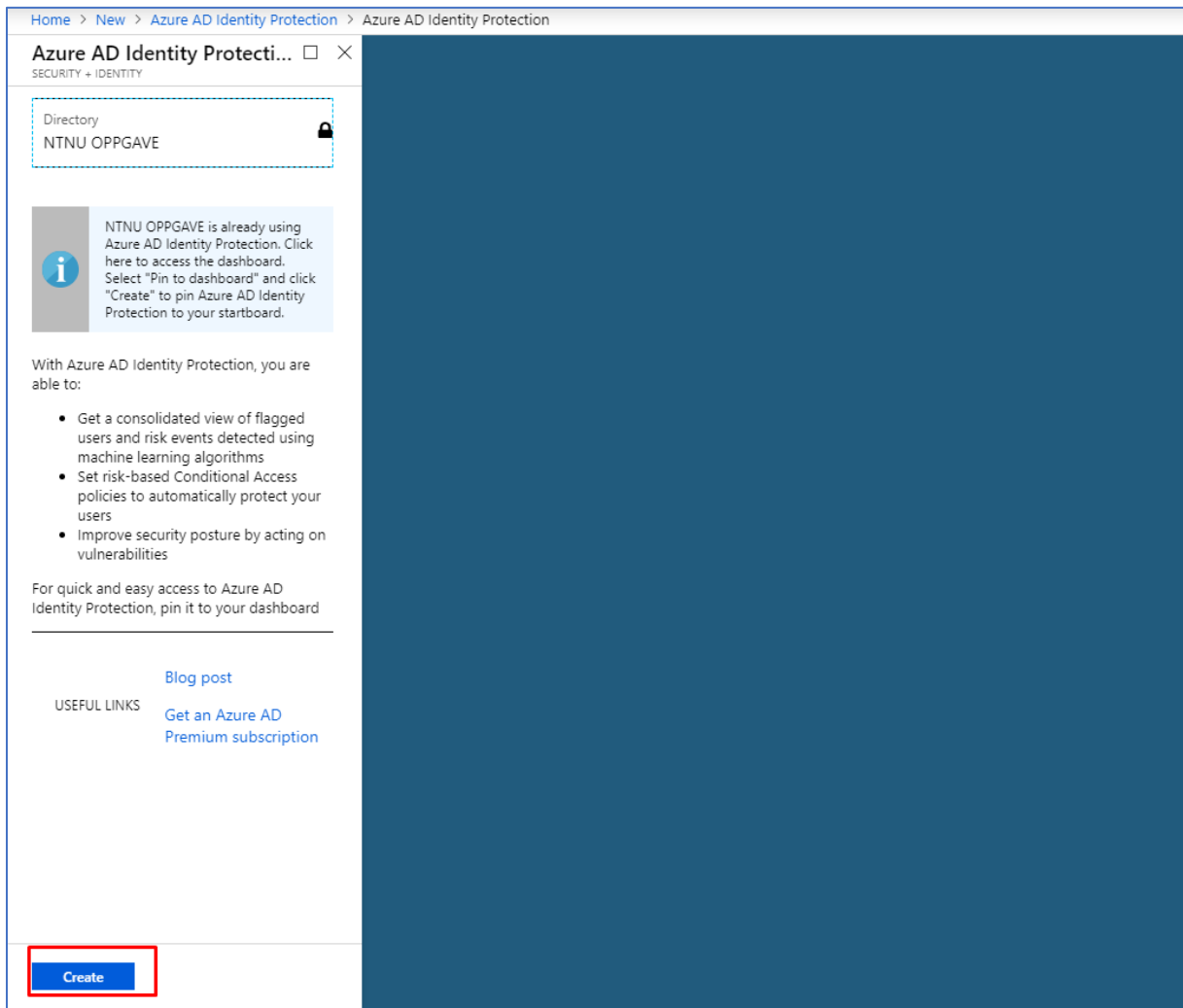
2.2.3 Azure Active Directory Identity Protection



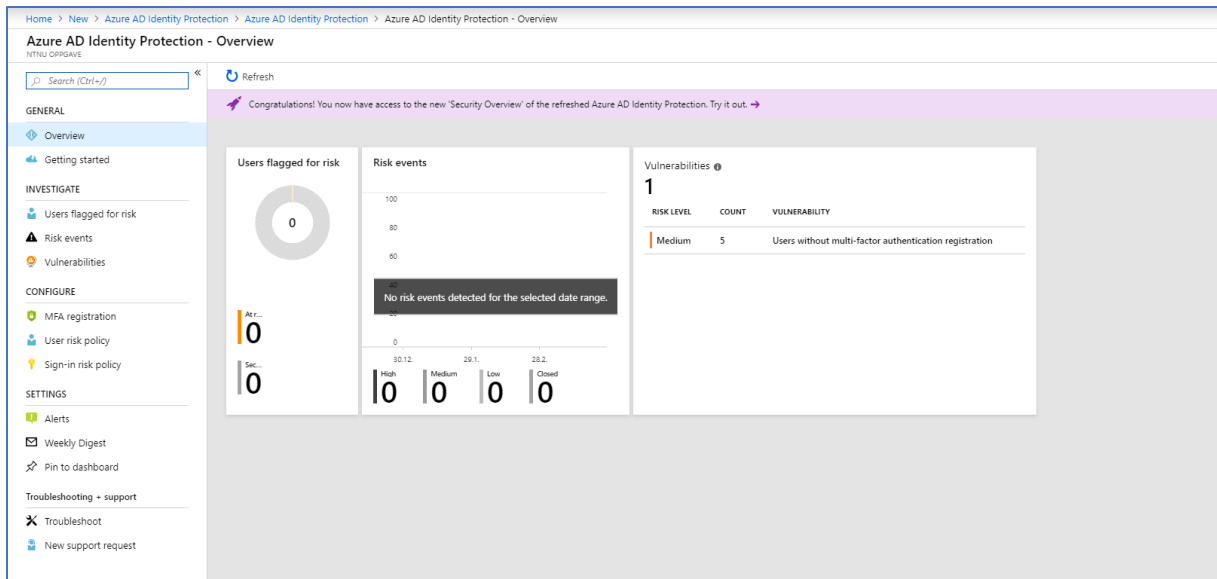
Azure Active Directory Identity Protection er en cloudbasert tjeneste i Microsoft Azure som gir deg mulighet til å gjenkjenne potensielle sårbarheter som er med på å påvirke identiteter til din organisasjon. Identity Protection gir også mulighet til å sette opp automatiske responser tilknyttet til mistenkelige handlinger som blir utført og er knyttet til identiteter som foreligger

i selve organisasjonen. Ikke minst har man med Azure Identity Protection mulighet til å etterforske mistenkelige hendelser og man har mulighet til å sette i gang aktuelle tiltak for å løse disse truslene/hendelsene.

1. For å sette opp Active Directory Identity Protection må vi først legge inn dette fra Marketplace i Azure. Dette gjør vi ved å søke etter Azure Active Directory Identity Protection, deretter klikker man på create knappen.

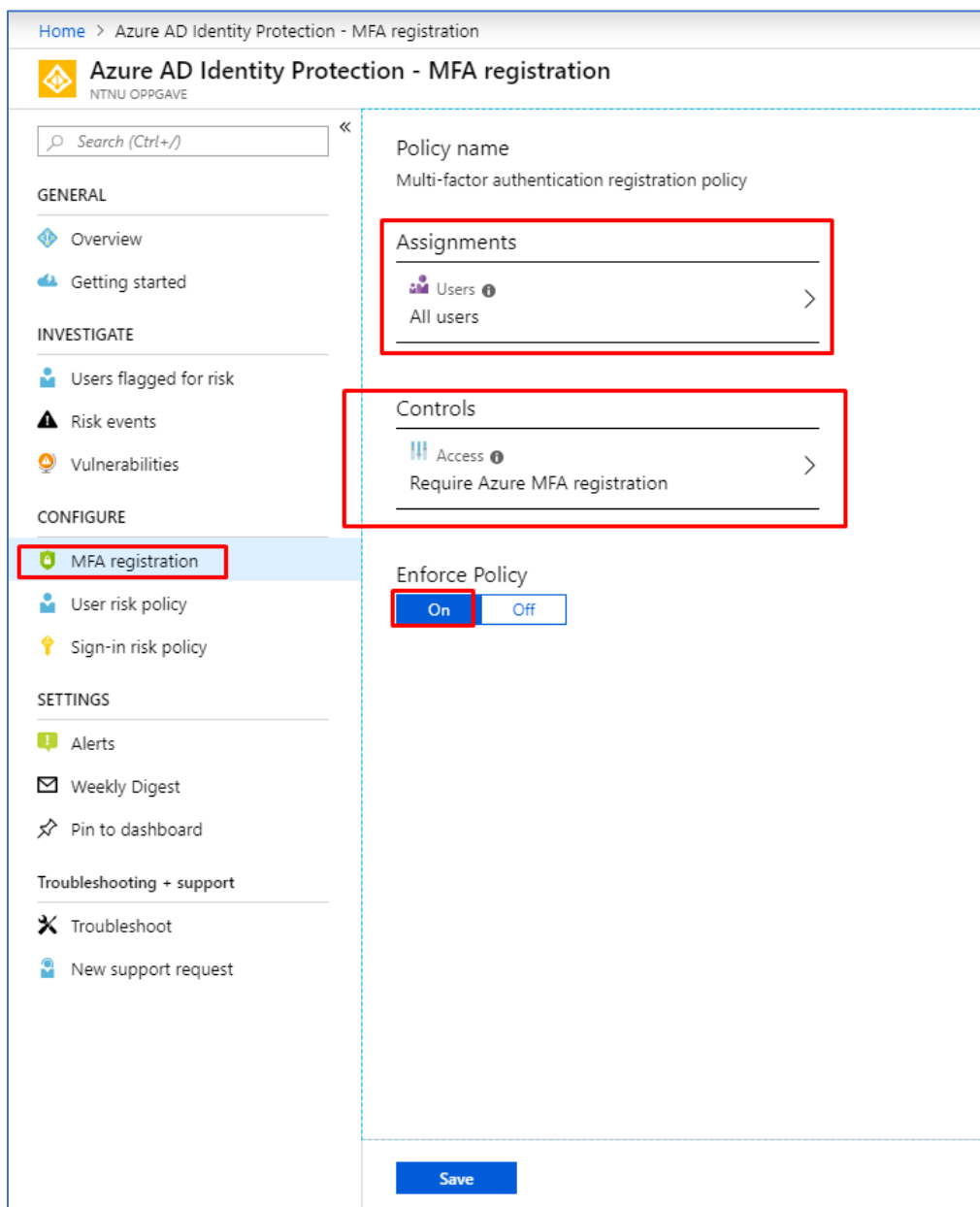


2. Videre klikker du på Create knappen etter å ha dobbelt sjekket om du er i riktig Directory Path. I dette tilfelle er vi i NTNU OPPGAVE directory Path noe som stemmer for meg. NTNU OPPGAVE Directory har allerede blitt satt opp fra DNBs side til meg.



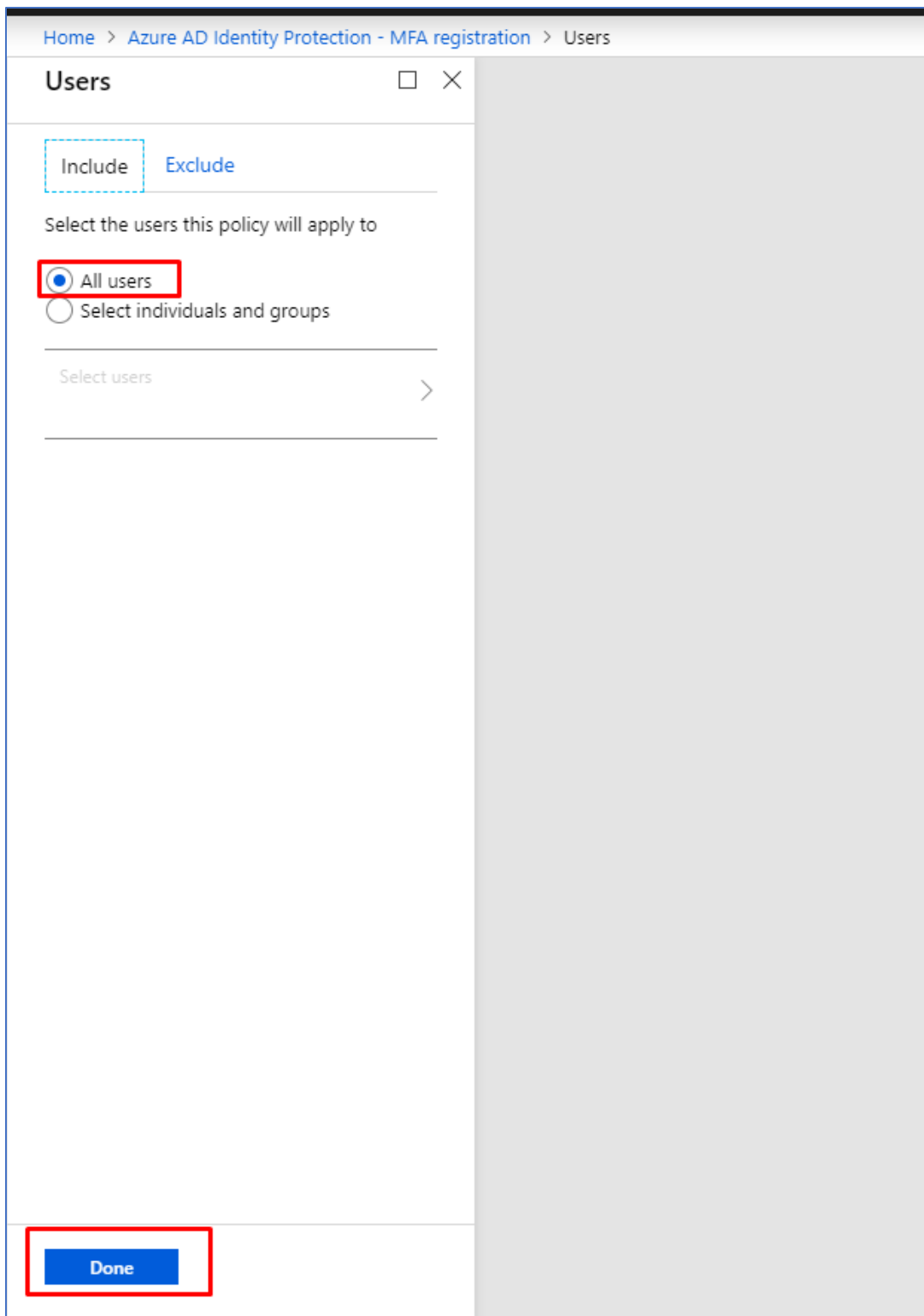
3. Nå er installasjonen av Identity Protection ferdig. Du ser nå dashboardet til Identity Protection.

2.2.3.1 Azure Multi Factor Authentication

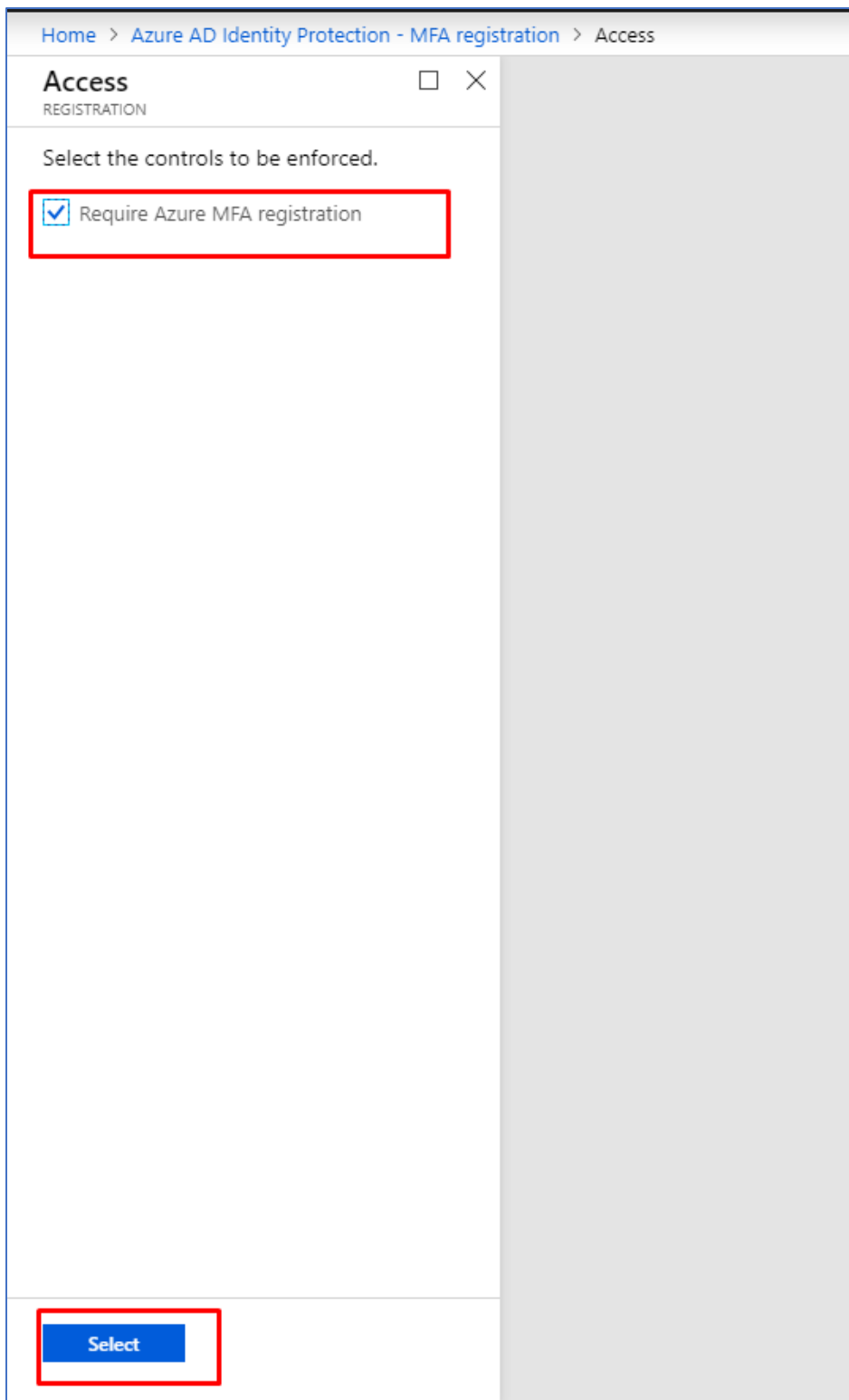


Azure Multi Factor Authentication er en tjeneste i Microsoft Azure Identity Protection som gir deg mulighet til å sikre tilgangen til dine data og applikasjoner gjennom å tilby ekstra sikkerhet ved å spørre om en ekstra autentisering etter den aktuelle innloggingen. Denne ekstra autentiseringen kan gis gjennom Microsoft Authenticator app, SMS og tale oppringing til din mobiltelefon.

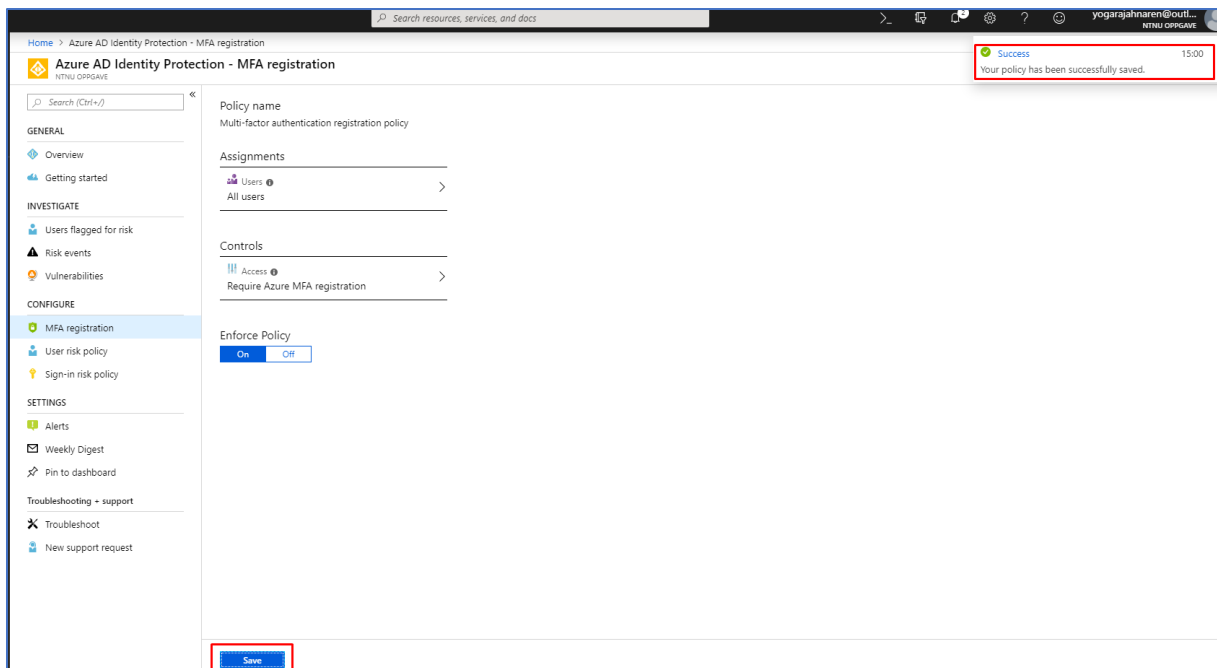
1. For å sette opp Multi Factor Authentication på alle brukere i Azure Active Directory må du først navigere deg til MFA registration under Identity Protection menyen. Deretter velger jeg å klikke på Users undermeny.



2. Jeg velger å sette policyen for alle brukere i Azure AD. Det er slike små policyer som vil utgjøre større forskjell i en eventuell trusselsituasjon en bedrift kan møte på og dermed er det viktig å sikre alle brukere i miljøet.



2. Videre etter å ha lagret øvre endringer, navigerer jeg meg videre til Controls. Deretter tikker jeg av for «Require Azure MFA registration». Det er viktig å huske på Select knappen, det er kun da valget blir satt til live.



3. Videre tikker jeg av for On under Enforce Policy og lagrer tilslutt.

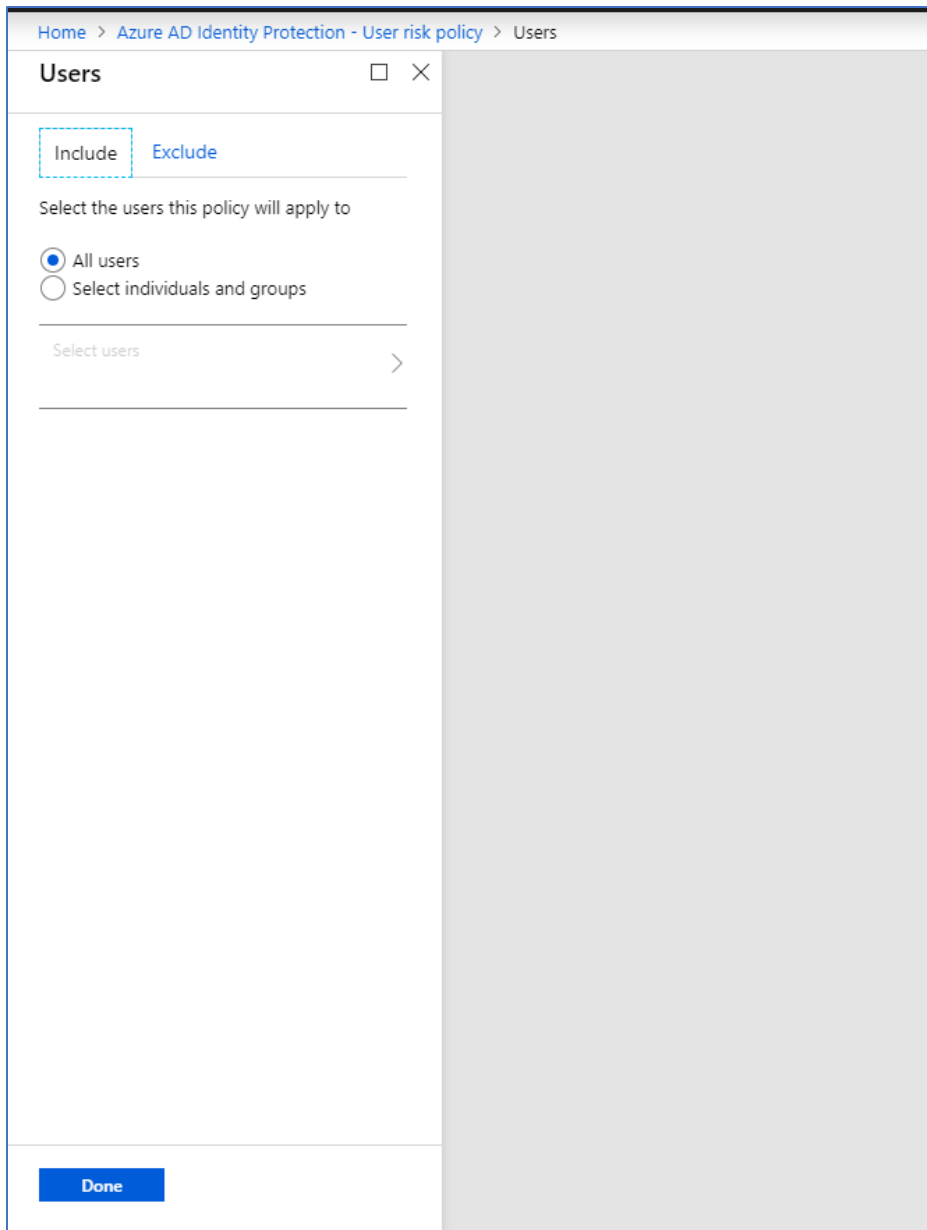
4. Vi kan se etter en liten tid at lagringen av policy har foregått suksessfullt.

2.2.3.2 User Risk Policy

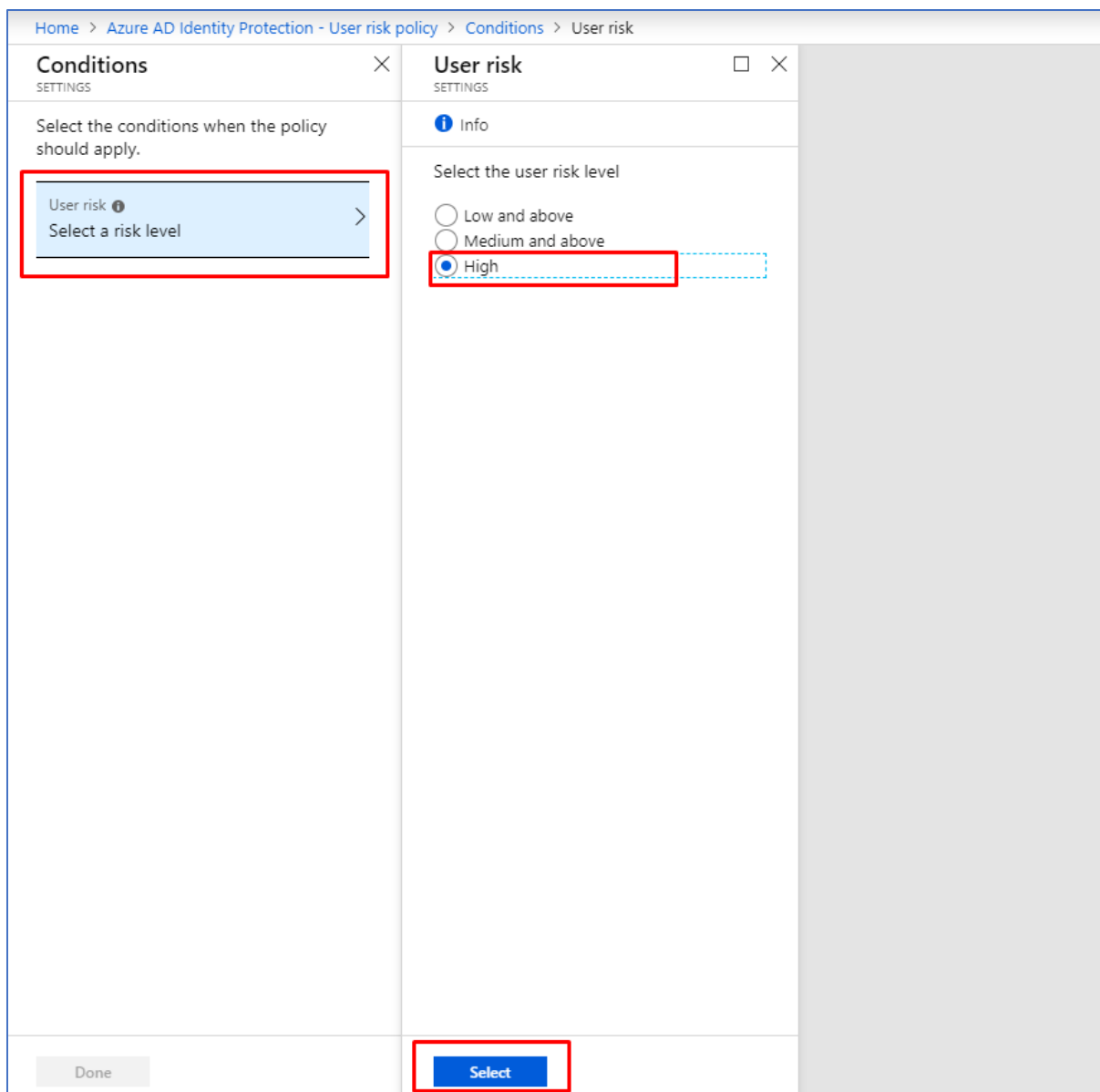
The screenshot shows the Azure AD Identity Protection - User risk policy configuration page. The left sidebar is dark-themed and contains a list of services, with 'Azure AD Identity Protection' highlighted in red. The main content area is light-themed and displays the following information:

- Policy name:** User risk remediation policy
- Assignments:**
 - Users: All users
 - Conditions: Select conditions
- Controls:**
 - Access: Select a control
- Review:**
 - Estimated impact: Number of users impacted
- Enforce Policy:** On/Off toggle (currently set to Off)

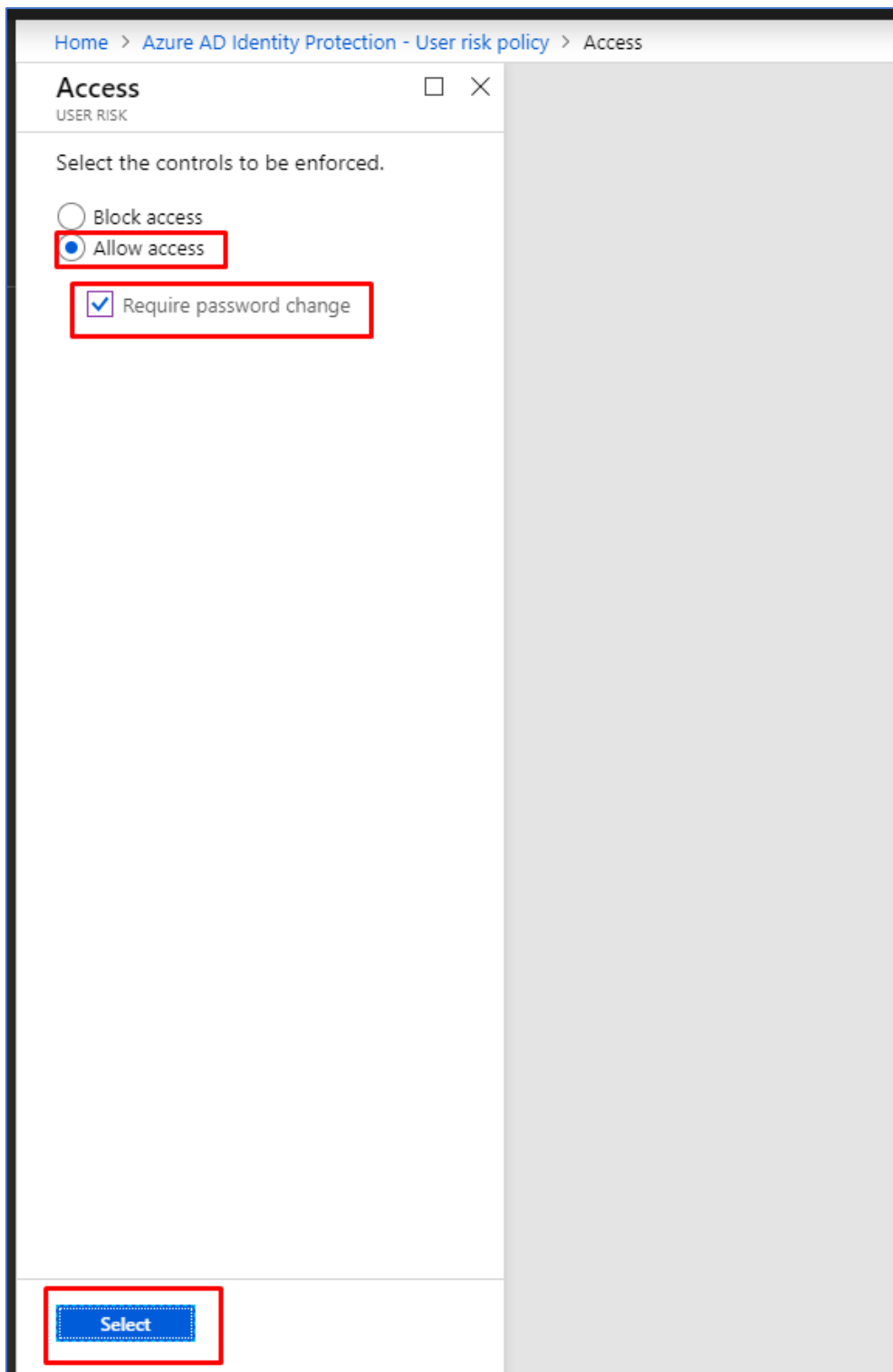
1. Under Azure Identity Protection, setter jeg opp User risk policy. Jeg starter med å definere hvilke brukere som skal komme under denne policyen.



2. Jeg vælger at alle brugere i Azure skal være konfigureret for User risk policy.




3. Videre under Conditions, velger jeg å definere denne til å være High og det er da det skal settes i gang umiddelbare tiltak.




4. Deretter under Access vil jeg helst ikke blokkere full tilgang. Jeg setter opp for å tillate tilgang for brukerne men på en betingelse at passordene blir gjenopprettet.


Policy name
User risk remediation policy

Assignments


 Users ⓘ >
All users

 Conditions ⓘ >
User risk

Controls

 Access ⓘ >
Require password change

Review

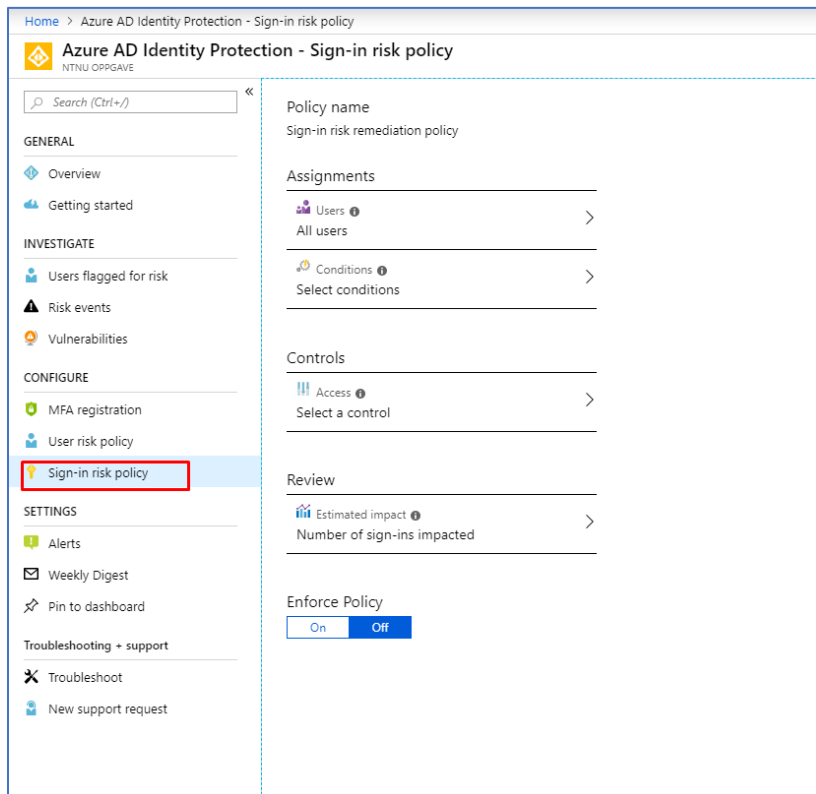
 Estimated impact ⓘ >
Number of users impacted

Enforce Policy

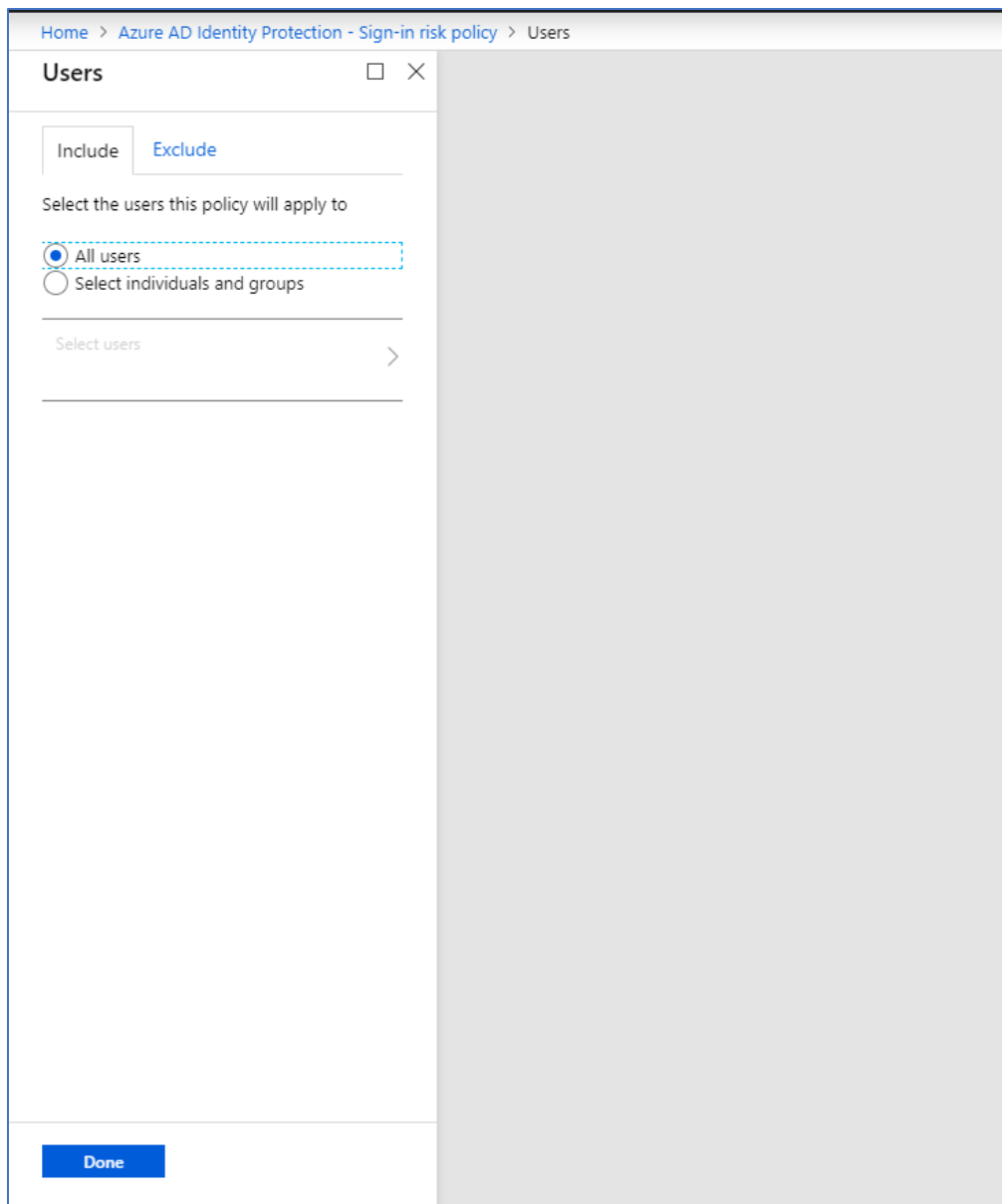
On Off

5. Enforce Policy blir tikket av til On.

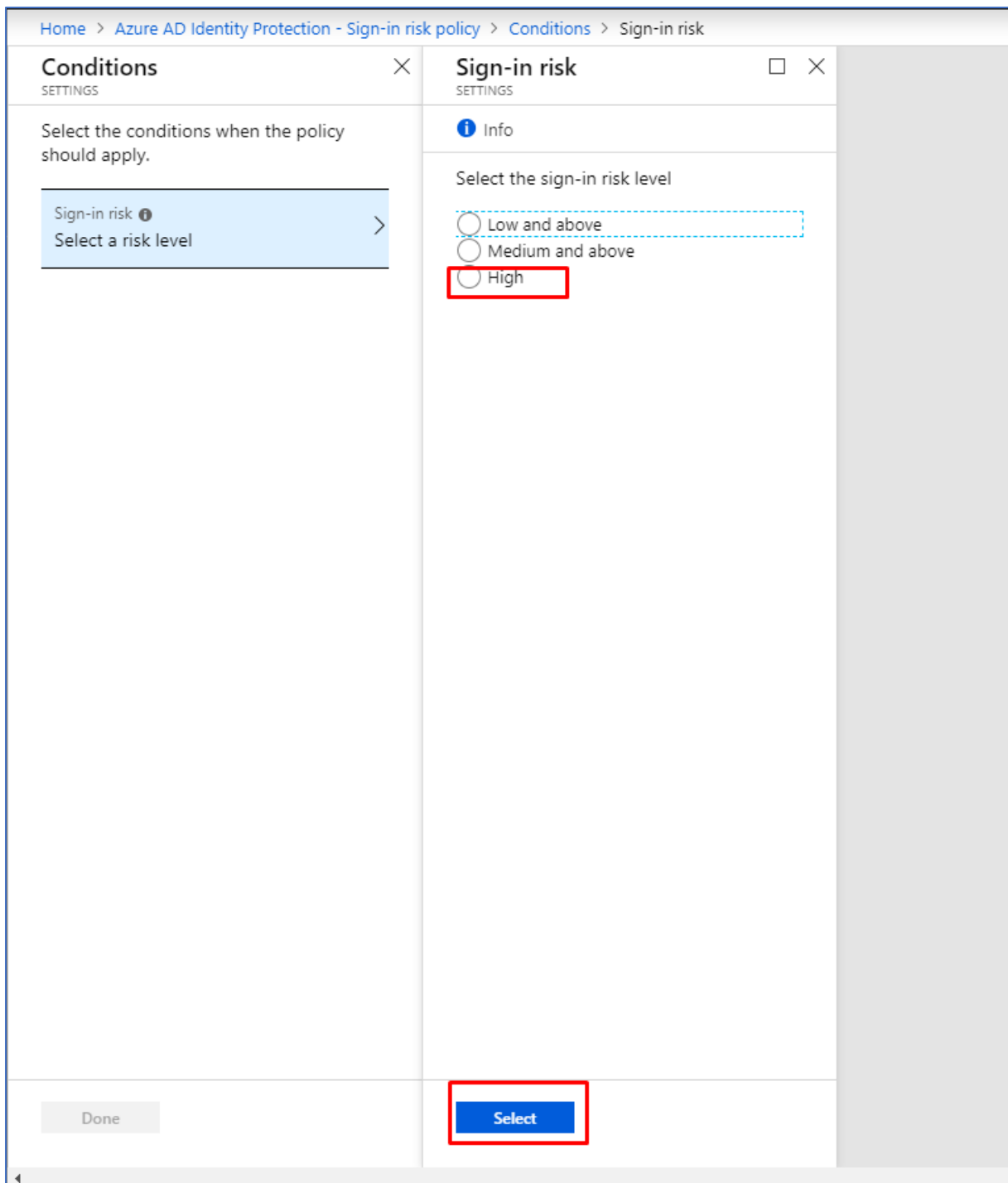
2.2.3.3 Sign-in risk policy



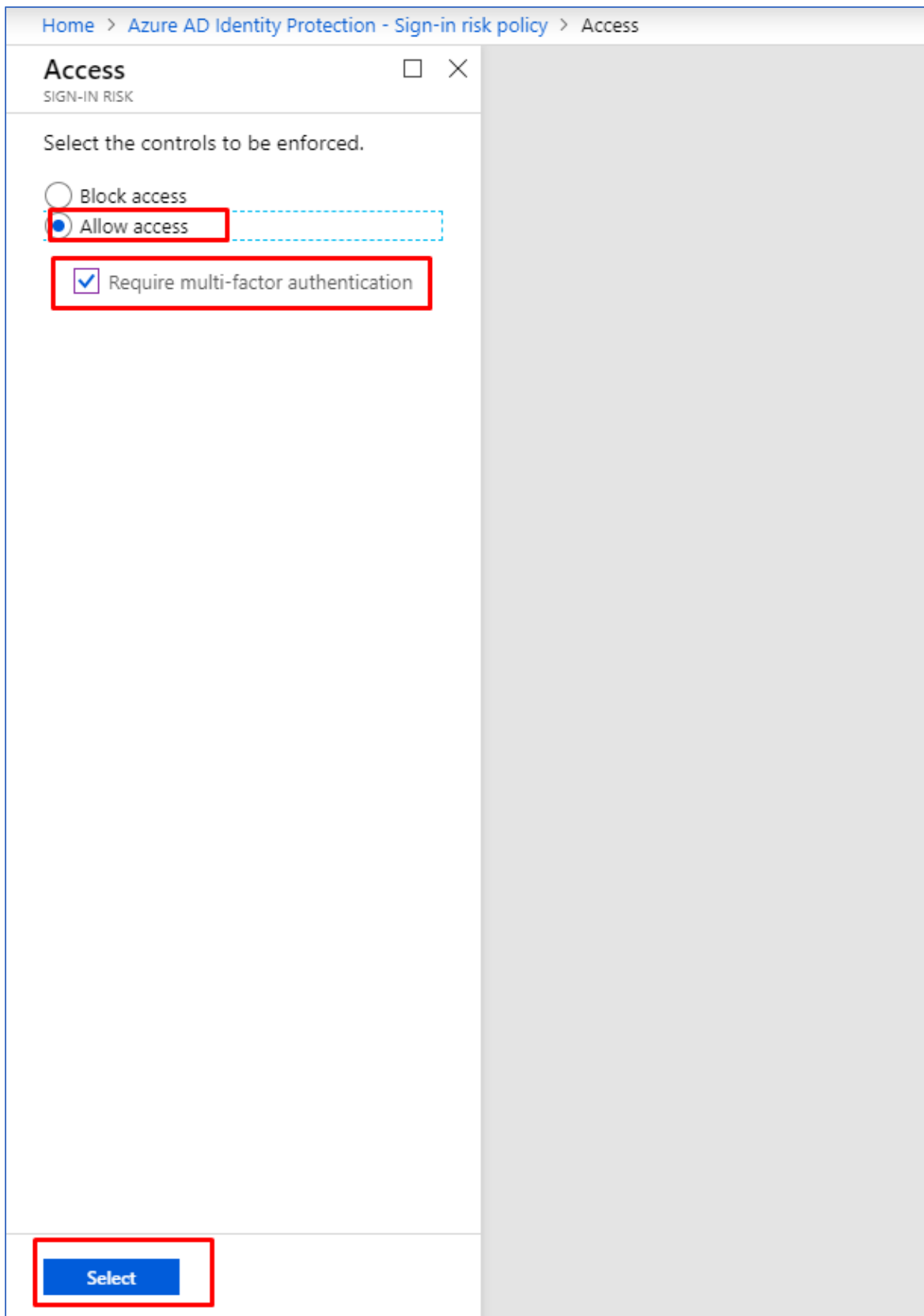
1. For å sette Sign-in risk policy, må vi navigere oss frem til Sign-in risk policy undermeny under Configure. Deretter starter jeg med å definere brukerne i neste skjermbilde.



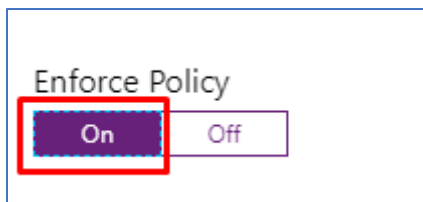
2. Jeg velger å tikke all users slik at man får kjørt sign-in policy på alle brukerne i Azure miljøet mitt.



3. Videre velger jeg å sette Conditions til å ha krav til å være på High før denne policyen skal settes i gang.

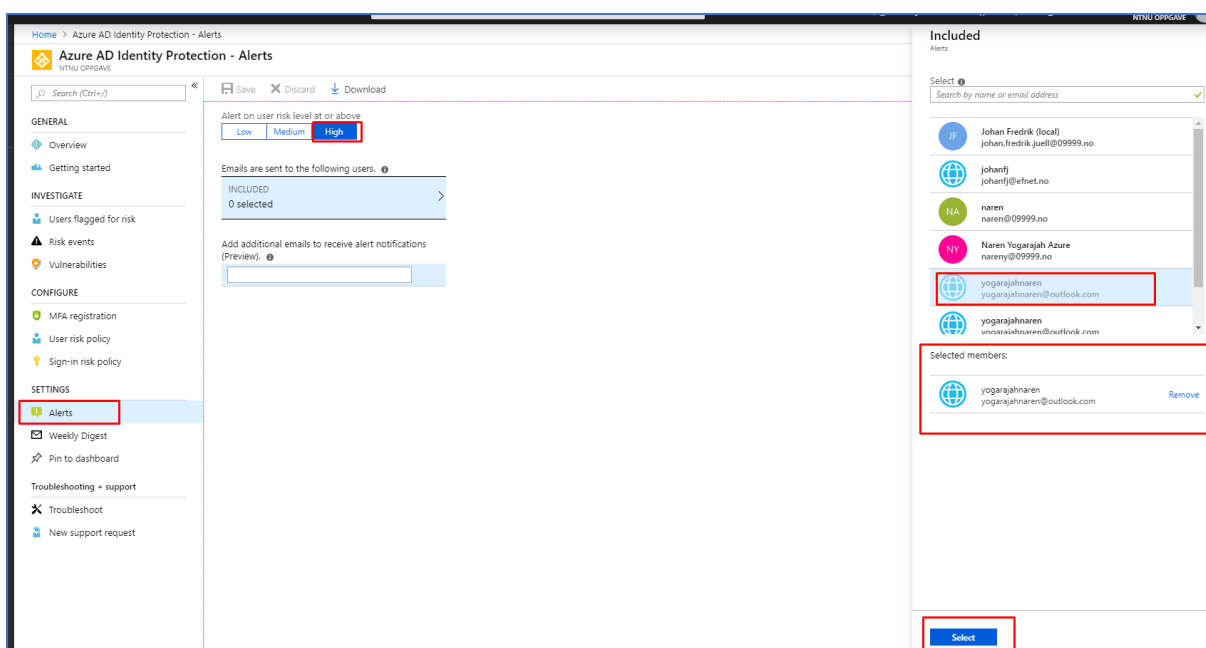


4. Derefter under Access setter jeg Allow access med en betingelse om at det kræves MFA autentisering.

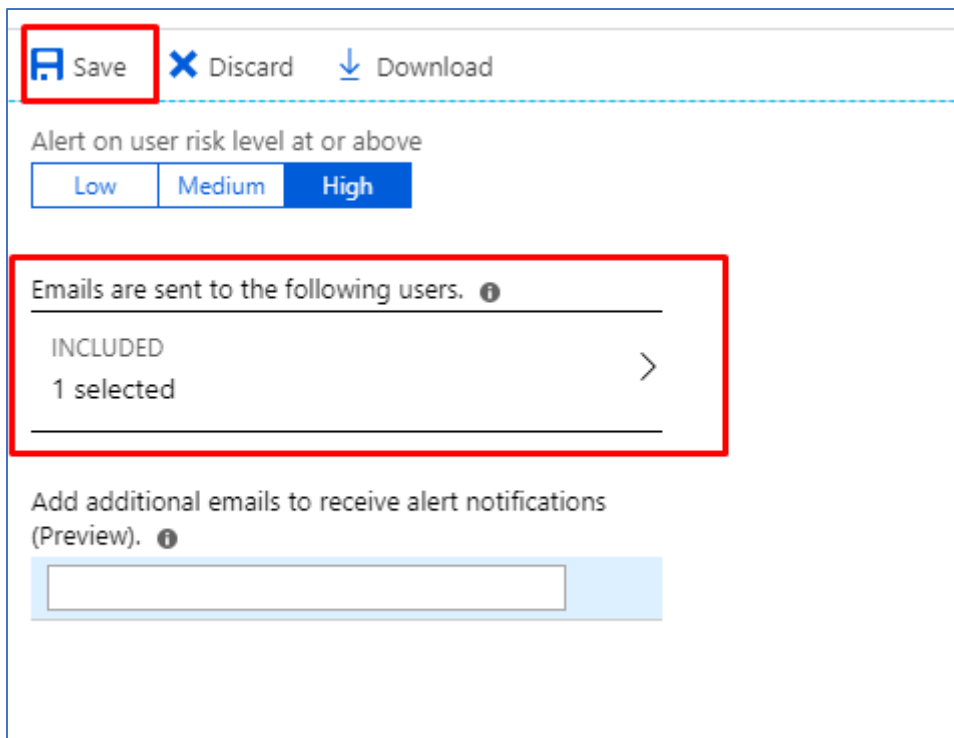


5. Videre tikker jeg av for «On» for at policyen skal bli aktivert og tilslutt lagrer jeg endringene.

2.2.3.4 Alerts

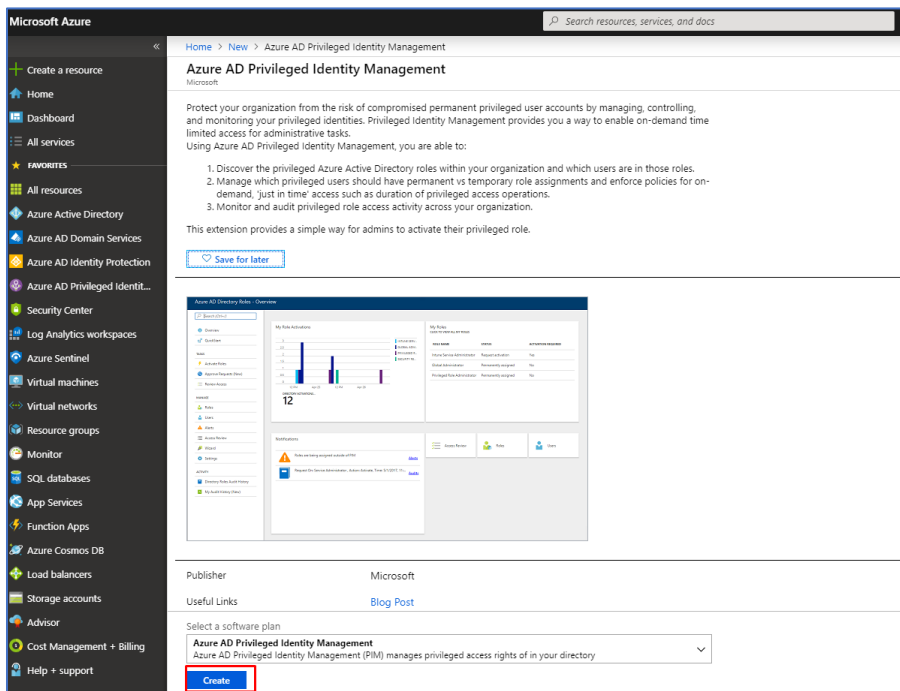


1. Det er nyttig å ha varsler fra Identity Protection på e-post da man kan holde seg oppdatert på hva som skjer i Azure miljøet sitt «On The Go». For å konfigurere mail varsler navigerer jeg meg frem til Alerts undermeny under Settings i Identity Protection. Deretter tikker jeg av for å få varsler på user risk level som er på nivå: High. Deretter velger jeg hvilken e-post som skal motta disse varslene.



2. Her ser vi at valgt e-post er lagt inn for alerts. Deretter er det bare å lagre endringene som er utført.

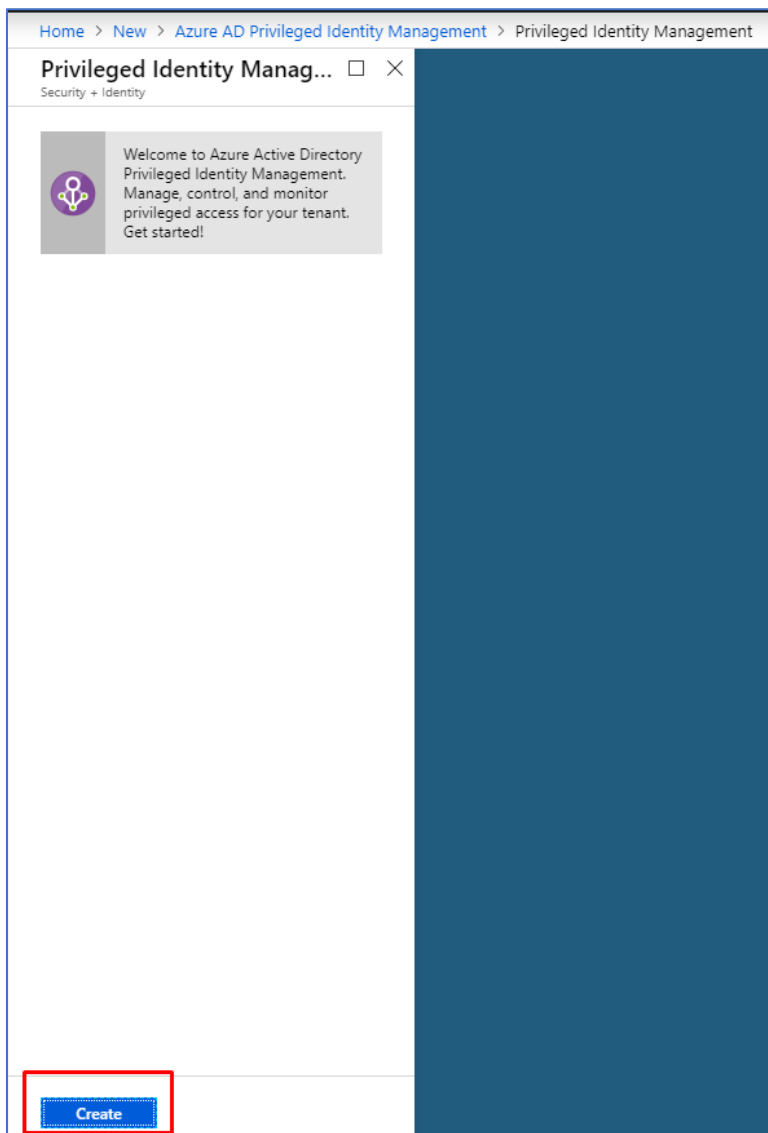
2.2.4 Azure Active Directory Privileged Identity Management



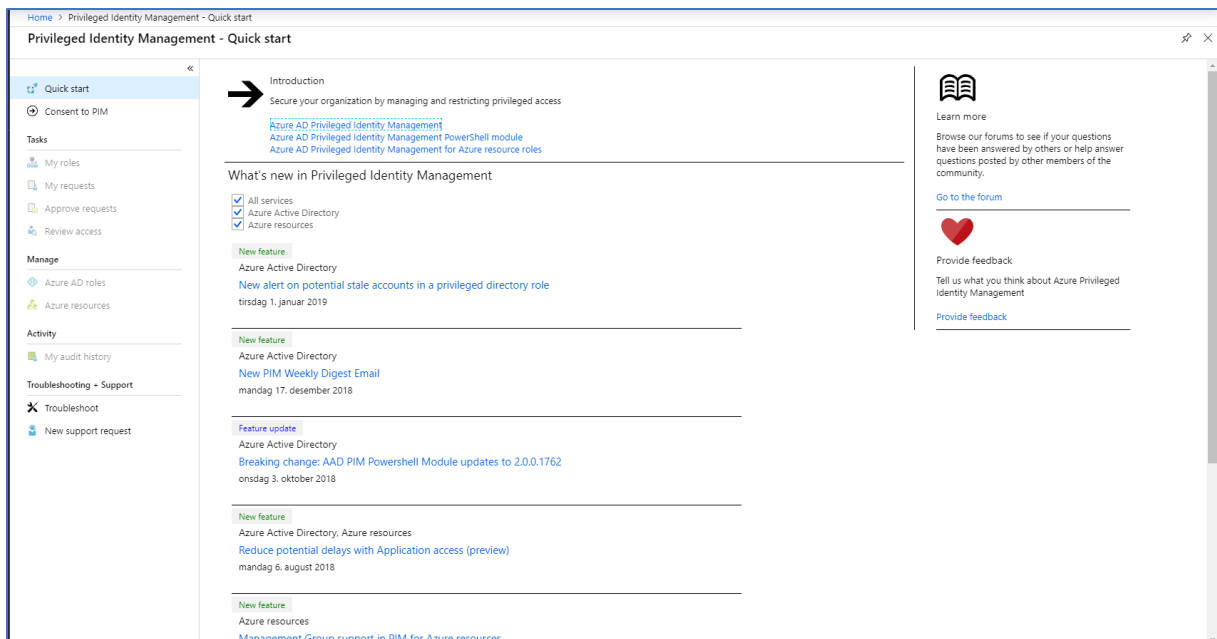
Azure Active Directory Privileged Identity Management er en tjeneste i Azure som gjør deg mulig for deg å administrere, kontrollere og overvåke tilgang til de viktigste ressursene som

befinner seg i din organisasjon. Ressurser i denne sammenheng vil være Azure Active Directory, Azure sine tjenester og andre tjenester som forekommer innenfor Microsoft Online Services som f.eks Office 365 og Microsoft Intune.

