Høgskulen på Vestlandet

Bacheloroppgave

ELE350

Predefinert informasjon

Startdato:	08-05-2023 09:00 CEST	**Termin:**	2023 VÅR
Sluttdato:	22-05-2023 14:00 CEST	**Vurderingsform:**	Norsk 6-trinns skala (A-F)
Eksamensform:	Bacheloroppgave		
Flowkode:	203 ELE350 1 O 2023 VÅR		
Intern sensor:	Ingvar Henne		

Deltaker

Navn:	Aleksander Kjeldsen
Kandidatnr.:	250
HVL-id:	152107@hvl.no

Informasjon fra deltaker

Egenerklæring *:	Ja
Inneholder besvarelsen konfidensielt materiale?:	Nei
Jeg bekrefter at jeg har registrert oppgavetittelen på norsk og engelsk i StudentWeb og vet at denne vil stå på vitnemålet mitt *:	Ja

Gruppe

Gruppenavn:	BO23EB-10 ABB SIEM
Gruppenummer:	15
Andre medlemmer i gruppen:	Thor Runar Lindgren

Jeg godkjenner avtalen om publisering av bacheloroppgaven min *

Ja

Er bacheloroppgaven skrevet som del av et større forskningsprosjekt ved HVL? *

Nei

Høgskulen på Vestlandet

Bacheloroppgave:

BO23EB-10: IBM QRadar som SIEM-løsning

Aleksander Kjeldsen
Thor Lindgren

Mai 2023

Dokumentkontroll

Rapportens tittel: BO23EB-10: IBM QRadar som SIEM-løsning	Dato/Versjon: 19. mai 2023/0.3
	Rapportnummer: BO23EB-10
Forfatter(e): Aleksander Kjeldsen Thor Lindgren	Studieretning: CYB
	Sidetall m/vedlegg: 48
Høgskolens veileder: Ingvar Henne, ingvar.henne@hvl.no	Gradering: Åpen
Eventuelle Merknader: Oppgaven kan publiseres	

Oppdragsgiver: ABB AS	Oppdragsgivers referanse:
Oppdragsgivers kontaktperson (inklusiv kontaktinformasjon): Erik Serck-Hanssen, erik.serck-hanssen@no.abb.com	

Revisjon	**Dato**	**Status**	**Utført av**
0.1	10.05.2023	Videreføring av forstudie	Aleksander Kjeldsen Thor Lindgren
0.2	15.05.2023	Utbedring av figurtekster	Aleksander Kjeldsen Thor Lindgren
0.3	19.05.2023	Rettet opp i skrivefeil og andre grammatiske feil	Aleksander Kjeldsen

Forord

Det er med stolthet og en følelse av prestasjon at vi presenterer vårt bachelorprosjekt som fokuserer på design og implementering av et Security Information and Event Management (SIEM) system ved bruk av QRadar utviklet av IBM. Prosjektet er en kulminasjon av års akademisk studie, praktisk erfaring og personlige kunnskaper, samt en lidenskap for informasjonsteknologi og sikkerhet.

Betydningen av et velfungerende SIEM-system i dagens hurtigbevegende digitale verden kan ikke overvurderes. Organisasjoner står ovenfor en stadig strøm av cybersikkerhetstrusler, fra eksterne angrep til interne trusler. Dette kan kompromittere sensitiv informasjon, forstyrre drift og skade virksomhetens omdømme. Et SIEM-system er et kritisk verktøy for å oppdage og begrense slike trusler ved å analysere og korrelere sikkerhetshendelser på tvers av flere kilder og varsle de ansvarlige administratorer om potensielle trusler.

Prosjektet hadde som mål å designe og implementere et SIEM-system som ville gi nødvendige funksjoner, inkludert sanntids hendelseskorrelasjon, loggadministrasjon og trusseldeteksjon, samtidig som det sikret skalerbarhet og brukervennlighet. Prosjektet hadde også som mål å evaluere systemets effektivitet ved å simulere ulike angrepsscenarioer og vurdere dets evne til å oppdage og respondere på slike trusler.

Vi vil benytte denne anledningen til å uttrykke vår oppriktige takknemlighet til våre veiledere, Erik Serck-Hanssen, Kristian Strætkvern og Ingvar Henne, som har gitt uvurderlig veiledning og støtte gjennom prosjektet. Vi vil også takke Peter Behnke Nes, for sin tålmodighet, tilgjengelighet og vilje til å hjelpe og støtte oss i å få ting til å fungere. Vi er også takknemlig for det akademiske personalet og instruktørene som gjennom særdeles utfordrende tider har gitt sin tid, kunnskap og ekspertise gjennom studiene våre.

Til sist vil vi gjerne utrekke en spesiell takk til våre samboere, som gjennom de siste årene med lesing, eksamener og lange dager med arbeid på prosjekter ikke har gitt annet enn støtte og oppmuntring. Tusen takk for alt, Åsne H. Vangen og Ingvild Adolfsen.

Avlsutningsvis er vi stolt av arbeidet vi har utført med å skape et SIEM-system, og håper at dette prosjektet vil være et godt bidrag til cybersikkerhetsavdelingen ved ABB, samt legge et grunnlag for videre arbeid. I tillegg håper vi at dette vil kunne være nyttig i videre opplæring av fagpersonell.

Sammendrag/Abstract

Norsk

Vi skal konfigurere IBM sin programvare QRadar til å fungere med ABB sitt eget 800xA system for å kunne brukes i en SIEM løsning. SIEM samler inn informasjon om systemet, med hovedfokus på mistenksom aktivitet og andre sikkerhetsbrudd. Hvis det oppdages noe alvorlig skal dette varsles til de som er ansvarlig, og andre nødvendige handlinger utføres automatisk, som f.eks å blokkere maskinen der mistenksom aktivitet er oppdaget midlertidig.

På grunn av utfordringer og hindringer vi støtte på i løpet av prosjektet i forbindelse med QRadar hos ABB har vi valgt å sette opp vårt eget test-system, med egne noder koblet til vårt eget nettverk hvor vi har forsøkt å replikere reglene ABB har definert på forhånd for sikkerhetsanalyse og håndtering av logger og hendelser så nært som mulig. Dette har vist seg å være en god løsning og vil kunne hjelpe ABB med både feilsøking og videre opplæring.

English

We are configuring IBM's software QRadar to work with ABB's own 800xA system to be used in a SIEM solution. SIEM collects information about the system, with a focus on suspicious activity and other security breaches. If anything serious is detected, it should alert those responsible and other necessary actions should be carried out automatically, such as temporarily blocking the machine where suspicious activity has been detected.

Due to challenges and obstacles we encountered during the project related to QRadar at ABB, we have chosen to set up our own test system with our own nodes connected to our own network where we have tried to replicate the rules ABB has defined in advance for security analysis and handling of logs and events as closely as possible. This has proven to be a good solution and can help ABB with both troubleshooting and further training.

Innholdsfortegnelse

Figurliste

1 Innledning

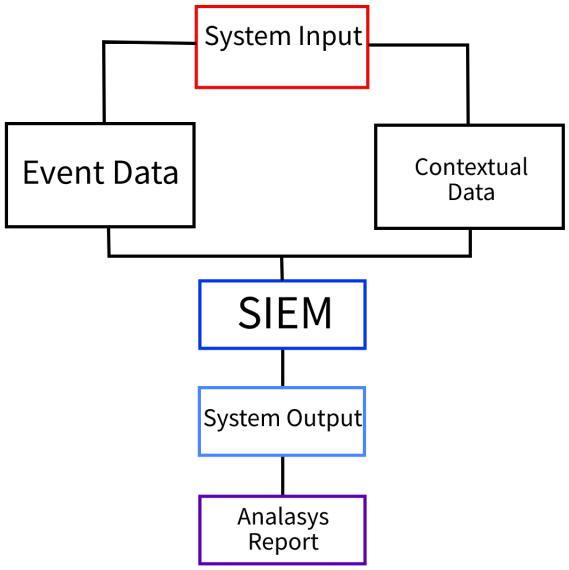
1.1 Oppdragsgiver

ABB er et multinasjonalt selskap med hovedkontor i Zürich i Sveits. De ble etablert i 1988 og er i dag ledende i distribuerte markedskontrollere. På verdensbasis har ABB over 147 000 ansatte, og ca. 1900 ansatte i Norge. Det norske hovedkontoret ligger på Fornebu, men de har også kontorer i Bergen, Stord, Bryne, Oslo, Skien, Stavanger, Trondheim, Hammerfest, Ulsteinvik og Harstad. I 2019 hadde ABB en omsetning på 28 588 000 000 dollar, og de hadde en markedsverdi på 51 603 000 000 dollar den 15. juli 2022. [1]

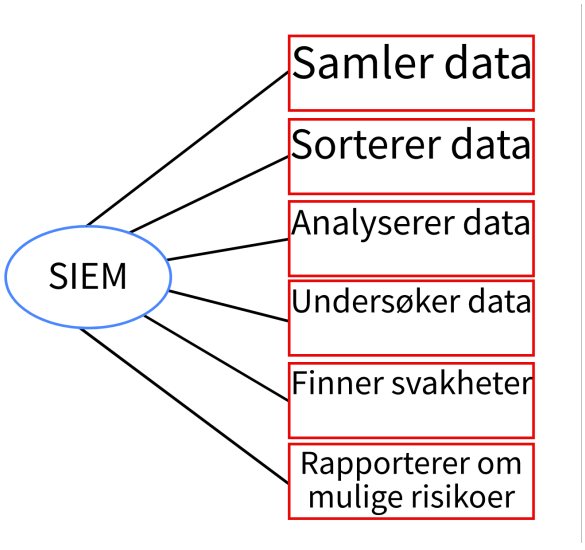
1.2 Problemstilling

ABB har et SIEM-testsystem (Security Information and Event Management) som brukes til å overvåke flere kritiske produksjonssystemer. De ønsker å konfigurere systemet for aktuelle situasjoner relatert til prosessanlegg med et ABB 800xA kontrollsystem. Vi vil her undersøke hvilke scenarioer som er aktuelle for implementering av et kontrollsystem innen prosessindustrien. Scenarioene er forhåndsprogrammerte og vil testes i et kontrollert miljø i testlaben på ABB Kokstad. Vi vil etter hvert også utvikle et grensesnitt mellom kontrollsystemet og SIEM-tjenesten, og vil i løpet av utviklingsfasen sammenligne funksjonalitet og eventuelle løsninger med andre aktuelle SIEM-verktøy som finnes på markedet, deriblant QRadar, Splunk og LogRhythm.

Vi har laget noen skisser for å gjøre SIEM konseptet klarere, i figur 1 ser vi hvor i systemet SIEM-komponenten skal befinne seg. I figur 2 ser vi hvilke funksjoner SIEM-komponenten har.



Figur 1: SIEM Arkitektur
SIEM-komponenten legger seg etter input for å kunne behandle data før det sendes videre.



Figur 2: SIEM funksjoner
SIEM-komponenten har mange funksjoner som bidrar til et mer sikkert nettverk.

Oppgaven vår baserer seg på å lage et program som tar i bruk QRadar og algoritmene fra LogRhythm og tilpasse det best mulig til bruk i et prosessanlegg, samtidig som at det kan bli brukt til opplæring i fremtiden. Vi vil også måtte koble dette programmet opp imot 800xA kontrollere og en RNRP-ruter og en eventuell brannmur.

1.3 Hva er SIEM

SIEM er en teknologi som gjør det mulig for organisasjoner å samle inn, analysere og svare på sikkerhetsrelaterte data fra en rekke kilder i sanntid. SIEM-systemer er designet for å gi en sentralisert oversikt over organisasjonens sikkerhets-posisjon ved å samle og korrelere sikkerhetsrelaterte data fra ulike kilder, som nettverksenheter, servere, applikasjoner og endepunkter. SIEM-systemer brukes av organisasjoner i alle størrelser for å forbedre sin totale sikkerhets-posisjon. De gir synlighet i sikkerhetsrelaterte data, som igjen gir organisasjoner mulighet til å oppdage og svare på trusler i sanntid, og også å overholde reguleringskrav. [2] SIEM-systemer har vanligvis to hovedkomponenter: en loggbehandlings-komponent som samler inn, lagrer og analyserer loggdata, og en sikkerhets-behandlingskomponent som bruker dataene til å identifisere og svare på sikkerhets-trusler.

