24/7 SOC

Kaster vi penger på luftslott?

Alexander Hatlen

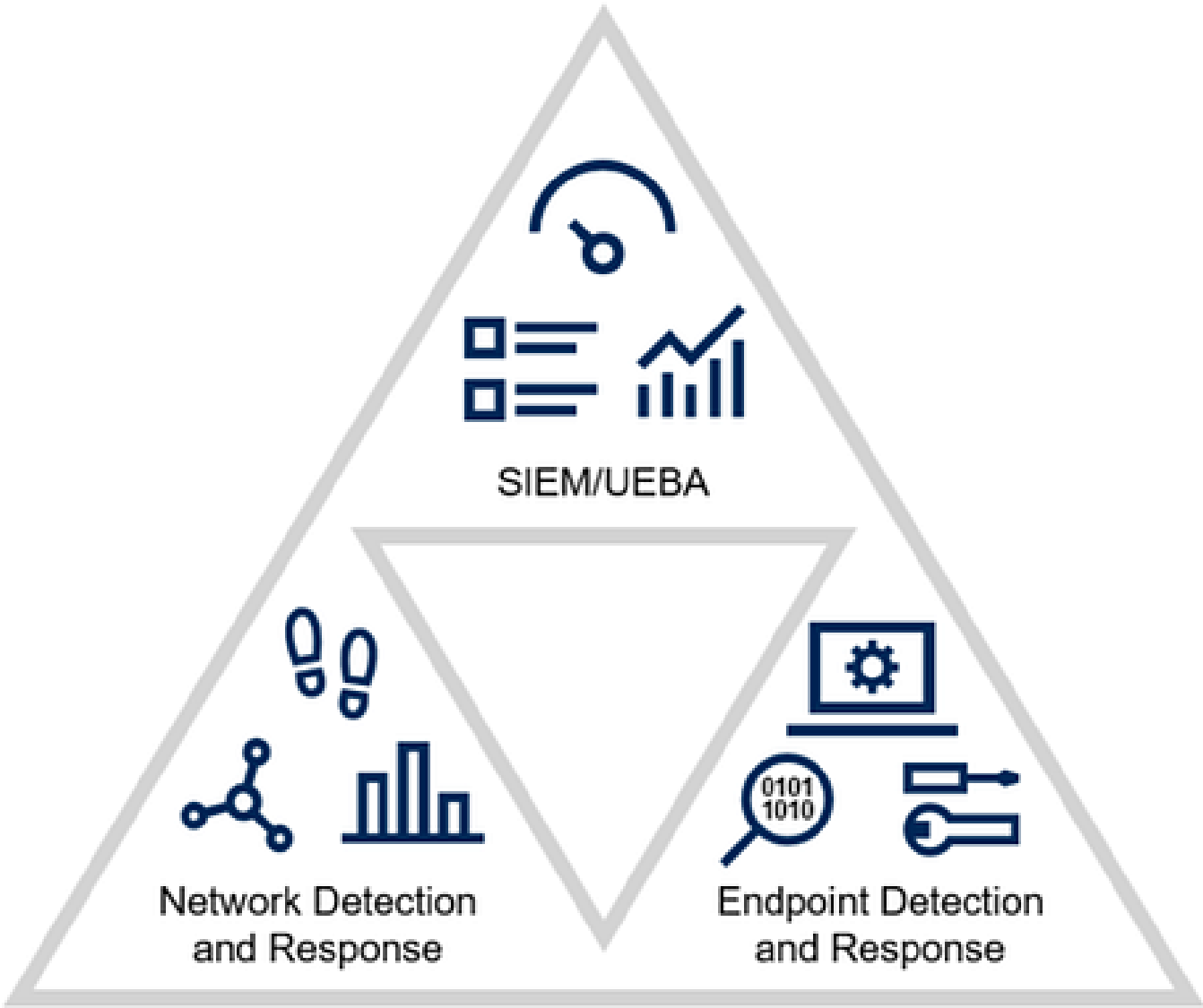
IT-sikkerhetsansvarlig

IT-seksjonen, Horten Kommune

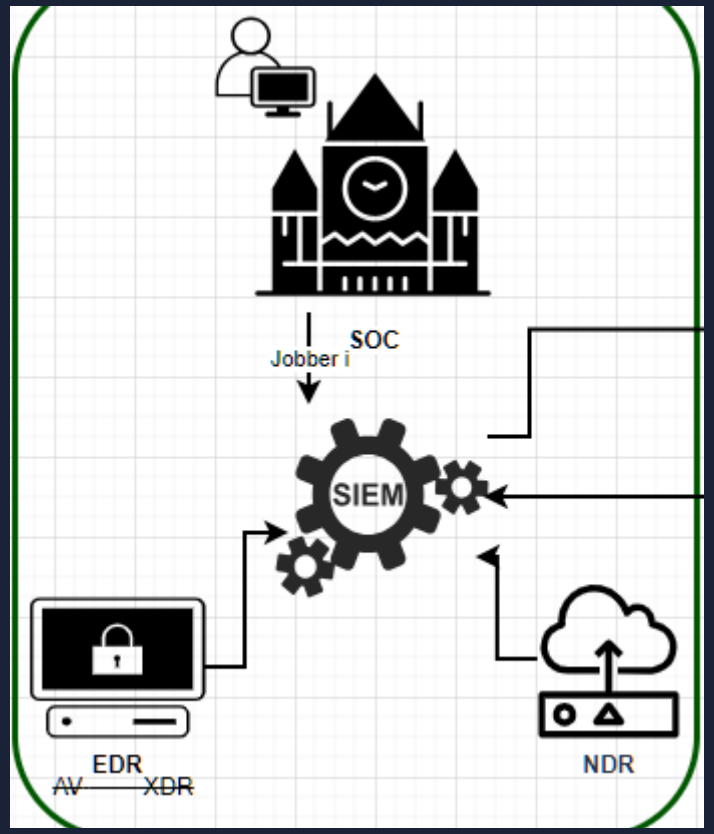
- Få et overblikk over produkter og tjenester
- Spørreundersøkelse
- Tema-monolog