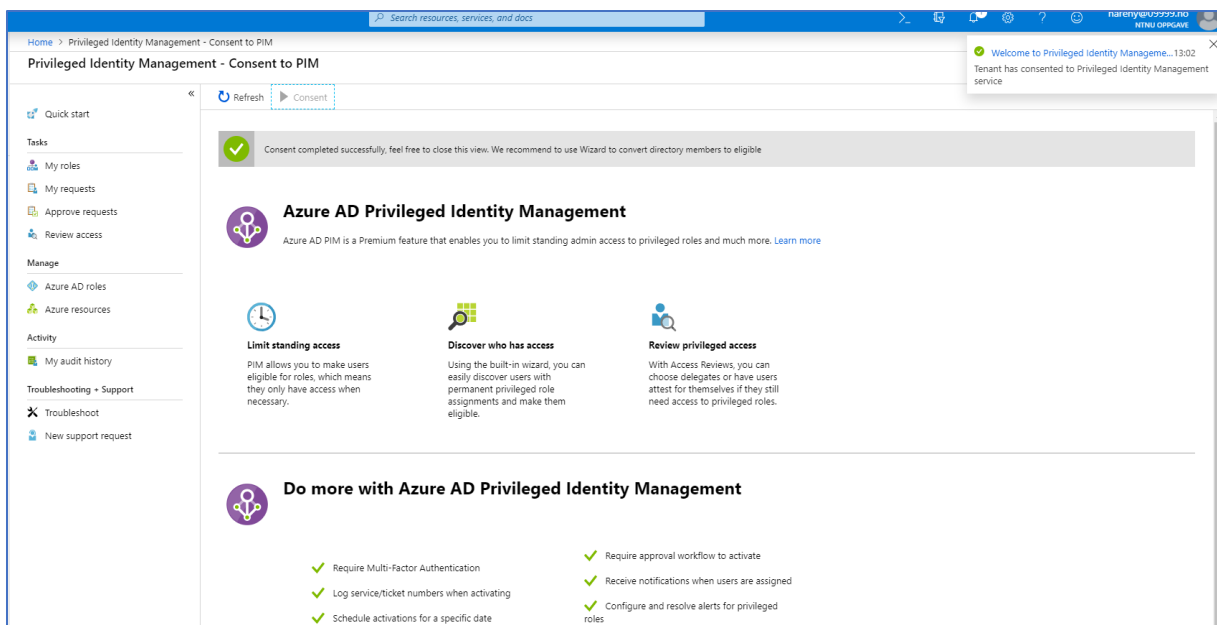
1. For å ta i bruk Azure AD Privileged Identity Management, må dette legges inn via Marketplace.



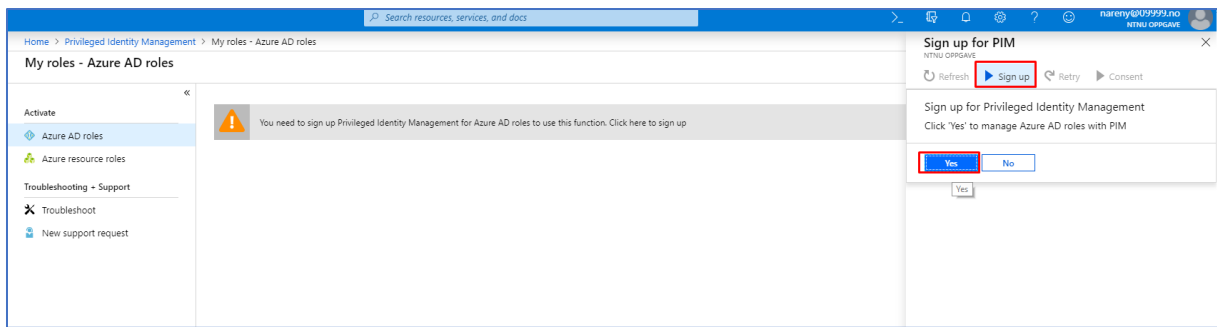
2. Videre klikker jeg på Create knappen for å opprette plattformen til Azure AD Privileged Identity Management.



3. Installasjonsprosessen går veldig fort. Nå er vi inne på dashboardet til Privileged Identity Management.

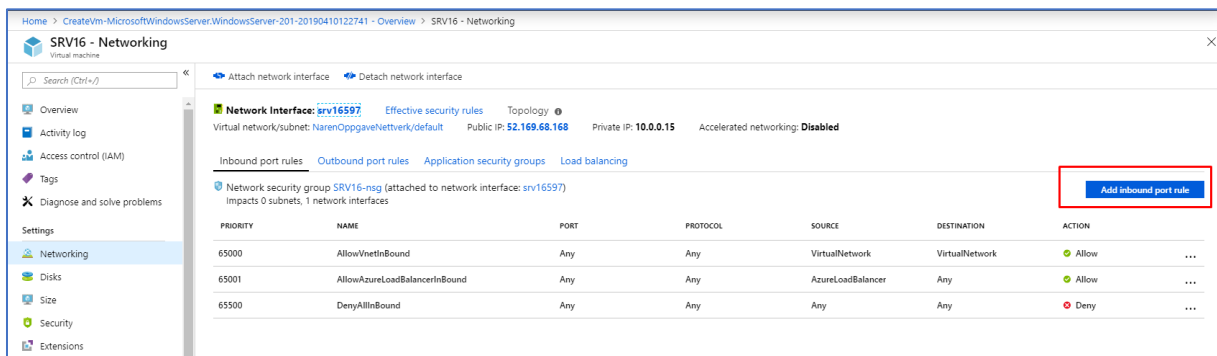


4. Deretter under Privileged Identity mangament – Consent to PIM klikker jeg på Consent knappen. Dette gjør jeg for å registrere min bruker til Privileged Identity Mangament.



5. Under Azure AD Roles signerer jeg min bruker for å kunne ta i bruk denne funksjonaliteten.

2.2.5 Active Directory Domain Services

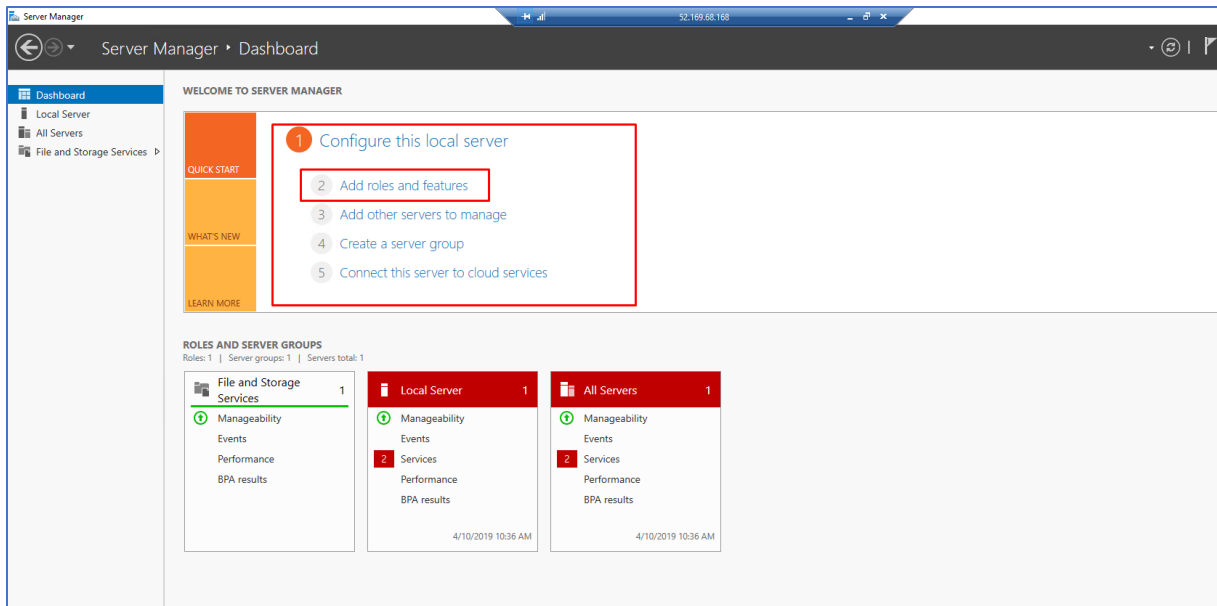


Active Directory Domain Services er en katalogtjeneste i Windows Server. Her har du mulighet til å opprette et domene. I dette domene har du mulighet til å opprette Organizational units og users. Dette domene lagrer informasjon om de ulike brukerne og OUene. Samtidig greier domene å verifisere deres innloggingsdetaljer og man har ikke minst mulighet til å definere ulike tilgangsrettigheter til de ulike brukerne.

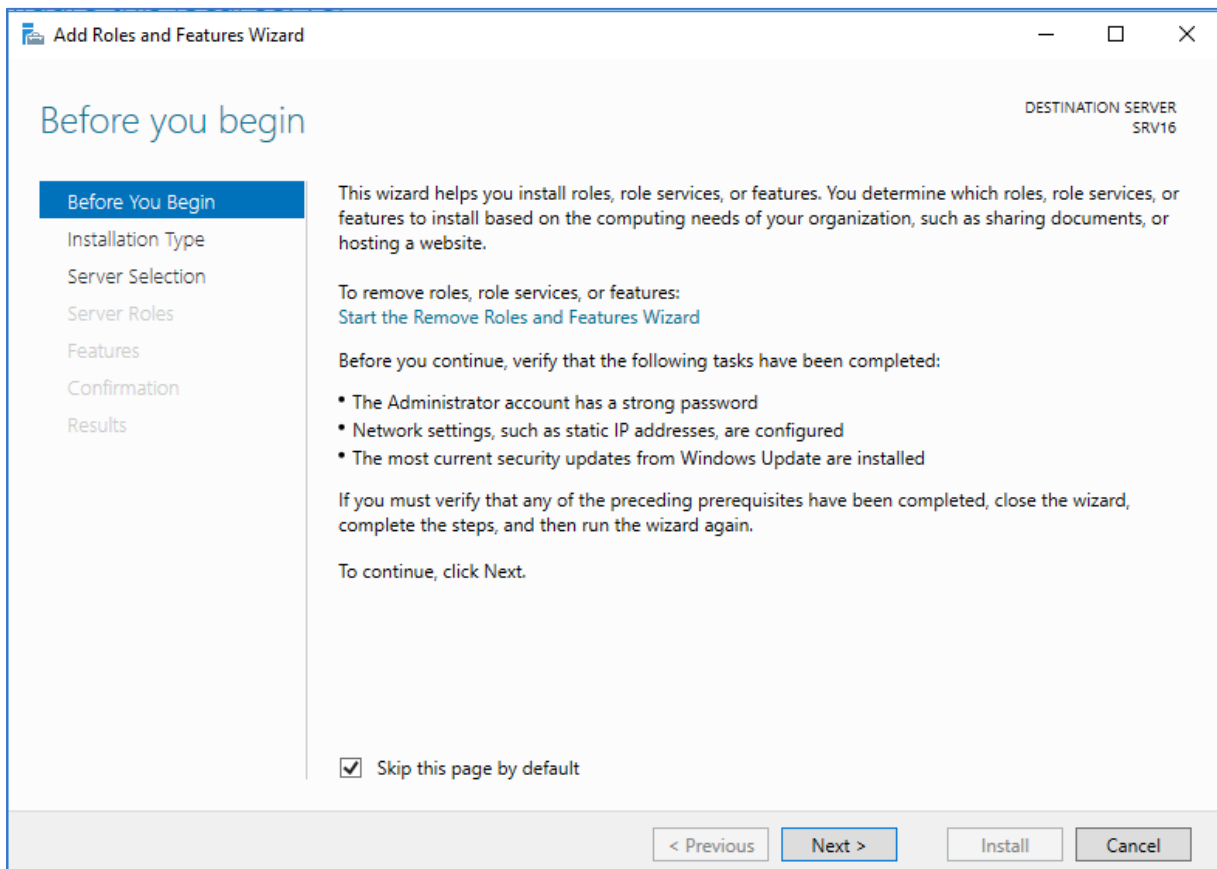
1. Før jeg starter opp min vm, så vil jeg gjerne ha RDP tilgang. Dette gjør jeg under Networking menyen på selve maskinen, deretter klikker jeg meg frem til Add Inbound port rule.

The screenshot shows the 'Add inbound security rule' dialog box in Azure. The dialog is titled 'Add inbound security rule' and shows configuration options for an inbound security rule. The 'Source' is set to 'Any', 'Source port ranges' is empty, 'Destination' is 'Any', and 'Destination port ranges' is '3389'. The 'Protocol' is 'Any', 'Action' is 'Allow', 'Priority' is '100', and 'Name' is 'RDP_TILKOBLING'. A warning message at the bottom states: 'RDP port 3389 is exposed to the Internet. This is only recommended for testing. For production environments, we recommend using a VPN or private connection.' The 'Add' button is highlighted with a red box.

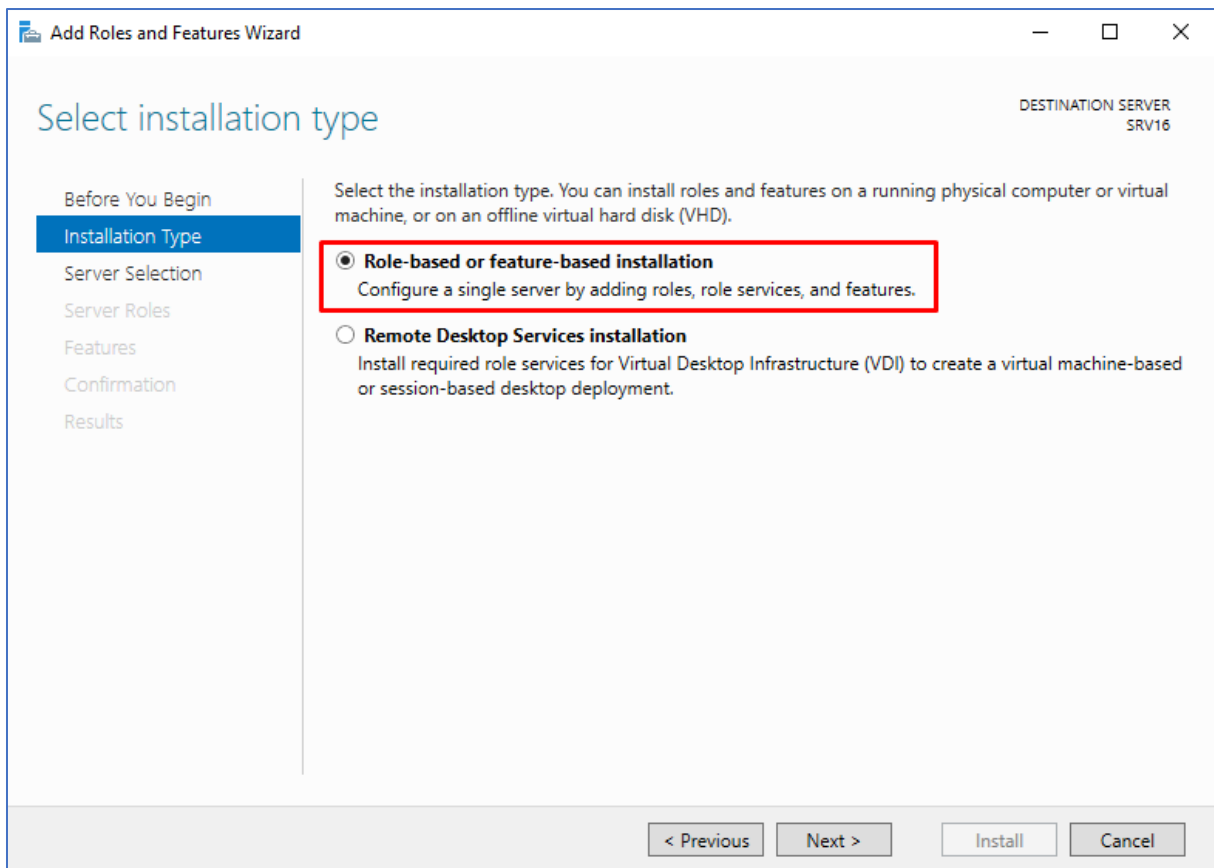
2. Videre legger jeg inn 3389 som er RDP porten og lagrer, slik at jeg får tilkobling gjennom Remote Desktop tilkobling.



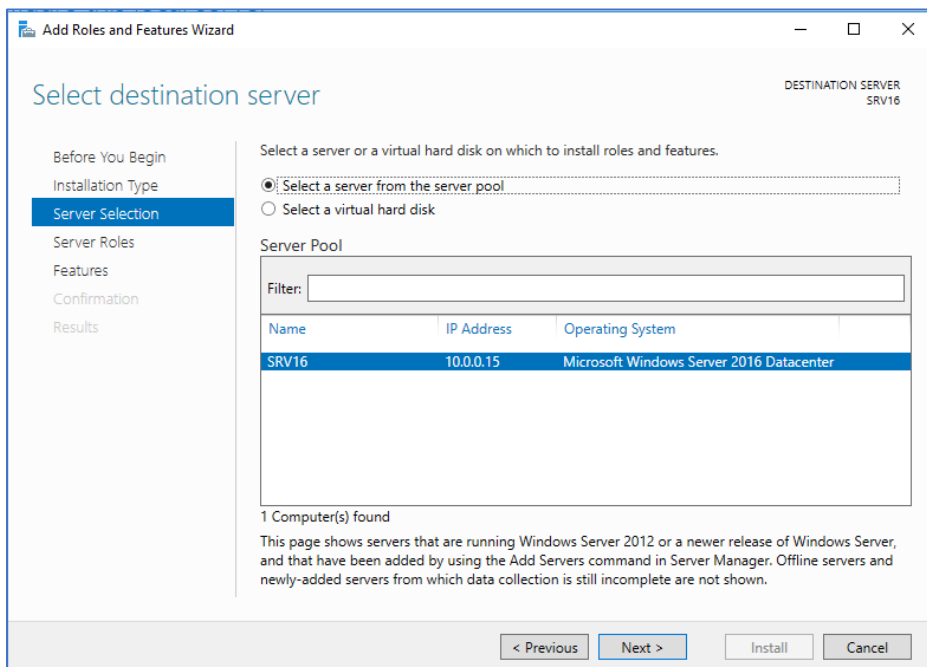
3. Deretter navigerer jeg meg videre inn på selve serveren SRV16. Etter dette åpner jeg opp Server Manager. Deretter klikker jeg på Add roles and features for å legge inn Active Directory Domain Services.



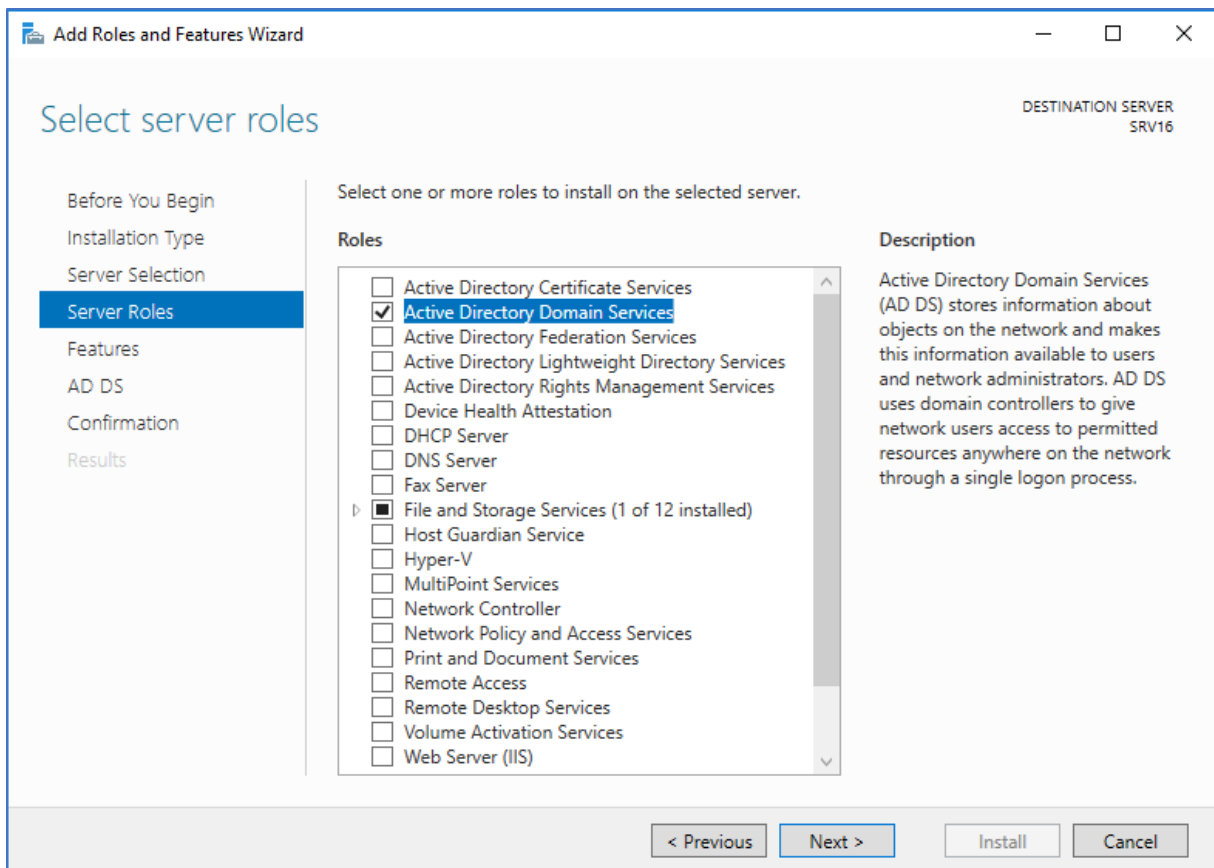
4. Jeg får opp et wizard der jeg tikker av for «Skip this page by default» og deretter klikker på next.



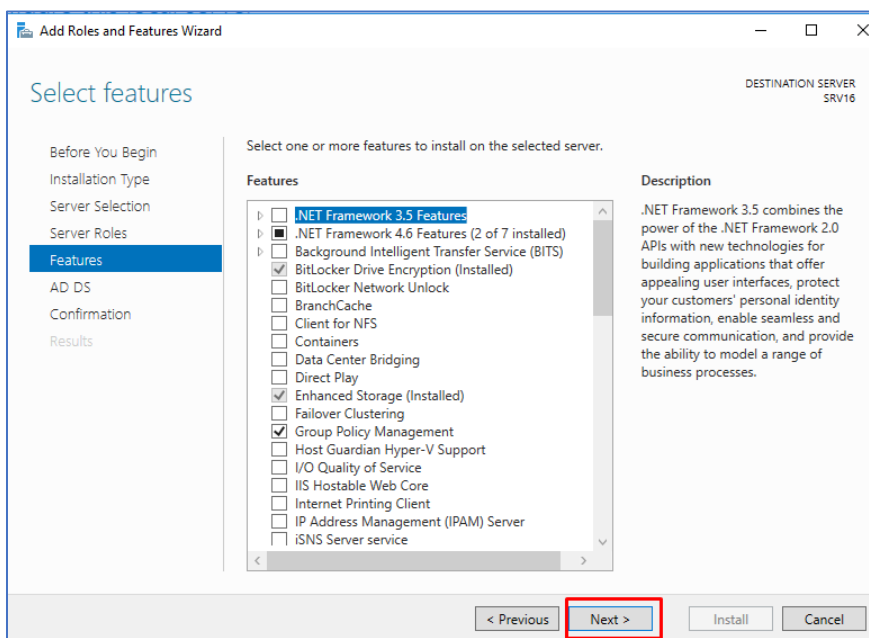
5. Videre tikker jeg av for Role-based or feature-based installation.



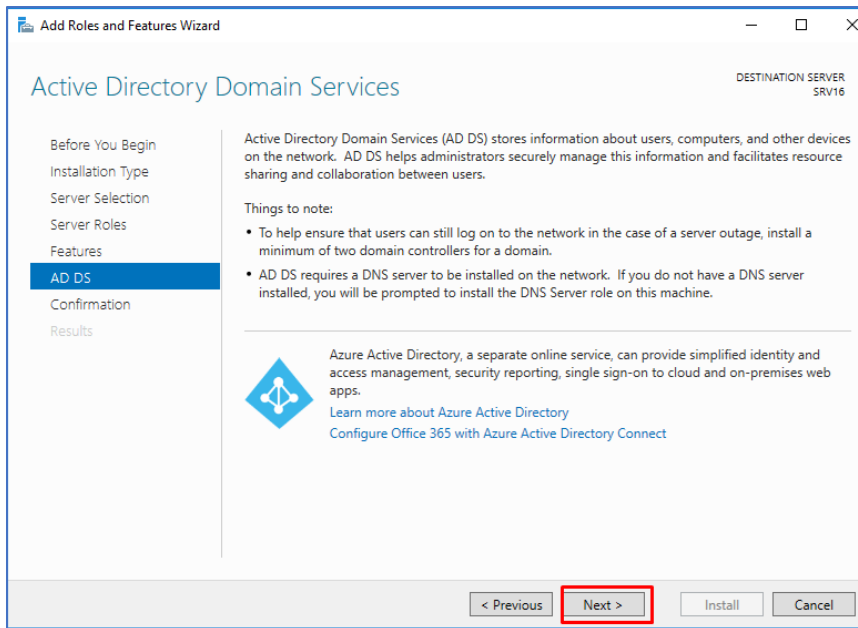
6. Deretter tikker jeg av for «Select a server from the server pool».



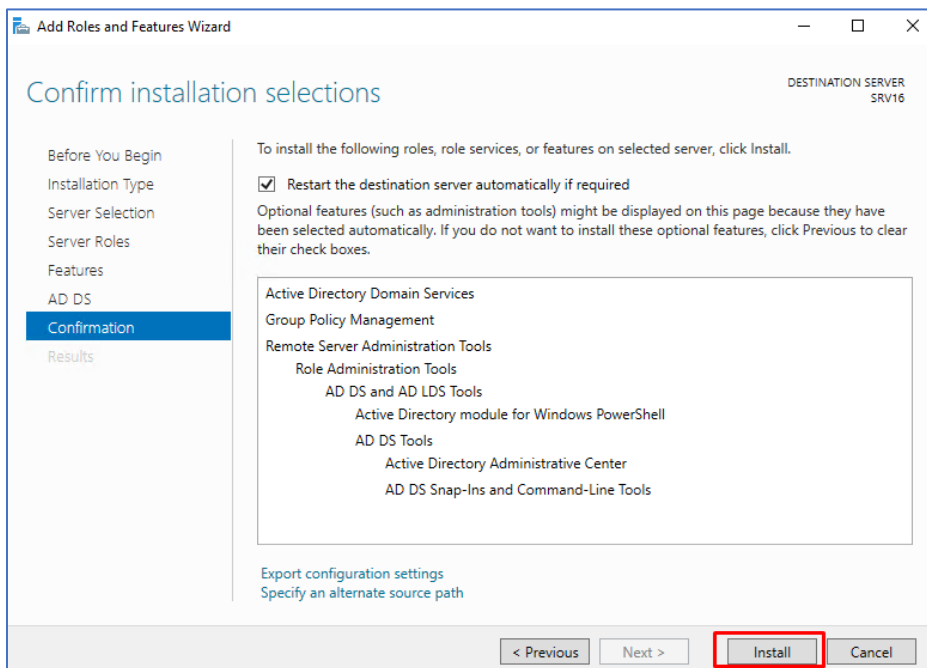
7. Videre tikker jeg av for Active Directory Domain Services.



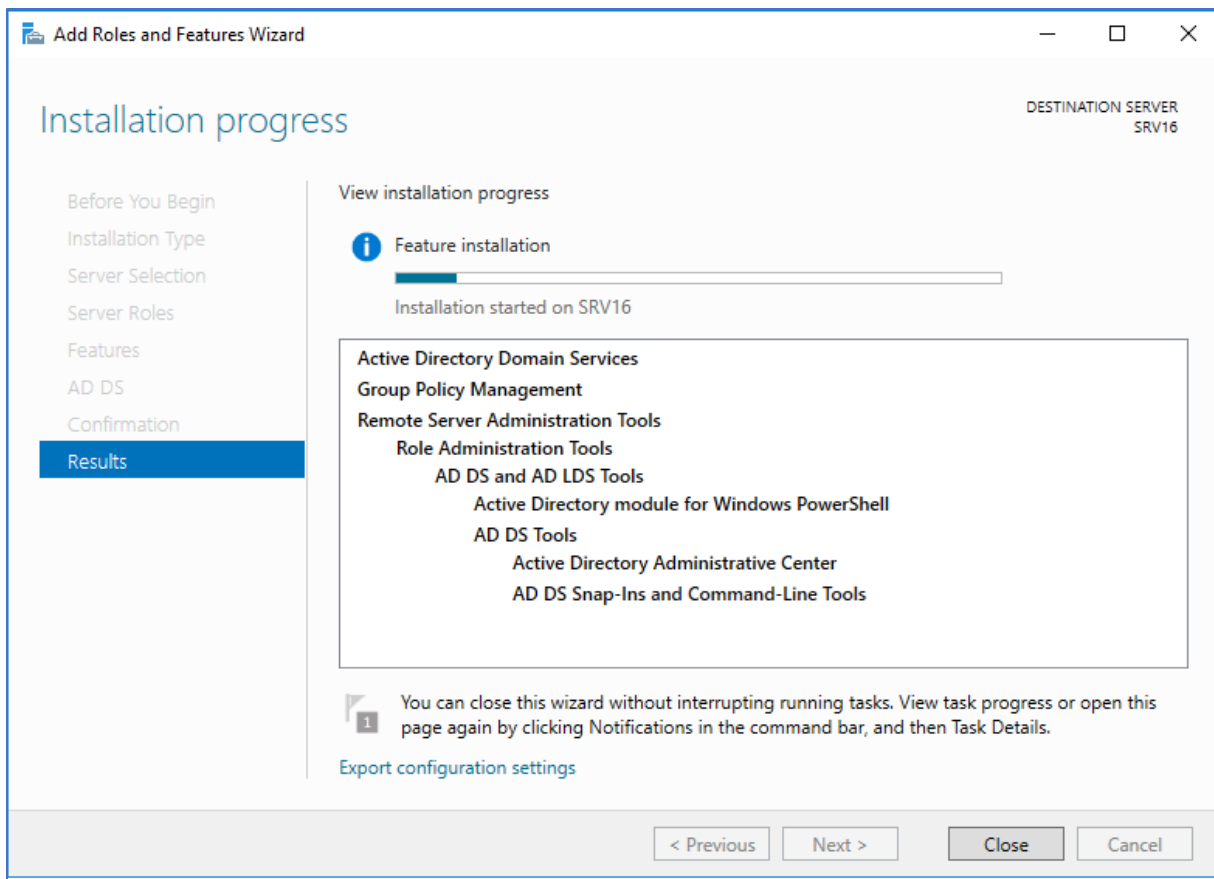
8. Deretter er det default valg som er lagt inn på siden som er vedlagt ovenfor. Disse lar jeg stå og klikker på next.



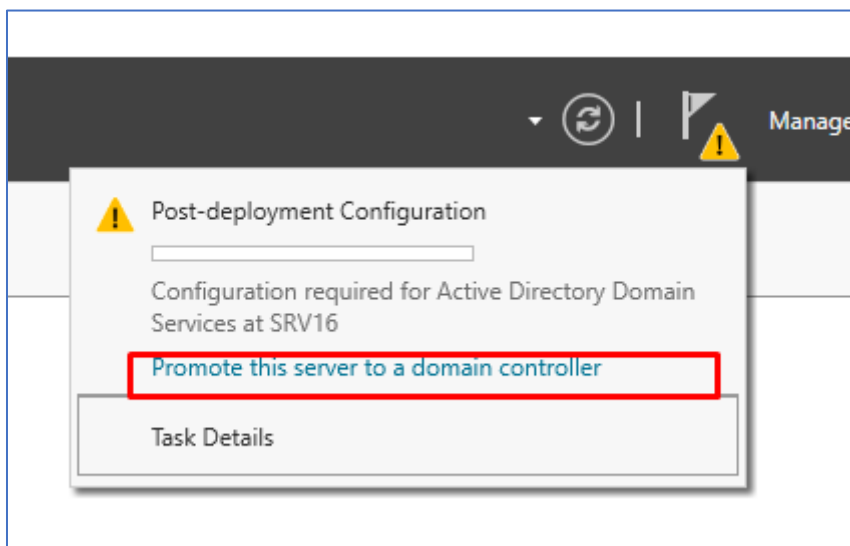
9. Her er det bare å klikke next.



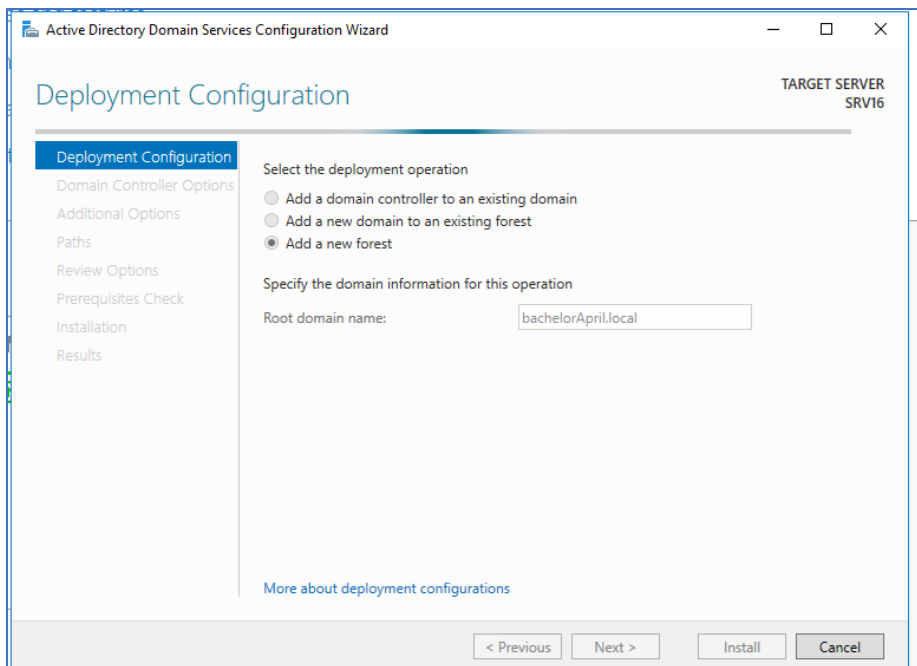
10. Jeg tikker av for Restart og videre klikker jeg på Install knappen.



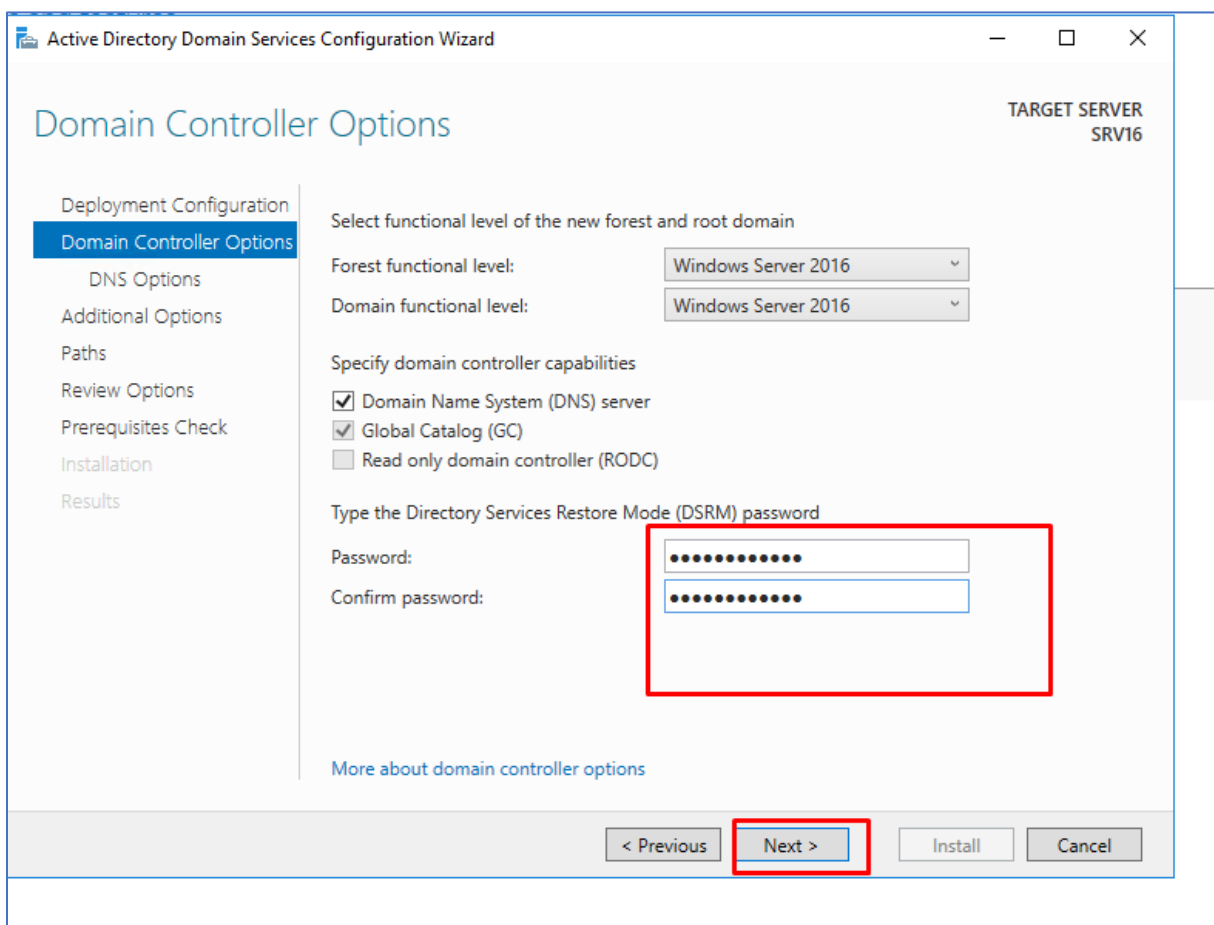
11. Nå er det bare å lukke vinduet og vente på at installasjonen blir ferdig.



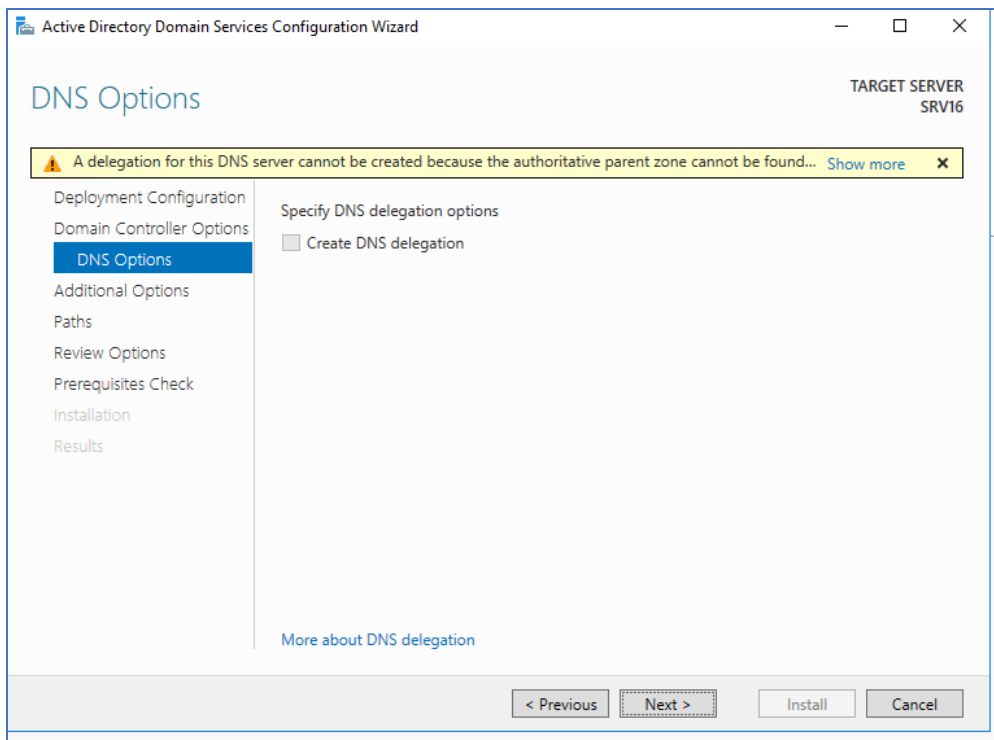
12. Etter en liten stund får du et varsel i Server Manager. Her må du videre klikke på «Promote this server to a domain controller».



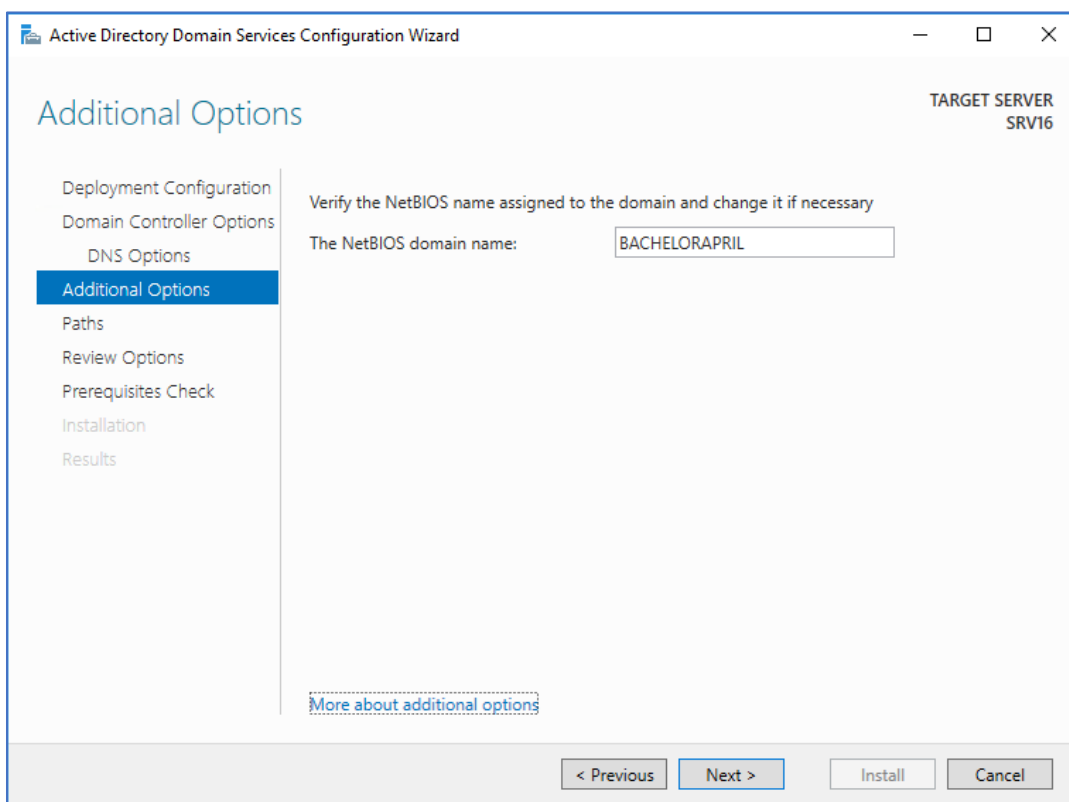
13. Deretter tikker du av for add a new forest og legger inn et navn for ditt domene.



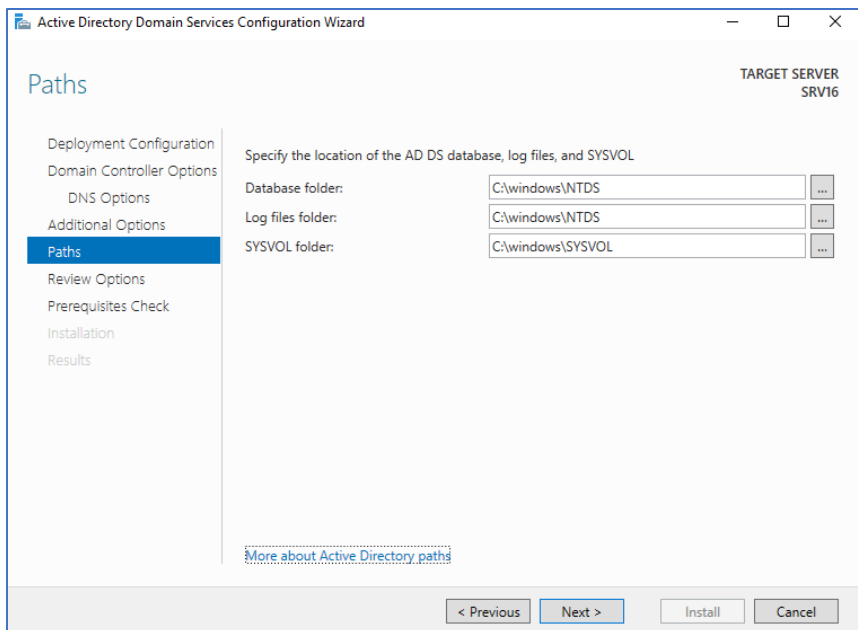
14. Deretter legger jeg inn et passord for domene kontrolleren. Domain Name System skal tikkes av her.



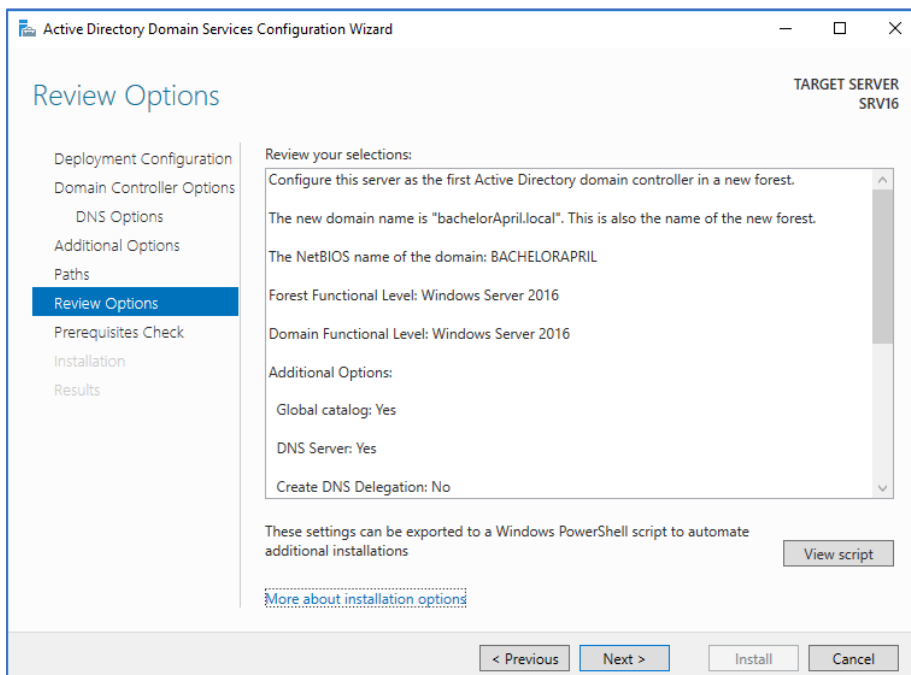
15. Her er det bare å klikke next.



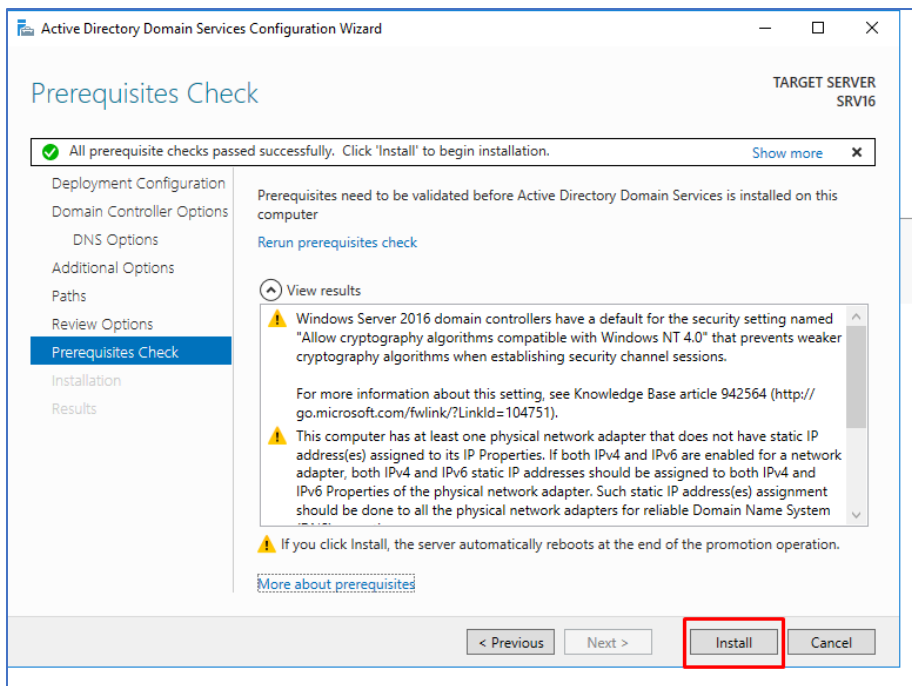
16. Det blir automatisk lagt inn et NetBIOS domain name som nemlig er BACHELORAPRIL. Dette har jeg allerede opprettet i tidligere fase.



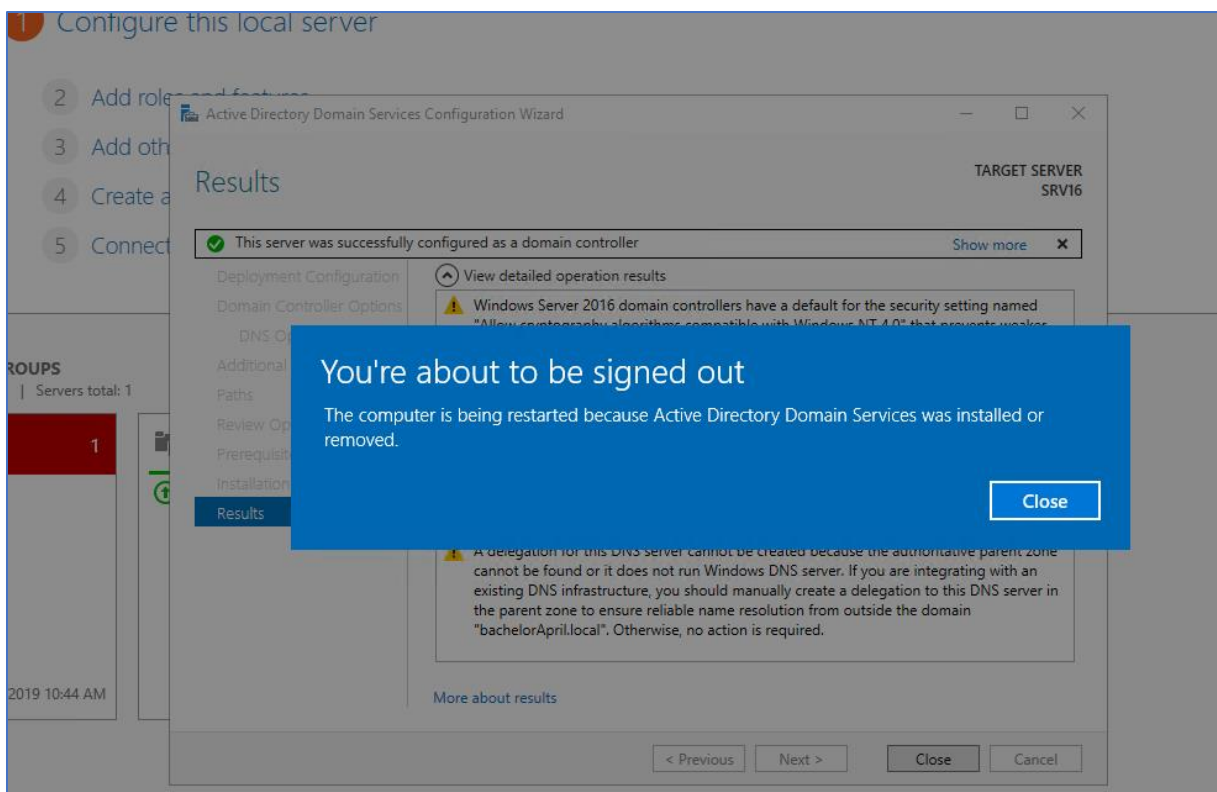
17. Videre er det bare å klikke på next.



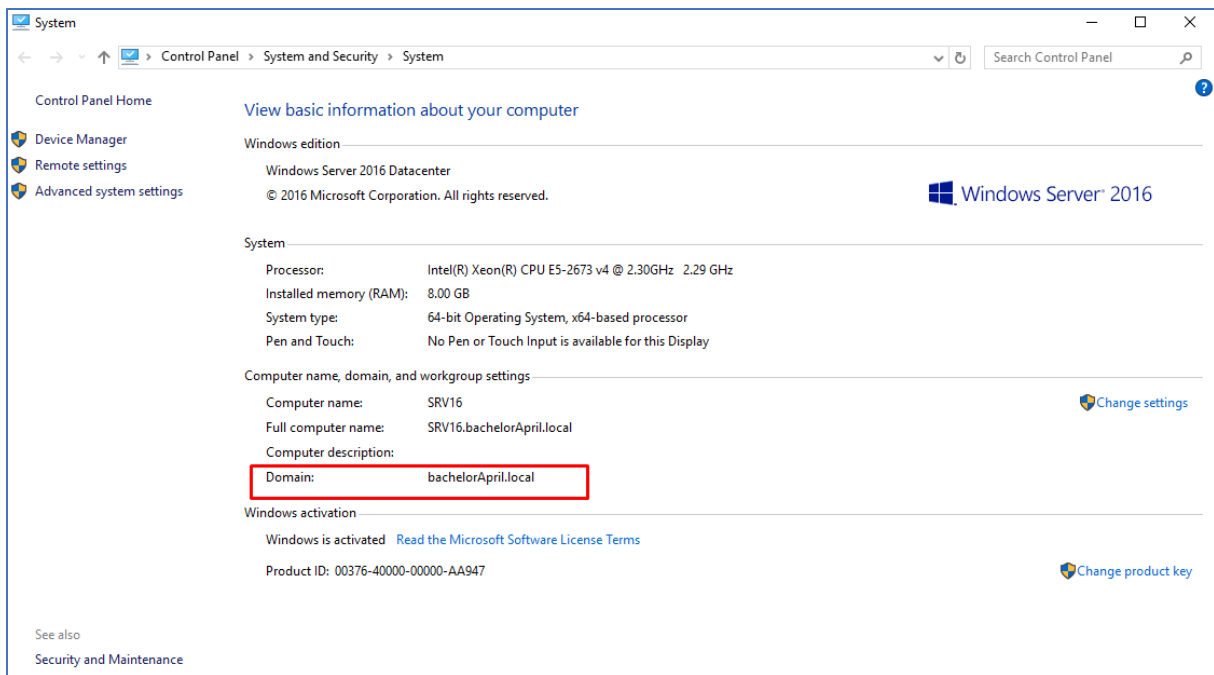
18. Videre er det bare å klikke på next.



19. Dersom alt går som planlagt, får du opp klart signal for videre installasjon. Da er det bare å sette i gang å installere.

