

Hvordan bygge en fullverdig og kostnadseffektiv SLEM løsning i eget miljø.

Sindre Olsen & Esben Jørgensen



HORTEN
KOMMUNE

Hvem er vi?

- Sindre Master Data sikkerhet
IKT sikkerhetsrådgiver i Horten
Kommune
- Esben Bachelor Dataingeniør -
Cybersikkerhet
IKT sikkerhetskonsulent i
Horten Kommune



Agenda

- Logging
- Sentralisert logging
- Kostnadseffektiv SIEM
- Regeltuning
- Respons
- Oppsummering/Anbefalinger



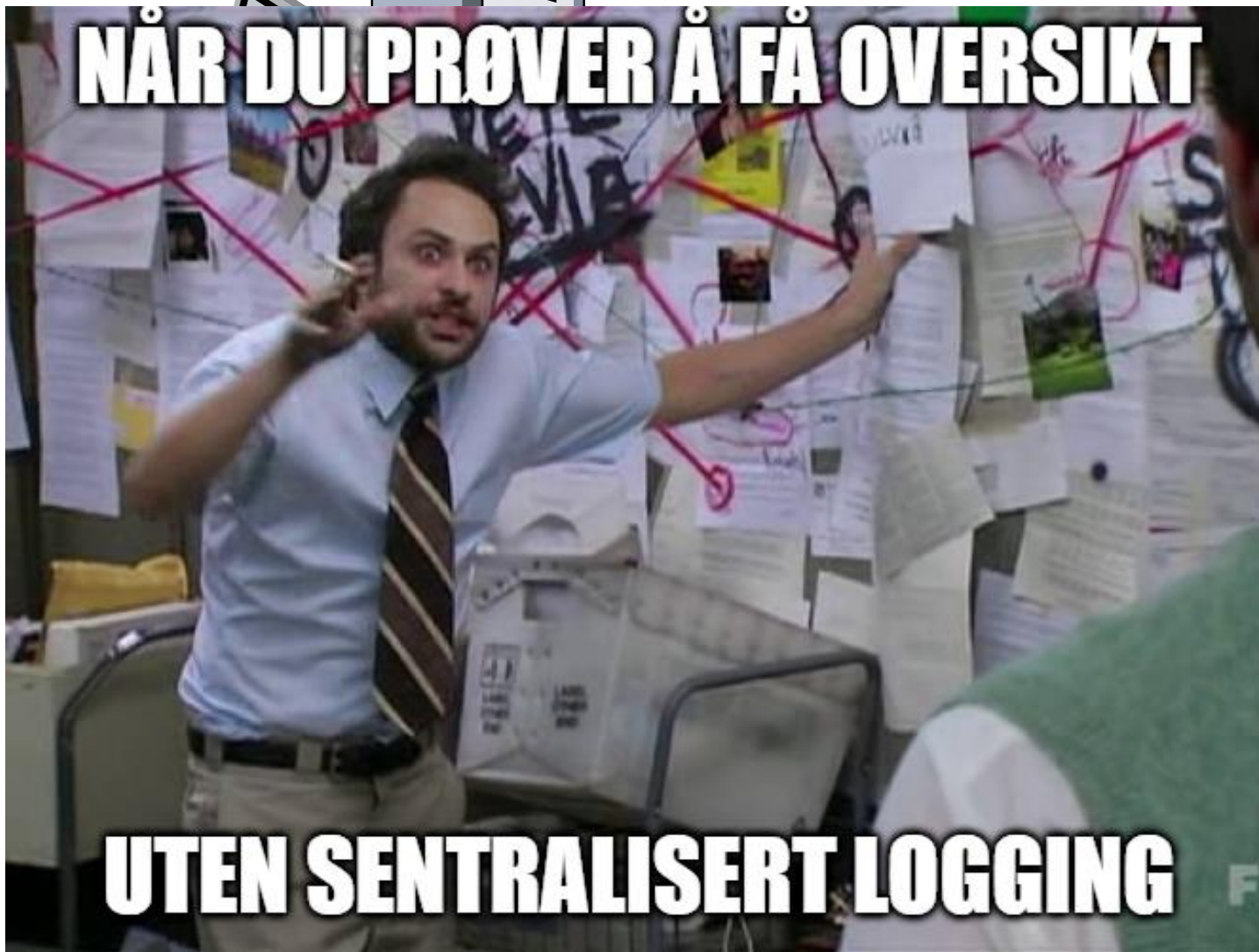


Logging

- Hvorfor logger?
 - Feilsøking
 - Sporbarhet (sikkerhet og drift)
 - Hvem, hva og når?
 - Tidslinje på angriper
- Må skrues på
 - Applikasjonslogger (debug/error/info)
 - Advanced Audit Configuration (Windows)
- Mange ulike loggkilder/formater
 - Klienter/Server, AD, Fagapplikasjoner, FW, Sky...
 - Manuell korrelering → tidkrevende
- Skripting vs kontinuerlig overvåkning