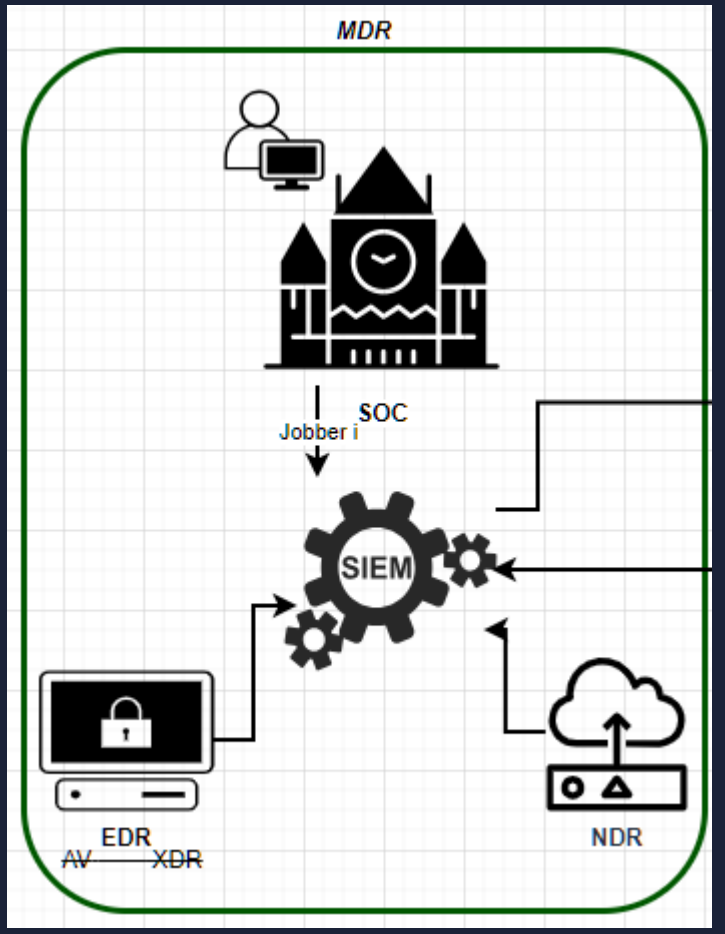
Begreps-suppe

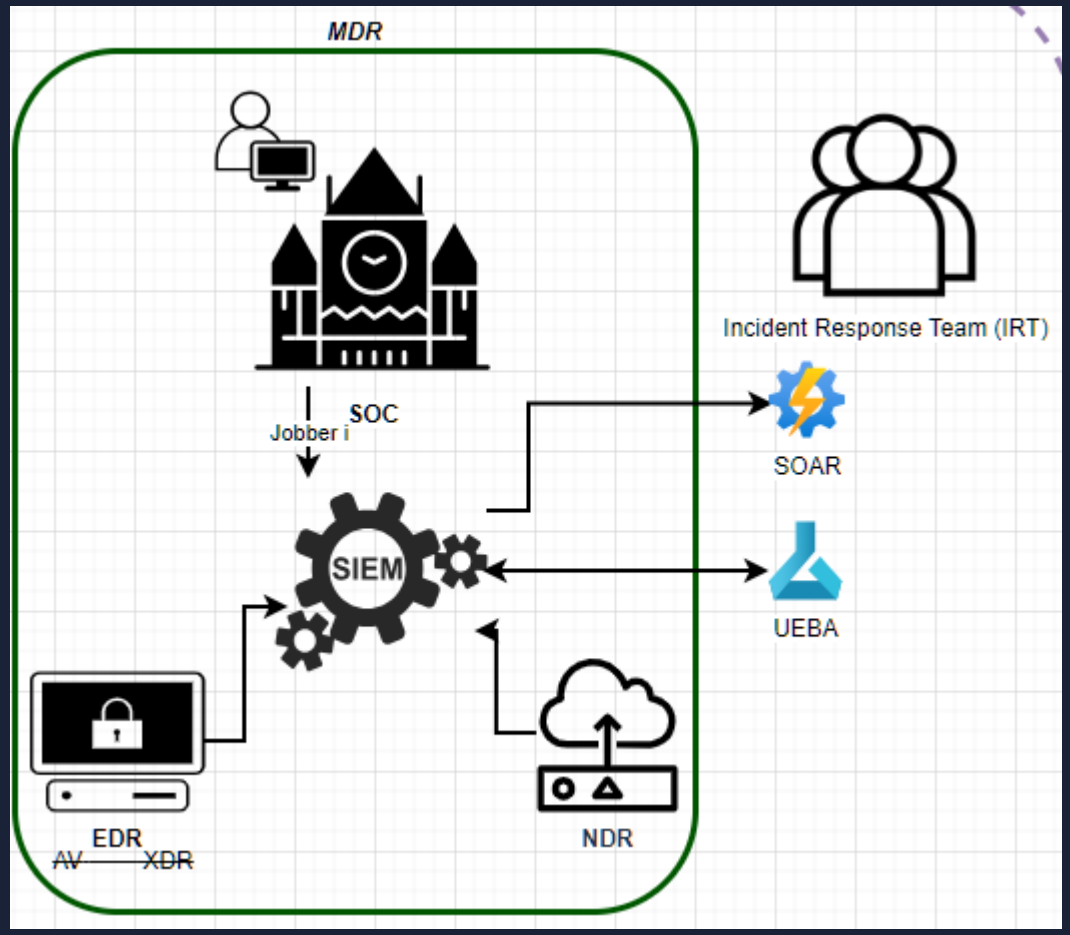
SOC Visibility Triad

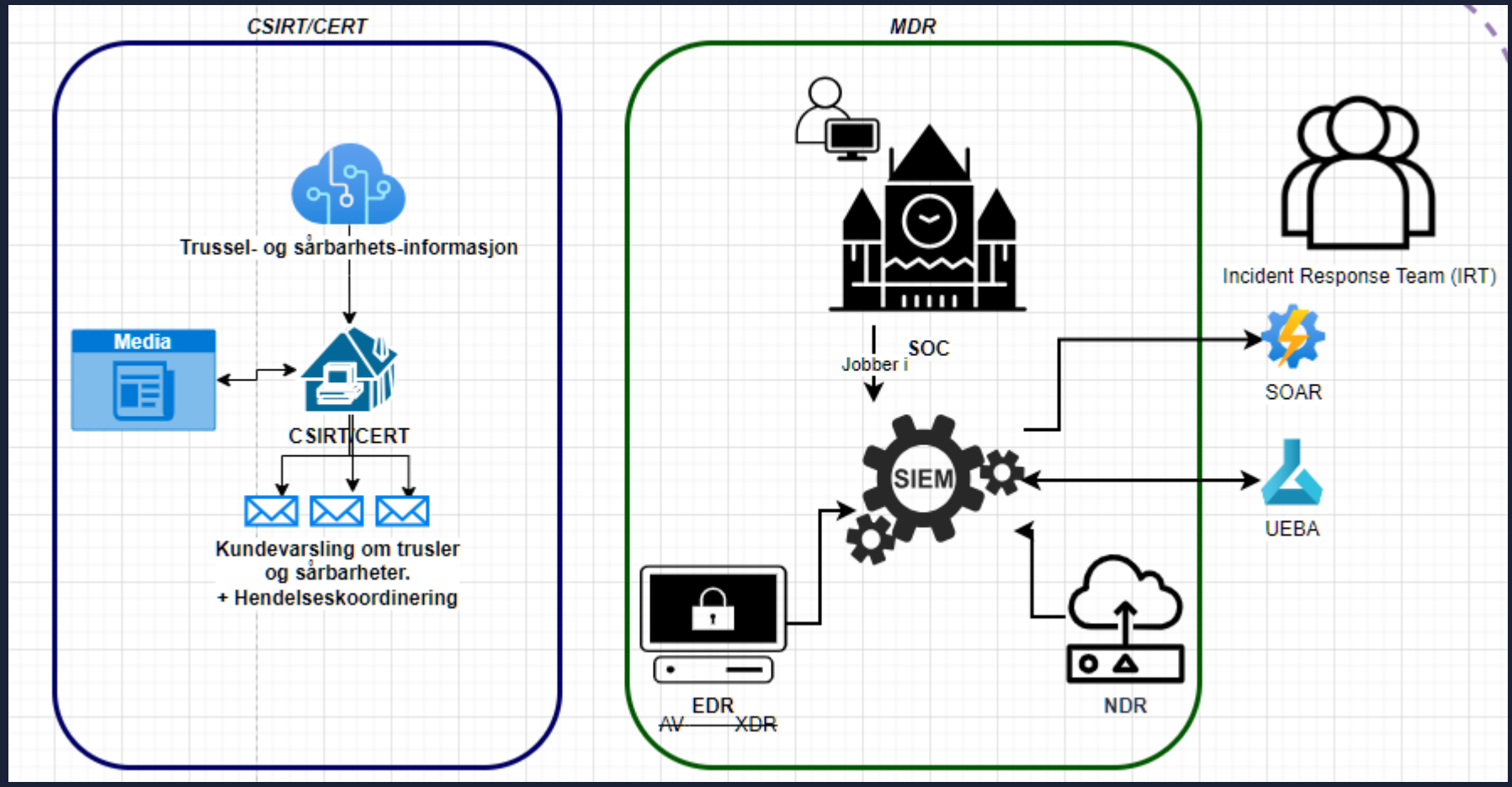


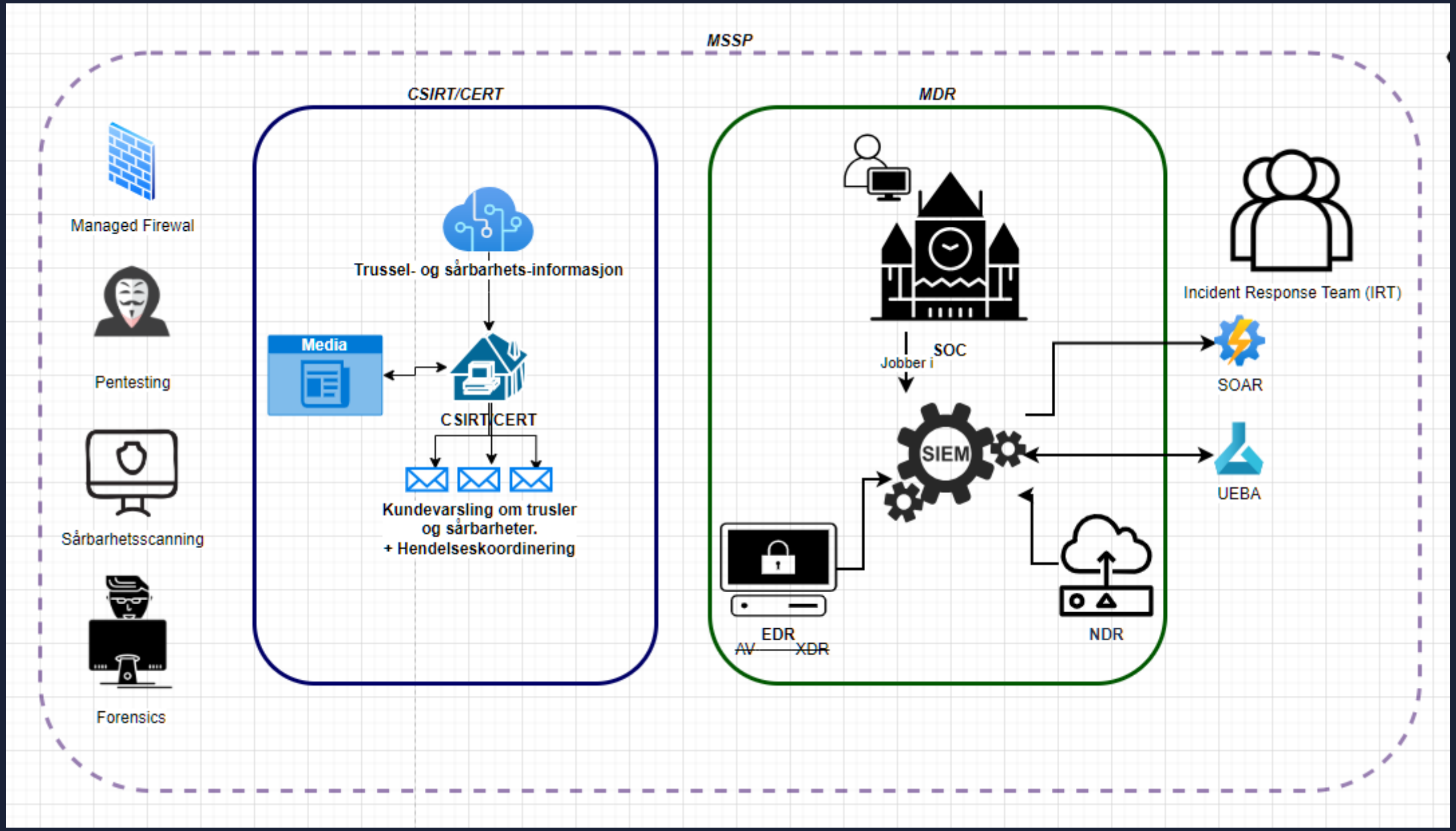
ID: 373460


Jobber i
SOC
SIEM
EDR
~~AV~~ ~~XDR~~
NDR


MDR
SOC
Jobber i
SIEM
EDR
AV
XDR
NDR


MDR
Incident Response Team (IRT)
SOC
Jobber i
SOAR
SIEM
UEBA
EDR
AV XDR
NDR


CSIRT/CERT
Trussel- og sårbarhets-informasjon
Media
CSIRT/CERT
Kundevarsling om trusler
og sårbarheter.
+ Hendelseskoordinering
MDR
Jobber i SOC
SIEM
EDR
AV XDR
NDR
SOAR
UEBA
Incident Response Team (IRT)


MSSP
CSIRT/CERT
MDR
Managed Firewal
Pentesting
Sårbarhetsscanning
Forensics
Trussel- og sårbarhets-informasjon
Media
CSIRT/CERT
Kundevarsling om trusler
og sårbarheter.
+ Hendelseskoordinering
Jobber i SOC
SIEM
EDR
AV XDR
NDR
SOAR
UEBA
Incident Response Team (IRT)


Oh boy. This is a lot.