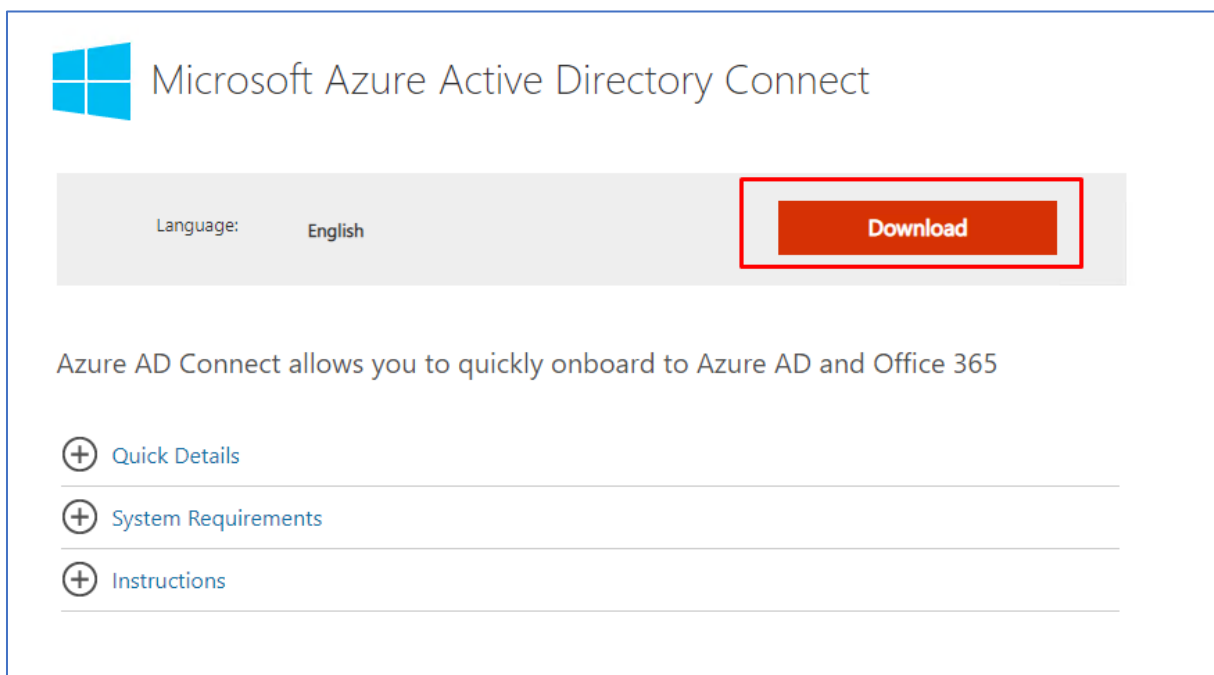


20. Ettersom installasjonen nærmer seg slutten, blir du automatisk logget av sesjonen.

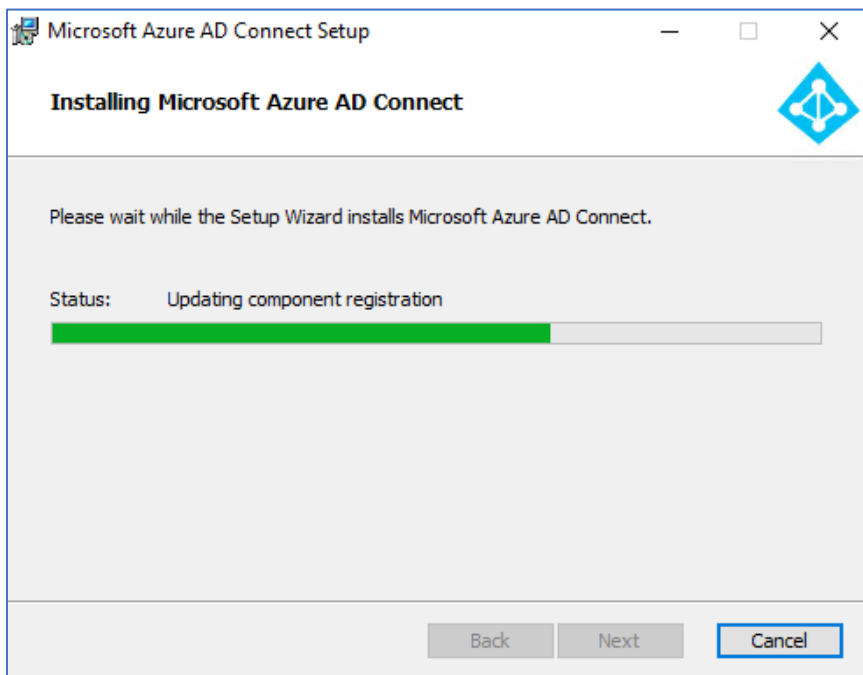


21. Under system innstillinger ser vi nå at domene «bachelorApril.local» er installert.

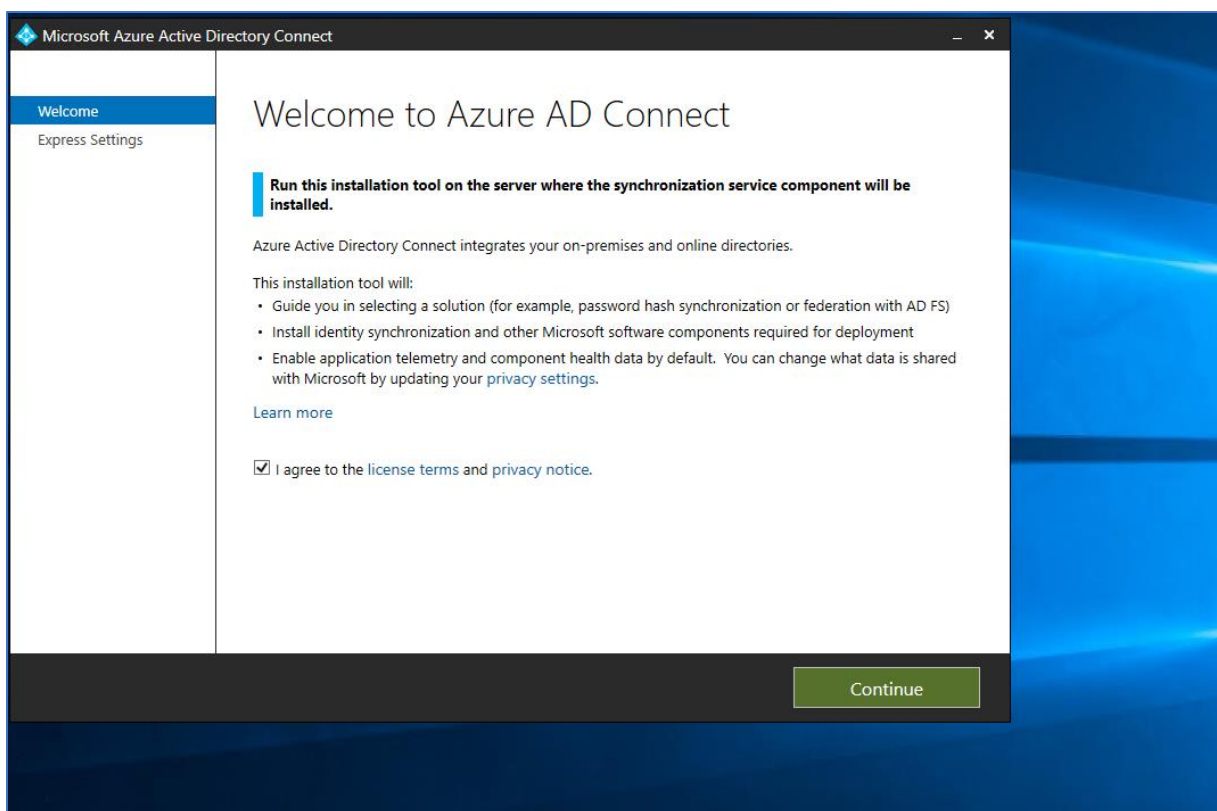
2.2.6 Microsoft Azure Active Directory Connect



1. Jeg starter med å laste ned installasjonsfilen til Microsoft Azure Active Directory Connect fra Microsoft sin side.

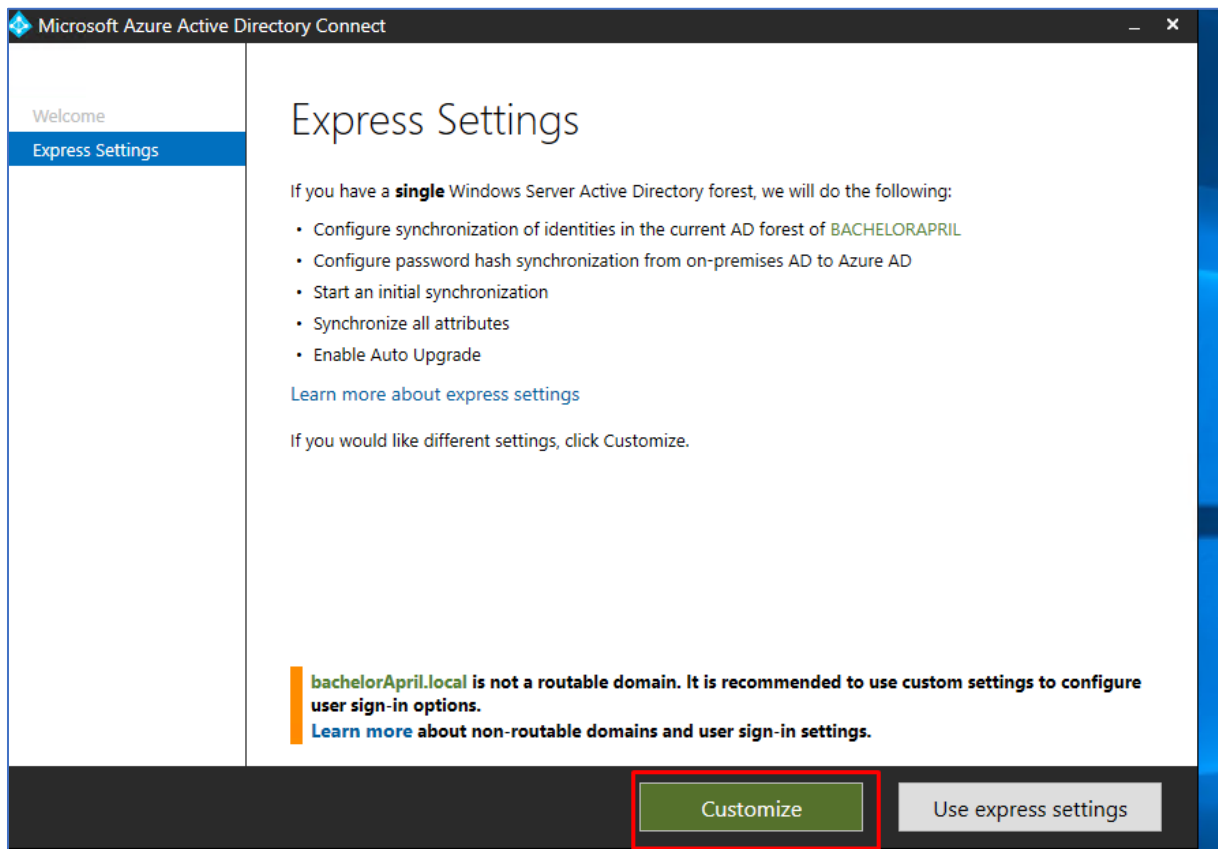


2. Videre starter jeg installasjonen av Microsoft Azure AD Connect.

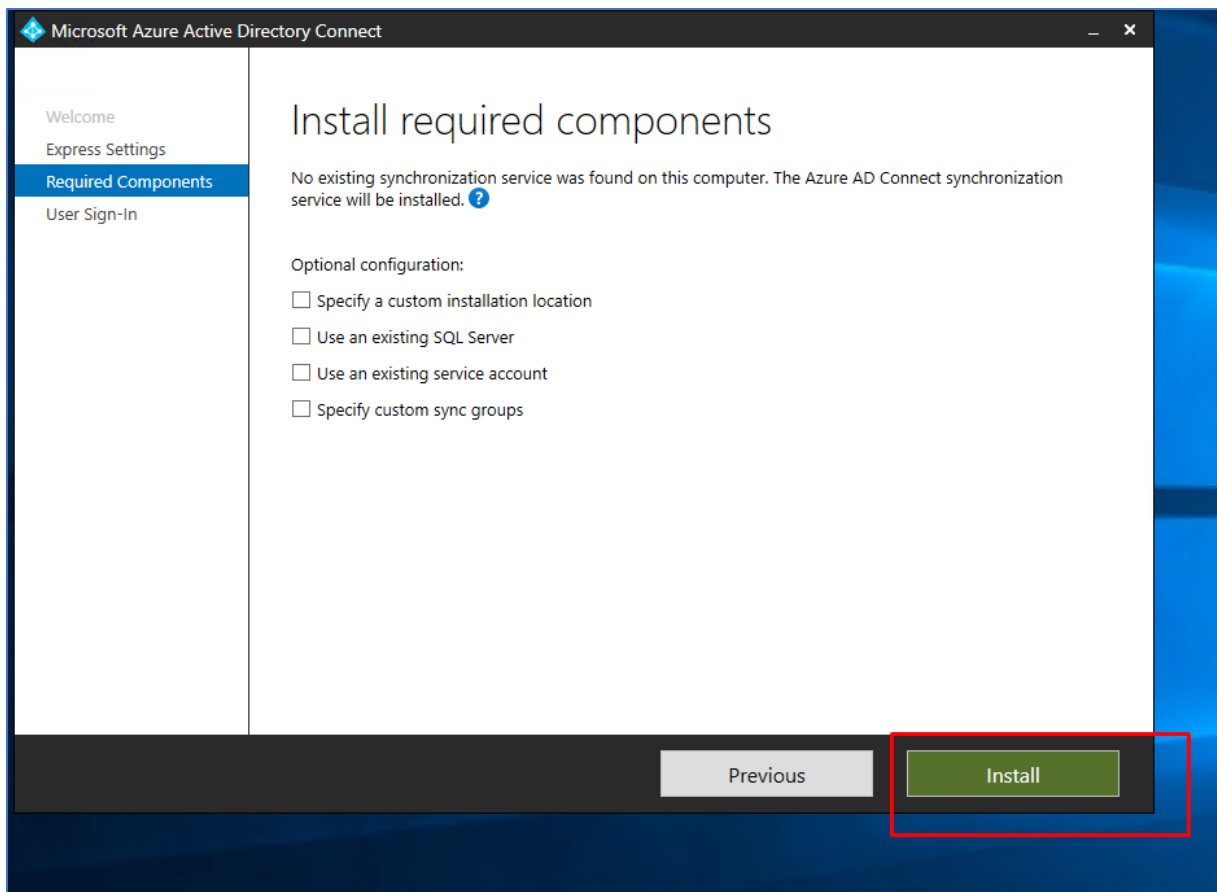


3. Etterhvert som installasjonen er ferdig, starter jeg opp Microsoft Azure AD Connect for

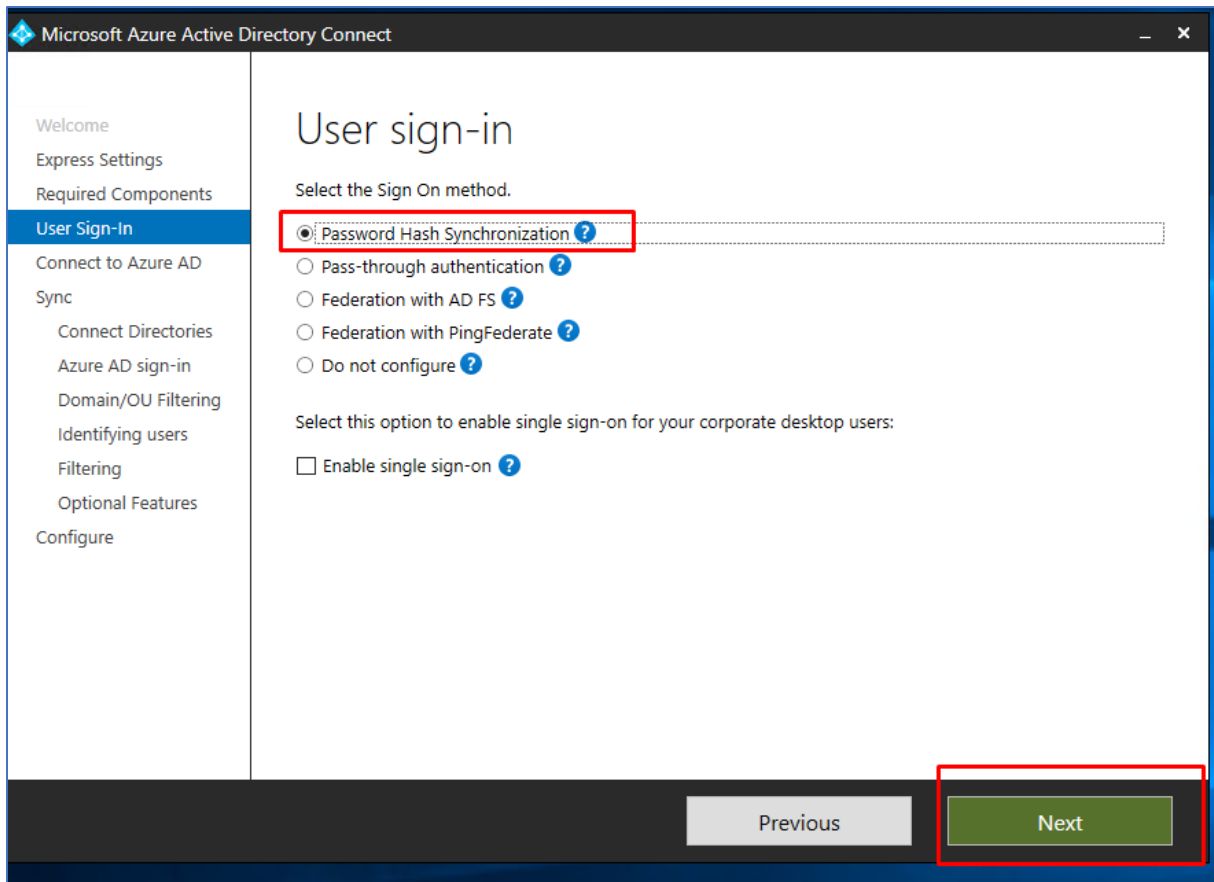
videre oppsett. Deretter tikker jeg av for agreement avtalen og klikker videre på Continue knappen.



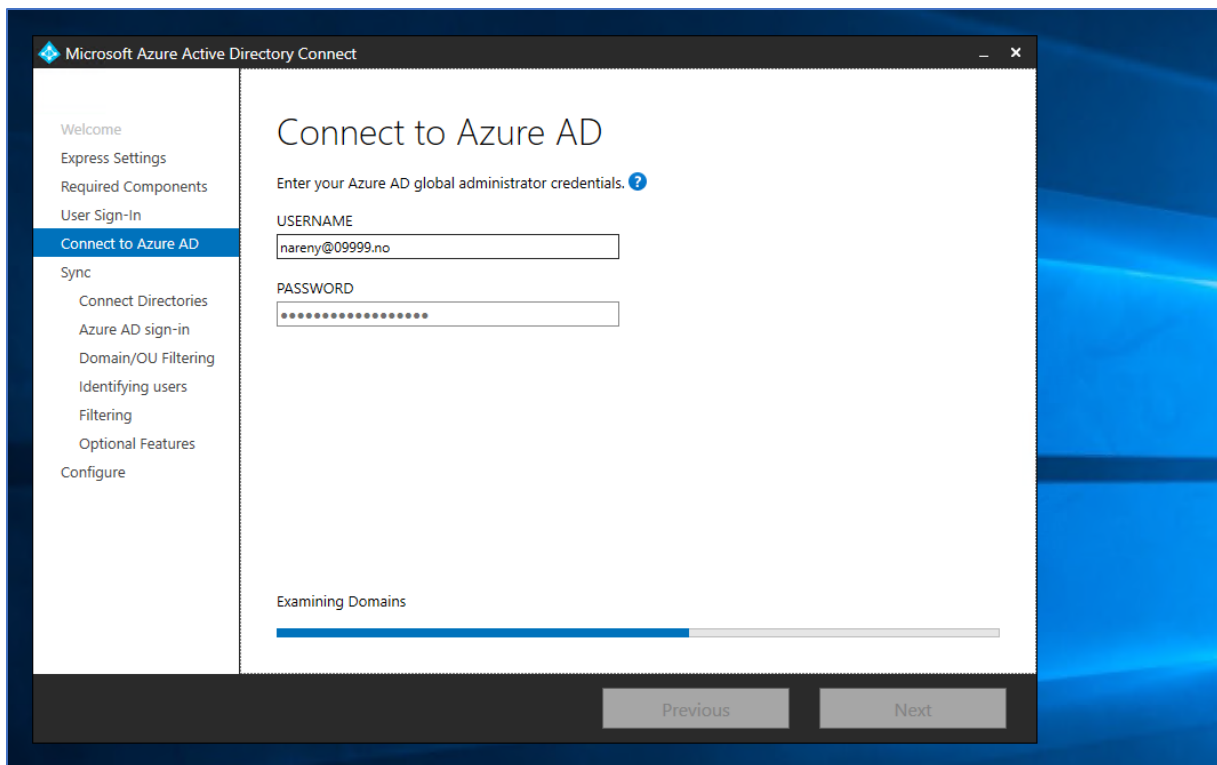
4. Videre klikker jeg på Customize knappen.



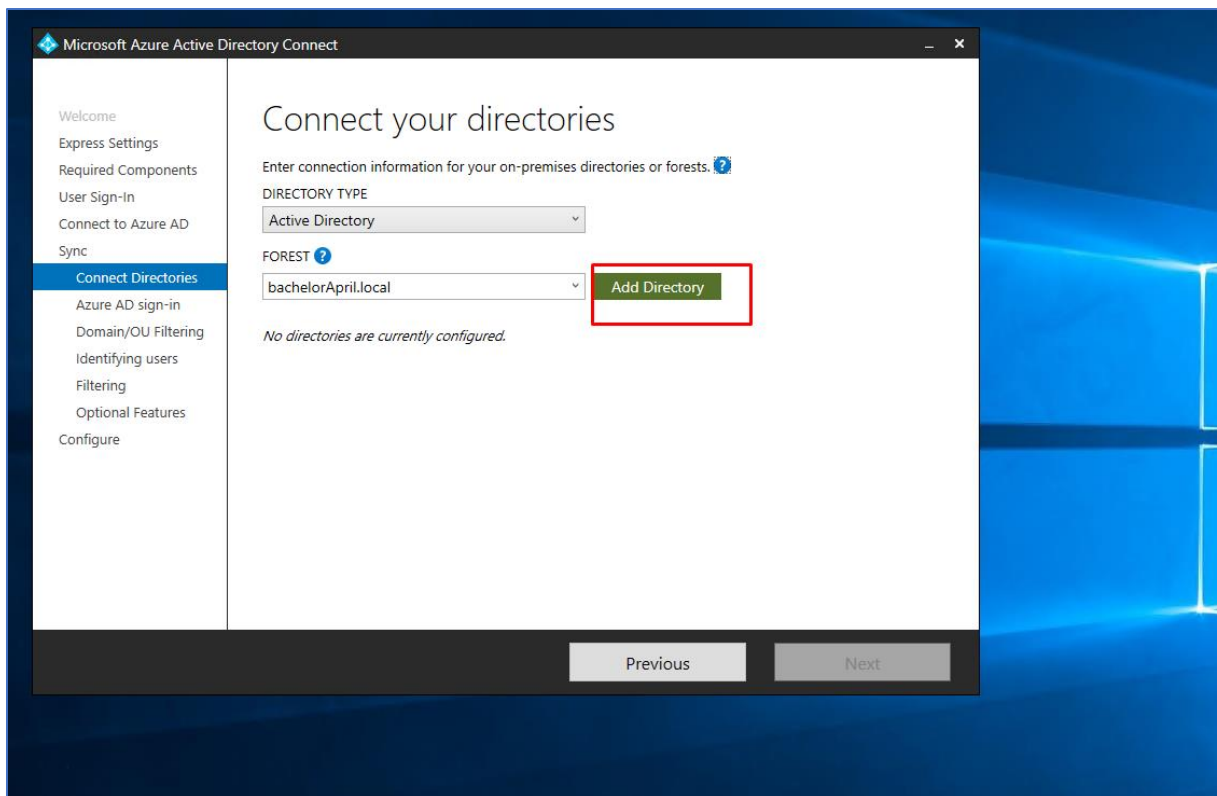
5. Deretter trenger man ikke å tikke av på noen valg. Det er bare å klikke på Install knappen og de tjenestene installeres automatisk.



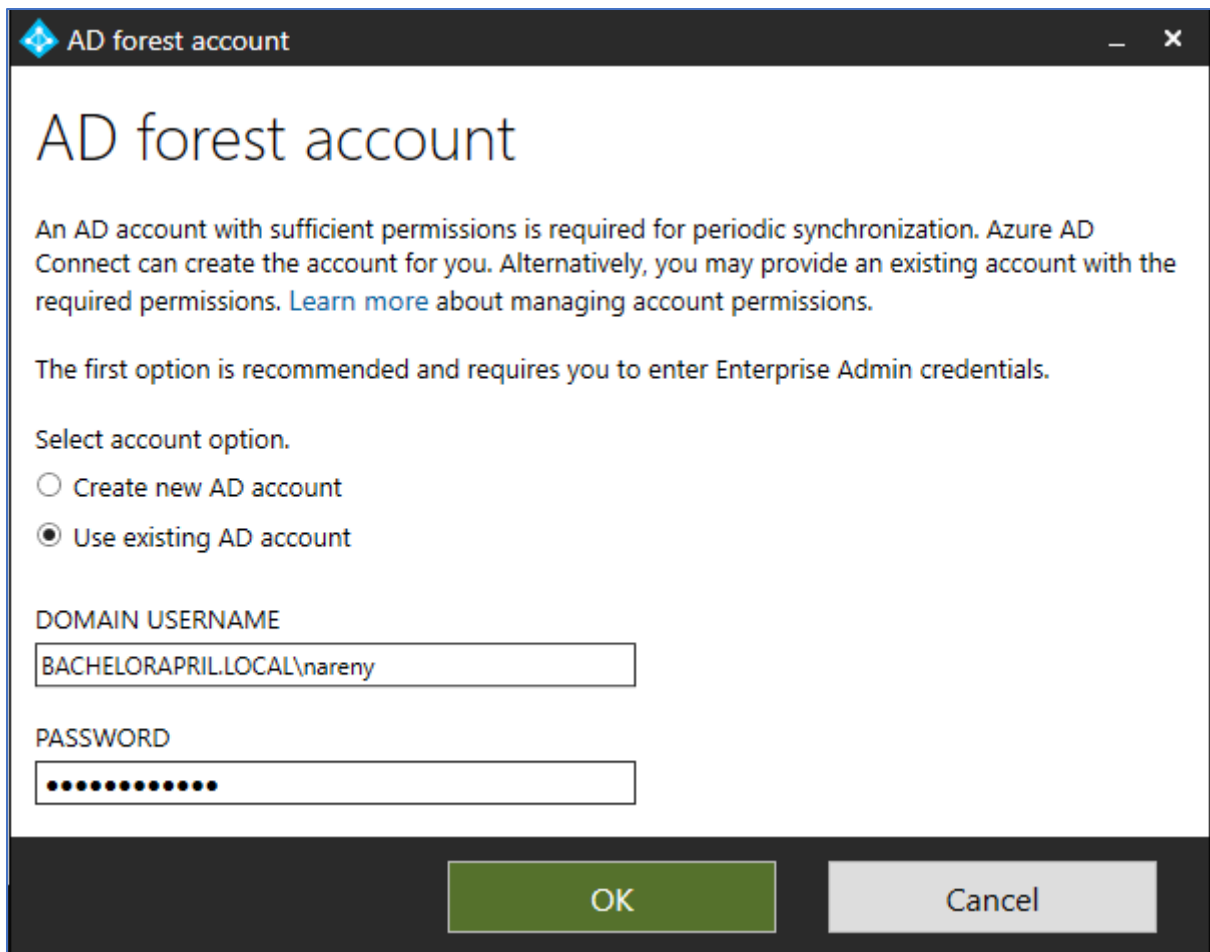
6. Deretter tikker jeg af for Password Hash Synchronization og klikker next.



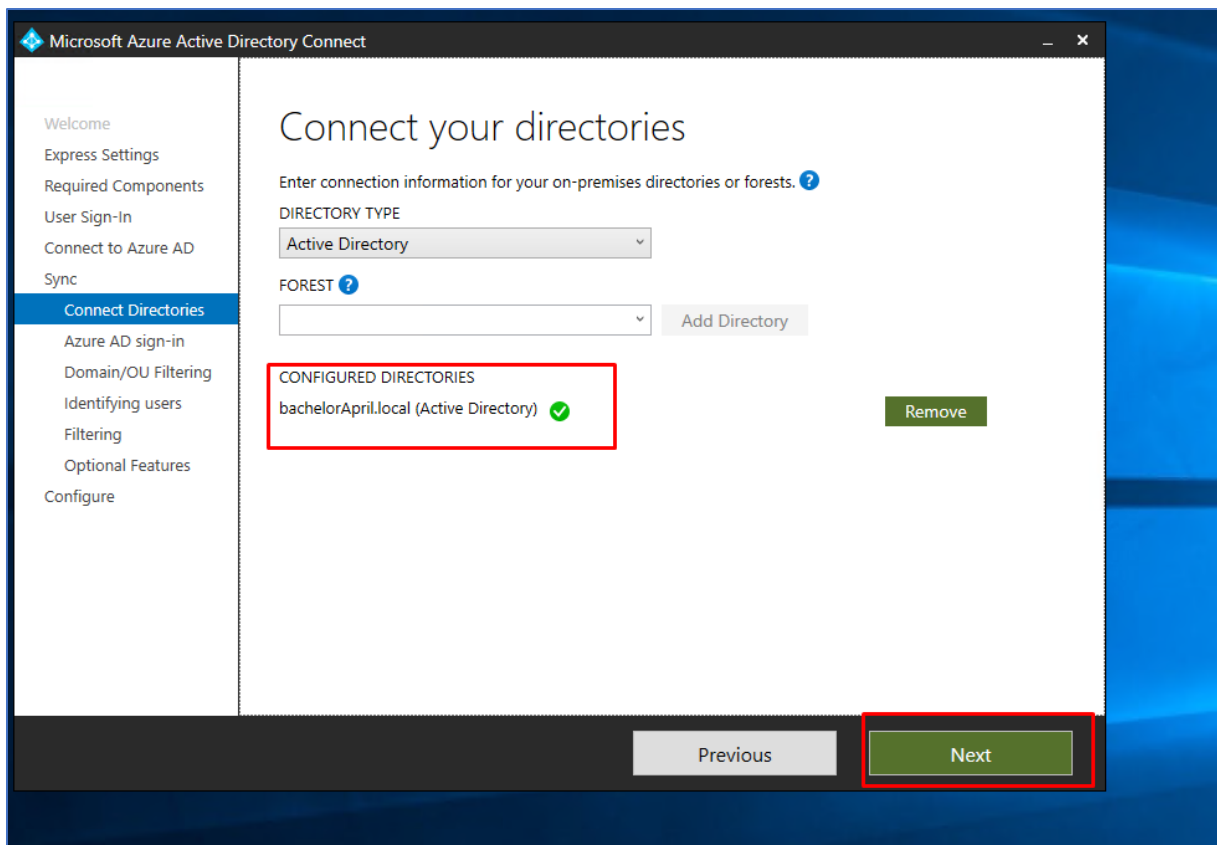
7. Videre må jeg legge inn Azure AD bruker detaljer slik at man får knyttet seg opp mot Azure AD.



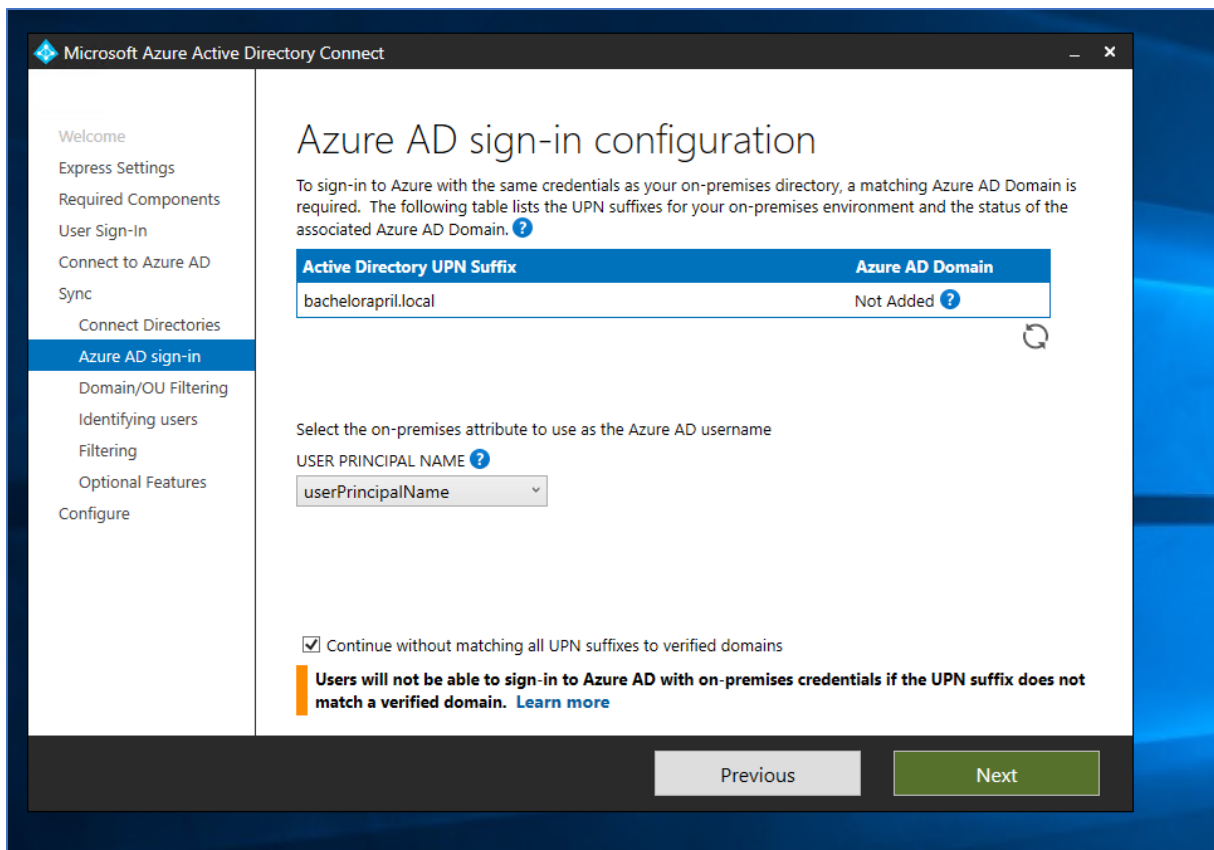
8. Deretter klikker jeg på Add Directory.



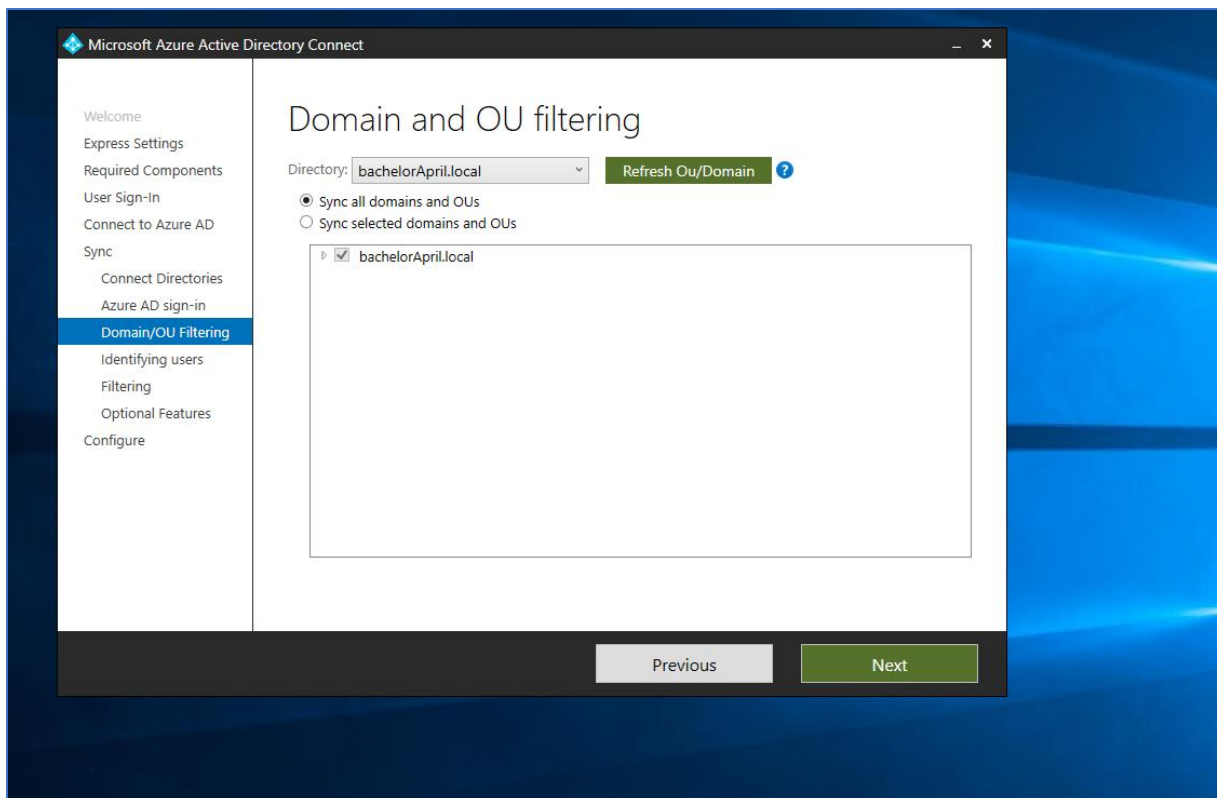
9. Videre skal vi legge inn en eksisterende AD konto. Dette er en konto fra domene BACHELORAPRIL.LOCAL.



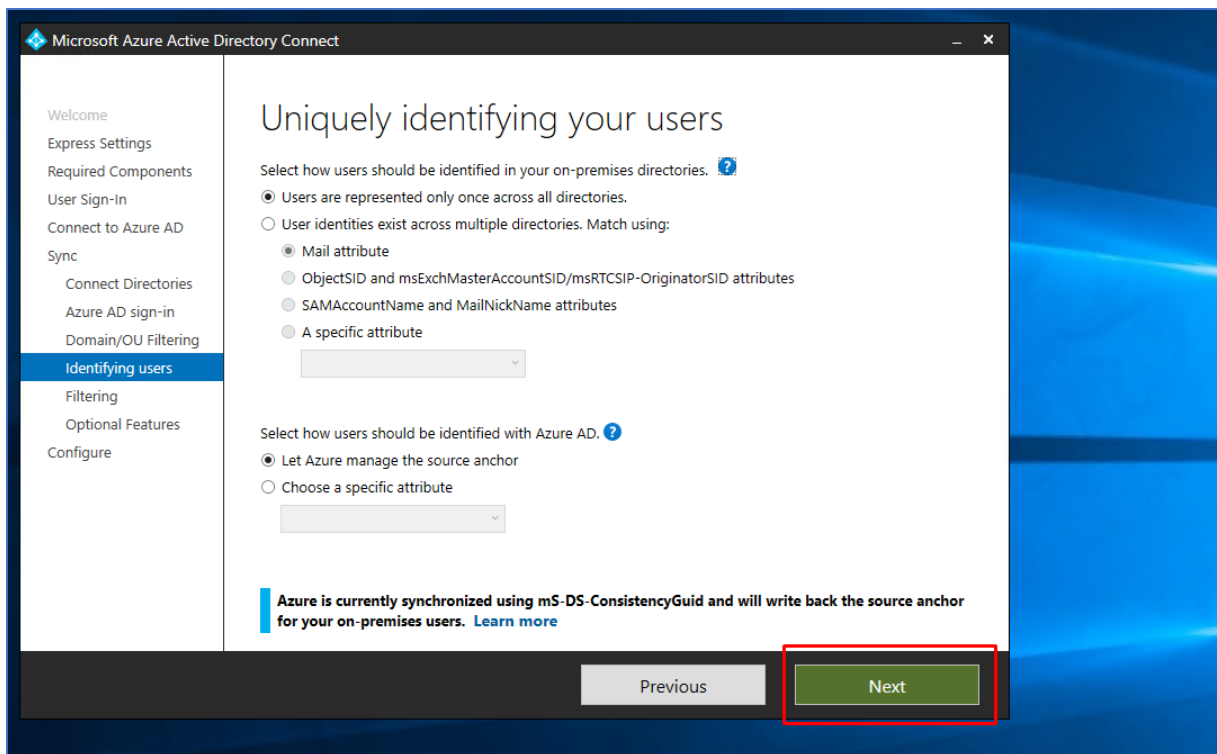
10. Nå ser vi av katalogene er riktig konfigurert. Dette ser vi gjennom at det har et grønt riktig tegn.



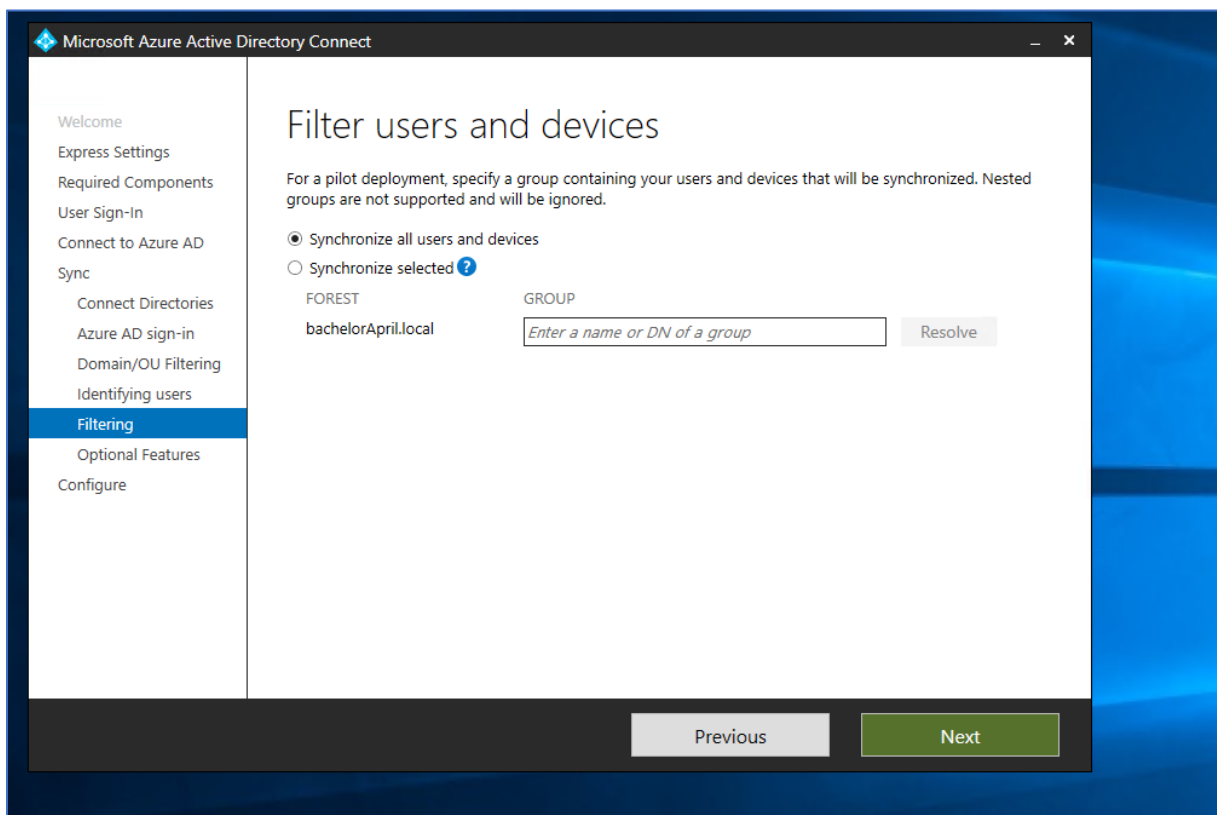
11. Nå kan vi videre tikke av for «Continue without matching all UPN suffixes to verified domains». Deretter kan vi gå videre.



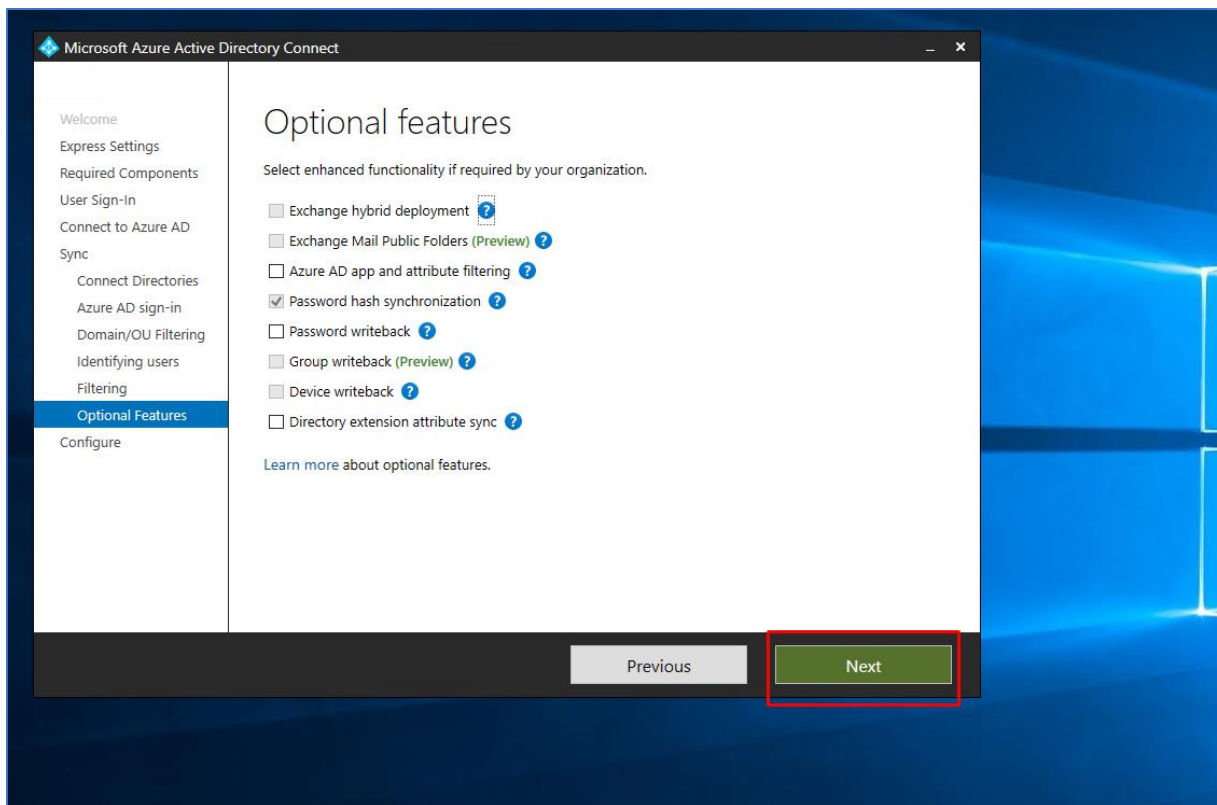
12. Videre kan vi tikker av for «Sync all domains and OUs.



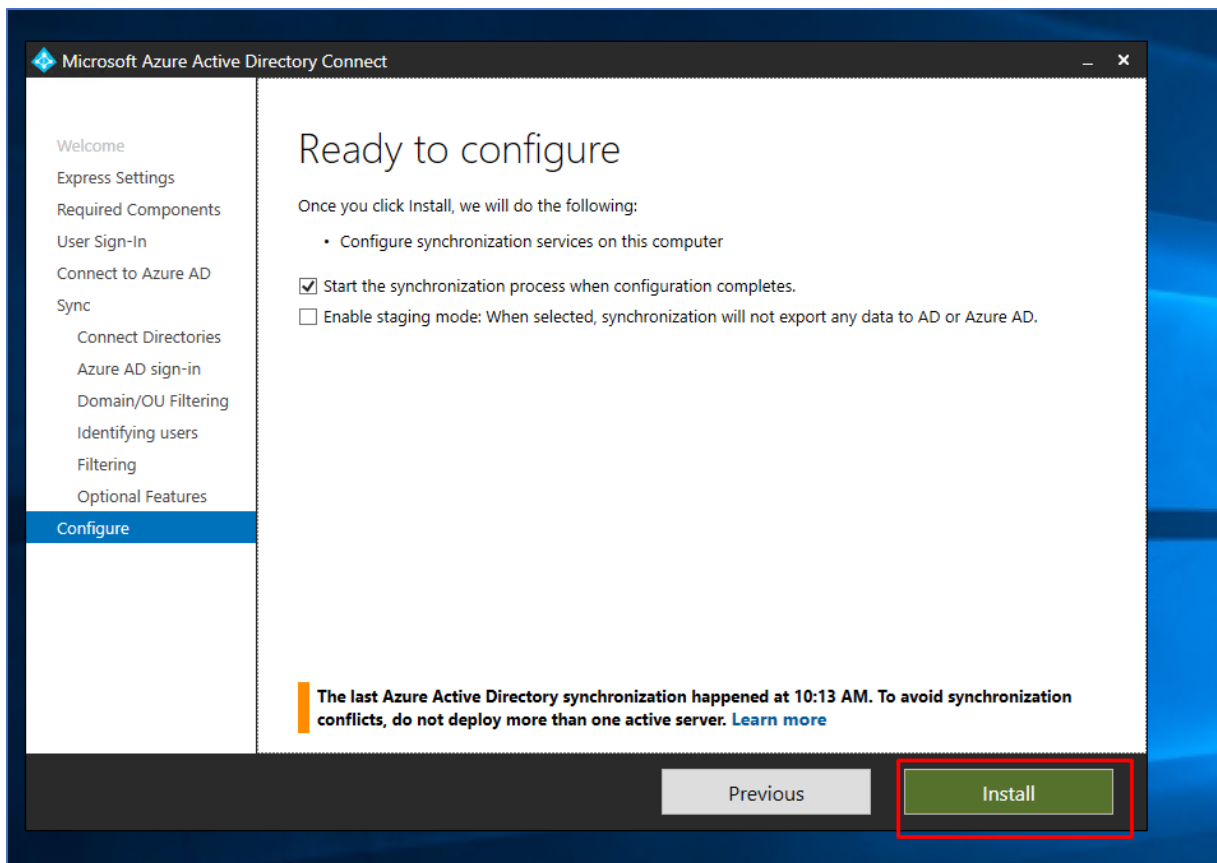
13. «Users are represented only once across all directories» blir ticket av. «Let Azure manage the source anchor» blir også ticket av i vedlagt bilde ovenfor.



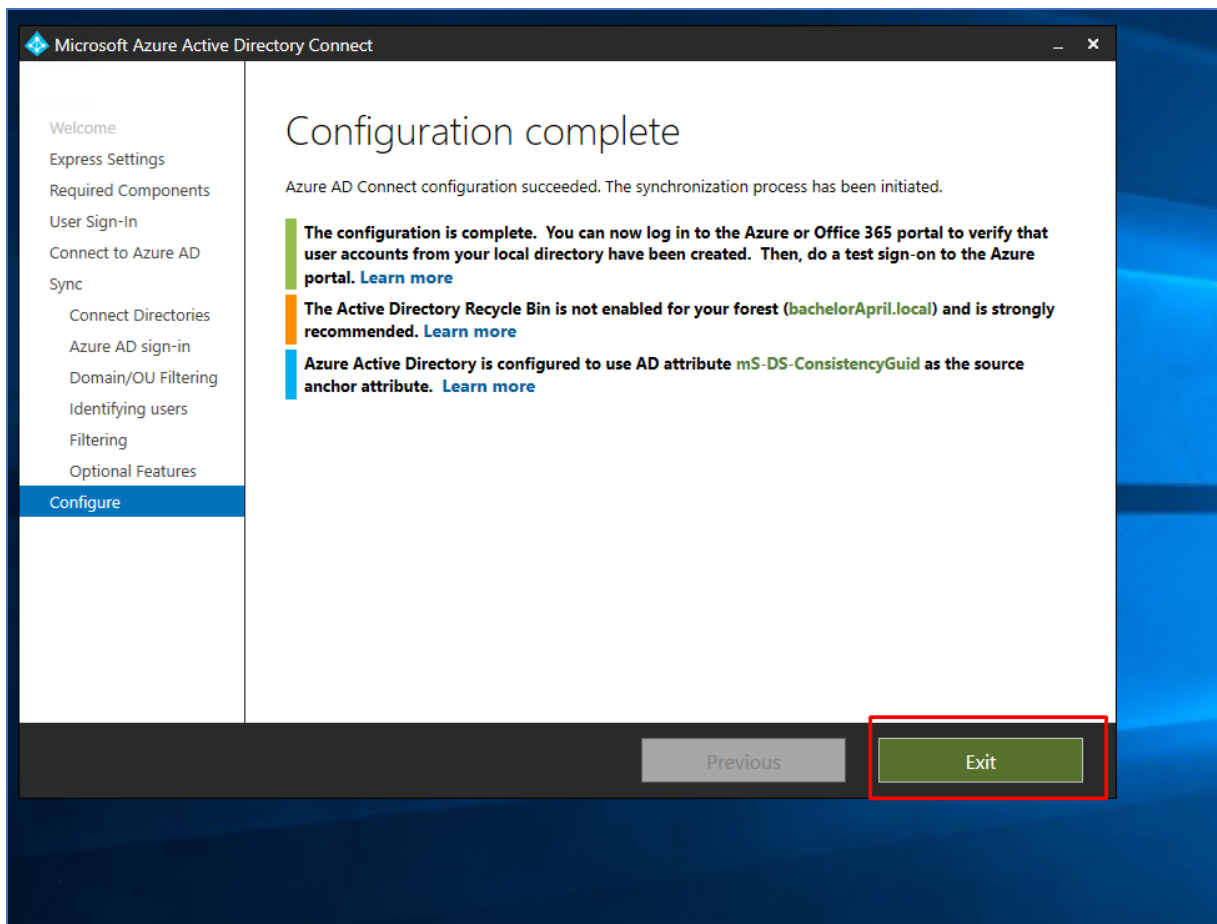
14. Videre er velger jeg å synkronisere alle brukere og enheter.



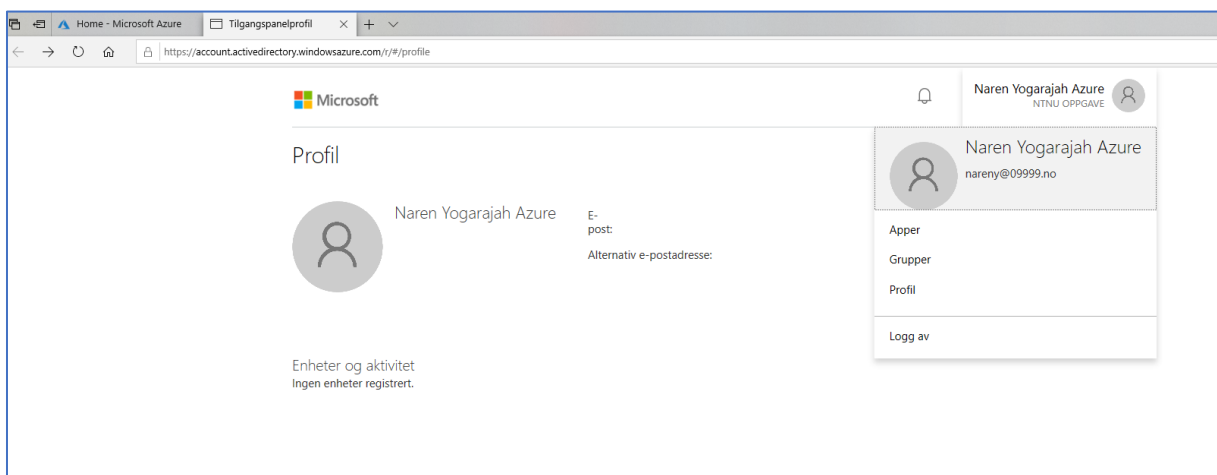
15. Deretter lar jeg default valg som allerede er tikket av stå og klikke meg videre med next knappen.



16. Jeg tikker videre av for å starte synkronisering av prosessen når konfigurasjonen er ferdig. Nå gjenstår det kun å installere AD connect.



17. Ovenfor ser vi at Azure AD Connect har blitt installert suksessfullt.



18. For at password Hash Sync skal gå smertefritt og fungere som normalt med riktig synkronisering mellom AD Connect og Azure velger jeg å endre passordet for brukeren nareny@09999.no. Denne passord endringen kan gjøres på <https://account.activedirectory.windowsazure.com>.

Profil

 Naren Yogarajah Azure

E-post: _____
Alternativ e-postadresse: _____

Administrer konto

Endre passord

[Konfigurer selvbetjent tilbakestilling av passord](#)

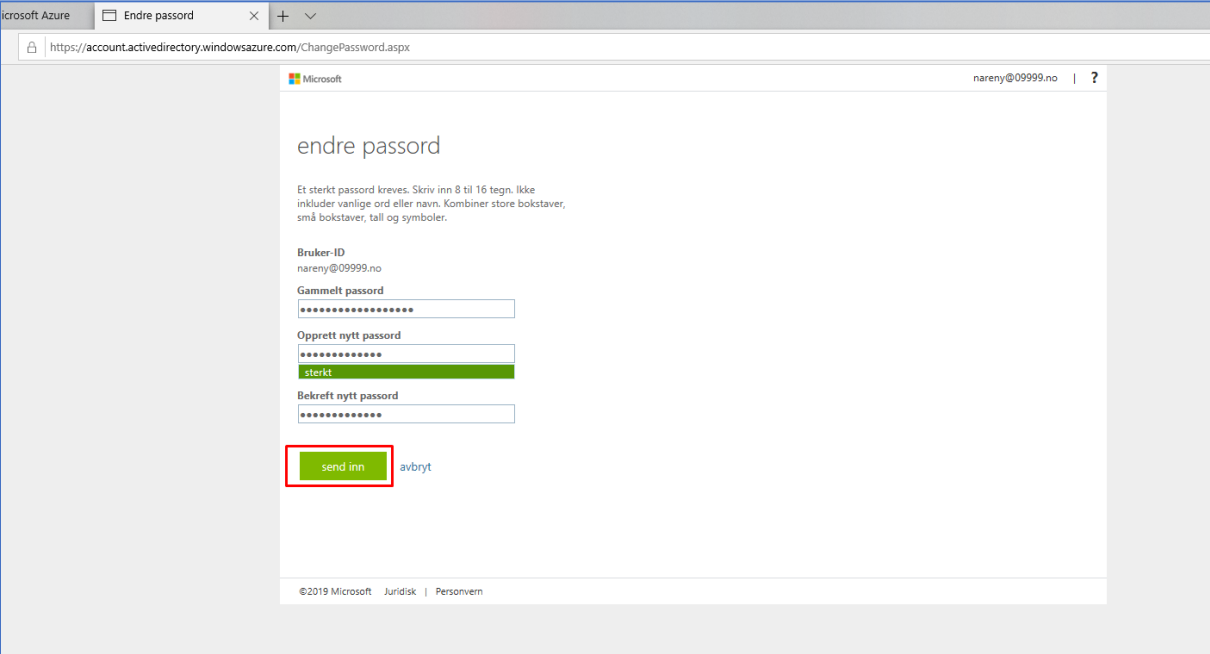
[Ytterligere sikkerhetsbekreftelse](#)

[Les gjennom vilkår for bruk](#)

[Logg av overalt](#)

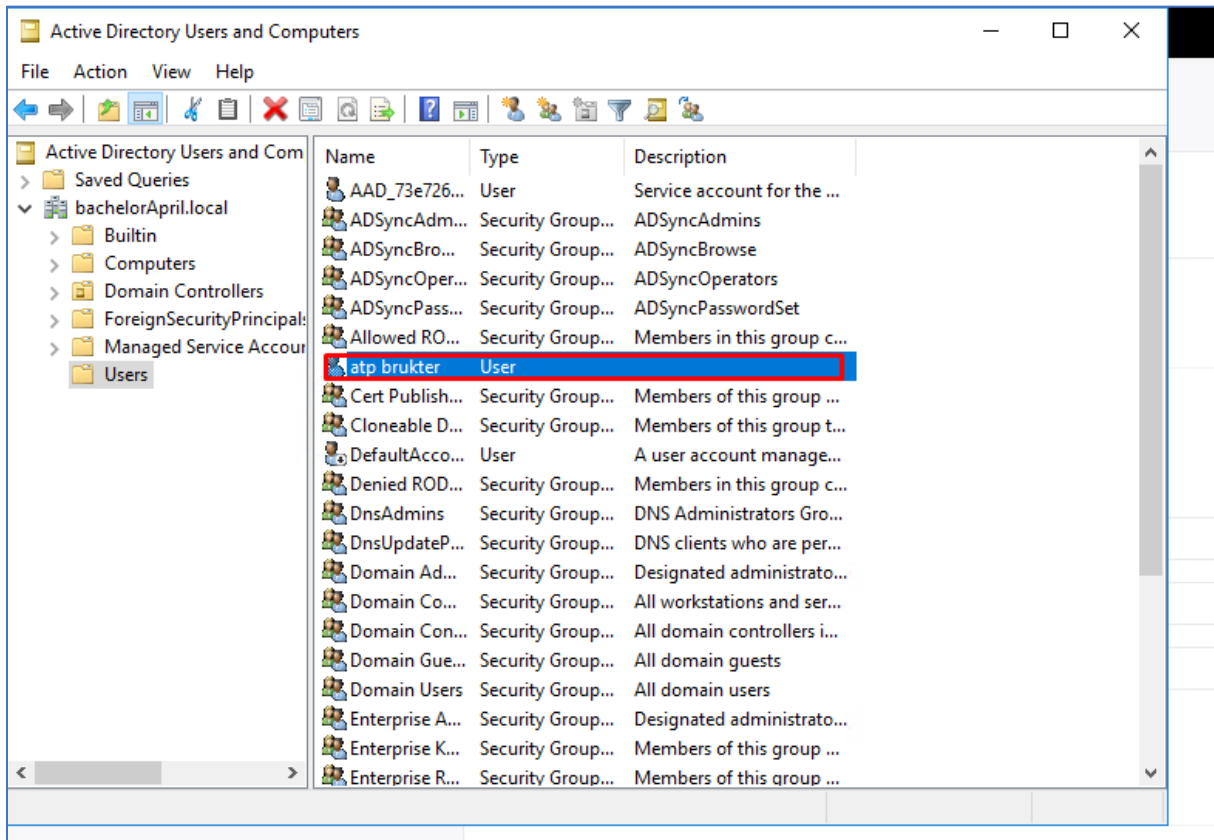
Enheter og aktivitet
Ingen enheter registrert.

19. Videre klikker man på å endre passord.



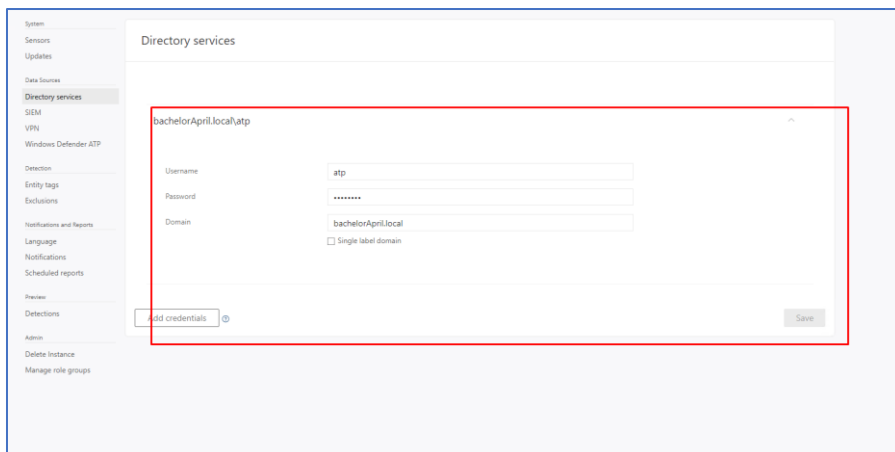
20. Deretter legger man inn ett ny passord og sender inn endringen.

2.2.7 Azure Advanced Threat Protection

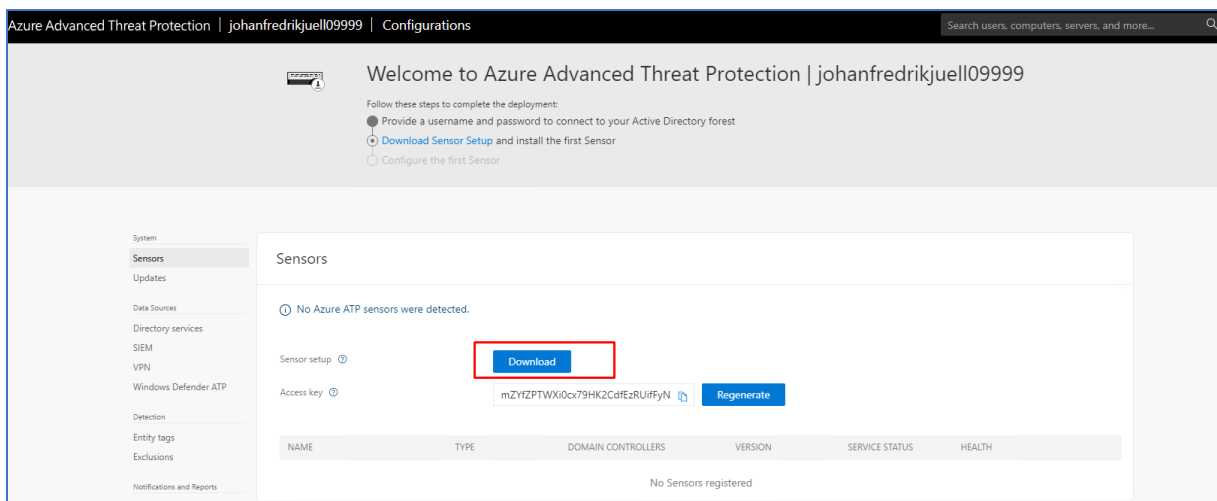


Azure Advanced Threat Protection (Azure ATP) er en sikkerhetstjeneste i Azure som tar i bruk Active Directory signaler for å identifisere, gjenkjenne og investigere avanserte trusler som forekommer i organisasjonen din. Man har i tillegg mulighet til å gjenkjenne identiteter som er kompromittert og andre ondsinnede og skadelige hendelser i organisasjonen.

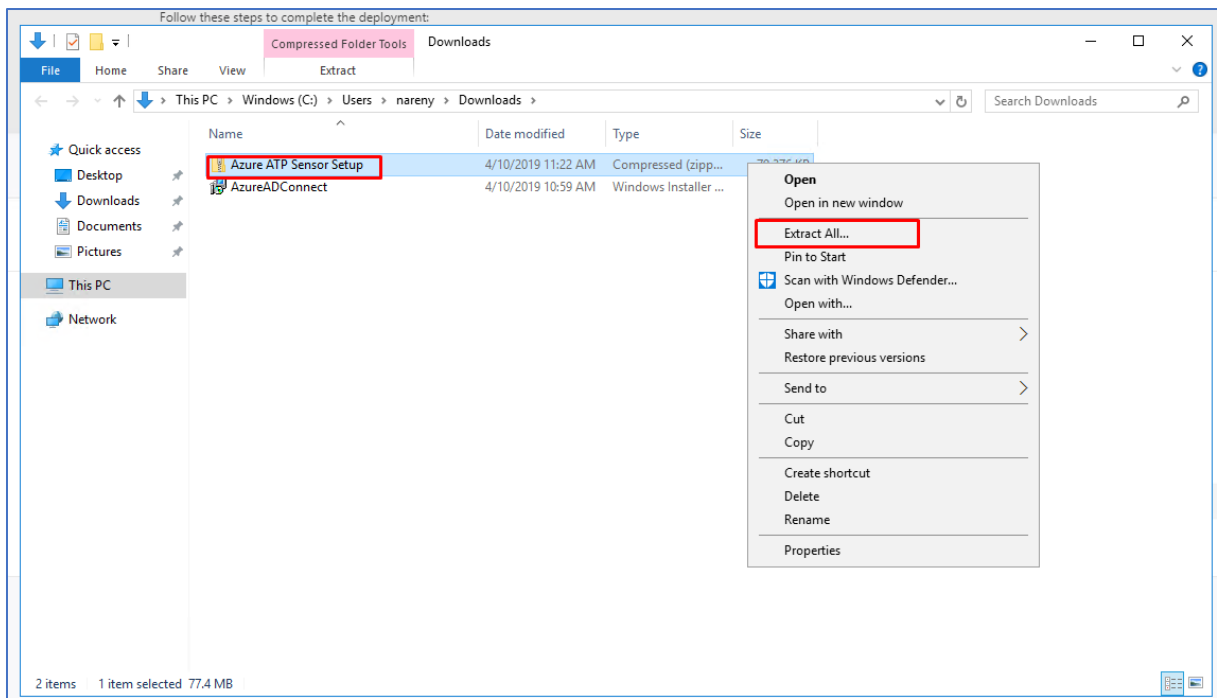
1. Jeg starter med å lage en bruker i domene som ble opprettet tidligere. Brukeren som blir opprettet heter `atp@bachelorApril.local`.



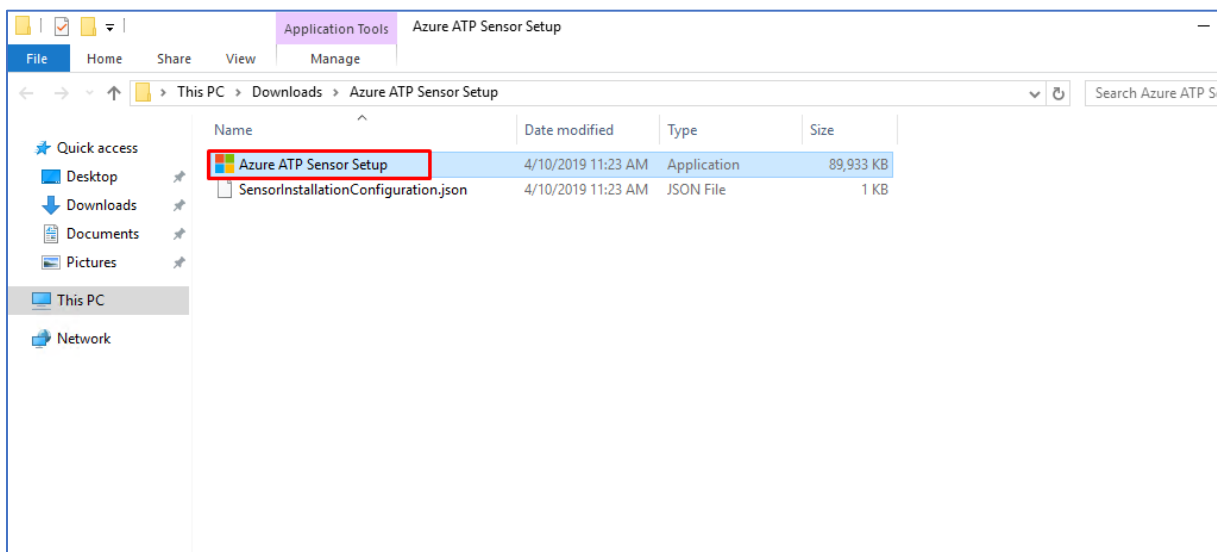
2. For å konfigurere Azure ATP må vi gå videre til <https://portal.atp.azure.com>. Deretter navigerer jeg meg videre frem til Directory services. Der legger jeg inn brukernavn og passordet til brukeren atp@bachelorApril.local som ble opprettet tidligere. Deretter legger jeg inn domene som er tilknyttet denne brukeren. Det er videre viktig å huske å lagre endringene.