NÅR DU PRØVER Å FÅ OVERSIKT



UTEN SENTRALISERT LOGGING



HORTEN
KOMMUNE



CENTRALIZED LOGGING



Event Trends

Recent Log Entries

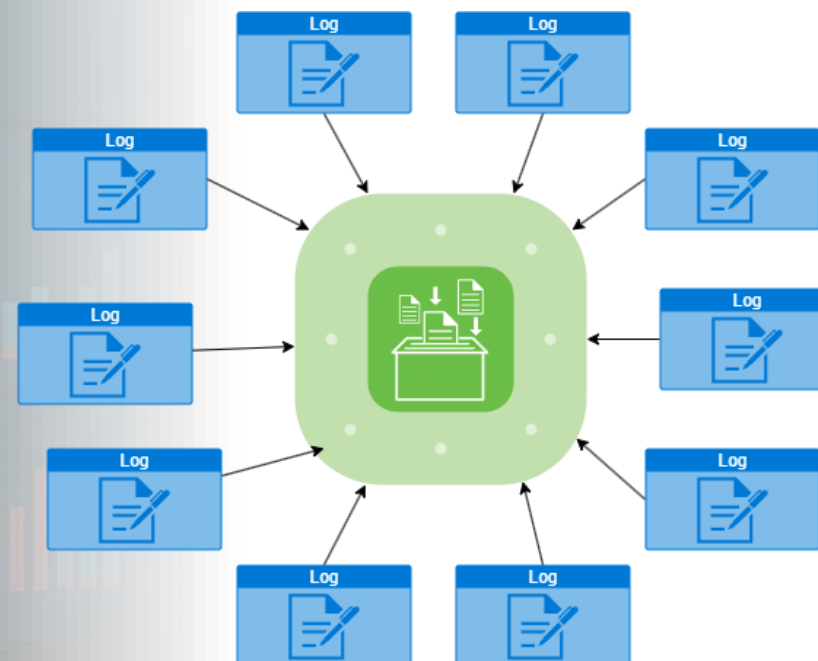
Timestamp	Event	Severity
10/09/2024 06:05:24.35	File Machine's Burnout	▲
10/09/2024 06:17:24.34	Event method: Belonged	▲
10/09/2024 06:07:24.34	Event method: Belonged	▲

Recent Log Entries



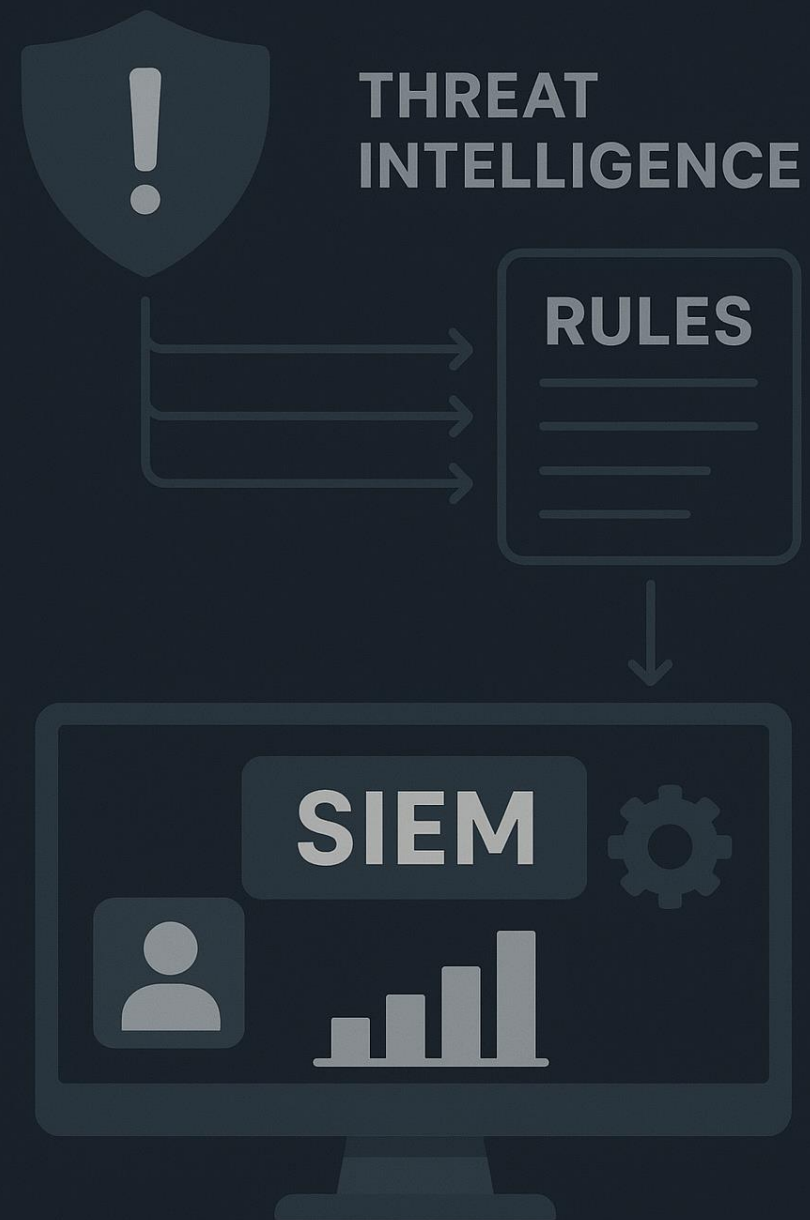
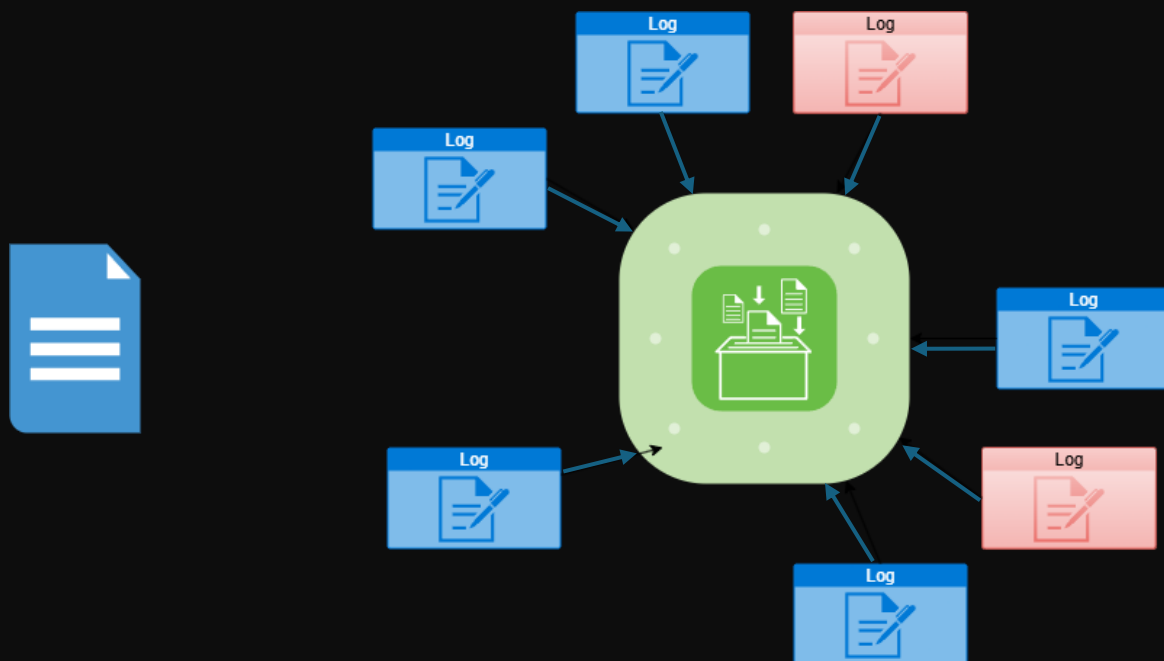
Sentralisert logging