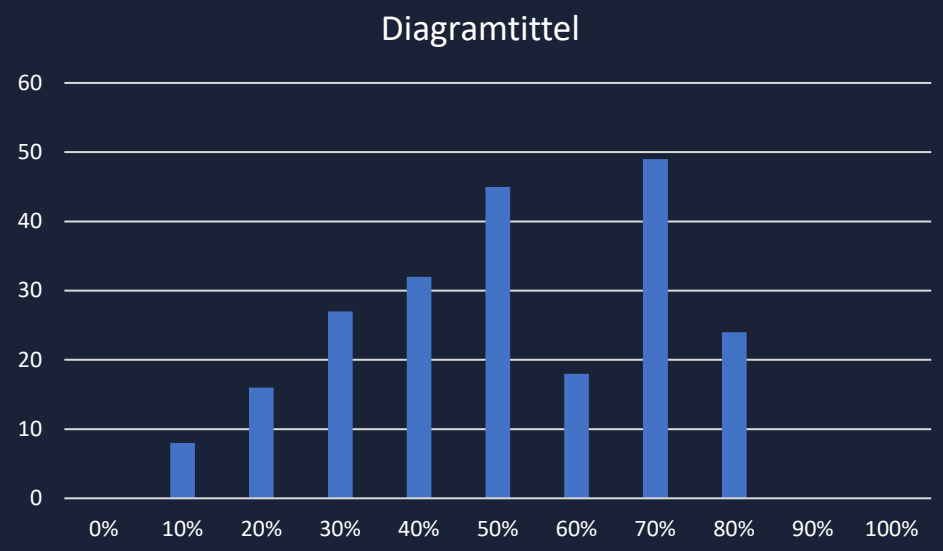

STOP

Spørreundersøkelsen

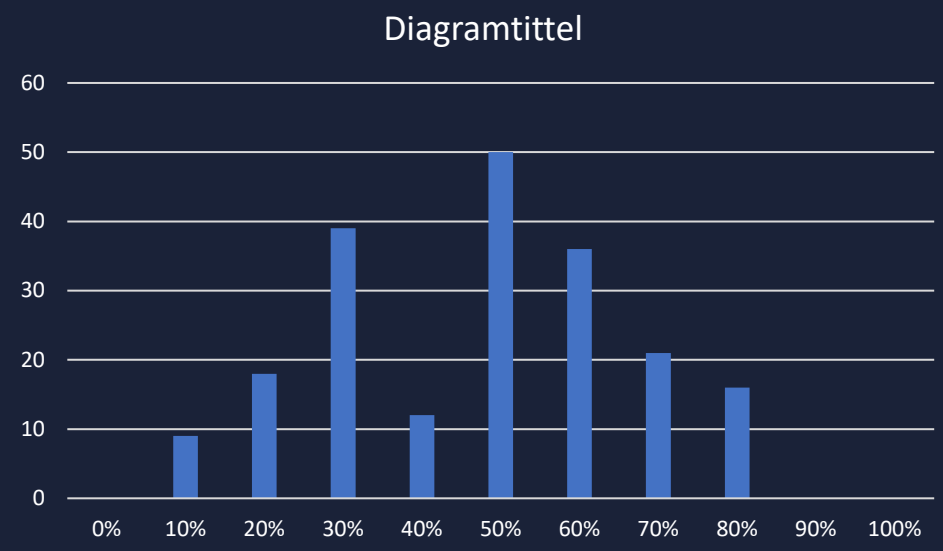
(Og et par avsporinger)

IT-ansatte: Hvor stor andel av [] tror du har en form for SOC?