1.4 Loggbehandlingskomponenten

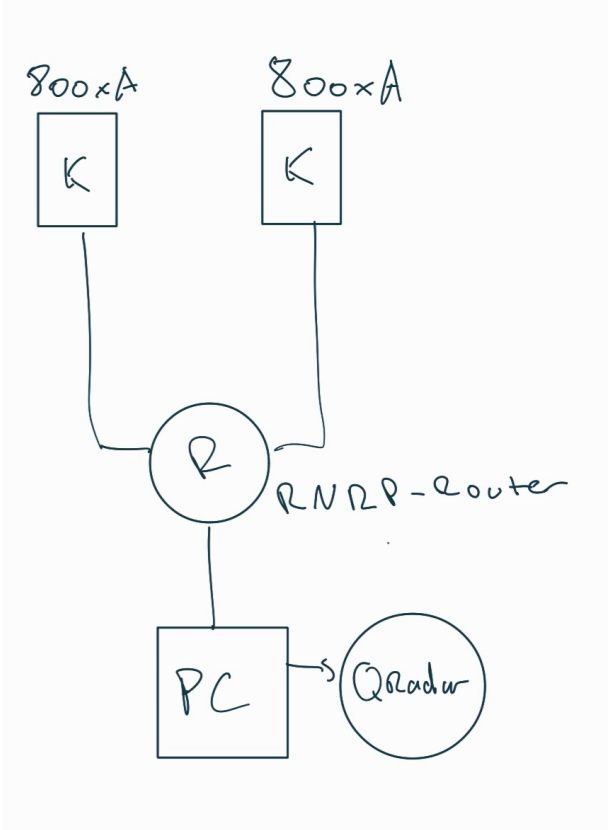
Loggbehandlingskomponenten i et SIEM-system samler inn loggdata fra ulike kilder, som nettverksenheter, servere og applikasjoner. Deretter lagres dataene i et sentralt depot hvor regler og algoritmer brukes til å analysere data som er loggført. Denne analysen hjelper til å identifisere mønstre og avvik som kan indikere en sikkerhetstrussel.

1.5 Sikkerhetsbehandlingskomponenten

Sikkerhetsbehandlingskomponenten i et SIEM-system bruker dataene fra logg-behandlingskomponenten for å identifisere og svare på sikkerhetstrusler. Det gjør dette ved å bruke regler og algoritmer på dataene for å identifisere mønstre og avvik. Hvis en trussel oppdages, genererer systemet et varsel og gir informasjon om trusselen, inkludert alvorlighetsgraden og den potensielle påvirkningen på organisasjonen.

2 Kravspesifikasjon

Systemet som skal kobles opp er i første omgang 800xA kontrollere sammen med en ruter og evt. switcher og brannmurer som igjen skal kobles opp mot en PC som har tilgang til det interne nettverket til bedriften. Her er det satt opp en mengde virtuelle maskiner som skal kobles til det ovennevnte systemet, hvor en SIEM-applikasjon skal overvåke hva som skjer over nettverket og sende informasjon fra de forskjellige PC-ene til kontrollerne. I figur 3 ser vi et enkelt overblikksbilde av hvordan komponentene er koblet sammen i test-systemet



Figur 3: Sammenkoblingsskjema
En pc med QRadar installert er koblet til en RNRP-ruter. Det er også noen 800xA kontrollere koblet til ruteren.

2.1 Prinsipper og terminologi

Det er viktig å sette seg inn i IT-OT prinsipper og terminologi samt dokumentasjon for OT (800xA komponenter), i tillegg til meldingsutveksling i ABB prosessteknologi. I tillegg vil vi se på SIEM håndtering av OT datatrafikk og implementering av "SIEM Use-Cases", regler for analyse og reaksjoner på hendelser. Punktvis vil vi gå igjennom;

- Sammenkobling 800xA controller, RNRP ruter, brannmur, SIEM
- Bruk av QRadar SIEM løsning
- Få et utvalg use-cases til implementering
- Dokumentere alle faser av installasjon/implementasjon/konfigurering
- Forslag til nye use-cases

2.2 Nødvendige krav

Vi vil konfigurere systemet etter ønske fra oppdragsgiver. For at QRadar skal fungere er det visse krav som må oppfylles. Vi har derfor satt opp en liste til krav vi anser som viktigst å fokusere på:

- Sørge for at QRadar er riktig konfigurert og oppdager alle nodene i nettverket.
- Maskinvarekrav: QRadar krever spesialisert maskinvare. Dette inkluderer servere og lagringssystemer med tilstrekkelig prosesseringskraft, minne og lagringsplass for å kunne håndtere store mangder data og sikkerhetshendelser. Vi vil derfor lage et mindre testsystem til å begynne med, med ikke mer enn opptil tre maskiner. Disse er virtuelle maskiner konfigurert passende til sitt formål i Virtual Box, koblet til en laptop og en stasjonær pc på et lukket nettverk.
- QRadar må ha tilgang til og kunne samle inn data fra ulike kilder og vi må sørge for at QRadar har tilgang til de virtuelle maskinene. Vi vil legge til andre nettverksenheter etterhvert, som brannmur, servere og evt. andre applikasjoner.
- Programmet må konfigureres riktig for å kunne fungere som det skal, med riktige innstillinger for hendelseskorrelasjon, varsling og rapportering.
- QRadar trenger tilgang til oppdatert trusselintelligens for å kunne identifisere nye og avanserte trusler og tilpasse seg endrede trusselbilder. Det vil derfor være nødvendig å konfigurere systemet slik at det kan oppdatere seg automatisk med jevne mellomrom.
- Det antas at det er strenge krav til oppetid av systemet og at innsamling av data skal gå ubemerket i henhold til produksjonen på prosessanlegget.

- Vi antar at systemet har høye sikkerhetskrav og rapporter bør kunne krypteres for å forhindre at data kommer på avveie.
- Det bør være mulig å overføre data via TCP/IP mot sikkerhets-behandlingskomponenten.
- QRadar krever opplæring av personell for å kunne brukes effektivt. Vi vil lage en brukermanual med nødvendig informasjon til bruk av ABB.
- Kontinuerlig vedlikehold og oppdateringer er også nødvendig for å sikre optimal ytelse og sikkerhet.

3 IBM QRadar

IBM QRadar er en sikkerhetsinformasjons- og hendelseshåndteringsplattform som brukes til å samle inn, analysere og rapportere om sikkerhetshendelser i en organisasjon. QRadar overvåker og analyserer hendelser fra ulike kilder i sanntid, som brannmurer, nettverksenheter, servere, applikasjoner og sikkerhetsverktøy, og gir en helhetlig oversikt over sikkerhetsstatusen i organisasjonen.

QRadar bruker en rekke teknikker, som hendelseskorrelasjon, trusselintelligens og maskinlæring, for å identifisere og klassifisere sikkerhetshendelser i sanntid. Når en sikkerhetshendelse oppdages, vil QRadar automatisk generere varsler og gi informasjon om hendelsen til et evt. sikkerhetsteam, slik at de kan iverksette tiltak for å løse problemet.

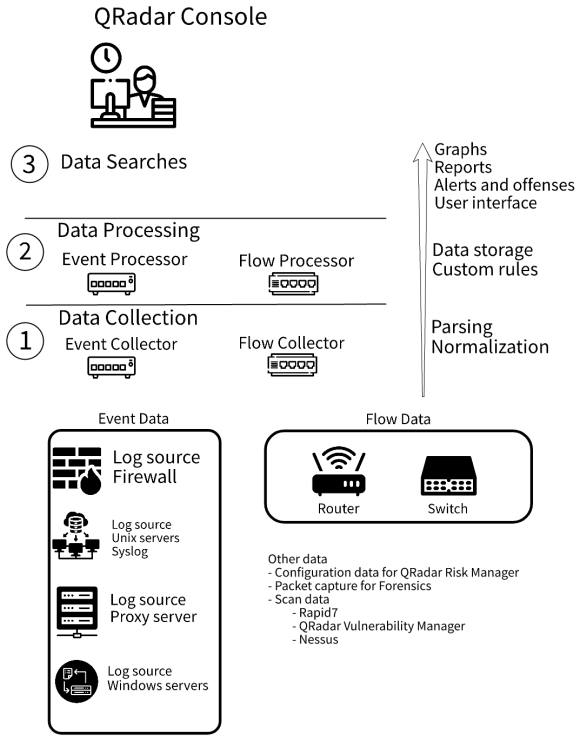
QRadar gir også et detaljert overblikk over sikkerhetshendelser gjennom ulike rapporter og dashbord, som vist i figur 4 under. Dette gir verdifull innsikt i sikkerhetsstatus og risikoer i organisasjonen. SIEM systemer som QRadar er viktig fordi de bidrar til å styrke organisasjonens sikkerhet ved å oppdage og respondere på sikkerhetshendelser raskt og effektivt, og gi ledelsen verdifull informasjon for å ta beslutninger om sikkerhet og risikostyring.

Figur 4: QRadar Pulse Dashbord
Her får man et greit oversiktsbilde av sikkerhetsstatus i QRadar-systemet.

3.1 QRadar arkitektur

Det er nødvendig å ha en god forståelse for IBM QRadar-arkitektur når man planlegger og implementerer en aktuell QRadar-løsning, se figur 5. QRadar er ansvarlig for å samle inn, behandle, aggregere og lagre nettverksdata i sanntid for å gi sanntidsinformasjon og overvåking, varsler og svar på nettverkstrusler.

IBM QRadar SIEM er en modulær arkitektur som gir sanntidsvisning av IT-infrastrukturen det er koblet til for å oppdage og prioritere trusler. Plattformen kan skaleres for å møte aktuelle behov for loggføring og analyse, og man kan legge til integrerte moduler.
Uavhengig av størrelsen og kompleksiteten til QRadar-implementeringen opererer plattformen med tre lag, som vist i diagrammet nedenfor. Ved å forstå hvordan disse fungerer sammen kan man vurdere hvordan komponentene vil fungere i et nettverk og planlegge og opprette en implementering som oppfyller nødvendige krav.



Figur 5: QRadar Architecture
QRadar kan deles inn i tre lag som jobber sammen for å gi en full oversikt over sikkerhetslandskapet i et skalerbart nettverk. Dette består av datainnsamling som det første laget bestående av fysiske datakilder som nettverksenheter. Det andre laget er behandling av data. Dette forekommer i QRadar, enten installert på en egen maskin eller som en alt-i-én løsning på samme maskiner som samler inn data. Det siste laget er datasøk. Dette er hvor man kan søke igjennom og etterforske loggdata for å undersøke hendelser eller feilsøke systemet.

3.1.1 Datainnsamling

Det første laget i diagrammet er Data Collection, eller datainnsamling. Her vil hendelser samles inn fra nettverket. Implemetasjonen av QRadar kan samle inn data direkte fra nettverket, eller man kan bruke innsamlere som QRadar Event Collectors, eller egne tredjepartsapplikasjoner. Før dataene sendes videre til dataprosessering blir de analysert og normalisert. Under denne analysen blir rådata også strukturert og formatert for brukervennlighet.

QRadar SIEM sin primærfunksjon fokuserer på å samle inn data fra hendelser.

Hendelsesdata består av brukerens miljøhendelser som oppstår til en bestemt tid, for eksempel innlogging av bruker, e-post, VPN-tilkoblinger (Virtual Private Network), brannmursperring og proxy-tilkoblinger. Det inkluderer alle hendelser man vil loggføre i enhetsloggene.

Flowdata, eller strømdata, omhandler nettverksinformasjon mellom to enheter i et nettverk. QRadar oversetter denne dataen til strømregistreringer. Rådata som IP-addresser, porter, byte- og pakketellinger og annen informasjon blir konvertert og brukt for å representere en økt mellom to eller flere enheter.
I tillegg til å bruke en flowcollector (som QRadar QFlow Collectors) for å samle inn disse dataene, kan QRadar også benyttes sammen med QRadar Incident Forensics for å benytte seg av total innsamling av nettverkspakker.

3.1.2 Dataprosessering

Den andre laget av QRadar-arkitekturen er dataproessering, der hendelsesdata og flytdata blir behandlet av Custom Rules Engine (CRE), som genererer overtredelser og varsler.

