Bacheloroppgave

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

Christian Fredrik Juell

Hvordan jobbe effektivt med sikkerhetsmonitorering og hendelseshåndtering i et multitenant miljø i Azure?

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Jostein Lund
Mai 2020

NTNU
Kunnskap for en bedre verden

Christian Fredrik Juell

Hvordan jobbe effektivt med sikkerhetsmonitorering og hendelseshåndtering i et multitenant miljø i Azure?

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Jostein Lund
Mai 2020

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

NTNU
Kunnskap for en bedre verden

Sammendrag

Sopra Steria ønsket å se på mulighetene til å benytte Azure Lighthouse og Azure Sentinel for å jobbe effektivt med sikkerhetsmonitorering og hendelseshåndtering i et multitenant miljø i Azure. Det er viktig at dataintegritet og konfidensialitet opprettholdes på tvers av kunder. Målet er å ikke mikse data på tvers av kunder, og sørge for at eventuelle rapporter ikke inneholder data som ikke gjelder kunden. Prosjektet ble gjennomført som en bacheloroppgave på studiet Informatikk, drift av datasystemer. Løsningen demonstrerer hvordan man kan jobbe effektivt på tvers av kunder i Azure Sentinel, ved hjelp av Azure Lighthouse.

Abstract

Sopra Steria wanted to look at the opportunities to work efficiently with security monitoring and event management across multiple tenants in Azure, using Azure Lighthouse and Azure Sentinel. It´s important that data integrity and confidentiality are maintained across customers. The goal is not to mix data across customers and ensure that any reports do not contain data that does not apply to the customer. The project was carried out as a bachelor´s thesis as part of the study program Informatics, operations of computer systems. The solution demonstrates how to efficiently work across customers in Azure Sentinel, using Azure Lighthouse.

Forord

En spennende og lærerik prosess er over. Jeg har oppnådd økt kompetanse på et område jeg synes er svært interessant, og realisert en egenutvikling i selvstendig prosjektarbeid.

Bakgrunnen for valg av tema i denne oppgaven er ny teknologi som er svært relevant for organisasjoner som jobber med skyløsninger, og spesielt organisasjoner med mange kunder. Det har vært en interessant periode, hvor mye eksisterende kunnskap, tilegnet over de tre siste årene på studiet, har blitt kombinert med nye erfaringer og kunnskap jeg kan ta med meg videre.

Først og fremst vil jeg rette en stor takk til Sopra Steria som ga meg muligheten til å jobbe med denne oppgaven. Jeg vil også takke mine veiledere fra Sopra Steria, Pål Mathisen og Hans O. Martinsen, som har delt sin kunnskap og bidratt med veiledning og gode råd når jeg har trengt det. Jeg er imponert over engasjementet dere har vist til dette prosjektet, spesielt i denne vanskelige perioden. Jeg vil også takke min veileder fra NTNU, Jostein Lund. De gode tilbakemeldingene og støtten du har gitt meg gjennom hele prosjektet har bidratt til økt motivasjon og et bedre sluttprodukt.

Sluttrapport

Innholdsfortegnelse

1. Oppgavebeskrivelse

Oppgaven gikk ut på å utforske mulighetene for å jobbe effektivt med sikkerhetsovervåking og hendelseshåndtering på tvers av kunder i et multi-tenant miljø i Azure, ved hjelp av tjenestene Azure Lighthouse og Azure Sentinel. Hensikten var å komme frem til en løsning som vil forenkle arbeidet på tvers av kunder. Arbeidet det er snakk om er utforming av rapporter og isolering av kundedata. Målet er å unngå sammenblanding av data på tvers av kundene, og opprettholde dataintegritet- og konfidensialitet. Problemstillingen ble utarbeidet i samarbeid med oppdragsgiver, Sopra Steria, og er som følgende:

"Hvordan jobbe effektivt med sikkerhetsmonitorering og hendelseshåndtering på tvers av kunder i et multitenant miljø i Azure?"

Kontaktpersonene fra Sopra Steria var:

- Pål Mathisen, Head of Security Operations Center
- Hans O. Martinsen, Senior Engineer, Public Cloud

Jostein Lund var veileder fra NTNU.

2. Hvordan ble oppgaven løst

2.1 Metoder og standarder som ble brukt

Annet enn det som ble oppgitt i dokumentasjonen knyttet til prosjektet, har det ikke blitt brukt noen andre standarder eller metoder. Dokumentasjonen beskriver kravene til hva som skulle dokumenteres i løpet av prosjektet. Dette inkluderer blant annet hva de forskjellige rapportene skal inneholde, samt en tidsramme for når de skal være ferdigskrevet.

Alt i alt har arbeidet gått veldig bra. Jeg har jobbet konsekvent og holdt de aller fleste tidsfristene jeg satte for meg selv. Unntaket her er designrapporten, som jeg brukte lenger tid på enn jeg hadde tenkt. Jeg begynte arbeidet med driftsrapporten før designrapporten ble ferdigstilt, da dette bidro til at jeg fikk bedre forståelse for teknologiene som skulle brukes i prosjektet, ved å gjøre det praktiske arbeidet først. Dette skapte forsåvidt ingen problemer, da jeg fikk til å jobbe med begge rapportene om hverandre.

2.2 Bruk av litteratur og Internett

Til informasjonshenting har det hovedsakelig blitt brukt Internett. Dokumentasjonen til Microsoft er en av de mest brukte kildene. Alle kildene som er referert til i teksten er listet opp i referanselister i dokumentasjonen. Råd fra oppdragsgiver og veileder har også vært til stor hjelp når det kommer til hva som skal være i fokus av teori og praktisk arbeid.

2.3 Oversikt over maskinvare

- Det har blitt tatt i bruk fire Azure-tenanter. I hver av tenantene har det blitt satt opp et miljø bestående av nødvendig oppsett og konfigurasjon i Azure, som har muliggjort implementering av løsningen.
- Et testmiljø for hver tenant. Testmiljøene ligger på virtuelle Windows 10-maskiner, med oppsett:
    - Standard F2s_v2 (2 vcpus, 4GiB minne)
    - Premium SSD (127 GiB)

2.4. Standardprogrammer som ble brukt

For dokumentasjon og andre prosjektrelaterte oppgaver har jeg tatt i bruk standardprogrammene:

- Microsoft Teams – For møteinnkallinger, online-møter, samt deling av dokumenter.
- Microsoft Office Word – For dokumentasjon av rapporter.
- Microsoft Outlook – For eventuelle spørsmål utenom møtene til oppdragsgiver og veileder.
- Microsoft Excel – For timeføring.
- Microsoft Project – For planlegging av prosjektet. Inkluderer milepæler og estimert tidsbruk på de ulike aktivitetene i prosjektet.
- Draw.io – For å lage tegninger om løsningsarkitektur.

3. Gjennomføring av prosjektet

Gjennomføringen av prosjekt har gått som forventet. Jeg visste lite om teknologiene som har blitt brukt i prosjektet før prosjektstart, og regnet med å bruke mye tid i starten på informasjonshenting og planlegging. Prosjektet skulle opprinnelig starte i begynnelsen av januar, men noen uforventede komplikasjoner med bedriften jeg hadde avtalt å skrive for opprinnelig, førte til en forsinkelse på nesten fire uker. I tillegg til dette ble det bestemt at jeg skulle skrive oppgaven alene, og ikke sammen med min opprinnelige partner. Det var altså mye å ta igjen på planleggingsdelen, da jeg ikke visse nøyaktig hva oppgaven skulle omhandle, og måtte starte litt på nytt. Heldigvis kom jeg raskt i kontakt med Sopra Steria, og vi ble fort enige om temaet for prosjektet. Jeg kom raskt i gang med planleggingen og skrivingen av forstudierapporten. Her ble det definert en problemstilling og prosjektmål. Resultatmålene fra forstudierapporten reflekterer hvordan utførelsen av prosjektet har gått. Alt som ble bestemt av resultatmål har blitt gjennomført, noe jeg er meget fornøyd med. Jeg har til og med fått gjort litt mer enn jeg hadde tenkt opprinnelig.

Etter planleggingsfasen var det tid for å finne en løsning til problemstillingen. Dette innebar å finne ut hvilke teknologier som skulle bli tatt i bruk, samt hvordan jeg skulle bruke de i løsningen. Dette var en del av prosjektet som tok lenger tid enn forventet. Det var mye å sette seg inn i, og mye som skulle på plass. I tillegg var dette rundt tiden da Covid-19-alvoret begynte i Norge. Fra dette tidspunktet ble det hjemmekontor, som var ganske uvant, som for de aller fleste. Som et resultat av denne vanskelige situasjonen har jeg opplevd en del problemer med Microsoft Azure. Det var en periode jeg slet med tilgang til abonnementene mine i Azure. Microsoft hadde nemlig blokkert «free trial»-abonnement i Azure. Heldigvis hadde jeg på dette tidspunktet allerede utført det meste av det praktiske arbeidet i prosjektet, og det påvirket ikke sluttresultatet noe særlig mye. Det var kun på slutten av arbeidet med driftsrapporten, at jeg innså at jeg manglet litt dokumentasjon på noe av arbeidet. Og siden Azure hadde slettet det meste av dataen fra tidligere, måtte jeg se meg nødt til å oppgradere abonnementet for å få tilgang på nytt. Dermed fikk jeg løst problemet til slutt.

Arbeidet med prosjektet har vært jevnt. Dette kan man se på timeregnskapet. Noen perioder har vært mer produktive enn andre, men alt i alt har jeg overholdt de prosessmålene jeg har satt, ved å hele tiden sette meg midlertidige mål for å holde motivasjonen oppe, og ved å jobbe systematisk gjennom hele prosjektet. Jeg har hatt god kontakt med både oppdragsgiver og veileder fra NTNU gjennom hele prosessen. Jeg synes det er en viktig del av prosjekter generelt å holde alle interessenter oppdatert gjennom hele prosjektet. Derfor har jeg prøvd å sørge for å holde regelmessige møter med alle interessenter, helst hver andre uke eller oftere.

Med tanke på hvor lite jeg kunne om temaet og teknologiene som har blitt brukt i prosjektet, vil jeg si meg fornøyd med egen innsats og hva som har blitt oppnådd i dette prosjektet. Jeg har lært utrolig mye om selvstendig prosjektarbeid, og føler jeg har tilegnet veldig mye kompetanse på området, spesielt i forhold til hvor sent jeg kom i gang med oppgaven.

4. Videre arbeid

Siden Azure Lighthouse og Azure Sentinel er såpass nye tjenester er det flere funksjoner som enda ikke er «public available», og som fortsatt er i «preview». Det er også noen funksjoner som man ikke kan være sikker på når kommer, eller om de kommer i det hele tatt. Et eksempel på dette er opprettelse av generelle regler på tvers av kunder. Dette er enda ikke mulig, da regler og logikk bare er definert innenfor samme Azure Sentinel-arbeidsområde. Dette betyr at regler opprettet i én Azure-tenant ikke er aktuelt for andre Azure-tenanter. Det samme gjelder for automatiserte oppgaver som blir opprettet [1].

Utenom disse funksjonene, er det flere ting jeg kunne gjort videre. Eksempler på dette er å opprette egendefinerte regler for hver kunde. Jeg kunne også laget automatisert respons på sikkerhetshendelser. En av grunnene til at jeg ikke gjorde dette er som nevnt fordi mye av det man kan gjøre i Azure Sentinel ikke er mulig på tvers av Azure-tenanter enda. Forhåpentligvis vil det komme flere funksjoner i nær fremtid, som gir flere muligheter for å jobbe på tvers av kunder i Azure Sentinel.

6. Referanseliste

[1] «Designing an Azure Sentinel Solution», Internett: https://msandbu.org/designing-an-azure-sentinel-solution/ [Besøkt 19.05.2020]

Forstudierapport

Innholdsfortegnelse

1. Introduksjon – hensikten med dokumentet

Dette dokumentet er en forstudierapport utarbeidet i sammenheng med et bachelorprosjekt skrevet i samarbeid med Sopra Steria. Hensikten med forstudierapporten er å sette et rammeverk for det videre arbeidet i bachelorprosjektet. Prosjektet går ut på å finne en løsning for hvordan man kan jobbe effektiv med sikkerhetsmonitorering og hendelseshåndtering på tvers av kunder i Azure. Med utgangspunkt i forstudierapporten skal prosjektgruppen og oppdragsgiver få en samstemt oppfatning av hva dette prosjektet dreier seg om og hva som kommer til å skje fremover.

Forstudierapporten beskriver innledningsvis bakgrunnen for prosjektet og problemer og behov. Dokumentet inneholder også prosjektets mål i form av effektmål, resultatmål og prosessmål. I tillegg beskrives her prosjektets omfang, samt prosjektets milepæler og hovedaktiviteter. Det er også foretatt en interessentanalyse og kartlegging av rammebetingelser. Videre vil forstudierapporten være til hjelp med å kartlegge prosjektets utfordringer ved å se på kritiske suksessfaktorer og analyser av risikoelementer. Retningslinjer og standarder er også et kapittel i forstudierapporten. Her beskrives krav til dokumentasjon, kvalitetsgjennomganger, standarder og metoder. I kapittelet "Prosjektorganisering" dokumenteres hvem som skal gjøre arbeidet og hvem som styrer arbeidet. Til slutt oppsummeres resultatene fra arbeidet i forstudiet, som en anbefaling om hva som bør skje videre.

Elementene i forstudierapporten danner et grunnlag for å beslutte om prosjektet skal gjennomføres. Forstudierapporten er videre grunnlag for en formell avtale mellom oppdragsgiver og oppdragstaker om å gjennomføre prosjektet i henhold til mål og rammer som fremgår av forstudiet.

2. Forkortelser og definisjoner

Begrep	**Beskrivelse**
Azure-tenant	En tenant i Azure representer en organisasjon i Active Directory.
Multitenancy/multi-tenant	Med «multitenancy» deles database og programvare-applikasjonen mellom kundene. Multi-tenant refererer til et miljø med flere kunder (Azure-tenanter)
Repository	Refererer til data samlet i et bibliotek.

3. Bakgrunn for prosjektet

Dette prosjektet startes på bakgrunn av en bacheloroppgave på studiet "Informatikk, drift av datasystemer". Bacheloroppgaven utarbeides i samarbeid med Sopra Steria og er oppbygd rundt en egendefinert problemstilling som omhandler temaene "multitenancy" og sikkerhetsmonitorering og hendelseshåndtering i Azure. Oppgaven baseres på eksisterende funksjonalitet i Azure, nemlig Azure Sentinel og Azure Lighthouse.

3.1 Beskrivelse av problemer og behov

Grunnlaget for å starte prosjektet er å se på mulighetene til å benytte Azure Sentinel og Azure Lighthouse for å kunne jobbe effektivt med sikkerhetsmonitorering og hendelseshåndtering på tvers av kunder i Azure. Det har vist seg å være en utfordring å separere og isolere data i et "multi-tenant" miljø. Dette er kritisk med tanke på blant annet data som er samlet i et "repository" og ved utforming av rapporter. Målet er å ikke mikse data som ikke skal mikses, og sørge for at eventuelle rapporter ikke inneholder data som ikke gjelder kunden. Med andre ord, at ikke-autoriserte personer får tilgang til sensitiv data som ikke omhandler dem. Dette er spesielt relevant når man jobber på tvers av kunder med mye data som skal behandles. Med dette som utgangspunkt har det blitt formulert en problemstilling:

"Hvordan jobbe effektivt med sikkerhetsmonitorering og hendelseshåndtering på tvers av kunder i et multitenant miljø i Azure?"

3.2 Kort om dagens systemer og rutiner

Sopra Steria ønsker ikke å dele hvordan de jobber internt.

4. Prosjektmål

Formålet med prosjektet er å informere brukerne av dokumentet om hvordan man kan jobbe effektiv på tvers av kunder ved hjelp av ny teknologi og funksjonalitet i Azure, mer konkret, Azure Sentinel og Azure Lighthouse. Det vil bli opprettet et testmiljø, bestående av fire Azure-tenanter. Resultater fra testmiljøet skal fremstilles i en driftsrapport. I driftsrapporten skal implementering av løsningen vises i praksis. Det skal også demonstreres hvordan man kan jobbe effektivt på tvers av kunder i Azure Sentinel.

4.1 Effektmål

Effekten Sopra Steria ønsker å oppnå med dette prosjektet er å få fremstilt en løsning som viser hvordan man jobber effektivt med sikkerhetsmonitorering og hendelseshåndtering på tvers av kunder i Azure. Det er viktig for Sopra Steria at dataintegritet- og konfidensialitet opprettholdes på tvers av kunder. Derfor blir målet for Sopra Steria å finne en løsning som forenkler arbeidet med å skille data på tvers av kunder.

4.2 Resultatmål

Her beskrives hva som skal gjøres i prosjektet for å oppnå den ønskede effekten:

- Produsere forståelig og tilfredsstillende dokumentasjon.
- Gjennomføre prosjektet med en total arbeidsmengde på 500 timer +/- 5%.
- Ferdigstille og levere prosjektet innen 20.05.2020.
- Sette opp og konfigurere Azure Sentinel.
- Sette opp et testmiljø for innhenting av data til Azure Sentinel.
- Sette opp og konfigurere Azure Lighthouse.

4.3 Prosessmål

Følgende prosjektmål har blitt satt av prosjektgruppen:

- Realisere en egenutvikling i form av økt kompetanse i selvstendig prosjektarbeid.
- Oppnå et godt samarbeid med veiledere fra Sopra Steria, samt veileder fra NTNU.
- Tilegne økt kompetanse i Azure Sentinel, Azure Lighthouse og multitenancy.
- Ferdigstille forstudierapporten innen tre uker.
- Ferdigstille designrapport de to påfølgende ukene.
- Ferdigstille driftsrapport innen de påfølgende åtte ukene.
- Ferdigstille sluttrapporten uken etter.
- Oppnå karakter B eller bedre i emnet.
- Jobbe jevnt og systematisk gjennom hele prosjektet, og sette midlertidige mål, slik at arbeidsmoral og motivasjon holder seg på topp.

4.4 Prosjektets omfang

I dette prosjektet skal jeg finne en løsning som forenkler arbeidet med sikkerhetsmonitorering og hendelseshåndtering på tvers av kunder. Prosjektet skal baseres på Azure Sentinel og Azure Lighthouse, og tar for seg punkter som:

- Nødvendig oppsett og konfigurasjon i Azure.
- Nødvendig oppsett og konfigurasjon i testmiljø.
- Hvordan man kan jobbe med overvåking og hendelseshåndtering på tvers av kunder i Azure Sentinel.

Prosjektet skal ikke ta for seg:

- Personvernforordningen.
- Data i forhold til landegrenser.
- Brukeropplæring.
- Kost/nytte-analyse

4.5 Prosjektets milepæler og hovedaktiviteter

Se gantt-diagram i vedlegg.

5. Interessenter og rammebetingelser

5.1 Interessentanalyse

Interessent	Suksesskriterier	Bidrag til prosjektet
Interne		
Veileder fra NTNU	Et godt gjennomført prosjekt, som tilfredsstiller veileders krav og forventning.	Beslutninger, hjelp med flyt og veiledning.
Prosjektgruppe	Vellykkede prosjektrapporter og løsning på problemstilling.	Utførelse, ansvar.
Eksterne		
Oppdragsgiver	En tilfredsstillende løsning, som kan bidra til et nytt perspektiv rundt temaet.	Veiledning, kunnskap om problemområdet.

5.2 Rammebetingelser

Her beskrives **absolutte krav** som stilles til prosjektets gjennomføring og til resultatet og som vil ha avgjørende innflytelse på planer og valg i prosjektet.

- Prosjektet skal ferdigstilles senest 20.05.2020.
- Prosjektet skal ikke overgå 525 arbeidstimer.
- Prosjektet skal dokumenteres i form av fire rapporter:
    1. Forstudierapport
    2. Designrapport
    3. Driftsrapport
    4. Sluttrapport
- Milepæler i prosjektplanen skal godkjennes underveis av oppdragsgiver.

6. Kritiske suksessfaktorer

6.1 Suksessfaktorer

Suksessfaktor	**Beskrivelse**
Minimalt arbeidsfravær.	Da prosjektgruppen kun består av én person, vil mye arbeidsfravær ha en negativ innvirkning på prosjektets gjennomføring.
God dokumentasjon gjennom hele prosjektet.	Dette er viktig for å holde oppdragsgiver og veileder oppdatert under hele prosjektet. Det er også viktig for prosjektgruppen, da det gjør arbeidet mer oversiktlig.
Jobbe jevnt.	For å holde motivasjonen oppe, er det viktig for prosjektgruppen å jobbe jevnt med prosjektarbeidet.
Innfri rammebetingelser.	For å hindre uønskede hendelser, er det viktig at rammebetingelsene innfris.
Møte jevnlig med veiledere.	Jevnlige møter med veiledere er gunstig både for prosjektgruppen og veiledere. Dette bidrar til at alle de involverte partene i prosjektet er på samme bølgelengde.
Hjelp fra veiledere.	Hjelp fra veiledere bidrar til økt faglig kompetanse og motivasjon, dersom det er nødvendig.

6.2 Informasjonsbehov

I dette prosjektet benyttes Microsoft Teams som en kommunikasjons- og samarbeidsplattform. Her deles dokumenter og versjonshåndtering blant medlemmene i teamet, som består av prosjektgruppen, samt veiledere fra både Sopra Steria og NTNU. I tillegg benyttes Teams til å planlegge og avholde møter med prosjektgruppen og veiledere. Dette er nyttig verktøy for å gi statusoppdateringer, slik at Sopra Steria og veileder på NTNU kan se fremgangen, samt bli oppmerksomme på eventuelle endringer i prosjektet.

7. Risikoanalyse

Risikoanalysen dokumenterer forhold som kan hindre at prosjektet lykkes. Analysen skal fungere som et hjelpemiddel for:

- Å avdekke og forhindre uønskede hendelser
- Bedømme sannsynligheten for at de skal inntreffe
- Analysere hvilke konsekvenser det vil få hvis de inntreffer
- Vurdere virkemidler som kan hindre at risikofaktoren oppstår eller som kan minske konsekvensene hvis det skjer

7.1 Risikomatrise

Risiko (R) er produktet av sannsynligheten (S) for at en hendelse inntreffer og hva konsekvensene (K) er hvis det skjer. Akseptkriteriet er satt til fire som betyr at man aksepterer risikoen og ingen tiltak er nødvendig. Ved hendelser med risikoverdi mellom fem og ni vurderes eventuelle tiltak, og ved hendelser med risikoverdi over 10 bør tiltak innføres.

5 Svært stor (Daglig)	5	10	15	20	25
4 Stor (Ukentlig)	4	8	12	16	20
3 Middels (Månedlig)	3	6	9	12	15
2 Liten (Semester)	2	4	6	8	10
1 Svært liten (Årlig)	1	2	3	4	5
	1 Ikke alvorlig	2 Mindre alvorlig	3 Alvorlig	4 Kritisk	5 Meget kritisk

7.2 Uønskede hendelser

De uønskede hendelsene blir vurdert med utgangspunkt i risikomatrisen.

Nr.	Uønsket hendelse	S	K	R	Forklaring
1	Uforutsett korttidsfravær	2	2	4	Redusert produktivitet over en kortere periode, for eksempel ved sykdom.
2	Uforutsett langtidsfravær	1	4	4	Langtidssykdom eller lignende. Konsekvens er kritisk siden prosjektgruppen kun består av én person.
3	Nedsatt arbeidskapasitet	2	2	4	Mindre tid til prosjektarbeid pga. arbeid med andre obligatoriske fag.
4	Utilgjengelige veiledere	1	3	3	Dårligere innblikk i hvordan prosjektet skal gjennomføres. Fører til færre tilbakemeldinger og mer usikkerhet i prosjektgruppen.
5	Korrupte datafiler	3	5	15	Datafiler blir korrupte før innlevering. Eksempelvis: Forstudierapport, Designrapport, Driftsrapport og Sluttrapport. Data fra testmiljø blir korrupt.
6	Tap av datafiler	3	5	15	Datafiler går tapt før innlevering. Eksempelvis: Forstudierapport, Designrapport, Driftsrapport og Sluttrapport. Tap av data fra testmiljø.
7	Tilgangsproblemer i Azure	2	5	10	Ingen tilgang i Azure pga. problemer hos Microsoft.

8	Problemer med programvare/systemer/utstyr	2	4	8	Uforutsette problemer med Azure Sentinel og Azure Lighthouse, samt PC og labutstyr.
9	Manglende motivasjon	3	3	9	Manglende fremdrift iht. prosjektplanen og lavere kvalitet på dokumentasjon.
10	Problemer med å skaffe kompetanse eller ressurser i prosjektgruppen	3	3	9	Manglende fremdrift iht. prosjektplanen og redusert produktivitet.
11	Dårlig planlegging	2	4	8	For dårlig planlegging som resulterer i at målene med prosjektet ikke blir nådd.

7.3 Tiltak

Det blir utarbeidet tiltak for uønskede hendelser med risikoverdi over 4.

Nr	R	Tiltak
5	15	Benytte skytjeneste med versjonskontroll (Google Docs)
6	15	Benytte skytjeneste med versjonskontroll (Google Docs)
7	10	Kontakte Microsoft Support.
8	8	Ha en alternativ PC. Gjøre feilsøk og eventuelt kontakte Microsoft Support eller spørre andre som kan systemet bedre.
9	9	Gi beskjed til veileder. Sette opp flere milepæler i prosjektplanen for å motivere for fremgang. Sørge for å ta fri når det er behov.
10	9	Spørre veiledere i Sopra Steria eller andre som kan mer om temaet.
11	9	Bruke god tid i starten på å planlegge og sette seg inn i problemstillingen. Ha jevnlige møter med veileder og oppdatere prosjektplanen underveis.

8. Retningslinjer og standarder

I dette kapitlet skal jeg kortfattet ta med de retningslinjene og standardene som prosjektet må forholde seg til.

8.1 Krav til dokumentasjon

Dette er dokumentasjonen som skal produseres i løpet av prosjektperioden:

- Forstudierapport: Denne rapporten skal være ferdig innen 26.02.2020.
- Designrapport: Dokumenterer det prosjektgruppen har behov for av programvare for at prosjektet skal kunne gjennomføres. Denne rapporten skal være ferdig innen 11.03.2020.
- Driftsrapport: Her dokumenteres løsningen. Dokumentet beskriver test-miljøet som blir satt opp og hvordan det fungerer i praksis. Driftsrapporten skal være ferdig innen 20.05.2020.
- Sluttrapport: En oppsummerende rapport som evaluerer prosjektarbeidet.
- Prosjekthåndbok: Innleveringsfrist 20.05.2020
    - Timelister: Daglig timeføring i excel-dokument, delt i Microsoft Teams.
    - Statusrapport: Ukentlige statusrapporter som oppsummerer hvordan prosjektarbeidet har gått for hver uke.
    - Møteinnkallinger og møtereferat.
- Prosjektplanlegging: Gantt-diagram med jevnlige revisjoner.
- Innlevering i Inspera:
    - Oppgaverapporten skal leveres som ett PDF-dokument med klikkbar innholdsfortegnelse.
    - Vedlegg: Presentasjon, prosjekthåndbok, kildekode eller lignende.

8.2 Krav til kvalitetsgjennomganger

Her beskrives rutiner for kvalitetsgjennomgang, slik at prosjektgruppen, oppdragsgiver og veileder ved NTNU har samme forståelse av hvilke resultater som skal leveres gjennom prosjektet.

- Prosjektmøter med oppdragsgiver: Det er planlagt ukentlige møter med oppdragsgiver for å opprettholde jevn flyt med prosjektarbeidet.
- Veiledningsmøte med faglærer: Holde veiledningsmøter med statusoppdatering hver 2-3. uke.
- Revidering: Det er planlagt jevnlig revidering av prosjektplanen.

8.3 Krav til standarder og metoder

Her referer jeg til de konkrete standarder, metoder og verktøy som prosjektet benytter.

Dokumentmal	Tittelside Forstudierapport Designrapport Driftsrapport Sluttrapport Ukesrapport Timelister Møteinnkallinger og møtereferat
Programvare	Microsoft Teams Microsoft Project Microsoft Word Microsoft Excel Microsoft Outlook
Metode	Maler gitt av NTNU vil bli brukt til å skrive dokumentasjonen.

8.4 Endringshåndtering

Ved endringsønsker fra interessenter vil det benyttes denne fremgangsmåten for håndtering:

1. Dokumentere endringens innhold
2. Analysere konsekvensene for prosjektet
3. Beregne eventuell kost/nytte
4. Godkjennelse og aksept
5. Logge endringen
6. Justere planene
7. Informere interessentene
8. Gjennomføre endringen

9. Prosjektorganisering

I dette kapittelet beskrives de involverte partene i prosjektet, og hvordan arbeidet er fordelt mellom dem.

Rolle	**Rolleinnehaver**	**Beskrivelse**
Prosjektgruppe	Christian Fredrik Juell	Christian jobber alene på dette prosjektet, og har dermed ansvar for alt av dokumentasjon. Han har også ansvar for møteinnkallinger og statusoppdateringer i prosjektet.
Veileder/faglærer	Jostein Lund	Jostein Lund er veileder, og fungerer som kvalitetskontroll i dette prosjektet.
Oppdragsgiver	Sopra Steria	Sopra Steria er oppdragsgiver, og er veiledende når det kommer til oppgaveutforming og faglig kompetanse.

10. Anbefaling om videre arbeid

Prosjektet anbefales videreført med de rammene og planene som er lagt frem i forstudierapporten.

Forstudiet legger frem en problemstilling som er aktuell både for oppdragsgivers definerte effektmål og prosjektgruppens prosessmål. Den planlagte tidsrammen på 500 timer arbeid er også passende med prosjektets omfang. Videre er det ikke estimert noen kostnader med utførelsen av dette prosjektet. Det er på den andre siden en rekke uønskede hendelser avdekket i risikoanalysen, men med innføring av de definerte tiltakene kan prosjektet gjennomføres med lav risiko.

Designrapport

Innholdsfortegnelse

1. Introduksjon

Dokumentet er designrapporten i faget “IDRI3001 Bacheloroppgave i drift av datasystemer”. Hensikten med dokumentet er å beskrive de tekniske detaljene rundt en multi-tenant løsning for generell deteksjon og hendelseshåndtering på tvers av kunder i Azure. Rapporten går nærmere inn på hvilke produkter som kan brukes for å implementere en slik løsning. Designrapporten skal bidra til at prosjektgruppen og oppdragsgiver har de samme opplysningene om hva som skal gjennomføres. Oppdragsgiver vil her få muligheten til å vurdere løsningsdesignet, og komme med tilbakemeldinger og endringsønsker.