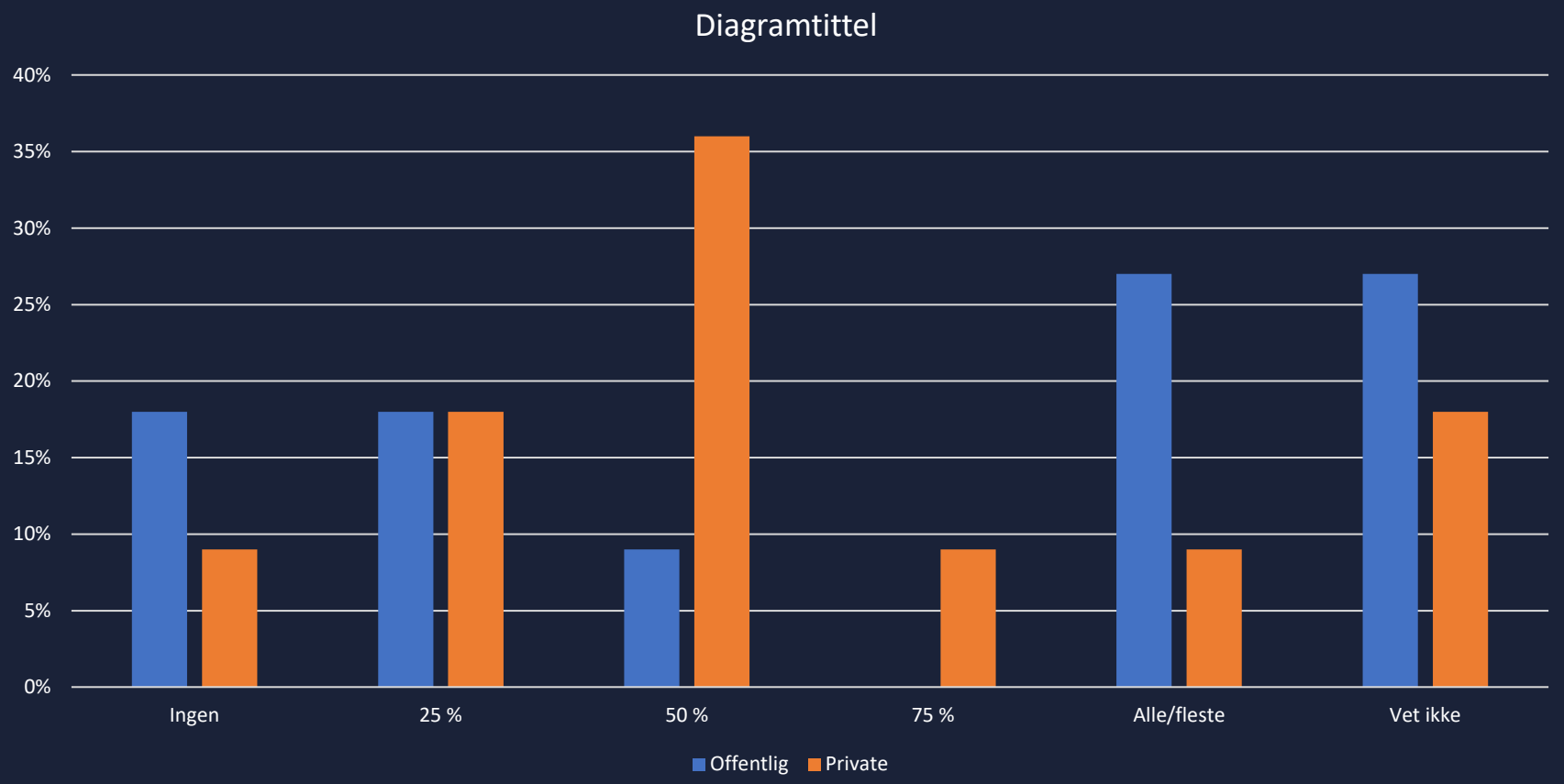
Offentlige organer



Private bedrifter



Sikkerhetstestere: Anslå hvor mange av kundene dine som har en SOC

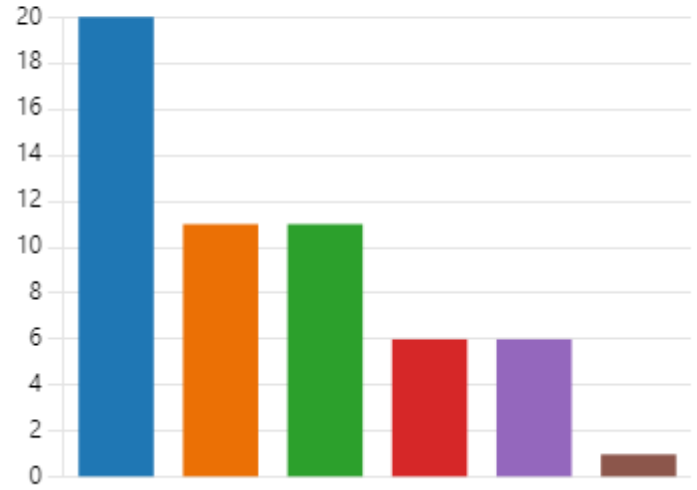


IT-ansatte: Hvor mange som faktisk har SOC!

3. Har din organisasjon en SOC?

Flere detaljer Innblikk

Ja, intern SOC	20
Ja, ekstern SOC	11
Ja, en hybrid intern/ekstern SOC	11
Nei, men vi har planer om å ans...	6
Nei, har ikke planer om å anskaf...	6
Annet	1

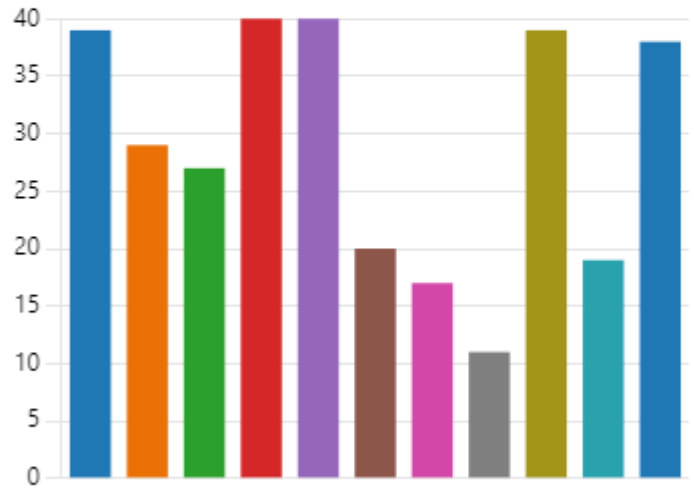


IT-ansatte: Forventningene til en SOC

7. Hvilke av disse tjenestene tenker du bør medfølge som et minimum i en ekstern SOC-tjeneste, uten ekstra opsjoner og kostnader?

Flere detaljer

Statistikkrapporter	39
Lagring av rå-logger	29
At du som kunde kan gjøre spør...	27
IR, Incident Reponse / hendelse...	40
Generell trusselinformasjon / va...	40
CERT-funksjon som hjelper deg ...	20
EDR-agent, endepunktsbeskytte...	17
Brannmur	11
At leverandøren lager alarm-reg...	39
At leverandøren lager alarm-reg...	19
Automasjon (SOAR)	38

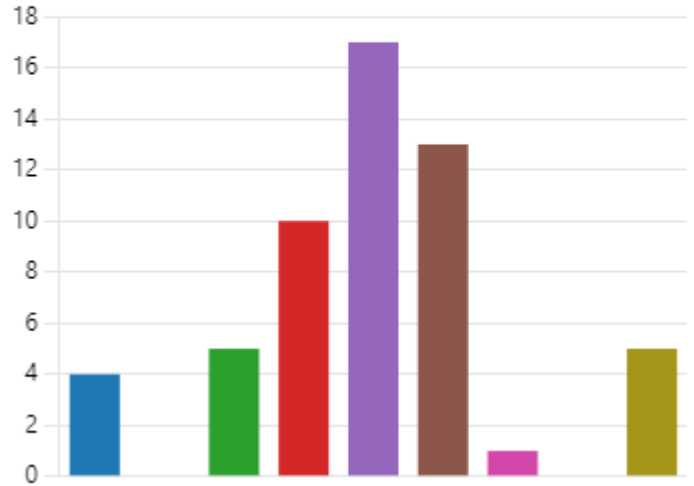


IT-ansatte: Lagringstid for logger

8. Hvor lenge tenker du en ekstern SOC lagrer rå-logger? (Når ikke annet er avtalt)

Flere detaljer Innblikk

Kun lenge nok til å lage alarmer ...	4
Et døgn	0
En uke	5
En måned	10
Noen måneder	17
Ett år	13
Noen år	1
Evig	0
Annet	5