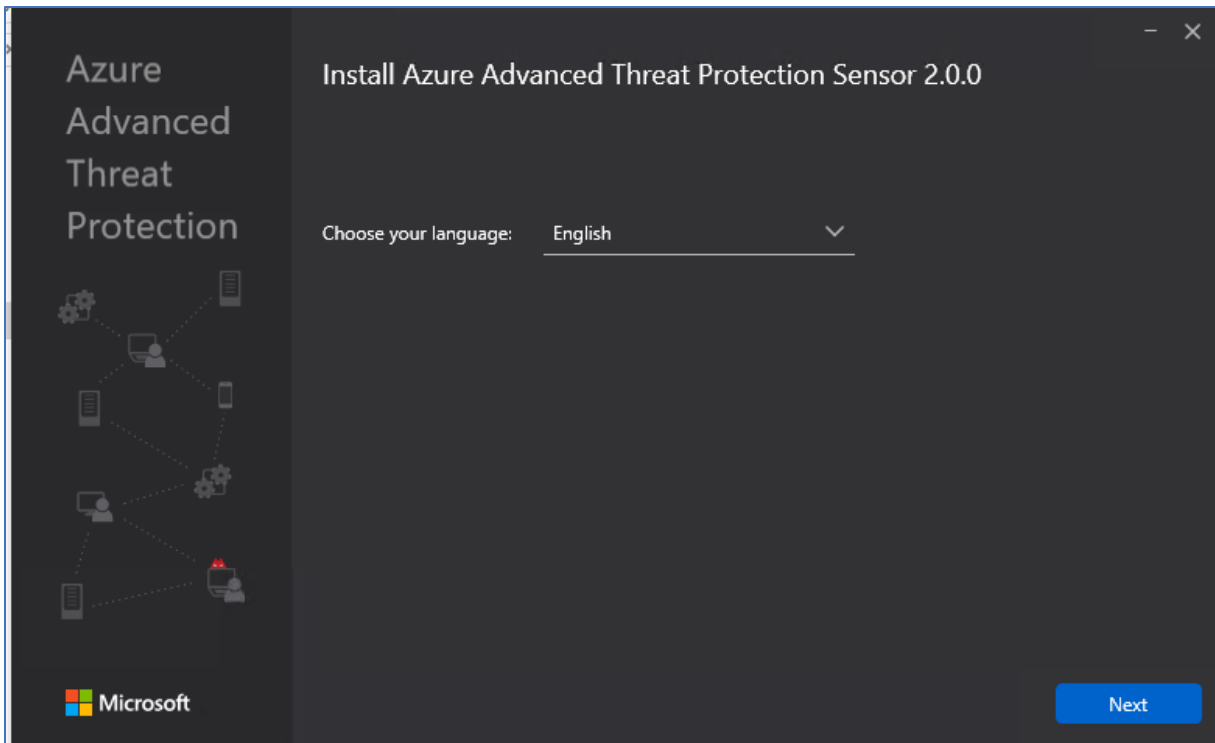
3. Deretter navigerer jeg meg frem til Sensors undermeny. Videre må jeg laste ned sensor installasjons fil ved å klikke på Download knappen.



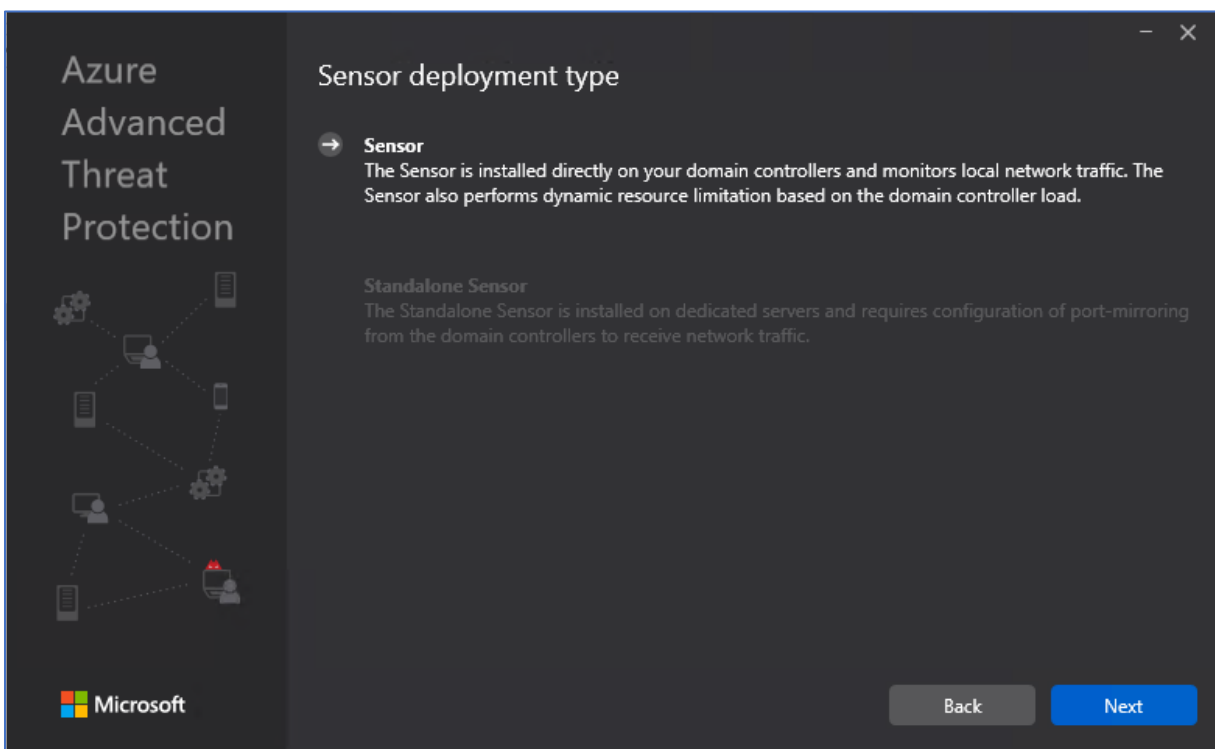
4. Jeg får videre opp en Azure ATP Sensor Setup fil som er en ZIP fil. Jeg høyre klikker på mappe strukturen og pakker opp mappen.



5. Deretter dobbelt klikker jeg på Azure ATP Sensor Setup filen for å installere Azure ATP Sensor.



6. Her velger jeg språket Engelsk og klikker meg videre.



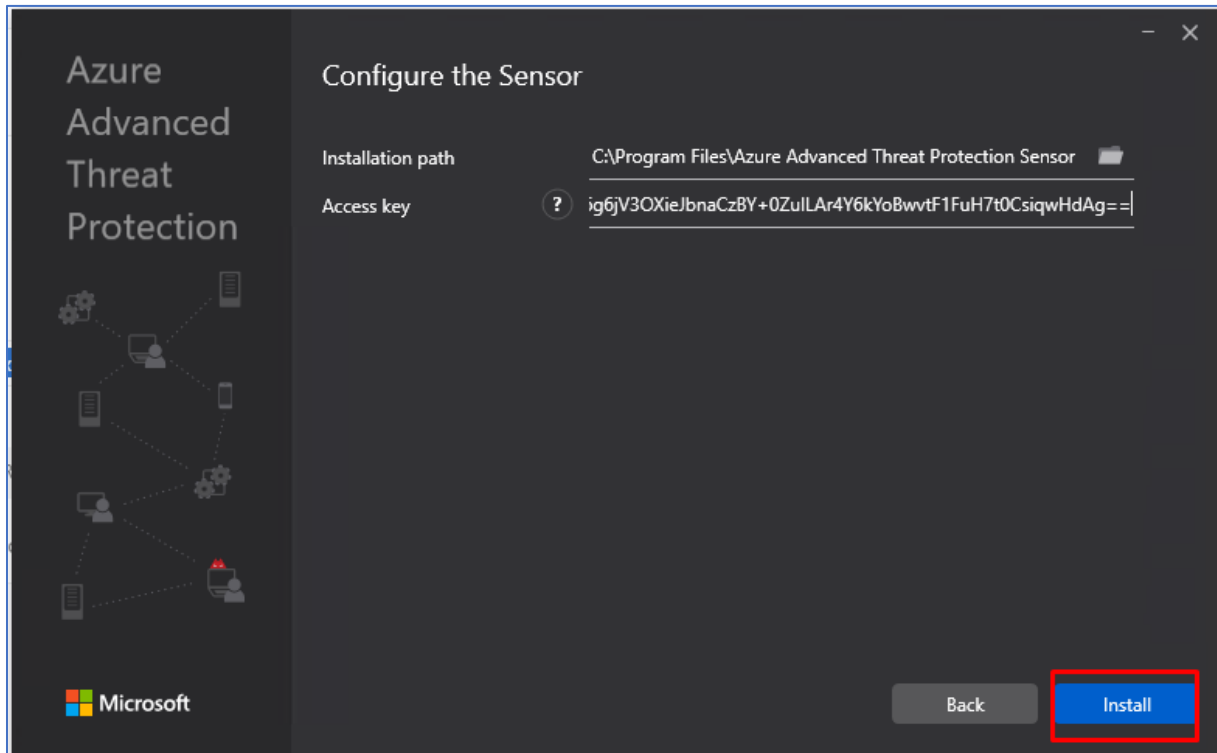
7. Deretter er det bare å klikke videre på next knappen.

Access key ?

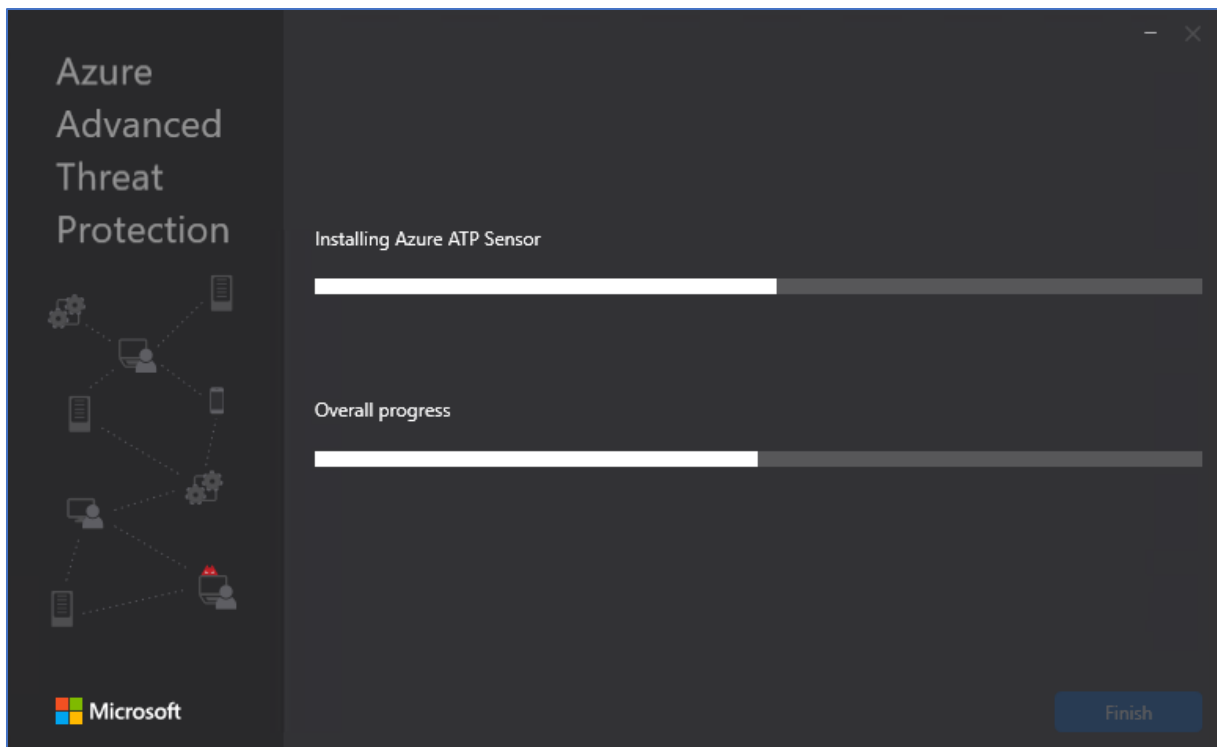
i0Kr1B69jFhiqFRy6Bvjfid9RiLTOe7xw6

Regenerate

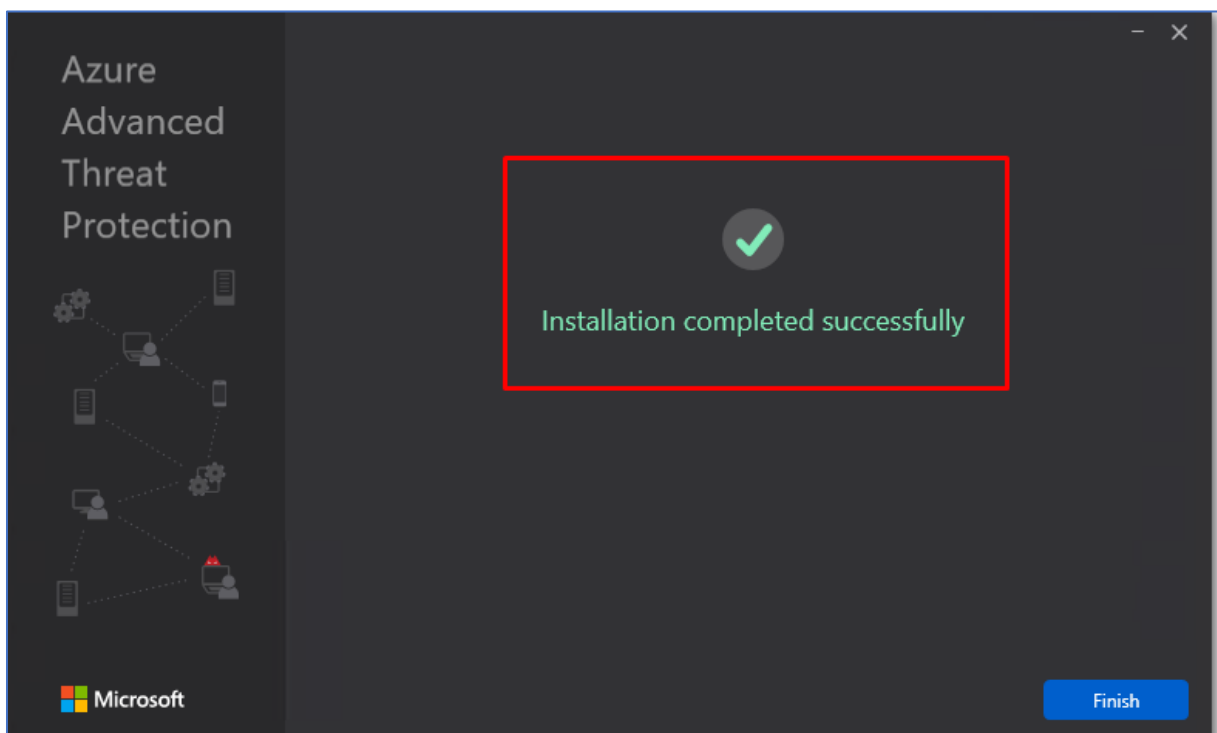
8. Access key fra ATP portal skal kopieres.



9. Denne nøkkelen skal videre limes inn under Access key og deretter er det bare å sette i gang installasjonen.



10. Installasjonen er under progress.



11. Installasjonen av ATP er suksessfull og det har ikke oppstått noen feil meldinger så langt.

NAME	↑	TYPE	DOMAIN CONTROLLERS	VERSION	SERVICE STATUS
SRV16		Sensor	SRV16.bachelorApril.local	2.72.6508	Starting

12. Videre navigerer jeg meg frem til Azure ATP portalen. Deretter under Sensors menyen kan vi se sensoren vår SRV16. Jeg klikker på SRV16.

Sensors

No Azure ATP sensors were detected.

Sensor setup ⓘ

Access key ⓘ

NAME	HEALTH
SRV16	

SRV16

Description

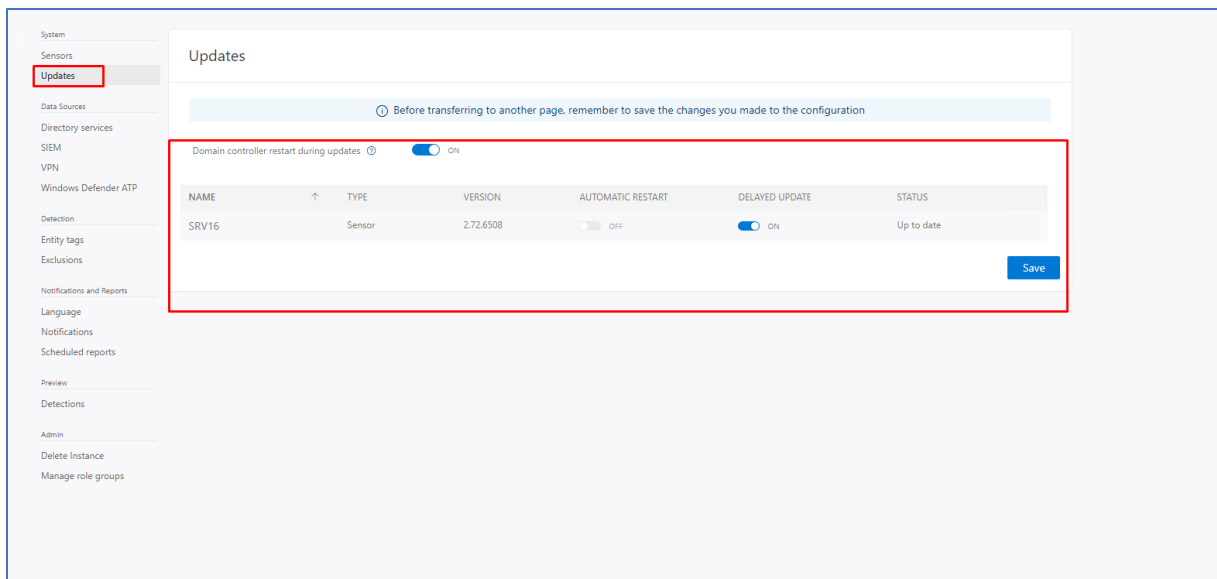
Domain Controller (FQDN) SRV16.bachelorApril.local

Capture network adapters Ethernet

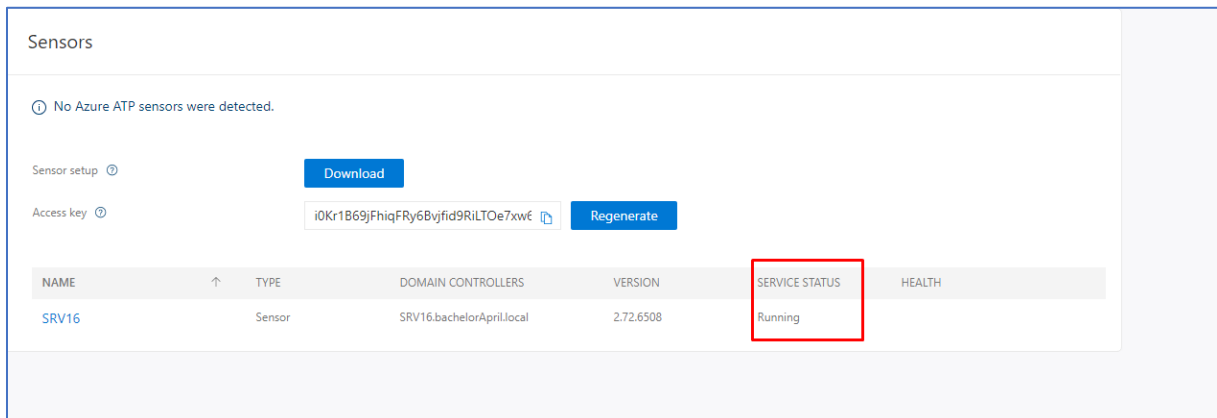
Domain synchronizer candidate ON

Save Cancel

13. Videre tikker jeg av for Ethernet. Deretter tikker jeg av for Domain synchronizer og lagrer endringene.



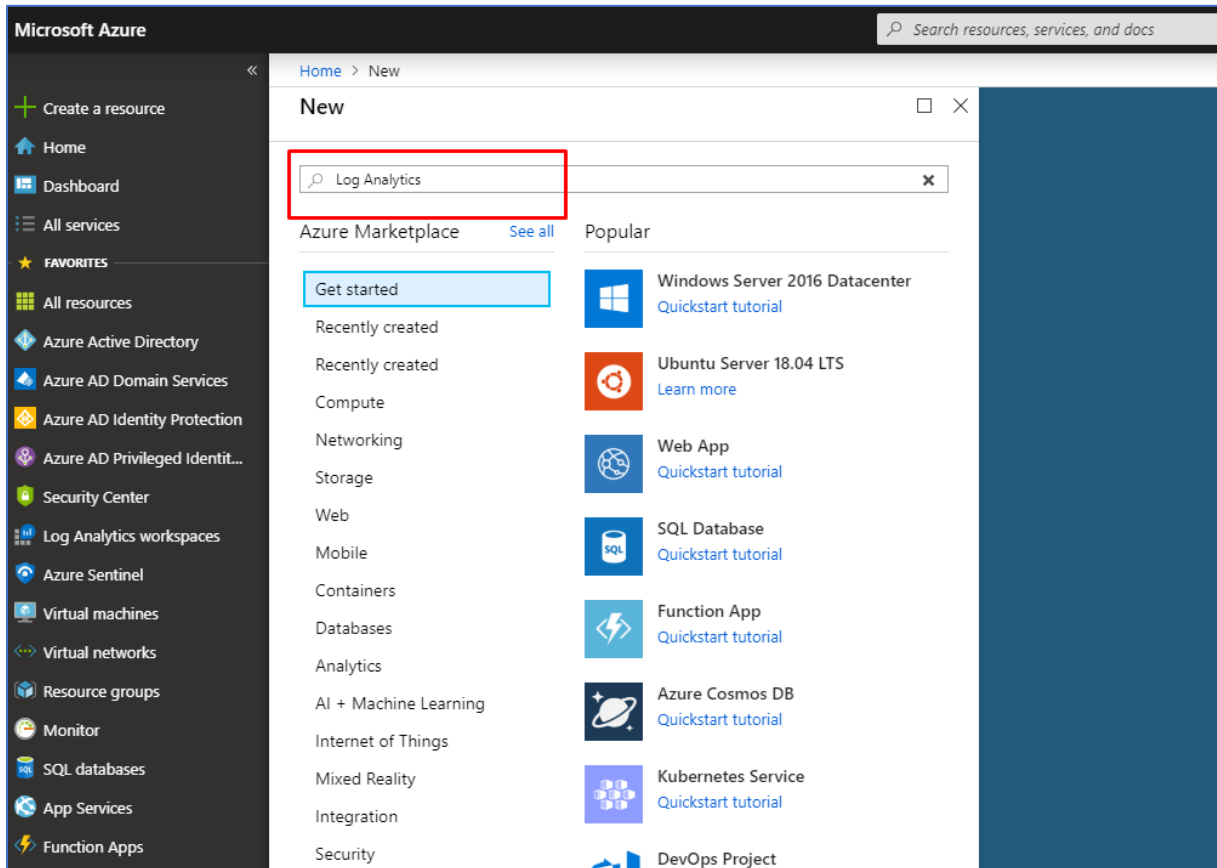
14. Jeg navigerer meg videre til Updates og tikker av for on på omstart av domene kontrollere under oppdateringer. Jeg tikker også av på on for Delayed update. Tilslutt lagrer jeg endringene.



16. Under sensors ser vi tilslutt av service status er på «running». Det betyr at vi har konfigurert Azure ATP riktig!

2.3 Azure Log Analytics

2.3.1 Installasjon av Log Analytics



Azure Log Analytics er en tjeneste i Azure hvor man har mulighet til å samle inn data fra tjenester tilknyttet i Azure. Man setter opp et eget workspace og deretter knytter tjenestene og ved hjelp av KQL spørrespråket kan man legge inn tilpassede queries for å få ut data om ulike type hendelser som f.eks security alerts.

1. Log Analytics skal installeres i Marketplace. Dette gjør vi ved å klikke på Create a resource og deretter søke etter Log Analytics.

Home > New > Log Analytics

Log Analytics

Microsoft

Create a new workspace
Workspace provides visibility and insight across all the machines you manage through Operations Management Suite, including Log Analytics. Workspace stores collected machine data in a region you have specified. To create a new workspace, select the Create button below.

Link an existing workspace to Azure subscription
Do you have an existing workspace in the OMS portal? You can link your workspace with your Azure subscription by selecting the Create button below.

About Log Analytics
The Microsoft Operations Management Suite (OMS) takes IT management solutions to the cloud and gives you greater control and new capabilities across your hybrid cloud. Manage and protect Azure or AWS, Windows Server or Linux, VMware or OpenStack with a cost-effective, all-in-one cloud IT management solution

[Save for later](#)

Publisher: Microsoft

Useful Links:
[Watch Video](#)
[Learn More](#)
[Documentation](#)

Select a software plan

Log Analytics
Collect, search and visualize machine data from on-premises and cloud

Create

2. Deretter klikker jeg på Create knappen for å opprette et Log Analytics Workspace. Vi har et valg meny ovenfor Create knappen, det blir satt til å være default på Log Analytics og dermed trenger man ikke å gjøre noen endringer her.

Home > New > Log Analytics > Log Analytics workspace

Log Analytics workspace

Create new or link existing workspace

Create New Link Existing

* Log Analytics Workspace ⓘ
DefaultWorkspace-3f6b0f35-d667-4770-a... ✓

* Subscription
Pay-As-You-Go

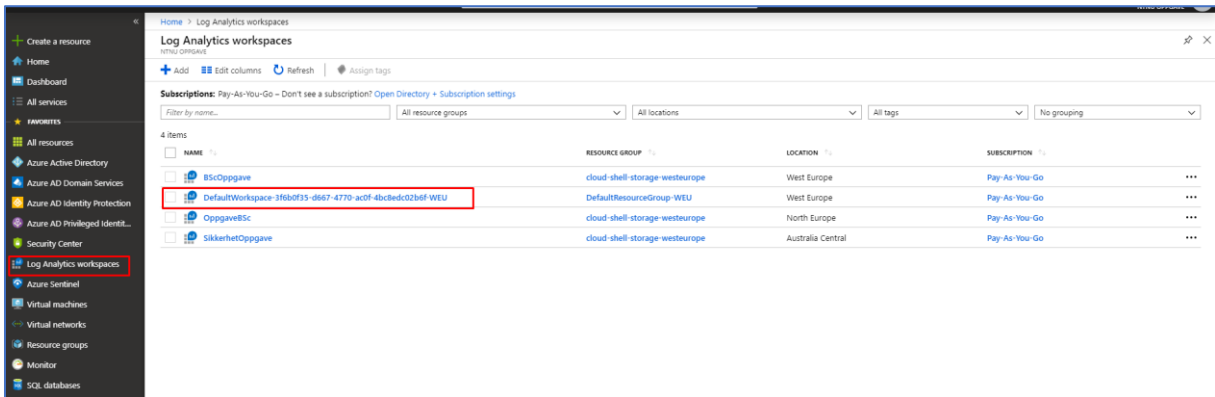
* Resource group ⓘ
 Create new Use existing
cloud-shell-storage-west europe

* Location
North Europe

* Pricing tier
Per GB

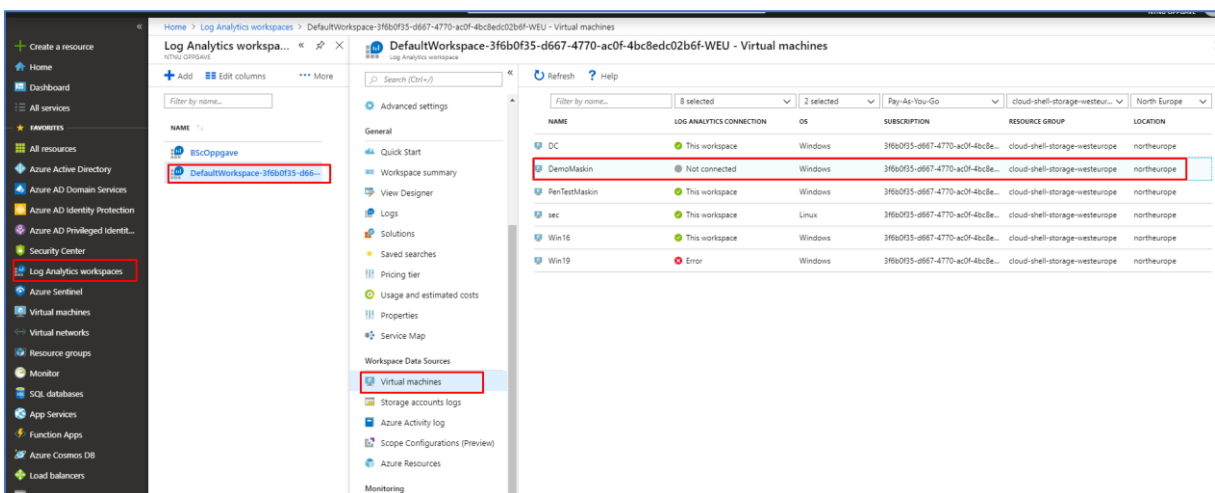
OK

3. Man oppretter et nytt Log Analytics Workspace og legger inn et navn for workspace. Deretter blir Subscription Pay-As-You-Go valgt. Videre velger man Use Existing Resource group til å være cloud-shell-storage-west europe. North Europe er satt til Location og Pricing tier er satt til default.

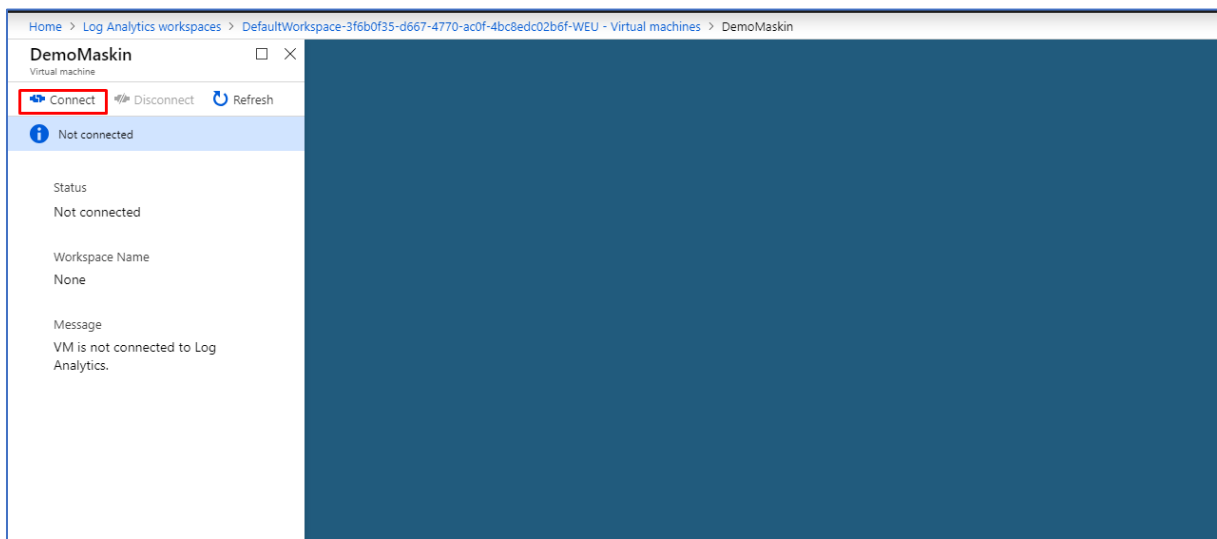


4. Ovenfor ser vi vår Log Analytics Workspace som har blitt opprettet.

2.3.2 Tilkobling av virtuelle maskiner til Log Analytics



1. For å tilkoble dine virtuelle maskiner til Log Analytics må vi navigere oss frem til Log Analytics Workspaces under Favorites i Azure Portal.
2. Deretter klikker vi på DefaultWorkspace.
3. Videre navigerer vi oss frem til Virtual machines.
4. Deretter klikker jeg på DemoMaskin. Dette er den virtuelle maskinen som skal tilknyttes til Log Analytics.



5. Videre klikker jeg på Connect for å tilkoble VMen min til Log Analytics Workspace.

Refresh ? Help

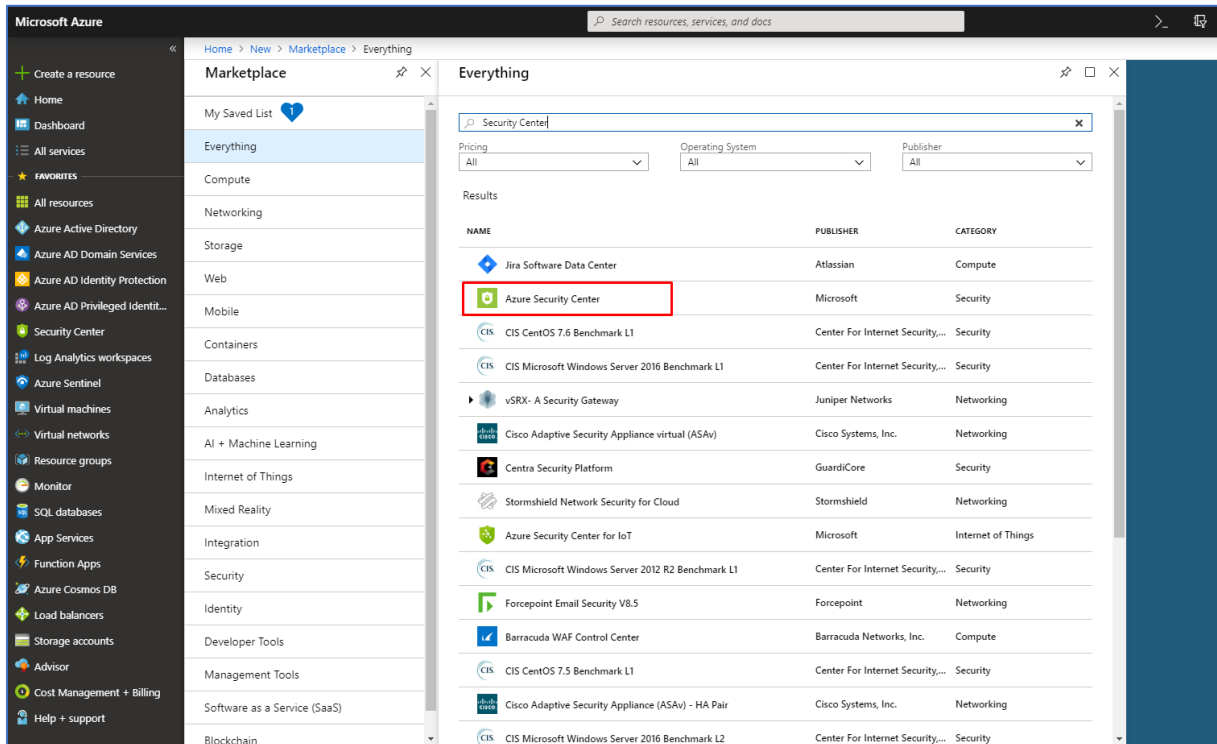
Filter by name... 8 selected 2 selected Pay-As-You-Go cloud-shell-storage-westeur... North Europe

NAME	LOG ANALYTICS CONNECTION	OS	SUBSCRIPTION	RESOURCE GROUP	LOCATION
DC	✔ This workspace	Windows	3f6b0f35-d667-4770-ac0f-4bc8e...	cloud-shell-storage-westeur...	northeurope
DemoMaskin	✔ This workspace	Windows	3f6b0f35-d667-4770-ac0f-4bc8e...	cloud-shell-storage-westeur...	northeurope
PenTestMaskin	✔ This workspace	Windows	3f6b0f35-d667-4770-ac0f-4bc8e...	cloud-shell-storage-westeur...	northeurope
sec	✔ This workspace	Linux	3f6b0f35-d667-4770-ac0f-4bc8e...	cloud-shell-storage-westeur...	northeurope
Win16	✔ This workspace	Windows	3f6b0f35-d667-4770-ac0f-4bc8e...	cloud-shell-storage-westeur...	northeurope
Win19	✘ Error	Windows	3f6b0f35-d667-4770-ac0f-4bc8e...	cloud-shell-storage-westeur...	northeurope

6. Nå ser vi at DemoMaskin er tilkoblet Log Analytics Workspace. Dermed har man mulighet til å få inn data fra DemoMaskin inn til Log Analytics.

2.4 Azure Security Center

2.4.1 Installasjon av Azure Security Center




Azure Security Center er en tjeneste i Microsoft Azure som fungerer som et Security Management System. Azure Security Center er et system som er med på å styrke sikkerheten av dine data i Azure og du får muligheten til Advanced threat Protection. Med Azure Security Center har du mulighet til å få verktøy som er med på å sikre nettverket ditt, sikre tjenestene på Azure plattformen og ikke minst en kontinuerlig oversikt over hva og hvilke trusler som forekommer i Azure cloud miljøet ditt.

1. For å installere Azure Security Center må vi installere dette via Marketplace. Jeg søker etter Security Center og legger til dette.

Home > New > Marketplace > Everything > Azure Security Center

Azure Security Center

Microsoft



[Create](#) [Save for later](#)

Security and Audit is now integrated into Azure Security Center. Azure Security Center is a security management tool that allows you to gain insight into your security state across hybrid cloud workloads, reduce your exposure to attacks, and respond to detected threats quickly. You can try Azure Security Center for free for the first 30 days. Afterwards, you will be billed per node regardless of the workspace pricing tier.

GAIN INSTANT SECURITY INSIGHTS ACROSS ALL YOUR IT ENVIRONMENTS

Manage security across all your hybrid cloud workloads—on-premises, Azure, and other cloud platforms—from Azure Security Center. Install an agent onto your cloud and on-premises virtual machines to monitor your security state, and identify issues such as systems with missing security updates, missing or outdated antimalware, and insecure OS configurations that can make them vulnerable to attack. It also provides insight into the security state of your network, storage and data, applications and access controls. Configure security policies per subscription to ensure new or current virtual machines maintain your security settings.

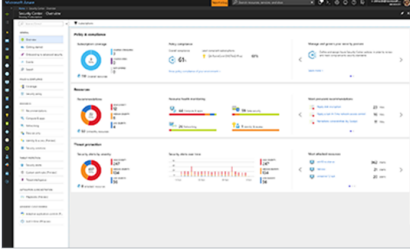
ENABLE PROTECTIONS TO REDUCE YOUR EXPOSURE TO ATTACKS

Security Center gives you several controls to help you reduce your exposure to attacks. Adaptive Applications Controls use machine learning to recommend applications that should be whitelisted to help you block malware and other unwanted applications from running. Just-in-Time VM Access allows you to protect against threats such as brute force attacks by reducing access to virtual machine management ports only when it is needed.

RESPOND QUICKLY TO DETECTED THREATS

By leveraging Microsoft's vast global threat intelligence and applying behavioral analytics, Security Center can detect successful or attempted attacks. Once a threat has been detected, for example a malicious process being executed or an attempt by the attacker to move laterally within your environment, you can explore this threat in the Investigation Path. It's an interactive and visual way to explore all the related entities of an attack and assess the scope and impact of an attack. You can run a Playbook built on Azure Logic Apps to quickly deploy solve against the attack.

Useful Links
[Watch Video](#)
[Pricing Details](#)
[Documentation](#)



2. Videre klikker jeg på Create knappen for å installere Azure Security Center.

Home > New > Marketplace > Everything > Azure Security Center > Getting started > Security Center - Overview

Security Center - Overview

Showing subscription: Pay-As-You-Go

Search (Ctrl+F)

Subscriptions

Policy & compliance

Secure score **393** OF 735
 Security score impact changed. [Learn more](#)
[Review your secure score](#)

Least compliant regulatory standards

SOC TSP	1 of 12 passed controls
ISO 27001	3 of 22 passed controls
PCI DSS 3.2	6 of 31 passed controls

Subscription coverage

Fully covered	1
Partially covered	0
Not covered	0
TOTAL	1

12 Covered resources

Make alert data available to your SIEM

You can make Security Center alerts available to a SIEM connector

[Set up SIEM connector](#)

Resource security hygiene

Recommendations

High Severity	15
Medium Severity	2
Low Severity	2
TOTAL	19

12 Unhealthy resources

Resource health monitoring

6 Compute & apps	4 Data & storage
1 Networking	1 Identity & access
0 IoT hubs & resources	

Top recommendations by secure score impact

- Enable MFA for accounts with owner permissions o... [+50](#)
- Remediate vulnerabilities on your SQL databases (P... [+30](#)
- Enable Network Security Groups on subnets [+30](#)

Threat protection

Security alerts by severity

High Severity	5
Medium Severity	12
Low Severity	8
TOTAL	25

8 Attacked resources

Security alerts over time

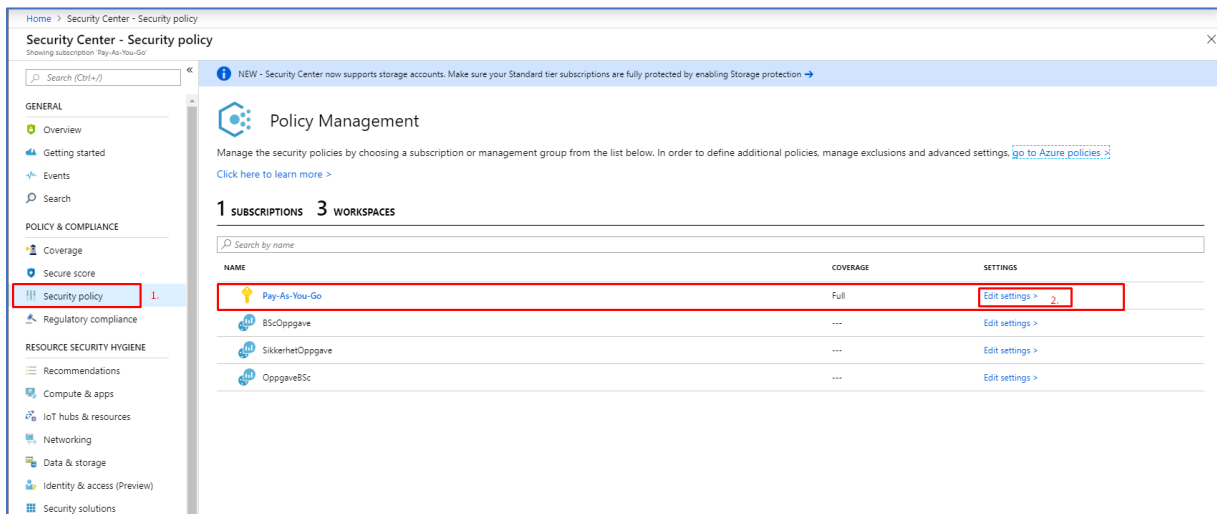
High severity	5
Medium severity	12
Low severity	8

Most prevalent alerts

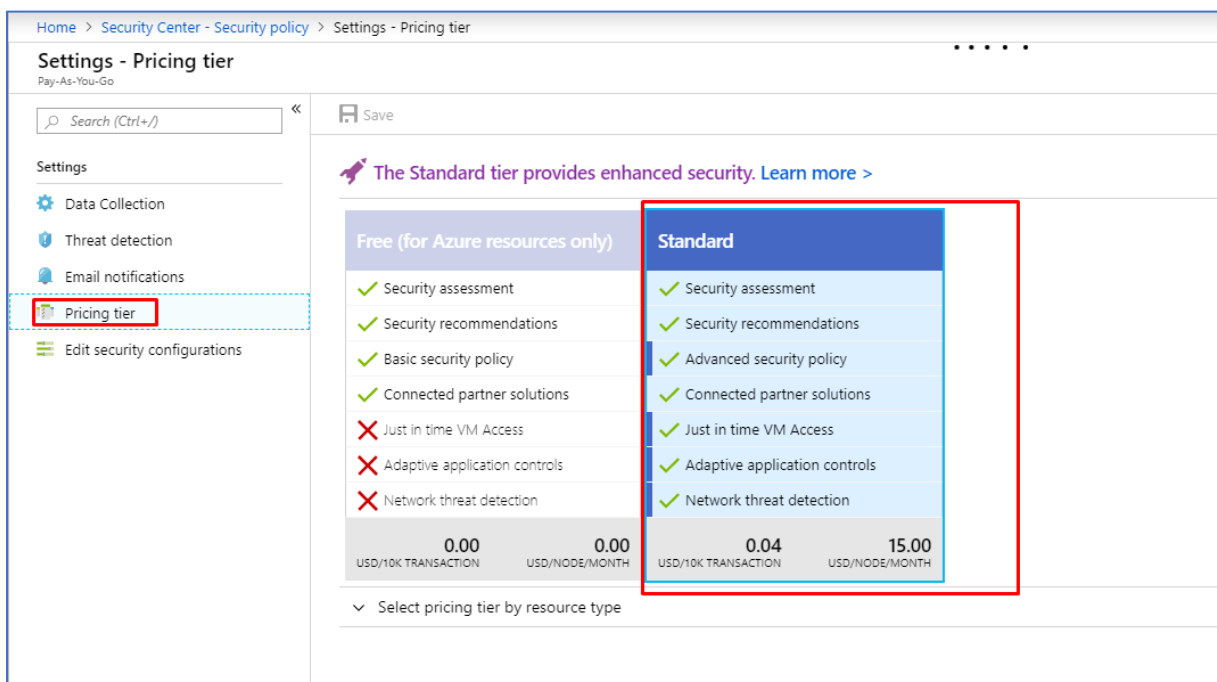
- [Preview] Traffic from unrecommended IP... 5 Resources
- Antimalware Action Taken 2 Resources
- Suspicious authentication activity 2 Resources

3. Nå har vi kommet inn på dashboardet til Azure Security Center.

2.4.2 Standard Tier Subscription



1. For å sette Security Center plan til Standard Tier versjon navigerer vi oss frem til Security Policy under Policy & Compliance. Deretter klikker vi på Edit Settings ved siden av Pay-AS-You-Go Subscription.



2. Videre navigerer vi oss frem til Pricing tier under Settings menyen. Deretter klikker vi på Standard og save knappen for å lagre endringene vi har gjort.

2.4.3 Policy & Compliance

2.4.3.1 Data Collection

The screenshot shows the 'Security Center - Overview' page. The left-hand navigation pane is expanded to 'Policy & Compliance', with 'Security policy' highlighted. The main content area displays several key metrics:

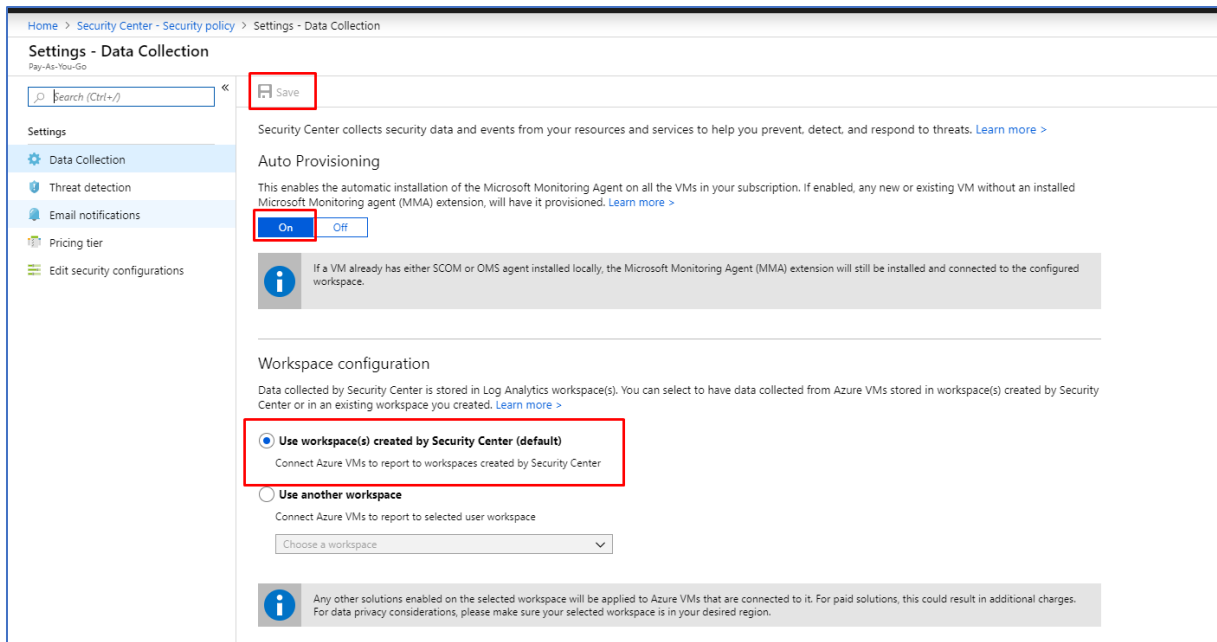
- Secure score:** 403 OF 735. A note indicates the score has changed.
- Least compliant regulatory standards:** SOC TSP (1 of 12 passed), ISO 27001 (3 of 22 passed), and PCI DSS 3.2 (6 of 31 passed).
- Subscription coverage:** 11 covered resources, 0 fully covered, 1 partially covered, and 0 not covered.
- Resource security hygiene:** 17 total recommendations (13 High Severity, 2 Medium Severity, 2 Low Severity) and 11 unhealthy resources.
- Resource health monitoring:** 5 Compute & apps, 4 Data & storage, 1 Networking, and 1 Identity & access.

1. For å kunne overvåke dine virtuelle maskiner i Azure må du slå på Data Collection. Dette gjør du under Security policy i undermeny Policy & Compliance i Security Center.

The screenshot shows the 'Security Center - Security policy' page. The left-hand navigation pane is expanded to 'Policy & Compliance', with 'Security policy' highlighted. The main content area displays the 'Policy Management' section, which includes a table of subscriptions:

NAME	COVERAGE	SETTINGS
Pay-As-You-Go	Partial	Edit settings >

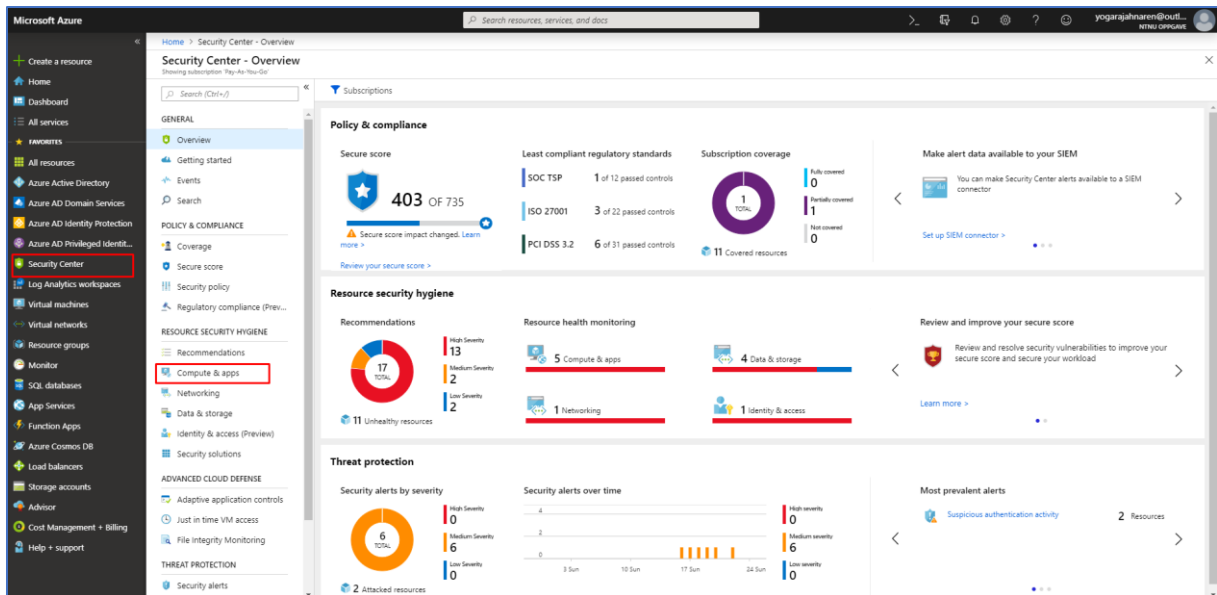
2. Videre klikker du på Edit settings ved siden av Pay-As-You-Go Subscription.



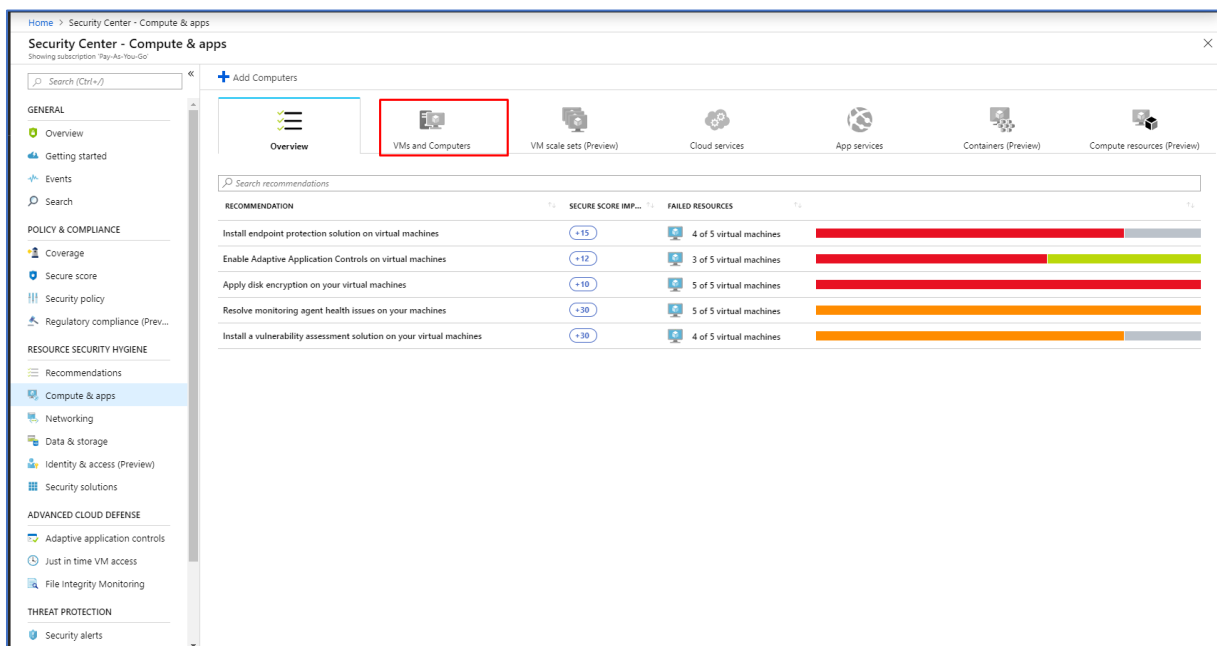
3. Deretter klikker du på On under Auto Provisioning. Dette gjør at du får tilgang for automatisk installasjon av Microsoft Monitoring Agent på alle dine virtuelle maskiner som befinner seg i Azure miljøet ditt.

4. Videre kan du også tikke av for Use workspace(s) created by Security Center (default) under Workspace configuration. Dette tillater deg å få data som er samlet inn i Security Center til også å bli lagret i Security Center sitt default workspace.

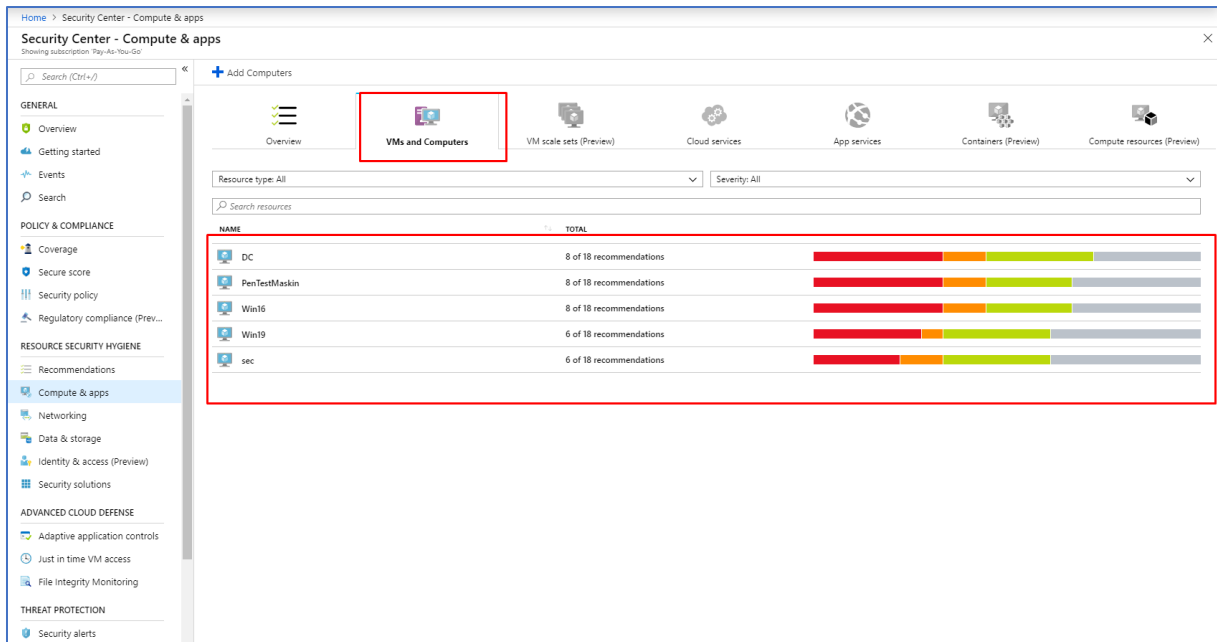
5. Tilslutt er det viktig å huske på å klikke på Save knappen øverst til venstre hjørne. Det er da dine endringer trår til og man får fullt ut ta i bruk tjenestene.



6. Nå kan du i Security Center, gå videre til Compute & apps i undermeny Resource Security Hygiene.

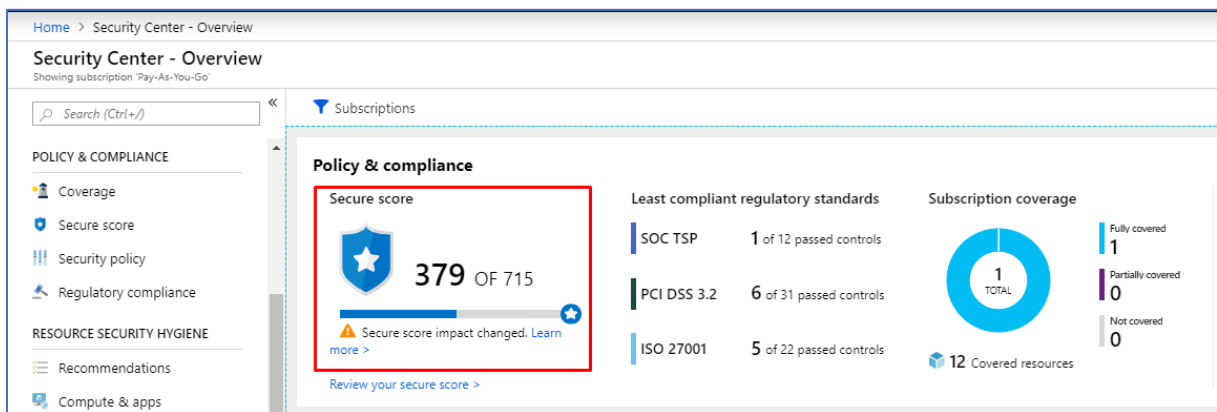


7. Deretter klikker du på VMs and Computers.



8. Her kan du nå se alle virtuelle maskiner og on-premises maskiner som er under overvåking på Security Center. Virtuelle maskiner blir markert med blå symbol skjerm. Mens, on-premises maskin blir markert som lilla stasjonær datamaskin symbol i VMs and Computers. Data fra disse maskinene blir videre utgangspunkt for Security Alerts, trussel deteksjon i Security Center og Log Analytics.

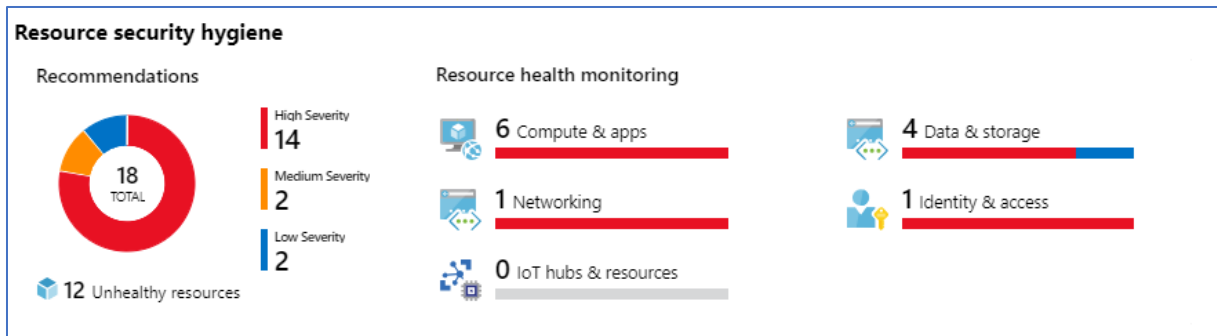
2.4.3.2 Secure Score



1. Secure Score viser en total kalkulasjon som er gjort av alle anbefalinger som bør utføres i Azure miljøet ditt. Secure Score vises i ditt dashboard i Azure Security Center.

2.4.4 Resource Security Hygiene

2.4.4.1 Recommendations



1. Under Resource Security Hygiene får man anbefalinger om tiltak som bør settes i gang umiddelbart. Resource Security Hygiene vises i dashboard i Azure Security Center.