- Sender alle logger til ett sted



Sentralisert logging

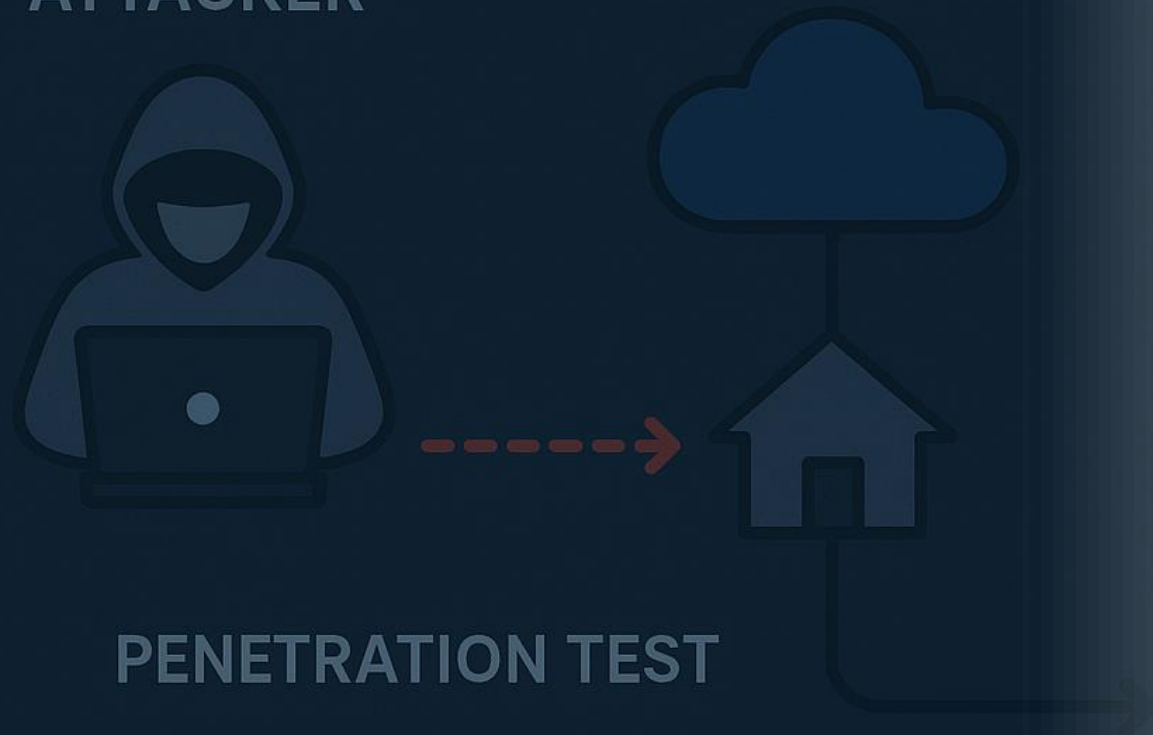
- Trussel → mangler logger → nye loggkilder