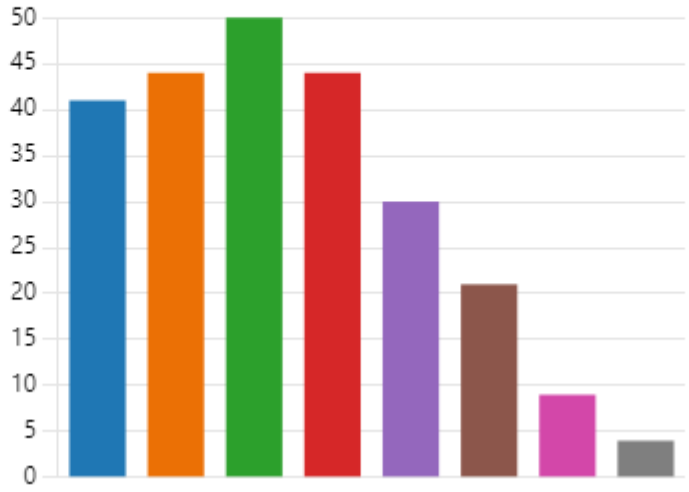


IT-ansatte: SOAR i praksis

9. Hvilke av disse punktene ville du latt en automatisert sikkerhetstjeneste gjøre ("SOAR")?

Flere detaljer

Kreve passordbytte på brukere	41
Starte antivirus-søk	44
Låse brukerkontoer	50
Låse maskinkontoer	44
Låse/isolere/stenge ned servere	30
Koble fra nettverkssoner	21
Koble organisasjonen fra internett	9
Annet	4



IT-ansatte: Leverandørs tilganger i driftsmiljøet ditt

Alt som behøves

Least privilege

Så lite som mulig

Global admin ved pim/pam

«Kommer an på avtalen som ligger til grunn, vår SOC har mandat til å iverkstette tiltak uten å måtte få godkjenning først»

Full tilgang, de må kunne handle raskt.

Egentlig ikke så veldig mye... paradoksalt dette her.

Egne (personlige) SOC-konti som har tilgang til EDR, brannmur, IDS/IDP, og nettverksinfrastruktur, men ingen direkte filtilgang. Servicekonti til EDR, som lar SOCen karantene / fjerne filer. SOC bør ha tilgang til AD for låsing av bruker- og maskinkonti, men strengt innsnevret tilgang ellers.

This guy/gal SOCs!

Prioriteringer

IT-ansatte

12. Rangér disse tiltakene ut i fra hva du tenker organisasjoner bør prioritere, fra mest prioritert (øverst) til minst prioritert (nederst)

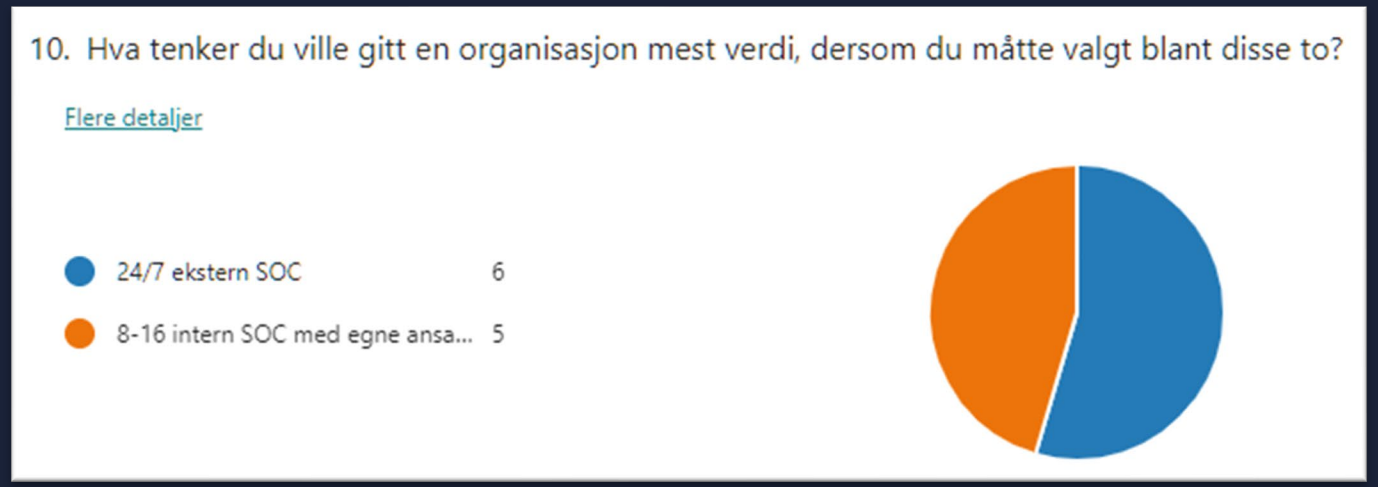
Flere detaljer

Sikkerhetstestere

8. Plasser disse tiltakene ut i fra hva du tenker organisasjonen bør prioritere, fra mest prioritert (øverst) til minst prioritert (nederst)

Flere detaljer

Interessante tilbakemeldinger fra sikkerhetstestere



Hvis du har erfaring fra kunder med SOC, kan du si noe om deres deteksjonskapabilitet?