Qradar Risk Manager (QRM), Qradar Vulnerability Manager (QVM) og QRadar Incident Forensics tilbyr ekstra funksjoner og samler inn forskjellige typer data.

QRadar Risk Manager samler inn konfigurasjonsdata for nettveret og gir en oversikt over nettverkstopologien. Man kan bruke denne dataen til å håndtere risiko ved å simulere forskjellige nettverksscenarioer og implementere regler og konfigurasjoner.

QRadar Vulnerability Manager skanner nettverket ditt og behandler sårbarhetsdata eller administrerer data som er samlet inn fra andre skannere som Nessus og Rapid7. Sårbarhetsdataen som samles inn, brukes til å identifisere sikkerhetsrisikoer i det aktuelle nettverket.

3.1.3 Datasøk

Det tredje og øverste laget i QRadar-arkitekturen gjør innsamlet data som er fedigbehandlet tilgjengelig for brukere. Data kan nå søkes opp, analyseres, sendes videre og etterforskes. Brukere kan også administrere sikkerhets-oppgaver og utføre søk fra brukergrensesnittet i QRadar Console.

Det er viktig å skille mellom et all-in-one system og et mer distribuert miljø ofte brukt i større anlegg. I et AIO-system vil all data samles inn og behandles og lagres på samme enhet. I distribuerte miljøer vil ikke QRadar Console utføre hendelses- og strømdatabehandling eller lagringsfunksjoner. Dette vil fungere primært som brukergrensesnitt.

3.2 Regler

Regler, også kjent som korrelasjonsregler, brukes til å søke etter eller oppdage avvik i hendelser. Når alle betingelsene for en test er oppfylt, utløser regelen en respons.

3.2.1 Hva er regler?

Regler er egendefinerte tester som kan oppdage abnormal aktivitet i nettverket ditt ved å bruke AND og OR-kombinasjoner av eksisterende regel-tester. Anomali-deteksjonsregler tester resultatene av lagrede søk på flyt eller hendelser for å oppdage uvanlige trafikkmønstre i nettverket ditt. Anomali-deteksjonsregler krever et lagret søk som er gruppert rundt en felles parameter.

3.2.2 Buildingblocks

Byggeblokker, eller buildingblocks, er en samling av tester som ikke resulterer i en respons eller handling. De grupperer vanlig brukte tester for å bygge kompleks logikk som kan gjenbrukes i regler, for eksempel IP-adresser, privilegerte brukernavn eller samlinger av hendelsesnavn. Standardregler er tilgjengelige i QRadar, og du kan også laste ned flere regler fra IBM Security App Exchange for å opprette nye regler.

3.2.3 Hvordan virker regler?

QRadar Event Collectors samler inn hendelser fra lokale og eksterne kilder, normaliserer disse hendelsene og klassifiserer dem i lavnivå- og høynivåkategorier. Hver Event Processor prosesserer hendelser eller flytdata fra QRadar Event Collectors. Flow Processors undersøker og korrelerer informasjonen for å indikere atferdsendringer eller brudd på policyen. Egendefinerte regler be-handler hendelser og sammenligner dem mot definerte regler for å søke etter avvik. Når en regelbetingelse er oppfylt, genererer Event Processor en handling

som er definert i regelresponsen. Systemene som er involvert i hendelsene spores av regelmotoren, som bidrar til hendelser i overtredelser og genererer varsler.

3.2.4 Hvordan blir en overtredelse laget ut fra en regel?

For å opprette en overtredelse fra en regel, må hendelser oppfylle testkriteriene som er angitt i reglene. QRadar analyserer informasjon som innkommende hendelser, informasjon om enhetene og kjente sårbarheter. Regelen som opprettet overtredelsen, bestemmer overtredelsestypen.

4 Analyse av problemet

4.1 Første fase

I første fase av prosjektet vil det bli nødvendig å få et overblikk over de virtuelle maskinene som skal inngå i simuleringen av de forskjellige scenarioene. Dette blir gjort på en PC som har tilgang til det interne nettverket til ABB via VPN og som gjør det mulig for oss å jobbe fra ønsket lokasjon. Vi vil da koble oss til de forskjellige nodene i nettverket og undersøke om alle kan koble seg til og bli oppdaget av QRadar.

4.2 Andre fase

Etter å ha identifisert de aktuelle virtuelle maskinene i VM-Ware var den opprinnelige planen å være fysisk tilstede i testlaben til ABB på Kokstad for å koble opp alle komponentene som skal inngå i systemet. Dette innebærer en 800xA kontroller som skal programmeres ved et senere tidspunkt, en RNRP-ruter, og en switch og brannmur om det er nødvendig. Pga. forsinkelser og brudd i kommunikasjonen med gjeldende personell har vi vært nødt til å endre denne fasen av prosjektet. Vi vil nå fokusere på å lage et eget nettverk av maskiner. Disse blir satt opp i programmet Virtual Box og vil bli konfigurert i likhet med maskinene i nettverket til ABB. Vi vil deretter sette opp en egen versjon av QRadar da den gitt av ABB ikke fungerer som den skal. QRadar vil deretter bli konfigurert tilnærmet slik kravspesifikasjonen tilsier, og testet opp imot vårt eget nettverk. Vi vil da sørge for at alle nodene blir oppdaget og er koblet sammen.

4.3 Videre arbeid

Når de to første fasene av prosjektet er gjennomført, vil vi benytte QRadar til å definere regler for hendelseskorrelasjon, varsling og rapportering. Formålet med dette er først og fremst å loggføre hendelser og sende meldinger videre til 800xA kontrolleren og deretter videre til applikasjonen om det oppstår noe utenom det vanlige. Dette kan være f.eks. at noen prøver å logge seg på for mange ganger, en ukjent enhet kobler seg på nettverket, og andre generelle sikkerhetsrisikoer. Dette vil bli testet gjennom forhåndsbestemte regler definert av ABB, og vi vil ved et senere tidspunkt definere egne regler og teste disse. På grunn av forsinkelser og tekniske problemer har vi måttet definere egne regler fra starten av. Dette har vert veldig lærerikt, og vi har forsøkt å definere reglene så tett opp imot de som er gitt oss på forhånd av ABB. Vi får desverre ikke testet disse opp imot 800xA kontrollerene på nåværende tidspunkt, men de fungerer på vårt eget system og er et godt utgangspunkt for videre testing og implementering.

4.4 Prosjektets faser oppsummert

Under er det satt opp en punktvis og mer detaljert gjennomgang av de forskjellige fasene i prosjektet:

- Definere et eget lukket nettverk, sammenkobling av noder og SIEM.
  Teste tilkobling både på lokasjon og fjerntilkobling via VPN.
- Bruk av QRadar SIEM løsning
  QRadar vil bli lagt på toppen av topologien, altså over de virtuelle maskinene og vil overvåke og varsle om eventuell mistenkelig adferd. Dette vil bli gjort ved bruk av egendefinerte regler for overvåking og håndtering av hendelser.
- Få et utvalg use-cases til implementering.
  Vi ønsket i første omgang å teste systemet i sin helhet med forhåndsprogrammerte hendelser gitt av ABB. Vi har måtte designe og implementere våre egne regler og eksperimentere med disse for å se hvordan systemet takler å bli satt på prøve utenfor de gitte parameterne. Reglene vi har implementert er en samling av våre egne samt noen tilnærmet like de gitt av ABB. Dokumentasjon vil bli satt inn og oppdatert fortløpende. Forslag til nye regler vil komme nærmere slutten av prosjektet når systemet er testet og de gitte scenarioene er bekreftet funksjonelle.

4.5 Hvordan lage et SIEM system

Under har vi satt opp en oppsummering av punktene vi må jobbe igjennom for å lage SIEM systemet:

- Definere mål og krav - vi må identifisere hvilke type data vi skal samle inn, hvilke sikkerhetshendelser vi ønsker å oppdage og reagere på, og hvilke type rapportering og analyse vi ønsker å utføre.
- Valg av SIEM løsning - her må vi evaluere ulike SIEM løsninger basert på krav og evt. budsjett, men i første omgang vil vi benytte oss av QRadar, og sammenligne denne med andre løsninger som finnes på markedet.
- Konfigurer datainnsamling - Sette opp ulik datainnsamling fra ulike kilder, som brannmurer, inntrengningsdeteksjonssystem, sluttpunktenheter og andre noder i nettverket.
- Definer varsler og rapporter - konfigurer SIEM til å generere varsler og rapporter basert på definerte sikkerhetsregler og kriterier.
- Implementere fin-innstilinger og testing - utføre finjusteringer og testing av SIEM ved bruk av use-case scenarioer/regler for å sikre at det fungerer som det skal.

- Integrer med andre sikkerhetsverktøy - integrer SIEM med andre sikkerhetsverktøy som antivirus, brannmur, inntrengningsforebygging og hendelseshåndtering for å danne et omfattende sikkerhetssystem.
- Opprett pågående vedlikehold og overvåking - for å sikre at det fungerer effektivt og kontinuerlig slik det skal.

4.6 Mulige løsninger

Som tidligere nevnt består systemet av to hovedkomponenter, en del tar seg av datainnsamling og generering av logger, den andre analyserer og reagerer på loggene avhengig av hvilke algoritmer som brukes. Systemet består av fysiske nettverkskomponenter som vi vil koble sammen via TCP/IP, som igjen vil bli koblet sammen med en PC som kjører QRadar. PC vil være hovedkomponenten da denne vil koble seg til virtuelle maskiner, teste systemet via prekonfigurerte scenarioer, og vi vil finjustere systemet alt etter hvordan det reagerer på disse.

4.6.1 Innsamling av data

Innsamling av data og generering av logger skal i all hovedsak være automatisert og vil være styrt av QRadar som vil bli konfigurert etter ønske fra oppdragsgiver.

4.6.2 Rapportering og overvåking

Systemet skal etter ønske fra oppdragsgiver rapportere og sende alarmer ved mistenkelig adferd og avvik fra forskjellige enheter koblet til systemet, og dette kan skje via forskjellige metoder. Vi vil i all hovedsak fokusere på rapportering via grensesnittet og evt. e-post til administrator av system, eller andre former for rapportering. Dette vil bli videre avtalt med oppdragsgiver.

4.6.3 Eget testsystem

Hvis vi ikke får testsystemet til ABB til å virke så kan vi spørre IBM om en testlisens til QRadar selv og sette opp et sett med virtuelle maskiner for å simulere deler av oppgaven på egenhånd. Vi kan ikke teste 800xA systemet på denne måten, men vi får ihvertfall testet og lært hvordan man bruker QRadar til å overvåke og utføre handlinger på et nettverk med andre maskiner. Dette vil gi oss et bedre grunnlag for dokumentasjon enn hvis vi bare skriver alt basert på teori.

4.7 Krav til hardware

IBM QRadar har visse krav til hardware for å kunne kjøre effektivt. Følgende er de grunnleggende/anbefalte kravene til hardware for å installere og kjøre QRadar:

- Prosessor: Minimum Intel Xeon eller tilsvarende, med flere kjerner og høy frekvens. For nøyaktige spesifikasjoner og anbefalinger kan du referere til IBM QRadar-dokumentasjonen for den spesifikke versjonen du bruker.
- Minne (RAM): Minimum 16 GB RAM, men anbefalt mengde kan variere avhengig av størrelsen på nettverket og dataene som skal behandles. For store og komplekse implementeringer kan det være behov for betydelig mer RAM.
- Lagringsplass: Minimum 500 GB harddiskplass for å håndtere QRadar-operativsystemet, programvare og loggdata. Imidlertid kan behovet for lagringsplass variere avhengig av loggdatastørrelse og retensjonskrav.
- Nettverkskort: Minimum 1 Gbps nettverkskort er anbefalt for å håndtere nettverkstrafikk effektivt.
- Operativsystem: QRadar støtter IBM-produserte operativsystemer som CentOS, Red Hat Enterprise Linux (RHEL) og SUSE Linux Enterprise Server (SLES).

Det er viktig å merke seg at disse er generelle krav, og nøyaktige spesifikasjoner kan variere avhengig av QRadar-versjon, lisensiert funksjonalitet og størrelsen på implementeringen. Det anbefales alltid å referere til offisiell IBM QRadar-dokumentasjon eller konsultere med IBM-teamet for å få nøyaktige og oppdaterte krav til hardware.