Sentralisert logging

ATTACKER

NETWORK

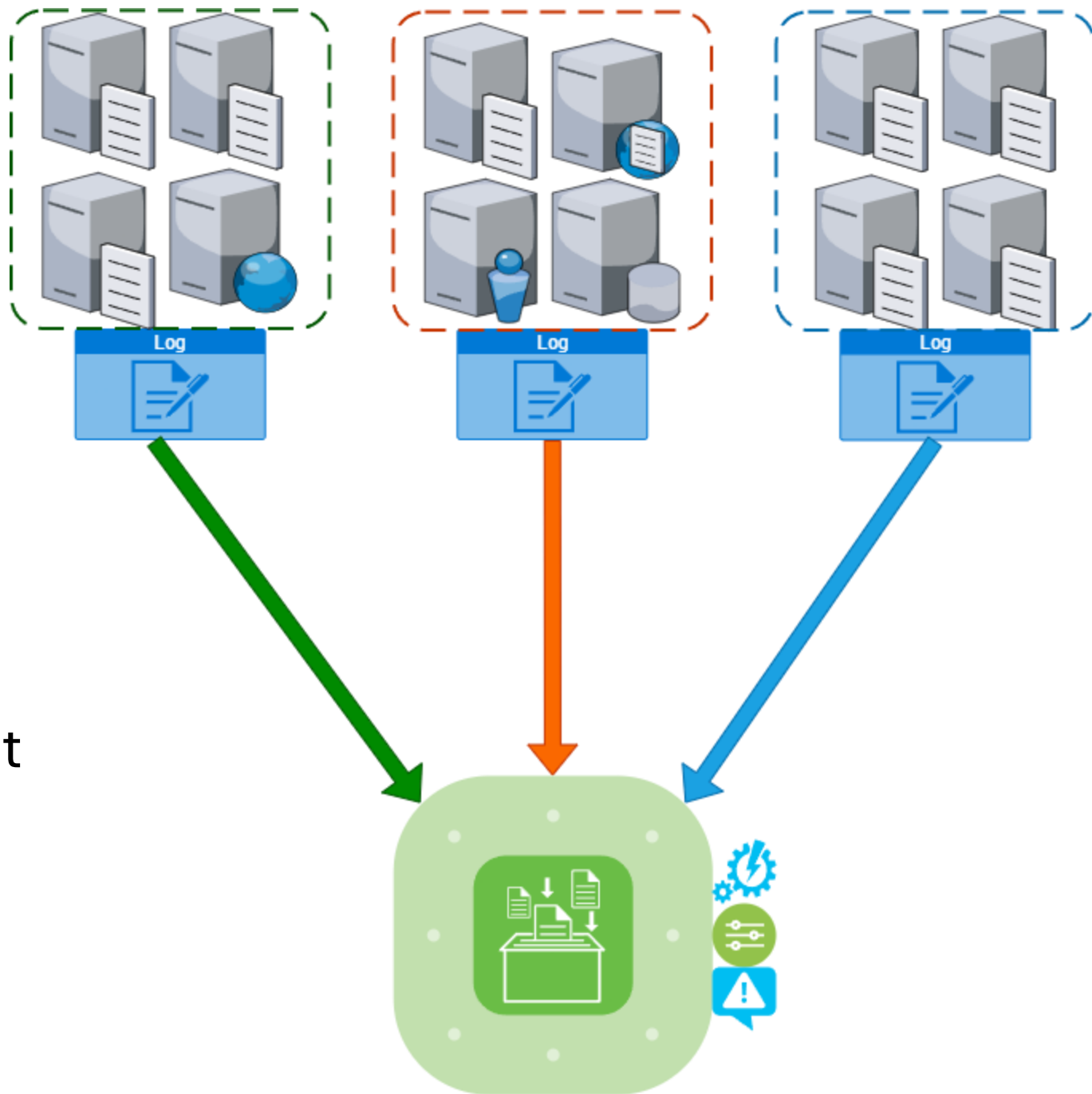


HORTEN
KOMMUNE

SIEM

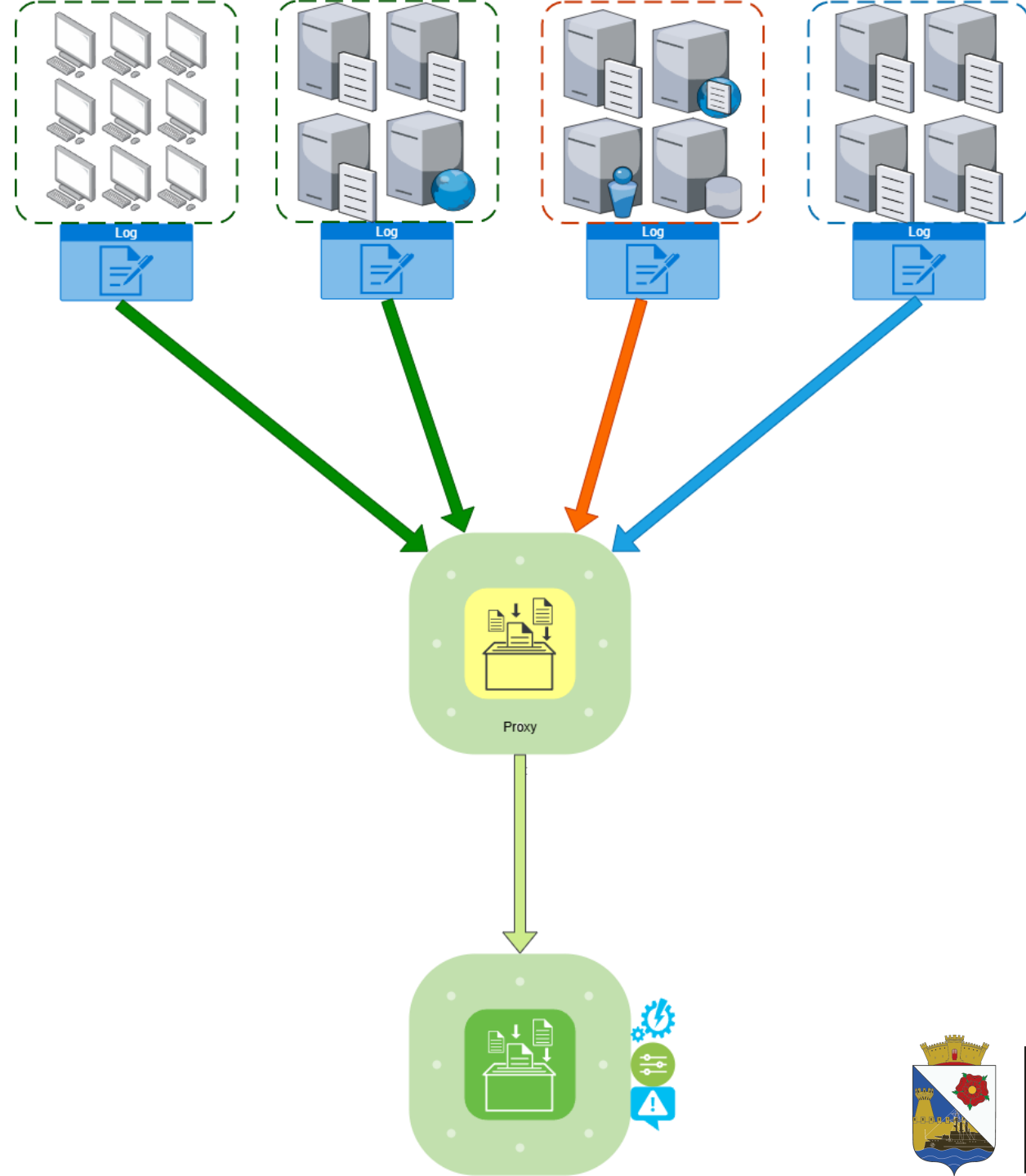
Security and Incident Event Management

- Automasjon
- Integrasjoner
- Regler
- Datakvalitet
- Prioriterte systemer først