1.1 Avgrensning

Dokumentet behandler en løsning basert på Azure Sentinel og Azure Lighthouse, for å jobbe effektivt på tvers av kunder. En multi-tenant løsning med Azure Sentinel og Azure Lighthouse er en helt ny løsning fra Microsoft, der deler av løsningen ikke er “public available” enda. Rapporten beskriver de ulike komponentene i Azure, som gjør det mulig å jobbe med overvåking og hendelseshåndtering på tvers av alle kunder.

2. Definisjoner og forkortelser

Begrep	**Beskrivelse**
Azure AD	Azure Active Directory
AI	Artificial Intelligence (kunstig intelligens).
Azure Monitor	Azure Monitor samler inn overvåkningstelemetri fra en rekke lokale kilder og Azure-kilder. Tjenesten aggregerer og lagrer denne telemetrien i et loggdatalager som er optimalisert for kostnad og ytelse.
«Contributor»-rettigheter	Lar deg administrere alt bortsett fra å gi tilgang til ressurser.
Jupyter notebooks	En åpen kildekode-applikasjon som lar deg lage og dele dokumenter som inneholder live-kode, ligninger, visualiseringer og «narrative»-tekst.
Managed Service Providers	Et selskap som eksternt forvalter kunders IT-infrastruktur og sluttbrukersystemer, typisk under en abonnementsmodell.
Microsoft Defender ATP	Microsoft Defender Advanced Threat Protection
Onboarding	Prosessen med å komme i gang med et produkt/programvare. For eksempel: «Onboarde Azure Sentinel», betyr å komme i gang med Azure Sentinel.
Open-source	Åpen kildekode.
SaaS	Software as a Service.
SIEM	Security information and event management. Programvareprodukter og tjenester kombinerer sikkerhetsinformasjonsstyring og sikkerhetshåndtering. De gir sanntidsanalyse av sikkerhetsvarsler

	generert av applikasjoner og nettverksmaskinvare.
SOAR	Security orchestration, automation and response. Programmer som tillater en organisasjon å samle data om sikkerhetstrusler fra flere kilder og respondere på sikkerhetshendelser uten menneskelig hjelp.
Workspace	Arbeidsområde.

3. Kort om oppdragsgiver og behov

Her beskrives hvem som er oppdragsgiver og hvilke behov og krav de har til dette prosjektet.

3.1 Oppdragsgiver

Oppdragsgiver er Sopra Steria. Sopra Steria er et ledende internasjonalt konsulentselskap med en av markedets mest omfattende tjenesteporteføljer innen digitalisering. Selskapet tilbyr strategiutvikling, IT-rådgivning, infrastruktur- og systemutvikling, digitale løsninger og drift. Blant annet drifter Sopra Steria Oslo kommune og Trondheim kommune. Hovedkontoret for Sopra Sterias skandinaviske virksomhet er i Posthuset i Oslo, Norge, med ca. 1800 ansatte. Selskapet er det største it-konsulentselskapet i Norge [1].

Kontaktpersonene for dette prosjektet er Pål Mathisen (Head of Security Operations Centre) og Hans O. Martinsen (Senior Engineer, Public Cloud). De bistår med veiledning og kunnskap dersom dette trengs.

3.2 Behov

Sopra Steria ønsker å se på mulighetene for å jobbe effektivt med sikkerhetsmonitorering og hendelseshåndtering på tvers av flere kunder i et multi-tenant miljø i Azure. Løsningen må dekke følgende behov:

- Må kunne kjøre generell trusselsdeteksjon på tvers av kunder.
- Hendelseshåndtering og rapportering må kunne skje uten sammenblanding av kundedata.
- Det må være spesifikke deteksjonsregler for hver kunde.

4. Hvorfor dette valget av teknologi

Azure Sentinel og Azure Lighthouse er to helt nye teknologier fra Microsoft. Bruken av disse teknologiene vil bli mer og mer vanlig i fremtiden, og for organisasjoner som Sopra Steria vil det være lønnsomt å ha kompetanse innen dette området. Sopra Steria må kunne jobbe effektivt med hendelseshåndtering og rapportering på tvers av alle sine kunder, uten sammenblanding av kundedata. Azure Sentinel og Azure Lighthouse er to produkter som sammen bidrar til å muliggjøre dette.

Azure Lighthouse muliggjør administrasjon på tvers av Azure-tenanter for MSP-er og organisasjoner som administrerer flere kunder, fra én enkel "Azure Portal". Azure Lighthouse er integrert med Azure Sentinel, som tillater organisasjoner å administrere Azure Sentinel-arbeidsområder på tvers av sine kunder [2].

5. Beskrivelse av teknisk løsning

Azure Active Directory

Azure Active Directory er Microsofts skybaserte katalogtjeneste for identitets- og tilgangsadministrasjon. Tjenesten tilbyr godkjenning av påloggінger og administrasjon av brukere og grupper med tilganger og rettigheter. Azure Active Directory gir ansatte tilgang til eksterne og interne organisasjonsressurser. Eksempler på eksterne ressurser er Azure portal, Microsoft Office 365 og andre SaaS-applikasjoner. Interne ressurser er eksempelvis lokale og skybaserte applikasjoner, som styres gjennom rollebasert tilgangsadministrasjon, og som er eksklusive til organisasjonen [3]. Azure Active Directory kan bidra til å øke sikkerheten i organisasjoner betydelig [4].

Azure Lighthouse

Microsoft Azure Lighthouse er ny teknologi fra Microsoft som har funksjoner for administrasjon av flere kunder i skala. Azure Lighthouse tilbyr bedre synlighet, forbedret sikkerhet og IP-beskyttelse [5].

Azure Sentinel

Microsoft Azure Sentinel er en skalerbar, skybasert SIEM og SOAR løsning. Azure Sentinel gir et fugleperspektiv over hele bedriften. Med innebygd AI som raskt analyserer store datamengder, er Azure Sentinel et viktig verktøy for trusseldeteksjon og rask respons. Azure Sentinel samler data fra alle kilder, inkludert brukere, programmer, servere og enheter som kjører lokalt eller i en hvilken som helst sky [6].

Azure subscription

Azure subscription er et abonnement for å få tilgang til Azure-plattformen. Det brukes for å betale for Azure-skytjenester. Det kan tegnes flere abonnement, og de knyttes til et kredittkort [7].

Azure Tenant

En Azure Tenant representerer en organisasjon i Active Directory. Når en organisasjon tegner et kontraktsbundet abonnement hos Microsoft Azure, opprettes en «tenant» automatisk. Hver Azure-tenant er forskjellige og separat fra andre Azure-tenanter [8].

Log Analytics workspaces

Azure Monitor logger data i Log Analytics workspaces. Et «workspace» er en container som inneholder data og konfigurasjonsinformasjon. Log Analytics workspaces gir administratorer en metode for å kontrollere flyten og isolasjonen av loggdata, samt muligheten til å lage en arkitektur som adresserer de spesifikke forretningsbehovene [9].

Multi Tenant

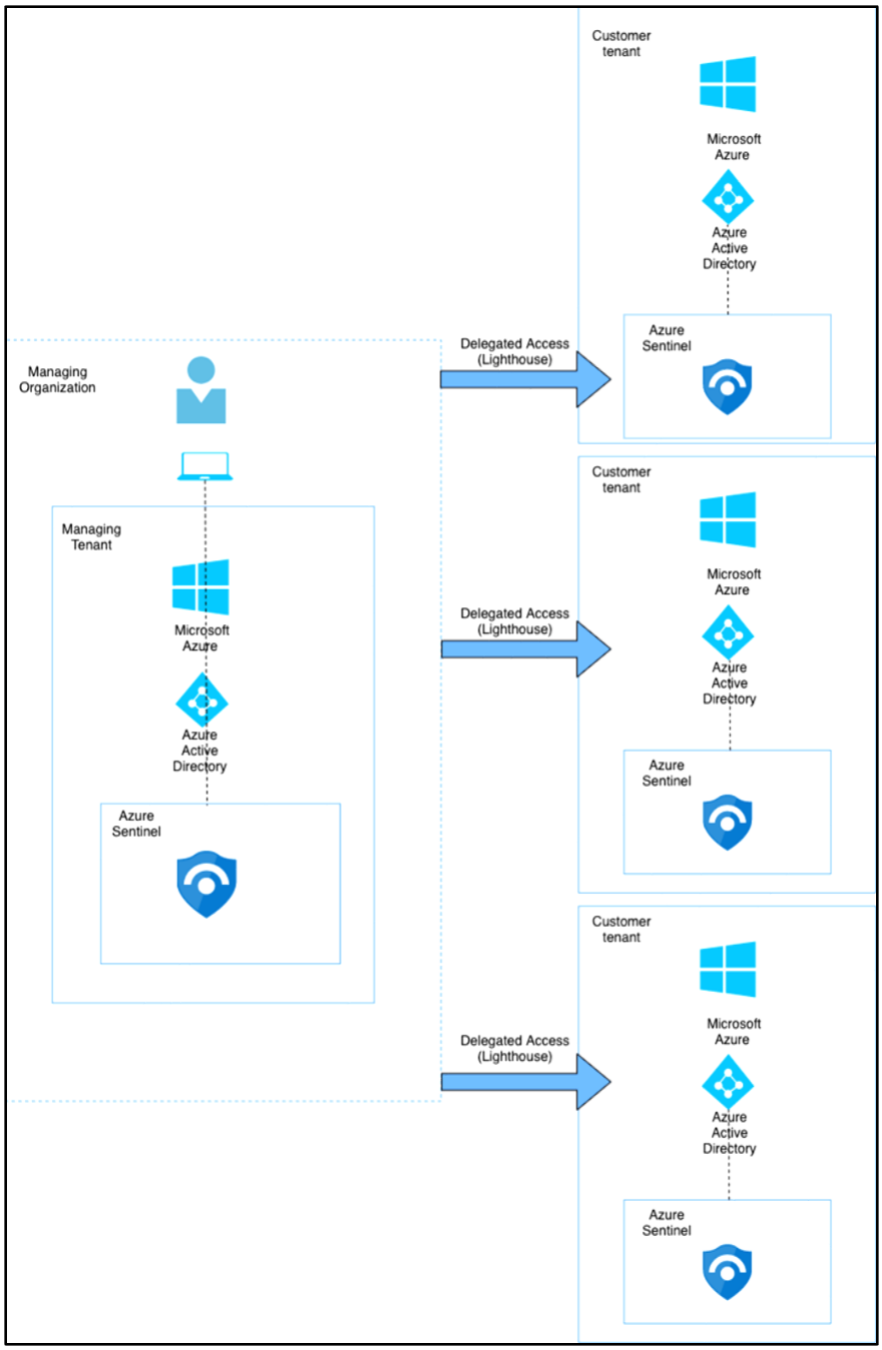
Multi Tenant kan defineres som Azure-tenanter som aksesserer andre tjenester i et delt miljø, på tvers av flere organisasjoner. Med «multi-tenancy» deles database og programvare-applikasjonen mellom kundene. Kundenes data er isolert og forblir usynlig for andre tenanter [10].

Single Tenant

Single Tenant kan defineres som Azure-tenanter som aksesserer andre tjenester i et dedikert miljø. Med «single-tenancy» har hver kunde sin egen database og forekomst av programvare [10].

6. Detaljert løsningsbeskrivelse

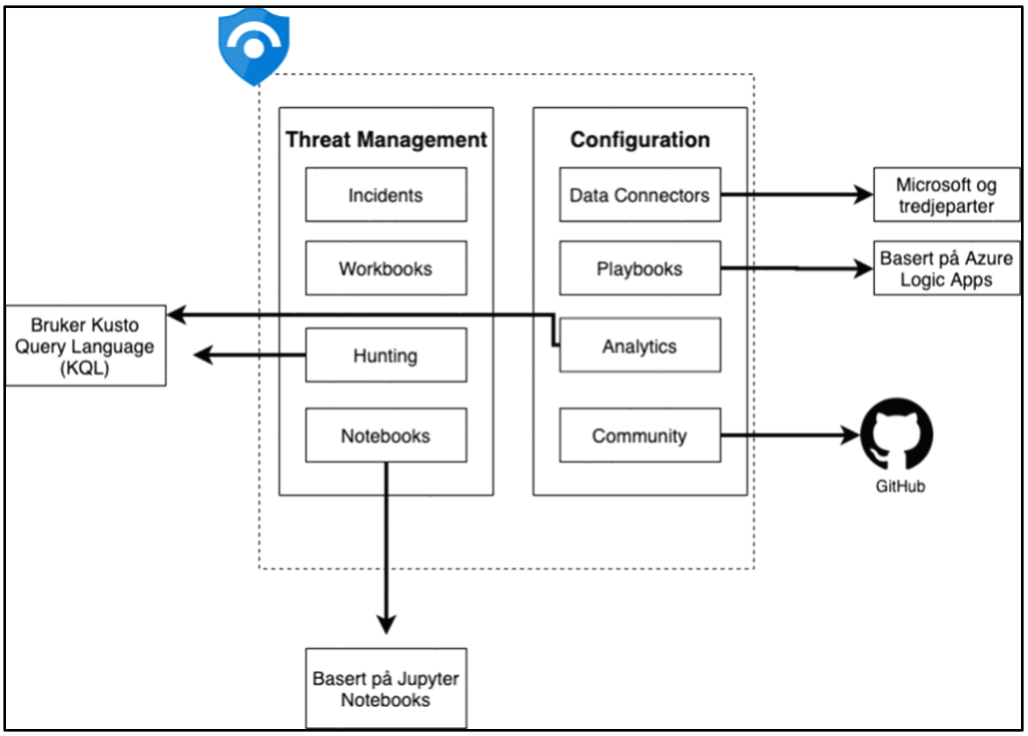
Løsningen baserer seg på et oppsett med fire Azure-tenanter, hvorav en er administrerende tenant. Denne tenanten tilhører i dette scenarioet en organisasjon som administrerer ressurser for tre kunder, som alle bruker Azure Sentinel. Abonnementene fra disse tre kundene kan bli «onboardet» til "Azure Delegated Resource Management", en av hovedkomponentene i Azure Lighthouse. Azure Delegated Resource Management tillater utpekte brukere i den administrerende tenanten å utføre administrerende oppgaver på tvers av Azure-tenanter på en sentralisert og skalerbar måte.



6.1. Azure Sentinel - Arkitektur

Siden Azure Sentinel er en del av Azure, er den første forutsetningen for å komme i gang å ha et aktivt abonnement i Azure. Videre må man opprette et Log Analytics Workspace. Det er dette som gjør det mulig for Azure Sentinel å samle data fra ulike kilder, enten det er fra ressurser i Azure eller fra enheter som kjører lokalt. Det er anbefalt å ha et dedikert "workspace" for Azure Sentinel, da alarm-regler og undersøkelser av alarmer ikke fungerer på tvers av arbeidsområder. Til slutt er det nødvendig å ha "contributor"-rettigheter for abonnementet som arbeidsområdet ligger i [11].

Figuren under viser hovedkomponentene i Azure Sentinel:



6.1.1 Data Connectors

Ved hjelp av Data Connectors kan man samle inn data fra en rekke ulike kilder. Azure Sentinel har Data Connectors for Microsoft-løsninger, som Microsoft Threat Protection, Azure AD, Office 365, Azure ATP og Microsoft Cloud Security. I tillegg finnes det innebygde "connectors" for ikke-Microsoft-løsninger [12]. I dette prosjektet skal det samles data hovedsakelig fra Microsoft Defender ATP på flere virtuelle maskiner.

Microsoft Defender Advanced Threat Protection
Microsoft Defender ATP er en sikkerhetsplattform utformet for å forhindre, oppdage, undersøke og respondere på avanserte trusler [13]. Microsoft Defender ATP oppretter alarmer når mistenkelig aktivitet blir oppdaget. For å hente alarmer og hendelser fra Microsoft Defender ATP til Azure Sentinel, kan man bruke den innebygde "connectoren" i Azure Sentinel. Dette gjør det mulig å analysere sikkerhetshendelser mer omfattende på tvers hele organisasjonen.

For å oppleve Microsoft Defender ATP i praksis kan man kjøre kontrollerte simuleringer av angrep på testmaskiner. På denne måten vil man også få generert alarmer og hendelser i Azure Sentinel, og få utforsket hvordan man kan respondere på mistenkelig aktivitet i organisasjonen.

6.1.2 Playbooks

En Playbook er en samling av prosedyrer som kan kjøres fra Azure Sentinel som respons på en alarm. Playbooks i Azure Sentinel hjelper med å automatisere og orkestrere arbeidsoppgaver- og flyt, og kan kjøres manuelt eller automatisk når spesifikke alarmer utløses. Playbooks er basert på Azure Logic Apps, noe som betyr at man får tilgang til innebygde maler fra Logic Apps [14].

6.1.3 Analytics

"Analytics" gjør det mulig å lage egendefinerte regler som søker etter spesifikke kriterier i miljøet ditt, og genererer hendelser slik at man kan undersøke nærmere hvis kriteriene passer [15]. Azure Sentinel har også innebygde maler for slike regler. Disse innebygde malene er laget av sikkerhetsteamet i Microsoft, og er basert på kjente trusler og normale angrepsvektorer. Malene søker automatisk etter mistenksom aktivitet i miljøet ditt. Mange av malene kan også tilpasses til å søke etter eller filtrere ut aktiviteter, alt etter hva det er behov for. Alarmene som genereres av disse malene vil opprette hendelser som du kan tildele og undersøke nærmere i ditt miljø [16].

6.1.4 Community

Azure Sentinel Community er et «open source»-samfunn lokalisert i GitHub for å legge til rette for samarbeid blant kunder og samarbeidspartnere. Sikkerhetsanalytikere fra Microsoft oppretter og legger stadig til nye «workbooks», «playbooks» og forskjellige spørringer for trusseloppdaging, som man kan bruke i sitt eget miljø [6].

6.1.6 Workbooks

Etter man har koblet til datakildene sine kan man visualisere og overvåke dataen gjennom Azure Sentinel Workbooks. Workbooks tilbyr fleksible visualiseringer som kan brukes for analyse av data og opprettelse av rapporter. Azure Sentinel lar deg lage spesialtilpassede "workbooks" på tvers av dataen du har hentet. Det finnes også innebygde maler, som raskt gir deg innsyn på tvers av dataen du har koblet til [6].

6.1.7 Incidents

En «incident», eller hendelse, består av en samling av relaterte alarmer som kan bli brukt for videre etterforskning [6]. Hendelser opprettes basert på regler definert i Azure Sentinel Analytics. Incidents-siden lar deg se hvor mange hendelser du har, hvor mange som er åpne, hvor mange som er pågående hendelser, samt hvor mange som er avsluttet. For hver hendelse kan du se når den ble opprettet og status for hendelsen. Du kan se på alvorlighetsgraden for å bestemme hvilken hendelse du skal håndtere først. Man kan også filtrere hvilke hendelser som vises, for eksempel etter alvorlighetsgrad eller status.

6.1.8 Hunting

"Threat hunting" er prosessen med å søke iterativt gjennom en rekke data med det formål å identifisere trusler i systemene. Azure Sentinel tilbyr en plattform for proaktiv "threat hunting", som kan hjelpe med å identifisere trusselatferd blant angripere. I Azure Sentinel kan man opprette spørringer, endre eksisterende spørringer, sette bokmerke på, kommentere og tagge interessante funn; og starte en mer detaljert undersøkelse. Azure Sentinel tilbyr innebygde spørringer som forenkler arbeidet med søking etter trusler i din eksisterende data [17].

6.1.9 Notebooks

Ved å integrere med Jupyter notebooks, utvider Azure Sentinel omfanget av hva du kan gjøre med data som har blitt samlet. Notebooks kombinerer full programmerbarhet med en enorm samling biblioteker for maskinlæring, visualisering, og dataanalyse [18].

6.2 Azure Lighthouse

Azure Lighthouse tilbyr tjenestetilbydere én enkel plattform for å se og administrere alle sine kunder med høyere automatisering, skala, og styrket styring. Med Azure Lighthouse kan tjenestetilbydere levere administrerte tjenester ved å bruke omfattende og robuste styringsverktøy som er innebygd i Azure-plattformen. Azure Lighthouse kan også være gunstig for store IT-organisasjoner som administrerer ressurser på tvers av flere Azure-tenanter [19].

6.2.1 Azure Delegated Resource Management

Azure Delegated Resource Management er en av hovedkomponentene til Azure Lighthouse. Dersom man er en tjenestetilbyder eller jobber innenfor en bedrift som har flere Azure-tenanter, kan man bruke Azure Delegated Resource Mangement for å forenkle arbeidet på tvers av disse. Autoriserte brukere kan jobbe direkte i sammenheng med et kundeabonnement uten å ha en konto og uten å være medeier i kundens Azure-tenant [20].

7.1 Referanseliste

[1] «Sopra Steria», Internett: https://no.wikipedia.org/wiki/Sopra_Steria [Besøkt 03.03.2020]

[2] «Azure Lighthouse og Azure Sentinel», Internett: https://techcommunity.microsoft.com/t5/azure-sentinel/using-azure-lighthouse-and-azure-sentinel-to-monitor-across/ba-p/1043899 [Besøkt 03.03.2020]

[3] "Azure Active Directory", Internett: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis [Besøkt 03.03.2020]

[4] "Azure Active Directory", Internett: https://www.red-gate.com/simple-talk/cloud/security-and-compliance/azure-active-directory-part-1-an-introduction/ [Besøkt 03.03.2020]

[5] "Azure Lighthouse", Internett: https://azure.microsoft.com/nb-no/services/azure-lighthouse/#features [Besøkt 03.03.2020]

[6] «What is Azure Sentinel?», Internett: https://docs.microsoft.com/en-us/azure/sentinel/overview. [Besøkt 02.03.2020]

[7] "Azure Subscription", Internett: https://docs.microsoft.com/en-us/office365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings [Besøkt 04.03.2020]

[8] "Quickstart – set up a tenant", Internett: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant [Besøkt 04.03.2020]

[9] "Manage access to log data and workspaces in Azure Monitor", Internett: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access [Besøkt 04.03.2020]

[10] "Single Tenant vs Multi Tenant", Internett: https://digitalguardian.com/blog/saas-single-tenant-vs-multi-tenant-whats-difference [Besøkt 04.03.2020]

[11] "Quickstart – On-board Azure Sentinel", Internett: https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard [Besøkt 05.03.2020]

[12] "Connect data sources", Internett: https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources [Besøkt 06.03.2020]

[13] "Microsoft Defender Advanced Threat", Internett: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection [Besøkt 15.03.2020]

[14] "Tutorial: Set up automated threat responses in Azure Sentinel", Internett: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook [Besøkt 07.04.2020]

[15] “Create custom rules to detect threats”, Internett: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom [Besøkt 07.04.2020]

[16] “Use built-in analytics to detect threats”, Internett: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in [Besøkt 07.04.2020]

[17] “Hutning”, Internett: https://docs.microsoft.com/en-us/azure/sentinel/hunting [Besøkt 09.04.2020]

[18] “Use notebooks to hunt”, Internett: https://docs.microsoft.com/en-us/azure/sentinel/notebooks [Besøkt 09.04.2020]

[19] “Azure Lighthouse”, Internett: https://docs.microsoft.com/en-us/azure/lighthouse/overview [Besøkt 11.04.2020]

[20] «Azure delegated resource management», Internett: https://docs.microsoft.com/en-us/azure/lighthouse/concepts/azure-delegated-resource-management [Besøkt 11.04.2020]

Driftsrapport

Innholdsfortegnelse

1. Hensikten med dokumentet

Dokumentet er driftsrapporten i faget IDRI3001 Bacheloroppgave i drift av datasystemer. Rapporten skal fungere som veiledning til hvordan man kan implementere en løsning med Azure Lighthouse og Azure Sentinel for å jobbe med sikkerhetsmonitorering og hendelseshåndtering på tvers av flere Azure-tenanter. Rapporten inneholder dokumentasjon om oppsett av en slik løsning med tilhørende tjenester. Dokumentet beskriver praktiske hendelser gjennom hele prosessen, fra nødvendige steg som må gjennomføres for å implementere løsningen, til hvordan man på en effektiv måte kan jobbe på tvers av kunder. Målet er å gi brukere av dette dokumentet en solid introduksjon til hvordan en slik løsning kan implementeres, samt hvordan man kan bruke funksjoner og tjenester i løsningen i praksis.

2. Definisjoner og forkortelser

Begrep	**Beskrivelse**
Azure AD	Azure Active Directory.
Azure Subscription	Abonnement for å få tilgang til Azure-plattformen.
Command and control server	Datamaskin kontrollert av en angriper. Brukes for å sende kommandoer til systemer som har blitt kompromittert av virus, samt for å motta stjålet data.
«Contributor»-rettigheter	Lar deg administrere alt bortsett fra å gi tilgang til ressurser.
«Data Connectors»	Gjør det mulig å koble til ulike kilder for å samle data til Azure Sentinel.
Microsoft Defender ATP	Microsoft Defender Advanced Threat Protection.
«Multi-tenant workbooks»	Refererer til workbooks på tvers av Azure Sentinel-arbiedområder. De kan være i samme eller i forskjellige Azure-tenanter.
Onboarding	Prosessen med å komme i gang med et produkt/programvare. For eksempel: «Onboarde Azure Sentinel», betyr å komme i gang med Azure Sentinel.
Playbooks	Referer til Playbooks i Azure Sentinel – En samling av prosedyrer som kan kjøres fra Azure Sentinel som respons på en alarm.
«Renderer»	Fremstiller et bilde eller en animasjon.
Windows Defender AV	Windows Defender Anti Virus.
«Wizard»	Veiledning/veiviser som brukes for oppsett og installasjoner.

3. Faser i implementasjonen

Dette kapittelet tar for seg de ulike fasene i implementasjonen av løsningen. I dette kapittelet skal brukeren av dokumentet få et generelt overblikk over innholdet i de ulike fasene. Fasene er delt opp slik:

- **Fase 1**: Oppsett og konfigurasjon i Azure.
- **Fase 2**: Oppsett og konfigurasjon av testmiljø.
- **Fase 3**: Azure Lighthouse onboarding.
- **Fase 4**: Hendelseshåndtering og arbeid på tvers av kunder i Azure Sentinel.

3.1 Beskrivelse av faser

Fase 1 – Oppsett og Konfigurasjon i Azure

Fase 1 tar for seg hvordan oppsett og konfigurasjon gjøres i Azure for at løsningen skal fungere. Kapittelet behandler oppsett av Azure Resource Group og Log Analytics Workspace, Azure Sentinel onboarding, samt utrulling av virtuelle maskiner for testmiljø. Denne fasen legger grunnlaget for det videre arbeidet i de neste fasene av implementasjonen.

Fase 2 – Oppsett og konfigurasjon av testmiljø

Etter at arbeidet i fase 1 er gjennomført kan oppsett og konfigurasjon av det lokale testmiljøet begynne. Dette inkluderer tilkobling til testmiljøet, installasjon av Office 365, Microsoft Defender ATP onboarding, samt hvordan man kan kjøre simulerte angrep i testmiljøet. Denne fasen bidrar til innhenting av data til Azure Sentinel. Dataen som blir hentet fra testmiljøet gjør det mulig å jobbe med hendelseshåndtering i Azure Sentinel. Videre vil fase 3 muliggjøre arbeid på tvers av Azure-tenanter.

Fase 3 – Azure Lighthouse

Denne fasen demonstrerer hvordan man som tenantadministrator, eller tjenesteleverandør, kan onboarde en kunde til Azure Delegated Resource Management. Som nevnt i Designrapporten, er Azure Delegated Resource Mangement en av hovedkomponentene til Azure Lighthouse. Ved å onboarde en kunde til Azure DRM vil tenantadministratoren kunne aksessere og administrere kundens delegerte ressurser (abonnement og/eller ressursgrupper) fra sin egen Azure AD-tenant.

Denne prosessen kan gjentas dersom du administrerer ressurser for flere kunder. Da, når en autorisert bruker logger inn i din tenant, kan denne brukeren autoriseres på tvers av kundenes leieforhold. Dermed kan brukeren utføre administrerende oppgaver uten å måtte logge på hver enkelt kunde-tenant.

Fase 4 – Hendelseshåndtering og arbeid på tvers av kunder i Azure Sentinel

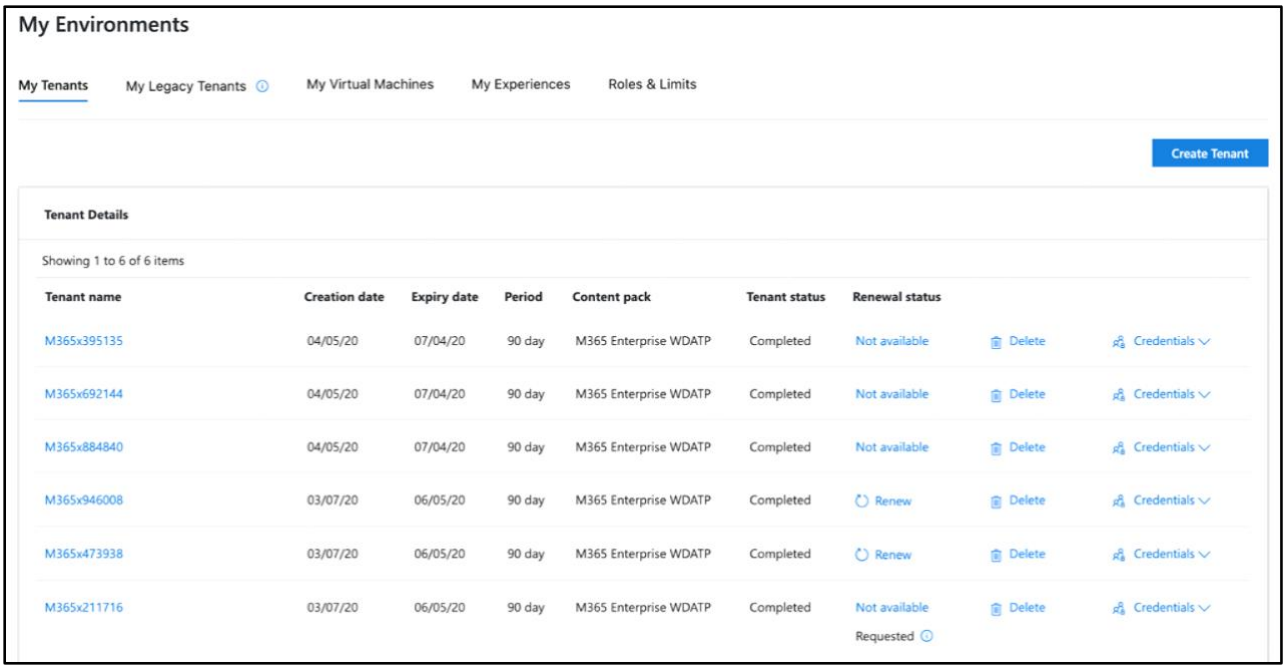
Etter hvert som alarmer fra Microsoft Defender ATP dukker opp som hendelser i Azure Sentinel kan man begynne arbeidet med hendelseshåndtering. For at hendelsene skal vises i Sentinel er det viktig å opprette regler som genererer alarmer basert på mistenkelig aktivitet i miljøet, og videre oppretter hendelser. Denne fasen forklarer hvordan man kan opprette slike regler basert på innebygde maler i Azure Sentinel. Siden de samme angrepene har blitt simulert på tvers av Azure-tenantene, vil det i denne fasen også bli demonstrert hvordan man kan jobbe med håndtering av hendelsene på tvers av flere Sentinel-arbeidsområder på en gang. Dette bidrar til bedre oversikt og kontroll over dine kunders Sentinel-arbeidsområder, da alle arbeidsområdene blir tilgjengelig fra samme sted.