5 Utfordringer

5.1 Førstegangsoppsett

Vi har i løpet av prosjektet opplevd flere tekniske utfordringer med konfigurering og bruk av QRadar. For det første så kan installering og konfigurasjon av QRadar være ganske komplekst og tidkrevende. Det innebærer å installere og konfigurere ulike komponenter, som Event Processor (i dette tilfellet ABB Event Collector), Data Nodes (ABB 800xA komponenter, samt virtuelle maskiner som fungerer som servere og loggsamlere). Dette kan være overveldende for de som ikke er kjent med eller har hatt kurs i produktet fra før, eller mangler nødvendig teknisk kompetanse. Videre kreves det konfigurering av ulike regler, varsler og rapporter, hvor en dyp forståelse av både QRadar-grensesnittet og sikkerhetslandskapet er nødvendig.

For det andre så er QRadar et kraftig verktøy som krever en betydelig mengde databehandlingskraft og lagring. Avhengig av størrelsen på miljøet som skal overvåkes og mengden data som samles inn, kan maskinvarekravene være ganske betydelige. Å sikre at systemet er tilstrekkelig dimensjonert og optimalisert for ytelse er avgjørende for å oppnå ønskede resultater.

Til slutt kan integrasjonen av QRadar med andre sikkerhetsverktøy og datakilder være utfordrende. QRadar støtter et bredt spekter av protokoller og loggformater, men det kan være tilfeller der egendefinerte analyseregler eller tilkoblinger må utvikles for å sikre at data samles inn og behandles på riktig måte. Dette har vert et hinder vi har forsøkt å navigere oss rundt på best mulig måte da ABB sitt eget system ikke har fungert. Vi har som tidligere nevnt brukt en testversjon av QRadar koblet opp mot vårt eget system av noder på vårt eget nettverk. Vi har hatt tilgang til analysereglene definert av ABB og forsøkt å replikere disse på best mulig måte.

5.2 Fordeler med QRadar

Tross disse utfordringene er fordelene ved å bruke QRadar som et SIEM-system klare. Det gir kraftige sikkerhets- og overvåkingsfunksjoner og en rekke avanserte funksjoner som kan bidra til å oppdage og respondere på sikkerhetstrusler raskt og effektivt. Ved å dra nytte av ekspertise fra erfarne fagpersoner til videre opplæring og følge beste praksis ved installering og konfigurering, kan de tekniske utfordringene knyttet til å opprette et QRadar SIEM-system enkelt overkommes.

5.3 Personlige erfaringer og løsning

Vi oppdaget tidlig at QRadar ikke virket som det skulle. De nødvendige funksjonene og applikasjonene man trenger var enten ikke tilstede eller fungerte som de skulle. Vi har i løpet av prosjektet vert i kontakt med flere ingeniører og samarbeidet tett med disse i et forsøk på å fikse feilene som vi har oppdaget. Dette har vert en langsom prosess uten mye fremgang i starten. Mye av hindringene har stammet fra mangel på kompetanse rundt installering og bruk av QRadar

fra begge parter, samt tekniske utfordringer hvor vi ikke har fått tilgang til nødvendige filer som trengtes for å oppdatere programmet.
I tillegg til dette så er nodene koblet til et LAN uten tilkobling til en ekstern ruter eller annen nettverksenhet og kan kun kommunisere med maskiner på det interne nettverket til ABB. Dette har vert et problem når vi har trengt å legge inn filer som mangler, kjøre oppdateringer eller koble til via remote desktop. Da vi ikke har tilgang til selve prosjektnettet til ABB så har vi løst dette ved å ta kontakt med en av ingeniørene på stedet og bedt om å få lagt inn spesifikke filer og tekstdokumenter med konfigurasjonskommandoer på den eksterne maskinen hvor QRadar er installert.

Alt dette har vært tidkrevende og gjort at vi havnet litt bak tidsskjema. Vi bestemte oss derfor for å sette opp vårt eget system og prøve å replikere ABB sitt oppsett og regler for analyse og håndtering av rapporter. Oppgaven vil derfor allikevel bli løst i henhold til arbeidskrav, og dokumentasjon samt vedlagt manual vil kunne bli brukt av ABB til videre opplæring som ønsket.

5.4 Feilsøking

Vi har stått overfor problemer med QRadar og systemet har ikke fungert slik det skulle i starten. Vi har tatt følgende feilsøkingssteg for å prøve å finne frem til en varig løsning:

- Sjekk systemstatus: Vi startet med å sjekke systemstatus for å se om QRadar-komponentene kjører som de skal. Du kan logge deg på QRadar Console og se etter eventuelle feilmeldinger, varsler eller indikasjoner på problemer.
- Logganalyse: Vi har gått gjennom loggdataene for å identifisere eventuelle feil eller advarsler. QRadar genererer loggdata som kan hjelpe med å diagnostisere problemer. Se etter loggfilene for de aktuelle komponentene som kan være involvert i feilen.
- Kontroller nettverksforbindelse: Vi undersøkte nettverksforbindelsen mellom QRadar-komponentene for å sikre at det ikke er noen problemer med nettverkskommunikasjonen. Vi har også sett på nettverks-innstillinger, brannmurkonfigurasjoner og sikkerhetsregler som kan påvirke QRadar-systemet. Vi har på dette punktet oppdaget feil med nettverket som tidligere nevnt da systemet ikke har tilgang til en ekstern ruter og derfor ikke tilgang til et nettverk.
- Restart tjenester: Vi har forsøkt å restarte de relevante tjenestene eller komponentene som kan være berørt av feilen. Dette kan bidra til å løse midlertidige problemer eller gjenopprette tjenesten til en stabil tilstand.
- Oppdateringer og patcher: For å sørge for at QRadar-systemet er oppdatert med de nyeste oppdateringene, patchene og sikkerhetsoppdaterin-

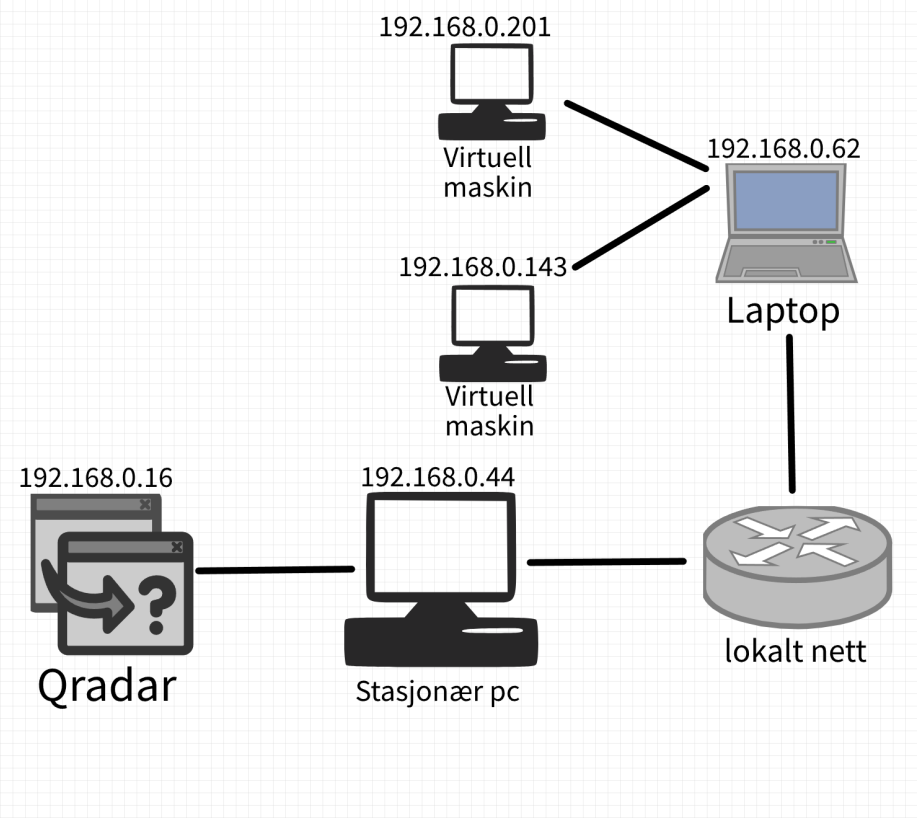
gene fra IBM har vi forsøkt å oppdatere programmet og de aktuelle komponentene. Mange problemer kan bli løst ved å installere de siste oppdateringene. Vi har her funnet noe som kan være årsaken til problemene vi har hatt. Grunnet den manglende tilkoblingen til nett har vi ikke kunnet laste ned de nødvendige filene som kreves for å oppdatere QRadar og en komponent kalt Autoupdate. Vi har gjort mange forsøk på å gjøre dette manuelt, da ved å få en av ingeniørene på ABB til å legge inn oppdateringsfiler og tekstdokumenter med kommandoer for å hente filene og oppdatere
programmet. Da vi klarte å oppdatere Autoupdate har vi ikke kommet videre med ABB sin installasjon av QRadar og har måttet gå videre fra dette og over til vårt eget testsystem da tiden ikke strekker til.

- For videre assistanse kan man konsultere dokumentasjon og bruker-fellesskap: Se gjennom IBM QRadar-dokumentasjonen, kunnskapsdatabaser, bruker-fellesskap og forum for å se om noen andre har opplevd lignende
problemer og funnet løsninger. Vi har funnet nyttige tips, triks og feilsøkingsveiledninger fra QRadar-fellesskapet, blant annet på IBM sine egne nettsider og Reddit.

Feilsøking kan variere avhengig av den spesifikke feilen eller problemet man opplever.

6 Løsning og implementering

Vi har satt opp et eget test-system da ABB sitt ikke har fungert slik det skulle. Vi bruker 2 fysiske maskiner, samt 2 virtuelle maskiner. QRadar er installert som en egen virtuell maskin på en fysisk maskin. Etter at alle komponenter er installert og satt opp får vi et oversiktsbilde over testsystemet:

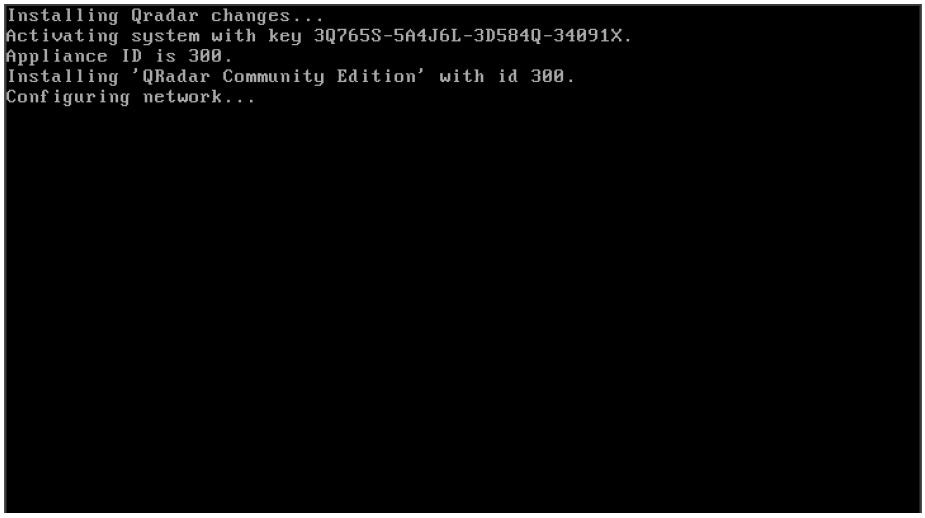


Figur 6: Nytt testsystem
Det nye test-systemet består av 2 fysiske maskiner og 2 virtuelle maskiner, alle med Windows 11 installert.