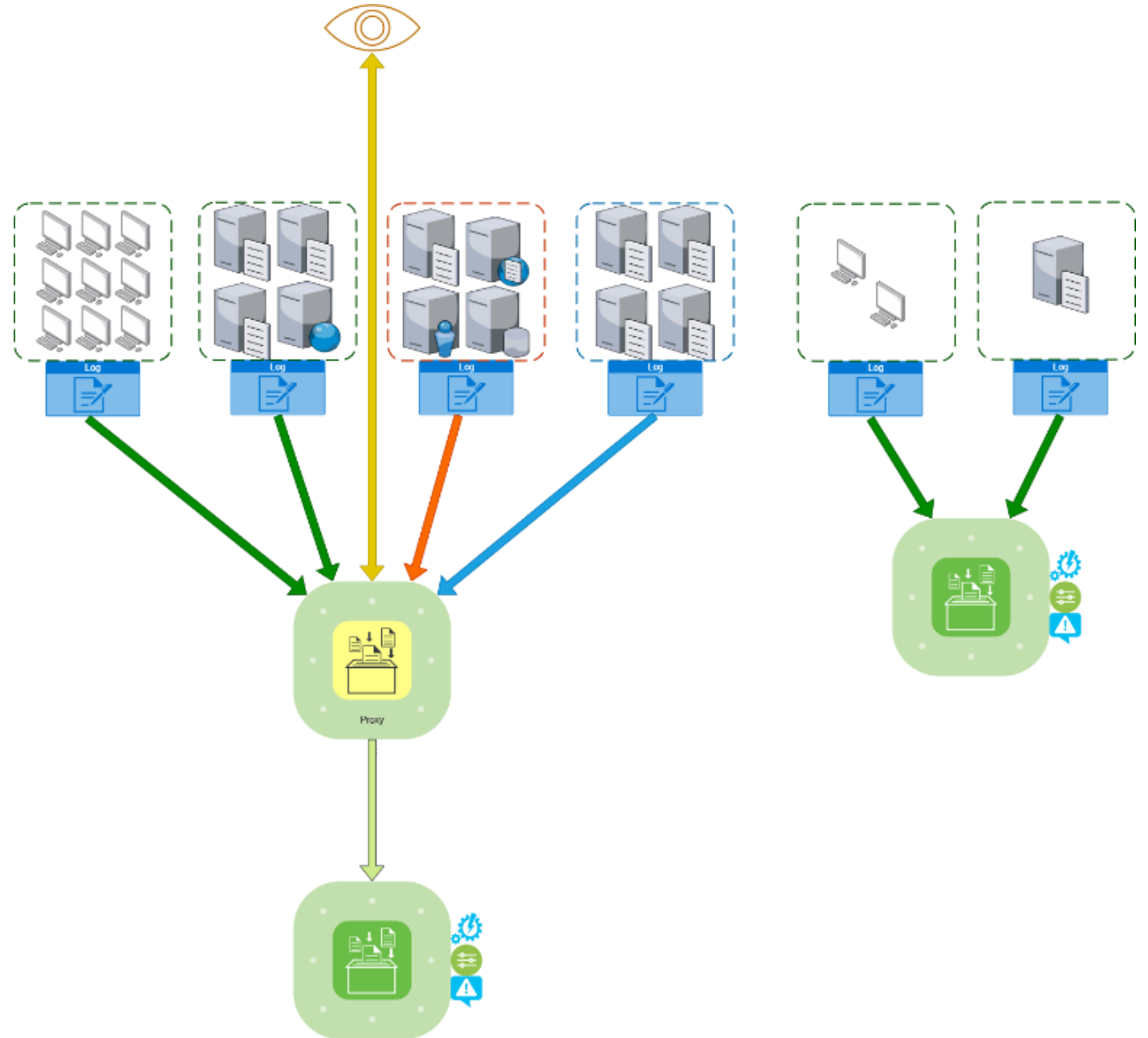
SIEM

- Klienter
- Proxy



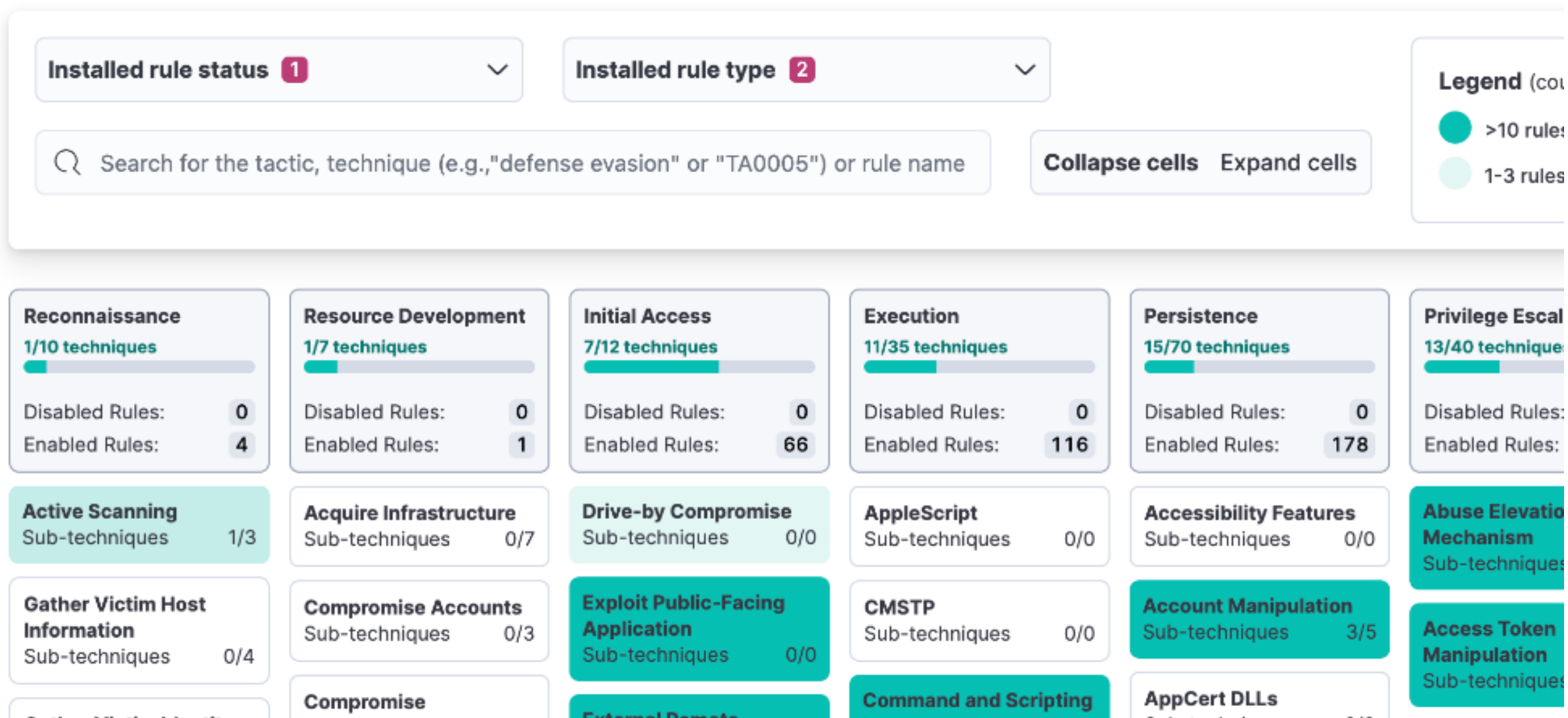
SIEM

- SOC
- Testmiljø
- Herding



MITRE ATT&CK® coverage

Your current coverage of MITRE ATT&CK® tactics and techniques, based on installed rules. Click a cell to view and enable a technique's rules. Rule framework to be displayed. [Learn more.](#) [🔗](#)



Flåtestyring

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Data streams](#)

Status ▾

Agent policy 3 ▾

Upgrade available

[+ Add agent](#)

Showing 9 agents

● Healthy 3 ● Unhealthy 0 ● Updating 2 ● Offline 4

☐	Host	Status	Agent policy	Version	Last activity	Actions
☐	901300820c15	Updating	Elastic Cloud agent policy  rev. 5	7.16.0		...
☐	6acd31ed7dc6	Updating	Elastic Cloud agent policy  rev. 5	7.16.0		...
☐	o11y-release-windows	Healthy	Test-Agent rev. 10	7.16.0	30 seconds ago	...
☐	o11y-release-linux	Healthy	Default policy rev. 8	7.16.0	10 seconds ago	...
☐	elastic-agent-helm-778f74b4d5-lq47r	Healthy	Default policy rev. 8	7.15.0	33 seconds ago	...
☐	elastic-agent-helm-778f74b4d5-lxhmr	Offline	Default policy rev. 8  Out-of-date	7.15.0	27 days ago	...