Videre innebærer denne fasen hvordan man kan utføre søk på tvers av Azure-tenantene for å finne alarmer eller hendelser av samme type. Dette vil spare tid, da man slipper å gjøre samme søk flere ganger på forskjellige kunders Azure-tenanter. Denne fasen tar også for seg hvordan man kan visualisere dataen til flere kunder på en gang, ved hjelp av «multi tenant workbooks» i Azure Sentinel. Dette bidrar til å gi en bedre oversikt over alle dine kunders miljøer.

4. Fase 1 - Oppsett og konfigurasjon i Azure

I dette prosjektet har jeg benyttet meg av demo-miljøer fra Microsoft. Microsoft har en nettside som gir deg muligheten til å opprette opptil 6 Azure-tenanter, som du kan benytte i 90 dager [1]. Dette har muliggjort en løsning med flere Azure-tenanter. Hver Azure-tenant har fått sitt eget abonnement i Azure. Det er nødvendig med tilgang til flere Azure-tenanter for å sette opp en løsning som vist i dette dokumentet.

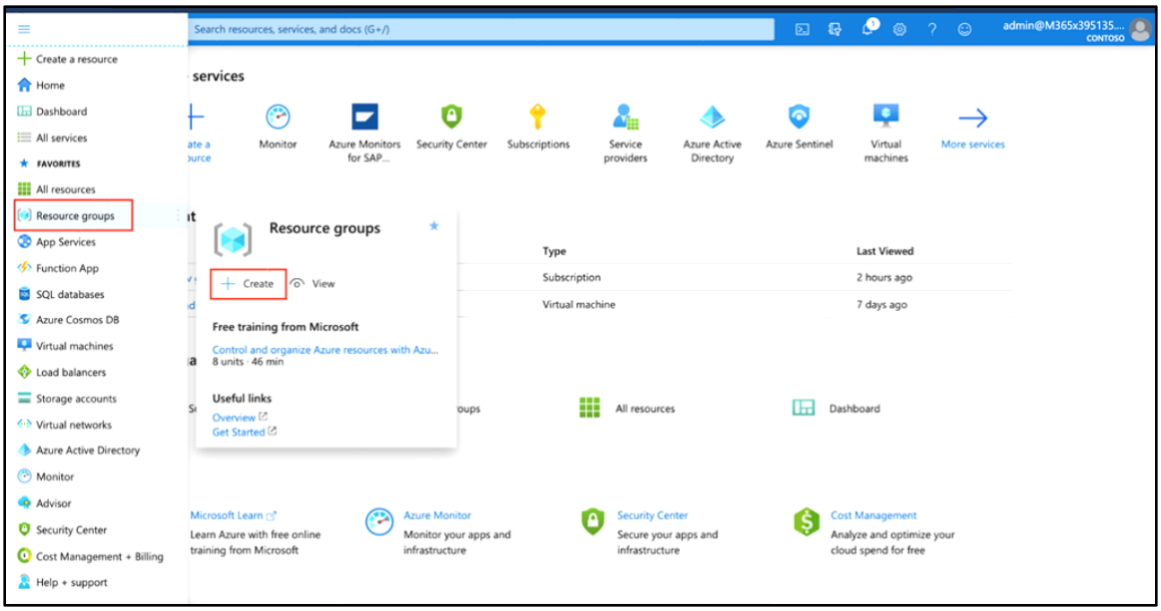
Bildet under viser mine demo-miljøer i Azure. Fire av seks har aktive abonnementer i Azure, og har blitt brukt i dette prosjektet. Det er ikke nødvendig med så mange Azure-tenanter for å sette opp en løsning med flere Azure-tenanter, men minst to er nødvendig.



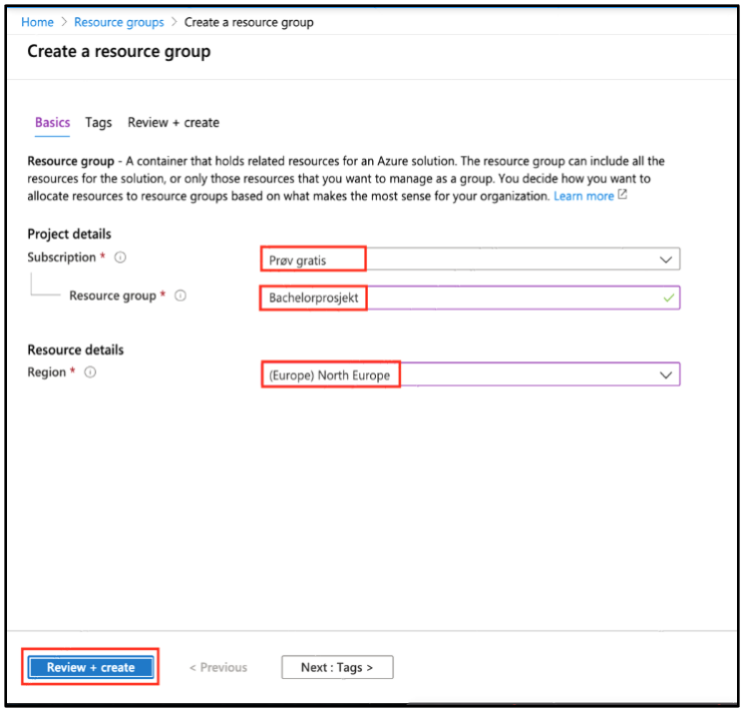
4.1 Opprette Azure Resource Group i Azure-portalen

Ressurser i Azure organiseres i ressursgrupper. Ressursgrupper samler ressurser, som virtuelle maskiner, offentlige ip-adresser, nettverkskort og disker. Komponentene hører gjerne sammen og deler samme livssyklus [2]. I dette prosjektet samles alle ressursene i hver enkelt tenant i én ressursgruppe.

1. Logg inn i Azure-portalen og velg **Resource Groups** i menyen til venstre.
2. Velg **Create**.

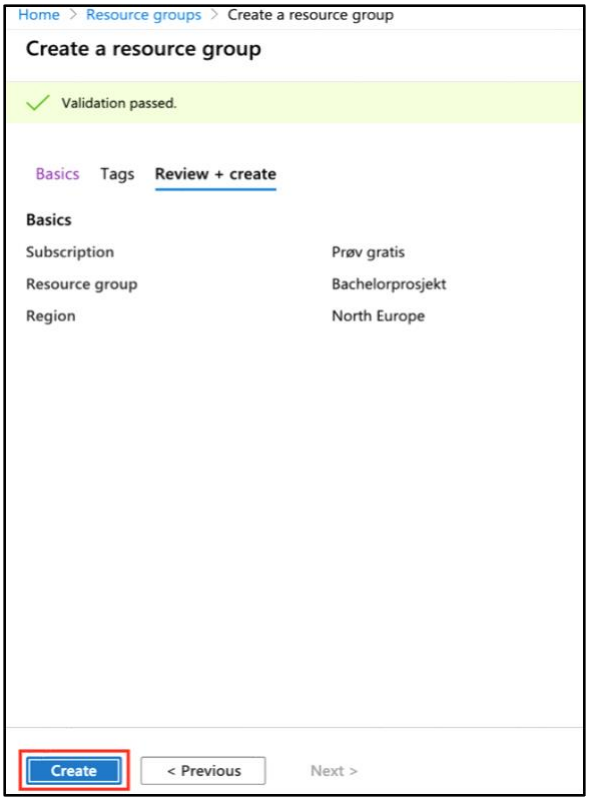


3. Fyll inn følgende verdier:
    - **Subscription:** Velg ditt Azure abonnement.
    - **Resource Group:** Skriv inn ønsket navn på ressursgruppen.
    - **Region:** Velg ønsket lokasjon, som for eksempel **North Europe**.



4. Velg **Review + create**.

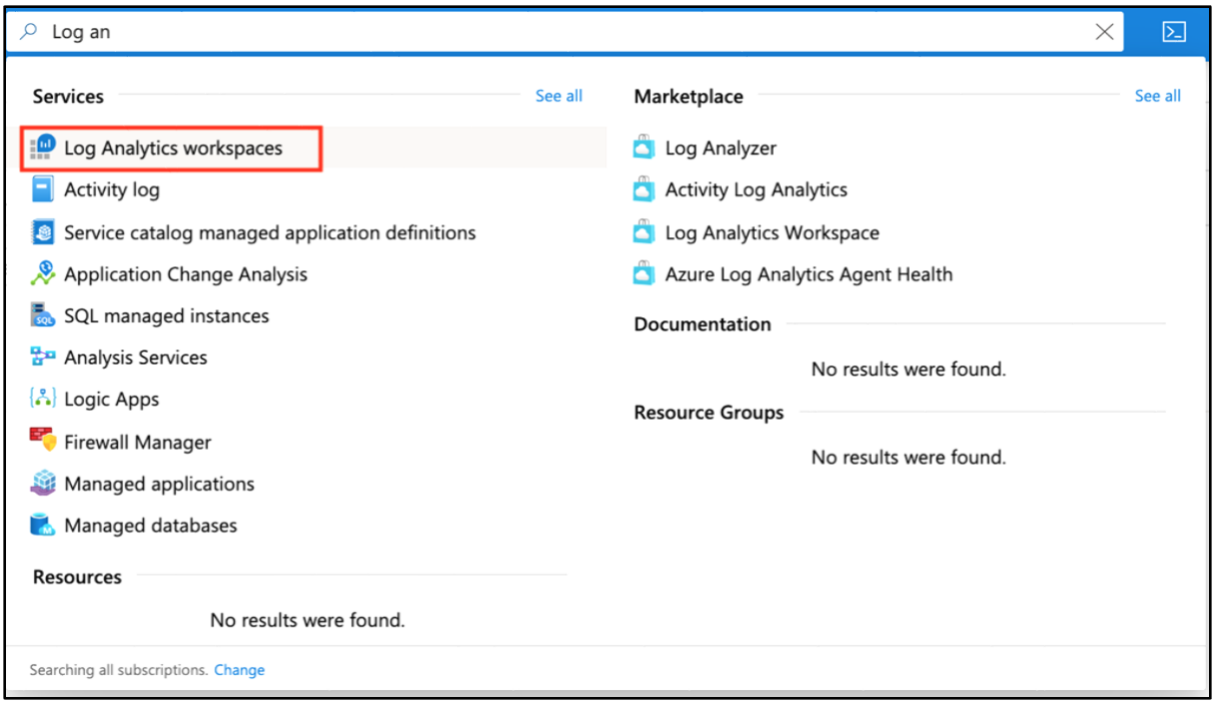
5. Velg **Create.** Det tar noen sekunder før ressursgruppen blir opprettet.



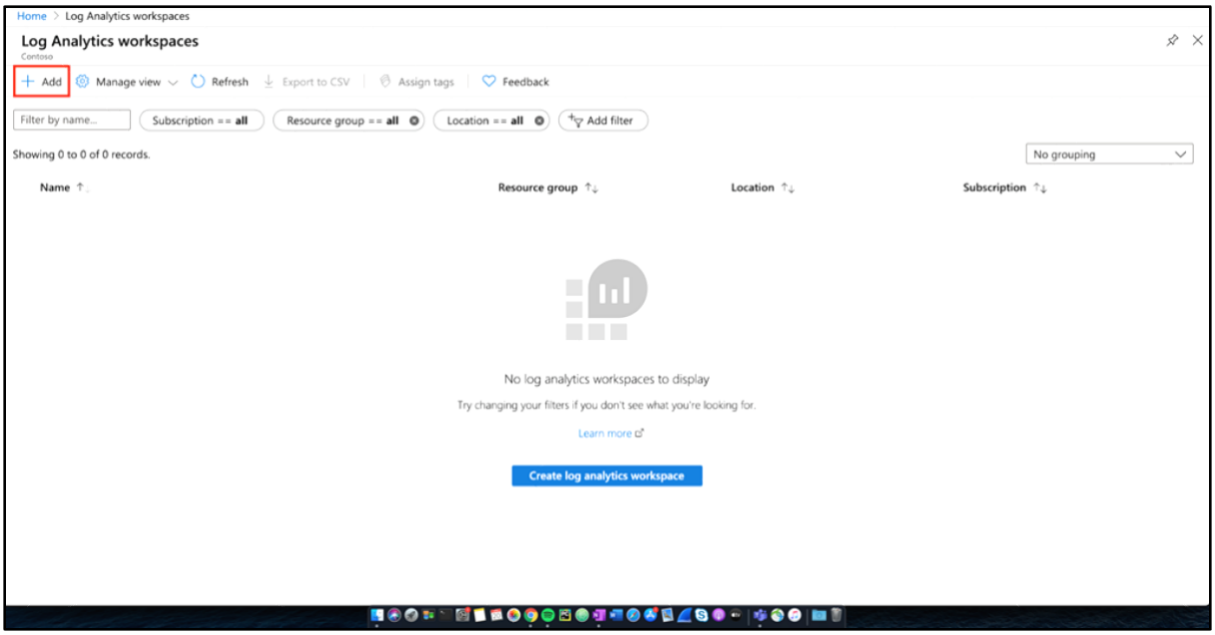
4.2 Opprette Log Analytics Workspace

For at Azure Sentinel skal kunne samle data, må det opprettes et Log Analytics Workspace.

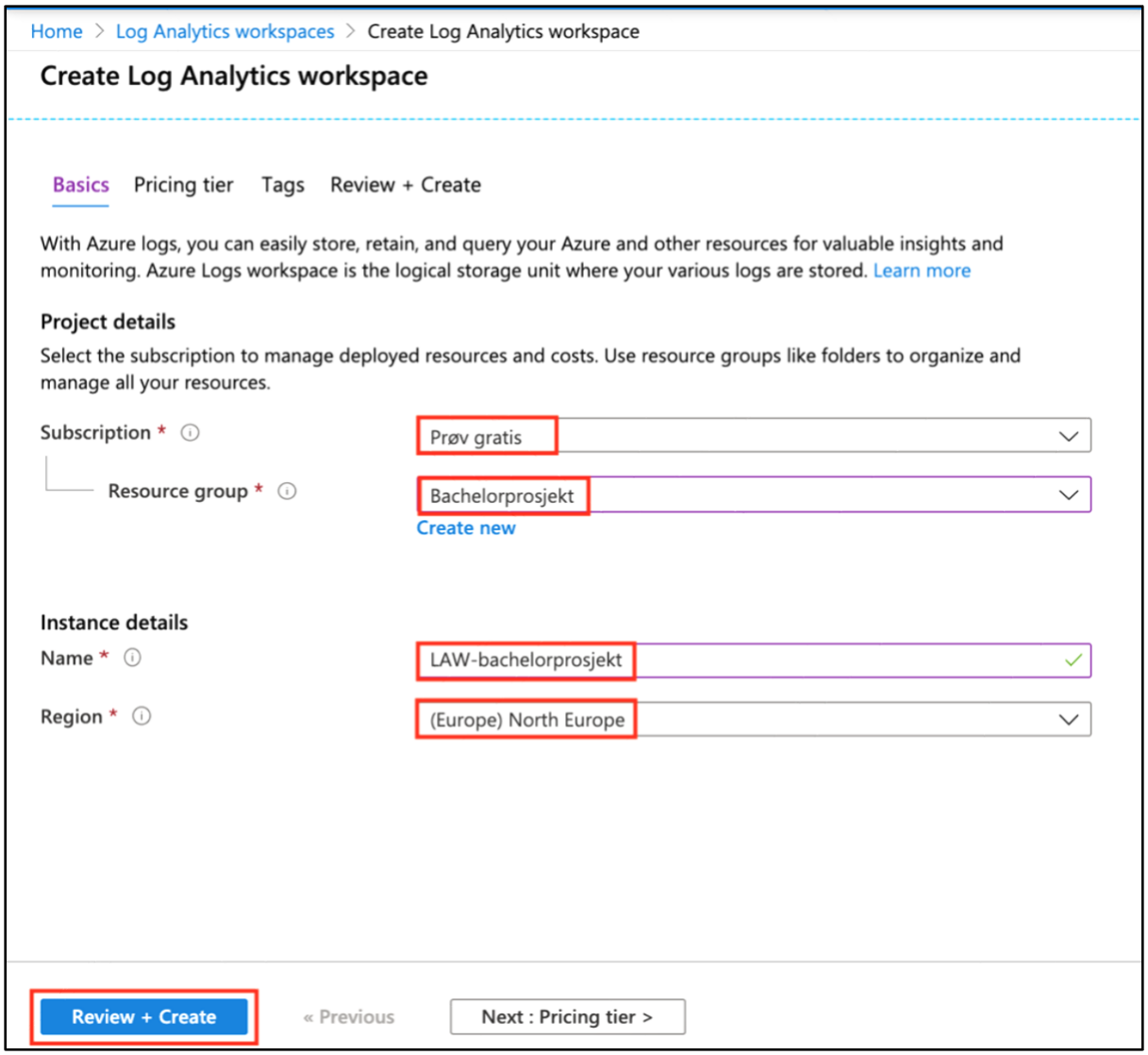
1. Begynn å skrive "Log Analytics" i søkelinjen. Velg **Log Analytics Workspaces**.



2. Velg **Add.**



3. Fyll inn følgende verdier:
    - **Subscription:** Velg ditt Azure-abonnement.
    - **Resource Group:** Velg enten en eksisterende ressursgruppe eller velg "Create new**".**
    - **Name:** Gi et navn for arbeidsområdet.
    - **Region:** Velg en tilgjengelig lokasjon.

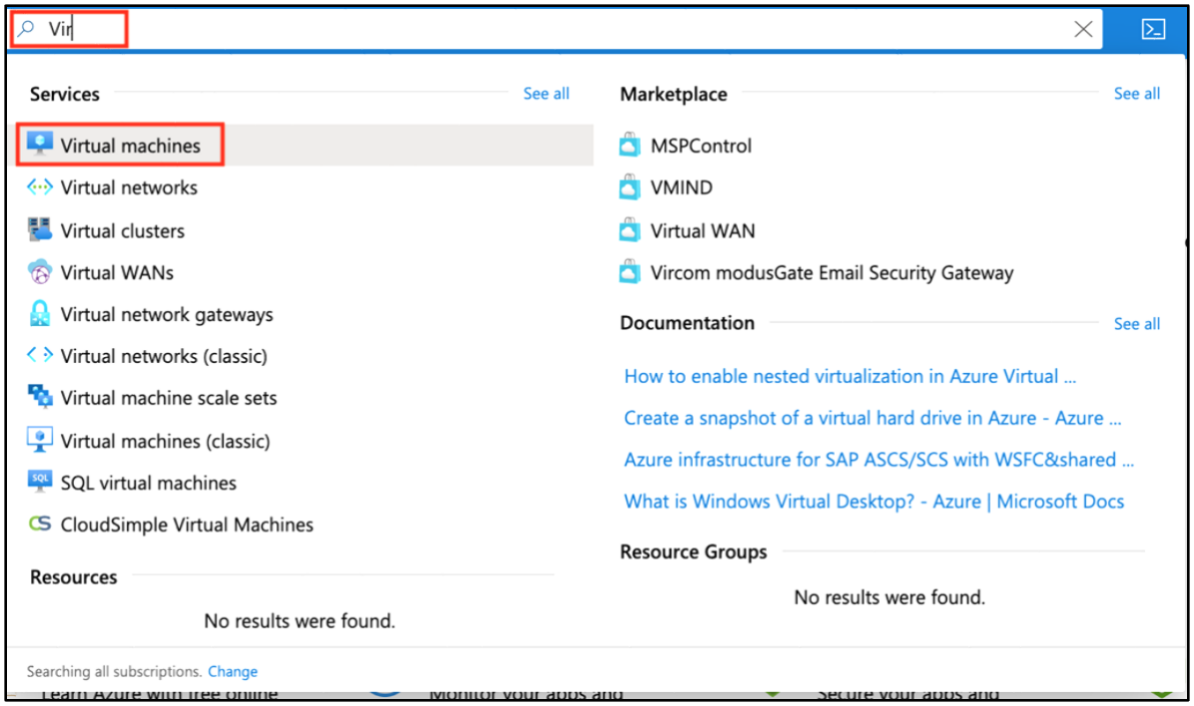


4. Velg **Review + Create**. Etter at valideringen er gjennomført, velg **Create.**

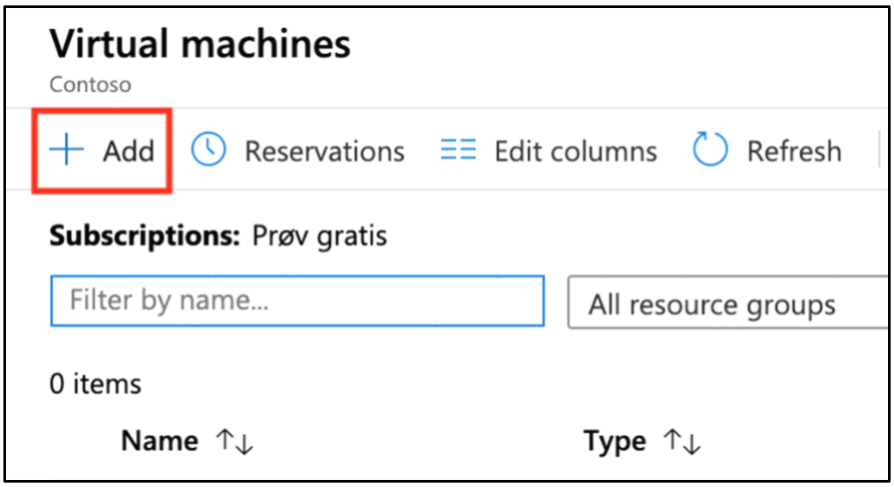
4.3 Opprette en virtuell maskin i Azure-portalen

I dette prosjektet består testmiljøet av én virtuell maskin i hvert tenant. Det opprettes én Windows 10 maskin i hver tenant.

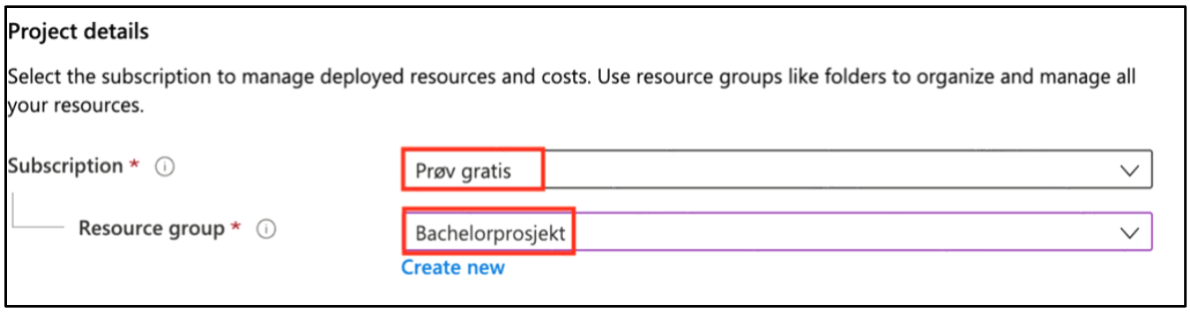
1. Søk etter og velg **Virtual Machines**.



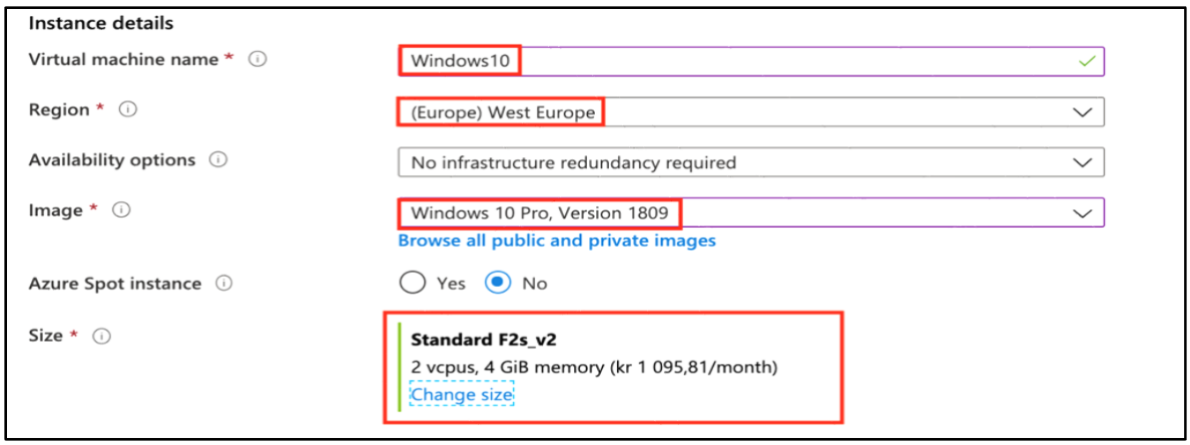
2. Velg **Add.**



3. I **Basics**-fanen, under **Project Details**, velg abonnement og ressursgruppe.

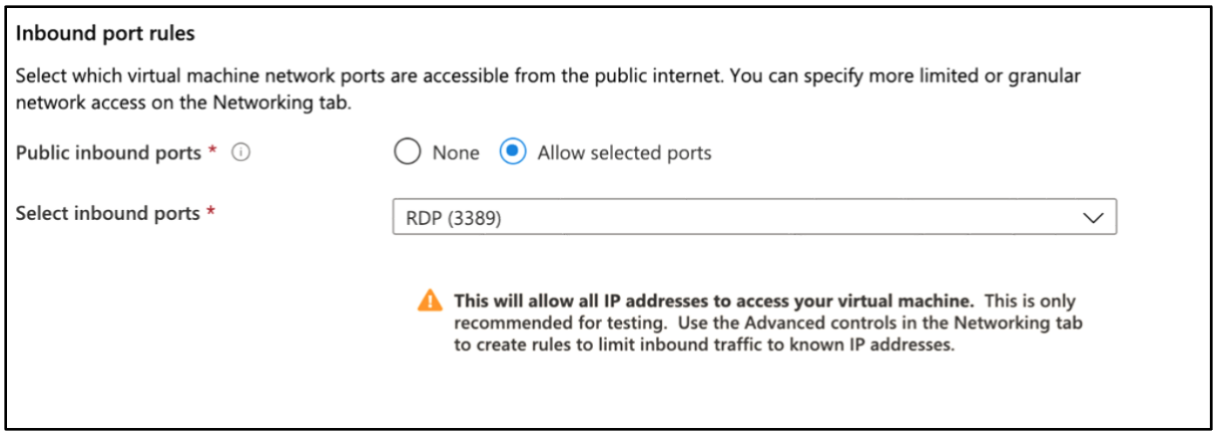


4. Under **Instance details**, fyll inn følgende verdier:

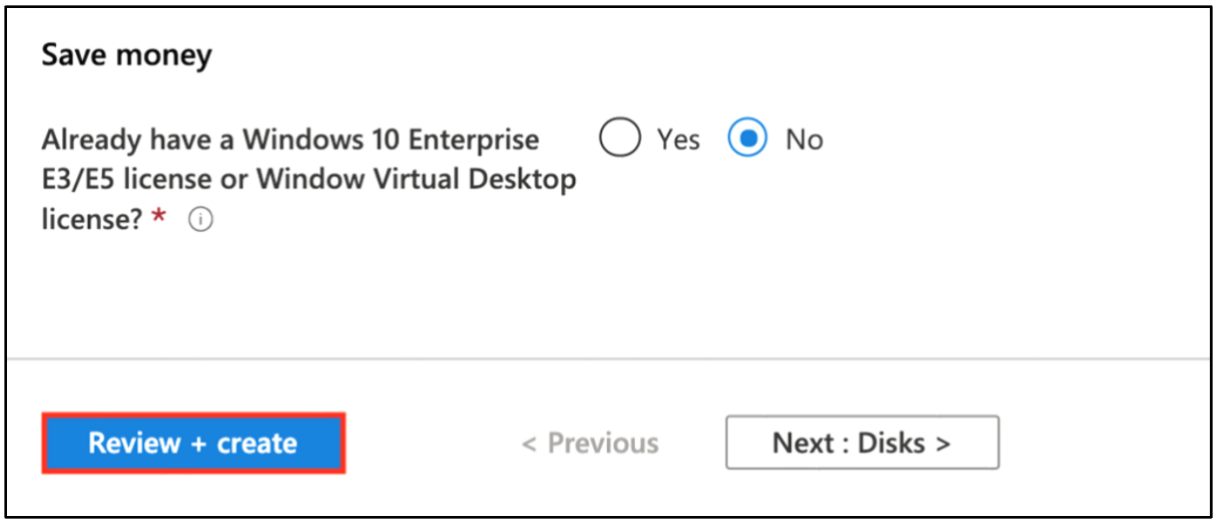


5. Under **Administrator Account** skriv inn brukernavn og passord. Passordet må være minst 12 tegn, og møte kravene som Microsoft har satt for opprettelse av VM [3].