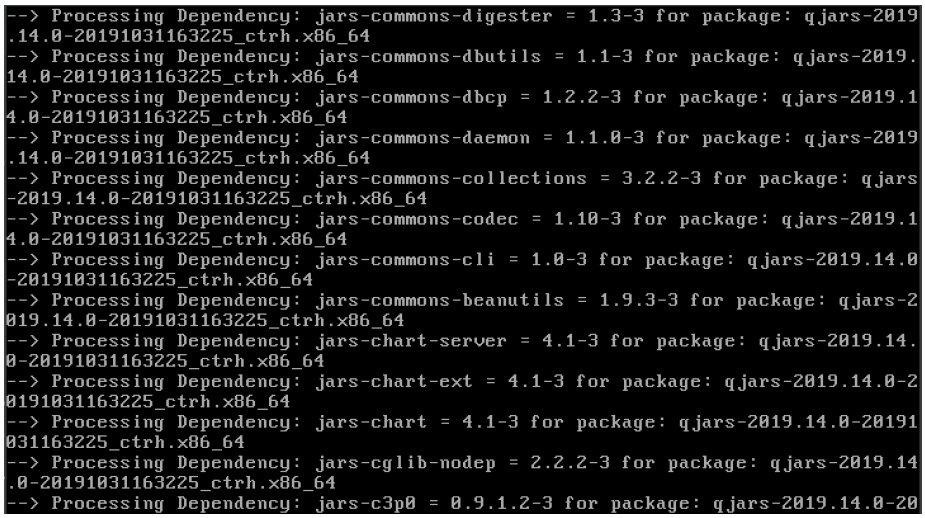
Som vi ser i figur 6 er det nye test-systemet er en del enklere enn det opprinnelige til ABB, men det vil fungere med noen begrensinger. Vi endte opp med å måtte bruke QRadar Community Edition fremfor Enterprise Edition, denne har noen begrensninger, men dette vil ikke påvirke oppgaven vår i noen grad.

6.1 Installering av QRadar

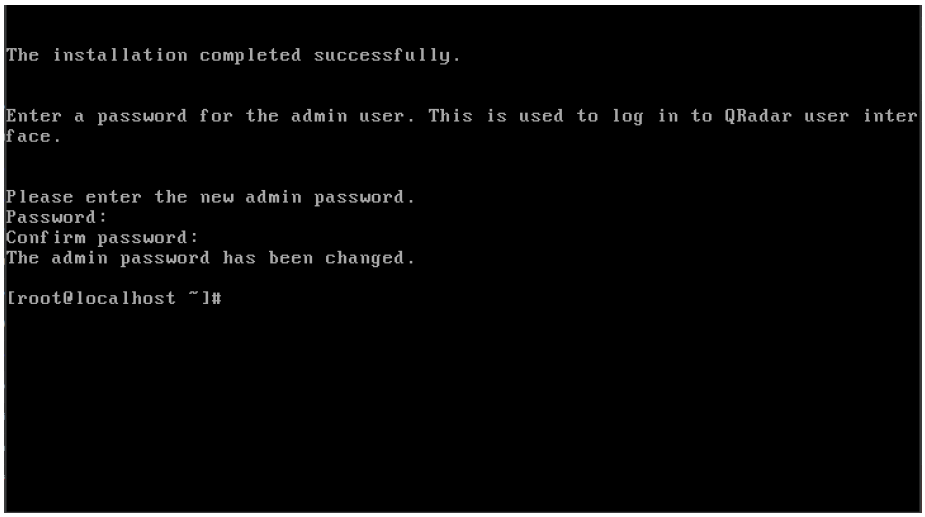
Å installere QRadar er ikke veldig komplisert, men det krever litt mer enn å bare dobbelklikke på QRadar.exe og trykke "neste" til man er i mål. QRadar installeres som en egen virtuell maskin, så først må man ha programvare som kan lage virtuelle maskiner. For dette valgte vi å bruke Virtual Box, siden dette er gratis og open-source. Deretter lastet vi ned QRadar Community Edition fra IBM sine sider. Da fikk vi en .OVA fil som satte opp en virtuell maskin med alt som er nødvendig for at QRadar skal fungere for oss. I figur 7, 8 og 9 ser vi installasjonsprosessen, dette tok noen timer. Når den virtuelle maskinen var klar, ble vi møtt med en Command Line Interface (CLI), og for å fullføre installeringen av QRadar måtte vi skrive inn noen kommandoer som heldigvis var godt dokumentert av IBM.



Figur 7: QRadar installasjon starter
Her starter installeringen av QRadar Community Edition.



Figur 8: QRadar installasjon pågår
Her ser vi at det er mange pakker som skal installeres for at QRadar skal fungere.



Figur 9: QRadar installasjon ferdig
Etter noen timer er installeringen ferdig og QRadar er klar til bruk.

Installeringen tok et par timer å fullføre, men når den var klar kan man prøve å logge seg på web-versjonen av QRadar.
Den virtuelle maskinen er koblet opp på et privat nettverk og har fått sin egen lokale IP-adresse, det er denne IP-adressen man bruker for å koble seg på QRadar web-versjon. For å logge på skriver man i dette tilfellet "https://192.168.0.16

inn i adressefeltet i nettleseren, og man blir møtt med en påloggings-skjerm for QRadar. Brukernavn og passord settes opp under installering av QRadar.

6.1.1 Oppdateringer

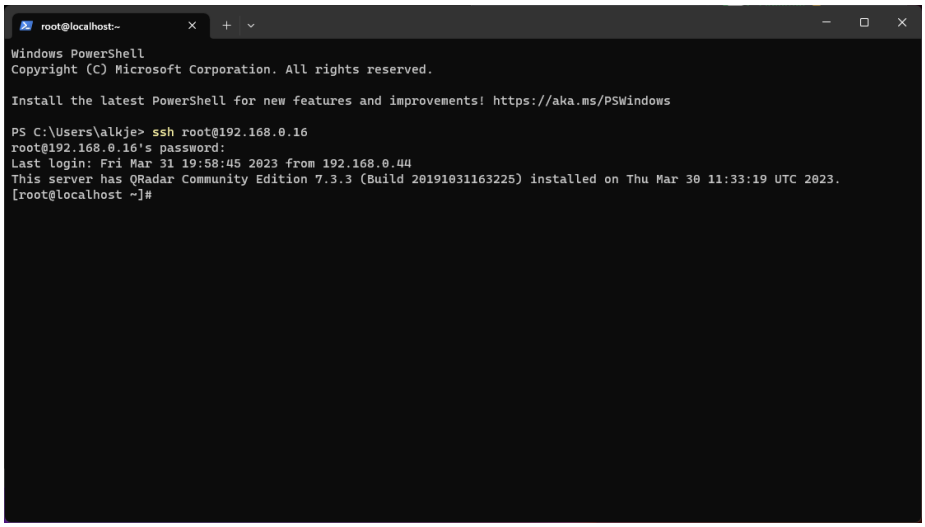
Selv om QRadar er installert og man får logget på, ser det ikke ut til at ting fungerer helt som de skal. Vi fant etterhvert ut at det er en del som må oppdateres selv om QRadar nettopp er installert. QRadar har en egen innebygget applikasjon som skal automatisk skal finne og installere oppdateringer, men denne appen er i seg selv utdatert og får ikke kontakt med serverne. Det første man kan prøve er å endre web serveren hvor "AutoUpdate" finner oppdateringer. Det er dokumentasjon på at denne er endret nylig. [3]

Dette fungerer ikke, og AutoUpdate må oppdateres manuelt. For å gjøre det må man bruke CLI da dette ikke kan gjøres i Graphical User Interface (GUI) (Web-versjon). Det er to måter å gjøre dette på;

- Skrive kommandoer rett inn i den virtuelle maskinen, men siden den kjører som en egen maskin blir dette vanskelig da man ikke kan kopiere kommandoer med lange linker inn mellom den fysiske maskinen og den virtuelle maskinen.
- Logge på den virtuelle maskinen ved å bruke Secure Shell (SSH). Dette gir mulighet til å kopiere kommandoer med lange linker rett inn i CLI slik at man slipper å skrive alt inn manuelt.

6.1.2 Logg inn med SSH

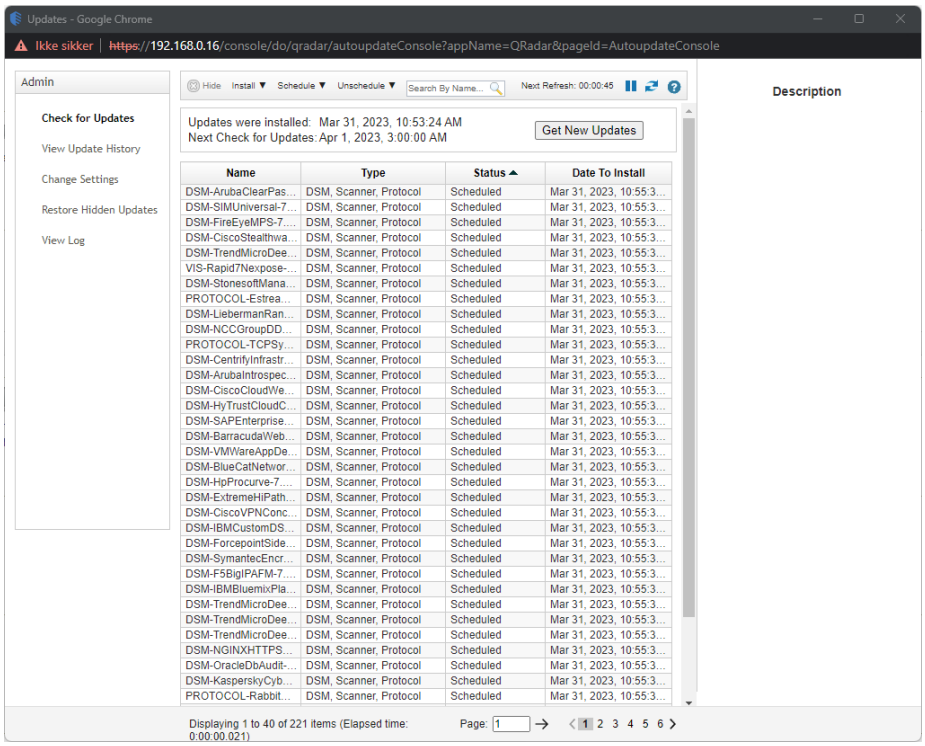
For å logge inn med SSH kan man bruke Windows PowerShell. Dette er innebygget i Windows og er enkelt å bruke. I dette tilfellet brukes kommandoen "ssh root@192.168.0.16" for å logge på som "root" på maskinen som kjører QRadar, som vist i figur 10. Man vil da bli bedt om å skrive inn et passord. Dette er passordet til den virtuelle maskinen, og ikke til QRadar.



Figur 10: Windows PowerShell SSH innlogging
Her ser vi en suksessfull innlogging via SSH, vi kan da se hvilken versjon som er installert og når den ble installert.

6.1.3 Oppdatering av AutoUpdate

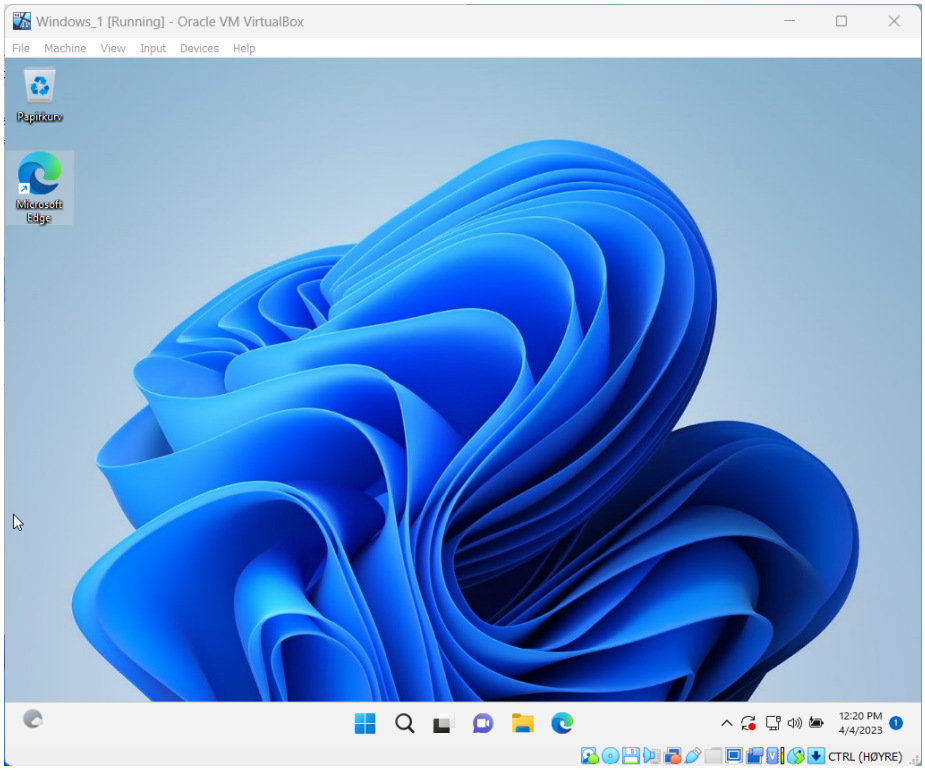
Man kan finne en oppdatert versjon av AutoUpdate på IBM sine sider. Denne kan enkelt lastes ned og legges inn på den virtuelle maskinen. Merk at denne kun kan installeres fra en spesifikk plass via QRadar. Finn frem til riktig lokasjon og installer filen. Logg på GUI og åpne AutoUpdate-appen. Her vil den finne ca 200 oppdateringer (avhengig av versjon og system). Her er det bare å trykke på "Get New Updates" og AutoUpdate fikser resten. Dette kan ta litt tid avhengig av hvilke og hvor mange oppdateringer som skal hentes og installeres. Etter at dette er gjort vil forhåpentligvis QRadar fungere som forventet. I figur 11 ser vi oppdateringene som trengs på vårt system.



