Silje Bakken | Cybersikkerhetsingeniør | SOC, hendelseshåndtering og skysikkerhet

Storgata 12, Oslo, Oslo, Norge, 0155
+47 123 45 678 • silje.bakken@protonmail.com • https://siljebakken.no
@siljebakken • @siljebakken

Grunnleggende informasjon

- Erfaren cybersikkerhetsingeniør med mastergrad i informasjonssikkerhet og 8 års erfaring fra SOC, hendelseshåndtering og sikkerhetsarkitektur.
- Spesialisert i trusseldeteksjon, logganalyse og automatisering av sikkerhetsprosesser i Microsoft Sentinel, Splunk og QRadar.
- Har ledet hendelsesrespons for kritisk infrastruktur og redusert responstid gjennom SOAR-playbooks og KQL-baserte deteksjoner.
- Sterk på risikovurdering, MITRE ATT&CK, sikkerhetsrevisjoner og samarbeid på tvers av teknologi-, drift- og ledelsesmiljøer.
- Opptatt av å bygge en proaktiv sikkerhetskultur gjennom opplæring, mentorvirksomhet og tydelig dokumentasjon.

Utdanning

Norges teknisk-naturvitenskapelige universitet **https://www.ntnu.no**
Master, Informasjonssikkerhet, Poeng: A (5) *aug. 2014–juni 2016*

- Fordypning i kryptografi, nettverkssikkerhet og sikker systemutvikling
- Gjennomførte masterprosjekt om trusseldeteksjon i kritisk infrastruktur
- Utviklet praktisk erfaring med risikovurdering, sikkerhetsrevisjon og hendelseshåndtering

Kurs: Kryptografi og sikkerhetsprotokoller, Nettsikkerhet, Systemering av sikre systemer, Risikostyring og personvern, Digital etterforskning, Sikkerhetsarkitektur

Universitetet i Oslo **https://www.uio.no**
Bachelor, Informatikk, Poeng: B (4) *aug. 2011–juni 2014*

- Solid grunnlag i programmering, systemforståelse og datanettverk
- Arbeidet i prosjektgrupper med sikker utvikling og testing av programvare
- Skrev bacheloroppgave om autentisering og tilgangskontroll i webløsninger

Kurs: Algoritmer og datastrukturer, Operativsystemer, Databaser, Nettverk, Programmering i Java, Diskret matematikk

Arbeidserfaring

Nordisk Energisikkerhet AS **https://www.nordiskenergisikkerhet.no**
Senior cybersikkerhetsingeniør *mars 2021–Nå*

- Leder daglig SOC-drift for et energiselskap med kritisk infrastruktur og 24/7-overvåking
- Utvikler og forvalter deteksjonsregler i Microsoft Sentinel og Splunk med fokus på OT- og IT-konvergens
- Gjennomfører hendelsesrespons for komplekse hendelser, inkludert analyse, isolering og rapportering
- Bygget SOAR-playbooks som reduserte manuell prioritering med 35 % og forkortet gjennomsnittlig responsstid
- Fungerer som teknisk rådgiver i sikkerhetsarkitektur, risikovurderinger og leverandørrevisjoner

Nøkkelord: SOC, Microsoft Sentinel, Splunk, SOAR, OT-sikkerhet, Hendelseshåndtering

Bergen Sikkerhetsrådgivning AS **https://www.bergensikkerhet.no**
Cybersikkerhetsingeniør *aug. 2016–feb. 2021*

- Overvåket og analyserte sikkerhetshendelser for kunder i finans- og helsesektoren
- Implementerte og vedlikeholdt SIEM-løsninger (QRadar, ArcSight) og utviklet egne korrelasjonsregler
- Deltok i hendelsesrespons og digital etterforskning, inkludert innsamling av bevis og rapportering
- Gjennomførte sårbarhetsanalyser og penetrasjonstester i samarbeid med eksterne konsulenter
- Bidro til utvikling av sikkerhetspolicyer og opplæring av ansatte i sikker bevissthet

Nøkkelord: SIEM, QRadar, ArcSight, Sårbarhetsanalyse, Penetrasjonstesting, Digital etterforskning

Språk

Norsk: Morsmål eller tospråklig nivå — **Nøkkelord**: Morsmål

Engelsk: Fullt profesjonelt nivå — **Nøkkelord**: TOEFL 110, IELTS 7.5

Tysk: Begrenset arbeidskunnskap — **Nøkkelord**: Grunnleggende

Ferdigheter

Sikkerhetsovervåking (SOC): Ekspert — **Nøkkelord**: Microsoft Sentinel, Splunk, QRadar, ArcSight, Logganalyse

Trusseldeteksjon og hendelseshåndtering: Ekspert — **Nøkkelord**: MITRE ATT&CK, KQL, SOAR, Playbooks, Digital etterforskning

Skysikkerhet: Avansert — **Nøkkelord**: Azure Security, AWS Security, Zero Trust, Identity Management

Risiko og samsvar: Avansert — **Nøkkelord**: ISO 27001, GDPR, Risikovurdering, Sikkerhetsrevisjon

Programmering og automatisering: Viderekommen — **Nøkkelord**: Python, PowerShell, Bash, KQL, REST API

Utmerkelser

Årets sikkerhetsprosjekt
Nordisk Energisikkerhet AS *nov. 2022*

- Anerkjent for utvikling av en automatisert hendelsesresponsplattform som reduserte responstiden med 40 %.

Sertifikater

CISSP **https://www.isc2.org/certifications/cissp**
(ISC)² *juni 2020*

Azure Security Engineer Associate **https://learn.microsoft.com/en-us/certifications/azure-security-engineer/**
Microsoft *sep. 2021*

CISM **https://www.isaca.org/credentialing/cism**
ISACA *mars 2019*

Publikasjoner

Norsk Informasjonssikkerhetskonferanse **https://www.nisk.no/paper/2018**
Detecting Advanced Persistent Threats in Critical Infrastructure *okt. 2018*

- Presenterer en metode for å oppdage APT-angrep i OT-miljøer ved hjelp av maskinlæring og nettverksanalyse.

Prosjekter

Sanntids trusseldeteksjon for OT-nettverk **https://github.com/siljebakken/ot-threat-detec**
Et åpent kildekode-prosjekt for å detektere unormal aktivitet i industrielle kontrollsystemer. *jan. 2020–des.*

- Utviklet en deteksjonsmotor basert på Python og Scapy for å analysere Modbus- og DNP3-trafikk.
- Implementerte varsling til Slack og Microsoft Teams ved mistenkelig aktivitet.
- Testet løsningen i et simulert OT-miljø med gode resultater.

Nøkkelord: OT-sikkerhet, Python, Scapy, Modbus, DNP3

Interesser

Sport: Fjellturer, Langrenn, Klatring

Musikk: Piano, Gitar

Frivillig arbeid

Women in Cybersecurity Norge **https://www.wics.no**

Mentor *jan. 2019–Nå*

- Mentorer unge kvinner som ønsker å starte karriere innen cybersikkerhet.
- Holder workshopserier om SOC-drift og hendelseshåndtering.
- Bidrar til å øke mangfoldet i sikkerhetsmiljøet.