Home > Security Center - Overview > Recommendations

Recommendations

18 TOTAL
12 Unhealthy resources

High Severity: 14
Medium Severity: 2
Low Severity: 2

Resource health monitoring

- 6 Compute & apps
- 1 Networking
- 0 IoT hubs & resources
- 4 Data & storage
- 1 Identity & access

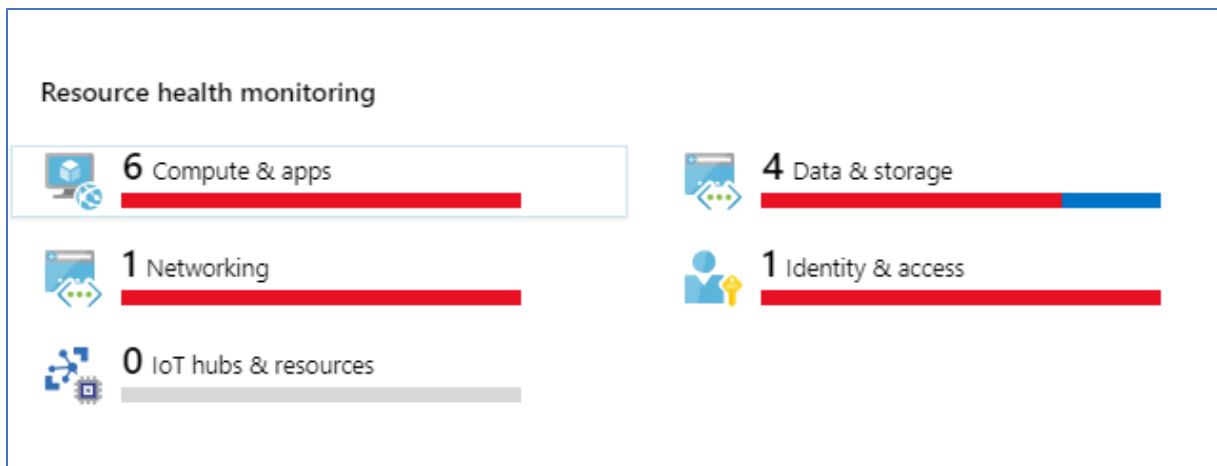
Review and improve your secure score

Review and resolve security vulnerabilities to improve your secure score and secure your workload

Learn more >

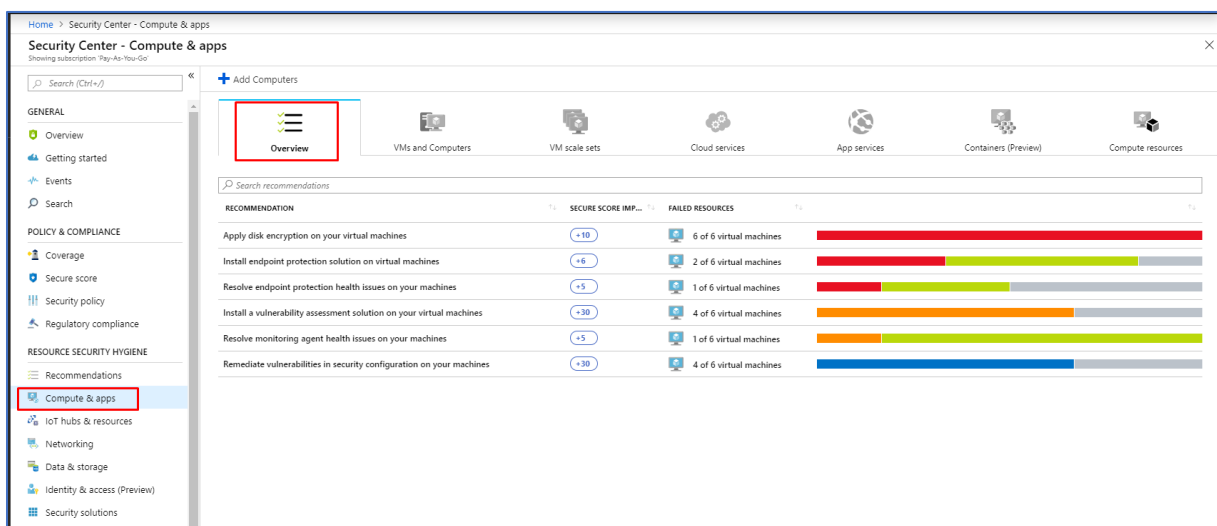
RECOMMENDATION	SECURE SCORE IMPACT	FAILED RESOURCES
Enable MFA for accounts with owner permissions on your subscription (Preview)	+50	1 of 1 subscriptions
Apply a Just-In-Time network access control	+30	6 of 6 virtual machines
Remove external accounts with owner permissions from your subscription (Preview)	+30	1 of 1 subscriptions
Remediate vulnerabilities on your SQL databases (Preview)	+30	1 of 1 SQL databases
Enable Network Security Groups on subnets	+30	1 of 1 subnets
Provision an Azure AD administrator for SQL server	+20	1 of 1 SQL servers
Harden NSGs of Internet facing virtual machine	+17	5 of 6 virtual machines
Harden Network Security Group rules of internet facing virtual machines (Preview)	+15	3 of 6 virtual machines
Apply disk encryption on your virtual machines	+10	6 of 6 virtual machines
Require secure transfer to storage account	+10	1 of 2 storage accounts
Close management ports on your virtual machines	+8	5 of 6 virtual machines
Install endpoint protection solution on virtual machines	+6	2 of 6 virtual machines
Resolve endpoint protection health issues on your machines	+5	1 of 6 virtual machines
Enable auditing on SQL server	+5	1 of 1 SQL servers

2. Hvis man klikker på hjulet som ligger under Recommendations får man mer detaljert informasjon om hvilke anbefalinger som bør settes i gang.

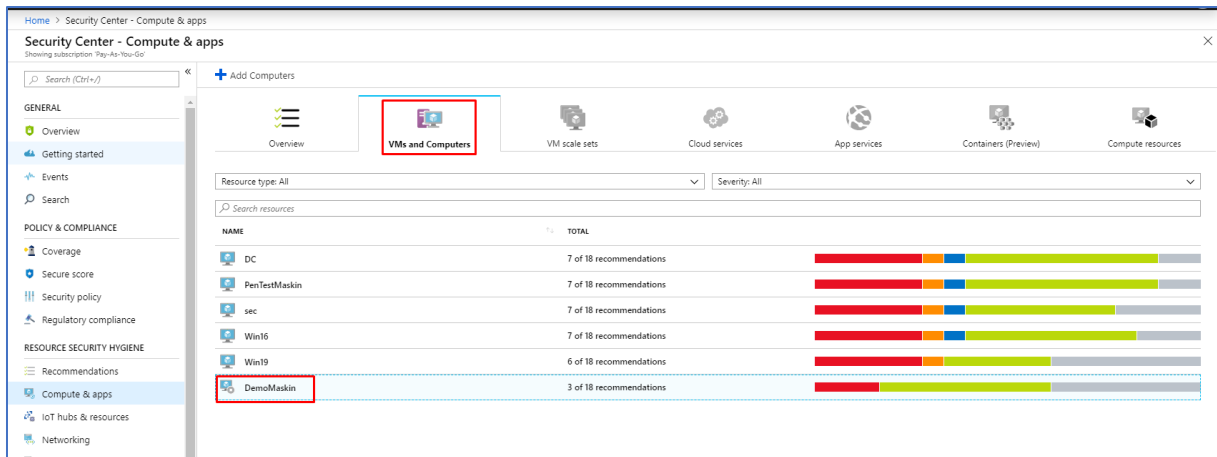


3. Vi har ulike kategorier av anbefalinger som bør utføres. De deles opp i Compute & apps, Networking, IoT hubs & resources, Data & storage og Identity & access.

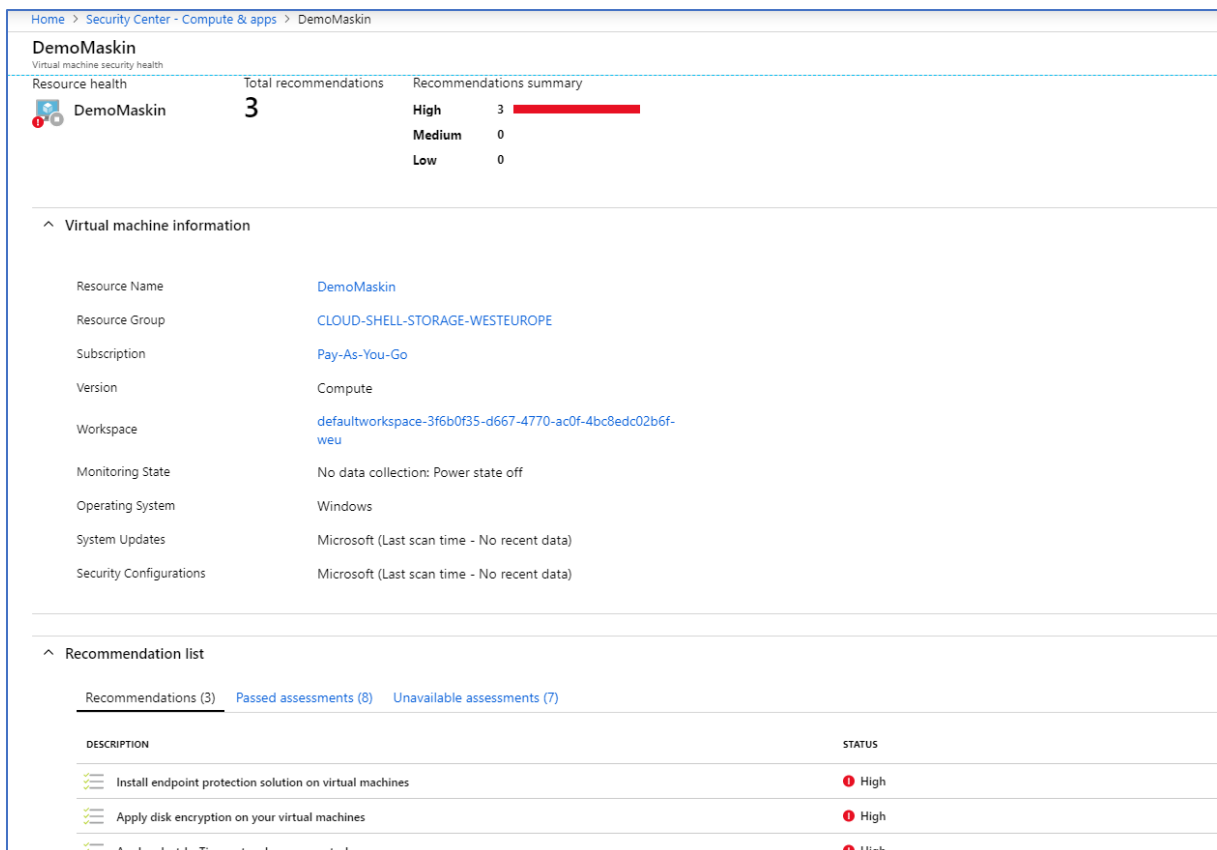
2.4.4.2 Compute & apps



1. Under Compute & apps får du en oversikt over anbefalinger som bør settes i gang. De blir kategorisert etter viktighets og fare nivå.



2. Videre hvis man går over til VMs and Computers får man et helhetlig bilde av hvilke maskiner som bør sette i gang anbefalinger etter farenivå. Hvis vi klikker på DemoMaskin får vi følgende:



3. Nå får vi en mer detaljert informasjon om hvilke anbefalinger som bør settes i gang og vi ser også at nivået er på High ettersom det er markert med rød farge. Da er det ofte lurt å installere disse anbefalingene umiddelbart slik at man sikrer maskinen.

^ Recommendation list

Recommendations (3) Passed assessments (8) Unavailable assessments (7)

DESCRIPTION	STATUS
Install endpoint protection solution on virtual machines	High
Apply disk encryption on your virtual machines	High
Apply a Just-In-Time network access control	High

4. For å installere anbefalingene, må du klikke på anbefalingen som vises. Deretter får du opp følgende:

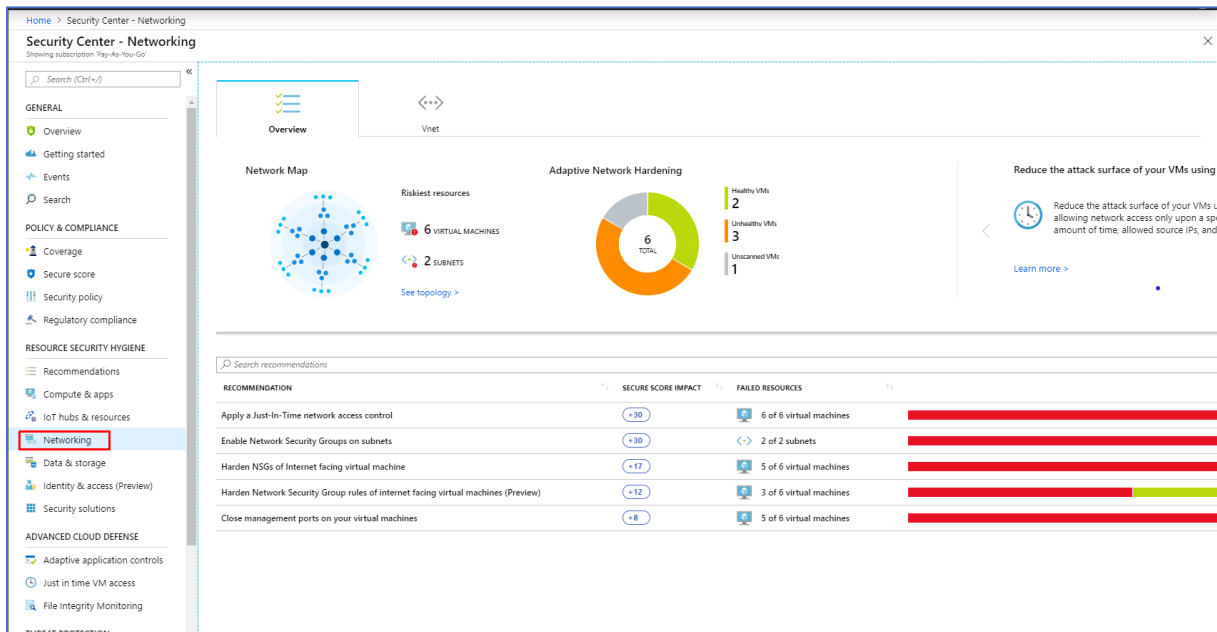
Apply a just in time VM access control

Filter **Enable JIT on 1 VMs**

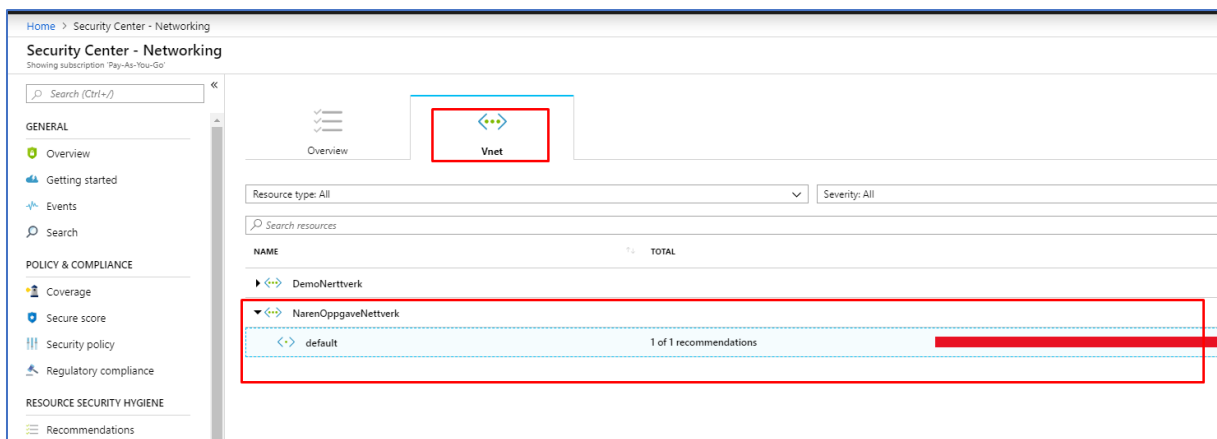
VIRTUAL MA...	RESOURE GR...	SUBSCRIPTI...	STATE	SEVERITY
DC	CLOUD-SHELL-...	Pay-As-You-Go	Open	High
<input checked="" type="checkbox"/> DemoMaskin	CLOUD-SHELL-...	Pay-As-You-Go	Open	High
PenTestMaskin	CLOUD-SHELL-...	Pay-As-You-Go	Open	High
sec	CLOUD-SHELL-...	Pay-As-You-Go	Open	High
Win16	CLOUD-SHELL-...	Pay-As-You-Go	Open	High
Win19	CLOUD-SHELL-...	Pay-As-You-Go	Open	High

5. Videre tikker du av for den maskinen vi skal installere JIT anbefalingen på og deretter klikker man på Enable JIT on 1 VMs.

2.4.4.3 Networking



1. I Networking delen av Security Center finner vi oversikt over anbefalinger som bør settes i gang på nettverksdelen av Azure. Et godt eksempel er anbefalinger som forekommer for de virtuelle nettverkene som er satt opp i Azure.



2. Vi har også en egen VNet seksjon under Networking delen. Her har vi en bredere oversikt over de virtuelle nettverkene i Azure. Når jeg f.eks klikker på NarenOppgaveNettverk ser vi at det er anbefalt å sette i gang 1 anbefaling. Jeg klikker videre på denne anbefalingen for å se hva jeg bør sette i gang.

Home > Security Center - Networking > default

default

security health

Resource health **default**

Total recommendations **1**

Recommendations summary




High	1
Medium	0
Low	0

^ information

Resource Name	default
Resource Group	cloud-shell-storage-westeuropa
Subscription	Pay-As-You-Go

^ Recommendation list

Recommendations (1) Passed assessments (0) Unavailable assessments (0)

DESCRIPTION	STATUS
   Enable Network Security Groups on subnets	High

3. Da står det her at jeg bør slå på NSG på subnettene. For å gjøre dette klikker jeg på selve anbefalingen.

Home > Security Center - Networking > default > Enable Network Security Groups on subnets

Enable Network Security Groups on subnets

^ Description

Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet. When an NSG is associated with a subnet, the ACL rules apply to all the VM instances and integrated services in that subnet, but don't apply to internal traffic inside the subnet. To secure resources in the same subnet from one another, enable NSG directly on the resources as well.

^ General Information

User impact	High
Implementation cost	Moderate

^ Threats

- Malicious insider
- Data spillage
- Data exfiltration

^ Remediation steps

To enable Network Security Groups on your subnets:

- Select a subnet to enable NSG on.
- Click the 'Network security group' section.
- Follow the steps and select an existing network security group to attach to this specific subnet.

Take action

4. Deretter klikker jeg på «Take action».

The screenshot displays the Azure portal interface for configuring a network resource. The left pane, titled 'default', shows the following configuration options:

- Address range (CIDR block):** 10.0.0.0/24 (10.0.0.0 - 10.0.0.255, 256 addresses)
- Available addresses:** 239
- Network security group:** None (highlighted with a red box)
- Route table:** None
- Users:** Manage users
- Service endpoints:** Services: 0 selected
- Subnet delegation:** Delegate subnet to a service: None

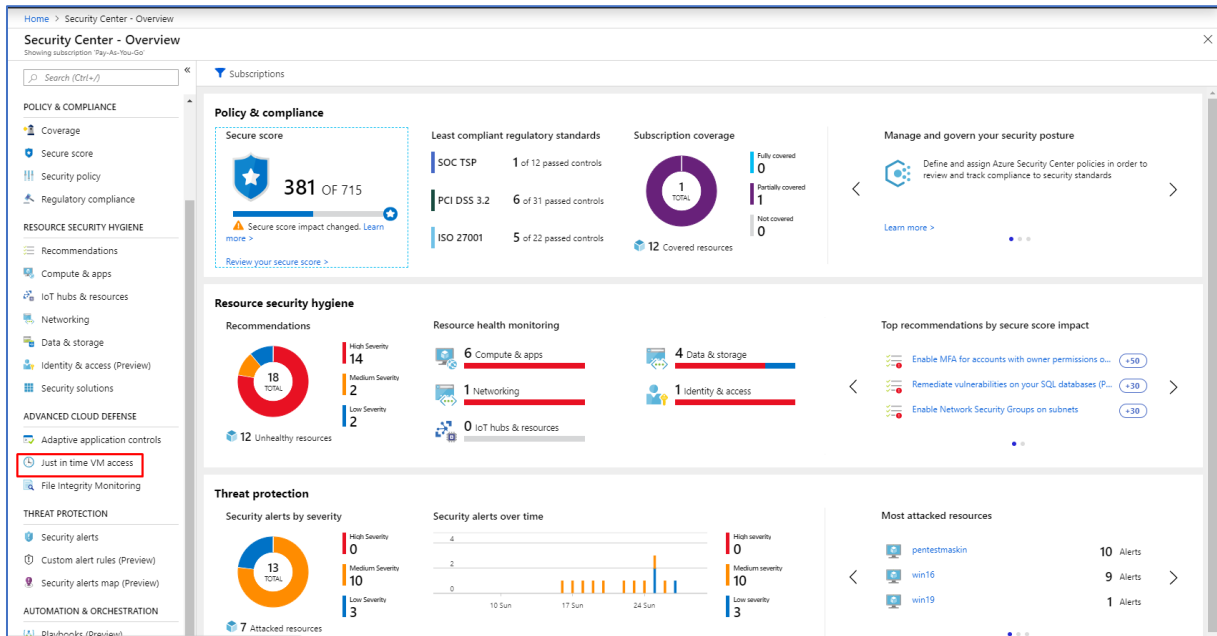
The right pane, titled 'Resource', shows a list of network security groups in the 'North Europe' location. The 'DC-nsg' resource is highlighted with a red box. The list includes:

- None
- DC-nsg (northeurope) - highlighted
- DemoMaskin-nsg (northeurope)
- DOMENE-nsg (northeurope)
- DOMENEng441 (northeurope)
- Kali-nsg (northeurope)
- PenTest2Linux-nsg (northeurope)
- PenTest3-nsg (northeurope)
- PenTestMaskin-nsg (northeurope)
- sec-nsg (northeurope)
- SRV16-nsg (northeurope)
- Win16-nsg (northeurope)
- Win19-nsg (northeurope)

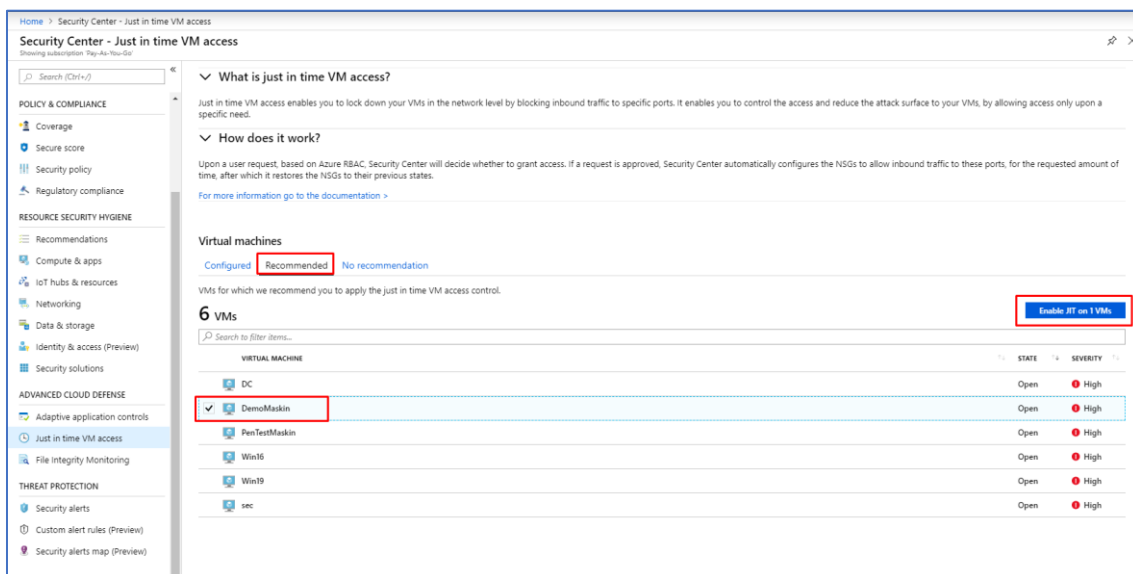
5. Videre velger jeg DC-nsg og lagrer tilslutt endringene.

2.4.5 Advanced Cloud Defense

2.4.5.1 Just-in-time VM Access

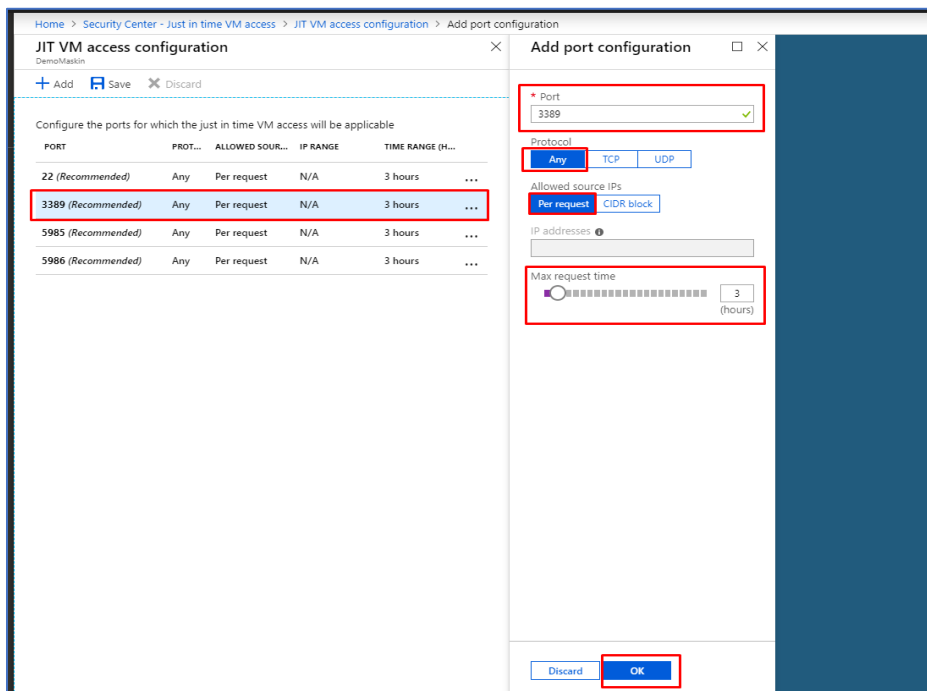


1. Just-in time VM Access setter man opp i Security Center. Når du er inne på Security Center må du navigere deg videre til Just in time VM Access undermeny under Advanced Cloud Defense.



2. Deretter klikker du på Recommended fanen. I dette tilfelle velger jeg å sette JIT til DemoMaskin, så det jeg gjør her er å dobbeltklikke på DemoMaskin og deretter videre klikke

på den blå knappen «Enable JIT on 1 VMs».



3. Videre får du en liste med ulike porter. Port 22 er for SSH, port 3389 er for RDP, 5985 og 5986 er for WinRM. I dette tilfelle vil jeg kun fokusere på RDP porten 3389. Da klikker jeg på denne porten, videre blir Port satt til default, Protocol skal velges til Any, Allowed source IPs blir satt til Per request. Deretter velger jeg å sette Max request time til å være på 3 timer. Dersom jeg tilpasser CIDR block, har jeg mulighet til å tilpasse hvilke IP-adresser som får tilgang under JIT overvåkning.

2.4.5.2 File Integrity Monitoring

WORKSPACE NAME	TOTAL CHANGES	TOTAL COMPUTERS	LOCATION	SUBSCRIPTION
bscoppgave	0	0	West Europe	Pay-As-You-Go
defaultworkspace-3f6b0f35-d667-4770-ac0f-4bc8edc02b6f-weu	0	5	West Europe	Pay-As-You-Go
sikkerhetoppgave	0	0	australacentral	Pay-As-You-Go
oppgavebsc	0	0	North Europe	Pay-As-You-Go

1. For å slå på File Integrity Monitoring klikker du på Enable for defaultworkspace.

What is File Integrity Monitoring?
File Integrity Monitoring (FIM), also known as change monitoring, validates files and registries integrity of operating system, application software, and others for changes that might indicate an attack. A comparison method is used to determine if the current checksum of the file is different from the latest scan of the file. You can leverage this comparison to determine if valid or suspicious modifications have been made to your files.

Enabling file integrity monitoring affects all machines connected to the selected workspace (defaultworkspace-3f6b0f35-d667-4770-ac0f-4bc8edc02b6f-weu)

3 Windows Computers 1 Linux Computers

RECOMMENDED SETTINGS

- Windows Files
- Registry
- Linux Files

Enable File Integrity Monitoring

2. Deretter klikker du på Enable File Integrity Monitoring.

Home > Security Center - File Integrity Monitoring > File integrity Monitoring

File Integrity Monitoring

Settings Refresh Filter Disable

Total computers: **5** Total changes: **0**

Change type	Count	Change category	Count
Files	0	Modified	0
Registry	0	Added	0
		Removed	0

[LEARN MORE](#)
[Learn more about File Integrity Monitoring...](#)

Computers Changes

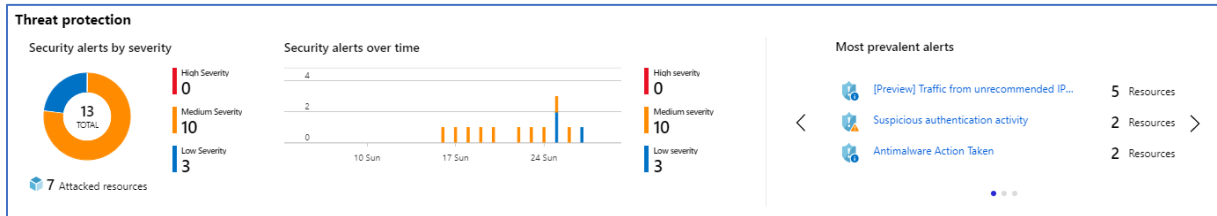
Search computers

NAME	TOTAL CHANGES	FILES	REGISTRY	LAST CHANGE TIME (LOCAL)
sec	0	0	0	
DC.narenbsc.local	0	0	0	
PenTestMaskin	0	0	0	
Win16	0	0	0	
DemoMaskin	0	0	0	

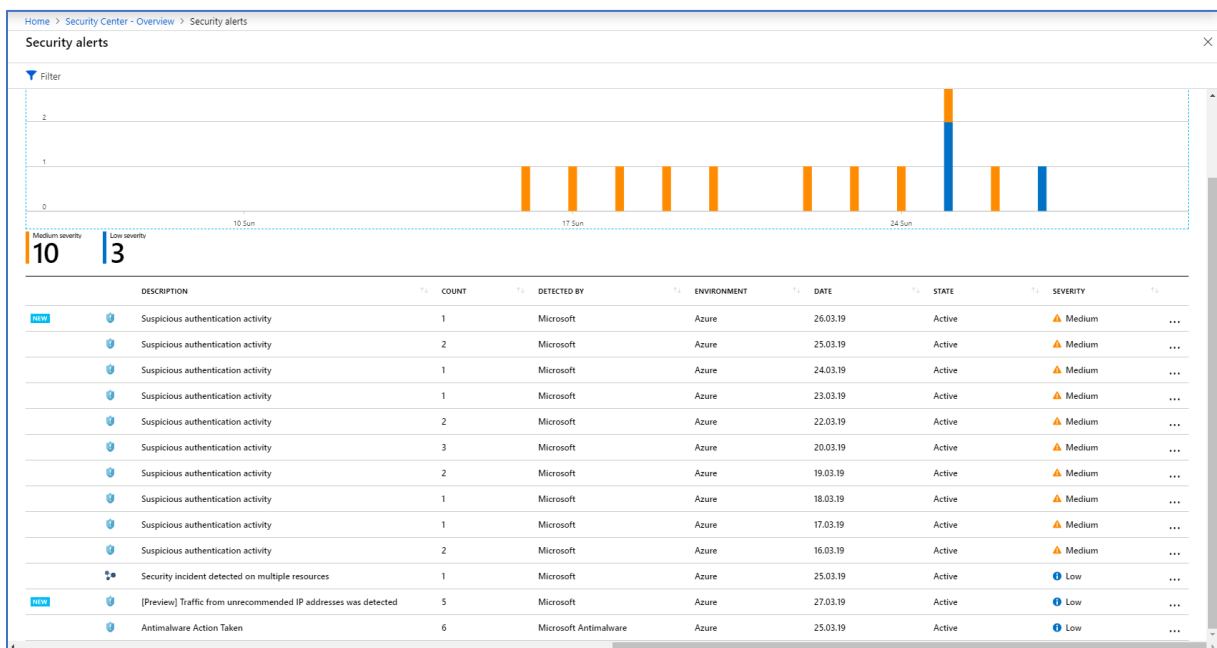
3. Ovenfor ser du et bilde av dashboardet til File Integrity Monitoring.

2.4.6 Threat Protection

2.4.6.1 Security Alerts

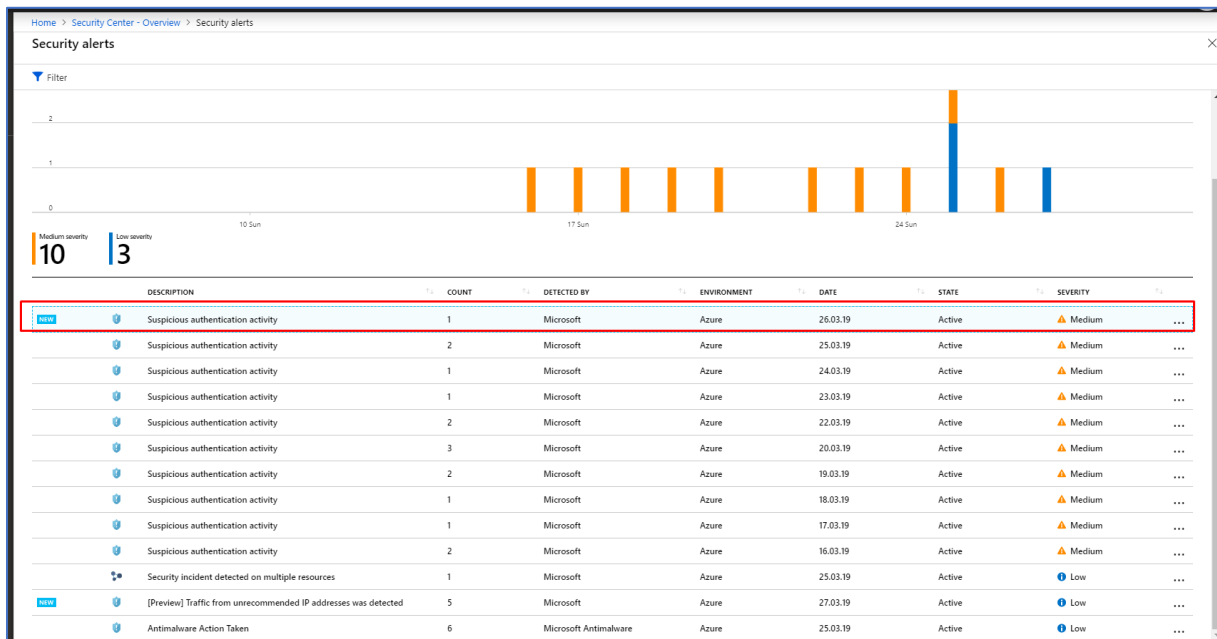
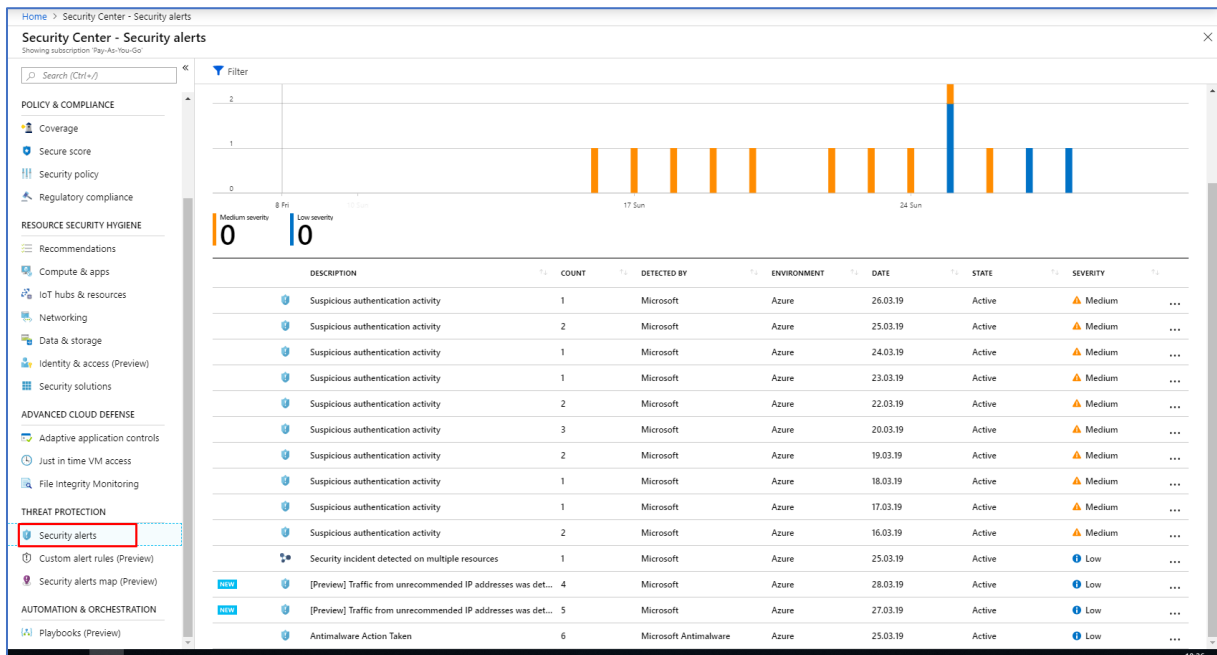


1. Under Threat Protection får du opp alle Security Alerts etter risikonivå. Vi har deler Security Alert etter nivåene High, Medium, Low Severity. Threat Protection vises i dashboard i Azure Security Center.



2. Hvis man klikker på hjulet som ligger under Threat Protection får man mer detaljert informasjon om hvilke Security Varsler som har forekommet. Du får i tillegg til dette anbefalinger får tiltak som bør settes i gang umiddelbart for de ulike varslene av trusler som kommer frem. Dette bildet får du også når du klikker på Security alerts Threat Protection

menyen.



3. Hvis vi klikker på det første varslet får vi videre opp som følgende:

Home > Security Center - Overview > Security alerts > Suspicious authentication activity

Suspicious authentication activity

Filter

ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY
PenTestMaskin	1	09:01:11	Azure	Active	Medium

4. Her vises den aktuelle ressursen som er angrepet. I dette tilfelle er det PenTestMaskin. Hvis vi klikker på PenTestMaskin får vi opp følgende:

Home > Security Center - Overview > Security alerts > Suspicious authentication activity > Suspicious authentication activity

Suspicious authentication activity

PenTestMaskin

[Learn more](#)

- General information
- Remediation steps

5. Vi får opp to deler: General Information & Remediation steps.

General information

DESCRIPTION: Although none of them succeeded, some of them used accounts were recognized by the host. This resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords in order to find valid credentials to access the host. This indicates that some of your host account names might exist in a well-known account name dictionary.

ACTIVITY TIME: tirsdag 26. mars 2019, 09:01:11

SEVERITY: ▲ Medium

STATE: Active

ATTACKED RESOURCE: PenTestMaskin

SUBSCRIPTION: Pay-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8edc02b6f)

DETECTED BY: Microsoft

ACTION TAKEN: Detected

ENVIRONMENT: Azure

RESOURCE TYPE: Virtual Machine

ACTIVITY START TIME (UTC): 2019/03/26 08:01:11.5317960

ACTIVITY END TIME (UTC): 2019/03/26 08:59:06.7367048

Was this useful? Yes No

[Investigate](#) [View playbooks](#)

6. Under General Information får vi generelt informasjon om angrepet og hvor angriperens IP-adresse stammer fra. I dette tilfelle har det blitt utprøvd et Brute-force angrep mot PenTestMaskinen uten å lykkes.

^ Remediation steps

REMEDIATION STEPS

1. Enforce the use of strong passwords and do not re-use them across multiple resources and services
2. In case this is an Azure Virtual Machine, set up an NSG allow list of only expected IP addresses or ranges. (see <https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/>)
3. In case this is an Azure Virtual Machine, lock down access to it using network JIT (see <https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>)

7. Den andre delen Remediation step forklarer hvordan man reduserer utfallet av den aktuelle trusselen.

Home > Security Center - Security alerts > Antimalware Action Taken > Antimalware Action Taken

Antimalware Action Taken
PenTestMaskin

[Learn more](#)

^ General information

DESCRIPTION	Microsoft Antimalware has taken an action to protect this machine from malware or other potentially unwanted software.
ACTIVITY TIME	mandag 25. mars 2019, 05:30:14
SEVERITY	i Low
STATE	Active
ATTACKED RESOURCE	PenTestMaskin
SUBSCRIPTION	Pay-As-You-Go (3f6b0f35-d567-4770-ac0f-4bc8edc02b6f)
DETECTED BY	Microsoft Antimalware
ACTION TAKEN	Blocked
ENVIRONMENT	Azure
RESOURCE TYPE	v Virtual Machine
THREAT STATUS	Quarantined
CATEGORY	Virus
THREAT ID	2147519003
FILE PATH	C:\Users\nareny\Downloads\eicar_com.zip https://www.ikarussecurity.com/fileadmin/user_upload/testviren/eicar_com.zip pid:6772.ProcessStart:131979616813893822
PROTECTION TYPE	Windows Defender

Was this useful? Yes No

Investigate [View playbooks](#)

8. Dette er et bilde fra en annen trussel som har forekommet i Azure. En veldig nyttig funksjon Azure Security Center har utviklet er Investigate funksjonen. Hvis vi klikker på Investigate knappen får man mulighet til å etterforske den aktuelle trusselen.

Home > Security Center - Security alerts > Antimalware Action Taken > Antimalware Action Taken > Investigation Dashboard (Preview)

Investigation Dashboard (Preview)
defaultworkspace-3f920f39-6967-4770-b40f-4bc9e02268f9eiu

Refresh Logs

Investigation path

Investigation > Antimalware Action Taken

3/24/2019 10:45 AM — 3/29/2019 10:45 AM (5 days)

Antimalware Action Taken

Related TO INCIDENT Low PRIORITY AntimalwarePublisher DETECTED BY Info

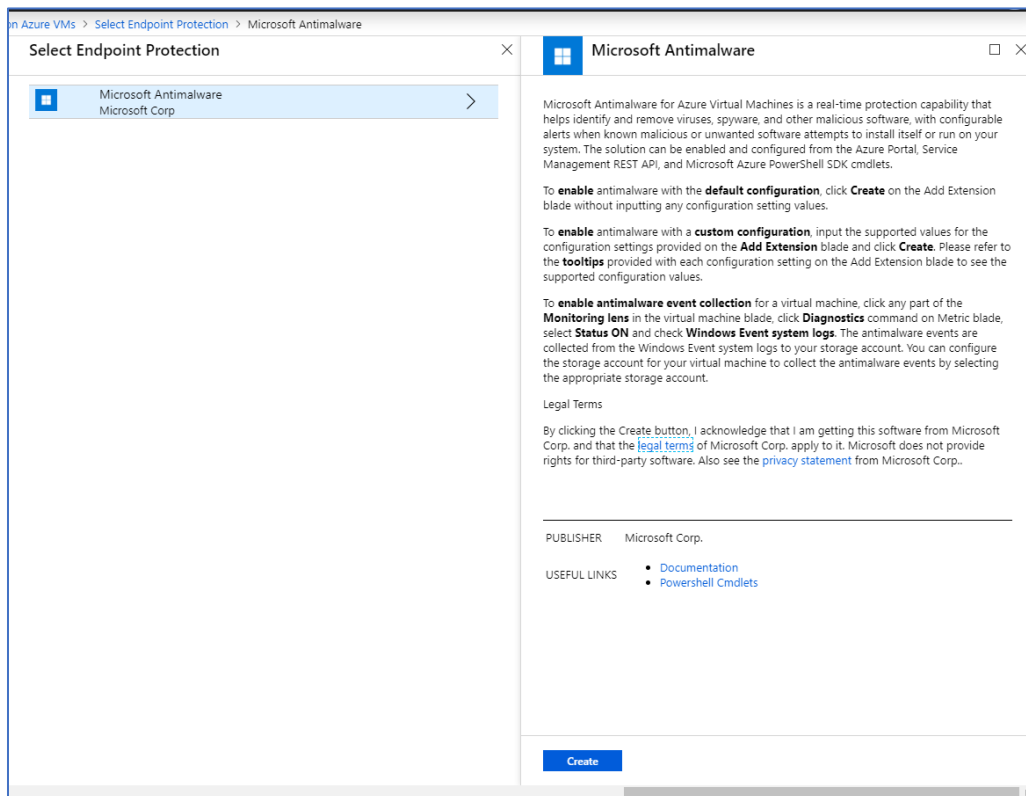
General Information

DESCRIPTION	Microsoft Antimalware has taken an action to protect this machine from malware or other potentially unwanted software.
ALERT ID	251848812585999999,2163a2c3-f8a0-4784-8ca4-e0591a000b06
TIME GENERATED	3/25/2019 6:00:54.000 AM
START TIME	3/25/2019 5:30:14.000 AM
END TIME	3/25/2019 5:30:14.000 AM
THREAT STATUS	Quarantined
CATEGORY	Virus
THREAT ID	2147519003
FILE PATH	C:\Users\larenj\Downloads\aicar_com.zip https://www.ikarussecurity.com/fileadmin/user_upload/hesviren/aicar_com.zip.pid:6772.ProcessStart:131979616813893822
PROTECTION TYPE	Windows Defender
ACTIONTAKEN	Blocked
RESOURCE TYPE	Virtual Machine
REPORTINGSYSTEM	Azure

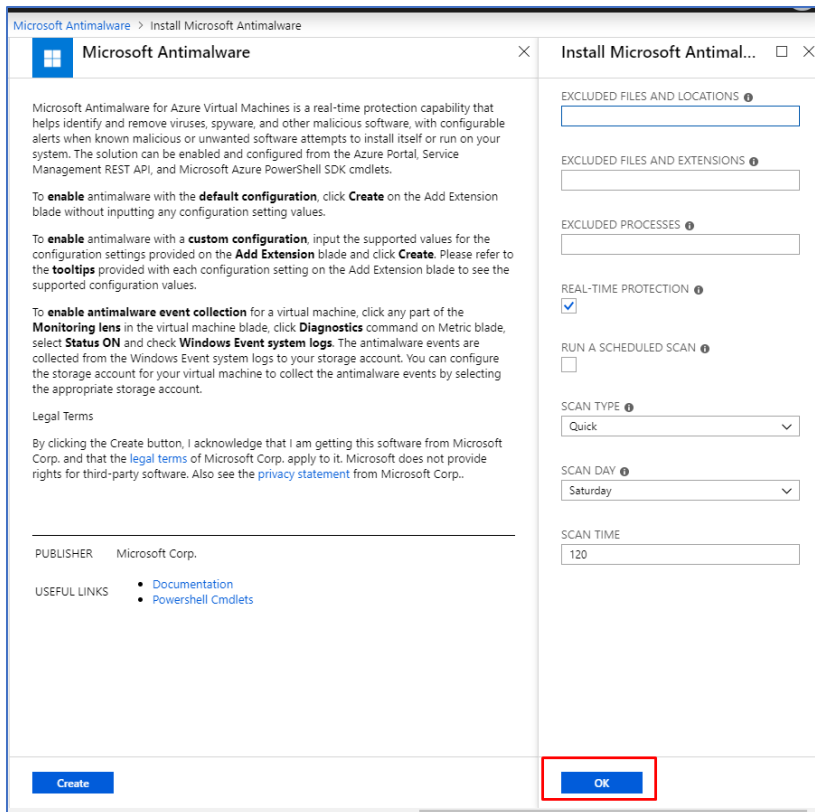
Info
Entites
Search
Exploration
Playbooks
Comments
Audit

9. Her ser vi hva Investigate funksjonen gjør. Med denne har vi muligheten har vi mulighet til å få et helhetlig bilde av den aktuelle trusselen og hvilke metoder man kan ta i bruk for å redusere utfallet angrepet. Du som bruker får en graf med ulike entiteter og får muligheten til å navigere deg fra en entitet til en annen. Investigation funksjonen er fortsatt under Preview, så det kan forekomme endringer og funksjonaliteter som fortsatt er under vurdering.

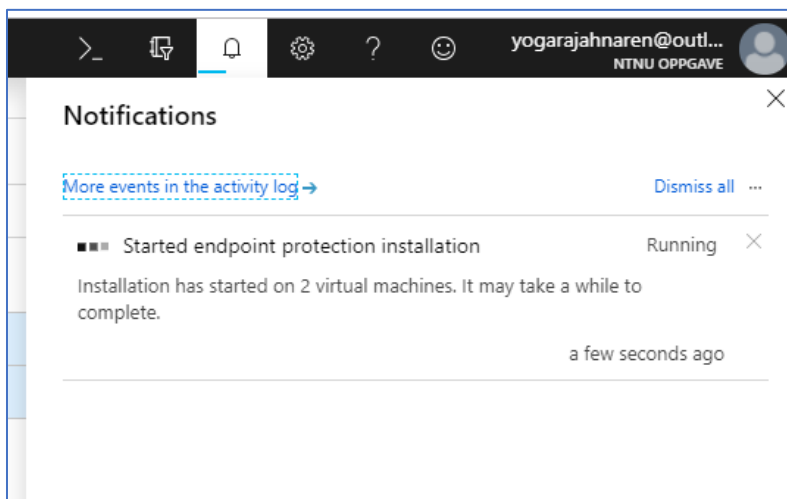
2.4.7 Microsoft Antimalware



1. Microsoft Antimalware er et tilbud i Marketplace som kan brukes for trussel deteksjon og fjerning av ondsinnede programvarer og virus. For å installere dette klikker man på Create knappen.



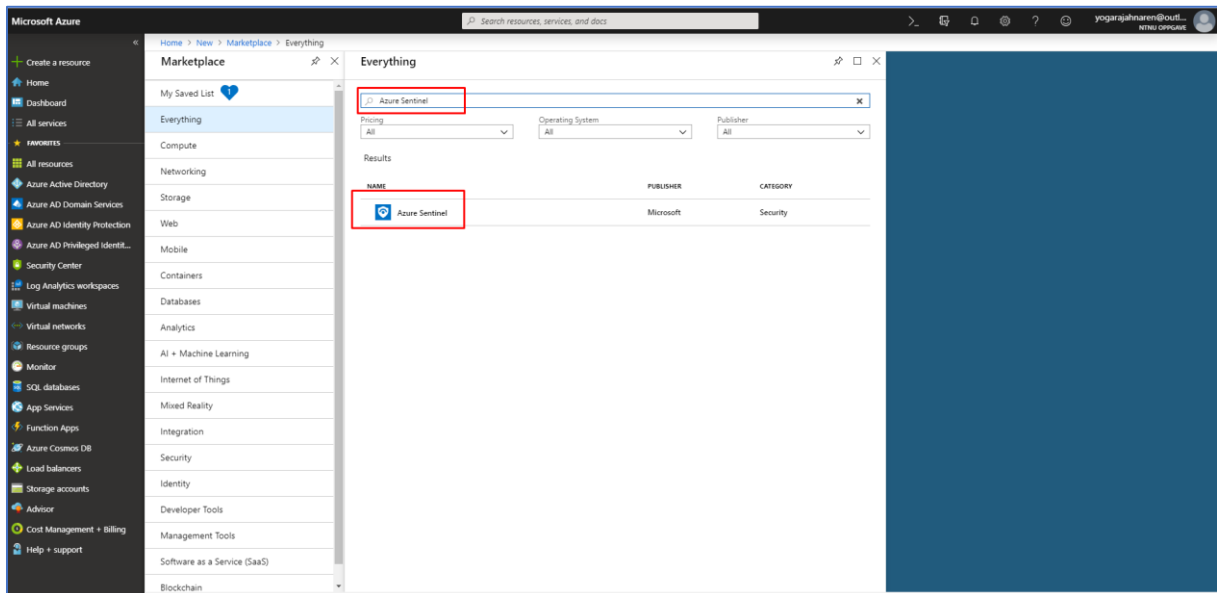
2. Deretter er det bare å klikke på Ok knappen.



3. Installasjonen av Microsoft Antimalware er i gang.

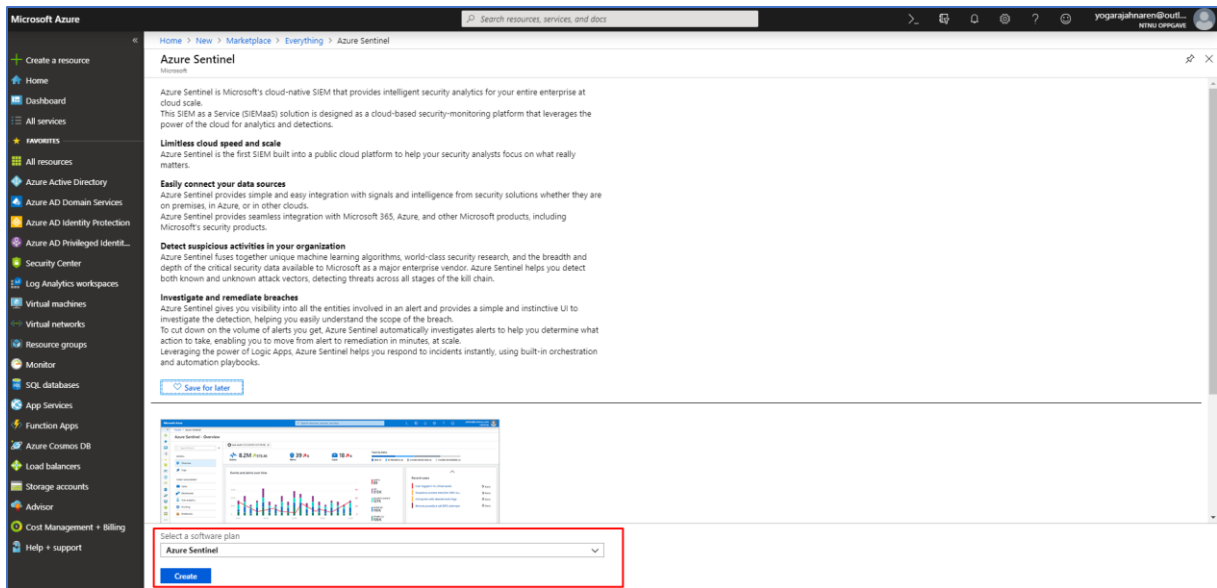
2.5 Azure Sentinel

2.5.1 Installasjon av Azure Sentinel

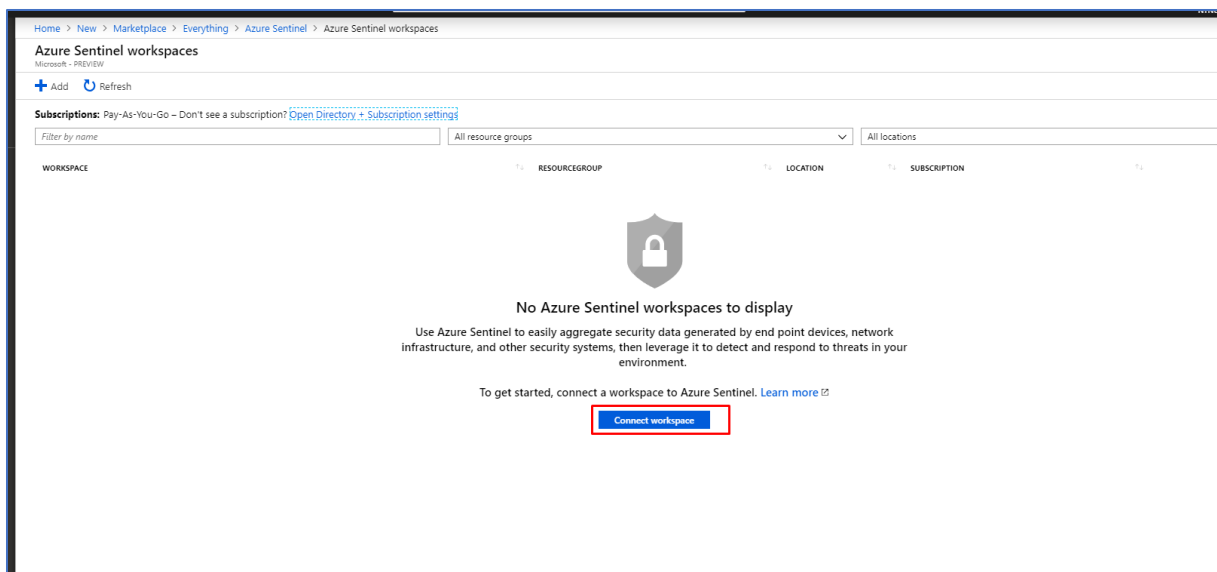


Azure Sentinel er en cloud basert SIEM(Security Information and event management) tjeneste. Med Azure Sentinel har du mulighet til å tilby intelligente sikkerhetsanalyser for hele din bedrift på cloud nivå. Vi har mulighet til å sette i gang automatiserte trussel respons og ta i bruk innebygd orkestrering. Ikke minst har man også mulighet til å ta i bruk automatiserte playbooks hvor man har lagt inn oppskrift på hva som bør gjøres dersom det har forekommet mistenkelige hendelser eller trusler i Azure miljøet.

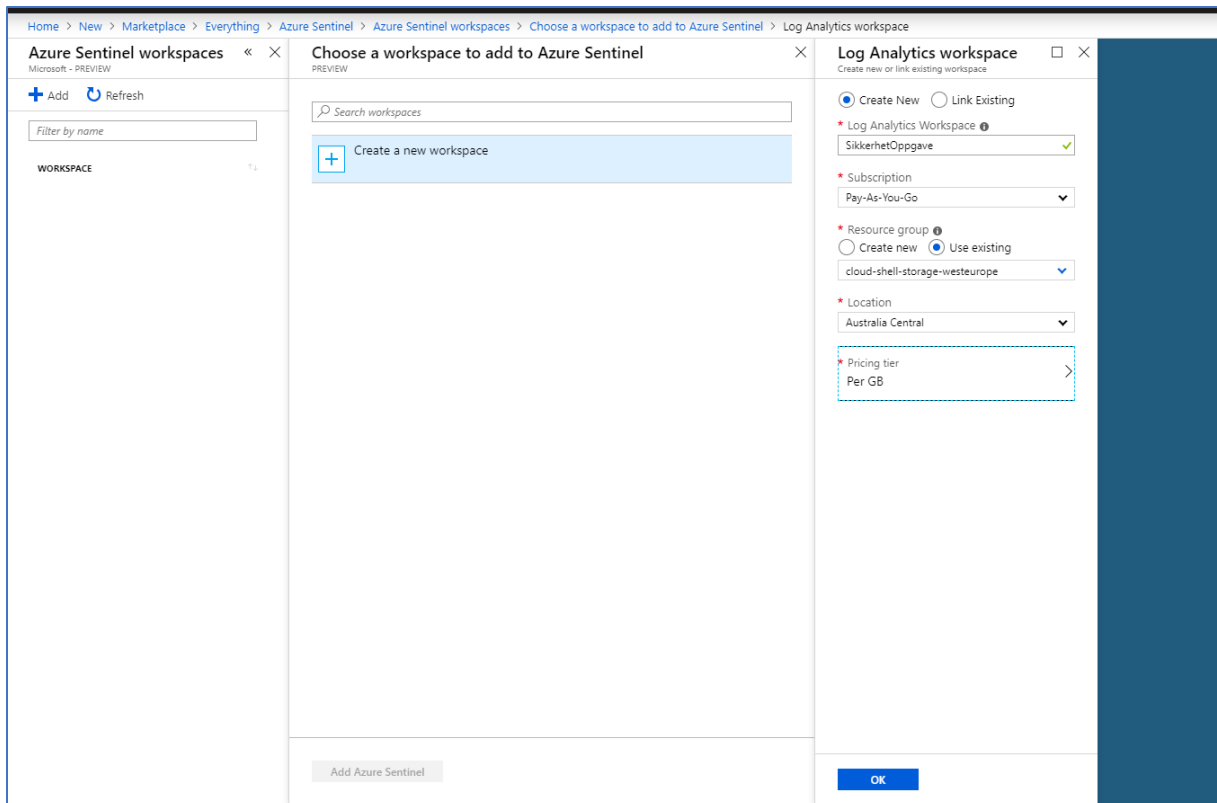
1. For å laste ned Azure Sentinel, må vi være inne på Marketplace og søke etter Azure Sentinel.



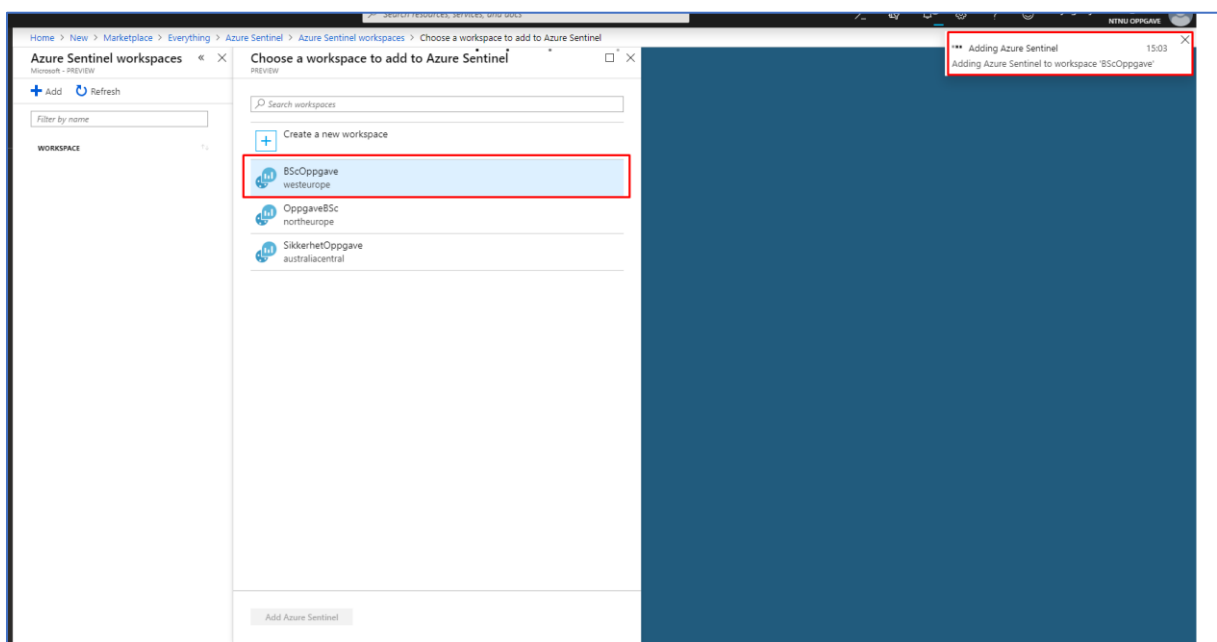
2. Deretter får du opp Azure Sentinel. Software plan kan settes til default som er Azure Sentinel og videre klikker du på Create.