Figur 11: QRadar - AutoUpdate
AutoUpdate fant 221 oppdateringer til vårt system.

6.2 Setter opp virtuelle maskiner

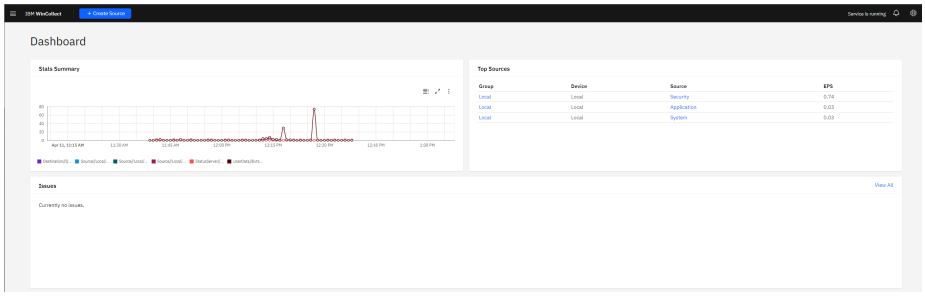
For at testsystemet vårt skal bli mer i henhold til det ABB har definert, må vi sette opp et par ekstra maskiner til testing. Vi bruker en laptop som testmaskin, i tillegg setter vi opp 2 virtuelle maskiner som skal være en del av testsystemet. For å sette opp disse bruker vi igjen Virtual Box, samme som vi brukte for å installere QRadar. Vi bruker en .iso fil med Windows 11 fra Windows sine egne sider. Iso-filen er perfekt for installasjon av Windows på en virtuell maskin, da den simulerer det på samme måte som å installere fra en installasjons-cd. Det er fort gjort å sette opp, da Windows sin installasjonsprosess er rask og enkel. I figur 12 ser vi Windows 11 kjører på en av de virtuelle maskinene. Man kan også selvfølgelig bruke en Linux distro eller MAC om man ønsker det. Merk at MAC ikke har blitt testet og funksjonalitet er ukjent. Til sist får begge de virtuelle maskinene sin egen lokale IP og har kontakt med QRadar.



Figur 12: Windows 11 på virtuell maskin
Virtuelle maskiner deler ressurser med maskinen de er installert på og kan derfor være krevende for systemet.

6.3 WinCollect

For å samle informasjon og logger fra de andre maskinene i nettverket var det opprinnelig tenkt at vi skulle bruke ABB Event Colletor. Da vi ikke får satt opp 800xA systemet dette blir brukt sammen med bruker vi WinCollect. WinCollect bruker Windows Event Log API til å samle og sende informasjon til QRadar og er på mange måter likt ABB Event Collector. Når man installerer WinCollect er det viktig å oppgi den lokale addressen der QRadar kjører, i vårt tilfelle "192.168.0.16". Dersom alt går bra, får WinCollect automatisk kontakt med QRadar etter at det er installert, og begynner med en gang å sende informasjon som vi ser i figur 13.



Figur 13: WinCollect kjører på stasjonær pc
WinCollect starter med en gang å sende informasjon, men kan konfigureres til å sende mer informasjon om ønskelig.

WinCollect samler inn hendelsesloggdata fra ulike Windows-komponenter og applikasjoner, inkludert Active Directory, DNS-servere, DHCP-servere, nettverkskomponenter, databaser, sikkerhetsapplikasjoner og operativsystemet selv. Dataene som samles inn, inkluderer detaljer om brukeraktivitet, system-hendelser, applikasjonsfeil, sikkerhetsbrudd og annen informasjon som kan gi innsikt i systemets sikkerhetsstatus og ytelse.

WinCollect støtter også filtrering av hendelsesloggdata og har mulighet for å sende varsler til sikkerhetsteamet når visse hendelser oppstår. Dette kan hjelpe organisasjoner med å identifisere og reagere raskt på sikkerhetshendelser.

WinCollect kan også konfigureres for å bruke TLS-kryptering og autentisering for å sikre at hendelsesloggdataene ikke blir kompromittert under overføringen.

I tillegg til å samle inn hendelsesloggdata fra Windows-baserte systemer, støtter WinCollect også samling av hendelsesloggdata fra andre plattformer, som Linux og Unix, ved hjelp av tilleggsprogramvare. [4]

6.4 Rules og offenses

Det er 4 ulike typer regler man kan sette opp i QRadar. Noen sjekker enkle egenskaper fra datasettet, mens andre er mer kompliserte.

- **Event Rules**
  Hendelsesregler tester mot innkommende loggkilde-data som behandles i sanntid av QRadar Event Processor. Du oppretter en hendelsesregel for å oppdage enkelt begivenheter eller hendelsessekvenser. For eksempel, for å overvåke nettverket ditt for mislykkede påloggingsforsøk, tilgang til flere verter, eller en rekogniseringshendelse etterfulgt av en utnyttelse, oppretter du en hendelsesregel. Det er vanlig for hendelsesregler å opprette overtredelser som svar.

- **Flow Rules**
  Strømregler tester mot innkommende strømdata som behandles av QRadar Flow Processor. Du kan opprette en strømregel for å oppdage en enkelt strøm eller strømsekvenser. Det er vanlig for strømregler å opprette overtredelser som svar.

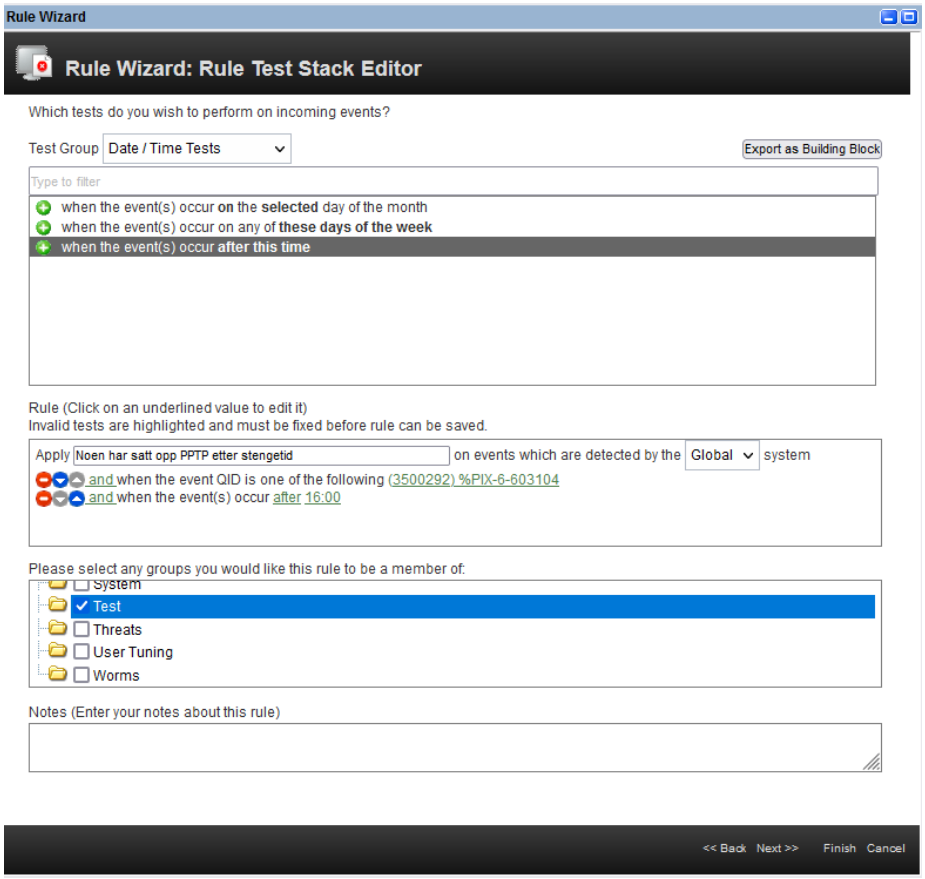
- **Common Rules**
  Fellesregler tester mot hendelses- og strømdata. Du kan for eksempel opprette en fellesregel for å oppdage hendelser og strømmer som har en bestemt kilde-IP-addresse. Det er vanlig for fellesregler å opprette overtredelser som svar.

- **Offense Rules**
  Overtredelsesregler tester paramaterne til en overtredelse for å utløse flere svar. For eksempel genereres det en respons når en overtredelse oppstår på en spesifikk dato og tid. En overtredelsesregel behandler overtredelser bare når endringene gjøres i overtredelsen. For eksempel når nye hendelser legges til, eller systemet planlegger overtredelsen for revurdering. Det er vanlig for overtredelsesregler å sende en e-postvarsling som svar.

[5]

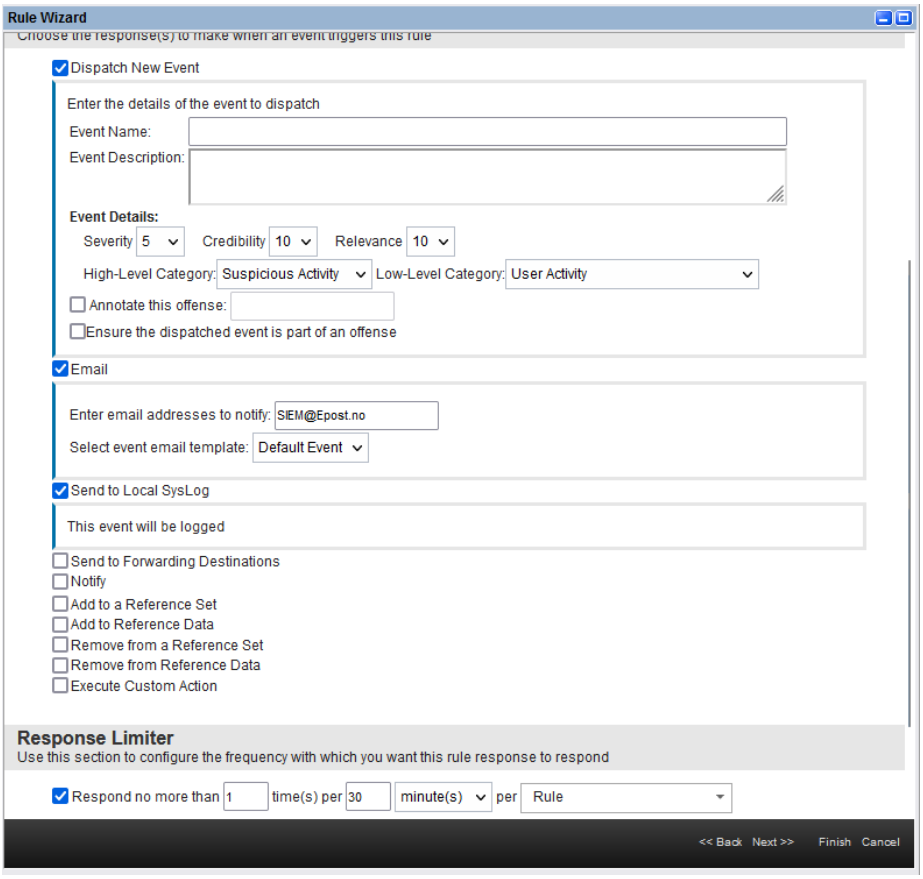
6.4.1 Lage en regel

For å lage en ny regel trykker man først på "Offenses"-fanen, deretter "Rules", etterfulgt av "Actions". Der kan man velge hvilken type regel man vil lage. Da åpnes "Rule Wizard", og det er her man kan sette opp regelen slik man ønsker. I figur 14 setter vi opp en hendelsesregel som skal varsle om noen setter opp Point-to-Point Tunneling Protocol (PPTP) etter klokken 16. Reglene kan være veldig spesifikke som dette, eller de kan være litt løsere.