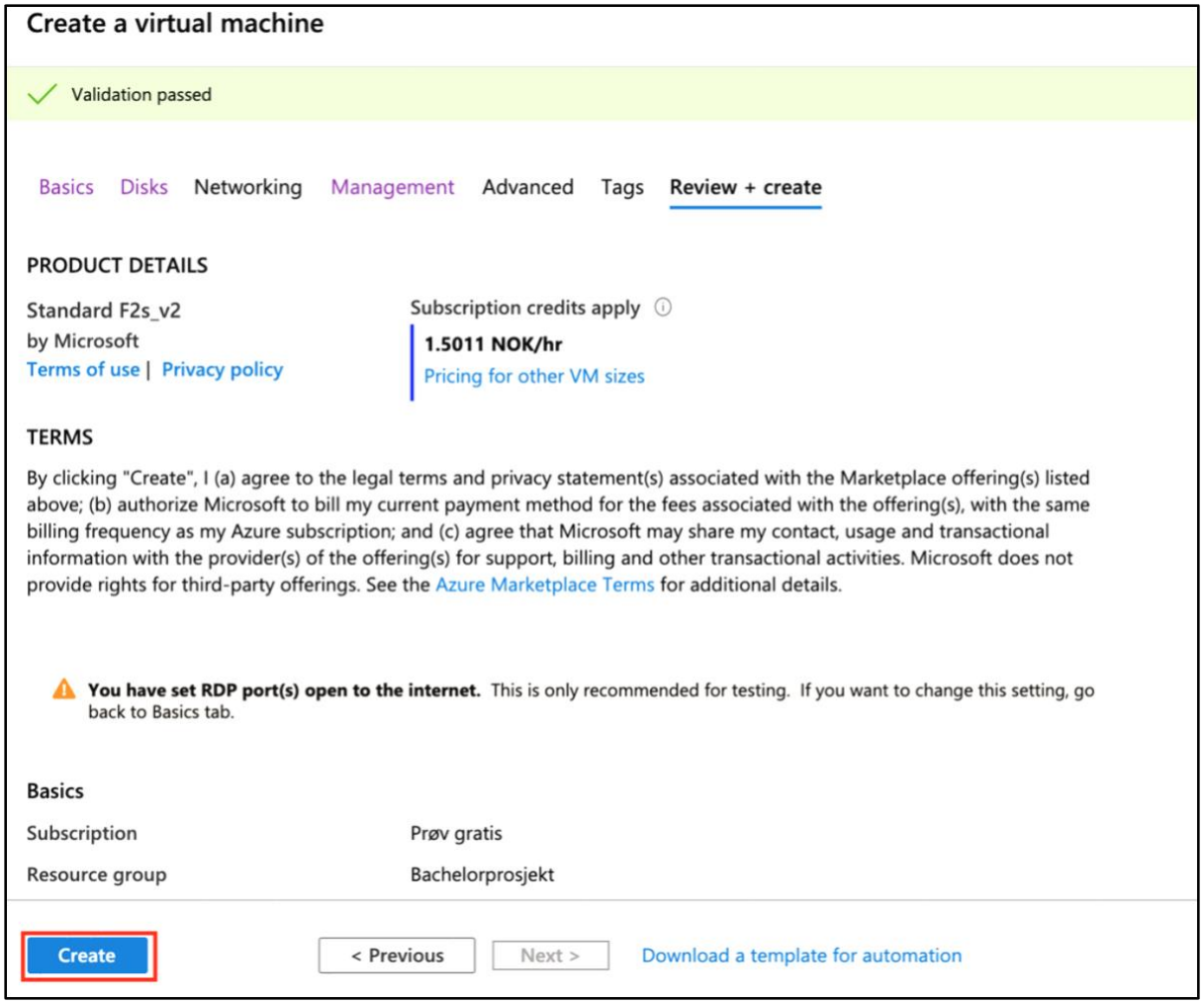
6. Under **Inbound port rules**, velg **Allow selected ports** og **RDP (3389)**.



7. La de gjenværende feltene stå som de er, og velg **Review + create**.



8. Velg **Create**.



4.4 Azure Sentinel onboarding

For å onboarde Azure Sentinel må man først aktivere tjenesten, og deretter koble til datakildene. Etter man har gjort dette kan man begynne arbeidet med visualisering av data, trusseldeteksjon, sikkerhetsmonitorering og hendelseshåndtering.

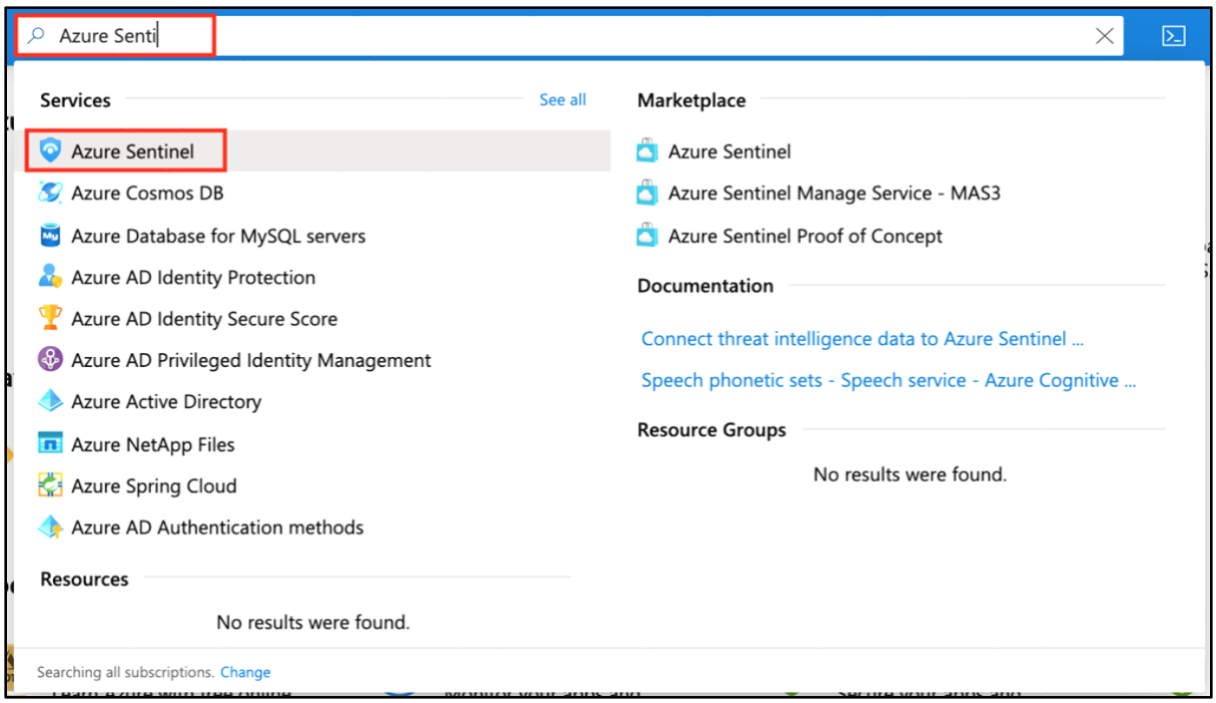
4.4.1 Globale forutsetninger

Før man kan legge til og konfigurere Azure Sentinel er det viktig at man har følgende forutsetninger:

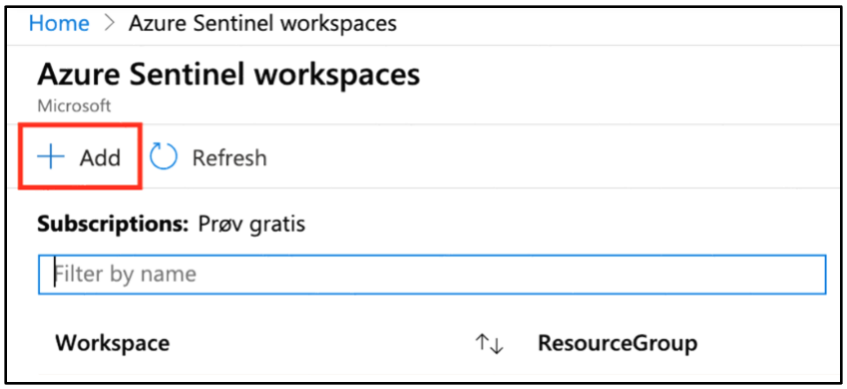
- Aktivt Azure Subscription.
- Log Analytics Workspace.
- For å aktivere Azure Sentinel må man ha "contributor"-rettigheter i samme abonnement som Azure Sentinel-arbeidsområdet skal ligge.
- For å bruke Azure Sentinel må man ha enten "contributor"- eller leserettigheter på ressursgruppen som arbeidsområdet hører til.
- Andre rettigheter kan være nødvendig for å koble til spesifikke datakilder.

4.4.2 Aktivere Azure Sentinel

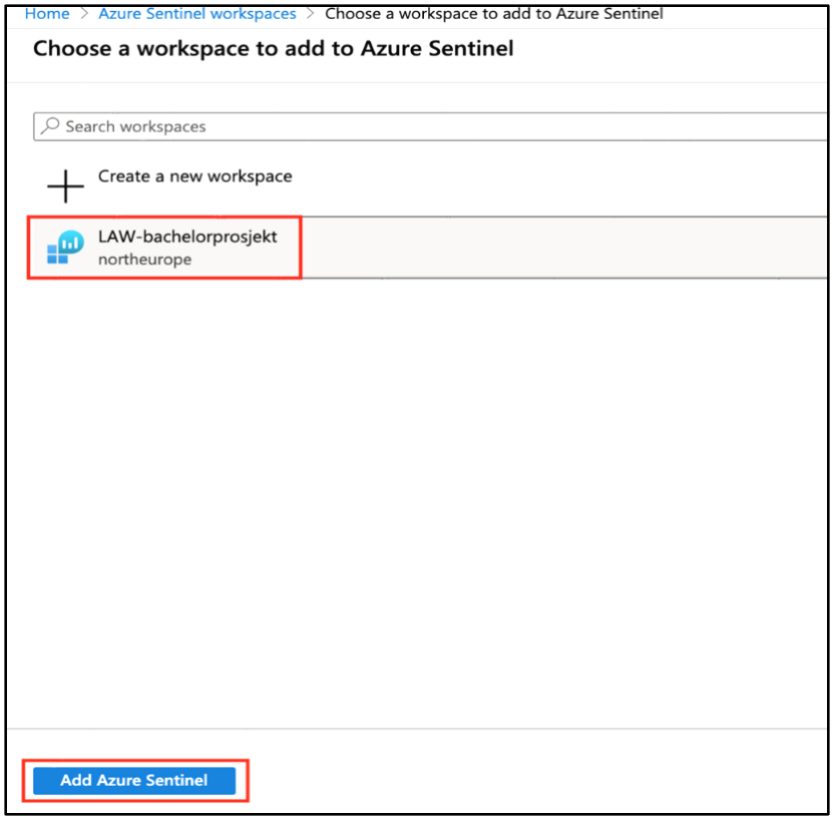
1. Logg inn i Azure-portalen. Søk etter og velg **Azure Sentinel.**



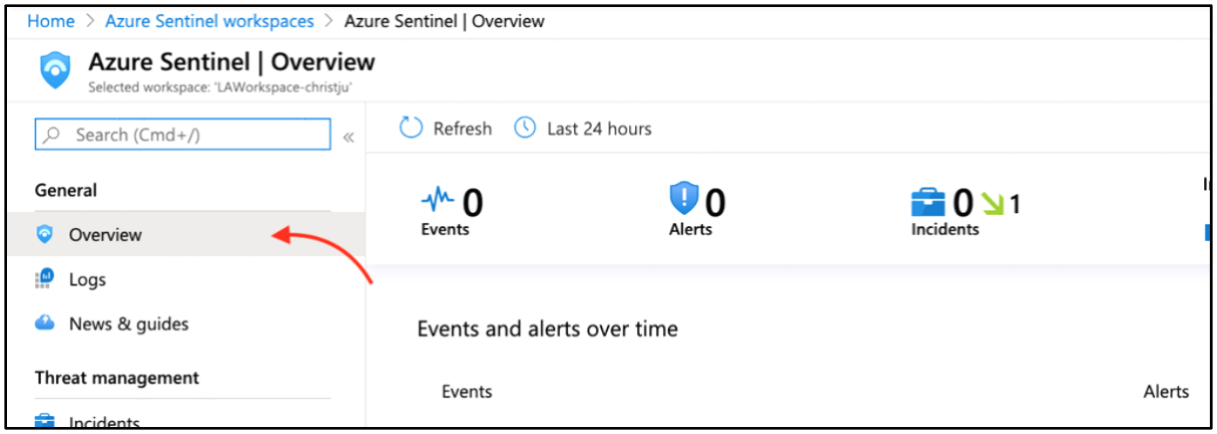
2. Velg **Add.**



3. Velg arbeidsområdet du vil bruke, eller opprett et nytt. Man kan kjøre Azure Sentinel på flere arbeidsområder, men dataen er isolert til ett arbeidsområde. Velg **Add Azure Sentinel.**



4. Når Azure Sentinel har blitt konfigurert, vil hoved-dashbordet til Azure Sentinel dukke opp uten data.

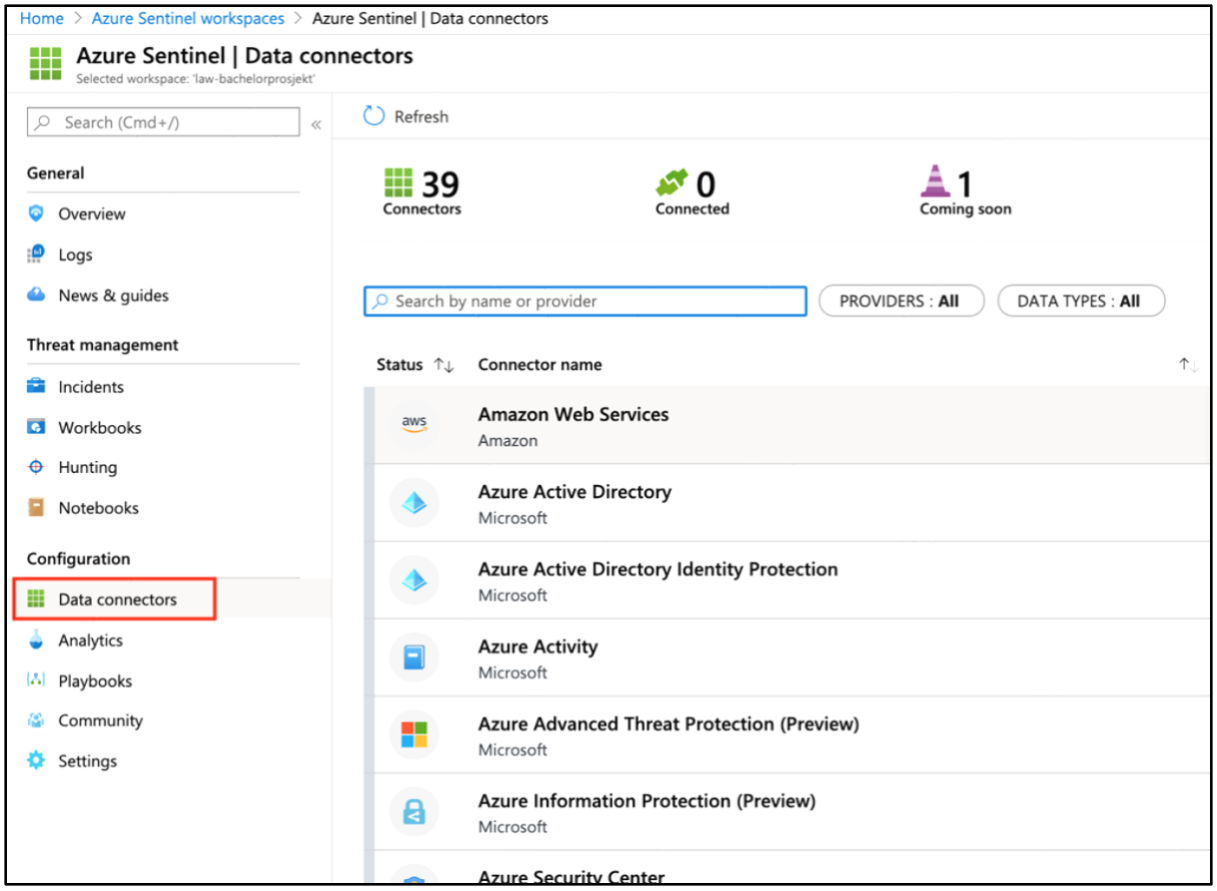


4.4.3 Koble til datakilder

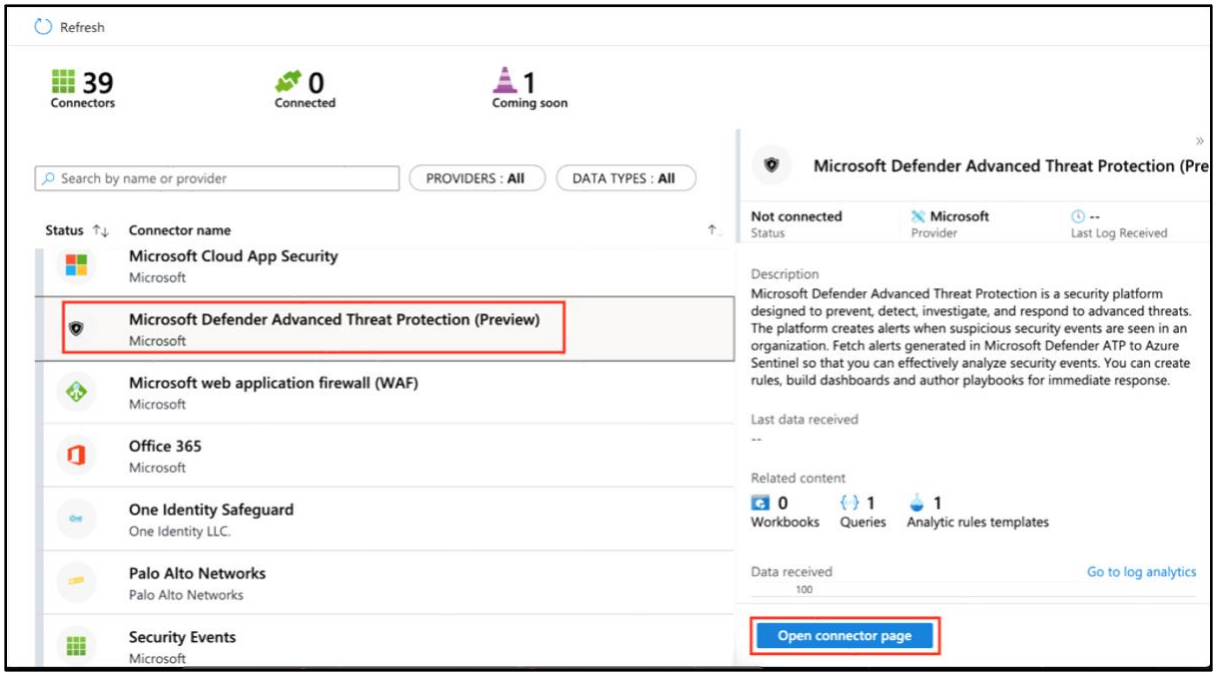
Azure Sentinel oppretter forbindelse til tjenester og applikasjoner ved å koble til tjenesten, og videresende hendelsene og loggene til Azure Sentinel. For maskiner og virtuelle maskiner kan man installere Azure Sentinel-agenten som samler loggene og videresender dem til Azure Sentinel. For brannmurer og proxyer bruker Azure Sentinel en Linux syslog server, som agenten blir installert på. Derfra blir loggene videresendt til Azure Sentinel [4].

Som nevnt tidligere har Azure Sentinel en rekke forskjellige "Data Connectors" fra både Microsoft-løsninger og ikke-Microsoft-løsninger. I dette prosjektet har det blitt hentet data hovedsakelig fra Microsoft Defender ATP. Dette er en ny "connector" i Azure Sentinel, som lar deg strømme alarmer fra Microsoft Defender ATP inn til Azure Sentinel. Alarmene vil dukke opp i Azure Sentinel som nye hendelser. Fra Azure Sentinel kan man undersøke disse hendelsene nærmere. Dette skal jeg komme tilbake til i fase 4, «Hendelseshåndtering og arbeid på tvers av kunder i Azure Sentinel».

1. Velg "**Data Connectors**". En oversikt over alle de forskjellige datakildene kommer opp.

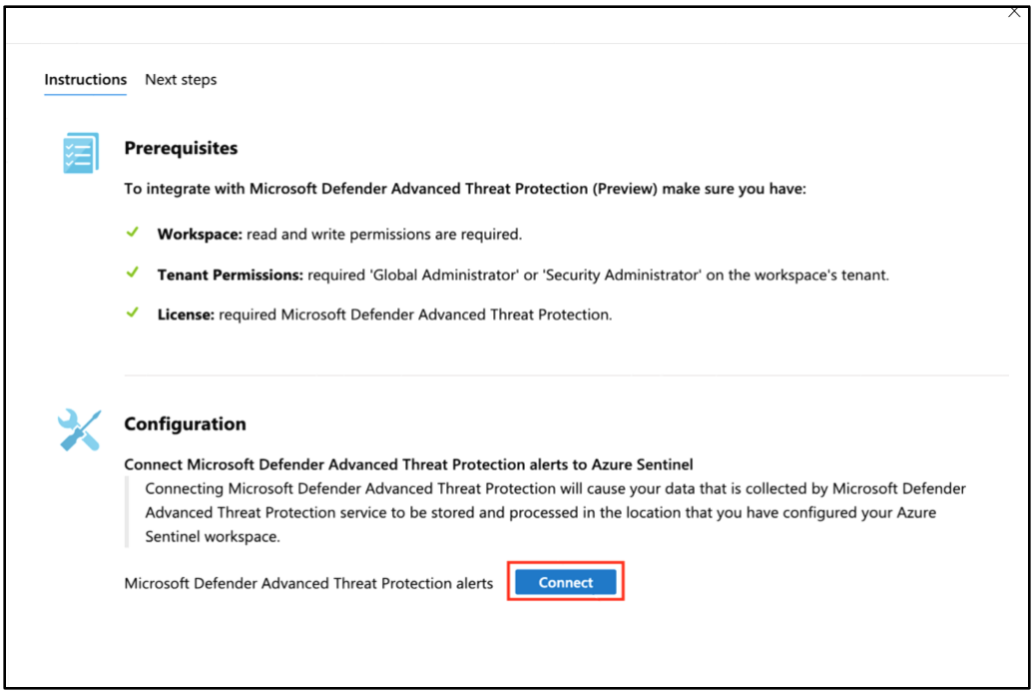


2. Bla ned til **Microsoft Defender Advanced Threat Protection** og velg **Open connector page.**

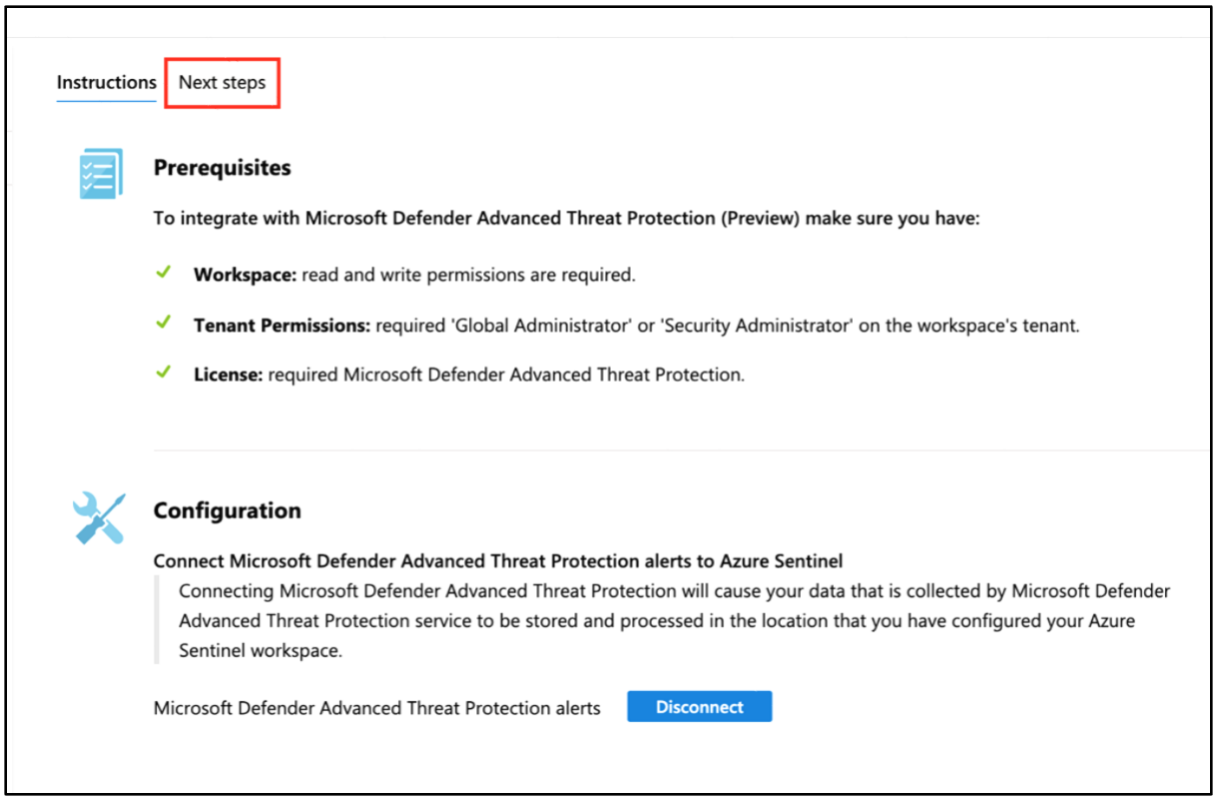


3. På "connector-siden" vises hvilke forutsetninger som må være på plass før man kan koble til datakilden.
    - **Workspace**: Lese- og skriverettigheter
    - **Tenant permissions**: "Global Administrator" eller "Security Administrator" er nødvendig.
    - **License:** Microsoft Defender Advanced Threat Protection

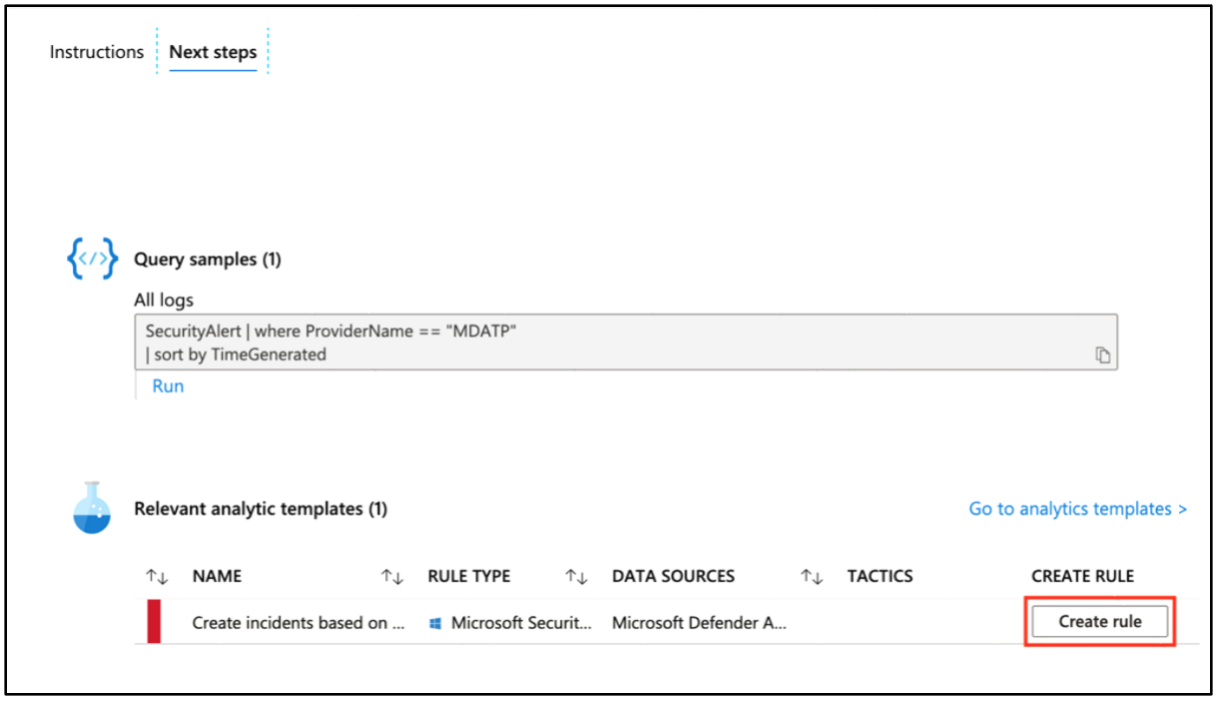
Velg **Connect**.



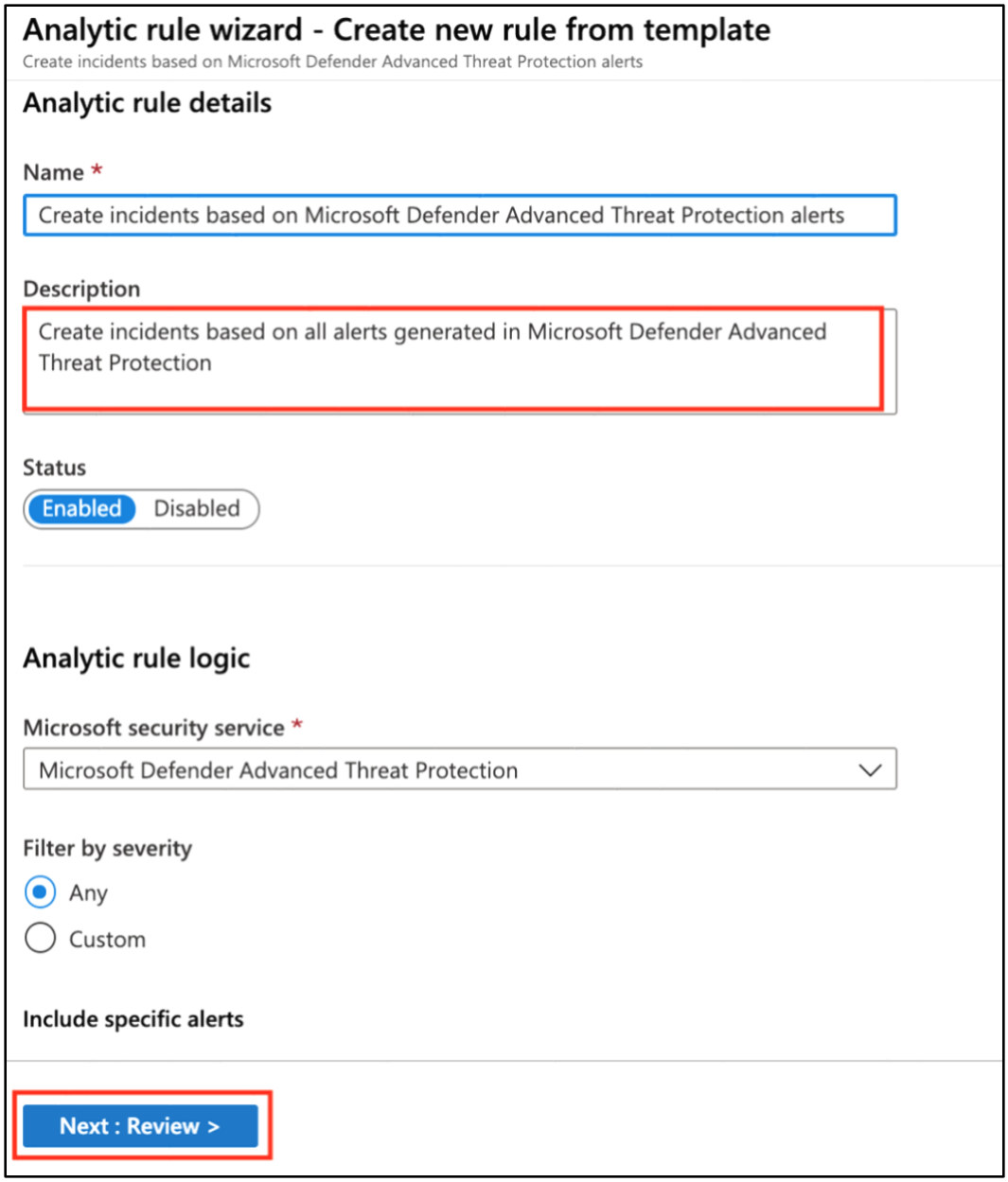
4. Velg **Next Steps**.