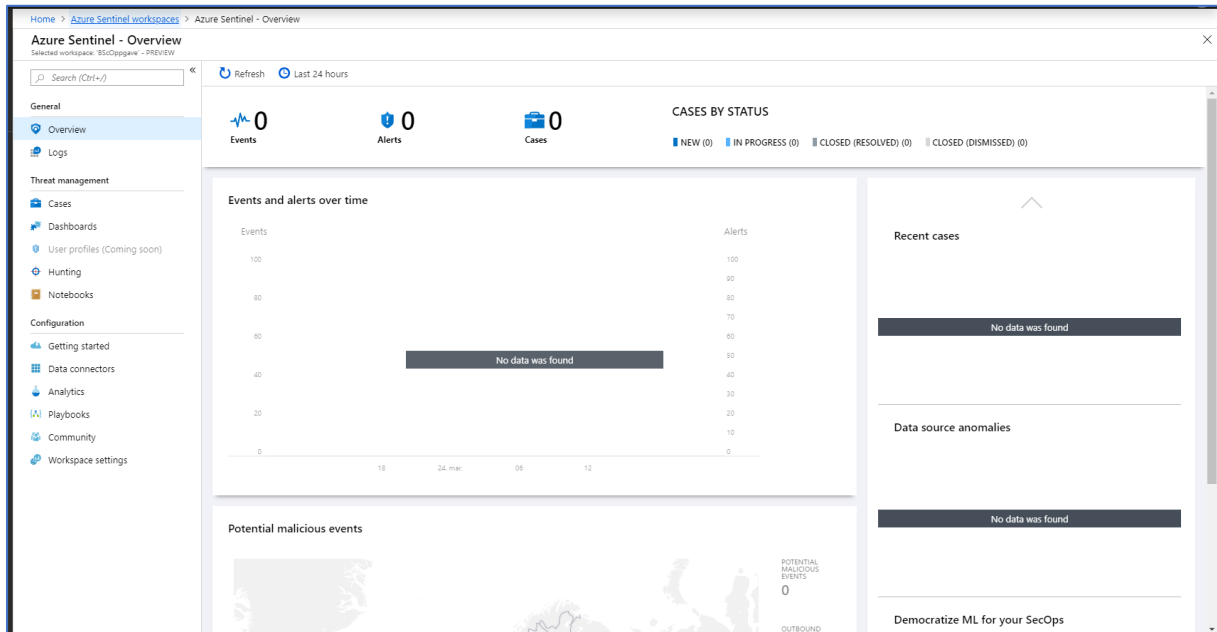
3. Når Azure Sentinel er installert suksessfullt, skal du videre klikke på knappen Connect workspace.



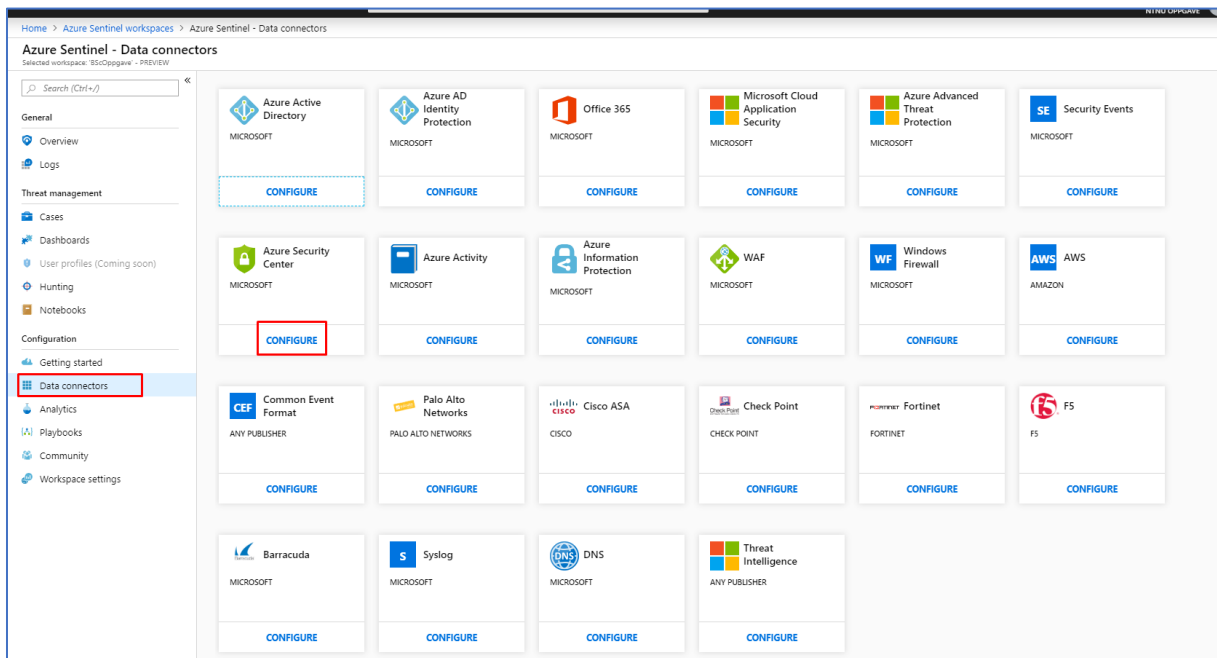
4. Deretter klikker du videre inn på Create a new workspace. Videre velger jeg å navne Log Analytics Workspace til BscOppgave, velger videre Subscription til Pay-As-You-Go. Deretter setter vi Resource group til å være eksisterende cloud-shell-storage-west-europe. Deretter skal Location settes til North Europe, mest hensiktsmessig med tanke på Norge. Pricing tier blir satt til å være default og dermed trenger den ikke noen endringer.



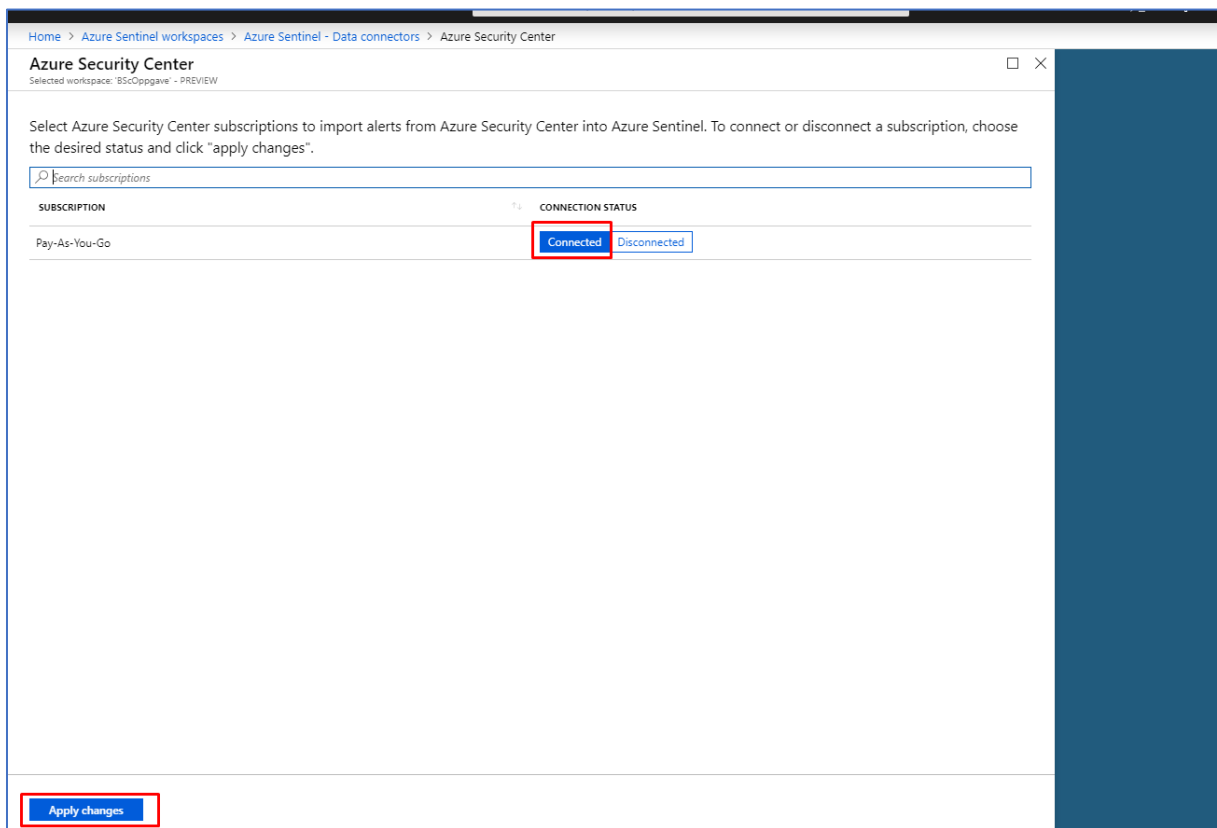
5. BscOppgave workspace velges til å bli tilknyttet til Azure Sentinel.



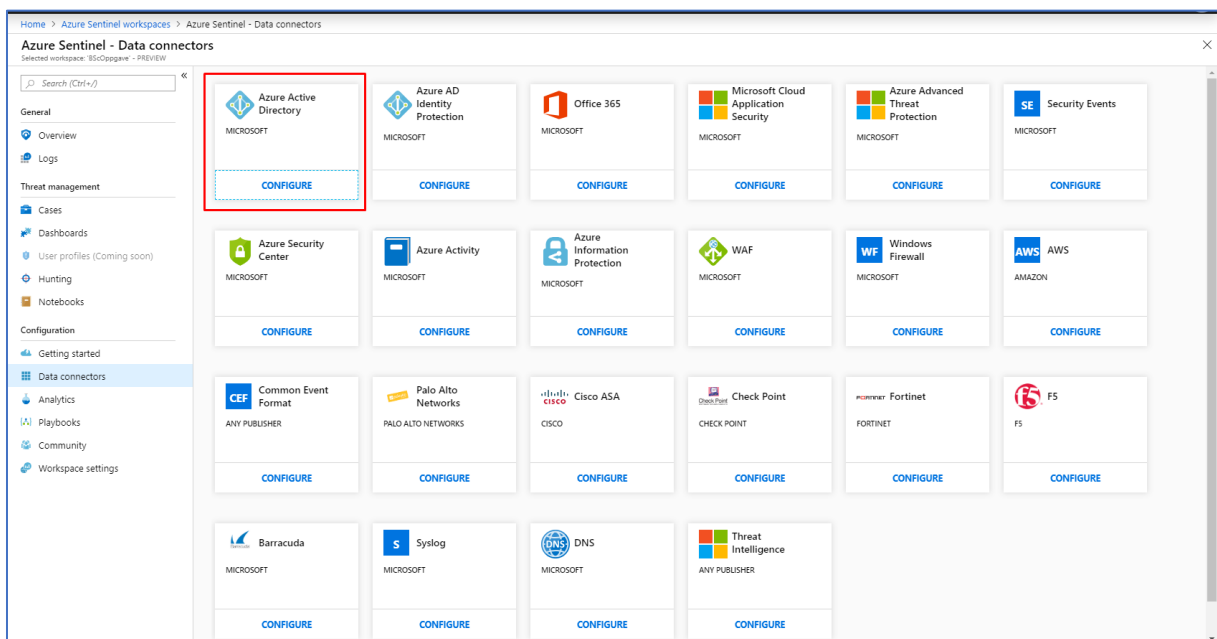
6. Azure Sentinel er installert suksessfullt, og ovenfor vises dashboardet til Azure Sentinel.



7. For at vi skal få inn data fra ulike kilder som er tilknyttet her i Azure må vi navigere oss frem til Data connectors. Videre velger jeg å få inn data fra Azure Security Center, da klikker jeg på Configure knappen under Azure Security Center boksen.

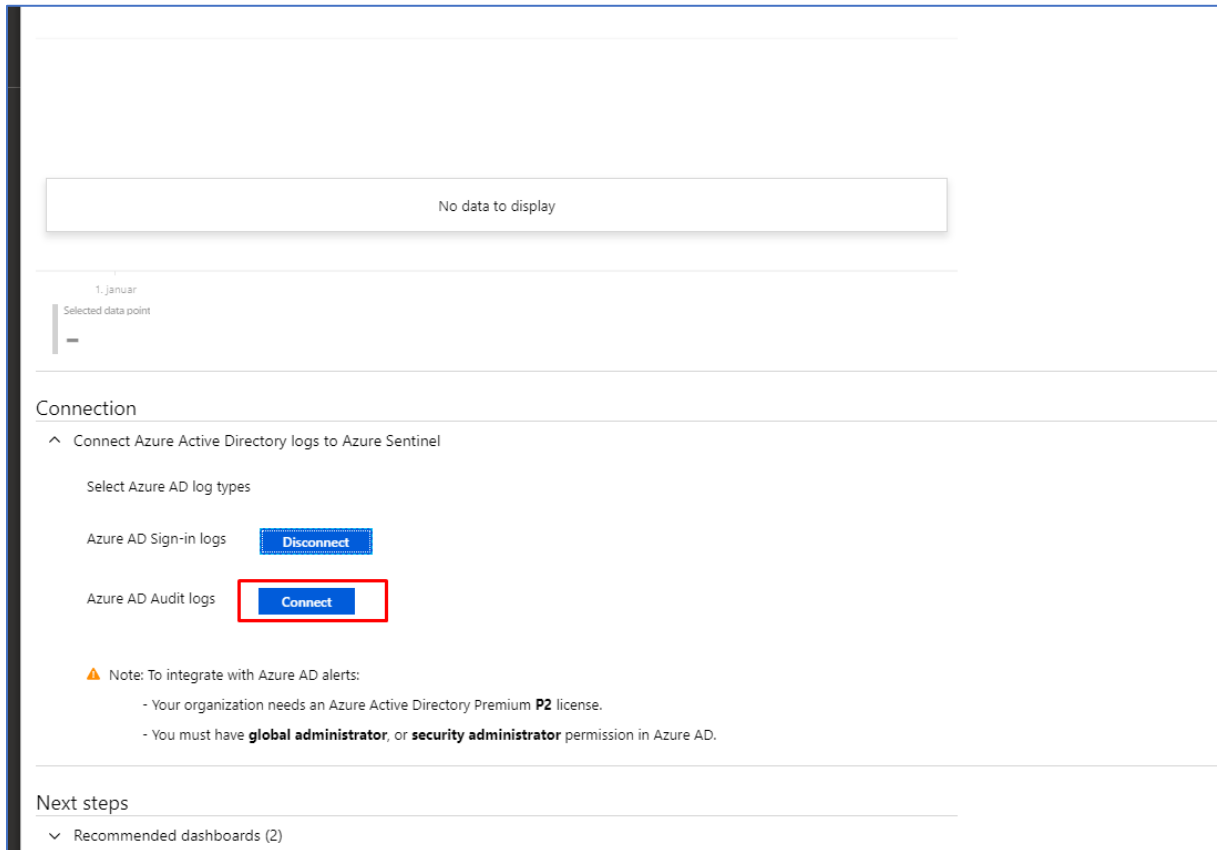


8. Deretter klikker jeg på Connected valget ved siden av Pay-AS-You-Go Subscription. Det er viktig å huske på å klikke på Apply changes, for å lagre de endringene som blir gjort.



9. Akkurat med bruk av samme metode ovenfor, gjør vi dette for Azure Active Directory og

Azure AD Identity Protection.



No data to display

1. januar
Selected data point
-

Connection

^ Connect Azure Active Directory logs to Azure Sentinel

Select Azure AD log types

Azure AD Sign-in logs [Disconnect](#)

Azure AD Audit logs [Connect](#)

Note: To integrate with Azure AD alerts:


- Your organization needs an Azure Active Directory Premium **P2** license.
- You must have **global administrator**, or **security administrator** permission in Azure AD.

Next steps


v Recommended dashboards (2)

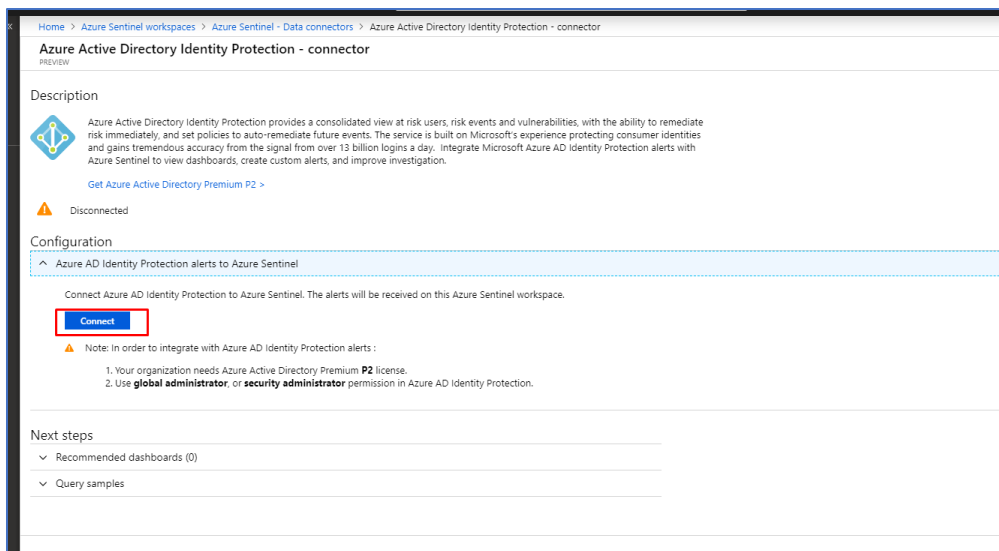
10. Jeg klikker på **Connect** for både Azure AD Sign-in logs og Azure AD Audit logs.

Description



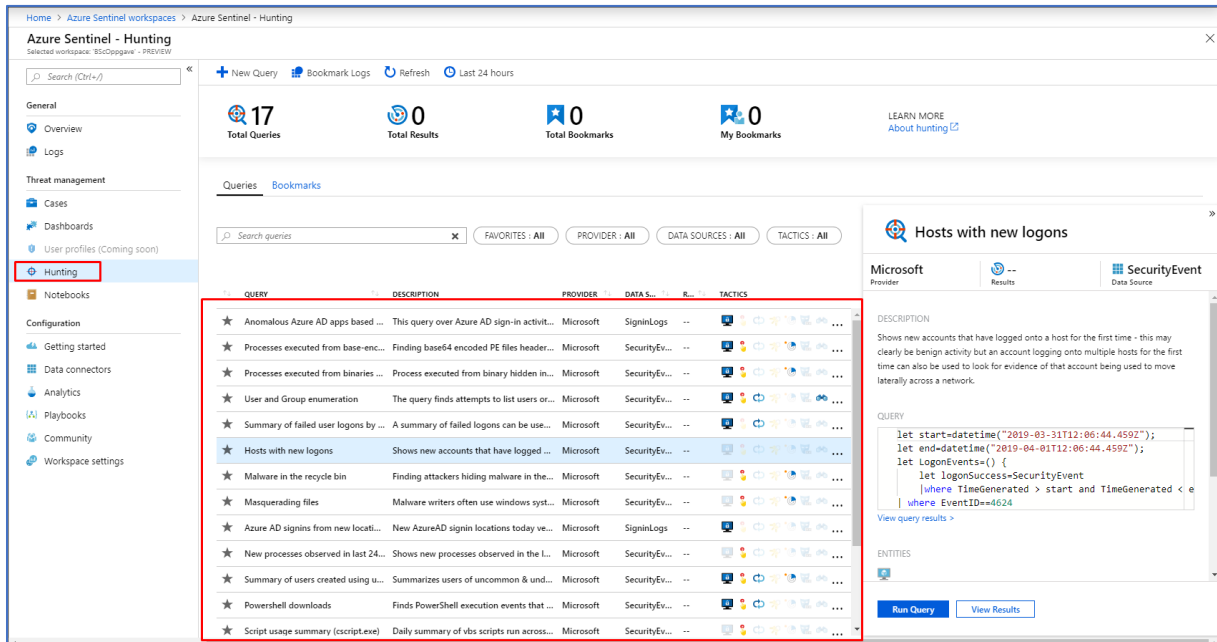
Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure AD scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your SSPR usage, Azure AD Management activities like user, group, role, app management using our Audit logs table.

 Connected.



11. Dette skal vi også gjøre under Identity Protection. Jeg klikker Connect, slik at jeg får inn data fra Azure AD Identity Protection i Azure Sentinel.

2.5.2 Hunting



1. Hunting er et verktøy du finner under Threat Mangament undermeny i Azure Sentinel. Dette er et veldig nyttig verktøy som inneholder flere queries som kan tas i bruk for etterforskning av trusler og mistenkelig aktivitet i Azure miljøet.

The screenshot displays the Microsoft Security Sentinel Hunting interface. At the top, there are navigation options like 'New Query', 'Bookmark Logs', 'Refresh', and 'Last 24 hours'. Below this, statistics show '17 Total Queries', '1 Total Results', '0 Total Bookmarks', and '0 My Bookmarks'. A search bar and filter buttons for 'FAVORITES: All', 'PROVIDER: All', 'DATA SOURCES: All', and 'TACTICS: All' are present. The main table lists various queries, with 'Azure AD signins from new locations' highlighted in a red box. The right-hand panel shows the details for this query, including its description, the KQL query code, and buttons for 'Run Query' and 'View Results'.

QUERY	DESCRIPTION	PROVIDER	DATA S...	R...	TACTICS
★ Anomalous Azure AD apps based on aut...	This query over Azure AD sign-in activit...	Microsoft	SignInLogs	--	
★ Processes executed from base-encoded ...	Finding base64 encoded PE files header...	Microsoft	SecurityEv...	--	
★ Processes executed from binaries hidde...	Process executed from binary hidden in...	Microsoft	SecurityEv...	--	
★ User and Group enumeration	The query finds attempts to list users or...	Microsoft	SecurityEv...	--	
★ Summary of failed user logons by reaso...	A summary of failed logons can be use...	Microsoft	SecurityEv...	--	
★ Hosts with new logons	Shows new accounts that have logged ...	Microsoft	SecurityEv...	0	
★ Malware in the recycle bin	Finding attackers hiding malware in the...	Microsoft	SecurityEv...	--	
★ Masquerading files	Malware writers often use windows syst...	Microsoft	SecurityEv...	--	
★ Azure AD signins from new locations	New AzureAD signin locations today ve...	Microsoft	SignInLogs	1	
★ New processes observed in last 24 hours	Shows new processes observed in the L...	Microsoft	SecurityEv...	--	
★ Summary of users created using uncom...	Summarizes users of uncommon & und...	Microsoft	SecurityEv...	--	
★ Powershell downloads	Finds PowerShell execution events that ...	Microsoft	SecurityEv...	--	
★ Script usage summary (cscript.exe)	Daily summary of vbs scripts run across...	Microsoft	SecurityEv...	--	

Azure AD signins from new locations
 Microsoft Provider | 1 Results | SigninLogs Data Source

DESCRIPTION
 New AzureAD signin locations today versus historical Azure AD signin data. In the case of password spraying or brute force attacks, one might see authentication attempts for many accounts from a new location.

QUERY

```
let start=datetime("2019-03-31T12:10:18.571Z");
let end=datetime("2019-04-01T12:10:18.571Z");
SignInLogs
| where TimeGenerated > start and TimeGenerated < end
| where TimeGenerated >= ago(1d)
| summarize perIdentityAuthCount=count() by Identity,
```

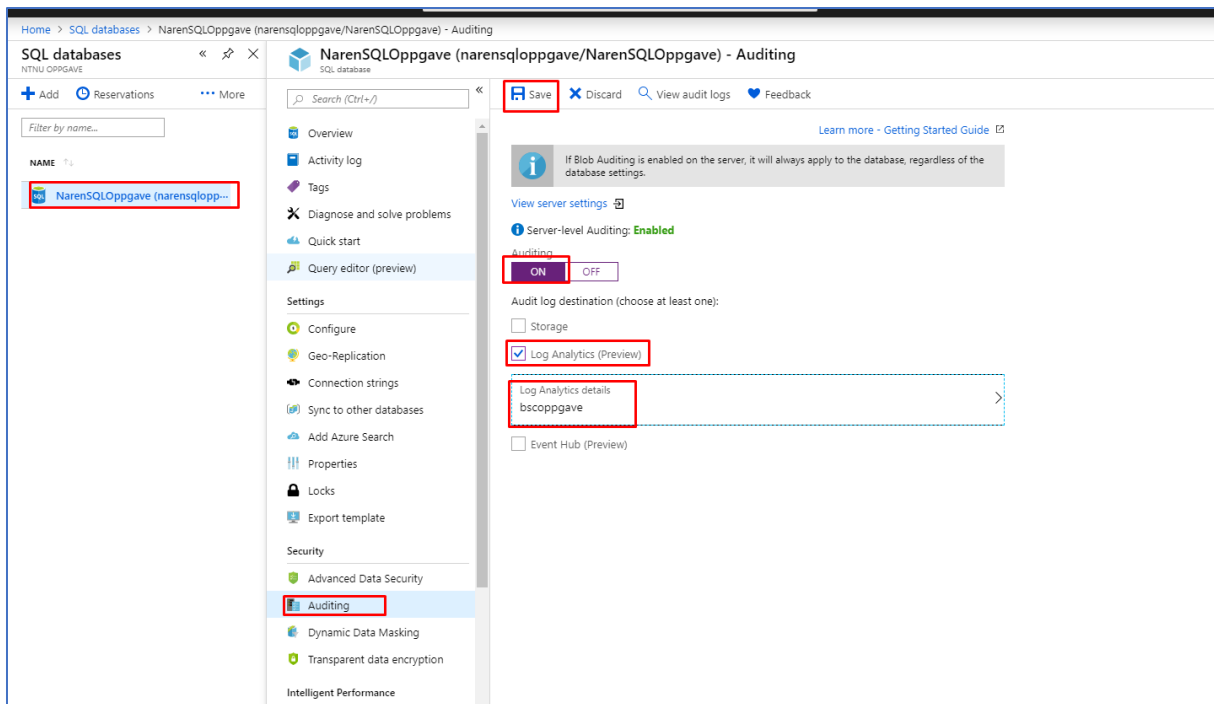
TACTICS
 Initial Access: The initial access tactic represents the vectors adversaries use to gain an initial foothold within a network. [read more on mitre.com](#)

Run Query **View Results**

2. En av Queryene vi kan ta i bruk i Hunting er etterforskning av Azure AD innlogginger. Da klikker man på denne spørringen i Hunting verktøyet. Den er markert i rektangulær boks med stjerne symbol foran.

3. Deretter kan man få kjøre Query som allerede er innlagt innenfor denne kategorien. Videre har man også mulighet til å se resultatet av spørringen.

2.6 Azure SQL Databases

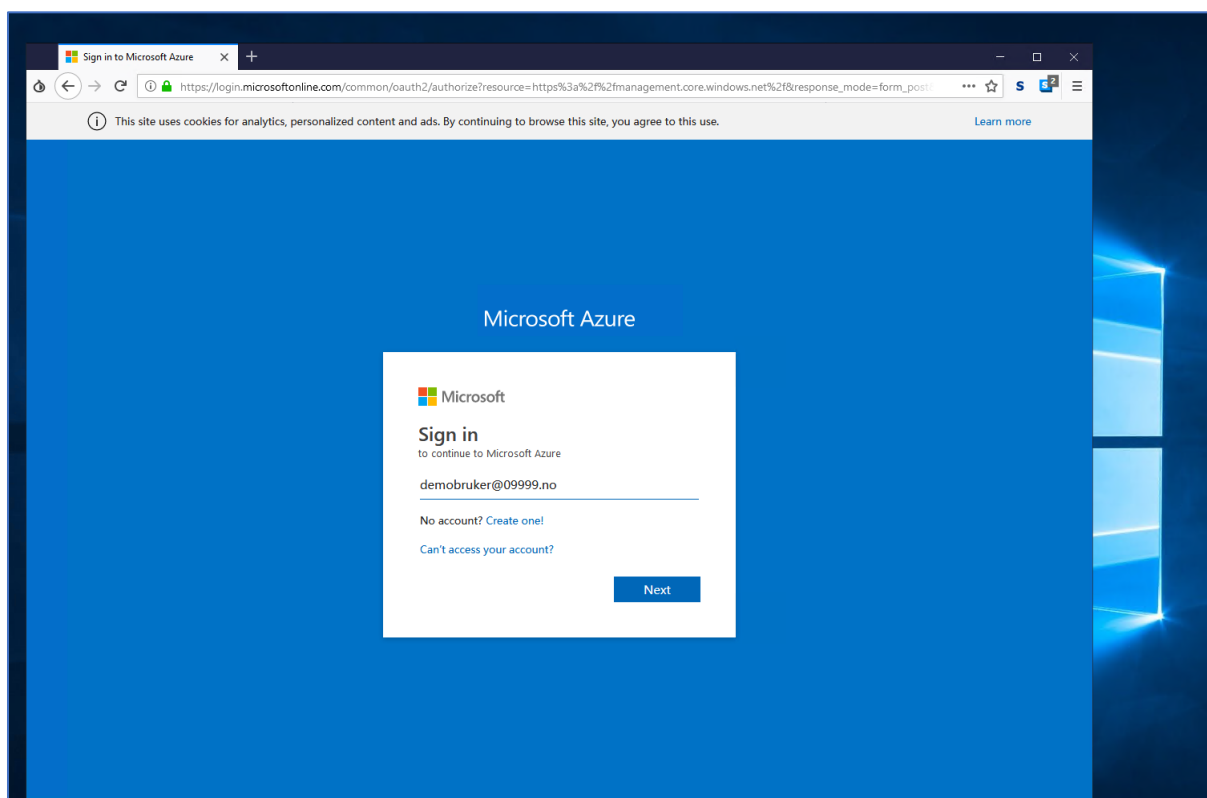


1. Gå inn på Azure portal: <https://portal.azure.com>.
2. Deretter går du videre til SQL databases menyen.
3. Videre velger jeg ønsket database, i dette tilfelle er det NarenSQLOppgave.
4. Deretter navigerer jeg meg videre til Auditing undermeny under Security.
5. Deretter tikker du av for ON i Auditing. Videre velger jeg å tikke av Log Analytics under Audit log destination. Når jeg velger Log Analytics må man videre velge ditt aktuelle workspace som skal knyttes til auditing. I mitt tilfelle blir det nå bscoppgave workspace som jeg har opprettet tidligere.
6. Videre klikker jeg på Save knappen for å lagre de endringene som har blitt utført.

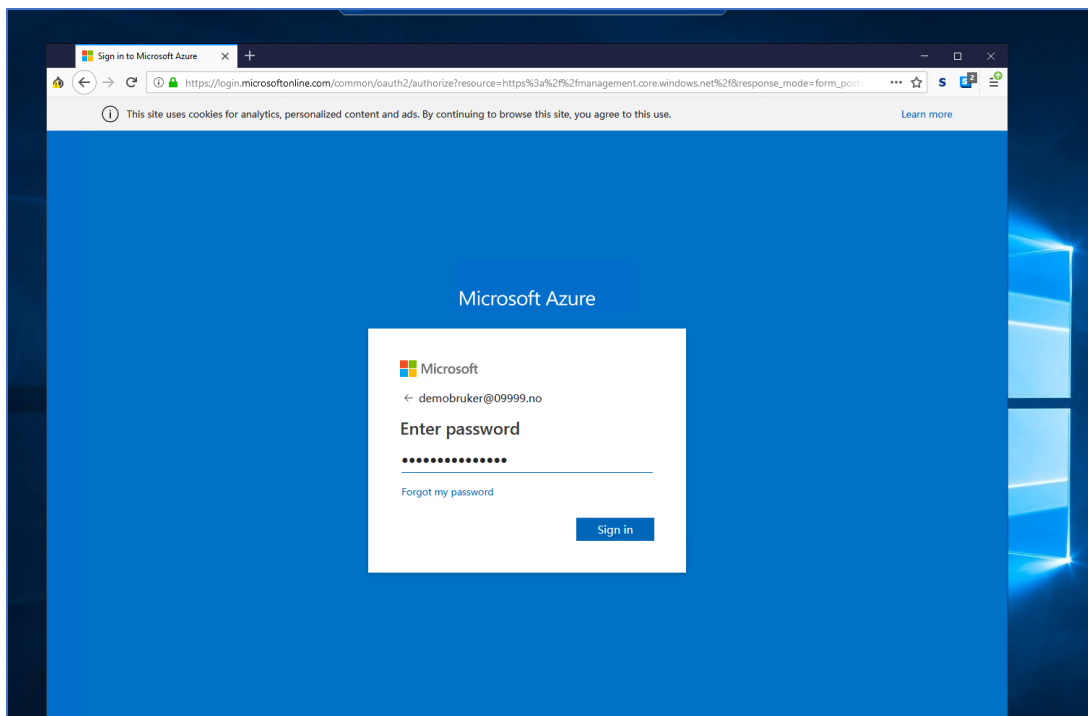
3. Deteksjon og overvåkning i Azure

3.1 Tor Browser

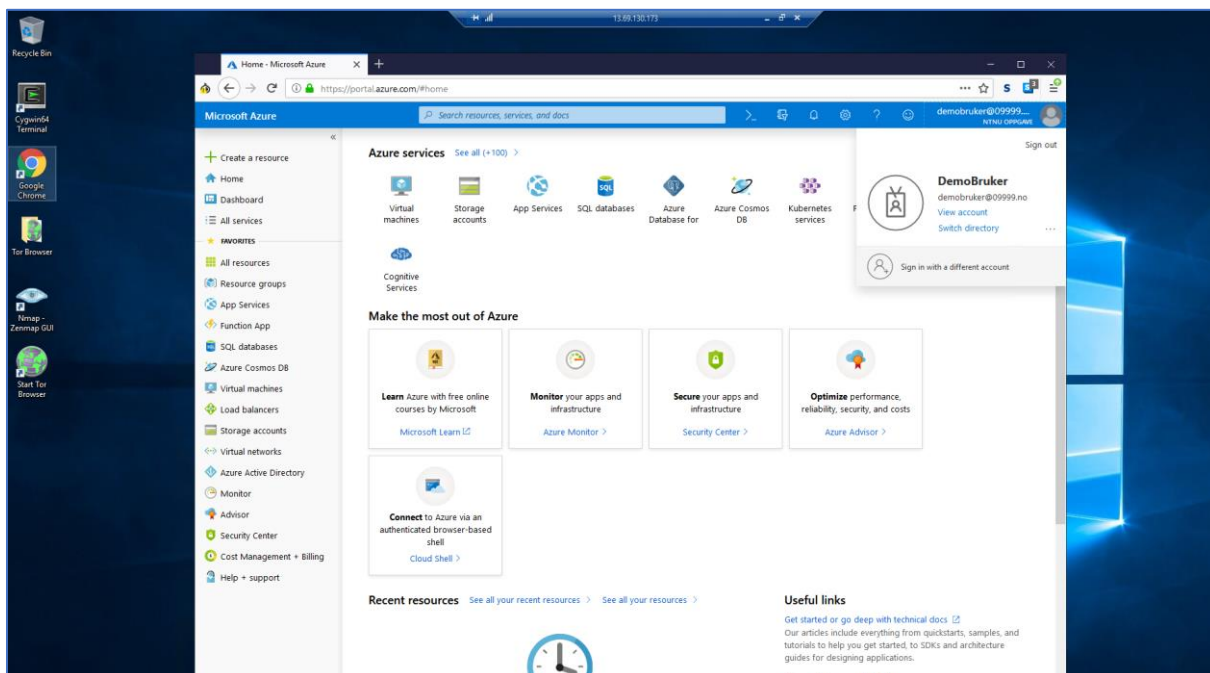
3.1.1 Identity Protection



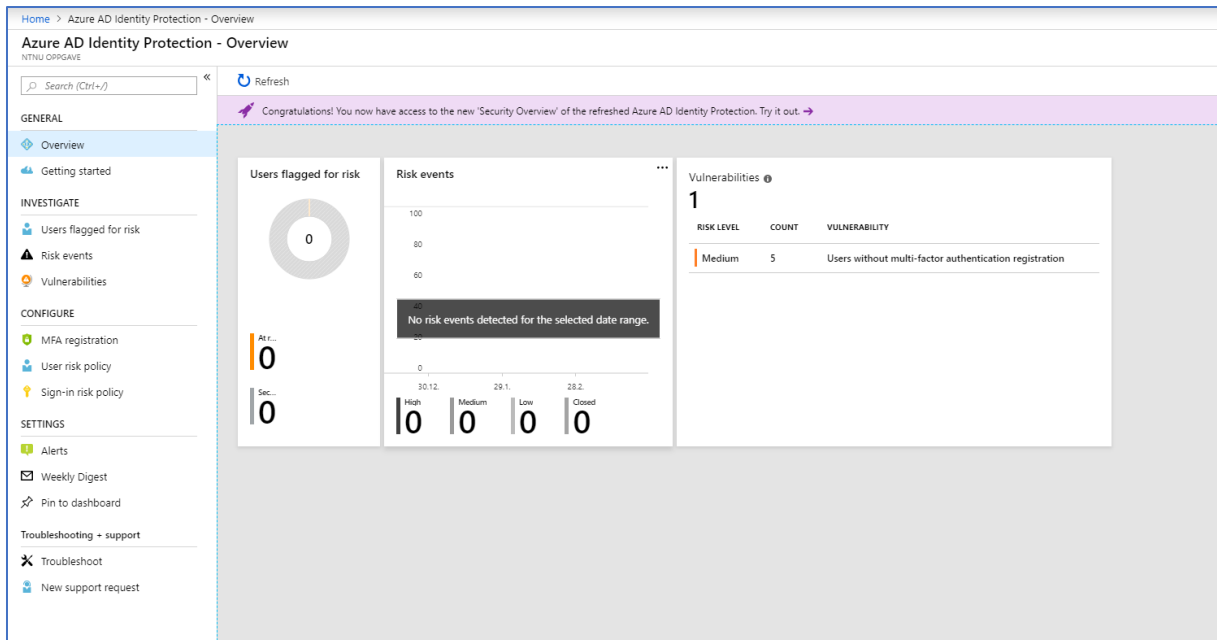
1. Her tar jeg i bruk Tor Browser får å logge inn med en Azure AD bruker i Azure Portal.



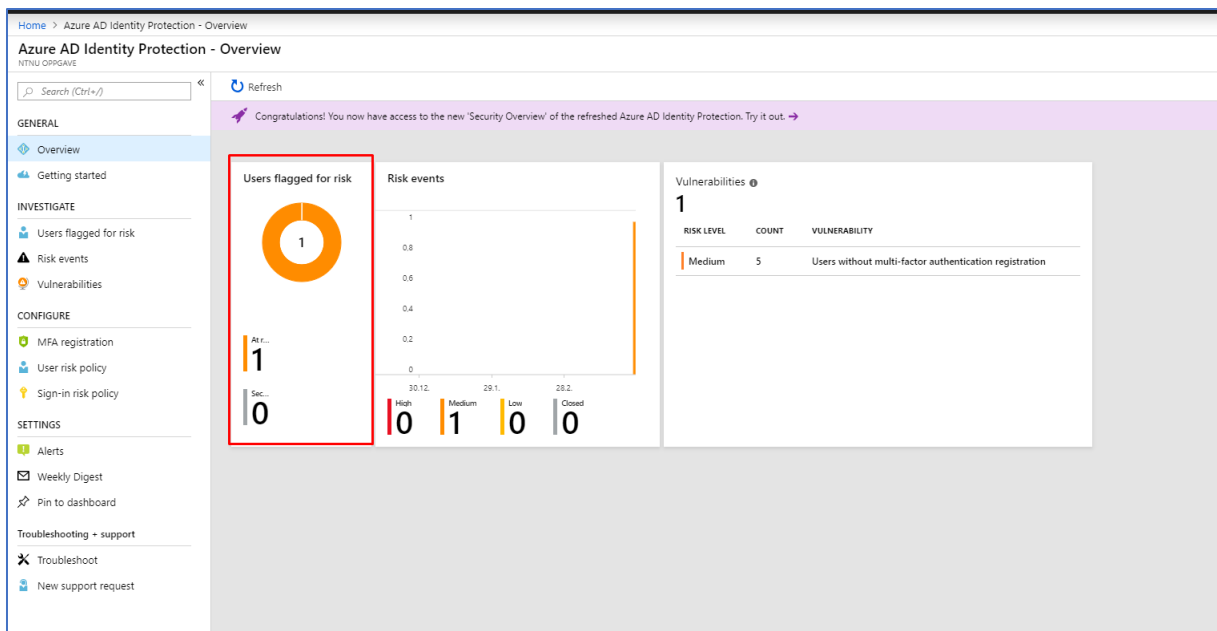
2. Videre skriver jeg inn passordet til DemoBruker.



3. Nå er jeg inne på DemoBruker fra Tor Browser i Azure Portal. Dette skal foregå fra en helt annen plassering enn Oslo og min originale IP. Tor Browser brukes ofte av hackere og andre som har ondsinnede hensikter og dermed trenger å skjule sin IP adresse og lokasjon. Videre skal vi se om dette gjenkjennes i Azure Identity Protection.



4. Jeg bytter med en gang fanen min til Azure Portal og ser for øyeblikket at det ikke er noe som har kommet opp med en gang.



5. Etter kort tid ser jeg at i Azure Identity Protection får jeg et varsel så som sier «Users flagged for risk». Jeg klikker videre på dette og da får jeg opp følgende:

Home > Azure AD Identity Protection - Overview > Users


Users

AZURE AD IDENTITY PROTECTION

Download Refresh

Congratulations! You now have access to the new 'Risky users' report of the refreshed Azure AD Identity Protection. Try it out. →

Search users

USER	RISK LEVEL	RISK EVENTS	STATUS	LAST UPDATED (UTC)
 Demo Bruker	Medium	1 risk event	Loading...	29.3.2019, 2:41 p.m.

6. Videre klikker jeg på Demo Bruker for å få mer informasjon om hendelsen.

Home > Azure AD Identity Protection - Overview > Users > DemoBruker


Users

AZURE AD IDENTITY PROTECTION

Download Refresh

Congratulations! You now have access to the new 'Risky users' report of the refreshed Azure AD Identity Protection. Try it out. →

Search users

USER	RISK LEVEL	RISK EVENTS	STATUS	LAST UPDATED (UTC)
 Demo Bruker	Medium	1 risk event	At risk	29.3.2019, 2:41 p.m.

DemoBruker


All sign-ins Reset password Dismiss all events

Essentials

Risk level	Medium	Status	At risk
Role	User	Contact	demobruker@09999.no
Location	N/A	MFA registered	No
Department	N/A	Object id	526e1108-1b7e-447f-8730-0d42f71eb7cf

Risk events

1



TIME (UTC)	IP ADDRESS	RISK EVENT TYPE	RISK LEVEL
29.3.2019 14:31	185.220.101.3	Sign-in from anonymous IP address	Medium

7. Da får status om at Demo Bruker er under risk og da bør man helst gjenopprette passordet så fort så mulig.

Home > Azure AD Identity Protection - Overview > Users > DemoBruker > DemoBruker - Sign-in events

DemoBruker - Sign-in events

Columns Refresh Download Power BI Troubleshoot

Date: 1 Month User: DemoBruker Application: Enter application name Client: Enter client name Status:

Apply

Search using username, application, status or IP address. Search requires exact text.

APPLICATION	STATUS	DATE	MFA AUTH METHOD
Azure Portal	Success	29.3.2019, 15:31:53	
Azure Portal	Failure	29.3.2019, 15:31:45	
Azure Portal	Success	29.3.2019, 15:25:20	
Azure Portal	Failure	29.3.2019, 15:25:17	
Azure Portal	Failure	29.3.2019, 15:25:17	
Azure Portal	Failure	29.3.2019, 15:23:39	

8. Det er også mulig å Se på Sign-in events ved å klikke på All sign-ins fra forrige bilde. Da får vi opp de ulike innloggingene på Demo Bruker og status på om de har virkelig blitt innlogget eller mislykket.

DemoBruker

All sign-ins **Reset password** Dismiss all events

Essentials

Risk level	Medium	Status	At risk
Role	User	Contact	demobruker@09999.no
Location	N/A	MFA registered	No
Department	N/A	Object Id	526e1108-1b7e-447f-8730-0d42f71eb7cf

Risk events

1

TIME (UTC)	IP ADDRESS	RISK EVENT TYPE	RISK LEVEL
29.3.2019 14:31	185.220.101.3	Sign-in from anonymous IP address	Medium

Reset password

DemoBruker

How would you like the password to be reset?

Generate a temporary password

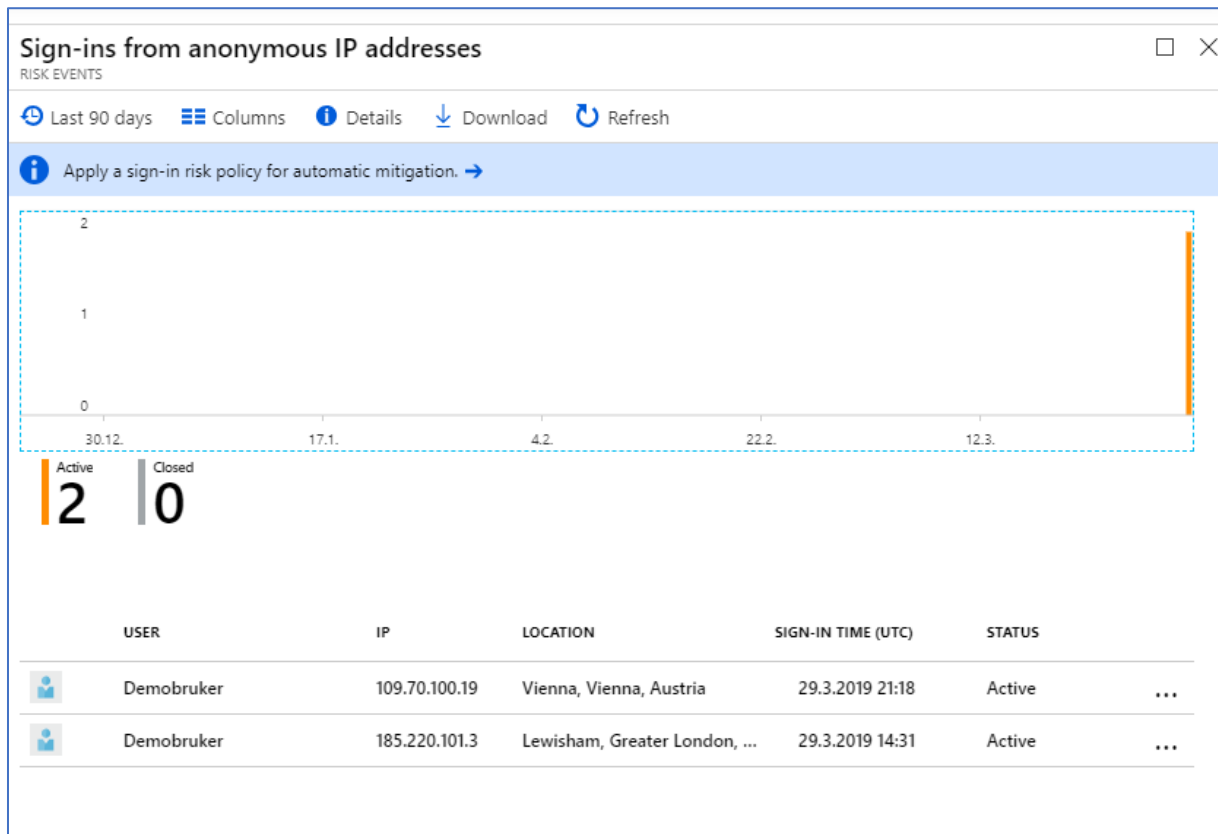
Require the user to reset their password

User is not registered for multi-factor authentication. Click here to enable multi-factor authentication registration.

Select

9. Det beste er å gjenopprette passordet så fort så mulig, siden det vanligvis ikke er vanlig at man blir logget inn fra ukjente steder med mindre man vet at man tar i bruk VPN tilkoblinger.

Dette gjør vi ved å klikke på Reset password. Deretter tikker jeg av for «Generate a temporary password» og deretter klikker jeg på select knappen. Da skal du få et midlertidig passord, som du kan videre endre etter innlogging av bruker.



10. Ovenfor ser man et bilde av når jeg logget meg inn med Demo Bruker fra Tor Browser igjen, forsøk nummer 2. Da ser vi at jeg får også en annen lokasjon Vienna, Austria, noe som også virker veldig mistenkelig for meg. Slike indikasjoner er tegn på mistenkelig aktivitet med mindre man vet at man har gjort det selv, og da blir hver og en av slike varsler veldig viktig å ta på alvor. Vi kan her se at Demobruker har hatt to innlogginger fra to ulike lokasjoner, den ene fra Vienna i Østerrike og har en IP-adresse på: 109.70.100.19 og den andre fra Lewisham, United Kingdom og har en IP-adresse på: 185.220.101.3.

Home > Azure AD Identity Protection - Users flagged for risk

Azure AD Identity Protection - Users flagged for risk

Download Refresh

Search (Ctrl+J)

Search users

Download Refresh

Congratulations! You now have access to the new 'Risky users' report of the refreshed Azure AD Identity Protection. Try it out. →

USER	RISK LEVEL	RISK EVENTS	STATUS	LAST UPDATED (UTC)
Demo Bruker	Secured	2 risk events	Remediated	13.4.2019, 11:03 a.m.

GENERAL

- Overview
- Getting started

INVESTIGATE

- Users flagged for risk**
- Risk events
- Vulnerabilities

CONFIGURE

- MFA registration
- User risk policy
- Sign-in risk policy

SETTINGS

- Alerts
- Weekly Digest
- Pin to dashboard

Troubleshooting + support

- Troubleshoot
- New support request

Home > Azure AD Identity Protection - Users flagged for risk > DemoBruker

DemoBruker

All sign-ins Reset password Dismiss all events

Essentials

Risk level	Status
Secured	Remediated
Role	Contact
User	demobruker@09999.no
Location	MFA registered
N/A	No
Department	Object Id
N/A	526e1108-1b7e-447f-8730-0d42f71eb7cf

Risk events

2

TIME (UTC)	IP ADDRESS	RISK EVENT TYPE	RISK LEVEL
29.3.2019 21:18	109.70.100.19	Sign-in from anonymous IP address	Medium
29.3.2019 14:31	185.220.101.3	Sign-in from anonymous IP address	Medium

11. Andre måter å få samme informasjon på som beskrevet tidligere er å i bruk Users flaggedged

for risk under Investigate funksjonen.

Azure AD Identity Protection - Risk events

GENERAL

- Overview
- Getting started

INVESTIGATE

- Users flagged for risk
- Risk events**
- Vulnerabilities

CONFIGURE

- MFA registration
- User risk policy
- Sign-in risk policy

SETTINGS

- Alerts
- Weekly Digest
- Pin to dashboard

Troubleshooting + support

- Troubleshoot
- New support request

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
Medium	Real-time	Sign-ins from anonymous IP addresses	2 of 2	29.3.2019, 9:18 p.m.

Azure AD Identity Protection - Risk events > Sign-ins from anonymous IP addresses

Sign-ins from anonymous IP addresses

RISK EVENTS

Last 90 days Columns Details Download Refresh

Apply a sign-in risk policy for automatic mitigation.

Active: 0 Closed: 2

USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS
Demobruker	109.70.100.19	Vienna, Vienna, Austria	29.3.2019 21:18	Closed (password ...)
Demobruker	185.220.101.3	Lewisham, Greater London, ...	29.3.2019 14:31	Closed (password ...)

12. Vi kan også ta i bruk Risk events funksjonen under Investigate for å se etter trusler som har forekommet under Identity seksjonen.

3.1.1.2 Vulnerabilities

Home > Azure AD Identity Protection - Vulnerabilities

Azure AD Identity Protection - Vulnerabilities
NTNU OPPGAVE

Search (Ctrl+V)

GENERAL

- Overview
- Getting started

INVESTIGATE

- Users flagged for risk
- Risk events
- Vulnerabilities**

RISK LEVEL	COUNT	VULNERABILITY
Medium		Users without multi-factor authentication registration (explore via Identity Secure Score)

1. En annen funksjon som er genial å bruke er Vulnerabilities funksjonen i Identity Protection. I Identity Protection finner du funksjonen under menyen Investigate med navn Vulnerabilities. Dette viser sårbarheter som kan bli misbrukt av en potensiell hacker eller en person med ondsinnede hensikter.

Home > Azure AD Identity Protection - Vulnerabilities > Identity Secure Score (Preview)

Identity Secure Score (Preview)

Learn more

Last updated 14.4.2019 00:00:00

Your Identity Secure Score

75 / 223

NTNU OPPGAVE: 75
Industry average: -1
Typical 0-5 person company: 25

Change industry

Improvement actions

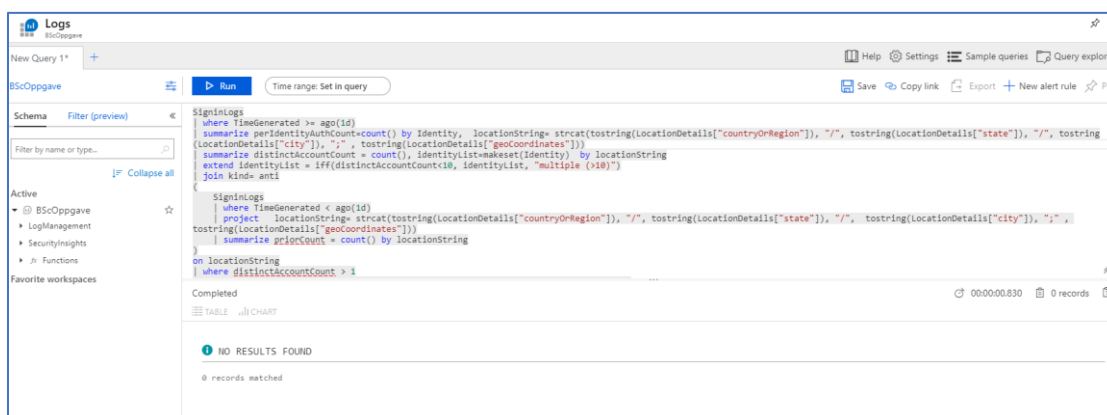
Column Download

Search to filter items...

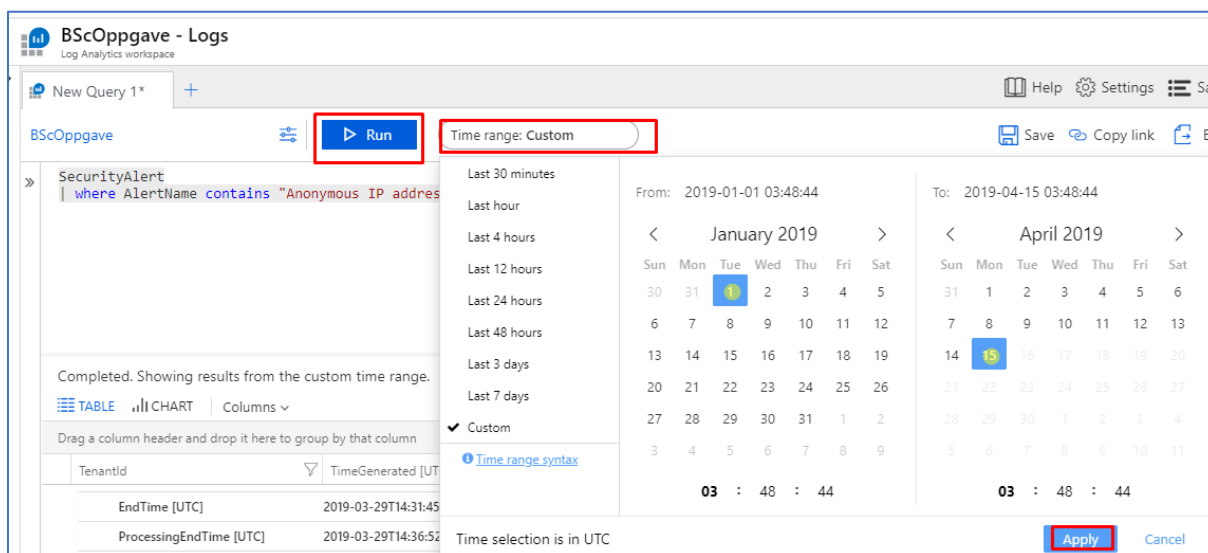
NAME	SCORE IMPACT	USER IMPACT	IMPLEMENTATION COST
Require MFA for Azure AD privileged roles	50	Low	Low
Require MFA for all users	30	Moderate	Moderate
Do not allow users to grant consent to unmanaged applications	0	Moderate	Low
Designate less than 5 global admins	0	Low	Low
Designate more than one global admin	0	Low	Low
Use limited administrative roles	0	Low	Low
Do not expire passwords	0	Moderate	Low
Delete/block accounts not used in last 30 days	0	Moderate	Low
Enable policy to block legacy authentication	20	Moderate	Moderate
Turn on sign-in risk policy	30	Moderate	Moderate
Turn on user risk policy	0	Moderate	Moderate

2. Når jeg videre klikker på sårbarheten som har blitt vist over, får jeg en med haug med anbefalinger og tiltak som bør settes i gang. Ved å sette i gang vil samtidig din Identity Secure Score forbedres og økes (☺)

3.1.2 Log Analytics



1. Her prøver jeg å kjøre en spørring opp mot loggene for å se om det har skjedd uvanlige innlogginger fra andre lokasjoner. Fra tidligere i Active Directory, har jeg brukt en DemoBruker til å logge inn fra TOR Browser på en virtuell maskin. Foreløpig har det ikke kommet noen data frem i Log Analytics om at det har skjedd uvanlige innlogginger fra andre lokasjoner.



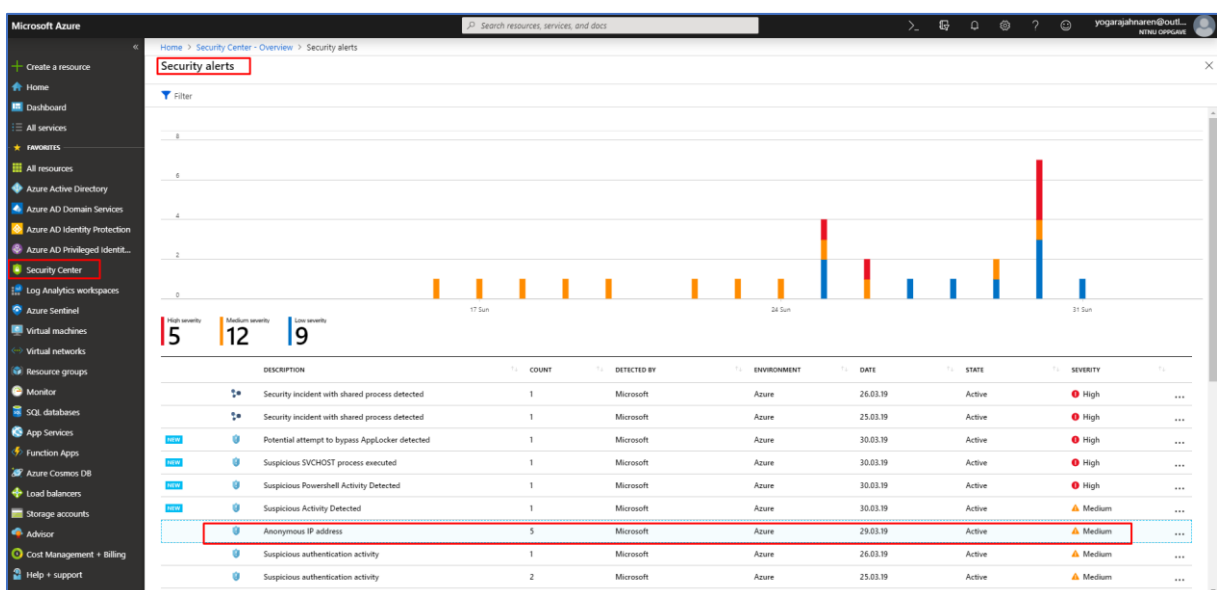
2. Videre prøver jeg å bruke en enklere query som spør opp mot alert name som allerede har forekommet i Security Center. Dermed er det også lettere å skrive en query i Log Analytics for å undersøke dypere mot en type trussel som har forekommet mot Azure miljøet. En nyttig funksjon som finnes i Log Analytics er «Time range: Custom» funksjonen. Med denne funksjonen er det mulig å tilpasse tidsperioden for søket, dermed i denne situasjonen søker jeg i tidsperioden fra og med 1 januar 2019 til og med 15 april 2019.

Drag a column header and drop it here to group by that column

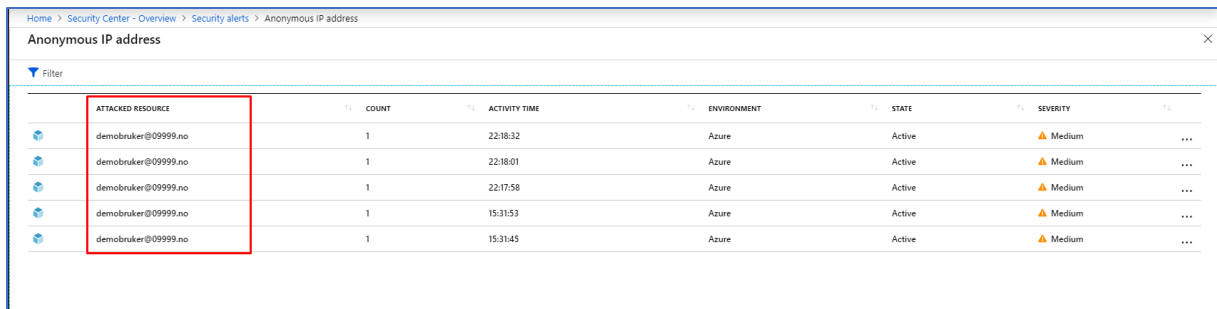
TenantId	TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity	Description	ProviderName	
	EndTime [UTC]	2019-03-29T14:31:45Z					
	ProcessingEndTime [UTC]	2019-03-29T14:36:52Z					
▼	ExtendedProperties	{"User Name": "DemoBruker", "User Account": "demobruker@09999.no", "Client IP Address": "185.220.101.3", "Client Location": "Lewisham, Greater London, GB", "Request Id": "97ed1def-634f-4d09-b810-d4a608ce7600"}					
	Client IP Address	185.220.101.3					
	Client Location	Lewisham, Greater London, GB					
	Detail Description	This risk event type indicates sign-ins from an anonymous IP address (e.g. Tor browser, anonymizer VPNs). Such IP addresses are commonly used by actors who want to hide their login telemetry (IP address, user agent, etc.)					
	Request Id	97ed1def-634f-4d09-b810-d4a608ce7600					
	User Account	demobruker@09999.no					
	User Name	DemoBruker					
>	Entities	[{"Sid": "3", "Name": "demobruker", "UPNSuffix": "09999.no", "AADTenantId": "f5770ea5-40b5-4695-8b59-c9f17ef6f804", "AADUserId": "526e1108-1b7e-447f-8730-0d42f71eb7cf", "DisplayName": "DemoBruker"}]					
	SourceSystem	Detection					
	Type	SecurityAlert					

3. Etter søket er utført får jeg med Log Analytics opp flere detaljer om trusselen som har kommet til Azure miljøet mitt. Ved bruk av Log Analytics får jeg litt mer bredere informasjon enn det jeg gjør i Azure Security Center, her i Log Analytics får vi med ulike egenskaper av trusselen som har forekommet. Vi ser videre hvilket brukerkonto som er angrepet. Klient IP adressen kommer frem og klient lokasjonen vises. Ut i fra dette kan vi selv vite om det er egentlig vi eller noen andre som har prøvd å logge inn på vår bruker. Når det forekommer uvanlige innlogginger fra ukjente steder som du ikke har vært eller vet at du ikke har brukt en VPN tilkobling gjennom må automatisk regnes som noe mistenkelig aktivitet som er på gang på din konto.