☐	o11y-release-windows	Offline	Test-Agent rev. 10  Out-of-date  Upgrade available	7.15.2	14 days ago	...



HORTEN
KOMMUNE

Regeltuning

- Trusseletteretning → manglede deteksjon → nye/tunede regler
- Falske positive
- Community
 - [\[Rule Tuning\] A scheduled task was updated #4541](#)
 - [\[Rule Tuning\] Potential Process Injection via PowerShell #4859](#)



SMB Data exfiltration

Filters

Custom query

Custom query language

Rule type

NOT Lokaltrafikk

data_stream.dataset: "fortinet_fortigate.log" and
fortinet.firewall.type: "traffic" and network.application : "SMB.v3"
or network.application : "SMB.v2" or network.application :
"SMB.v1"

KQL

Query

Rules

[+ Add Elastic rules](#) 22 [Manage value lists](#) [Import rules](#) [+ Create new rule](#)

[Installed Rules](#) 1562 [Rule Monitoring](#) 1562

SMB data		Tags 210	Last response 3	Elastic rules (1502) Custom rules (60)	Enabled rules Disabled rules
Showing 1-1 of 1 rule Selected 0 rules Select all 1 rule Bulk actions Refresh Clear filters					
☐ Rule		Risk s...	Severity	Last run	Last response
☐ SMB Data exfiltration		47	Medium	1 minute ago	Succeeded
					Last updated
					May 13, 2025 @ 10:05:19.964
					Notify
					Enabled