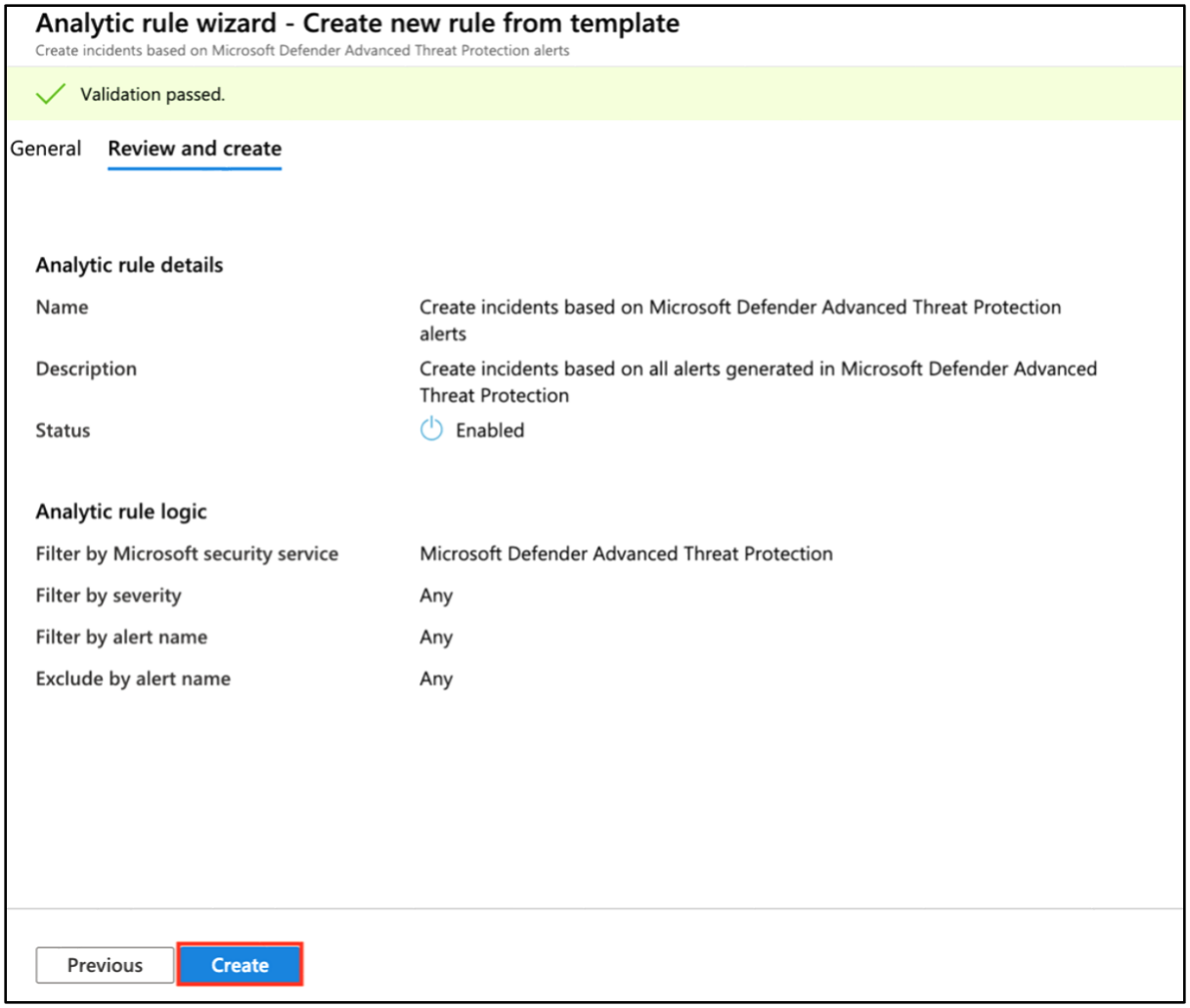
5. Velg **Create rule**.



6. Denne regelen oppretter hendelser i Azure Sentinel, basert på alle alarmer som blir generert i Microsoft Defender ATP. Velg **Next: Review >**.



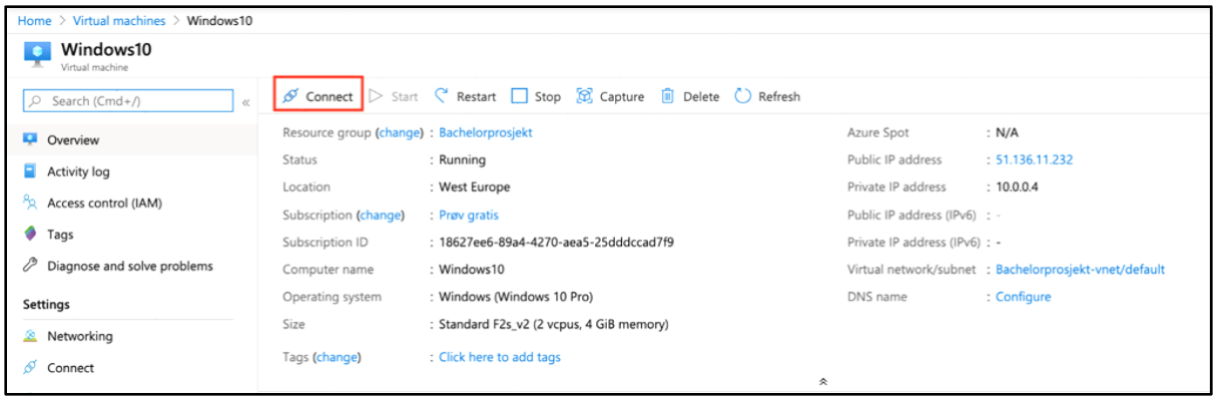
7. Etter at valideringen er gjennomført, velg **Create**.



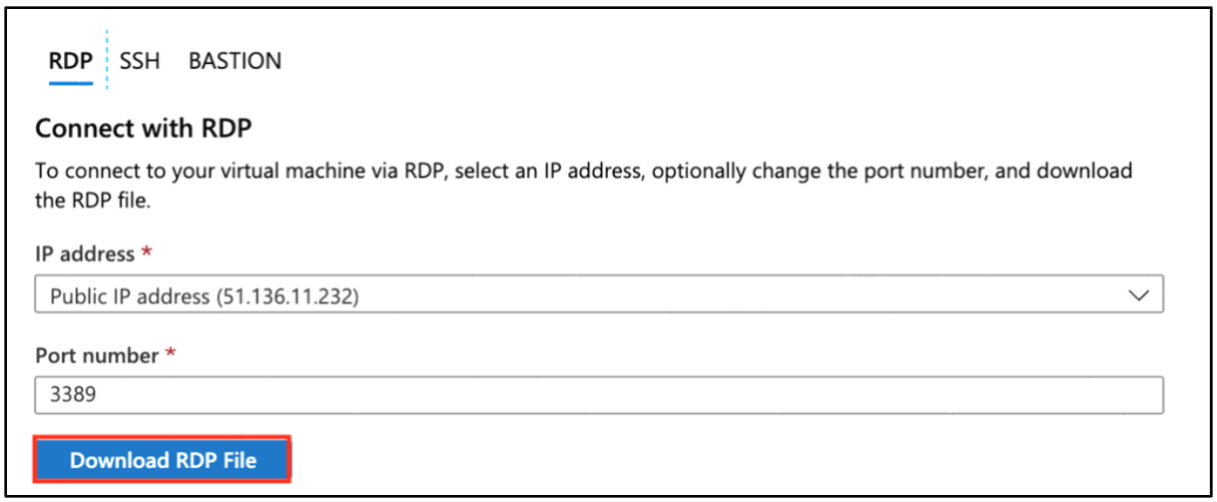
5. Fase 2 - Oppsett og konfigurasjon av testmiljø

5.1 Koble til testmiljøet

1. Velg den virtuelle maskinen du skal bruke til testmiljøet. Under oversikten, velg **Connect.**



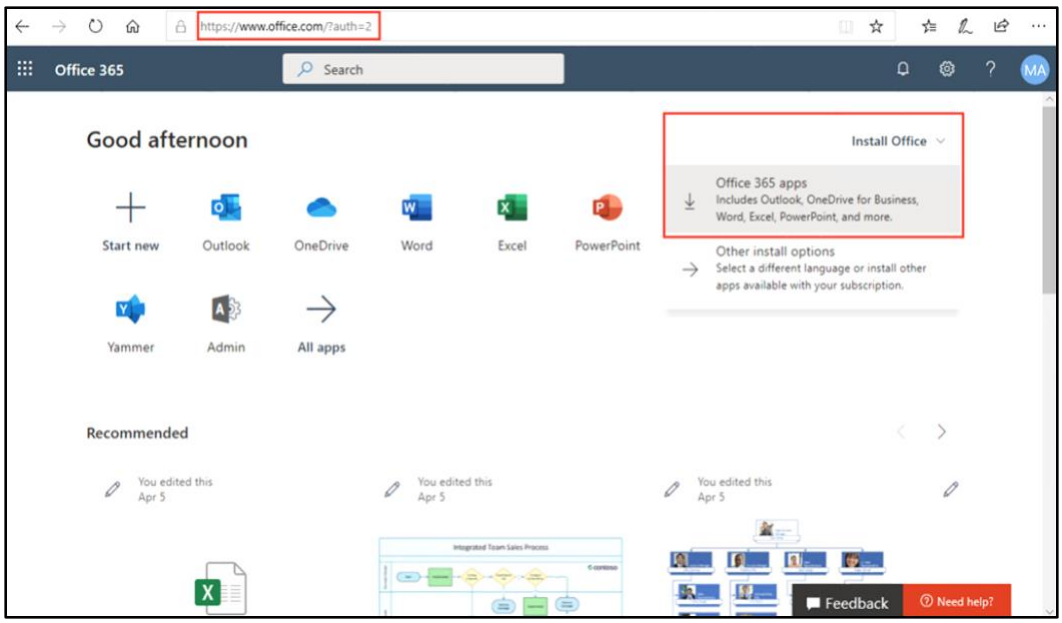
2. Under RDP, velg **Download RDP file**. Åpne deretter filen i **Microsoft Remote Desktop**.



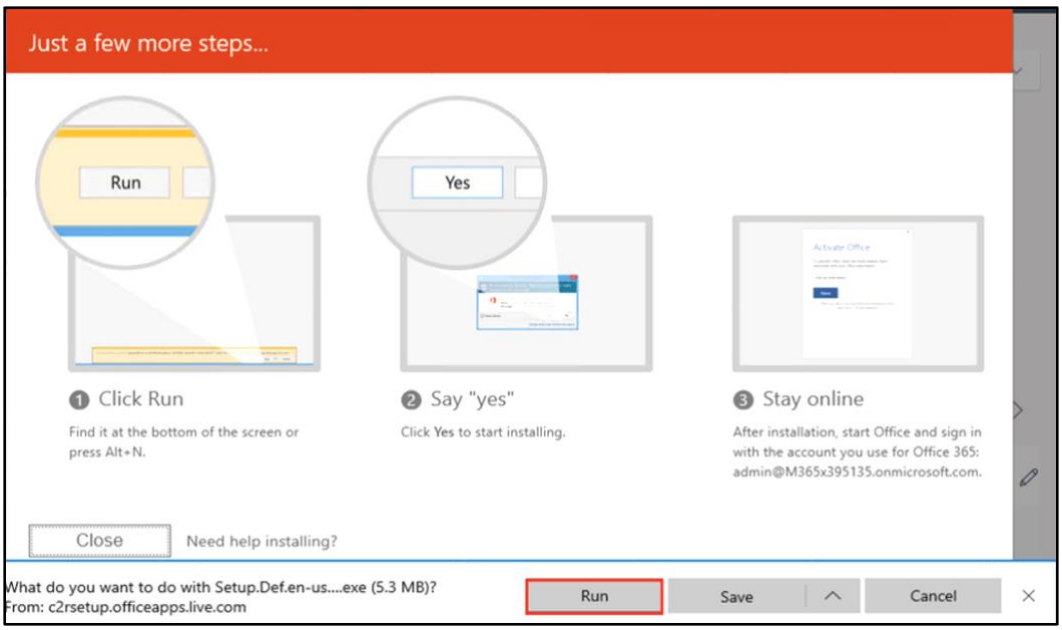
5.2 Installasjon av Office 365

I testmiljøet skal det simuleres kontrollerte angrep ved hjelp av **Microsoft Defender ATP Simulations and tutorials.** For å kjøre disse simulasjonene trenger man minst én maskin som er onboarded til Microsoft Defender ATP. Et av disse angrepene krever tilgang til Microsoft Word. Bildene nedenfor viser hvordan man installerer Microsoft Office 365, som inkluderer Outlook, OneDrive for Business, Word, Excel, PowerPoint, og mer.

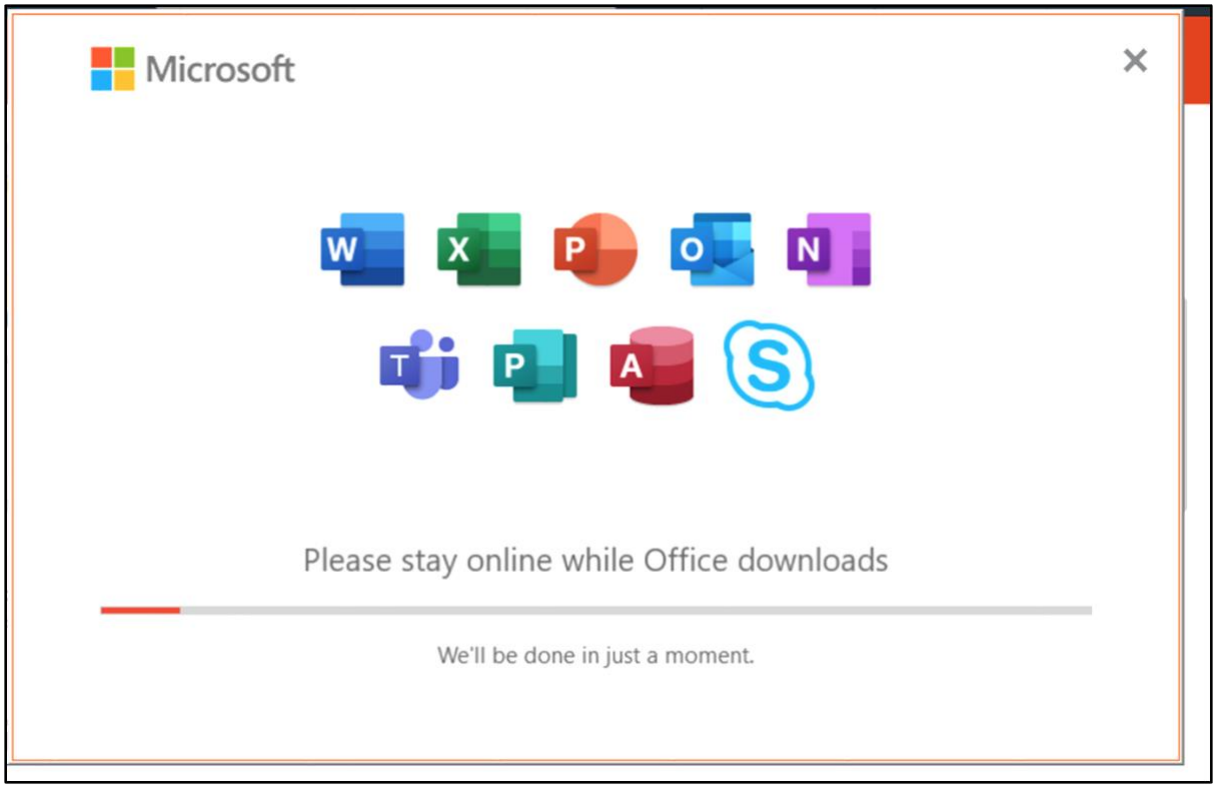
1. Gå inn i nettleseren på maskinen din. Logg inn på **office.com**. Under **Install Office**, velg **Office 365 apps**.



2. Velg **Run**



3. Vent på at installasjonen fullføres.

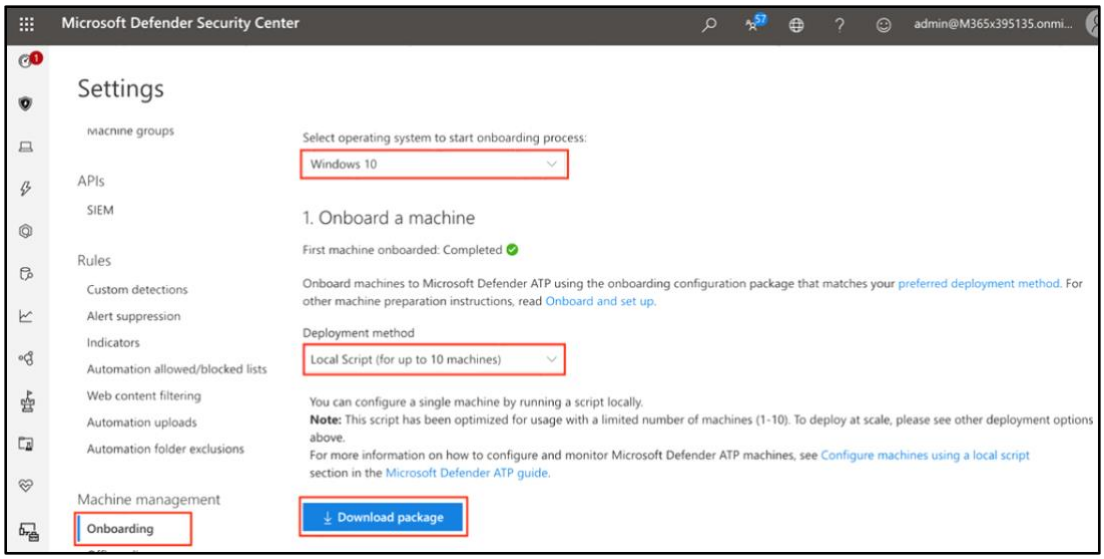


5.3 Microsoft Defender Advanced Threat Protection

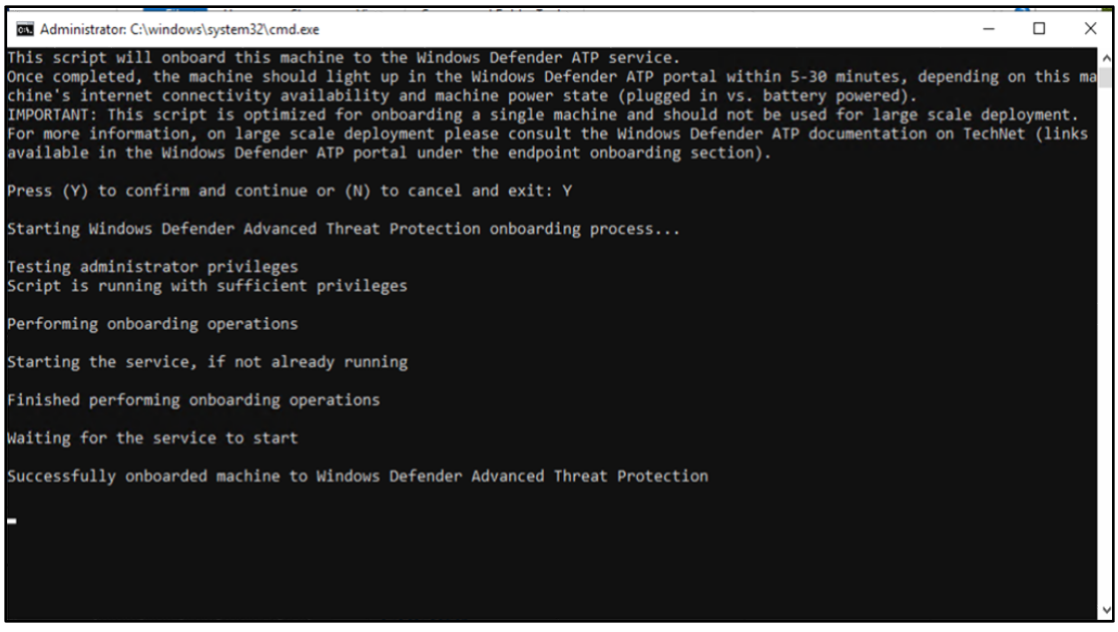
Det er også mulig å onboarde maskiner med andre operativsystemer for å ta i bruk Microsoft Defender ATP, eksempelvis Windows Server 2012 R2 og Windows Server 2016, eller tidligere versjoner av Windows. Man kan også benytte ikke-Windows-maskiner. Jeg har valgt å bruke Windows 10, hovedsakelig fordi dette er den enkleste måten å onboarde en maskin til Microsoft Defender ATP på.

5.3.1 Onboarding

1. Logg inn i Security Center. Gå til Settings, og velg **Onboarding** under **Machine management.** Velg **Windows 10** som operativsystem, og **Local Script** under **Deployment method**. Velg **Download package**.



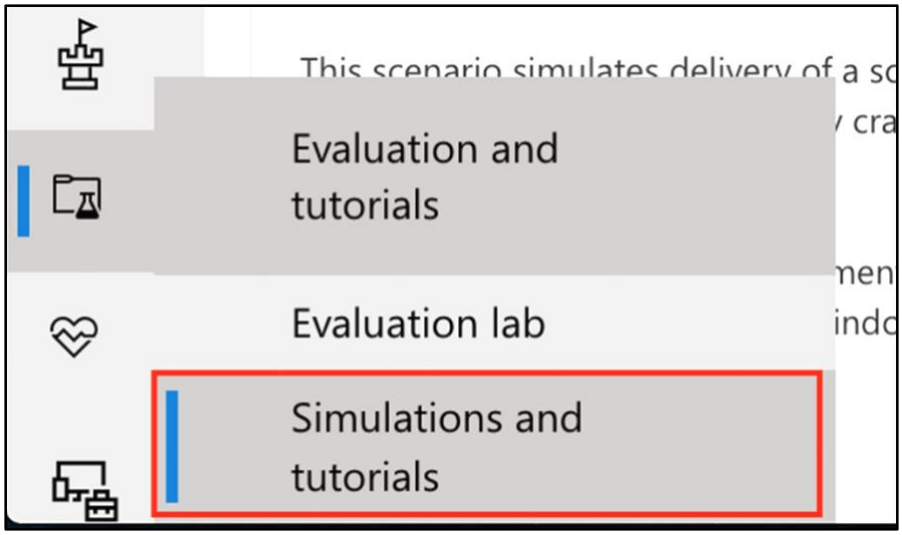
2. Kjør scriptet.



5.3.2 Simulations and tutorials

For å oppleve Microsoft Defender ATP i praksis, benyttes Microsoft Defender ATP simulations and tutorials. Det finnes flere scenarioer med angrep man kan kjøre. I dette prosjektet har jeg kjørt to scenarioer. Disse blir vist i veiledningen nedenfor. Alarmene som dukker opp i Microsoft Defender ATP vil vises som hendelser i Azure Sentinel etter at angrepene har blitt kjørt.

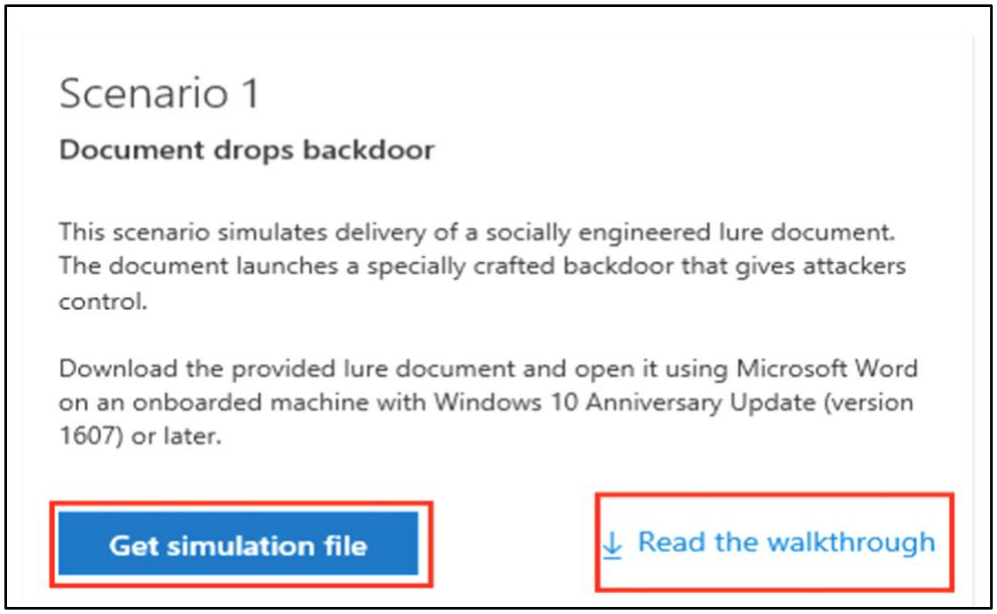
1. Velg **Simulations and tutorials** i menyen til venstre.



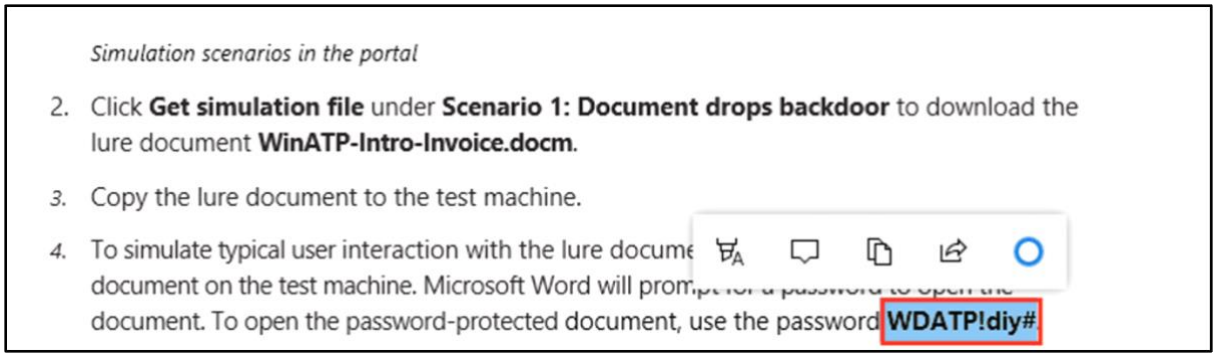
Scenario 1: Dokument åpner bakdør
Dette scenarioet simulerer leveringen av et sosialt konstruert lokkedokument. Dokumentet åpner en bakdør som gir angripere kontroll.

For å kjøre simulasjonen følg disse stegene:

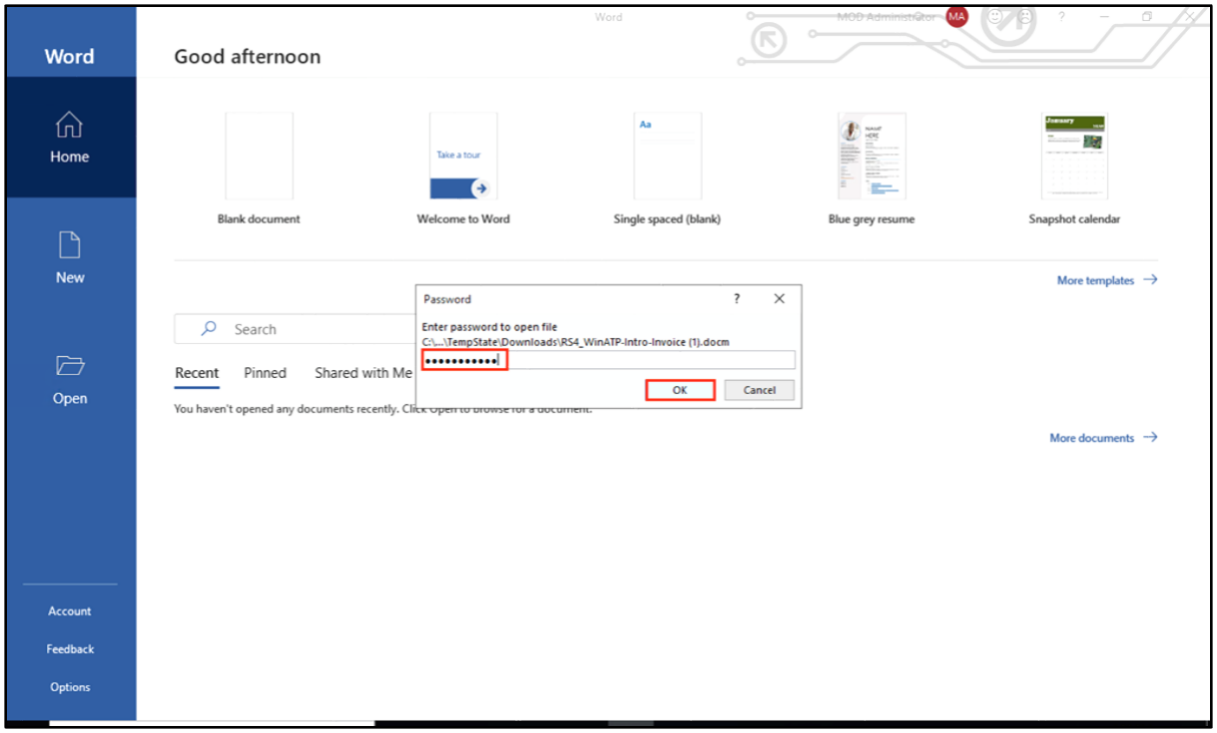
1. Last ned og les gjennomgangen. Velg deretter **Get simulation file**.