3.1.3 Security Center



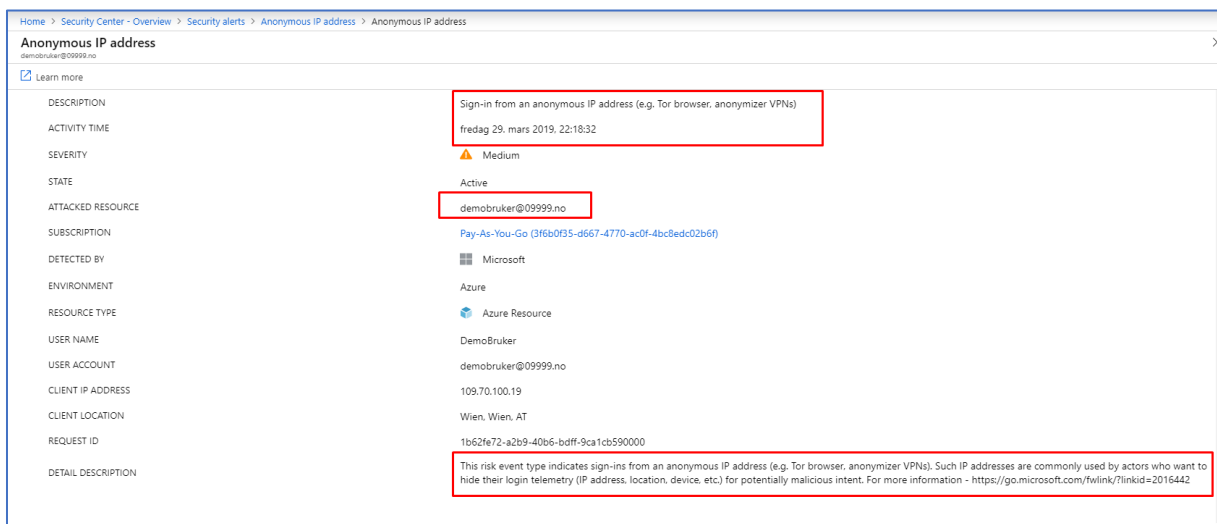
1. I Azure Security Center har det kommet opp et varsel om Anonyme IP Adresser. Jeg klikker videre inn på dette varsllet.



The screenshot shows a table of security alerts in Azure Security Center. The table has columns for 'ATTACKED RESOURCE', 'COUNT', 'ACTIVITY TIME', 'ENVIRONMENT', 'STATE', and 'SEVERITY'. Five rows are visible, all with 'demobruker@09999.no' as the attacked resource, a count of 1, and a severity of 'Medium'. The first row's 'ATTACKED RESOURCE' cell is highlighted with a red box.

ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY
demobruker@09999.no	1	22:18:32	Azure	Active	Medium
demobruker@09999.no	1	22:18:01	Azure	Active	Medium
demobruker@09999.no	1	22:17:58	Azure	Active	Medium
demobruker@09999.no	1	15:31:53	Azure	Active	Medium
demobruker@09999.no	1	15:31:45	Azure	Active	Medium

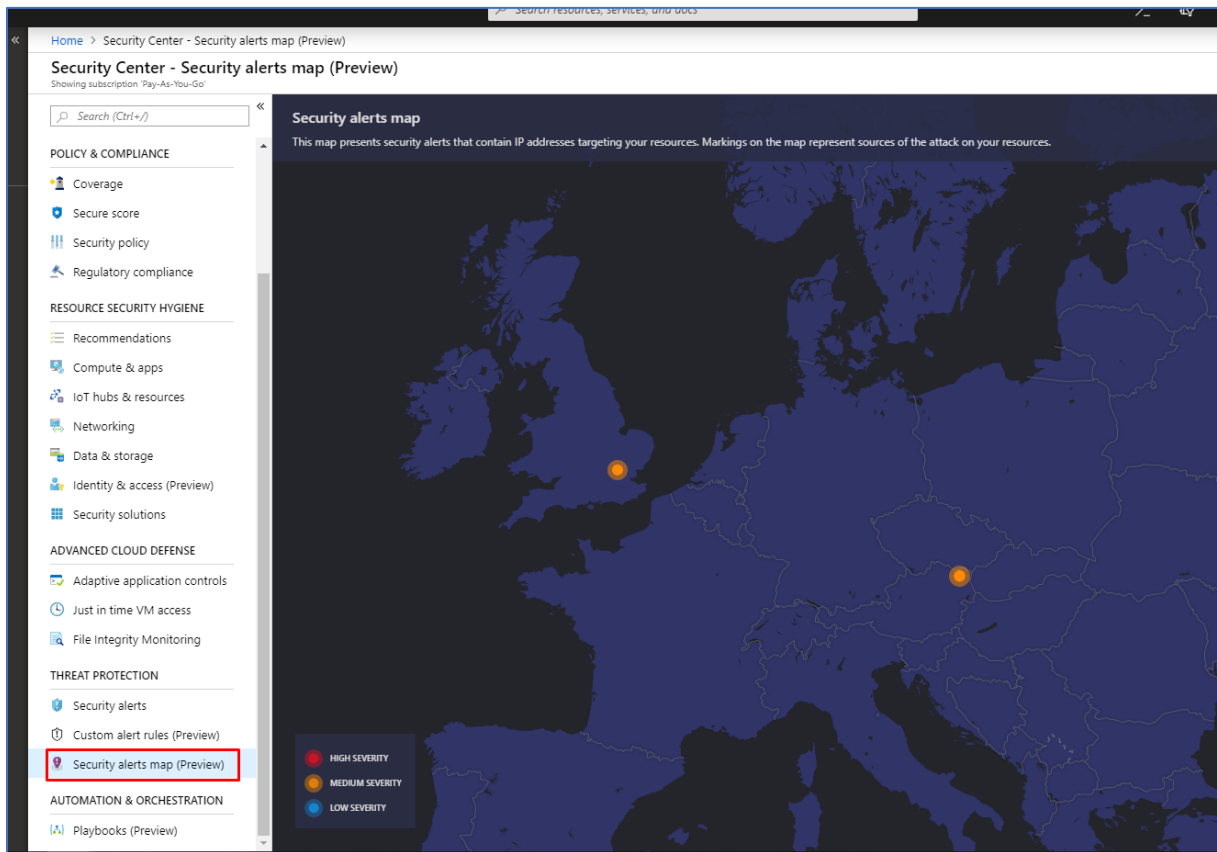
2. Videre ser jeg at demobruker@09999.no er angrepet. Jeg klikker på en av ressursene for angrepet for videre etterforskning.



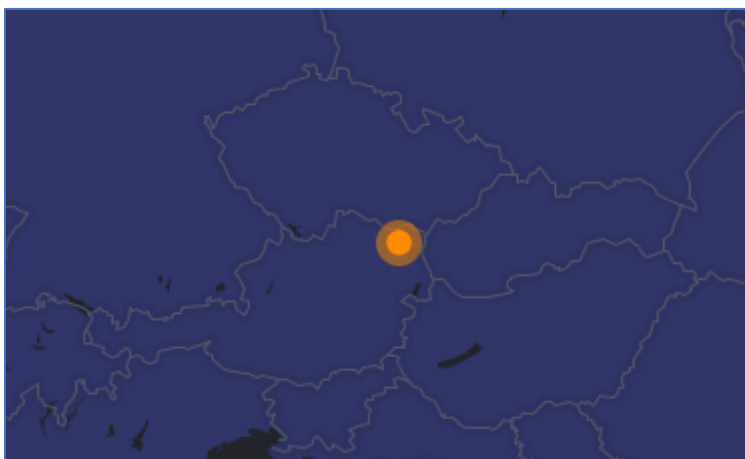
The screenshot shows the detailed view of a security alert. The 'DESCRIPTION' field is highlighted with a red box and contains the text: 'Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)'. The 'ATTACKED RESOURCE' field is also highlighted with a red box and contains the email address 'demobruker@09999.no'. At the bottom, a 'DETAIL DESCRIPTION' field is highlighted with a red box and contains a warning message: 'This risk event type indicates sign-ins from an anonymous IP address (e.g. Tor browser, anonymizer VPNs). Such IP addresses are commonly used by actors who want to hide their login telemetry (IP address, location, device, etc.) for potentially malicious intent. For more information - https://go.microsoft.com/fwlink/?linkid=2016442'.

3. Da får jeg mer informasjon om at det har skjedd innlogginger med anonyme IP adresser fra TOR Browser eller også andre anonymiserte VPNer. I dette tilfelle er det riktig at det har skjedd innlogging med TOR Browser. Trussel deteksjonen med Security Center har virket og jeg har fått frem innloggingen jeg gjorde via TOR Browser i tidligere fase her i Security Center. Detaljert beskrivelse (Detail Description) fra Microsoft sin side viser seg å stemme med metoden som har blitt tatt i bruk for å sette i gang trusselen, Microsoft har klart å gjenkjenne innlogging foretatt med TOR Browser eller også med andre anonymiserte VPN.

3.1.3.1 Security Alerts Map



1. Jeg navigerer meg videre til Security Alerts Map under Threat Protection menyen i Security Center. Her finner jeg to alerts markert i orange farge med medium severity nivå.



2. Videre klikker jeg på en av disse prikkene med security alerts.

Home > Security Center - Security alerts map (Preview) > 109.70.100.19

109.70.100.19

Filter

ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY	
demobruker@09999.no	1	29.03.19, 22:18	Azure	Active	▲ Medium	...
demobruker@09999.no	1	29.03.19, 22:18	Azure	Active	▲ Medium	...
demobruker@09999.no	1	29.03.19, 22:17	Azure	Active	▲ Medium	...

3. Da får jeg opp ressurser som er angrepet. Jeg velger å klikke på første ressursen som er angrepet i dette tilfelle.

Home > Security Center - Security alerts map (Preview) > 109.70.100.19 > Anonymous IP address

Anonymous IP address
demobruker@09999.no

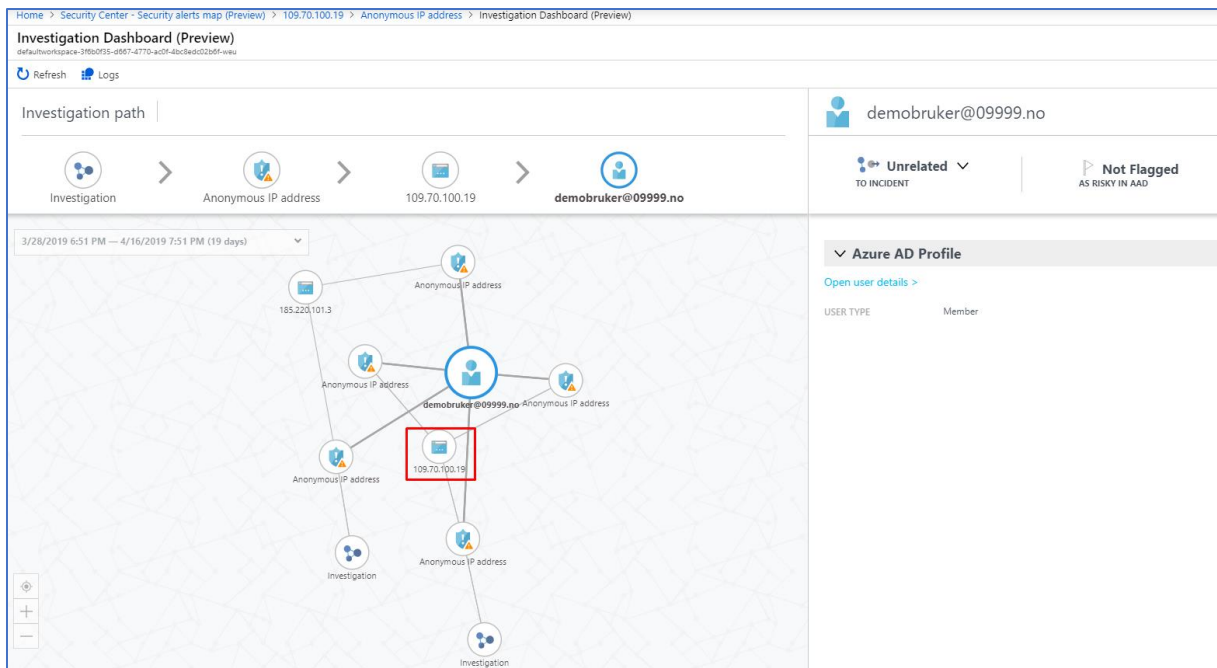
Learn more

DESCRIPTION	Sign-in from an anonymous IP address (e.g. Tor browser, anonymizer VPNs)
ACTIVITY TIME	fredag 29. mars 2019, 22:18:32
SEVERITY	▲ Medium
STATE	Active
ATTACKED RESOURCE	demobruker@09999.no
SUBSCRIPTION	Pay-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8edc02b6f)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Azure Resource
USER NAME	DemoBruker
USER ACCOUNT	demobruker@09999.no
CLIENT IP ADDRESS	109.70.100.19
CLIENT LOCATION	Wien, Wien, AT
REQUEST ID	1b62fe72-a2b9-40b6-bdff-9ca1cb590000
DETAIL DESCRIPTION	This risk event type indicates sign-ins from an anonymous IP address (e.g. Tor browser, anonymizer VPNs). Such IP addresses are commonly used by actors who want to hide their login telemetry (IP address, location, device, etc.) for potentially malicious intent. For more information - https://go.microsoft.com/fwlink/?linkid=2016442

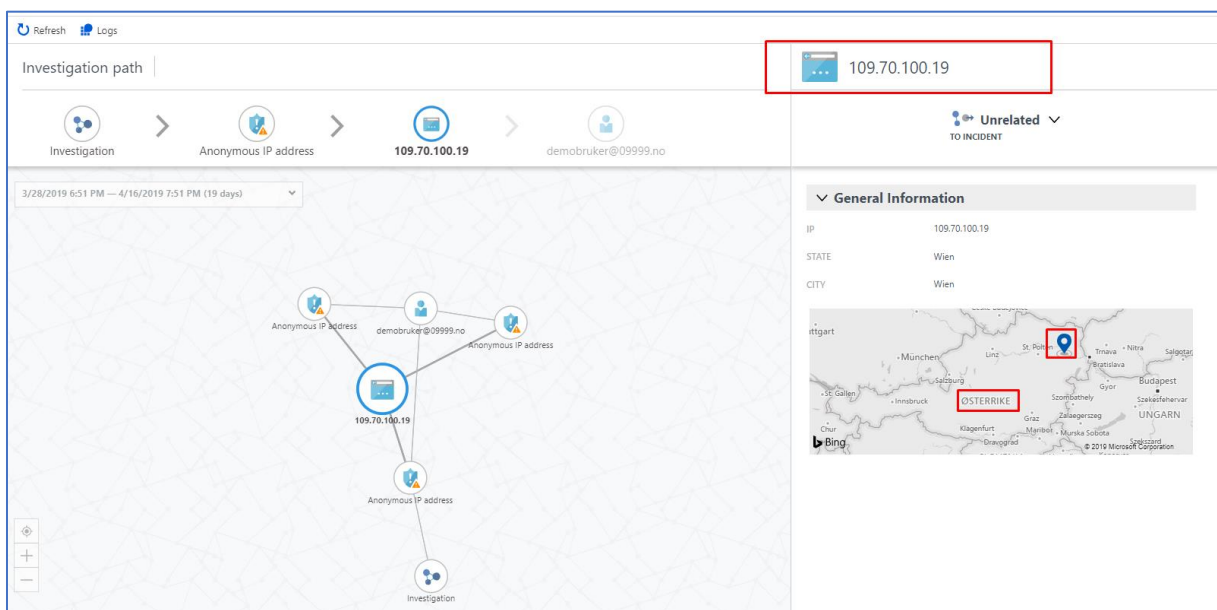
Was this useful? Yes No

Continue investigation View playbooks

4. Da får jeg videre en mer detaljert informasjon om angrepet som har tatt sted. Jeg velger videre å klikke på Continue investigation.



5. Jeg velger videre å klikke på IP adressen som er markert i rød boks, siden det er denne IP - adressen angrepet stammer fra.



6. Videre får jeg da opp et skjermbilde av et kart med lokasjonspinn. Denne lokasjonen viser hvor angrepet stammer fra. Det er ofte at angripere tar i bruk TOR Browser og da får man opp forskjellige lokasjoner siden TOR Browser skjuler spor og oppfører seg som de er fra flere ulike lokasjoner. Mer eksakt så vet vi også at angrepet kommer fra Wien i Østerrike fra tidligere skjermbilde fra Security Center.

Home > Security Center - Overview > Security alerts > Suspicious Powershell Activity Detected > Suspicious Powershell Activity Detected

Suspicious Powershell Activity Detected

WIN16

[Learn more](#)

General information

DESCRIPTION	Analysis of host data detected a powershell script running on WIN16 that has features in common with known suspicious scripts. This script could either be legitimate activity, or an indication of a compromised host.
ACTIVITY TIME	torsdag 4. april 2019, 02:40:58
SEVERITY	● High
STATE	Active
ATTACKED RESOURCE	WIN16
SUBSCRIPTION	Pay-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8edc02b6f)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
ACCOUNT SESSION ID	0x99b371a9
SUSPICIOUS PROCESS	c:\windows\system32\windowspowershell\v1.0\powershell.exe
SUSPICIOUS COMMAND LINE	"c:\windows\system32\windowspowershell\v1.0\powershell.exe" -nop -exec bypass -encodedcommand "cabvahcazqbyahmaablagwabaaga0aywvbag0abqbhag4azaagacjagahsalabpahcagag aggadab0ahaacvaf6ac0alwbkag0adwbuagwawbwhagqalgzahnkacwbpag4adablahibghagwac

Was this useful? Yes No

4. Videre klikker jeg meg inn på maskinen, og får jeg en mer detaljert beskrivelse av angrepet som er gjenkjent. Azure Security Center har mulighet til å gjenkjenne PowerShell aktivitet som virker mistenkelig. Deretter kan Azure Security Center varsle brukeren med en mer detaljert rapport om hva som forekommer i mistenkelig aktivitet som er oppdaget eller et eventuelt angrep som er forekommet i Azure. Basert på Microsoft sin side, kan slik type melding som «Suspicious Powershell Activity Detected» være enten en legitimert aktivitet eller også en indikasjon på at den aktuelle hosten er kompromittert.

Fokusert Annet Filtre

Suspicious Powershell Activity Detected alert on subscription 3f6b0f35-d667-4770-ac0f-4bc8edc02b6f

Microsoft Azure <azure-noreply@microsoft.com>
to: 04.04.2019 02:41
Du

HIGH SEVERITY

Azure Security Center has discovered a potential security threat on your environment

Suspicious Powershell Activity Detected
Analysis of host data detected a powershell script running on WIN16 that has features in common with known suspicious scripts. This script could either be legitimate activity, or an indication of a compromised host.
April 4, 2019 0:40 UTC

WIN16
Attacked Resource

Microsoft
Detected by

[Explore in Azure Security Center >](#)

f t y in

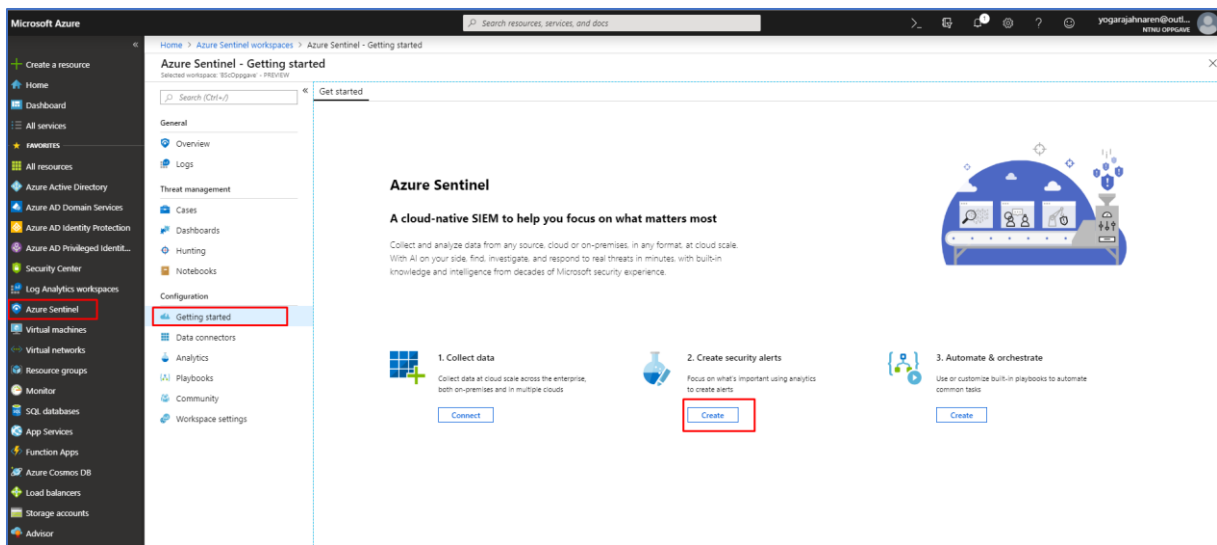
5. I mailboksen min har jeg samtidig fått et varsel om at Azure Security Center har gjenkjent en potensiell trussel hvor det innebærer mistenkelig aktivitet av Powershell.

3.2.2 Log Analytics

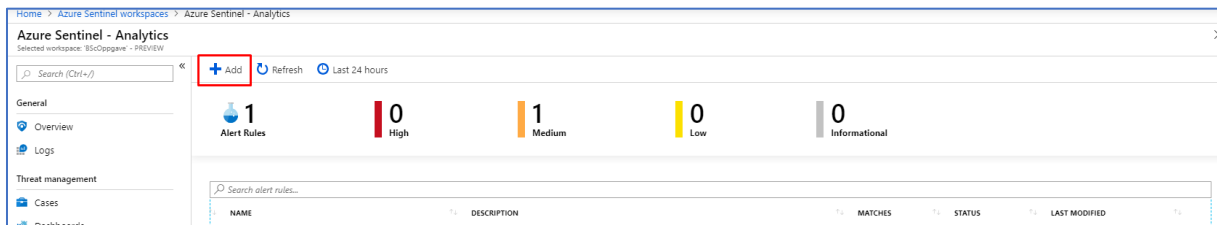
The screenshot displays the Azure Log Analytics interface. At the top, there's a search bar and navigation options. Below that, the workspace name and logs are visible. A KQL query is entered in the 'New Query' box, highlighted with a red border. The query is: `SecurityEvent | where Process contains 'powershell.exe' and CommandLine contains '-enc' | extend b64 = extract('[A-Za-z0-9|+|/|/](30,)', 0, CommandLine) | extend utf8_decode=base64_decodestring(b64) | project TimeGenerated, Computer, CommandLine, utf8_decode, SubjectLogonId`. Below the query, the results are shown in a table format, also highlighted with a red border. The table has columns for TimeGenerated [UTC], Computer, CommandLine, utf8_decode, and SubjectLogonId. Two records are displayed, both for the computer 'PenTestMaskin' and the user '0x146863'. The first record shows a Powershell command executed on 2019-03-30T20:13:57.123Z. The second record shows a Powershell command executed on 2019-03-30T20:03:06.440Z.

1. Jeg prøver her å søke etter det mistenkelige Powershell scriptet som ble utført i tidligere steg. Første øverste boks markert i rødt viser KQL spørring som blir utført for å se etter det mistenkelige Powershell scriptet. Deretter i andre boks nedenfor får jeg resultatet av spørringen. Denne boksen viser resultatet av det mistenkelige Powershell scriptet som har blitt kjørt tidligere

3.1.4 Azure Sentinel



1. Jeg ønsker å lage en alert rule basert på data som har blitt samlet inn fra tilkoblede dataressurser. Dette gjør jeg ved å navigere meg frem til Azure Sentinel menyen, deretter videre til Getting started undermeny og videre klikker på create under «Create security alerts».



2. Videre klikker jeg på Add for å opprette en ny Security Alert.

Home > Azure Sentinel workspaces > Azure Sentinel - Analytics > Create alert rule

Create alert rule

PREVIEW

Status

Details

* Name ✓

Description ✓

Severity

Logic

Alert simulation

* Set alert query
Set time and interval parameters only using the **Period** field under **Alert scheduling**.

✓

3. Deretter legger jeg inn en Security Alert for TOR IP-adresser. Jeg legger deretter inn en tilpasset query for å gjenkjenne anonymiserte IP Adresser fra TOR nettverket under «Set alert query».

Home > Azure Sentinel workspaces > Azure Sentinel - Analytics > Create alert rule

Create alert rule

PREVIEW

Account	<input type="text" value="Choose column"/>	<input type="button" value="Add"/>
Host	<input type="text" value="Choose column"/>	<input type="button" value="Add"/>
IP address	<input type="text" value="Choose column"/>	<input type="button" value="Add"/>

Alert trigger

Operator:

* Threshold:

Alert scheduling

* Frequency:

* Period:

Realtime automation - coming soon!

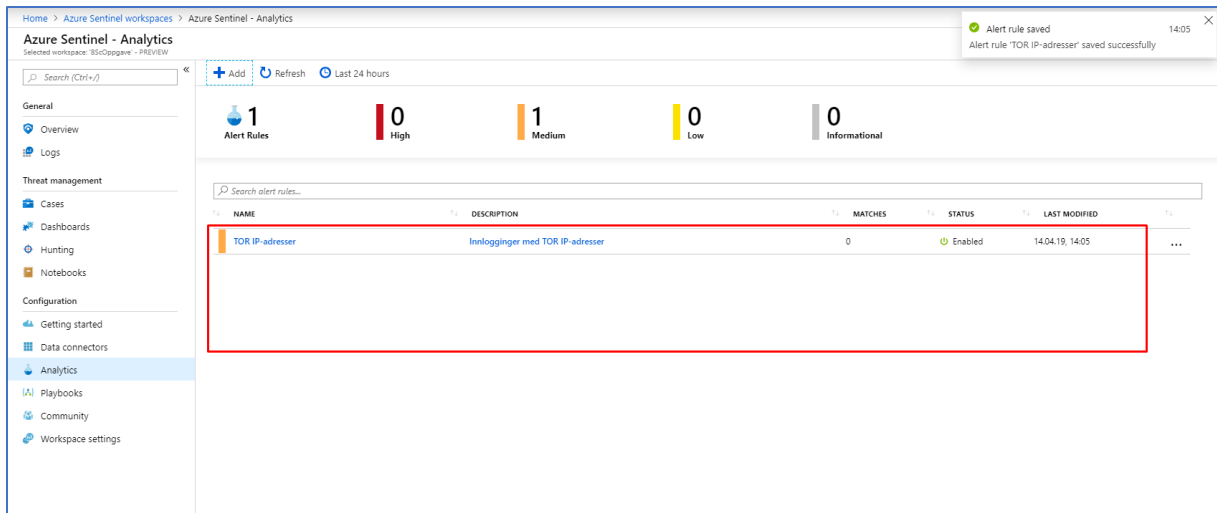
Triggered playbooks:

Alert suppression

Suppression status:

* Suppress alerts for:

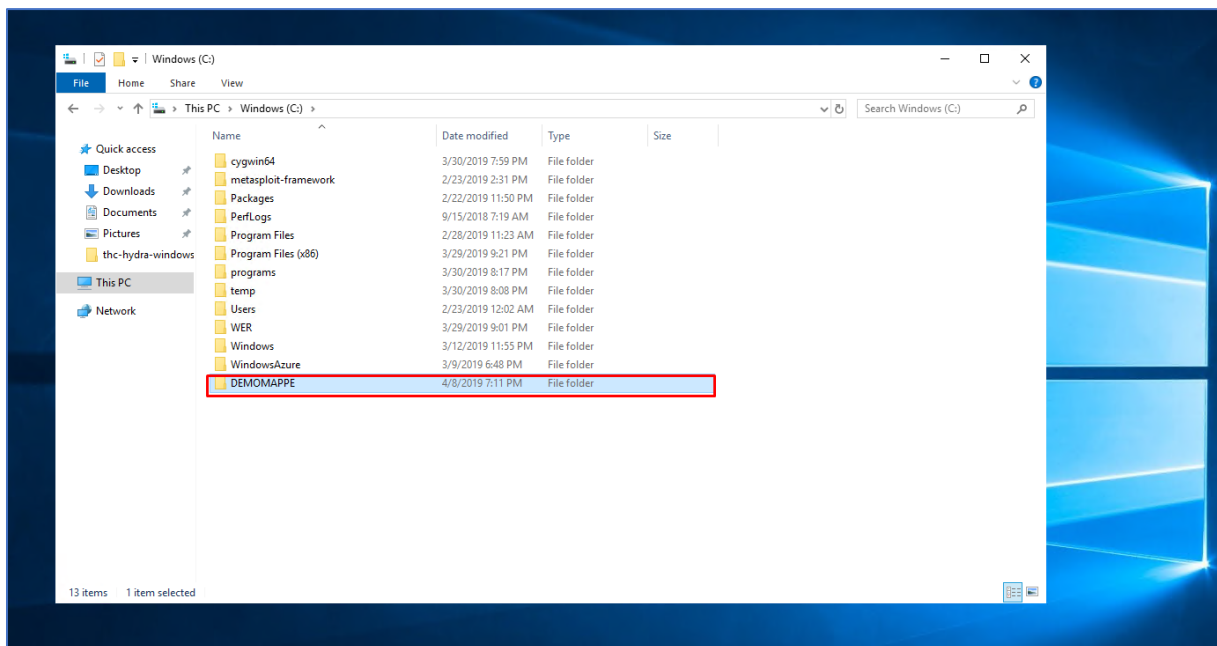
4. Videre setter jeg Threshold til 1.



5. Her ser vi at tilpasset Security Alert er opprettet og synlig i Azure Sentinel – Analytics.

3.3 Suspicious SVCHOST process executed

3.3.1 Security Center



1. Jeg lager en DEMOMAPPE under C:/ drive.


```
C:\ Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\nareny>cd\DEMOMAPPE

C:\DEMOMAPPE>
```

2. Deretter åpner jeg CMD og navigerer meg frem til DEMOMAPPE stien.

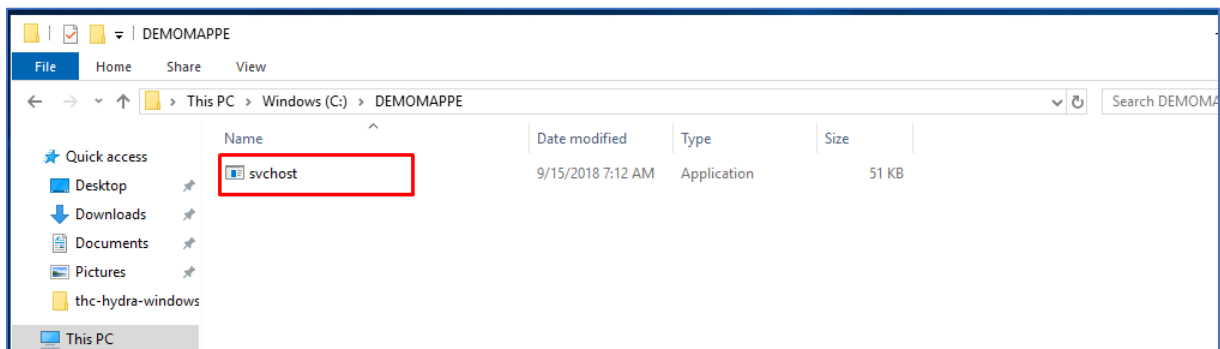
```
C:\ Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\nareny>cd\DEMOMAPPE

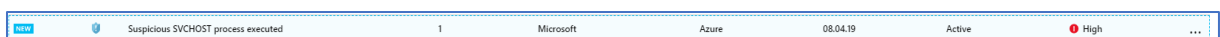
C:\DEMOMAPPE>copy c:\Windows\System32\svchost.exe
1 file(s) copied.

C:\DEMOMAPPE>
```

3. Videre kopierer jeg svchost.exe filen til DEMOMAPPE.



4. Deretter dobbel klikker jeg på svchost filen som ligger i DEMOMAPPEN, for å få kjørt prosessen.



5. Videre går jeg til Security Center. Etter en liten stund får jeg opp meldingen «Suspicious SVCHOST process executed». Dette er en god indikasjon på det har skjedd noe mistenkelig i mitt Azure miljø. Man kan enten ha blitt angrepet i denne sammenhengen, eller det kan kun

ha vært satt i gang en mistenkelig prosess av selve systemet. Jeg klikker meg videre inn på sikkerhetsvarslet for å lære mer om denne hendelsen.

Home > Suspicious SVCHOST process executed

Suspicious SVCHOST process executed

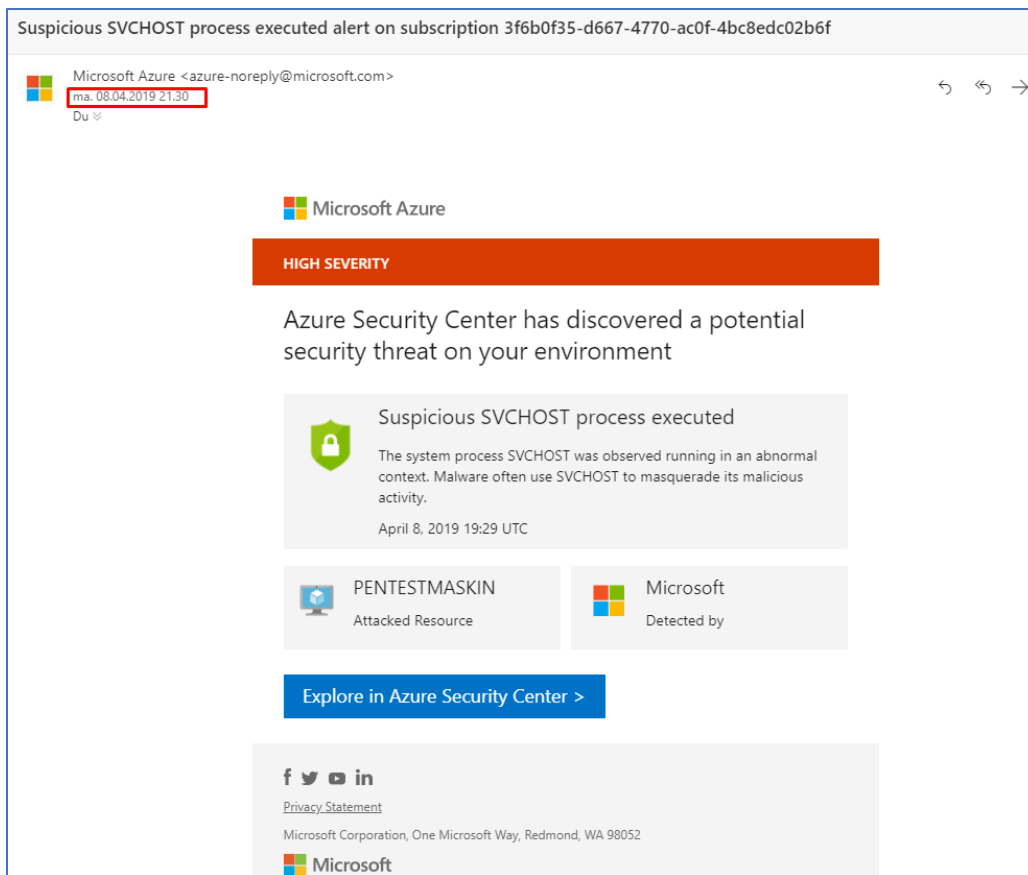
PENTESTMASKIN

[Learn more](#) [Security Center](#)

General information

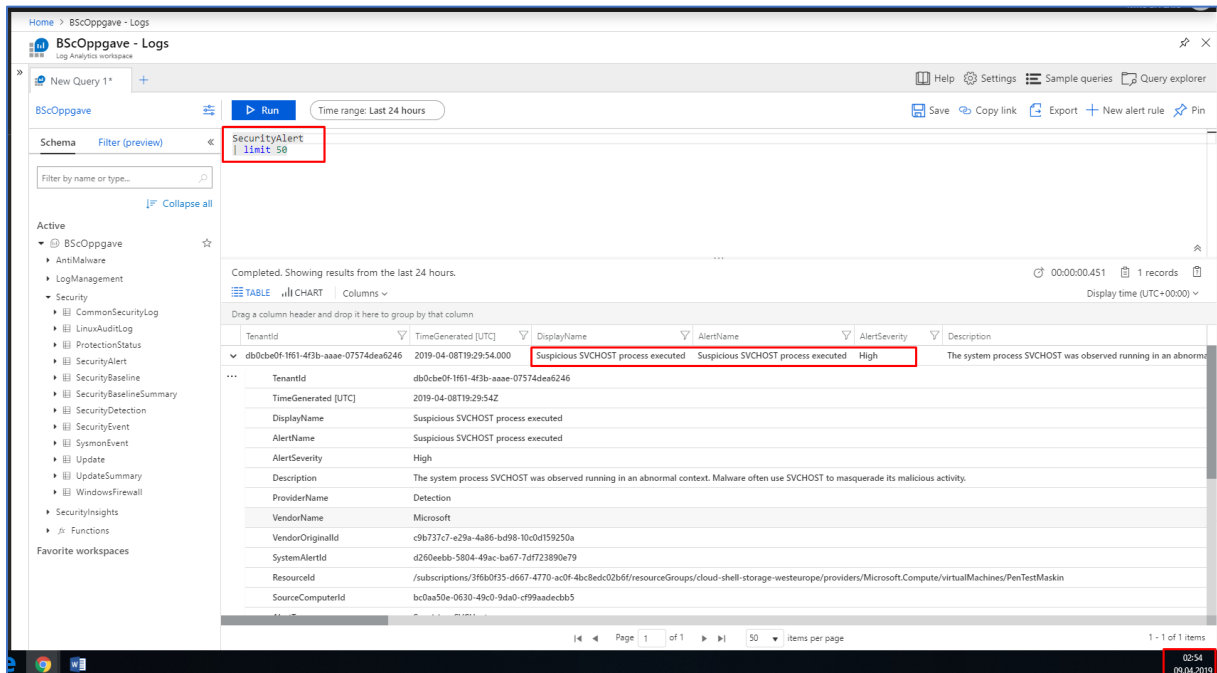
DESCRIPTION	The system process SVCHOST was observed running in an abnormal context. Malware often use SVCHOST to masquerade its malicious activity.
ACTIVITY TIME	mandag 8. april 2019, 21:29:47
SEVERITY	● High
STATE	Active
ATTACKED RESOURCE	PENTESTMASKIN
SUBSCRIPTION	3f6b0f35-d667-4770-ac0f-4bc8edc02b6f
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
DOMAIN NAME	PenTestMaskin
USER NAME	PENTESTMASKIN\ntareny
PROCESS NAME	c:\demomappe\svchost.exe
COMMAND LINE	"c:\demomappe\svchost.exe"
PARENT PROCESS	explorer.exe

6. Videre får jeg informasjon om at det er har blitt kjørt svchost prosessen har blitt kjørt i en uvanlig kontekst. Noe som også stemmer med det jeg har testet. Her ser vi at Security Center greier å gjenkjenne slike type mistenkelig aktivitet ganske raskt. Basert på Microsoft sin beskrivelse av denne meldingen ovenfor er det ofte en oppfatning at det er ofte at Malware som tar i bruk denne SVCHOST prosessen til å gjemme utføringen sin av ondsinnet aktivitet.



7. Bildet ovenfor viser at varslet som har forekommet i Azure Security Center også har blitt sendt til min mail. Jeg har nemlig knyttet Security Center med min mail, slik at jeg får tilsendt varsler som forekommer i Security Center når jeg er «on the go». Dermed når jeg er «on the go» så får jeg informasjon om det som foregår i Azure miljøet mitt og videre mulighet til å sette i gang tiltak når det forekommer trussel situasjoner.

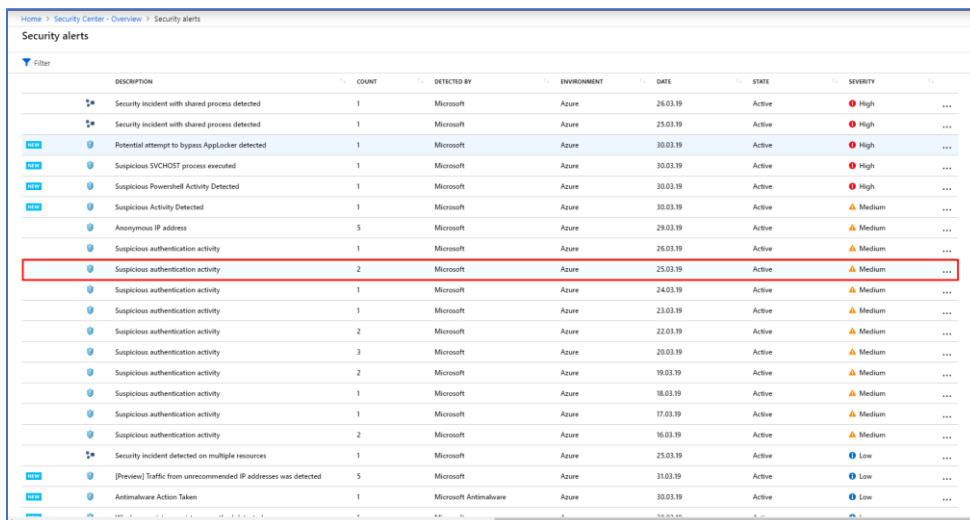
3.3.2 Log Analytics



1. Jeg bruker Log Analytics for å søke gjennom de siste Security Alerts som har forekommet i mitt Azure miljø. Videre får jeg da opp den mistenkelige svchost prosessen som ble satt i gang fra tidligere fase. Mye av informasjonen fra Security Center får vi også gjennom Log Analytics, og her ser vi at disse tjenestene har en sterk tilknytning til hverandre.

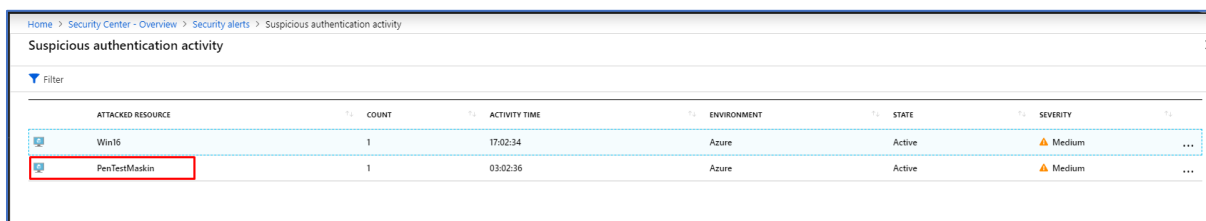
3.4 Brute-force angrep

3.4.1 Security Center



DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY
Security incident with shared process detected	1	Microsoft	Azure	26.03.19	Active	High
Security incident with shared process detected	1	Microsoft	Azure	25.03.19	Active	High
Potential attempt to bypass AppLocker detected	1	Microsoft	Azure	30.03.19	Active	High
Suspicious SVCHOST process executed	1	Microsoft	Azure	30.03.19	Active	High
Suspicious Powershell Activity Detected	1	Microsoft	Azure	30.03.19	Active	High
Suspicious Activity Detected	1	Microsoft	Azure	30.03.19	Active	Medium
Anonymous IP address	5	Microsoft	Azure	29.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	26.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	25.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	24.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	23.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	22.03.19	Active	Medium
Suspicious authentication activity	3	Microsoft	Azure	20.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	19.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	18.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	17.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	16.03.19	Active	Medium
Security incident detected on multiple resources	1	Microsoft	Azure	25.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	5	Microsoft	Azure	31.03.19	Active	Low
Antimalware Action Taken	1	Microsoft Antimalware	Azure	30.03.19	Active	Low

1. Security Center har oppdaget noe mistenkelig og fått flere varsler med «Suspicious Authentication activity». Jeg klikker på varslet markert i rød boks.



ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY
Win16	1	17:02:34	Azure	Active	Medium
PenTestMaskin	1	03:02:36	Azure	Active	Medium

2. Videre ser jeg at det er 2 ressurser som er angrepet. Både PenTestMaskin og Win16 er angrepet. Jeg klikker videre inn på PenTestMaskin for å lære mer om hendelsen.

Home > Security Center - Overview > Security alerts > Suspicious authentication activity > Suspicious authentication activity

Suspicious authentication activity

Learn more

General information

DESCRIPTION	Although none of them succeeded, some of them used accounts were recognized by the host. This resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords in order to find valid credentials to access the host. This indicates that some of your host account names might exist in a well-known account name dictionary.
ACTIVITY TIME	mandag 25. mars 2019, 03:02:36
SEVERITY	Medium
STATE	Active
ATTACKED RESOURCE	PenTestMaskin
SUBSCRIPTION	Pay-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8edc02b6f)
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
ACTIVITY START TIME (UTC)	2019/03/25 02:02:36.6068109
ACTIVITY END TIME (UTC)	2019/03/25 02:57:43.8014127

3. Videre får jeg en mer detaljert informasjon om den mistenkelige hendelsen som har foregått. Det dreier seg om et Brute-force angrep som ikke har lyktes. Et Brute-force angrep har blitt satt i gang tidligere for å sjekke om det blir gjenkjent av security center og det har det gjort. Operasjon suksess. Microsoft presiserer videre at det er en indikasjon av at noen av host Account names foreligger i en kjent Account name Dictionary. Det kan stemme med det jeg gjorde når jeg satt i gang Brute-force angrepet. Jeg har nemlig lagt inn, flere kombinasjoner av mitt brukernavn og passord i denne Dictionary som brukes for Brute-force angrepet, noe som også er veldig vanlig dersom man ønsker å teste et slikt Brute-Force angrep.

Home > Security Center - Security alerts

Security Center - Security alerts

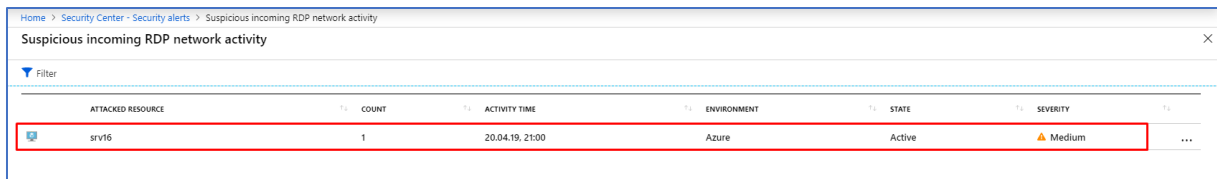
Showing subscription Pay-As-You-Go

Filter

DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY
Azure Security Center test alert (not a threat)	4	Microsoft	Azure	19.04.19	Active	High
Suspicious SVCHOST process executed	1	Microsoft	Azure	11.04.19	Active	High
Suspicious SVCHOST process executed	1	Microsoft	Azure	08.04.19	Active	High
Suspicious incoming RDP network activity	1	Microsoft	Azure	20.04.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	19.04.19	Active	Medium
[Preview] Traffic from unrecommended IP addresses wa...	2	Microsoft	Azure	25.04.19	Active	Low
[Preview] Traffic from unrecommended IP addresses wa...	2	Microsoft	Azure	24.04.19	Active	Low
[Preview] Traffic from unrecommended IP addresses wa...	6	Microsoft	Azure	23.04.19	Active	Low
[Preview] Traffic from unrecommended IP addresses wa...	6	Microsoft	Azure	22.04.19	Active	Low

4. Den 20 april 2019 ser jeg at det har Azure har gjenkjent mistenkelig RDP nettverksaktivitet i mitt Azure miljø. Jeg klikker på dette varslert for å lære mer om hendelsen. Dette er første

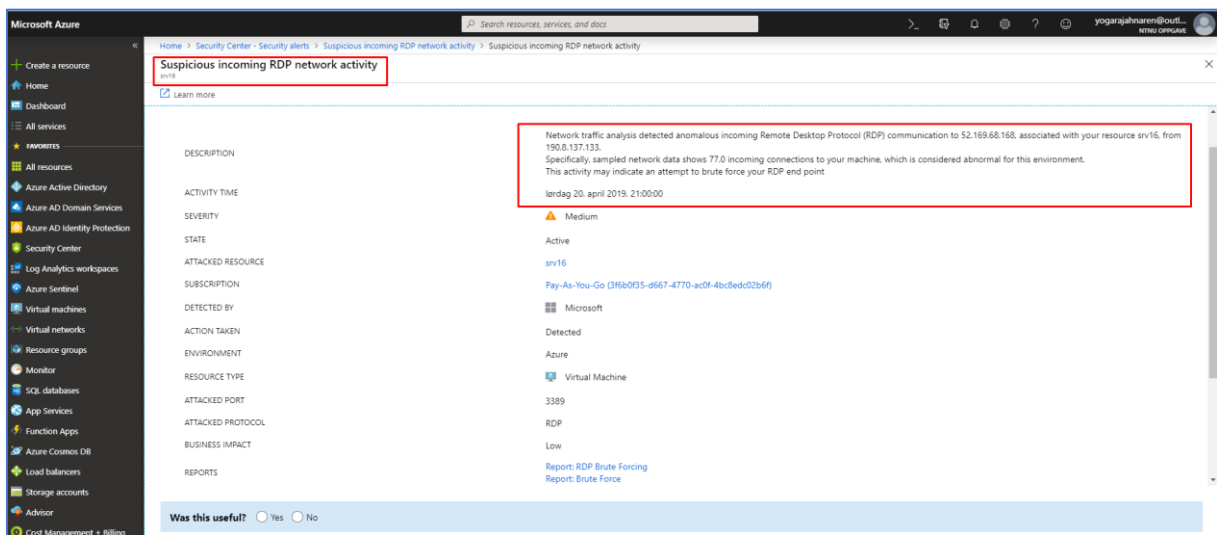
gang jeg opplever å gjenkjenne konkret mistenkelig RDP nettverksaktivitet i mitt Azure miljø.



The screenshot shows a table of security alerts in Azure Security Center. The table has columns for ATTACKED RESOURCE, COUNT, ACTIVITY TIME, ENVIRONMENT, STATE, and SEVERITY. A red box highlights the first row, which contains the following data:

ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY
srv16	1	20.04.19, 21:00	Azure	Active	Medium

5. Videre ser jeg at ressursen som er angrepet er den virtuelle maskinen srv16. Jeg klikker videre på angrepet ressurs for å lære mer om denne aktuelle hendelsen.



The screenshot shows the details of the security alert for resource 'srv16'. The alert title is 'Suspicious incoming RDP network activity'. The description states: 'Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to 52.169.68.168, associated with your resource srv16, from 190.8.137.133. Specifically, sampled network data shows 77.0 incoming connections to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point. lrdag 20. april 2019, 21:00:00'. The severity is 'Medium', the state is 'Active', and the attacked resource is 'srv16'. The subscription is 'Play-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8ed02b6f)'. The detected by is 'Microsoft', the action taken is 'Detected', and the environment is 'Azure'. The resource type is 'Virtual Machine', the attacked port is '3389', and the attacked protocol is 'RDP'. The business impact is 'Low'. There are two reports: 'Report: RDP Brute Forcing' and 'Report: Brute Force'. At the bottom, there is a 'Was this useful?' section with 'Yes' and 'No' radio buttons.

Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to 52.169.68.168, associated with your resource srv16, from 190.8.137.133. Specifically, sampled network data shows 77.0 incoming connections to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point

6. Jeg får informasjon om at Nettverkstrafikk analyser har gjenkjent anomali aktivitet tilknyttet til RDP. Jeg ser deretter at dette har vært et forsøk på Brute force angrep mot min virtuelle host. Det er en liten egenskap kalt Reports i Security Center på denne siden. Ved å klikke å lese på disse rapportene «Report: RDP Brute Forcing» og «Report: Brute Force» får du en mye mer bredere grunnlag fra Microsoft sin side som forklarer forekomsten av angrepet, grunnen til dette og hvilke tiltak du bør sette i gang.

Home > Security Center - Security alerts > Suspicious incoming RDP network activity > Suspicious incoming RDP network activity

Suspicious incoming RDP network activity

Learn more

BUSINESS IMPACT: Low

REPORTS: [Report: RDP Brute Forcing](#)
[Report: Brute Force](#)

Geo and Threat Intelligence Information

IP 190.8.137.133

Geo Information

IP ADDRESS	190.8.137.133
CITY	Lima
COUNTRY CODE	PE
COUNTRY NAME	Peru
STATE	Lima Province
ASN	19180
LATITUDE	-12.05
LONGITUDE	-77.05

7. Videre navigerer jeg meg til undermeny Geo and Threat Intelligence Information. Her ser jeg IP adressen som stammer fra angrepet og Peru er landet som angrepet kommer fra. Mer spesifikk kommer det fra Lima Province.

Home > Security Center - Security alerts > Suspicious incoming RDP network activity > Suspicious incoming RDP network activity

Suspicious incoming RDP network activity

Learn more

General information

Geo and Threat Intelligence Information

Remediation steps

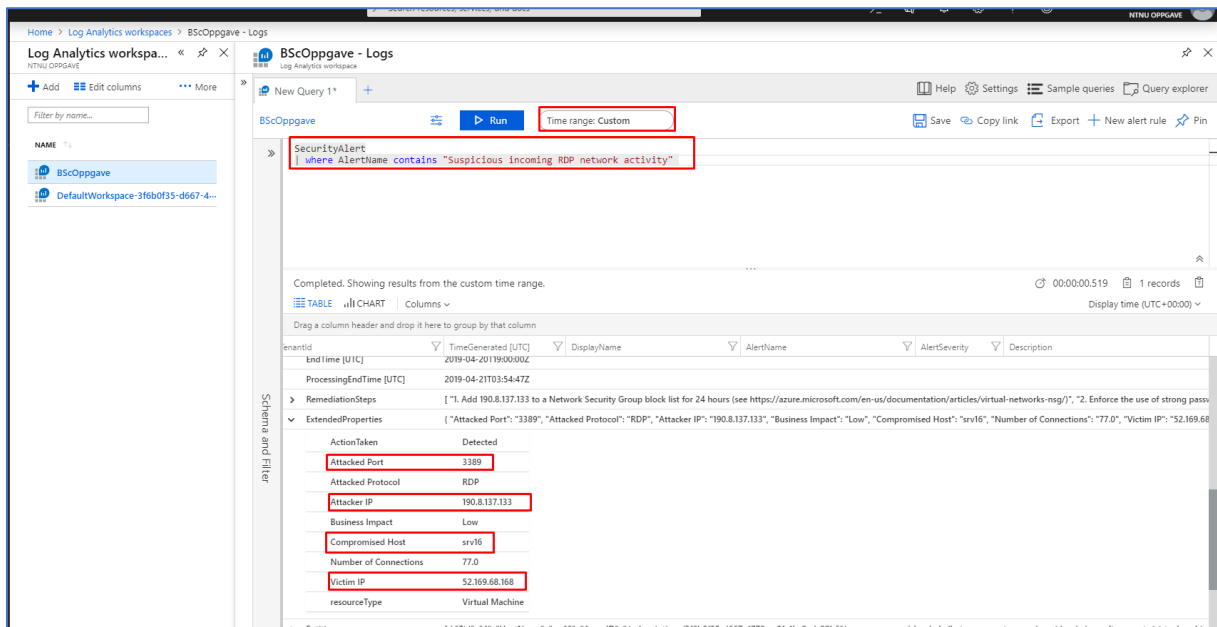
REMEDIATION STEPS

1. Add 190.8.137.133 to a Network Security Group block list for 24 hours (see <https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/>)
2. Enforce the use of strong passwords and do not reuse them across multiple resources. (see <http://windows.microsoft.com/en-us/Windows7/Tips-for-creating-strong-passwords-and-passphrases>)
3. Create an allow list for RDP access in NSG (see <https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/>).

[Apply the JIT VM access mechanism to reduce your attack surface](#)

8. Under Remediation steps får jeg mulighet til å sette i gang tiltak for å redusere utfallet av angrepet. Jeg får dermed informasjon om at jeg bør legge inn IP-adressen angrepet stammer fra i Network Security Group for blokkering. Deretter bør jeg også øke styrken på passordene mine og ikke ta i bruk samme passord på flere ressurser! Deretter bør vi typisk under slike angrep ha allerede konfigurert JIT. Ellers bør dette settes i gang med en eneste gang. Ved å ta i bruk just-in-time vm access har du mulighet til å sette valgt ip-adresser til å få tilgang til en maskin i et bestemt tidsrom. En annen ting som er lurt er å opprette en Playbook med regler av

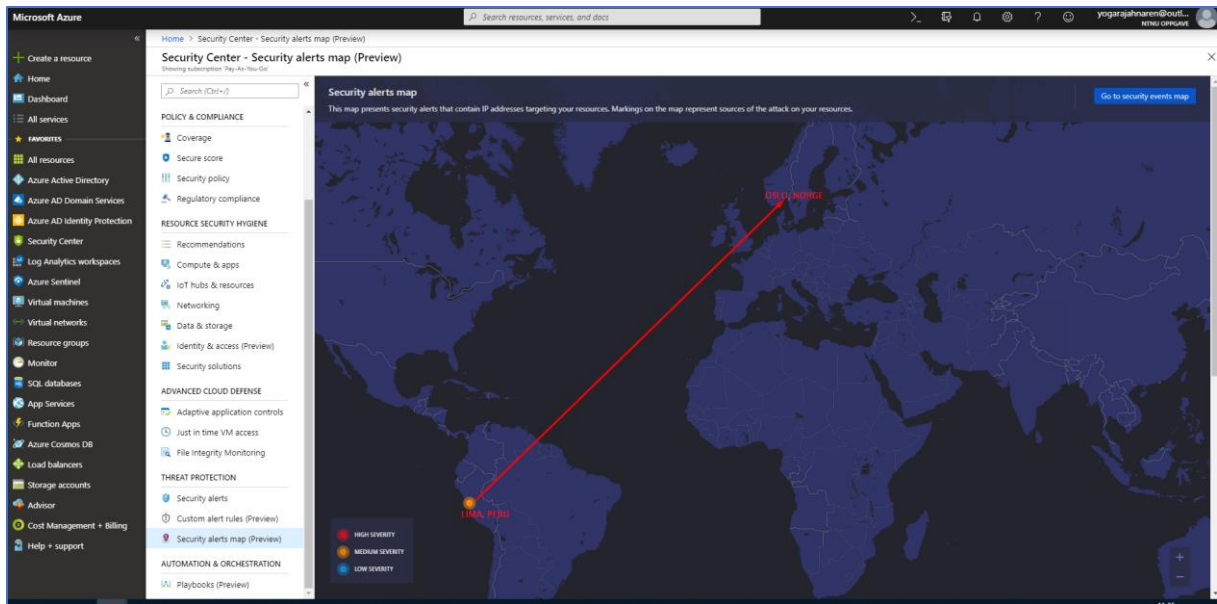
allerede forekommende angrep. Da kan man definere de aktuelle angrepene som har forekommet i Azure og vet hvilke tiltak som bør settes i gang umiddelbart etter gjenkjent mistenkelig aktivitet eller angrep.



9. Videre bruker jeg også Log Analytics for å etterforske hendelsen som skjedde den 20 april 2019. Jeg skriver inn en query i min Log Analytics Workspace BscOppgave:

```
SecurityAlert  
| where AlertName contains "Suspicious incoming RDP network activity"
```

Videre får jeg opp data som gir en mer detaljert informasjon om angrepet som har tatt sted. Et av de mest gunstige funksjonene som finnes i Log Analytics er Time range funksjonen. Ved å klikke på denne knappen har man mulighet til å sette en tilpasset og bestemt tidsperiode hvor man vil kjøre query innen denne tidsperioden. Da blir det også litt enklere å få ut data når man får informasjon om når angrepet/trusselen har funnet sted fra Security Center kan man basert på dette sette en tidsperiode for søk i Log Analytics. Nok en gang ser vi her at det er en sterk tilknytning til alle tjenester som kjøres i Azure og de samarbeider veldig godt.



10. Her ser vi Security Alerts Map som viser hvor de ulike angrepene kommer fra. I dette tilfelle har vi et varsel fra Lima, Peru. Dette varslet er tilknyttet mistenkelig RDP nettverksaktivitet fra tidligere. Ved å klikke på det gule punktet får du opp de samme detaljene om angrepet fra Azure Security Center fra tidligere steg. Et slikt kart vil alltid være til hjelp når man har flere ulike angreper i gang mot seg. Da er det lett å se hvor disse angrepene stammer fra og ved å gjøre dette kan man lage en slags sammenhengs kart ut i fra attributtene som kommer fra hver ulike angrep. I og med at Security Alert Map fortsatt er i Preview mode så kan det forekomme større endringer og det kan også være grunnen til at de andre varslene som har forekommet i Security Center ikke vises på kartet på foreløpig tidspunkt.