Figur 14: Rule Wizard
Dette er en henholdsvis enkel regel bare for illustrasjon, men reglene kan bli veldig kompliserte og inneholde flere tester.

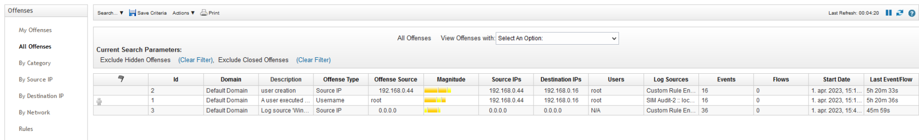
Man trykker på "Next", da kan man velge hva som skjer når QRadar opp-dager at noen har satt opp PPTP etter klokken 16. Vi velger da at den skal lage en ny hendelse, at QRadar skal varsle på epost, og at det skal loggføres i den lokale SysLoggen slik vi ser i figur 15 Etter dette steget er regelen ferdig, og klar til bruk. Man kan velge om den skal aktiveres med en gang, eller ikke.



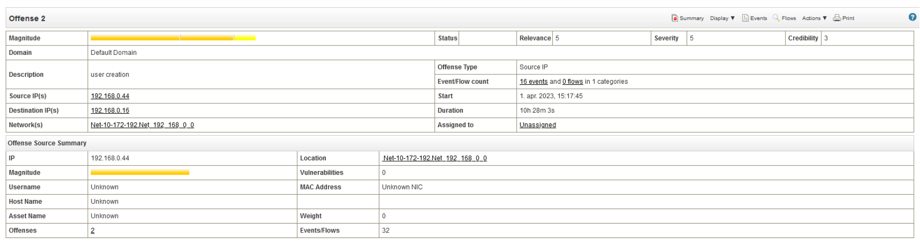
Figur 15: Rule Wizard del 2
Her sier vi at når regelen inntreffer så skal systemet sende et nytt event, varsle på epost, og i tillegg sende til SysLog/Log Activity.

6.4.2 Offenses

For å se alle "Offenses" i vårt system velger vi "All Offenses" i "Offenses"-menyen, se figur 16. Her får man opp all informasjon om ulike hendelser som har skjedd. Hvis man trykker seg inn på en av hendelsene, får man opp all informasjon om denne spesifikke hendelsen, se figur 17. Her kan man få informasjon om hvor mange ganger det har hendt, fra hvilke IP-addresser, alvorlighetsgrad samt en hel del annen informasjon.



Figur 16: All Offenses
Her vises grunnleggende informasjon om hendelsen, som IP-addresser, alvorlighetsgrad, brukerenheter m.m.

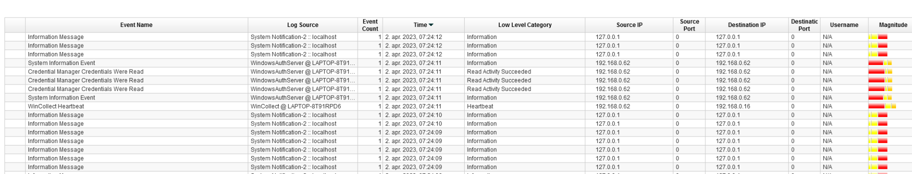


Figur 17: Informasjon om en spesifikk hendelse
Her finner man mer informasjon om hendelsen, blant annet mer utfyllende informasjon om enheten eller brukeren det gjelder, fra hvilken lokasjon det kommer fra om tilgjengelig m.m.

Man kan også velge å sende denne informasjonen på epost dersom man ønsker at noen andre skal se på det, eller man kan tildele ”offensen” til en annen administrator som også har tilgang til QRadar.

6.5 Log activity

Nesten all informasjon om hva som foregår i QRadar havner i ”Log Activity”, se figur 18. Dette kan være informasjon om de ulike systemene som er innebygget i QRadar, eller informasjon fra andre maskiner eller utstyr som er koblet til. Det kan være veldig mye informasjon som kommer på kort tid her, men heldigvis kan man sortere og filtrere etter behov.



Figur 18: Log Activity
I Log Activity kan man se blant annet source og destination IP, hvilken enhet det kommer fra og hvilke regler og tester som har blitt utløst. Under Magnitude kan man også se alvorlighetsgraden av hendelsene.

Hver oppføring har en del informasjon som er verdt å merke seg, deriblant; "Log Source", "Source IP", "Destination IP" og "Magnitude". Man kan også trykke inn på hver enkelt oppføring for å få enda mer informasjon, dette er fint hvis det er noe som ser suspekt ut.

6.6 Installere applikasjoner i QRadar

For at QRadar skal fungere optimalt til ditt behov er det et stort utvalg av applikasjoner man kan installere. IBM har laget mange av disse applikasjonene selv, men det finnes også applikasjoner som andre utviklere har laget. Applikasjonene finner man på IBM sin platform "IBM X-Exchange". For å installere en applikasjon må man generere en "Authentication Token". En authentication token er en autoriseringskode som brukes til å bekrefte en brukers identitet. [6] Her er applikasjonene vi har brukt i vårt system:

- **QRadar Assistant**
  QRadar Assistant er en veldig nyttig applikasjon, og burde være den første man installerer. Her får man oversikt over alle applikasjonene som ligger på "IBM X-Exchange", i tillegg får man anbefalinger om hvilke apper man burde installere til sitt system. Den gjør det også lettere å installere nye applikasjoner da den er direkte koblet til "IBM X-Exchange" så man kan installere de rett fra QRadar Assistant. Man får også enkel tilgang til mange videoer laget av QRadar eksperter som forklarer hvordan man kan implementere sitt system. [7]

- **QRadar Deployment Intelligence**
  QRadar Deployment Intelligence er en teknologi som hjelper brukere å planlegge og implementere QRadar SIEM-systemet på en optimal måte for å oppnå best mulig sikkerhetsresultater. Denne funksjonen bruker maskinlæringsalgoritmer og dataanalyse for å vurdere informasjon om nettverksinfrastrukturen, eventuelle eksisterende sikkerhetstiltak og andre variabler som påvirker implementeringsprosessen. Resultatet er en rapport som gir anbefalinger for hvordan man skal implementere QRadar-systemet på en måte som er tilpasset organisasjonens behov og ressurser. Dette kan hjelpe organisasjoner med å redusere risikoen for cyberangrep og optimalisere sikkerhetsytelsen på tvers av nettverk og IT-infrastruktur. QRadar Deployment Intelligence er et verdifullt verktøy for organisasjoner som ønsker å implementere QRadar SIEM-systemet på en effektiv og optimal måte. [8]

- **QRadar Pulse**
  QRadar Pulse gir en enkel måte å visualisere sikkerhetsdata og -trender i sanntid, og gir en mer intuitiv måte å oppdage og håndtere sikkerhetshendelser på. Det lar brukerne enkelt utforske og analysere sikkerhetsdata ved hjelp av ulike diagrammer, grafer og kart.

  QRadar Pulse kan også bidra til å forbedre samarbeidet mellom sikkerhetsanalytikere og administratorer ved å gi en enkel måte å dele informasjon

og rapporter på. Administratorer kan få innsikt i sikkerhetsstatusen til organisasjonen på en enkel måte, og sikkerhetsanalytikere kan raskt og enkelt dele hendelsesinformasjon og rapporter med kolleger og administratorer. [9]

- **Experience Center**
  QRadar Experience Center gir brukerne tilgang til en rekke opplæringsressurser, inkludert opplæringsvideoer, opplæringsøkter, brukerhåndbøker og tekniske artikler. Det gir også brukerne muligheten til å kommunisere direkte med IBM-eksperter og andre QRadar-brukere gjennom et dedikert fellesskap.

  En av fordelene med QRadar Experience Center er at det gir en enkel måte å lære om QRadar-plattformen og dens funksjoner, uavhengig av brukerens nivå av kunnskap eller erfaring. Det kan også hjelpe organisasjoner med å optimalisere QRadar-plattformen for å møte deres spesifikke sikkerhetsbehov og utfordringer. [10]

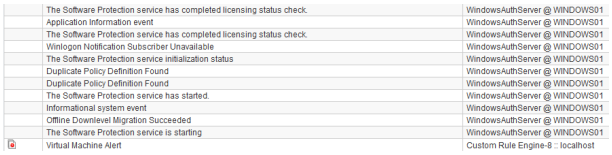
- **Log Source Manager**
  QRadar Log Source Manager lar brukerne enkelt legge til nye loggkilder og konfigurere dem for å samle inn relevant sikkerhetsinformasjon. Det gir også brukerne muligheten til å endre konfigurasjonen til eksisterende loggkilder og teste loggkildene for å sikre at de fungerer som forventet.

  En av fordelene med QRadar Log Source Manager er at det kan bidra til å redusere kompleksiteten og arbeidsbelastningen i administreringen av loggkilder. Det kan også hjelpe organisasjoner med å sikre at alle relevante sikkerhetsdata samles inn og analyseres, noe som kan bidra til å forbedre sikkerheten og redusere risikoen for cyberangrep. [11]

7 Testing

7.1 Enkle regler

For å teste at systemet vårt fungerer har vi laget noen regler som er enklere å teste. Vi begynner med å teste en regel som skal varsle hver gang en spesifikk maskin sender informasjon. I dette tilfellet bruker vi en av de virtuelle maskinene, men regelen kan tilpasses til en hvilken som helst "log source" som er koblet til systemet. Informasjonen som blir vist i QRadar kan sees i figur 19.



Figur 19: Varsel om melding fra den virtuelle maskinen
Vi kan se at QRadar sender ut informasjon om hvilken enhet som kobler seg til nettverket og hvilke data den sender. Nederst kan vi også se hvilke regler som blir aktivert.

Vi ser i figur 19 at når vi starter den virtuelle maskinen og den begynner å sende meldinger, så kommer det et eget varsel om dette. Merket helt til venstre viser til at dette er en "offense".

Vi har også en regel som varsler dersom maskinen oppdager at noen har prøvd å logge på mer enn 3 ganger på kort tid uten hell. For å teste dette logger vi ut av brukeren på den virtuelle maskinen, deretter prøver vi å logge inn igjen mer enn 3 ganger med feil passord. Data som vises i QRadar kan sees i figur 20.

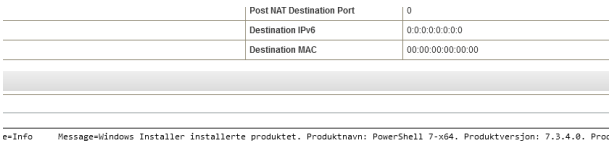
Figur 20: Mislykkede påloggingsforsøk
Man kan her se hvordan QRadar plukker opp og responderer på et spesifisert antall mislykkede påloggingsforsøk. Her er det 3 mislykkede forsøk på å logge på brukeren, hvor brukeren blir utestengt på det tredje mislykkede forsøket.

7.2 Installering av program i Windows

Som standard i QRadar ligger det allerede inne en del regler, noen av disse reglene forteller om noen installerer et program på maskinen. I dette tilfellet installerte vi en oppdatering av PowerShell for å se om systemet plukket det opp.
Vi ser i figur 21 at det først kommer en melding "Windows Installer initiated install", deretter "Windows Installer ending installer transaction", "Windows Installer completed installation successfully", og til slutt "Windows Installer installed a product.

Figur 21: Installasjon
Systemet plukker opp informasjonen og hendelsesforløpet blir vist og loggført.