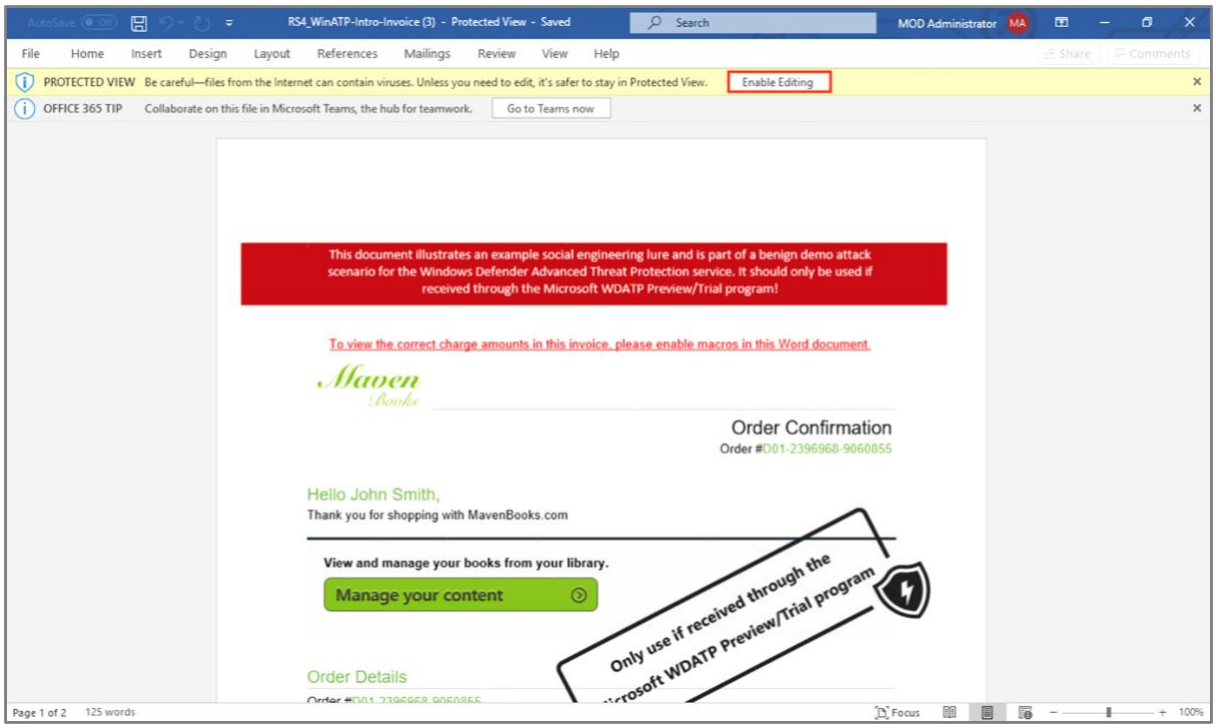
2. Kopier passordet fra gjennomgangsdokumentet.



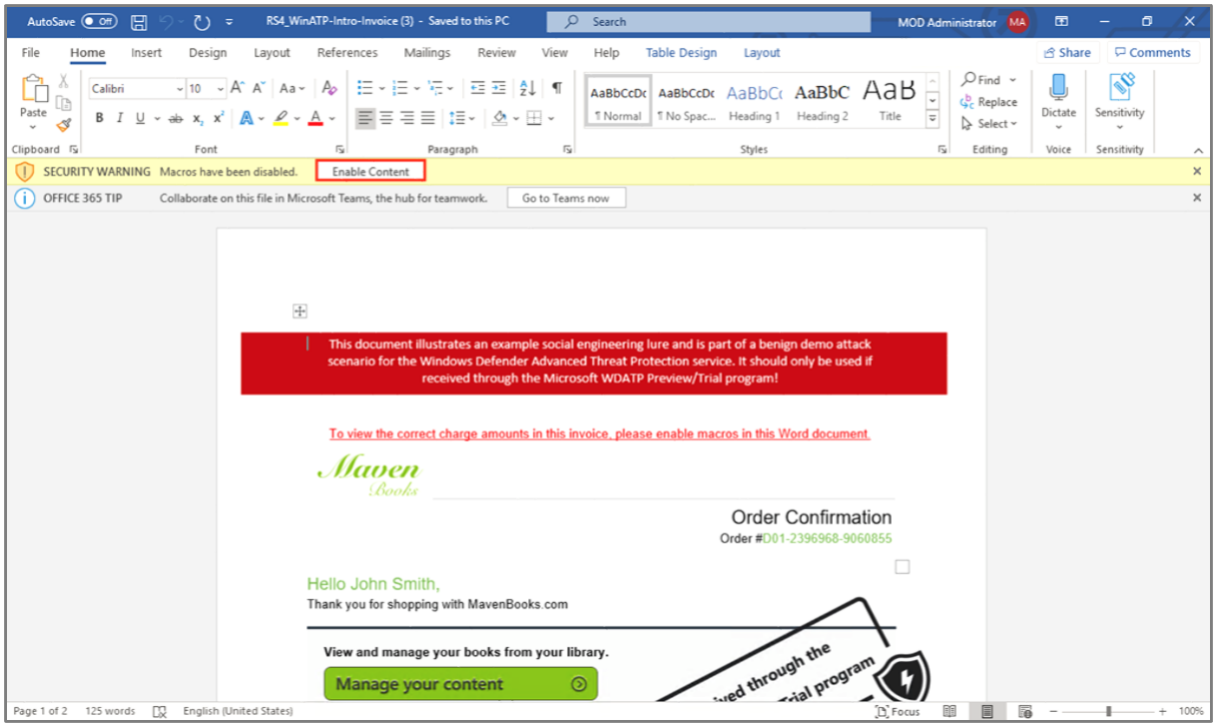
3. Skriv inn passordet, og trykk **OK** for å åpne filen.



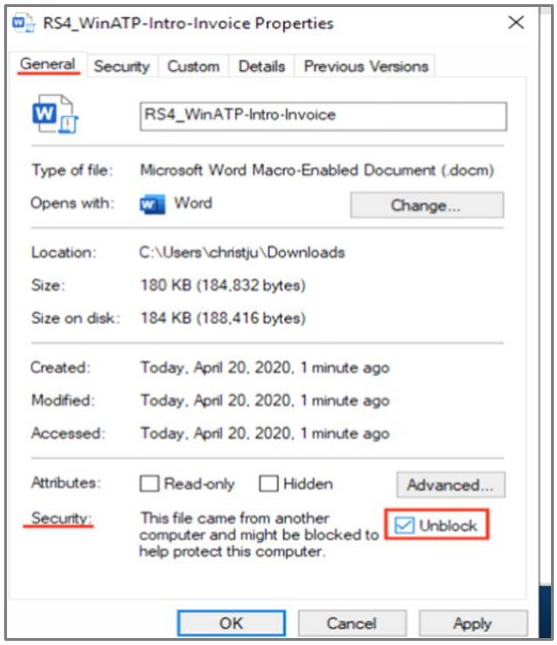
4. Hvis dokumentet åpnes i “Protected view”, velg **Enable Editing**.



5. Hvis du får et varsel om at makroer er deaktivert, velg **Enable Content**.

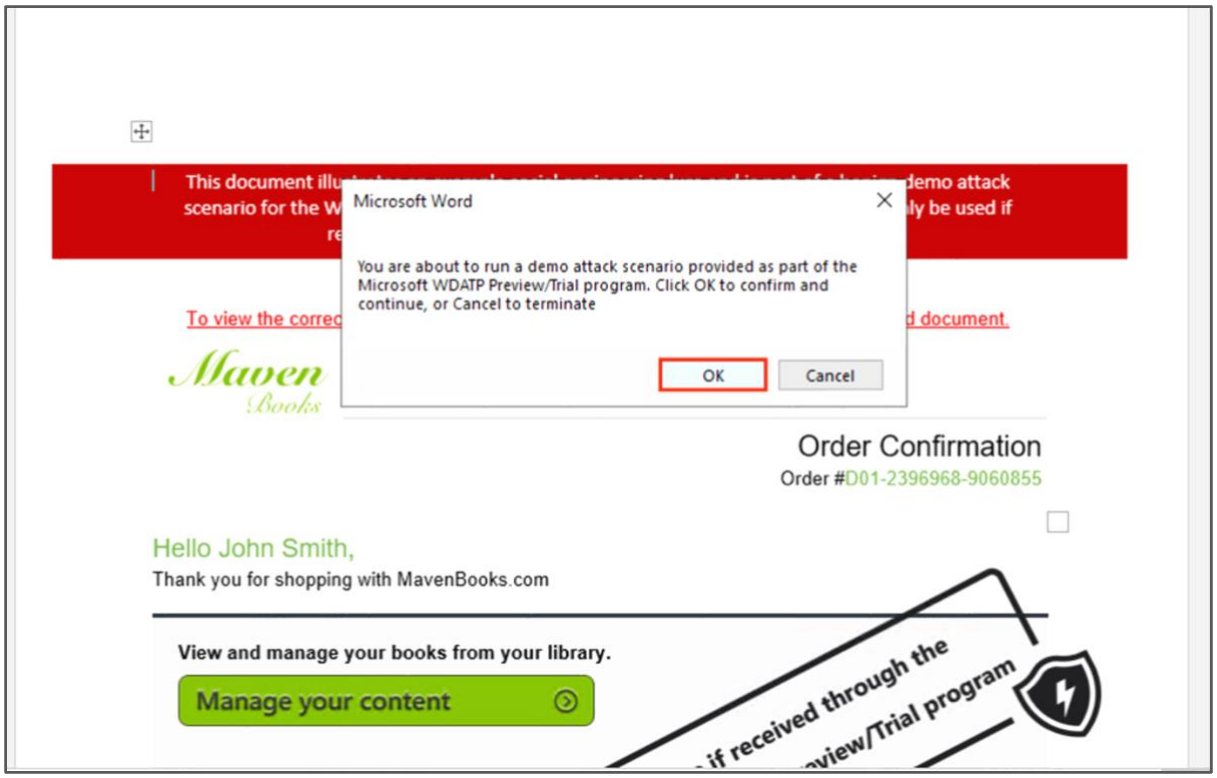


Merk: Hvis organisasjonen din blokkerer makroer i dokumenter fra internett, må du kanskje avblokkere dokumentet for at **Enable Content** skal fungere. For å gjøre dette gå til filens plassering i filutforsker. I filutforsker, høyreklikk på dokumentet, velg **Properties.** Under **General-**fanen, velg **Unblock** under **Security**:



Merk: Hvis du har tredjeparts sikkerhetsprodukter kan du støte på vanskeligheter. Det er anbefalt å bruke en onboarded testmaskin med standard Windows 10-konfigurasjon og Windows Defender AV skrudd på.

6. Velg **OK**.



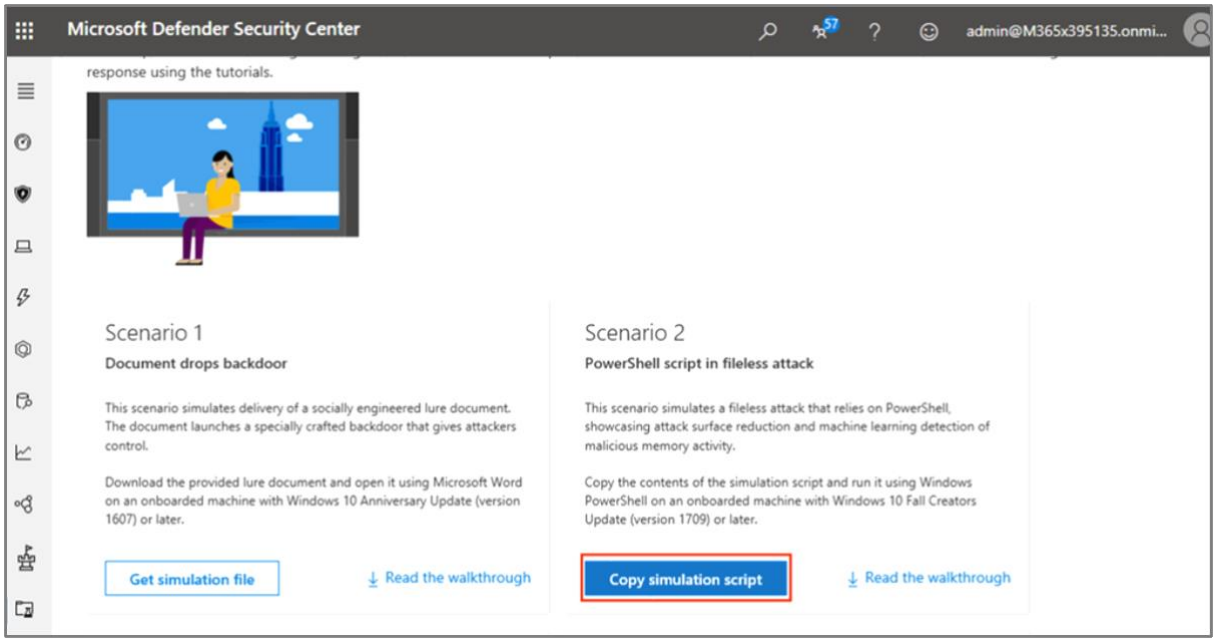
Scenario 2: Powershell-script i filløst angrep

Dette scenarioet simulerer et filløst angrep som starter med et PowerShell-script. Denne kategorien angrep inkluderer vanligvis ikke filer som dukker opp på offerets maskin, men forekommer utelukkende i minnet. Angrep som dette bruker kun eksisterende system- og administrative verktøy, og injiserer kode inn i systemprosesser for å skjule utførelsen. En bruker kan bli lurt til å kjøre et script som dette, eller scriptet kan bli kjørt eksternt fra en annen maskin i organisasjonen. Deteksjon av slike script er vanskelig fordi administratorer ofte kjører script eksternt på andre maskiner for å utføre diverse administrative oppgaver.

Under simulasjonen blir skallkode injisert i en prosess, i dette tilfellet *notepad.exe*. Reelle angripere vil mest sannsynlig velge en mer langvarig systemprosess, som for eksempel *svchost.exe*. Den injiserte skallkoden vil videre kontakte angriperens «command-and-control (C&C)»-server for å motta instruksjoner for hvordan den skal fortsette angrepet.

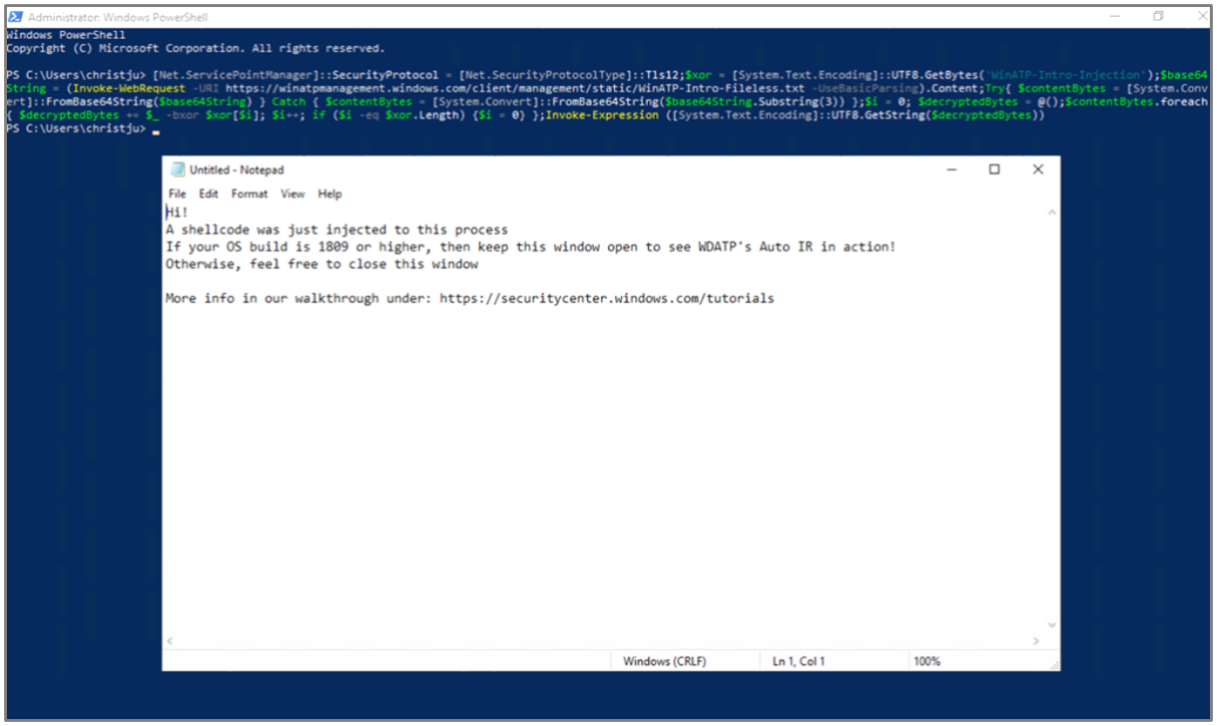
For å kjøre simulasjonen, følg disse stegene:

1. Velg **Copy simulation script**.



2. Åpne et Windows PowerShell-vindu med administrator-rettigheter.
3. Lim inn og kjør scriptet.

4. Et par sekunder senere starter *notepad.exe* og den simulerte angrepskoden blir injisert inn i prosessen.



6. Fase 3 - Azure Lighthouse

Merk: I veiledningen nedenfor demonstreres hvordan man kan onboarde én tenant til Azure Delegated Resource Manager. Denne prosessen kan gjentas for hver ny kunde som skal få sine ressurser administrert av en administrerende Azure-tenant.

6.1 Onboarding av kunde til Azure Delegated Resource Management

Før man begynner må man bestemme om man vil delegere rettigheter til en eller flere ressursgrupper, eller et helt abonnement. I dette prosjektet har det blitt delegert rettigheter til et helt abonnement. Dette betyr at den administrerende Azure-tenanten vil få de rettighetene som kunden bestemmer, til det abonnementet kunden velger å onboarde.

For å onboarde en kunde må kunden ha et aktivt Azure-abonnement. I tillegg må man ha «**tenant ID**»-en til den administrerende Azure-tenanten**.**

6.1.1 Definer roller og rettigheter

Som en bruker i en administrerende tenant er det kanskje ønskelig å ha muligheten til å utføre flere typer oppgaver for en enkelt kunde. Da trenger man ulike tilgangsrettigheter til de ulike type oppgavene. Azure sin rollebaserte tilgangskontroll (Role Based Access Control, eller RBAC) har flere innebygde roller man kan tildele brukere i sin tenant.

Det er anbefalt å bruke Azure AD-brukergrupper for hver rolle man vil tildele. På denne måten kan man legge til eller fjerne individuelle brukere til gruppen istedenfor å tildele rettigheter direkte til en bruker [5]. Det er viktig at brukere kun har de rettighetene som trengs for å utføre oppgaven, og ikke mer enn dette.

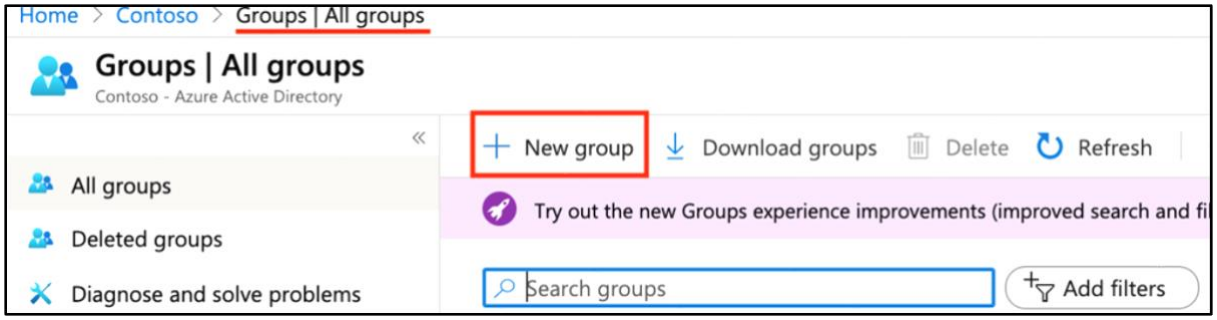
Viktig: For å legge til rettigheter for en Azure AD-brukergruppe må gruppen være av typen **Security**, ikke **Office 365**. Dette velger man når man oppretter gruppen [5].

For å definere autorisasjoner må man vite:

- **Object ID** til hver Azure AD-brukergruppe og bruker som skal få tilgangsrettigheter til kundens ressurser.
- «**Role definition ID**» for hver innebygget rolle som skal tildeles.

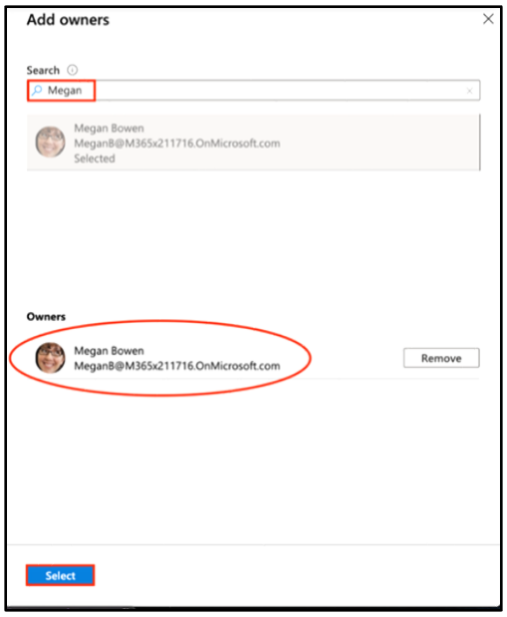
6.1.2 Opprette brukergruppe

2. Logg inn i Azure-portalen med en konto som er **Global administrator**.
2. Søk etter og velg **Azure Active Directory**.
2. Velg **Groups** og **New Group**.

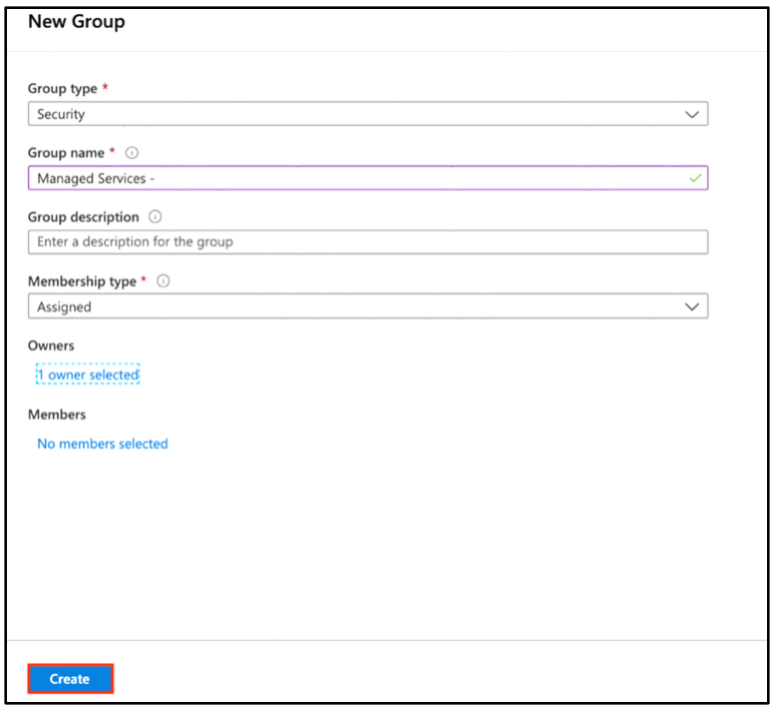


2. Fyll inn punktene under, og trykk på **No owners selected**.

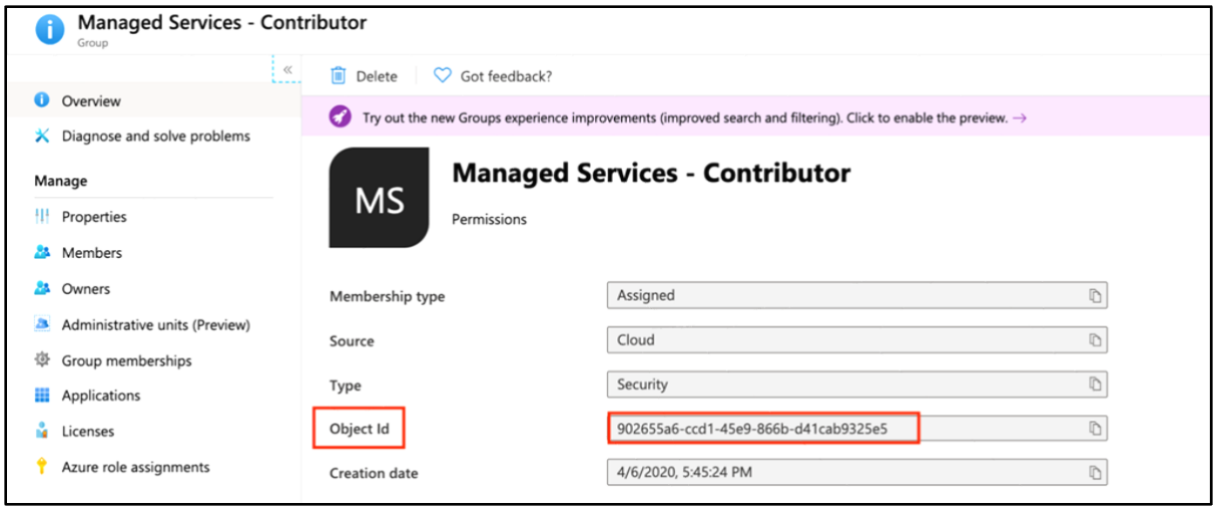
2. Velg en bruker som har rettigheten **Owner** i abonnementet, og velg **Select.**



2. Velg **Create**.



2. Inne i gruppen kan man finne **Object ID**. Denne trengs senere i gjennomgangen.



6.1.3 Opprette Azure Resource Manager template

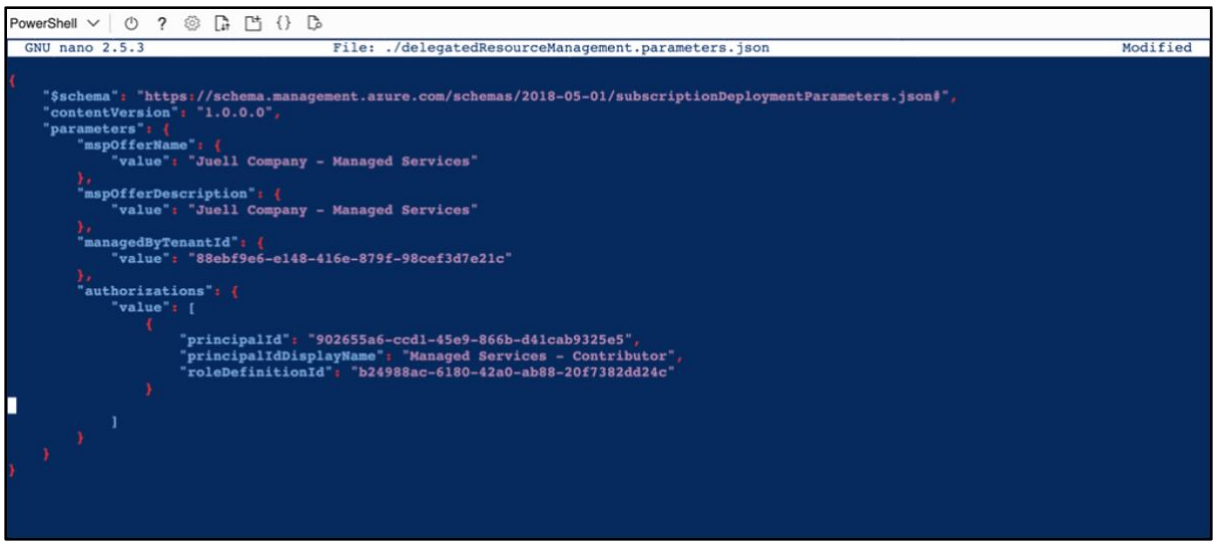
For å onboarde en kunde må man først opprette en «Azure Resource Mangager template». Dette er en mal som inneholder følgende informasjon [5]:

Felt	**Definisjon**
mspOffername	Dette er navnet på tjenesten som blir tilbudt.
mspOfferDescription	Beskrivelse av tjenesten.
managedByTenantId	Din tenant-ID.
authorizations	**PrincipalId (Object ID)** fra gruppen i din tenant. Under dette feltet er det også et **principalDidsplayName** (f.eks «Contributor»), som beskriver meningen med autorisasjonen. Til slutt kommer verdien **roleDefinitionId**, for å spesifisere aksessnivå. Dette er id-en til den innebygde rollen som gis til gruppen.

Prosessen krever altså en «Azure Resource Manager template». En slik mal kan man finne i Github, hvor Microsoft har et bibliotek med forskjellige maler [6]. I malen finnes en rekke ulike filer, hvorav en er en parameterfil. Denne filen må endres for å passe til din konfigurasjon, samt for å definere autorisasjoner.

For å onboarde:	**Bruk denne malen:**	**Endre denne parameterfilen:**
Abonnement	delegatedResourceManagement.json	delegatedResourceManagement.parameters.json

1. Oppdater parameterfilen med informasjonen ovenfor.



2. Nå må vi «deploye» malen i kundens tenant på abonnementet vi ønsker å onboarde. Dette kan kun gjøres av en identitet med eier-rettigheter på abonnementet, og det kan ikke gjøres av en gjestekonto.