3.4.2 Log Analytics

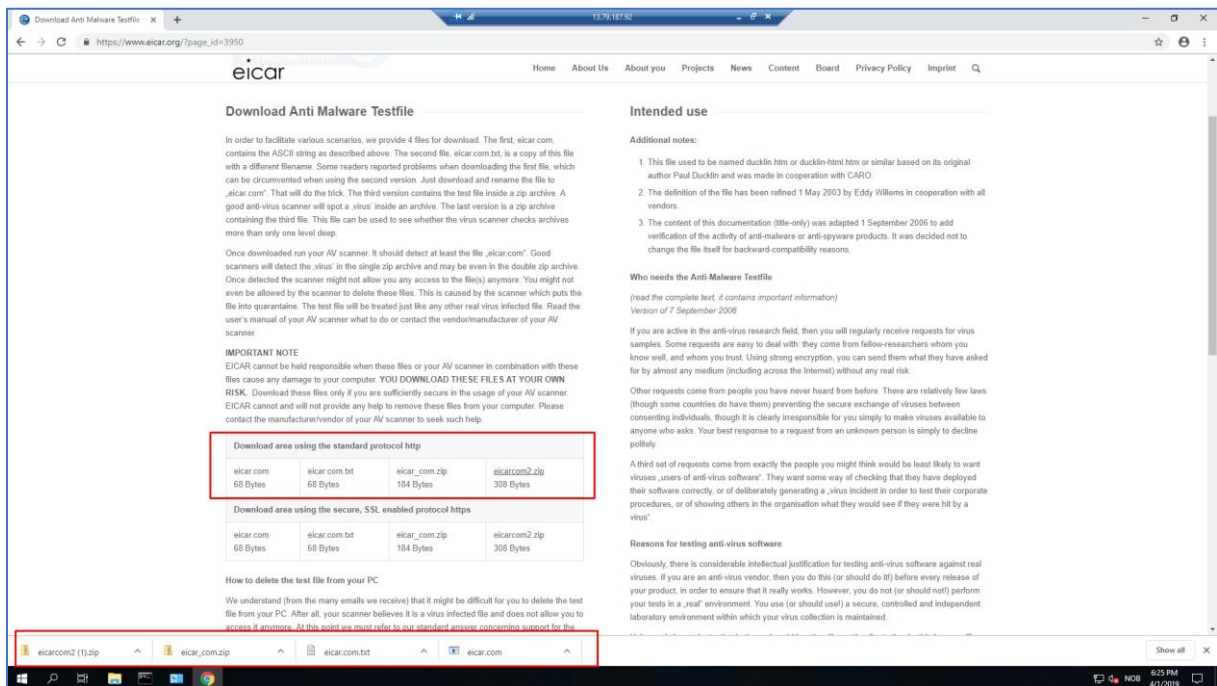
The screenshot shows the Microsoft Log Analytics workspace interface. At the top, there's a navigation bar with 'BScOppgave - Logs' and 'Log Analytics workspace'. Below that, a query editor shows a query: `SecurityAlert | where AlertName contains "Suspicious authentication activity"`. The query is highlighted with a red box. Below the query editor, there's a 'Run' button and a 'Time range: Custom' dropdown. The results section shows a table with columns: TenantId, TimeGenerated [UTC], DisplayName, AlertName, AlertSeverity, and Description. The first row of data is expanded, showing details for a 'Suspicious authentication activity' alert with a severity of 'Medium'. The description of the alert reads: 'Although none of them succeeded, some of them used accounts were recognized by the host. This resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords in order to find valid credentials. This indicates that some of your host account names might exist in a well-known account name dictionary.'

1. Jeg bruker først Security Center for å vite mer om angrepet. Deretter for å etterforske denne trusselen videre i Log Analytics tar jeg i bruk det samme varsel navnet som har forekommet i Security Center. Dermed skriver jeg en query som videre gir en detaljert informasjon om påfølgende trussel.

```
SecurityAlert
| where AlertName contains "Suspicious authentication activity"
```

3.5 Eicar Virus

3.5.1 Security Center



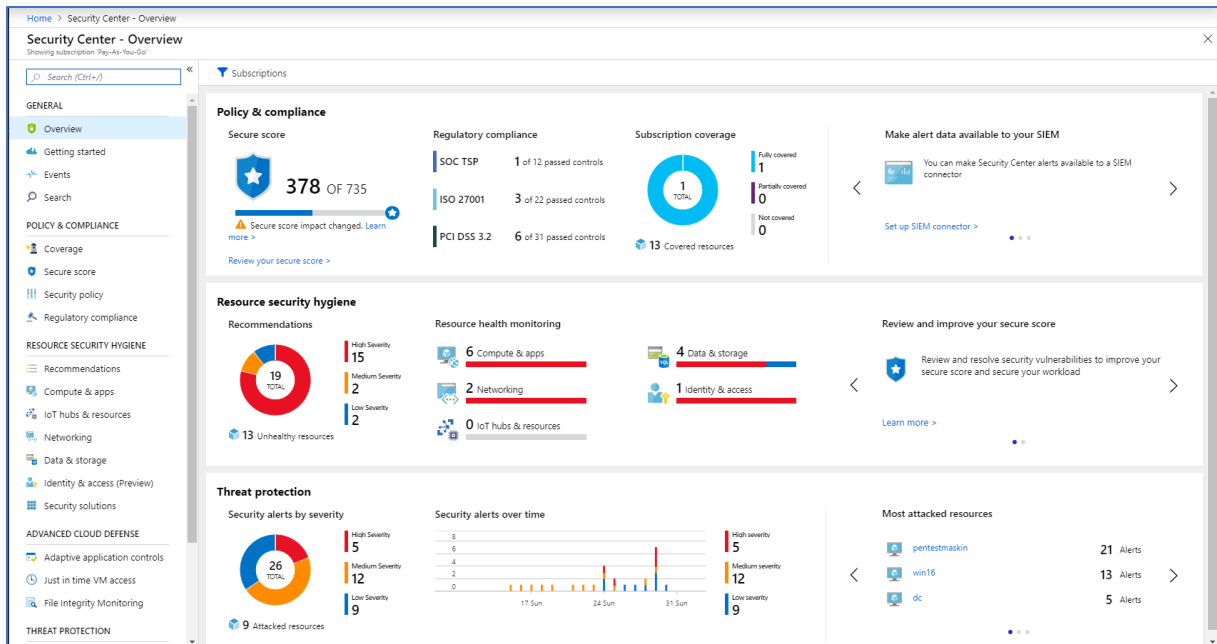
The screenshot shows the EICAR website page titled "Download Anti Malware Testfile". The page provides instructions on how to download and use the testfile. It lists four files for download: eicar.com (68 Bytes), eicar.com.bt (68 Bytes), eicar_com.zip (184 Bytes), and eicarcom2.zip (308 Bytes). The files are listed under two download areas: "Download area using the standard protocol http" and "Download area using the secure, SSL enabled protocol https". The files are also listed in the Windows taskbar at the bottom of the browser window.

Download area using the standard protocol http			
eicar.com	eicar.com.bt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

Download area using the secure, SSL enabled protocol https			
eicar.com	eicar.com.bt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

Windows taskbar files: eicarcom2 (1).zip, eicar_com.zip, eicar.com.bt, eicar.com

1. Eicar Virus er et test virus som brukes for å teste antiviruset på maskinen. Den lastes ned fra deres offisielle [hjemmeside](#). Du kan velge om du vil kjøre filen/filene eller ikke. Du kan velge å laste ned en eller flere av filene markert i første røde boks. I dette tilfelle har jeg lastet ned og prøvd å kjøre filene.



2. Så langt har det ikke vært indikasjoner på deteksjon av Eicar filen i Security Center.

Alert Type	Count	Provider	Resource	Time	Status	Severity
Suspicious authentication activity	1	Microsoft	Azure	26.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	25.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	24.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	23.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	22.03.19	Active	Medium
Suspicious authentication activity	3	Microsoft	Azure	20.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	19.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	18.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	17.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	16.03.19	Active	Medium
Security incident detected on multiple resources	1	Microsoft	Azure	25.03.19	Active	Low
Antimalware Action Taken	1	Microsoft Antimalware	Azure	02.04.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	3	Microsoft	Azure	01.04.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	5	Microsoft	Azure	31.03.19	Active	Low
Antimalware Action Taken	1	Microsoft Antimalware	Azure	30.03.19	Active	Low
Windows registry persistence method detected	1	Microsoft	Azure	30.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	3	Microsoft	Azure	30.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	2	Microsoft	Azure	29.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	4	Microsoft	Azure	28.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	5	Microsoft	Azure	27.03.19	Active	Low
Antimalware Action Taken	6	Microsoft Antimalware	Azure	25.03.19	Active	Low

3. Neste morgen etter at test viruset Eicar ble lagt inn på maskinen har det blitt oppdaget i Security Alerts i Security Center.

Home > Security Center - Overview > Security alerts > Antimalware Action Taken

Antimalware Action Taken

Filter

ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY
DC.narenbsc.local	1	05:07:46	Azure	Active	Low

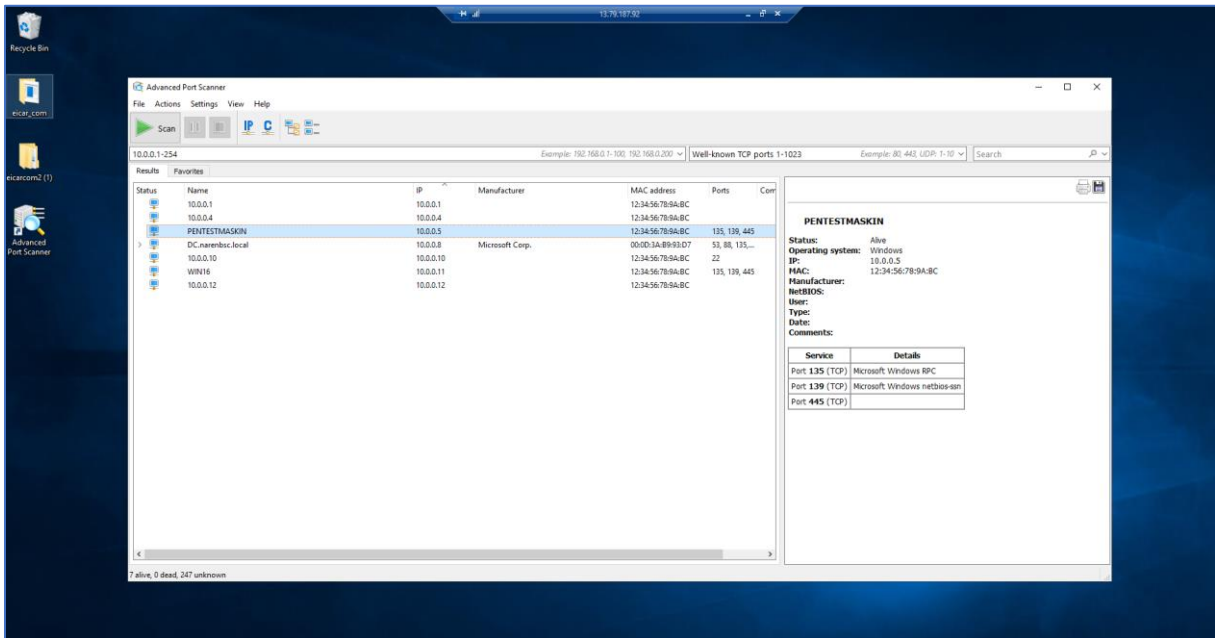
4. Her ser vi den angrepe ressursen. Dette stemmer med den virtuelle maskinen jeg testet Eicar viruset på.

DESCRIPTION	Microsoft Antimalware has taken an action to protect this machine from malware or other potentially unwanted software.
ACTIVITY TIME	tirsdag 2. april 2019, 05:07:46
SEVERITY	Low
STATE	Active
ATTACKED RESOURCE	DC.narenbsc.local
SUBSCRIPTION	Pay-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8edc02b6f)
DETECTED BY	Microsoft Antimalware
ACTION TAKEN	Blocked
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
THREAT STATUS	Quarantined
CATEGORY	Virus
THREAT ID	2147519003
FILE PATH	C:\Users\nareny\Desktop\ieicar_com.zip\ieicar.com
PROTECTION TYPE	Windows Defender
THREAT INFORMATION	Virus:DOS/EICAR_Test_File

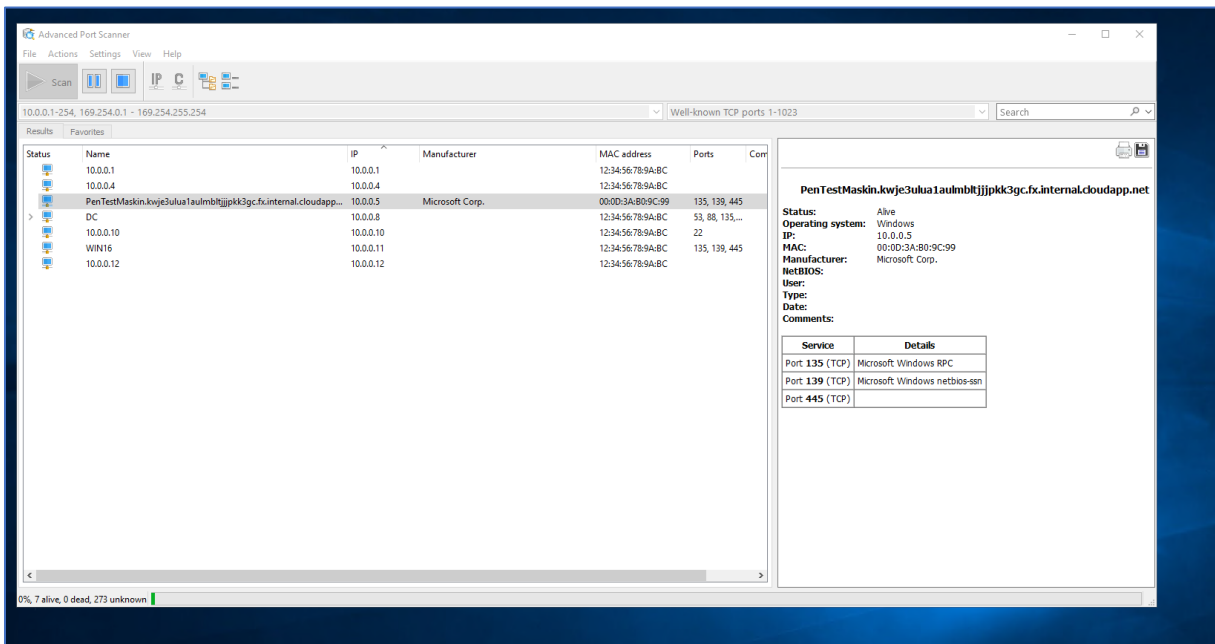
5. Videre ser vi mer detaljer om test angrepet. Vi kan også se at Microsoft Antimalware har satt i gang tiltak og blokkert filen.

3.6 Port skanning

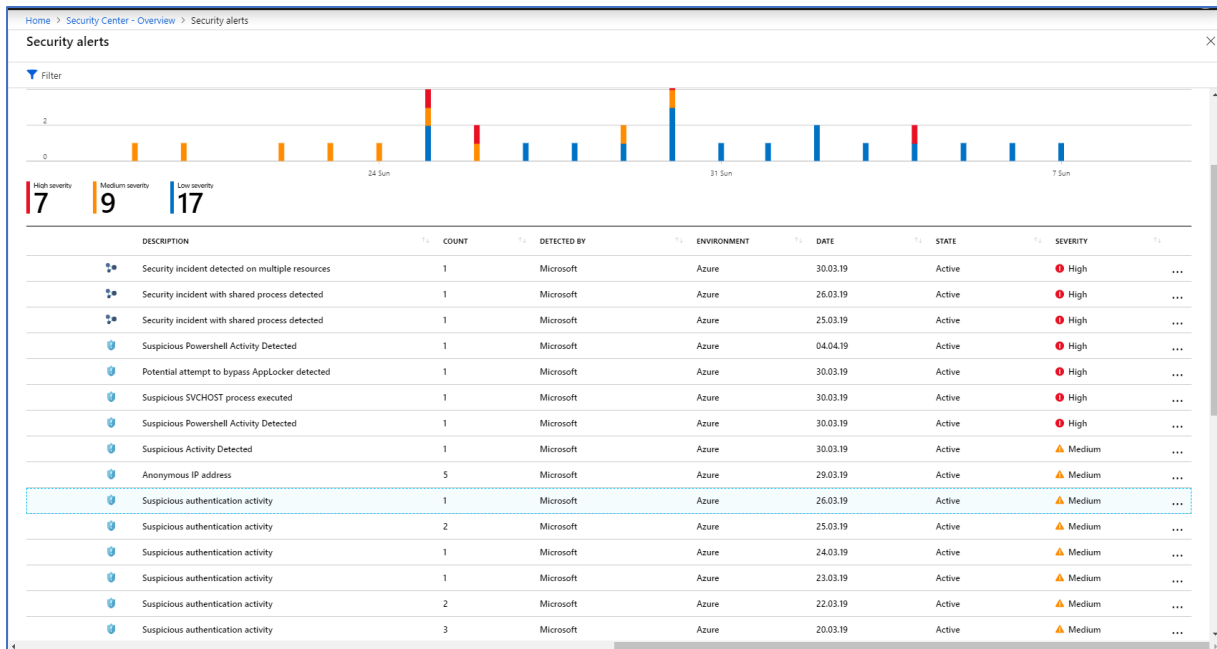
3.6.1 Security Center



1. Her kjører jeg port skanning på en virtuell maskin i Azure miljøet mitt.



2. Etter en stund får jeg opp maskiner med liste over åpne porter som kan videre utnyttes av hackere for ondsinnede hensikter.



3. Videre sjekker jeg Azure Security Center om jeg får opp noen varler tilknyttet til port skanning. Dette finner jeg ikke. Jeg prøver også å vente en lenger periode før jeg sjekker Azure Security Center. Men, her får jeg fortsatt ikke opp noen sikkerhetsvarsler tilknyttet til portskanning.

3.7 Traffic from unrecommended IP addresses was detected

3.7.1 Security Center

NEW	[Preview] Traffic from unrecommended IP addresses was detected	5	Microsoft	Azure	31.03.19	Active	Low
NEW	Antimalware Action Taken	1	Microsoft Antimalware	Azure	30.03.19	Active	Low
NEW	Windows registry persistence method detected	1	Microsoft	Azure	30.03.19	Active	Low
NEW	[Preview] Traffic from unrecommended IP addresses was detected	3	Microsoft	Azure	30.03.19	Active	Low
	[Preview] Traffic from unrecommended IP addresses was detected	2	Microsoft	Azure	29.03.19	Active	Low
	[Preview] Traffic from unrecommended IP addresses was detected	4	Microsoft	Azure	28.03.19	Active	Low
	[Preview] Traffic from unrecommended IP addresses was detected	5	Microsoft	Azure	27.03.19	Active	Low
	Antimalware Action Taken	6	Microsoft Antimalware	Azure	25.03.19	Active	Low

1. Jeg får opp en melding om trafikk som har kommet fra IP adresser som ikke anbefales å komme fra. Jeg klikker videre inn på varslet markert i rød boks.

Home > Security Center - Overview > Security alerts > [Preview] Traffic from unrecommended IP addresses was detected

[Preview] Traffic from unrecommended IP addresses was detected

Filter

ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY
win16	1	01:00:06	Azure	Active	Low
dc	1	01:00:06	Azure	Active	Low

2. Videre ser jeg at win16 og dc virtuelle maskiner er utsatt for denne hendelsen. Jeg klikker meg videre inn på dc maskinen og får opp følgende:

[Preview] Traffic from unrecommended IP addresses was detected

dc

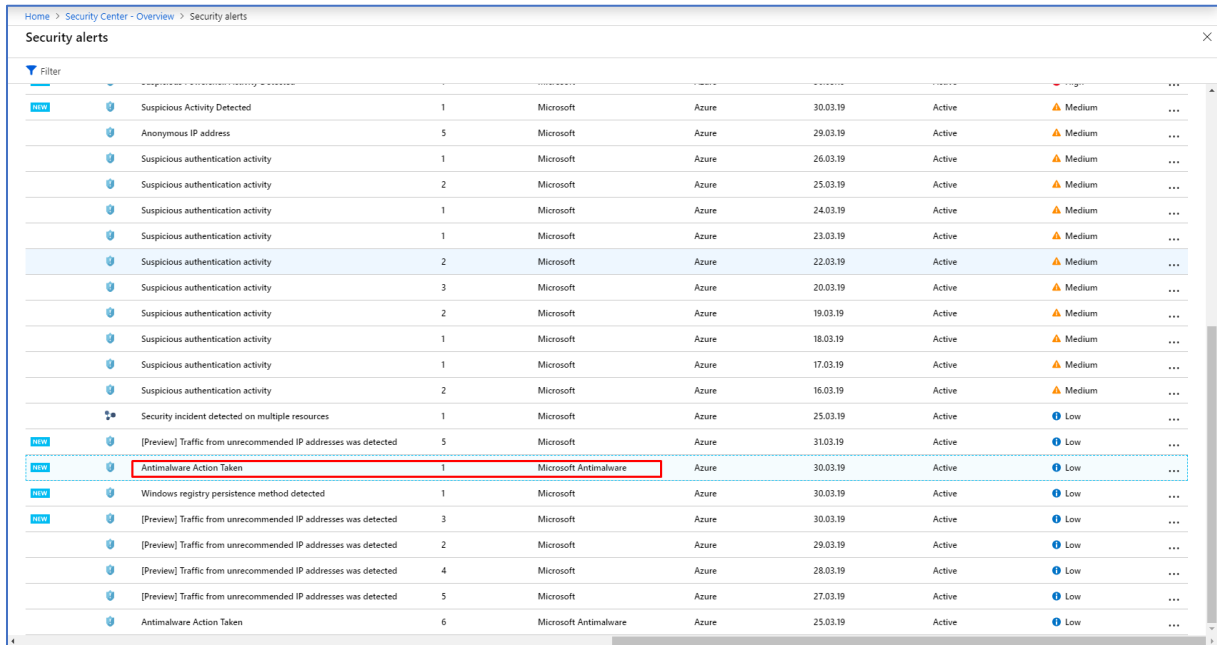
Learn more

DESCRIPTION	Azure security center has detected incoming traffic from IP addresses, which have been identified as IP addresses that should be blocked by the Adaptive Network Hardening control
ACTIVITY TIME	fredag 29. mars 2019, 01:00:06
SEVERITY	Low
STATE	Active
ATTACKED RESOURCE	dc
SUBSCRIPTION	Pay-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8edc02b6f)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
DESTINATION PORT	3389
PROTOCOL	TCP
	IP: 190.105.226.80 [1] IP: 68.67.45.66 [1] IP: 160.153.247.14 [1] IP: 192.99.137.254 [1] IP: 198.23.214.160 [1] IP: 193.188.22.2 [1] IP: 3.84.147.248 [1] IP: 23.91.74.220 [1] IP: 114.143.242.225 [1]

3. Videre ser vi at statusen på hendelsen er fortsatt aktiv og hvilke IP adresser som har prøvd å tilkoble seg på mine virtuelle maskiner.

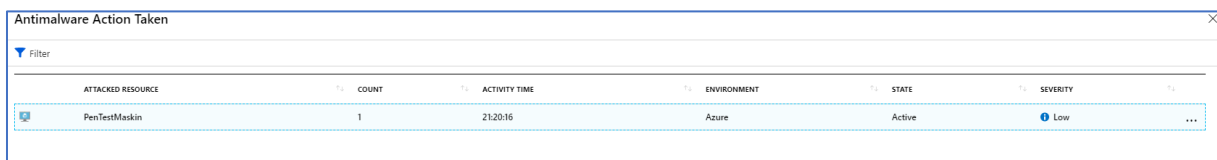
3.8 Trojan: Win32/Powrmry.A! atk

3.8.1 Security Center



Alert Name	Count	Source	Environment	Date	State	Severity
Suspicious Activity Detected	1	Microsoft	Azure	30.03.19	Active	Medium
Anonymous IP address	5	Microsoft	Azure	29.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	26.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	25.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	24.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	23.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	22.03.19	Active	Medium
Suspicious authentication activity	3	Microsoft	Azure	20.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	19.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	18.03.19	Active	Medium
Suspicious authentication activity	1	Microsoft	Azure	17.03.19	Active	Medium
Suspicious authentication activity	2	Microsoft	Azure	16.03.19	Active	Medium
Security incident detected on multiple resources	1	Microsoft	Azure	25.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	5	Microsoft	Azure	31.03.19	Active	Low
Antimalware Action Taken	1	Microsoft Antimalware	Azure	30.03.19	Active	Low
Windows registry persistence method detected	1	Microsoft	Azure	30.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	3	Microsoft	Azure	30.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	2	Microsoft	Azure	29.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	4	Microsoft	Azure	28.03.19	Active	Low
[Preview] Traffic from unrecommended IP addresses was detected	5	Microsoft	Azure	27.03.19	Active	Low
Antimalware Action Taken	6	Microsoft Antimalware	Azure	25.03.19	Active	Low

1. En annet varsel som dukker opp i Security Alerts er Antimalware varslet. Jeg klikker videre på dette varslet for å se hva det dreier seg om.



ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY
PenTestMaskin	1	21:20:16	Azure	Active	Low

2. Videre ser jeg at ressursen som er angrepet er en virtuell maskin kalt PenTestMaskin.

Antimalware Action Taken

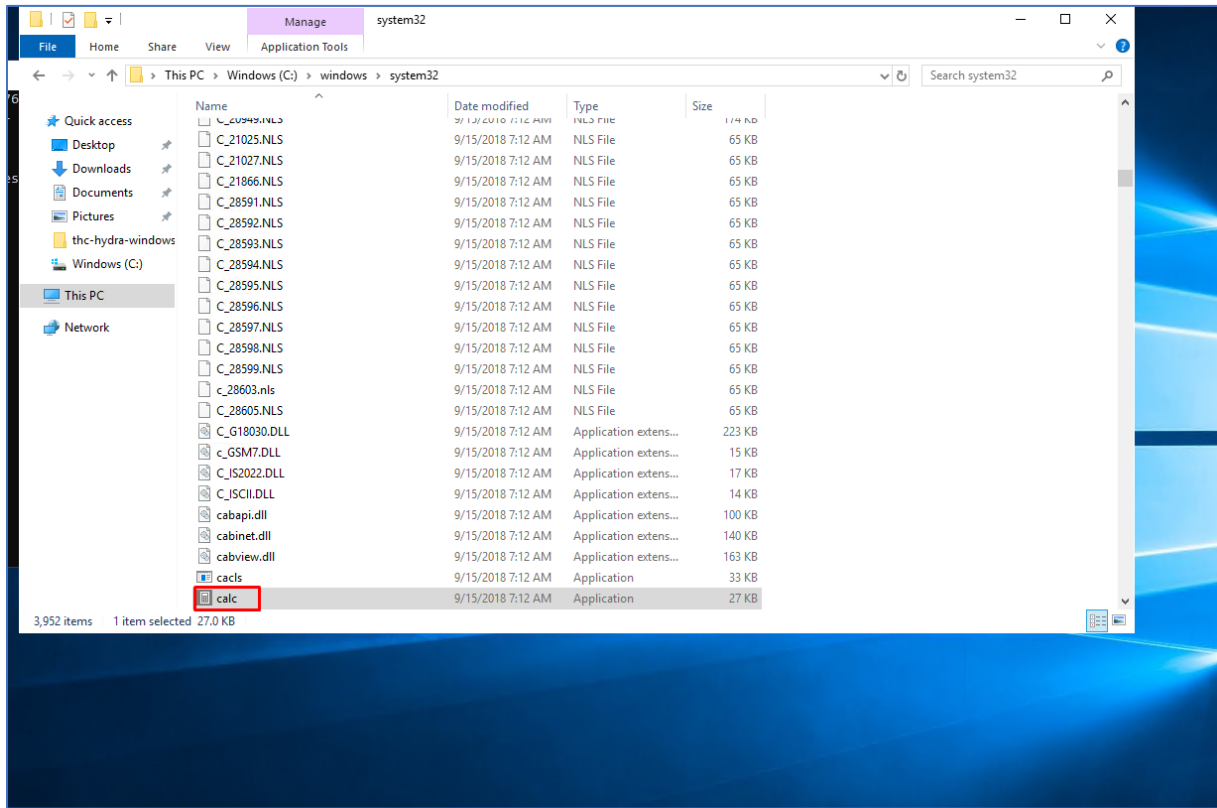
Learn more

General information

DESCRIPTION	Microsoft Antimalware has taken an action to protect this machine from malware or other potentially unwanted software.
ACTIVITY TIME	lørdag 30. mars 2019, 21:20:16
SEVERITY	Low
STATE	Active
ATTACKED RESOURCE	PenTestMaskin
SUBSCRIPTION	Pay-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8edc02b6f)
DETECTED BY	Microsoft Antimalware
ACTION TAKEN	Blocked
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
THREAT STATUS	Remediated
CATEGORY	Trojan
THREAT ID	2147725438
PROTECTION TYPE	Windows Defender
THREAT INFORMATION	Trojan:Win32/Powemet.Alattk

3. Jeg dobbeltklikker videre på maskinen og får melding om at Microsoft Antimalware har satt i gang tiltak for å beskytte maskinen fra ondsinnede programvare. Vi kan også se at det står blokkert under «action taken». Da betyr det at Antimalware blokkert det ondsinnede programmet som er kategorisert til å være en Trojan type.

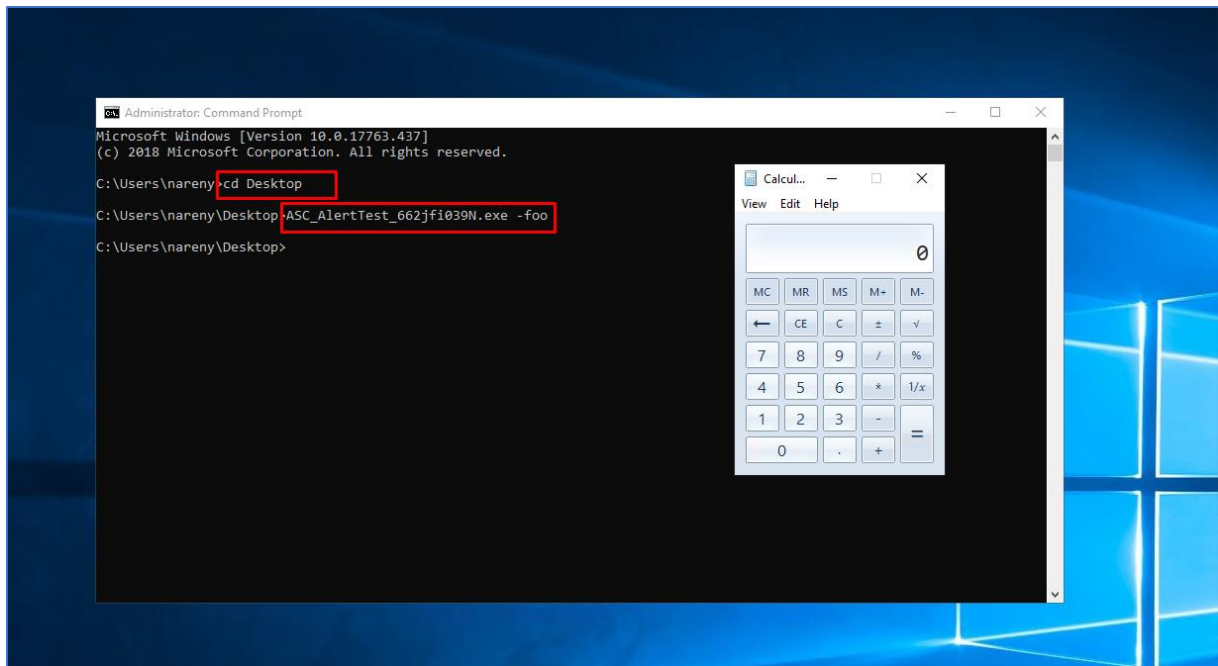
3.9 Alert validation



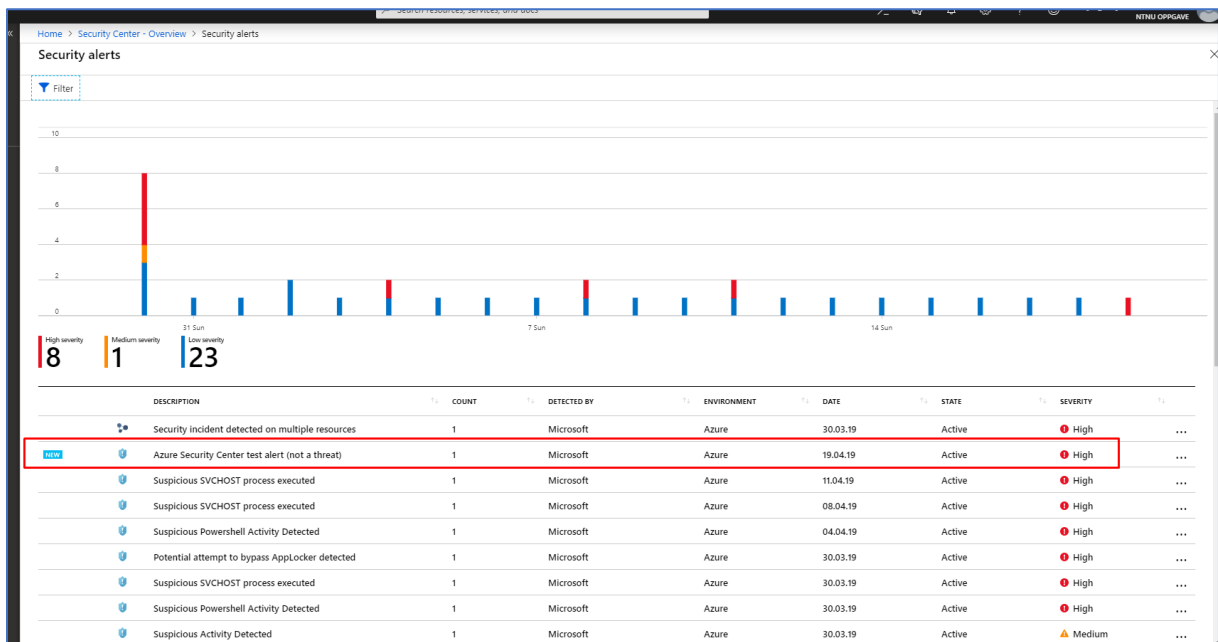
1. Nå skal jeg sette opp en alert validation og sjekke om varslet forekommer i Azure Security Center. Jeg kopierer calc.exe filen fra C:/windows/system32 til desktop.



2. Deretter endrer jeg navnet calc.exe til ASC_AlertTest_662jfi039N.exe.



3. Videre navigerer jeg meg til CMD. Jeg navigerer meg frem til Desktop stien min. Deretter skriver jeg inn kommandoen `ASC_AlertTest_662jfi039N.exe -foo` som er et falskt argument navn. Etter å ha kjørt kommandoen får man opp kalkulator programmet. Videre venter jeg 5-10 minutter før jeg starter opp Security Center. Da får jeg opp følgende:



Home > Security Center > Overview > Security alerts > Azure Security Center test alert (not a threat)

Azure Security Center test alert (not a threat)

Filter

ATTACKED RESOURCE	COUNT	ACTIVITY TIME	ENVIRONMENT	STATE	SEVERITY	
PENTESTMASKIN	1	19.04.19, 10:22	Azure	Active	High	...
PENTESTMASKIN	1	19.04.19, 10:21	Azure	Active	High	...
PENTESTMASKIN	1	19.04.19, 10:21	Azure	Active	High	...
PENTESTMASKIN	1	19.04.19, 10:13	Azure	Active	High	...

Home > Security Center > Overview > Security alerts > Azure Security Center test alert (not a threat) > Azure Security Center test alert (not a threat)

Azure Security Center test alert (not a threat)

PENTESTMASKIN

Learn more

DESCRIPTION	This is a test alert generated by Azure Security Center. No further action is needed.
ACTIVITY TIME	fredag 19. april 2019, 10:22:29
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	PENTESTMASKIN
SUBSCRIPTION	Pay-As-You-Go (3f6b0f35-d667-4770-ac0f-4bc8edc02b6f)
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
COMPROMISED HOST	PENTESTMASKIN
USER NAME	PENTESTMASKIN\ntareny
ACCOUNT SESSION ID	0xf6beb
SUSPICIOUS PROCESS	c:\users\ntareny\desktop\asc_alerttest_662jfi039n.exe.exe
SUSPICIOUS COMMAND LINE	asc_alerttest_662jfi039n.exe -foo
PARENT PROCESS	c:\windows\system32\cmd.exe
SUSPICIOUS PROCESS ID	0x1424

Was this useful? Yes No

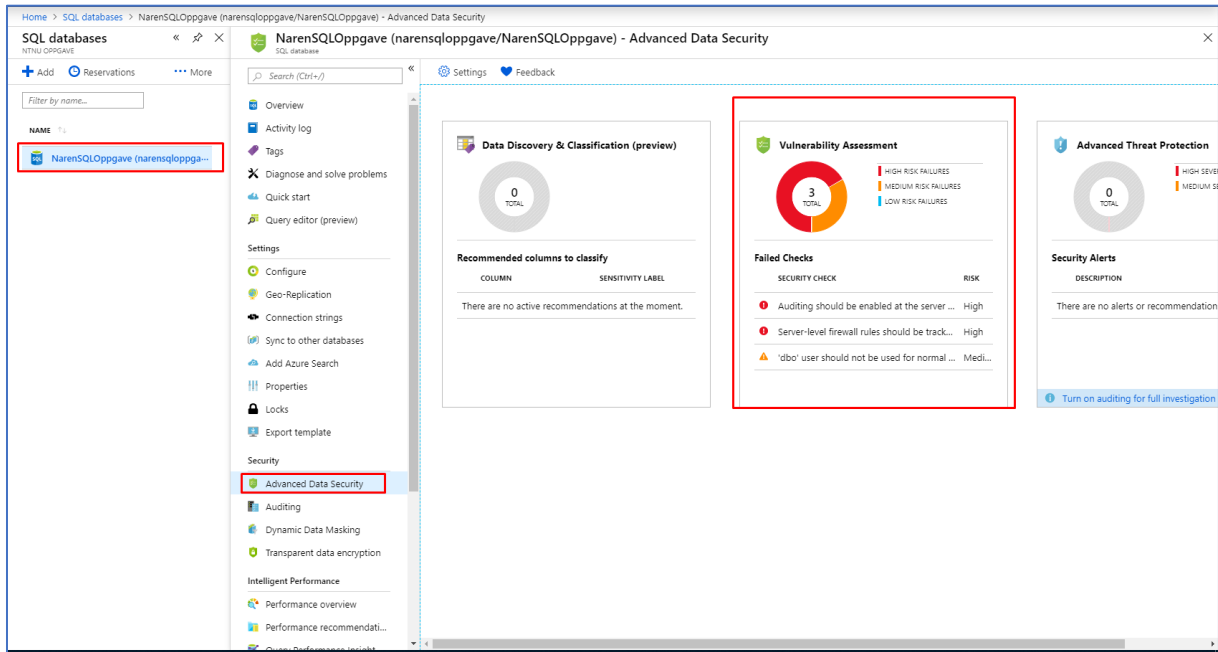
Investigation not available Playbooks not available

4. Jeg får opp et varsel i Security Center som sier «Azure Security Center test alert (not a threat).

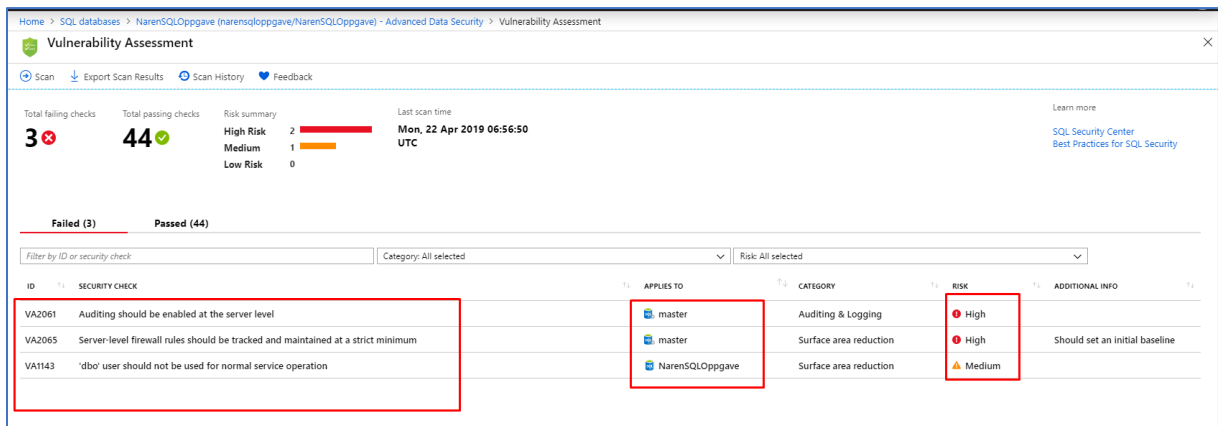
5. Deretter klikker jeg meg inn på dette varslet og da ser jeg at PENTESTMASKIN har blitt utsatt for dette varslet/testingen. Videre klikker jeg på den øverste PENTESTMASKIN.

6. Da får jeg informasjonen om at dette kun er en test som er generert av Azure Security Center. Det trengs her i dette tilfelle, ikke å sette i gang noen form for tiltak for å fjerne dette.

4.0 SQL Database Vulnerability Assessment



1. SQL Databaser har også en innebygd Security feature som kalles for SQL Database Vulnerability Assessment. Dette verktøyet finner man under Advanced Data Security under Security menyen til SQL databases.



2. Når man klikker på Vulnerability Assessment verktøyet får man en oversikt over sårbarheter som er i SQL databasesystemet. I dette tilfellet har vi to sårbarheter knyttet til master Branch SQL database. Den siste er knyttet til NarenSQLOppgave databasesystemet som jeg opprettet for prosjektet. Dersom vi klikker på sårbarheten som er knyttet til min database får vi opp følgende informasjon.

Home > SQL databases > NarenSQLOppgave (narensqloppgave/NarenSQLOppgave) - Advanced Data Security > Vulnerability Assessment > VA1143 - 'dbo' user should not be used for normal service operation

Approve as Baseline Clear Baseline

name: VA1143 - 'dbo' user should not be used for normal service operation

risk: Medium

status: FAIL

Applies To: NarenSQLOppgave

description: The 'dbo', or database owner, is a user account that has implied permissions to perform all activities in the database. Members of the sysadmin fixed server role are automatically mapped to dbo. This rule checks that dbo is not the only account allowed to access this database. Please note that on a newly created clean database this rule will fail until additional roles are created.

impact: A compromised service that accesses the database with the 'dbo' user account will have full control of the database. To avoid this situation, lower privileged users should be defined for normal service operation, while the 'dbo' account should only be used for administrative tasks that require this privilege.

BENCHMARK REFERENCES:

- FedRAMP

RULE QUERY:

```
IF([SELECT count(*) from sys.database_principals WHERE principal_id >= 5 AND principal_id < 16384 ] > 0) SELECT 0 AS Violation
ELSE SELECT 1 AS Violation
```

MICROSOFT RECOMMENDATION: True

BASELINE: Not set

ACTUAL RESULT: False

REMEDIATION: Create users with low privileges to access the DB and any data stored in it with the appropriate set of permissions.

3. Jeg får opp informasjon om at dbo bruker ikke bør brukes for normal service operation. Dette godtar jeg og klikker på «Approve as Baseline».

Home > SQL databases > NarenSQLOppgave (narensqloppgave/NarenSQLOppgave) - Advanced Data Security > Vulnerability Assessment > VA1143 - 'dbo' user should not be used for normal service operation

VA1143 - 'dbo' user should not be used for normal service operation

Approve as Baseline Clear Baseline

You are now setting the current result as your approved baseline for this security check on this database. It will no longer appear as a failure in your Vulnerability Assessment after your next scan. Do you want to continue?

4. Deretter klikker jeg på Yes.

Home > SQL databases > NarenSQLOppgave (narensqloppgave/NarenSQLOppgave) - Advanced Data Security > Vulnerability Assessment

Vulnerability Assessment

Scan | Export Scan Results | Scan History | Feedback

Executing Vulnerability Assessment scan...

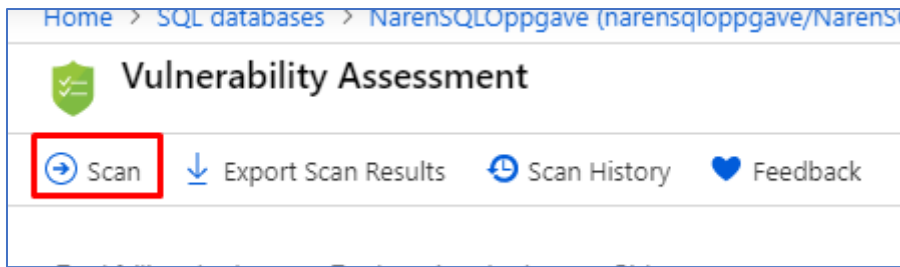
Total failing checks: **3** Total passing checks: **44**

Risk summary: High Risk: 2, Medium: 1, Low Risk: 0

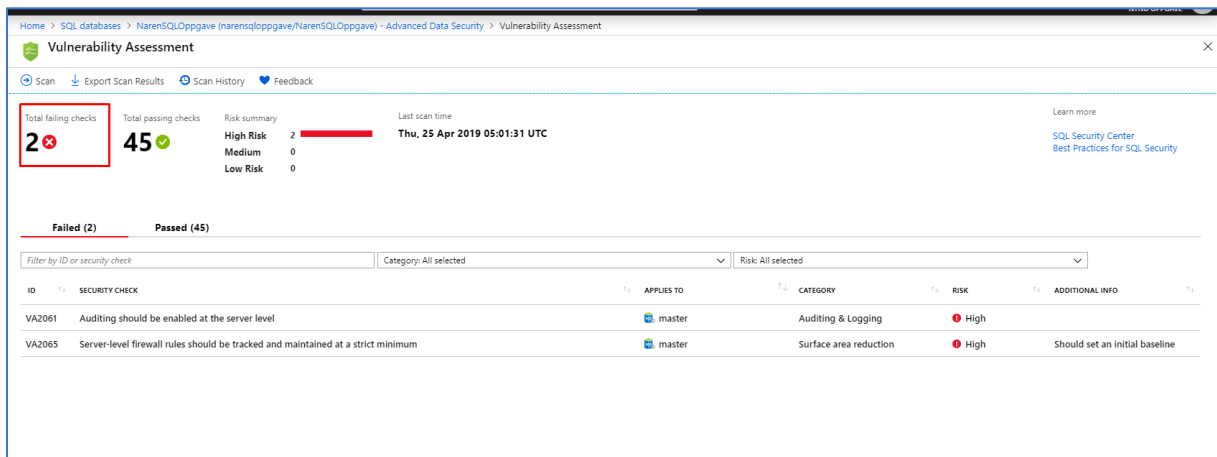
Last scan time: Mon, 22 Apr 2019 06:56:50 UTC

Failed (3) | Passed (44)

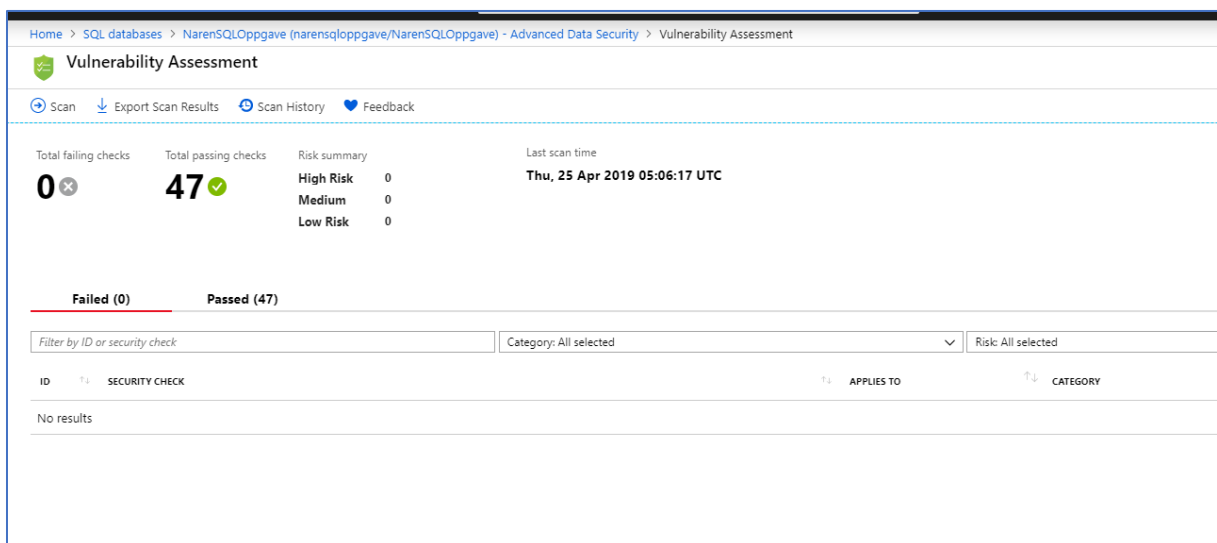
ID	SECURITY CHECK	APPLIES TO	CATEGORY	RISK	ADDITIONAL INFO
VA2061	Auditing should be enabled at the server level	master	Auditing & Logging	High	
VA2065	Server-level firewall rules should be tracked and maintained at a strict minimum	master	Surface area reduction	High	Should set an initial baseline
VA1143	'dbo' user should not be used for normal service operation	NarenSQLOppgave	Surface area reduction	Medium	



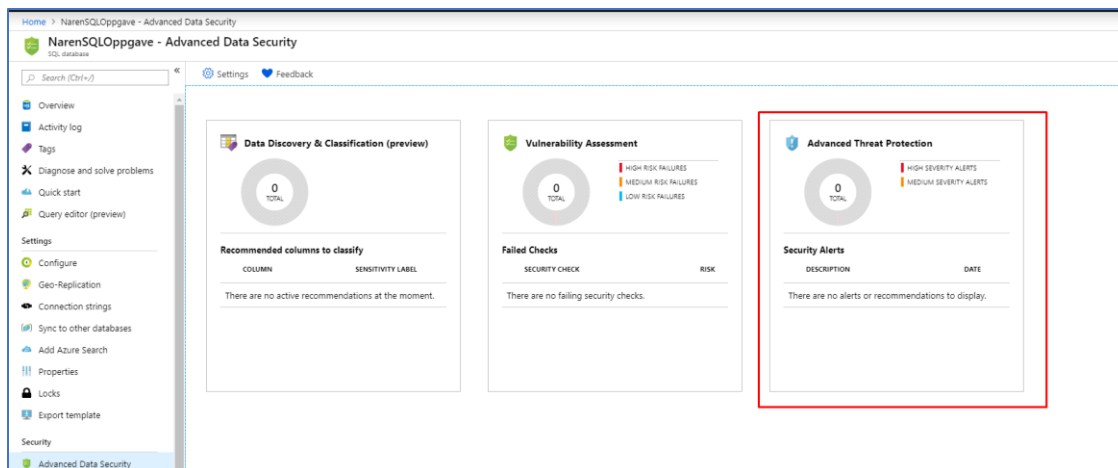
5. Videre kjører jeg en ny Scan i Vulnerability Assessment ved å klikke på Scan knappen.



6. Etter en liten stund får jeg opp resultatet. Da ser jeg at sårbarheten knyttet til min bruker er fjernet i Vulnerability Assessment. Samme metode brukes for å bli kvitt de andre to sårbarhetene som vises.



7. Da får vi dette resultatet. Når er databasene clean får sårbarheter.



8. Så langt ser jeg også at det ikke er oppdaget trusler under Advanced Threat Protection knyttet til SQL Databasene.

5. Kilder

- [1] Prakash, Ajeeth. «How Security Center and Log Analytics Can Be Used for Threat Hunting.» *Blog | Microsoft Azure*, 12 Sept. 2018, <https://azure.microsoft.com/nb-no/blog/ways-to-use-azure-security-center-log-analytics-for-threat-hunting/>.
- [2] Prakash, Ajeeth. «How Security Center Helps Analyze Attacks Using Investigation and Log Search.» *Blog | Microsoft Azure*, 16 Jan. 2018, <https://azure.microsoft.com/nb-no/blog/how-azure-security-center-helps-analyze-attacks-using-investigation-and-log-search/>.
- [3] Microsoft. «Azure Active Directory Domain Services: Enable Password Hash Synchronization.» *Azure Active Directory Domain Services: Enable Password Hash Synchronization | Microsoft Docs*, 04 Feb. 2018, <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-getting-started-password-sync>.
- [4] Brezicky, Mark. «Azure ATP Basic Deployment.» *Azure ATP Basic Deployment*, 4 May 2018, <https://blog.enablingtechcorp.com/azure-atp-basic-deployment>
- [5] Lamppu, Sami. «Use Azure Sentinel to Investigate Security Alerts.» *Sam's Corner*, 5 Mar. 2019, <https://samilamppu.com/2019/03/05/use-azure-sentinel-to-investigate-security-alerts/>.
- [6] Lamppu, Sami. «Azure AD Identity Protection in Action.» *Sam's Corner*, 10 Oct. 2016, <https://samilamppu.com/2016/10/10/azure-ad-identity-protection-in-action/>
- [7] Microsoft. «Security.» *Blog | Microsoft Azure*, <https://azure.microsoft.com/en-us/blog/topics/security/>.
- [8] Microsoft. «Azure/Azure-Sentinel.» GitHub, 15 april. 2019, <https://github.com/Azure/Azure-Sentinel>
- [9] Microsoft. «Alerts Validation in Azure Security Center.» *Microsoft Docs*, <https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>
- [10] Microsoft. «Threat Detection – Azure SQL Data Warehouse.» *Threat detection – Azure SQL Data Warehouse | Microsoft Docs*, 17 april, 2018. Lokalisert 25

april, 2019 fra <https://docs.microsoft.com/en-us/azure/sql-data-warehouse/sql-data-warehouse-security-threat-detection>

Sluttrapport

Innholdsfortegnelse

1.Oppgavebeskrivelse	281
2. Hvordan ble oppgaven løst?	281
2.1 Litteratur og Internett.....	281
2.2 Oversikt over maskinvare	281
2.3 Standard Programvare	282
2.4 Arbeidsfordeling	282
3. Gjennomføring av prosjektet.....	283
4. Videre arbeid	285

1. Oppgavebeskrivelse

Bachelorprosjektet jeg har tatt for meg handler om sikkerhet i Azure. Mer spesifikt jobbes oppgaven under en arbeidshypotese som går ut på følgende: «Hvilke muligheter finnes det for trussel deteksjon i Azure ved bruk av tjenester som Azure Active Directory, Azure Log Analytics og Azure Security Center.

Dette prosjektet har hovedsakelig ikke dreid seg om hverken å lage et programsystem eller drifte et system som det har vært i tidligere studieløp. Denne oppgaven handler om å bli kjent med og forstå hvilke funksjoner som finnes i Azure som kan brukes for å gjenkjenne, overvåke og redusere trusler i Azure miljøet. Oppdragsgivere for dette bachelorprosjektet har i hovedsak vært et samarbeid mellom DNB og NTNU. DNBs Cyber Defense Center er hovedoppgave stillere. Fra DNB har vi Roger Schage Storløkken som er Expert Lead på Security Incident Response og Lars Arne som er Expert Lead på Security Incident Detection som har fungert som veiledere for studenten under hele prosjektet. Fra NTNU har vi Stein Meisingseth som har fungert som akademisk veileder for studenten.

2. Hvordan ble oppgaven løst?

2.1 Litteratur og Internett

I dette prosjektet har jeg tatt i bruk faglitteratur bøker, YouTube videoer og google som kilder for å lære mer om Azure. Stort til hjelp har vært gode fagbøker som er veldig til hjelp for å forstå grunnleggende og dypere teoretisk anvendelse av Azure og hvordan deres sikkerhetskomponenter fungerer. Ikke minst må jeg si at Microsoft Docs, altså Microsoft sin dokumentasjon også har vært veldig til hjelp for å forstå sikkerhetsarkitekturen til Azure.

2.2 Oversikt over maskinvare

Maskinvare som er tatt i bruk under prosjektet er følgende:

- Microsoft Azure
- Privateid stasjonær datamaskin
- Privateid stasjonær laptop

2.3 Standard Programvare

Standard programvare som er tatt i bruk i dette prosjektet er:

- Google Chrome
- Office 365
- Windows Server 2012 Datacenter
- Windows Server 2016
- Windows Server 2019
- Windows 10 Pro
- Ubuntu 18.04
- Outlook

2.4 Arbeidsfordeling

Jeg har valgt å jobbe individuelt med dette bachelorprosjektet. Når man jobber alene med et så stort bachelorprosjekt krever det å ha god struktur og disiplin under hele perioden med arbeidet med prosjektet. Jeg har greid å utvikle en god framdriftsplan som har vært nøkkelen til at jeg har greid å ha en god oversikt og plan om når jeg skal utarbeide og blir ferdig med ulike faser av prosjektet. I den anledning har jeg også greid å nå fristene mine som er blitt satt som «last deadline». Det har vært tøffe 5 måneder med hardt arbeid hvor jeg har hatt både oppturer og nedturer. Når jeg sto fast i noen tilfeller, spesielt på starten av prosjektet da man har en hel haug med informasjon man må sette seg inn i prøvde jeg ofte å dele opp arbeidet i flere faser slik at jeg fikk både en god og grundig forståelse og tid for arbeidet jeg skulle gjøre. Når man ofte jobber individuelt er det veldig mye man selv har ansvar for og da kan det også være litt krevende og stressende, men dette synes jeg har håndtert utmerket under hele prosjektet.

2.5 Oversikt over dokumentasjon utarbeidet i prosjektet

Dokumentasjon som er utarbeidet i prosjektet er følgende:

- Framdriftsplan
- Forstudierapport
- Systemkravrapport
- Driftsdokument
- Sluttrapport
- Timeliste med statusrapporter
- Prosjekthåndbok
- Individuelt refleksjonsnotat

3. Gjennomføring av prosjektet

Jeg kan konkludere med at jeg har i løpet av de siste 5 månedene lært veldig mye om Azure og sikkerhetsperspektivet som finnes i Azure. Jeg har greid å følge framdriftsplanen som var satt opp tidlig i startfasen av dette prosjektet. Jeg har gått frem for å lære Azure noe som var veldig nytt for meg i januar, men gjennom timevis lesing av dokumentasjon og opplæring gjennom video tutorials har jeg greid å nå det målet jeg har satt i starten av prosjektet. Ikke minst, har jeg greid å nå arbeidshypotesen jeg har satt opp for hele prosjektet, og veldig mye god informasjon er inkludert i prosjektet. I tillegg til dette har jeg også fått en god forståelse av hvordan DNB arbeider med sin IT sikkerhet i et større finanskonsern som dette. Digital samhandling har vært en stor del av dette prosjektet, bruk av verktøy som Outlook, Skype for Business og Office 365 har vært sentralt under hele perioden av bachelorprosjektet. Jeg har lært veldig mye og tatt med meg gode og nyttige tips. Dette er meget nyttig i og med at store deler av arbeidslivet tar i bruk slike verktøy i deres bedrifter

I starten av prosjektet hadde jeg samlet veldig mye av faglitteratur for videre lesing. Her samlet jeg veldig mye informasjon i en mappe uten en struktur. Det kunne vært litt bedre med en gang å strukturere lese materialet slik at det ble videre enklere å jobbe med oppgaven. Jeg

mener at framdriftsplanen som er satt opp i dette prosjektet har blitt oppnådd.

Systemkravrapporten og driftsdokumentet sine tidsfrister for prosjektet ble skjøvet litt fremover tid da det trengtes litt mer tid for disse 2 rapportene. Målet om å lære mer om trussel deteksjons muligheter som finnes i Azure er absolutt oppnådd. Jeg har greid å finne mange gode tjenester i Azure. Jeg har greid å sette meg inn i dette stoffet, jeg har forstått og bearbeidet dette stoffet grundig de siste 5 månedene. De 2 rapportene som har krevet mest tid i hele prosjektet har vært både systemkravrapporten og driftsdokumentet. Dermed har det også blitt utdelt mer tid til disse rapportene, men de andre rapportene har blitt ferdig innen satt frist i framdriftsplanen. Når jeg startet på bachelorprosjektet mitt bestemte jeg meg at jeg skulle jobbe minst 5-6 timer hver dag med prosjektet fra start til slutt, dette har jeg klart og dette vil også garantert vises frem i prosjektet mitt.

Hvis vi tar for oss risikoanalysen som ble utført tidlig i fasen i bachelorprosjektet kan jeg si følgende:

For problemer som kommer på bakgrunn av maskinvare og dens funksjonalitet, har jeg ikke møtt på slike problemer under prosjektet. Jeg kan stolt si at jeg har vært meget flink på å ta konstant sikkerhetskopier etter at jeg har jobbet med de ulike rapportene dag for dag. Hovedsakelig har jeg alltid sendt siste utgave av dokumentene til min mail for å ha de liggende som sikkerhetskopier dersom det skjer noe feil med maskinvaren dokumentene ligger på. I tillegg har jeg også hyppig i tatt i bruk cloud for å lagre mine dokumenter her også. Hvis vi ser på det andre punktet under risikoanalysen: **Sykdom som oppstår underveis under utføring av oppdraget.** Jeg kan si at jeg har vært heldig under dette prosjektet og ikke vært syk i under utføring av prosjektet. Uansett om det hadde oppnådd sykdom underveis i bachelorprosjektet, så hadde jeg jobbet med oppgaven, siden dette er en veldig viktig oppgave og det er veldig viktig for meg at jeg oppnår en meget god karakter. **Tredje punktet i risikoanalysen går ut på at prosjektgruppen som utfører oppdraget mangler kompetanse og ressurser.** Dette har stort sett ikke vært et problem, da dette er en forskningsoppgave og jeg selv har ansvar for å ta i bruk ulike kilder for å lære mer om oppgaven som er tatt for seg. Jeg har vært god på å bruke både fagbøker, Internett og YouTube videoer for å lære mer om Azure og dens muligheter for trussel deteksjon. **Det fjerde punktet om naturkatastrofer som ødelegger datasentre** har ikke påvirket meg i det hele tatt. I den anledning er jeg heldig og har fått jobbet med oppgaven min i fred og ro.

Et godt og utfyllende systemkravrapport er et meget sentralt dokument i prosjektet som har vært veldig til hjelp for meg når jeg skulle utføre selve installasjonen i driftsdokumentet og

konfigurere tjenestene beskrevet i systemkravrapporten. Nå som jeg har utarbeidet begge disse to rapportene, synes jeg selv at jeg har greid å oppnå kravene som er satt i systemkravrapporten i driftsdokumentet med både installasjon og deteksjon. Jeg har klart å dekke de viktigste tjenestene som finnes i Azure for trussel deteksjon i mitt bachelorprosjekt.

4. Videre arbeid

I og med at dette prosjektet handler mer om trussel deteksjon, kunne jeg tenkt meg å jobbe videre i Azure med trussel deteksjon. Det kommer stadig nye tjenester i Azure for trussel deteksjon, og holde meg oppdatert på dette vil bli en utfordring som jeg er meget interessert i å ta. Jeg tenker også videre å prøve å knytte tredjeparts tjenester med Azure for både deteksjon og overvåkning for å se hvordan dette fungerer. Et godt eksempel på dette kan være tjenesten SPLUNK. Ikke minst tenker jeg å lære mer om sikkerhet innenfor IT sektoren, penetrasjonstesting og sikkerhetsanalyse er en del av dette som interesserer meg. Hvis man skal jobbe med trussel deteksjon er det også ganske viktig å ha god kunnskap om IT sikkerhet og hvilke muligheter man har innenfor denne sektoren. Samtidig vil jeg også lære mer om Azure sine andre komponenter, og hvordan man kan sammenkoble disse komponentene med bachelorprosjektets tjenester som Azure Active Directory, Azure Security Center og Azure Log Analytics. Alt har en tilknytning i Azure og denne er meget viktig å forstå, dette er noe jeg også tenker å sette meg dypere inn i på et senere tidspunkt.