For å få mer informasjon om hvilket program som ble installert, trykker vi inn på den siste meldingen; "Windows installer installed a product". Der finner vi informasjon om hvilket program som ble installert og ser fra figur 22 at dette var PowerShell 7.3.4.0 for Windows 64-bit.



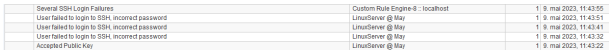
Figur 22: PowerShell 7.3.4.0 ble installert
Her vises informasjon om hva som ble installert, fra hvilken enhet og hvilket program som initierte installasjonen.

7.3 Experience Center

Formålet med QRadar Experience Center er å demonstrere QRadar sin funksjonalitet, samt fordeler og bruksområder i ulike scenarioer. Experience Center gir også en rekke ressurser og verktøy som hjelper brukere med å forstå og utforske QRadar. Dette inkluderer demonstrasjoner av plattformens funksjoner, simulerte trusselscenarioer, veiledninger for implementering og konfigurasjon, samt opplæringsressurser.
QRadar Experience Center kan da brukes til å teste om systemet fungerer. En av funksjonene til Experience Center er Threat simulator som lar deg simulere ulike trusler som f.eks mistenksom bruk av PowerShell. Man kan også laste opp

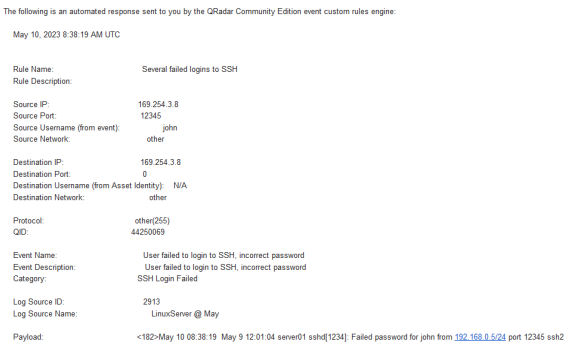
en SysLog og bruke den til å simulere hendelser.

Her har vi fått kunstig intelligens til å generere en SysLog som simulerer at noen prøver å logge på via SSH men bruker feil passord gjentatte ganger. Dette vises i QRadar som vist i figur 23. Vi har laget en regel som sjekker om noen prøver å logge på med SSH mer enn 3 ganger innen 3 minutter og deretter varsler både i QRadar og i tillegg sender ut en epost for å varsle om dette, med informasjon som vist i figur 24.



	Several SSH Login Failures	Custom Rule Engine-8 :: localhost	1	9. mai 2023, 11:43:55
	User failed to login to SSH, incorrect password	LinuxServer @ May	1	9. mai 2023, 11:43:51
	User failed to login to SSH, incorrect password	LinuxServer @ May	1	9. mai 2023, 11:43:41
	User failed to login to SSH, incorrect password	LinuxServer @ May	1	9. mai 2023, 11:43:32
	Accepted Public Key	LinuxServer @ May	1	9. mai 2023, 11:43:22

Figur 23: SSH login failure i Log Activity
Slik vil det se ut i QRadar konsoll når en hendelse blir plukket opp og håndtert. Man kan også se tidsforløpet og responsen på hendelsen.



The following is an automated response sent to you by the QRadar Community Edition event custom rules engine:

May 10, 2023 8:38:19 AM UTC

Rule Name: Several failed logins to SSH
Rule Description:

Source IP: 169.254.3.8
Source Port: 12345
Source Username (from event): john
Source Network: other

Destination IP: 169.254.3.8
Destination Port: 0
Destination Username (from Asset Identity): N/A
Destination Network: other

Protocol: other(255)
QID: 44250069

Event Name: User failed to login to SSH, incorrect password
Event Description: User failed to login to SSH, incorrect password
Category: SSH Login Failed

Log Source ID: 2913
Log Source Name: LinuxServer @ May

Payload: <182>May 10 08:38:19 May 9 12:01:04 server01 sshd[1234]: Failed password for john from 192.168.0.5/24 port 12345 ssh2

Figur 24: Epostvarsel om mislykket SSH pålogging
Slik ser informasjonen ut i epostvarselet sendt ut av QRadar. Her får man informasjon om IP-adresser, hva som utløste hendelsen og hvilken bruker det gjelder, om det er en intern bruker.

8 Gjenstående arbeid

Det gjentår enda en del arbeid i forhold til den opprinnelige kravspesifikasjonen. Vi har blant annet ikke fått koblet opp noen 800xA kontrollere og det gjenstår en del testing i forbindelse med dette. Dette inkluderer blant annet:

- Installere QRadar-programvare på de relevante serverne og komponentene.
- Konfigurere QRadar og ABB 800xA systemene slik at QRadar blir integrert og for å sikre en sømløs datastrøm.
- Teste systemet på områder som datainnsamling og behandling ved å overføre simulerte hendelser og flytdata fra 800xA systemene og videre til QRadar.
- Utføre testing av QRadar og systemets funksjonalitet, inkludert hendelsesregistrering, alarmsystem, trusseloppdagelse og responsfunksjoner.
- Verifisere at QRadar og maskinene som er integrert i nettverket klarer å håndtere det forventede datavolumet uten feilmeldinger og ytelses-problemer.
- Utføre integrasjonstesting for å sikre at QRadar kan skaleres og installeres i større produksjonsmiljøer og samhandle korrekt med andre sikkerhets- og nettverkssystemer i organisasjonen.
- Dokumentere installasjonsprosessen av 800xA-systemet og resultatene av testingen for fremtidig referanse og bruk.

9 Konklusjon

I denne rapporten har vi sett på QRadar, en avansert sikkerhetsinformasjons- og hendelseshåndteringsteknologi. Vi har undersøkt funksjonene og fordelene ved QRadar, og hvordan det kan hjelpe organisasjoner med å identifisere og håndtere sikkerhetstrusler. Vi har også sett på utfordringene ved å implementere QRadar og gitt anbefalinger for å sikre en vellykket implementering.

Installasjonsprosessen for IBM QRadar har vist seg å være en omfattende prosess, men også svært lærerikt. Gjennom grundig planlegging og samarbeid har vi lykkes med å implementere QRadar i vårt eget testsystem og skapt et solid grunnlag for nettverkssikkerhet.

Ved å følge de anbefalte trinnene for installasjon og konfigurasjon som kan finnes i de forskjellige seksjonene i rapporten kan man sikre at QRadar blir riktig integrert og konfigurert i den gjeldende infrastrukturen man ønsker å implementere systemet i. Vi har igjennom prosessen satt opp nødvendige servere, nettverkskomponenter og loggsamlere som støtter QRadar funksjonalitet.

Testing har vert en viktig del av prosessen, hvor vi har verifisert at QRadar fungerer som forventet. Vi har på dette tidspunktet ikke mulighet til å teste det opp i mot 800xA komponentene, men systemet fungerer på samme måte med mindre endringer av reglene, og forventes derfor å fungere om det skulle blitt implementert i ABB sin testlab ved et senere tidpunkt.

Vi har simulert ulike scenarier og hendelser for å sikre at systemet klarer å oppdage og fange opp trusler, generere relevante varsler som ønsket og produsere logger som gir en detaljert innsikt i hele nettverket.

Selv om prosessen har vert vellykket, har det også vert utfordringer underveis. Noen av disse inkluderer forsinkelser fra oppdragsgiver, samt mangel på nødvendig kunnskap rundt QRadar og installasjonsprosessen. I tillegg inkluderer dette også kompleksiteten i integrasjonen med virtuelle maskiner og nettverkskomponenter samt nødvendigheten for å tilpasse konfigurasjonen til vårt behov. Vi har imidlertid vært istand til å overvinne disse utfordringene ved hjelp av et godt samarbeid og god teknisk kompetanse og kreativitet.

Det er også viktig å fortsette med å oppdatere og vedlikeholde QRadar-systemet over tid om det er installert i et nettverk hos en organisasjon. Dette for å sikre optimal ytelse og beskyttelse over tid. Dette innebærer regelmessig oppdatering av programvare og tilleggsprogrammer, overvåking av sikkerhetstilstand og kontinuerlig opplæring av ansatte.

For å konkludere så vil vi si at installeringen og konfigurering av QRadar har vært vellykket, og systemet har gitt oss et kraftig verktøy for overvåking og beskyttelse av nettverk i forskjellige størrelser. Vi har med dette etablert et

solid fundament for nettverkssikkerhet og er bedre rustet til å implementere et system som kan oppdage og respondere på trusler i sanntid.

Oppsummert har prosjektet vært en suksess, og vi ser frem til å dra nytte av både kunnskapen vi har tilegnet oss og systemets funksjoner og bidra med å styrke vår egen og eventuelle bedrifters nettverkssikkerhet over tid.

Referanser

[1] *ABB*, in *Wikipedia*, Page Version ID: 23240671, Jan. 16, 2023. [Online]. Available: https://no.wikipedia.org/w/index.php?title=ABB&oldid=23240671 (visited on 02/27/2023).

[2] S. M. M. Hossain, J. Rusk, R. Couturier, and K. B. Kent, "Automatic event categorizer for SIEM," 2021.

[3] "QRadar: Important auto update server changes for administrators." (Nov. 10, 2021), [Online]. Available: https://www.ibm.com/support/pages/qradar-important-auto-update-server-changes-administrators (visited on 04/11/2023).

[4] "WinCollect overview - TechLibrary - juniper networks." (), [Online]. Available: https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-wincollect-user-guide/topics/concept/jsa-wincollect-wincollect-overview.html (visited on 05/08/2023).

[5] R. Qradar Rules. "Qradar rules." (Mar. 6, 2023), [Online]. Available: https://www.ibm.com/docs/en/qsip/7.5?topic=rules-custom (visited on 04/19/2023).

[6] T. Authentication. "What is an authentication token?" Fortinet. (), [Online]. Available: https://www.fortinet.com/resources/cyberglossary/authentication-token (visited on 04/25/2023).

[7] Q. IBM. "Qradar assistant." (Oct. 3, 2022), [Online]. Available: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-assistant-app (visited on 04/26/2023).

[8] I. Deployment. "IBM deployment intelligence app." (Jan. 24, 2023), [Online]. Available: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-deployment-intelligence-app (visited on 04/25/2023).

[9] Q. IBM. "Qradar pulse." (Apr. 11, 2023), [Online]. Available: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-pulse-app (visited on 04/26/2023).

[10] Q. IBM. "Experience center." (Aug. 24, 2022), [Online]. Available: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-experience-center-app (visited on 04/26/2023).

[11] Q. IBM. "Log source manager." (Feb. 16, 2023), [Online]. Available: https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-log-source-management-app (visited on 04/26/2023).

Forkortelser og ordforklaringer

Forkortelser

CLI Command Line Interface. 27, 29

CRE Custom Rules Engine. 16

GUI Graphical User Interface. 29, 30

IP Internet Protocol. 13, 16, 17, 21, 28, 32, 34, 36–38

IT Informasjons Teknologi. 12, 15, 38

OT Operasjons Teknologi. 12

PPTP Point-to-Point Tunneling Protocol. 34, 35

QRM Qradar Risk Manager. 16

QVM Qradar Vulnerability Manager. 16

RHEL Red Hat Enterprise Linux. 22

RNRP Redundant Network Protocol. 10–12, 19

SIEM Security Information and Event Management. 3–5, 7–12, 14–16, 20, 21, 23, 38

SLES SUSE Linux Enterprise Server. 22

SSH Secure Shell. 6, 7, 29, 30, 42

TCP Technical Control Protocol. 13, 21

VPN Virtual Private Network. 16, 19, 20

Ordforklaringer

800xA ABB sitt eget prossesskontroll system. 4, 8, 10–12, 19, 21, 23, 33, 43, 44

LogRhythm SIEM software utviklet av LogRhythm inc. 8, 10

PowerShell CLI programvare utviklet av Windows. 7, 29, 30, 41

QRadar SIEM software utviklet av IBM. 3–8, 10–35, 37–44

Splunk SIEM software utviklet av Splunk inc. 8

Virtual Box Programvare for å lage virtuelle maskiner. 12, 19, 27, 32

VM-Ware Software for å kjøre virtuelle maskiner. 19

WinCollect Software for a samle og sende informasjon til Qradar. 6, 7, 33