Ofte god deteksjonsevne på endepunkt (via EDR eller lignende løsninger), kommer du rundt endepuntks løsningen er det vanskelig å oppdage hva som skjer. Varierende grad av deteksjonsevne på nettverkstrafikk som ikke går via en ekstern brannmur.

Dette varierer veldig. Noen er veldig modne med veldig bra deteksjonskapabiliteter mens andre klarer ikke detektere deg uansett hvor mye du prøver å støye (føles det ut som ihvertfall). I en del tilfeller så får SOC skylden når dette skjer, det kan jo godt hende de har dårlige deteksjoner, men veldig ofte så mangler de telemetry fra kunden og har da ikke muligheten til å detektere angrepene. Derfor er det også viktig og teste at deteksjoner og forventninger for å sørge for at ting fungerer som det skal.

«Ikke glem at leverandører må følges opp, de er ofte der for å spille en bedrift gode, men man må kunne være med å spille, ikke bare overlate alt til leverandøren og late som problemet er borte.»

Fungerer SOC, eller er det luftslott?

Sikkerhetstestere:

3. Har du noen gang hatt et oppdrag hvor kunden har en SOC som *burde* ha oppdaget deg, men ikke gjorde det?

Flere detaljer

Ja	10
Nei	1
Ikke relevant, har ikke hatt kund...	0
Annet	0

4. Har en kundes SOC noen gang forhindret deg i å klare å fullføre et oppdrag?

Flere detaljer

Ja	6
Nei, og jeg har erfaring fra kund...	3
Ikke relevant, har ikke hatt kund...	0
Annet	2

5. Har du blitt oppdaget av en kundes SOC *etter* et oppdrag?

Flere detaljer Innblikk

Ja	6
Nei / ikke som jeg vet	3
Annet	2

IT-ansatte

4. HVIS JA: Har SOCen forhindret et angrep som ellers ville vært suksessfullt?

Flere detaljer

Ja	22
Nei	12
Vet ikke	10
Annet	0

Erfaringer med SOC

Primært falske positive. Opplever at det krever mye å vurdere alarmer, og at SoC ofte lar junior analytikere vurdere alarmene og deretter la oss som kunde gjøre egne vurderinger. Mangler ofte anbefalinger knyttet til enkelthendelser.

SOC merker stor forskjell ut fra hvilket EDR/SIEM som blir brukt. Sentinel/Defender og Cortex XDR. Er klart best. Husk også at custom regler er veldig viktig for tjenestene.

«Noen ganger oppdager vi hendelser og responderer lenge før vi blir kontaktet av SOC.
Andre ganger fanger SOC opp hendelser som ingen andre av våre mekanismer har plukket opp på.»

Canary Tokens

hvor alle logger blir alarmverdig

Ta med seg hjem / protips

- Gøran, KS, NIST og NSM sine anbefalinger for anskaffelse-kravspec og anbefalte loggkilder: https://gorantomte.no/anbefalinger-til-krav-i-en-soc-foresporsel/
- Ha en god forståelse av hva du vil oppnå med anskaffelsen.
- Prioriteringsrekkefølge. Se på dagens tech stack for å velge mdr eller soc, EDR og SOC henger tett sammen.
- Elastic Stack er en SIEM med EDR-agent, loggagenter og har et community repo av regler. GCHQ har en guide; https://github.com/ukncsc/lme («Logging made easy»)
- Be om opsjon på resten av forkortelsene, eller kjøp de andre steder. Ikke utelukk en god SOC som ikke tilbyr pentest.
- Din tilgang til dine loggdata – hvem eier loggene og hvor lett er de å søke i for å kunne gi deg operasjonell verdi i drift?
- Vurder en prismodell som lar deg logge mest mulig, gjerne 13 måneder+. Husk at hvis du lagrer loggene selv (Log Analytics i din tenant for eksempel) kan det være skjulte kostnader på mange hundretusen.
- Ansvarsskille leverandør / kunde. Hvor mye «manpower» følger med i avtalen?
  Eks: Implementering av regelønsker, tidsbruk hos en SOC-analyst før IR-teamet begynner å ta betalt, veiledning
- Alert tuning: Vær forberedt på å stille dine ressurser til rådighet når SOCen onboarder deg. Du MÅ hjelpe de å finne endepunktene dine, rulle ut agenter og ikke minst tune regler i et par måneder! Tuning av regler bør skje så spesifikt som mulig.
- Avklare Eskaleringsplan:hva en leverandør skal og kan gjøre ved forskjellige kritikalitetsnivå, også når de ikke får tak i deg
- Leverandørs tilgangsnivå inn i din organisasjon. Både SOARens rettigheter, samt SOC/IR teamets rettigheter.
- Risiko med lovnad om få falske positive: hva går du glipp av?
- Kontrollspørsmål til leverandør: hvordan gjør de kundesegmentering? Loggene dine innwholder ofte mye sikkerhetskritisk informasjon!
- Er du moden nok til å teste SOCen din; lag noen scenario utifra din forrige pentest eller MITRE ATT&CK og se om de detekterer det. (Stikkprøver)
- Plant Honey Tokens i miljøet ditt, og implementer varsler på disse i SIEM/SOCen.
- Husk at alle IRT på NSM sin kvalitetsordning plikter å yte 24/7 respons også for ikke-eksisterende kunder!
- Husk at en SOC er reaktiv. Du har ikke kjøpt sikkerhet, den forhindrer ikke angrep. Du har kjøpt alarm, men trenger fortsatt dørlås!

Alexander Hatlen

Konklusjon