AD Enumeration - Computer Object Dump

Definition

Index patterns

apm-*-transaction*

auditbeat-*

endgame-*

filebeat-*

logs-*

packetbeat-*

traces-apm*

winlogbeat-*

-*elastic-cloud-logs-*

Custom query

event.code : 4662 and winlog.event_data.ObjectName :
██

Custom query language

KQL

Rule type

Query

Timeline template

None

Author

Colin Tortoise

Severity

● High

Risk score

73

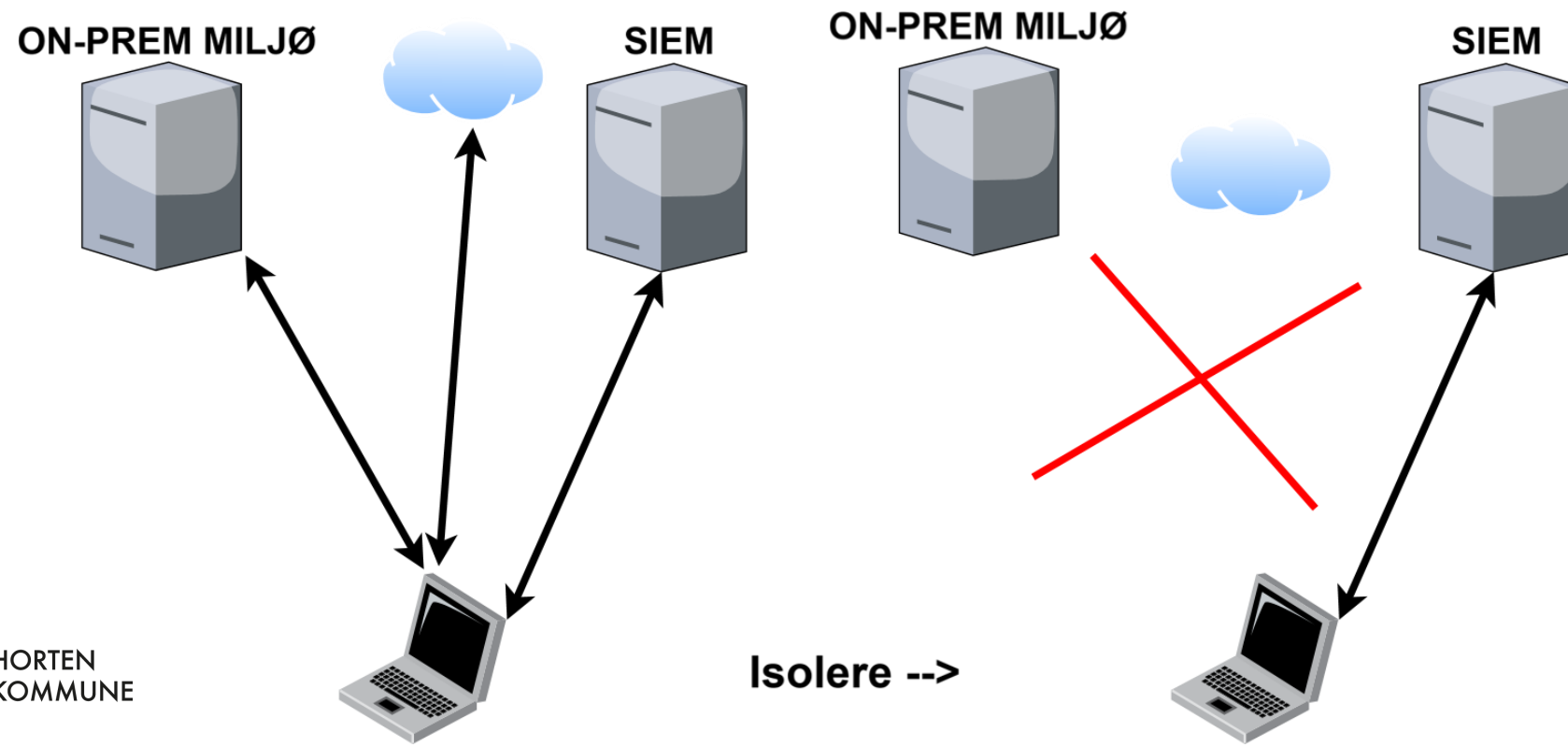
Max alerts per run

100



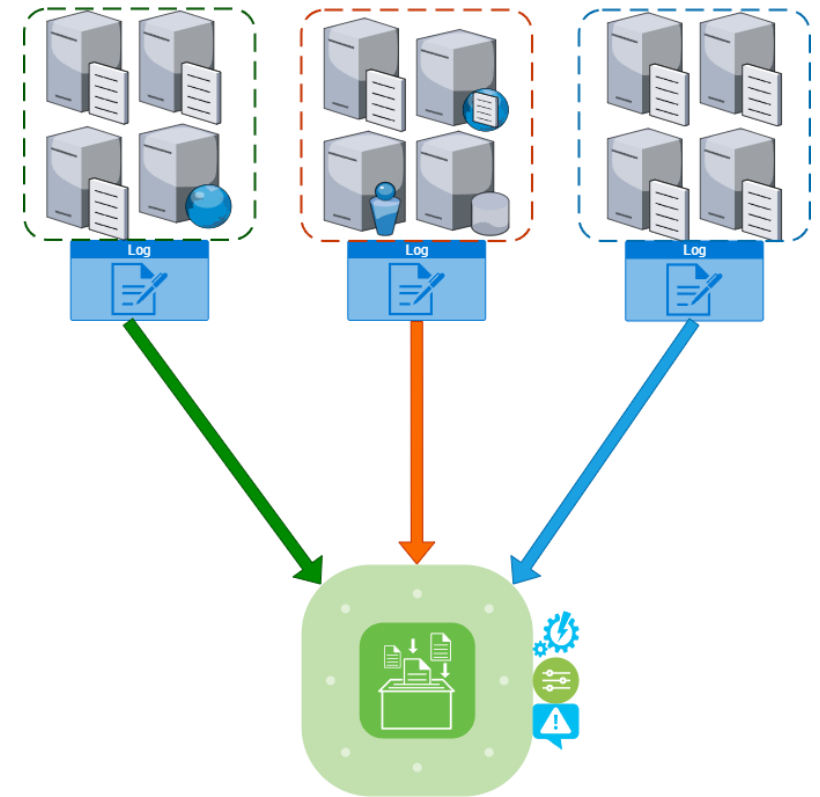
Respons

- Manuell (Responstid)
- Automatisert → Isolering/avisolering av klienter



Oppsummering/Anbefalinger

- Logging
- Test & produksjonscluster
- Gradvis utrulling (Prioriterte systemer først)
- SOC
- [Docker](#)
- Kostnadsfritt å komme i gang
- Observability for å erstatte SCOM





HORTEN KOMMUNE

Sindre Kristoffersen Olsen
IT Sikkerhetsrådgiver



Esben Jørgensen
IT-sikkerhetskonsulent



Spørsmål?