   Logget inn som en bruker med eier-rettigheter på abonnementet i kunde-tenanten, kjør denne kommandoen i PowerShell:

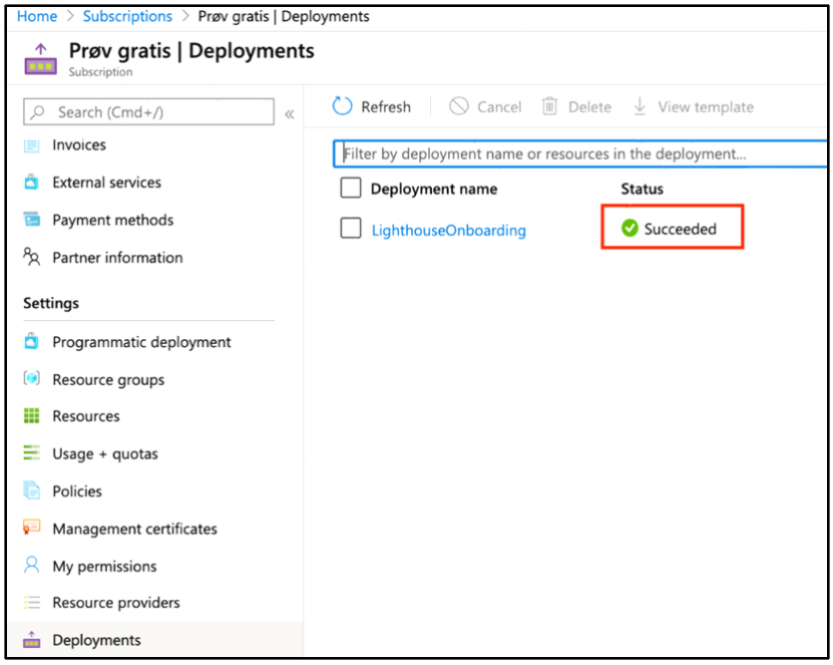
```
az deployment sub create --name LighthouseOnboarding --location westeurope --template-file
delegatedResourceManagement.json --parameters delegatedResourceManagement.parameters.json
```

6.1.4 Bekreft vellykket onboarding

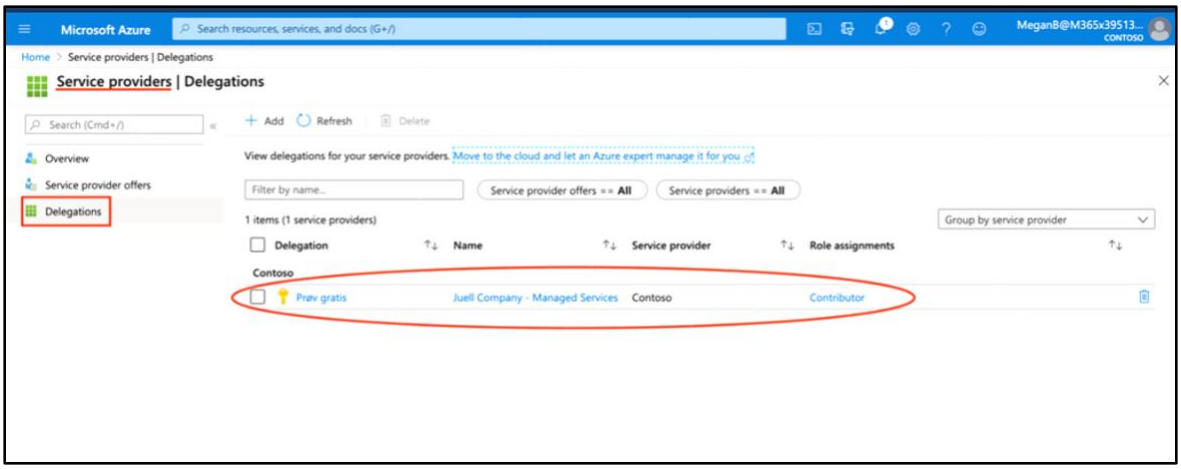
Når et kunde-abonnement har blitt onboardet til Azure Delegated Resource Mangement suksessfullt, kan brukere i den administrerende Azure-tenanten se abonnementet og ressursene hvis de har fått tilgang ved å være medlem av gruppen vi opprettet tidligere [5].

I kunde-tenant:

1. Logget inn som kunden, ser vi at "onboardingen" var en suksess.

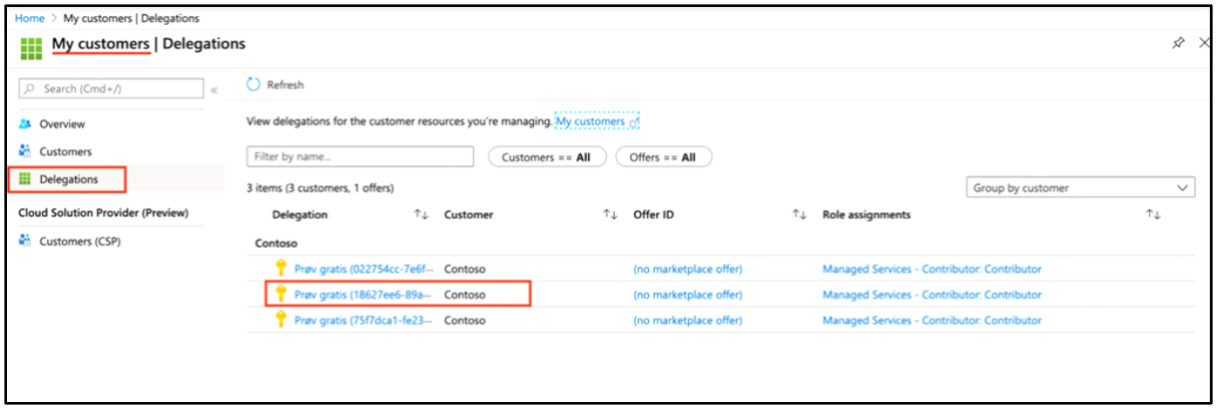


2. Gå til **Service Providers**. Her ser du delegasjonen du nettopp har gitt.

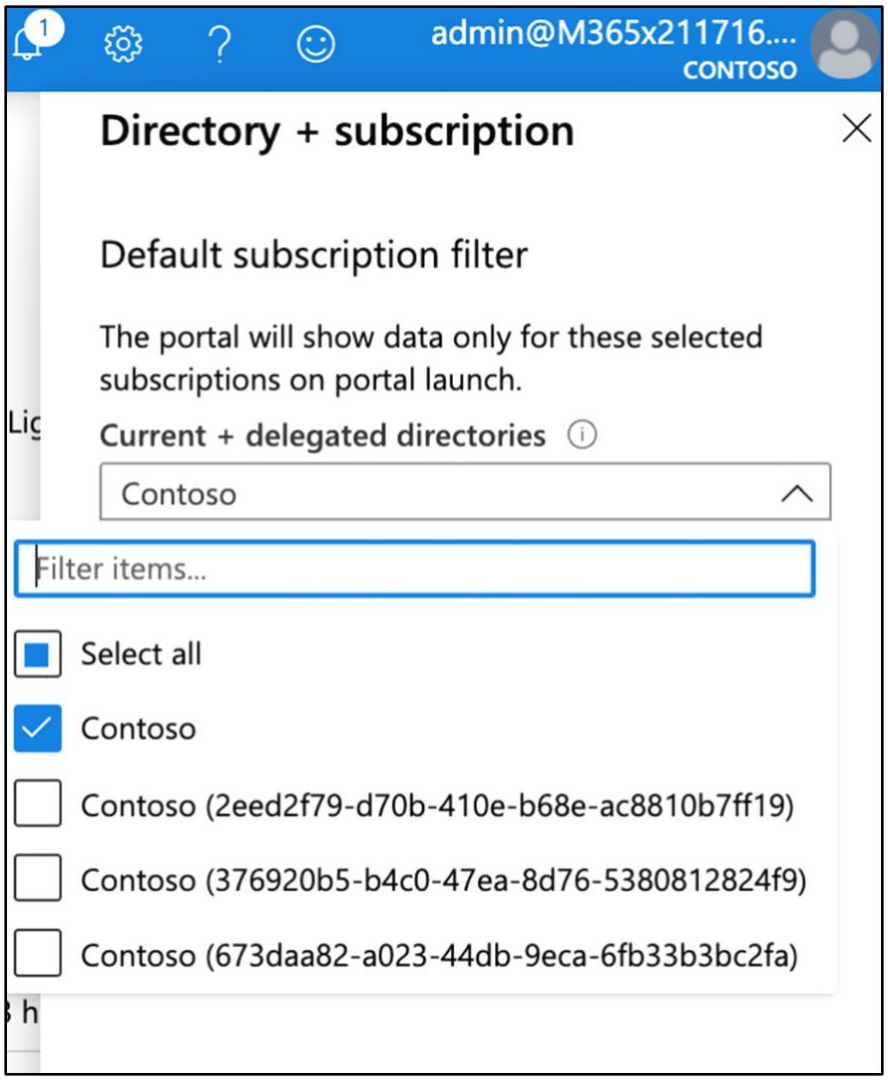


I administrerende tenant:

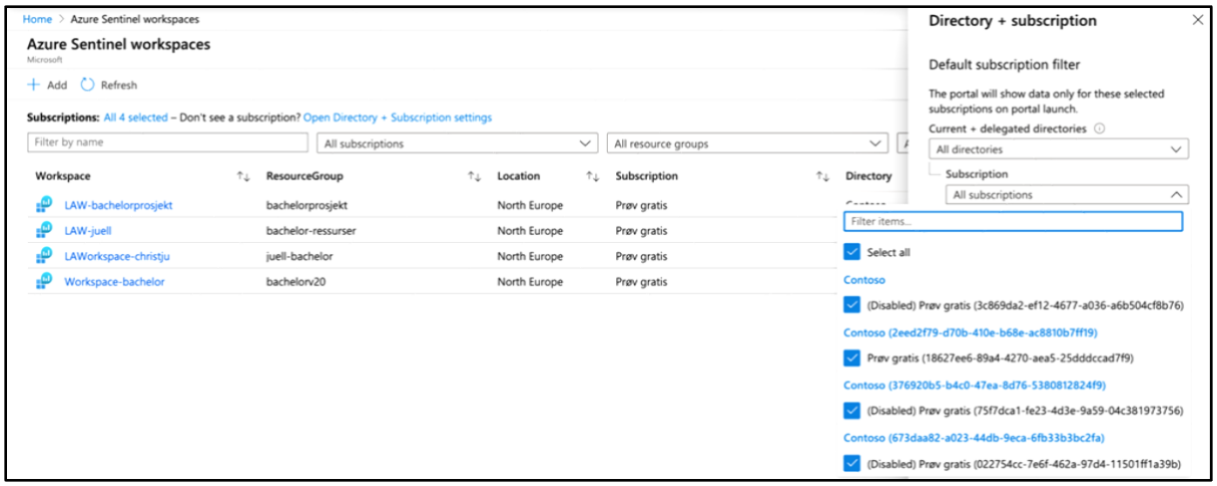
1. Logget inn som brukeren som ble lagt til i gruppen vi opprettet tidligere, gå til **All Services > My Customers**. Her ser du den nye kunden og delegasjonen som ble tildelt.



2. Klikk på identiteten din øverst i høyre hjørne > **Switch directory**, og legg merke til at du nå kan velge flere «directories», og dermed flere abonnement.



3. Når du har valgt abonnement fra listen over, kan du jobbe med kundens ressurser fra den administrerende Azure-tenanten. Jeg har gjort denne onboarding-prosessen med tre forskjellige Azure-tenanter, og kan dermed velge å jobbe med ressurser som tilhører alle tre kunder, alt fra én enkelt Azure-portal. Et eksempel er Azure Sentinel. Jeg kan nå aksessere hver enkelt kunde sitt Azure Sentinel-arbeidsområde fra egen portal i Azure.

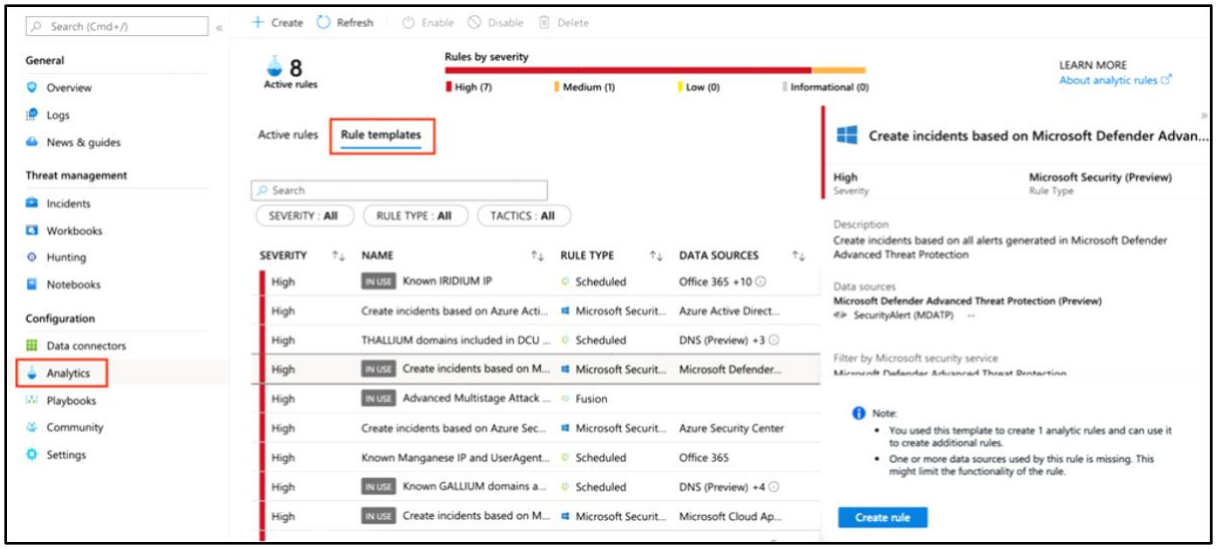


7. Fase 4 - Hendelseshåndtering og arbeid på tvers av kunder i Azure Sentinel

7.1 Bruk av innebygde regler for trusseldeteksjon

Etter at man har koblet til datakildene i Azure Sentinel ønsker man gjerne å bli varslet dersom noe mistenkelig skjer. For å muliggjøre dette tilbyr Azure Sentinel innebygde maler for opprettelse av regler. Etter å ha aktivert en slik mal, vil den automatisk søke etter aktivitet som virker mistenkelig på tvers av ditt miljø. Alarmene som blir generert av disse malene vil opprette hendelser som man kan tildele brukere og undersøke nærmere.

Under **Analytics** og **Rule templates** finner man alle malene for innebygde regler i Azure Sentinel.

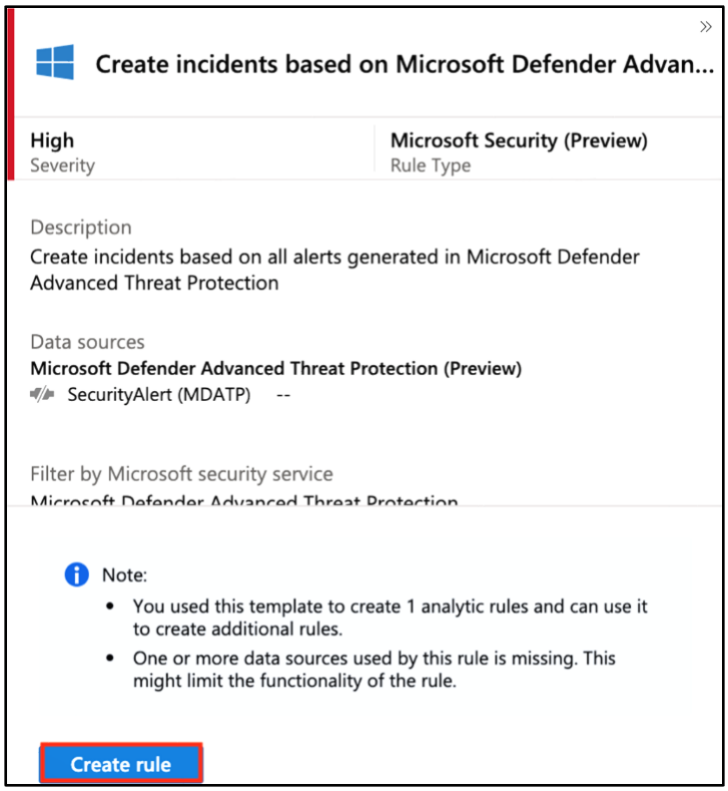


Følgende typer maler for regler er tilgjengelige:

- **Microsoft Security** – Microsoft Security-maler oppretter hendelser automatisk fra alarmer som har blitt generert i andre Microsoft Security-løsninger. Man kan bruke Microsoft Security-regler som mal til å opprette nye regler med lignende logikk [7].
- **Fusion** – Bruker maskinlæringsalgoritmer som kombinerer informasjon fra diverse alarmer for å generere alarmer om ting som ellers kan være veldig vanskelig å oppdage [8]. Dette kan være veldig nyttig, da noen alarmer med lavere alvorlighetsgrad kanskje ikke betyr mye hvis man ser på dem hver for seg, men kombinert kan de indikere et mye større problem.
- **Machine learning behavioral analytics** – Disse malene er basert på Microsofts egne maskinlæringsalgoritmer. Dette betyr at man ikke kan se den interne logikken bak hvordan reglene fungerer eller når de kjører, og man kan derfor ikke bruke dette som en mal til å lage mer enn én regel [7].

- **Scheduled** – Denne typen regler er planlagte spørringer skrevet av sikkerhetseksperter i Microsoft. Her kan du se spørringslogikken, og utføre endringer til den. Man kan bruke disse reglene som mal til å lage nye regler med lignende logikk [7].

1. For å opprette en regel, klikk på **Create rule**.



2. Dette åpner en «wizard» for opprettelse av regler, basert på den valgte malen. Alle detaljene er fylt ut automatisk, og for både **Scheduled**- og **Microsoft security**-regler kan man tilpasse regellogikken til å bedre passe din organisasjon. Man kan også legge til ytterligere regler basert på den innebygde malen. Etter å ha fulgt stegene i «wizarden» og fått opprettet en regel basert på malen, vil den nye regelen dukke opp under **Active rules**.

Merk: I fase 1, under «Azure Sentinel onboarding», opprettet jeg en regel som genererer hendelser i Azure Sentinel basert på alarmer fra Microsoft Defender ATP. Denne var av typen Microsoft Security, og er nødvendig for å få generert hendelser som dukker opp i Azure Sentinel. Regelen er den samme som på bildet ovenfor.

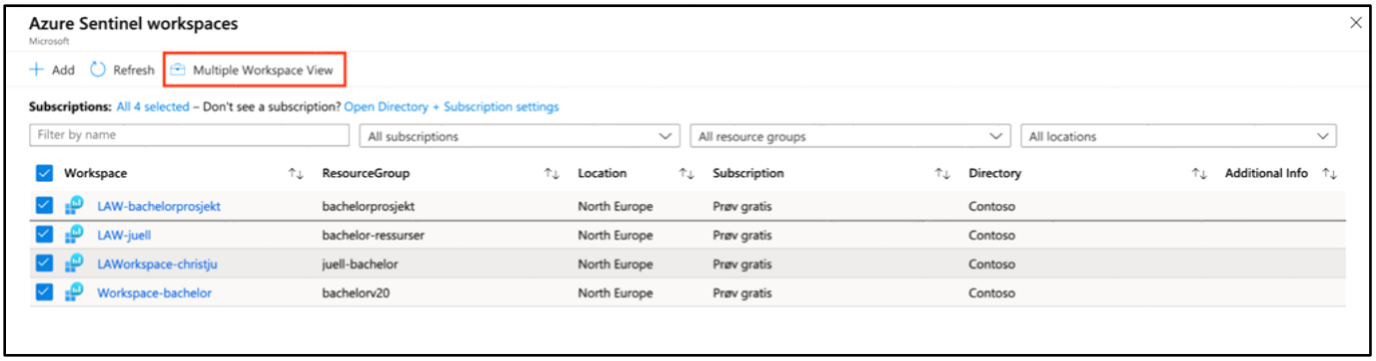
Merk: Det er også mulig å opprette egendefinerte regler som søker etter spesifikke kriterier på tvers av ditt miljø, og genererer hendelser når kriteriene er samsvarende.

7.2 Hendelseshåndtering på tvers av Sentinel-arbeidsområder

Multiple Workspace View lar deg se og jobbe med sikkerhetshendelser på tvers av flere Azure Sentinel-arbeidsområder samtidig. Dette gjelder også om arbeidsområdene er på tvers av Azure-tenanter [9].

7.2.1 Åpne **Multiple Workspace View**

Når man åpner Azure Sentinel blir man presentert med en liste over de forskjellige arbeidsområdene som man har tilgangsrettigheter til, på tvers av alle valgte Azure-tenanter og abonnement. Ved å klikke på navnet til et enkelt arbeidsområde kommer du inn i det arbeidsområdet. For å velge flere arbeidsområder, klikk på alle de tilhørende avkrysningsrutene, og velg **Multiple Workspace View** øverst på siden.

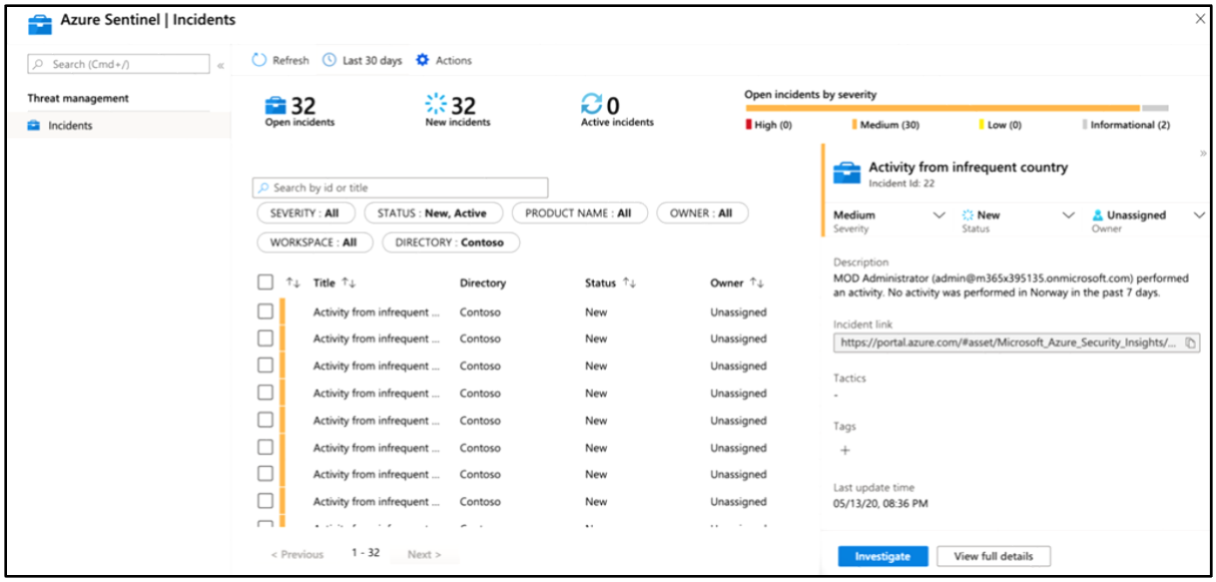


Merk at man i listen over de forskjellige arbeidsområdene kan se «Directory», «Subscription», «Location» og «Resource Group», som er assosiert med hvert enkelt arbeidsområde. «Directory» tilsvarer Azure-tenanten.

Viktig: Multiple Workspace View støtter for øyeblikket maksimalt 10 arbeidsområder som vises samtidig [9].

7.2.2 Jobbe med hendelser i **Multiple Workspace View**

I **Multiple Workspace View** er det foreløpig kun **Incidents**-siden som er tilgjengelig. Den ser ut som og fungerer som den vanlige **Incidents**-siden. Det er imidlertid noen viktige forskjeller [9]:



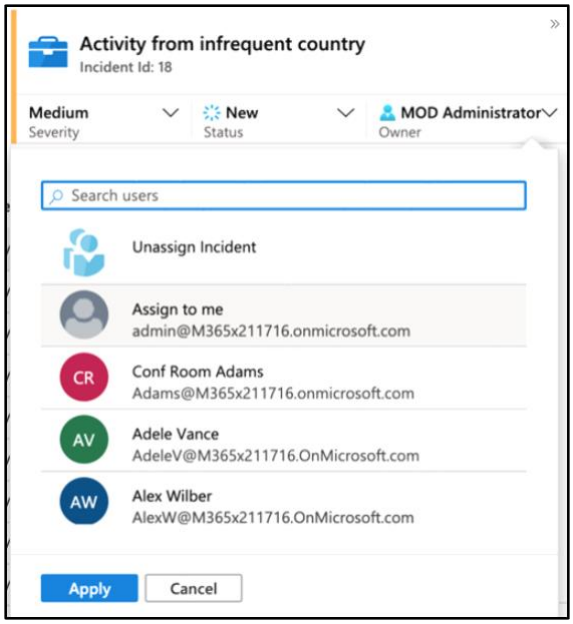
- Tellerne øverst på siden – «**Open incidents**», «**New incidents**» og «**Active incidents**», viser tallene for alle de valgte arbeidsområdene samlet sett.
- Hendelsene fra de valgte arbeidsområdene og katalogene (Azure-tenantene) vises i en samlet liste. Man kan filtrere listen etter arbeidsområde («WORKSPACE») og katalog («DIRECTORY»), i tillegg til filtrene fra den vanlige **Incidents**-siden.
- Du må ha lese- og skriverettigheter på alle arbeidsområdene du har valgt hendelser fra. Hvis du kun har leserettigheter på noen av arbeidsområdene, vil du få advarsler hvis du velger hendelser i de arbeidsområdene. Du vil ikke kunne gjøre endringer på hendelsene eller andre hendelser du har valgt sammen med disse (selv om du har tillatelser for de andre).
- Hvis du velger en enkelt hendelse og klikker på **View full details** eller **Investigate**, vil du fra da av være i datasammenheng for den hendelsens arbeidsområde, og ingen andre.

Merk: Under **Directory** er alle navnene like (Contoso). Dette er fordi alle demo-kontoene man oppretter gjennom Microsoft får dette navnet. I realiteten vil det stå navnet på organisasjonen man administrerer ressurser for. Bildet over viser altså hendelser for fire forskjellige Azure-tenanter (inkludert tenantadministrator), og ikke for én enkelt Azure-tenant.

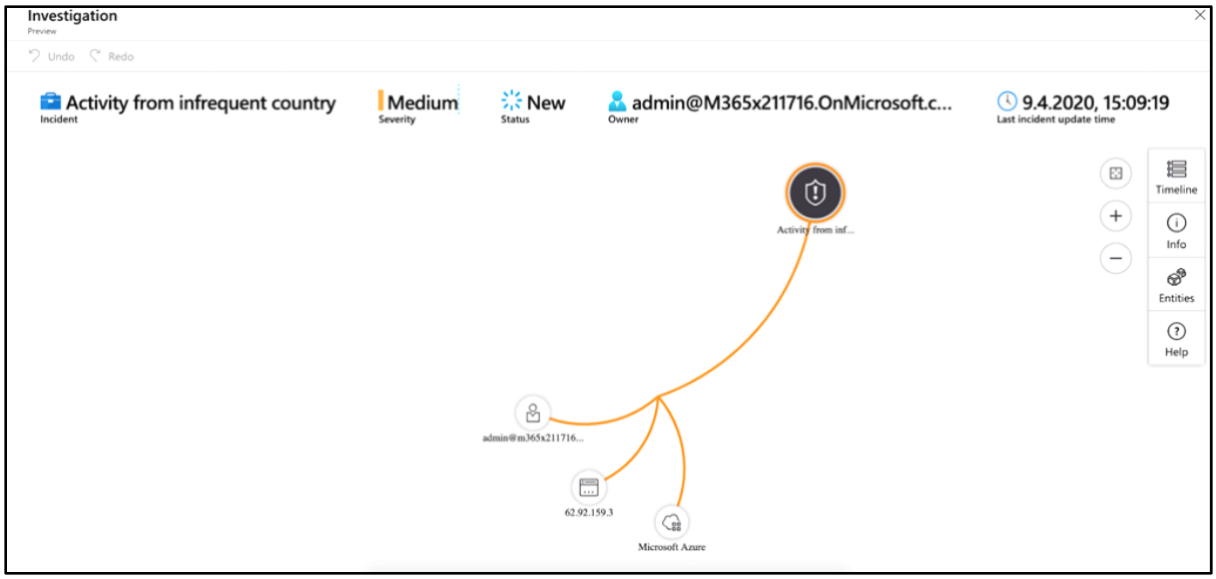
7.2.2.1 Hvordan undersøke hendelsene nærmere

Hendelser kan undersøkes nærmere ved å velge en spesifikk hendelse. Til høyre for hendelsen ser man detaljert informasjon om hendelsen, inkludert alvorlighetsgrad, antall enheter involvert i hendelsen, de rå hendelsene som utløste denne hendelsen, og hendelsens unike ID. Hvis man vil ha flere detaljer rundt hendelsen, kan man trykke på "**View full details**".

Hendelser kan tildeles spesifikke brukere. For hver hendelse kan du tildele en "eier":



Alle hendelser starter uten en eier. Man kan også legge til kommentarer, slik at andre analytikere kan skjønne hva du har undersøkt, og hva dine bekymringer rundt hendelsen er. Ved å velge "**Investigate**" blir man navigert til et utredningskart. Utredningskartet hjelper med å forstå omfanget og identifisere hovedårsaken til en potensiell sikkerhetstrussel ved å samkjøre relevant data med enhver involvert enhet.



Merk: Siden det kun er **Incidents**-siden som for øyeblikket er tilgjengelig i **Mulitple Workspace View**, har jeg valgt å unnlate å vise hvordan man kan opprette **Playbooks** for å svare på trusler i Azure Sentinel. **Playbooks** kan kun opprettes inne i hvert enkelt arbeidsområde, og i denne oppgaven har det blitt fokusert på arbeid på tvers av arbeidsområder og Azure-tenanter.

7.3 Flere muligheter for å arbeide på tvers av kunder i Azure Sentinel

7.3.1 Søk på tvers av kunder

De fleste funksjoner i Azure Sentinel er foreløpig knyttet til ett enkelt arbeidsområde. Men det er derimot mulig å kjøre spørringer på tvers av arbeidsområder for å undersøke og jakte på trusler som kan ha innvirkning på flere Azure-tenanter på en gang. For å gjøre dette kan man bruke «*union*»-operatøren for å slå sammen en tabell fra et arbeidsområde med en annen. For eksempel, hvis du ønsker å se en liste over alle sikkerhetsalarmer fra forrige uke fra to arbeidsområder, ville du brukt følgende spørring [10]:

```
union SecurityAlert, workspace('<Second Workspace Name>').SecurityAlert
| where TimeGenerated > ago(7d)
```

Dette kan også utvides til et hvilket som helst antall arbeidsområder, bare ved å legge til flere arbeidsområder i «*union*»-spørringen:

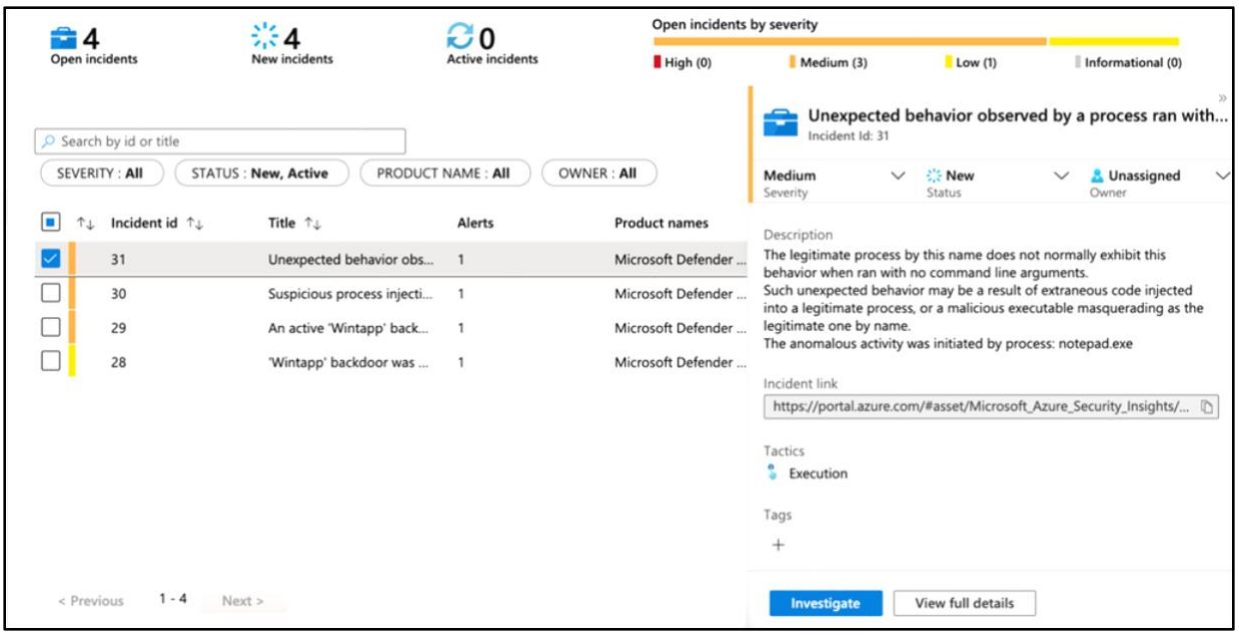
```
union SecurityAlert, workspace('<Second Workspace Name>').SecurityAlert, workspace('<Third Workspace Name>').SecurityAlert
| where TimeGenerated > ago(7d)
```

Resultatet vil vises i en enkelt tabell, men du kan identifisere hvilken kunde hvert punkt kommer fra ved hjelp av «**TenantId**»-feltet.

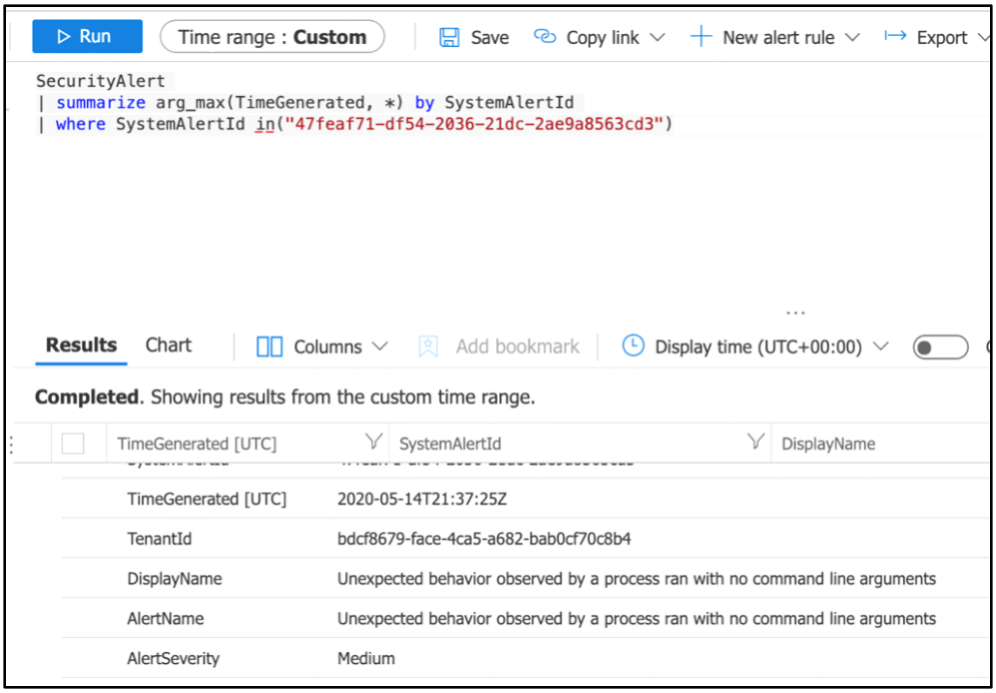
7.3.1.2 Sporing av et angrep på tvers av flere kunder

Et overvåkningsteam som overvåker for flere kunder kan oppleve at mistenksom aktivitet påvirker flere Azure-tenanter samtidig. I dette eksempelet skal vi se på hvordan man kan kjøre søk etter trusler på tvers av Azure-tenanter. I fase 2, i et testmiljø, kjørte vi simulerte angrep i Microsoft Defender ATP. Dette resulterte i flere hendelser som dukket opp i Azure Sentinel, som et resultat av alarmer generert i Microsoft Defender ATP.

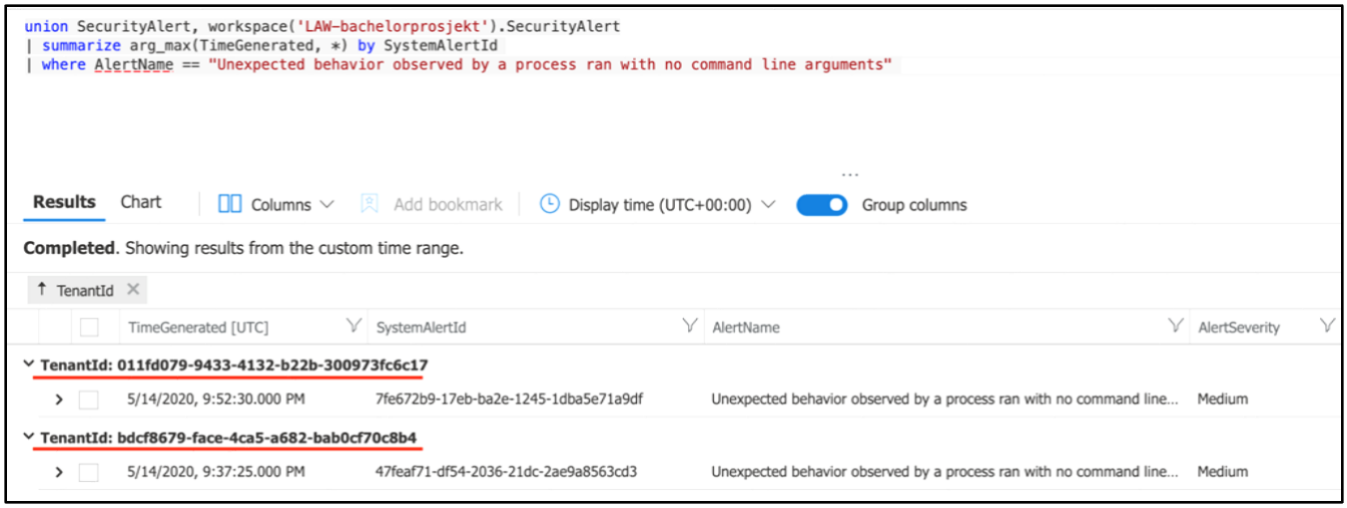
Vi kan starte med å se på en av hendelsene som kom som et resultat av et filløst angrep i testmiljøet:



Hvis vi ser nærmere på loggen kan vi få mer informasjon om angrepet:



Dersom man som tenantadministrator mistenker at et lignende angrep har skjedd hos en av kundene sine, kan man kjøre et søk på tvers av kunden/kundene også:



Spørringen over søker etter hendelser med samme navn som hendelsen som dukket opp i Azure Sentinel-arbeidsområdet til tenantadministratoren. Den søker i arbeidsområdet til både tenantadministratoren og en av kundene. Resultatet av spørringen viser at samme hendelse har dukket opp hos kunden også.

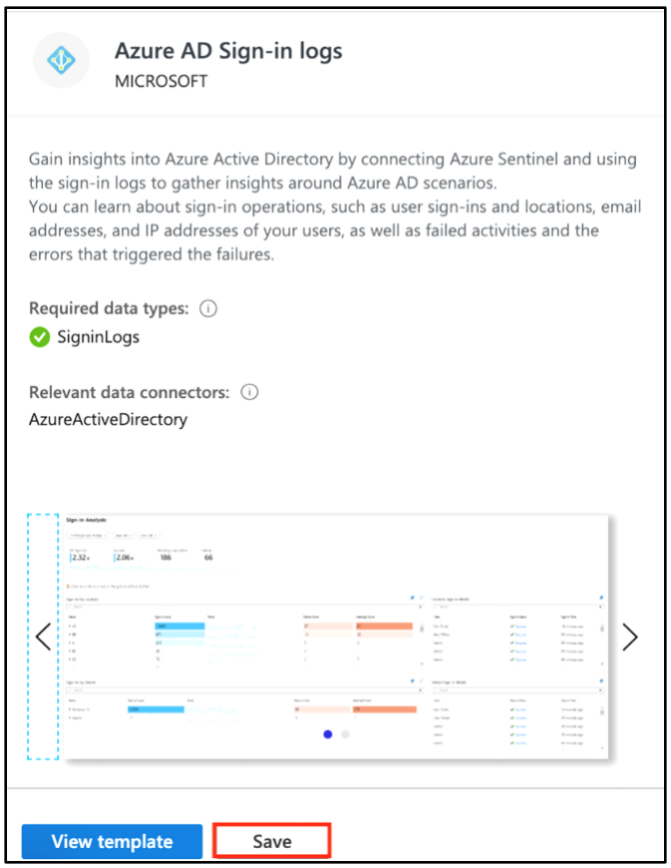
7.3.2 Multi-tenant workbooks

Som tenantadministrator er det en fordel om man kan få en samlet oversikt over sine kunders miljøer, istedenfor å måtte forholde seg til mange forskjellige oversikter. I dette kapittelet skal jeg forklare hvordan man kan opprette «multi-tenant workbooks», slik at man kan få en samlet oversikt over sine Sentinel-arbeidsområder, uansett om de er innenfor samme Azure-tenant eller ikke.

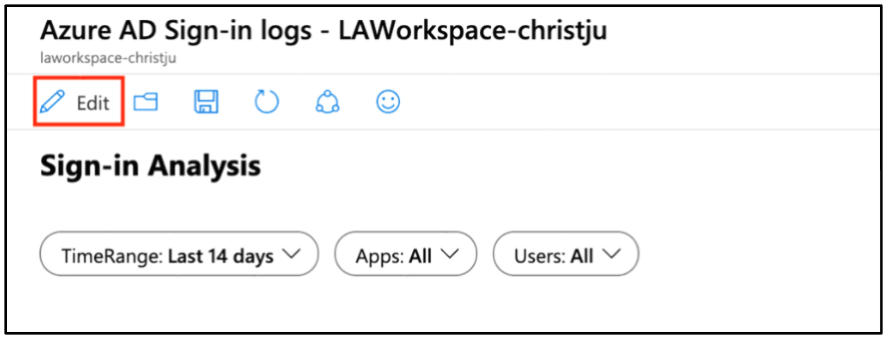
Det er mange innebygde «workbooks» som følger med når man installerer Azure-Sentinel, men disse ble laget for å jobbe med data som kommer fra ett enkelt Log Analytics-arbeidsområde. Derfor må de tilpasses til et «multi-tenant»-scenario [11].

7.3.2.1 Endring av eksisterende workbook

1. I Sentinel, under **Workbooks > Templates**, velg en eksisterende workbook, eksempelvis «Azure AD Sign-in logs». Hvis du ikke allerede har gjort det, velg **Save** (du vil bli spurt om å velge en lokasjon for den lagrede «workbooken»).

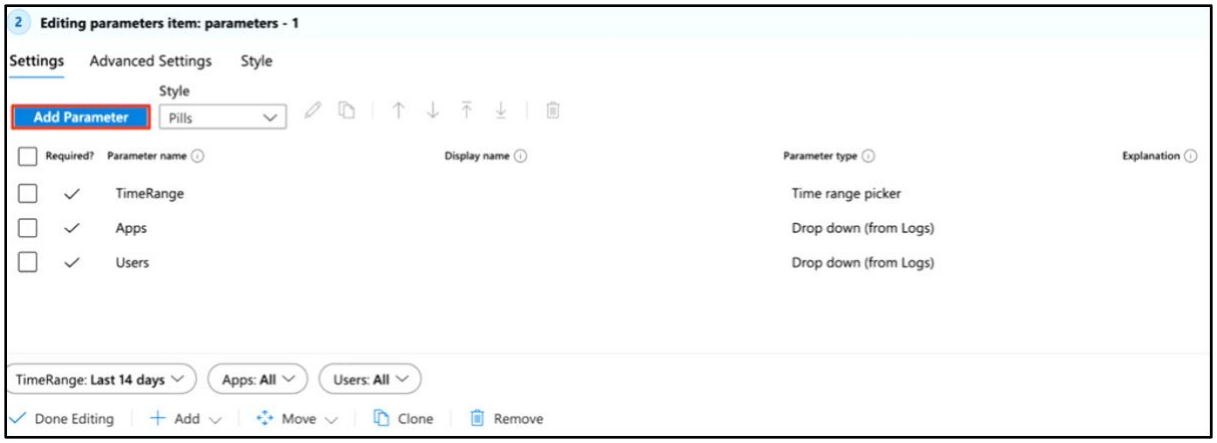


2. Nå som den er lagret, velg **View saved workbook**. Inne i «workbooken», velg **Edit** øverst til venstre.

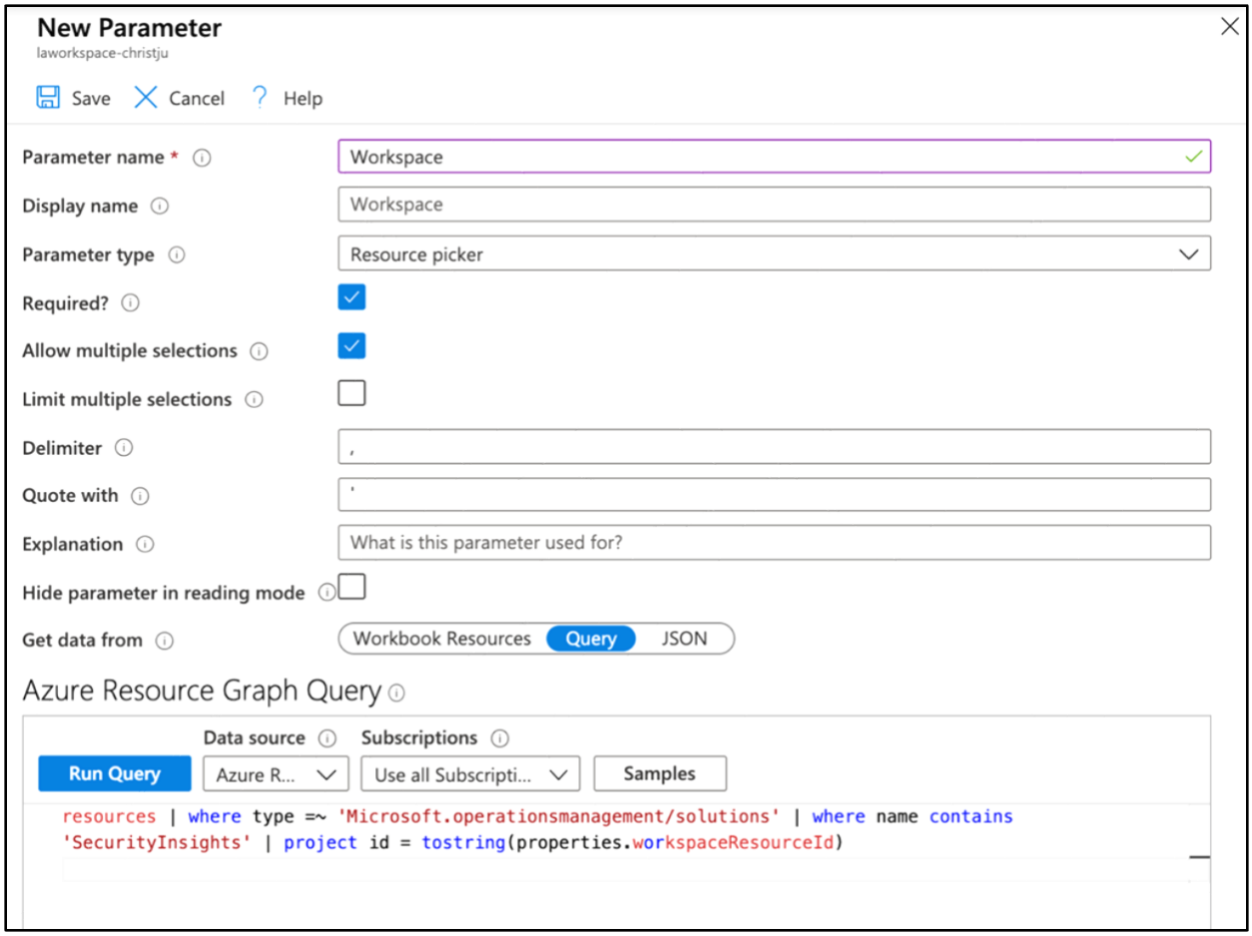


3. Nå skal vi legge til en ny paramater, som vil fungere som en «drop down»-meny for arbeidsområder (kunder). Velg **Edit** under den første raden med «drop down»-menyer, som vist under:

4. Velg **Add Parameter**.

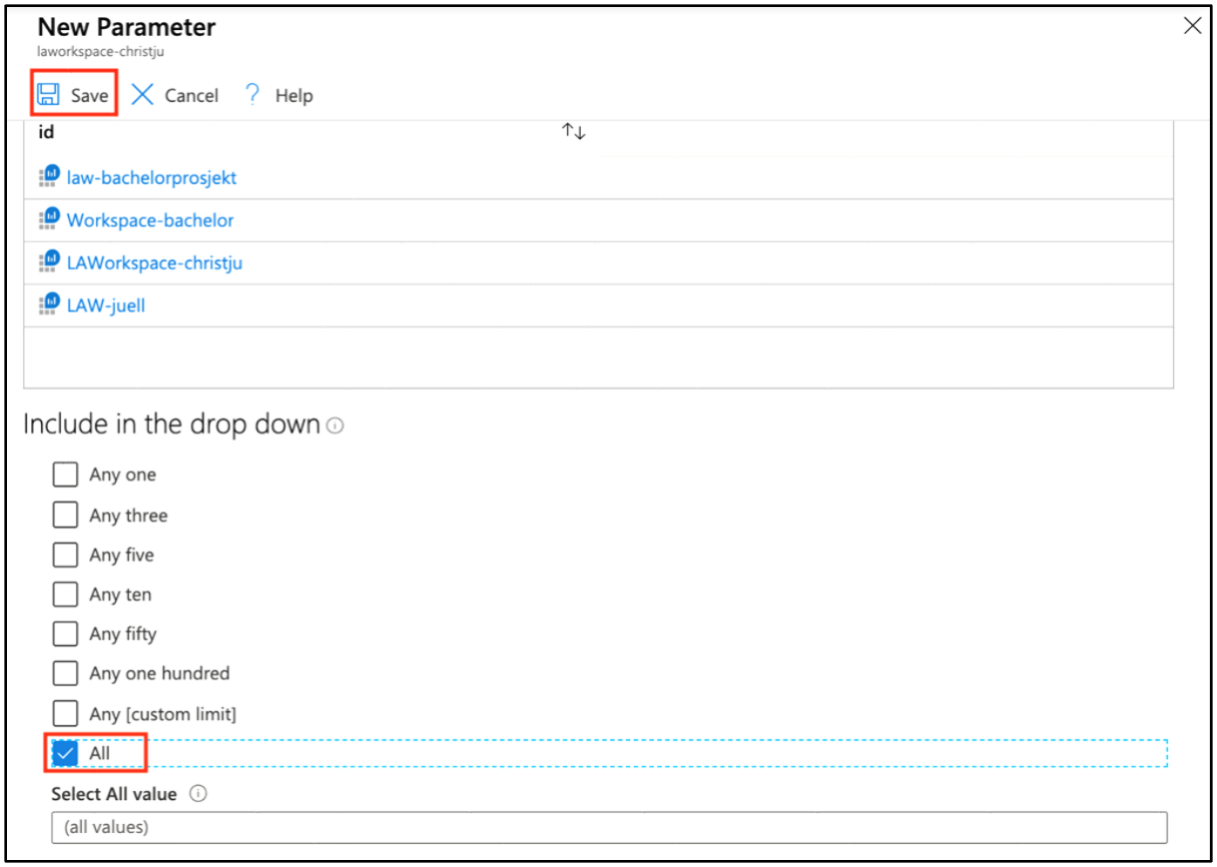


5. Fyll ut de forskjellige feltene, som vist under:

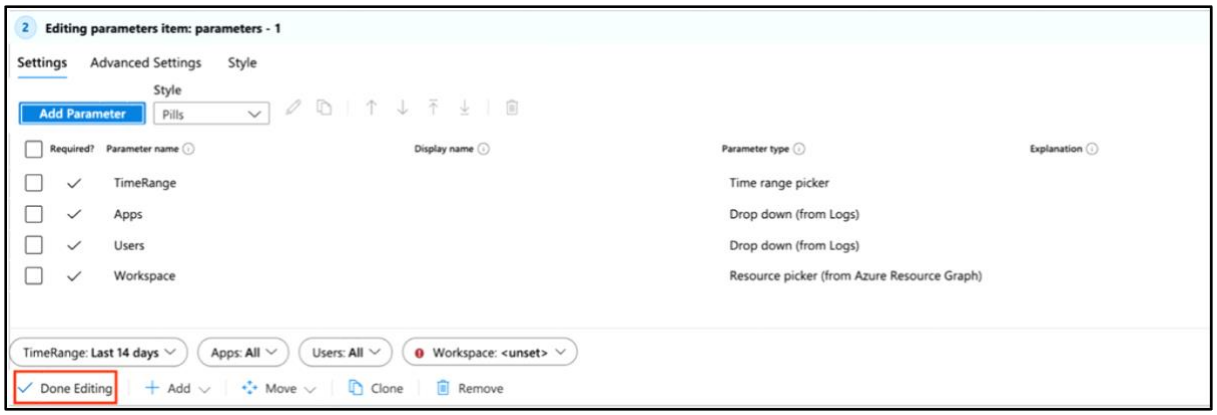


Som man kan se på bildet ovenfor, opprettes det en ny parameter med navn «**Workspace**», av typen «**Resource picker**» (en liste med Azure-ressurser å velge fra). Måten å fylle denne listen på er gjennom en «**Azure Resource Graph Query**». Det er dette vi spesifiserer i «**Get data from**»-feltet. Nøkkelen her er spørringen. Den returnerer en liste med «workspace-ID-er» der hvor «SecurityInsights» (Sentinel) er installert. Dermed ser vi bare arbeidsområder som har Azure Sentinel aktivert. Selv om de returnerte verdiene er ID-er, vises de som navn i portalen, takket være en innebygget «renderer» i Resource Graph.

6. Bla nedover i samme «New Parameter»-vindu. Under **Include in the drop down**, velg **All**. På denne måten vil alle arbeidsområder som har Sentinel installert bli vist. Velg deretter **Save**.



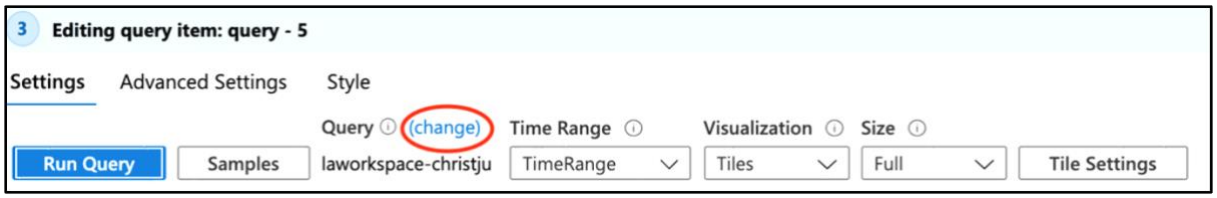
7. Velg **Done Editing**.



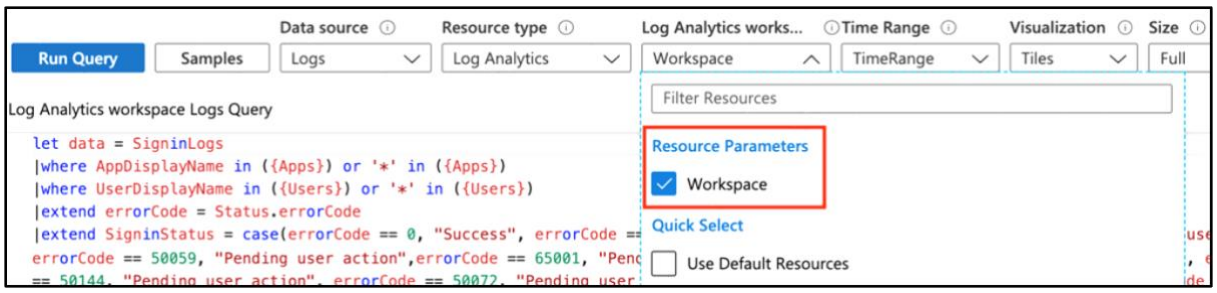
Etter å ha opprettet parameteren må vi redigere hver enkelt spørring eller visualisering i «workbooken» til å bruke den nye parameteren.. Vi fortsetter med det samme eksempelet ved å redigere den første visualiseringen i «workbooken», den som er organisert i såkalte «tiles» for de forskjellige påloggingsresultatene («All Sign-ins», «Success», «Pending user action»).

1. Velg **Edit** nederst til høyre for visualiseringen.

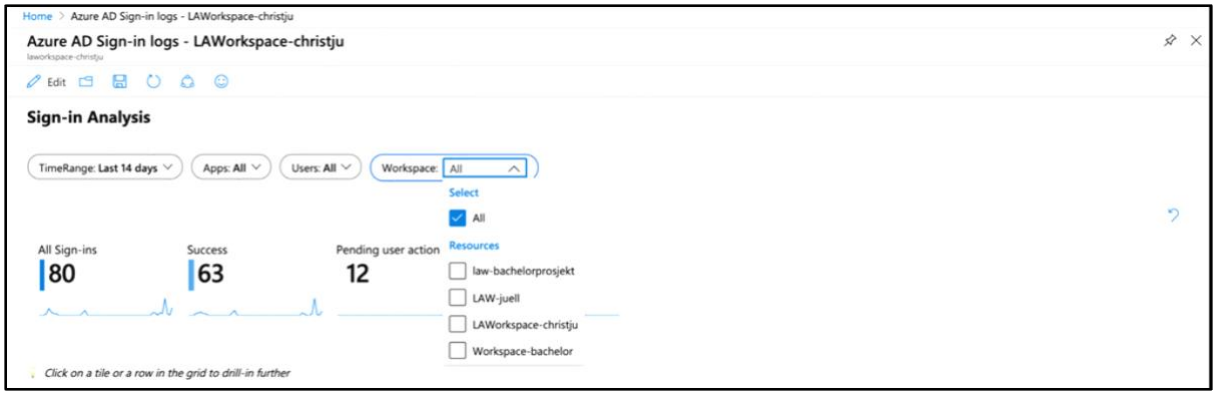
2. Velg (**change)**.



3. Under **Log Analytics workspace**, velg parameteren vi tidligere opprettet (**Workspace).**



Etter å ha valgt **Done editing** igjen er det mulig å velge en eller flere arbeidsområder, og visualiseringen oppdaterer seg basert på hvilket arbeidsområde som er valgt. Man kan også velge å se visualiseringen for alle arbeidsområdene på en gang, som vist under:



For å gjøre resten av «workbooken» multi-tenant, repeterer de siste stegene for alle visualiseringene i «workbooken». Bildet under viser visualiseringen for antall påloggінger basert på enhet de siste 14 dagene, for alle arbeidsområdene:

8. Referanseliste

[1] «Customer Digital Experiences», Internett: https://cdx.transform.microsoft.com/ [Besøkt 11.03.2020]

[2] «Azure-komponenter», Internett: https://blogg.lit.no/microsoft-azure-komponenter-og-kjernetjenester [Besøkt 27.04.2020]

[3] «Password requirements when creating a VM», Internett: defined complexity requirements [Besøkt 27.04.2020]

[4] «Onboarding Azure Sentinel», Internett: https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard [Besøkt 28.04.2020]

[5] «Onboard a customer to Azure delegated resource management», Internett: https://docs.microsoft.com/en-us/azure/lighthouse/how-to/onboard-customer [Besøkt 30.04.2020]

[6] «Azure Lighthouse samples», Internett: https://github.com/Azure/Azure-Lighthouse-samples/ [Besøkt 30.04.2020]

[7] «Use built-in analytics to detect threats», Internett: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in [Besøkt 13.05.2020]

[8] «Advanced multistage attack detection», Internett: https://docs.microsoft.com/en-us/azure/sentinel/fusion [Besøkt 13.05.2020]

[9] «Work with incidents in multiple workspaces», Internett: https://docs.microsoft.com/en-us/azure/sentinel/multiple-workspace-view [Besøkt 14.05.2020]

[10] «Using Azure Lighthouse and Azure Sentinel to Monitor Across Multiple Tenants», Internett: https://techcommunity.microsoft.com/t5/azure-sentinel/using-azure-lighthouse-and-azure-sentinel-to-monitor-across/ba-p/1043899 [Besøkt 14.05.2020]

[11] «Making your Azure Sentinel Workbooks multi-tenant», Internett: https://www.linkedin.com/content-guest/article/making-you-azure-sentinel-workbooks-multi-tenant-javier-soriano/ [Besøkt 15.05.2020]

Christian Fredrik Juell

Hvordan jobbe effektivt med sikkerhetsmonitorering og hendelseshåndtering i et multitenant miljø i Azure?

NTNU
Kunnskap for en bedre verden