Hvordan bygge en fullverdig og kostnadseffektiv SIEM 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

HORTEN
KOMMUNE

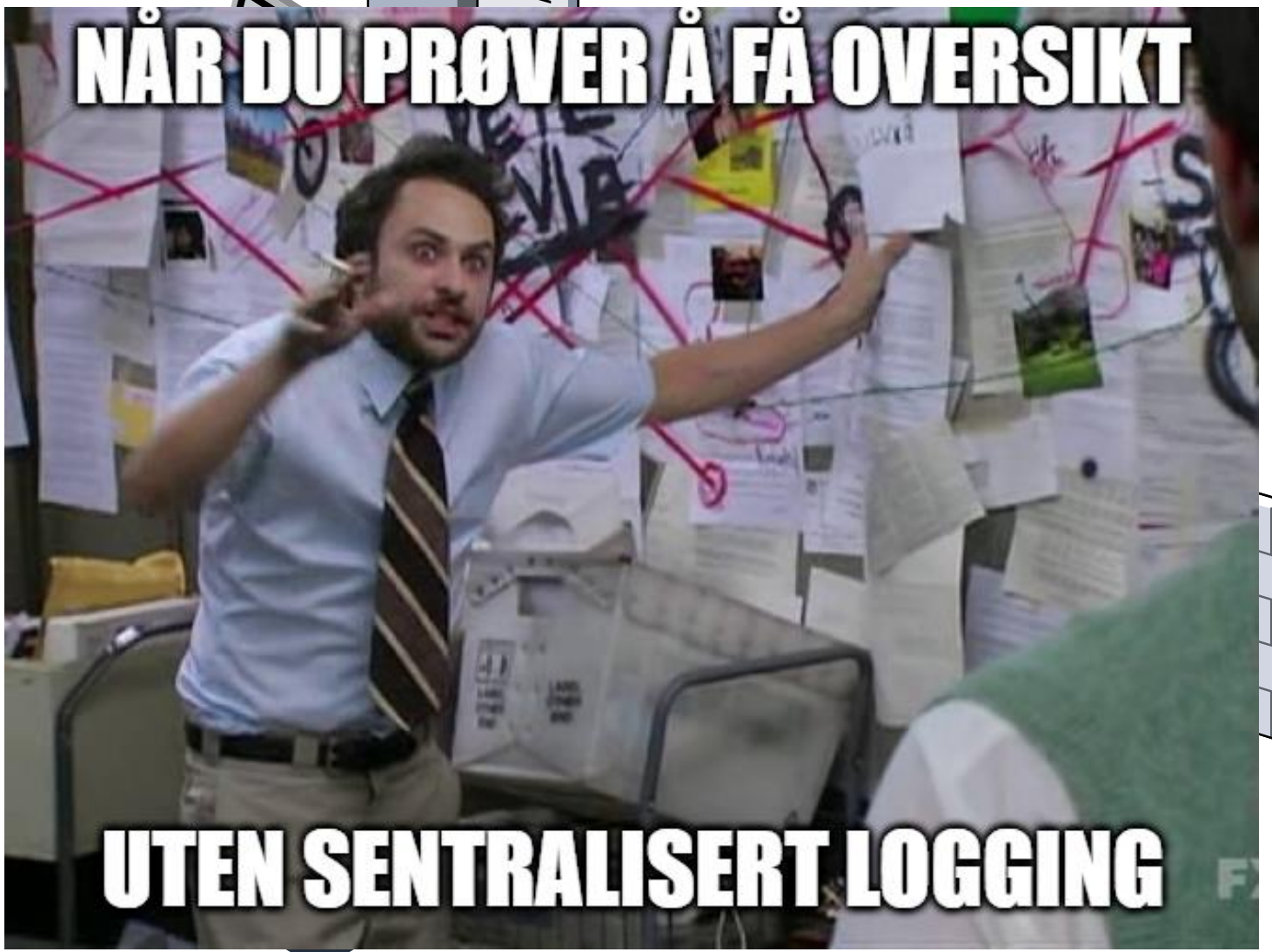
Agenda

- 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

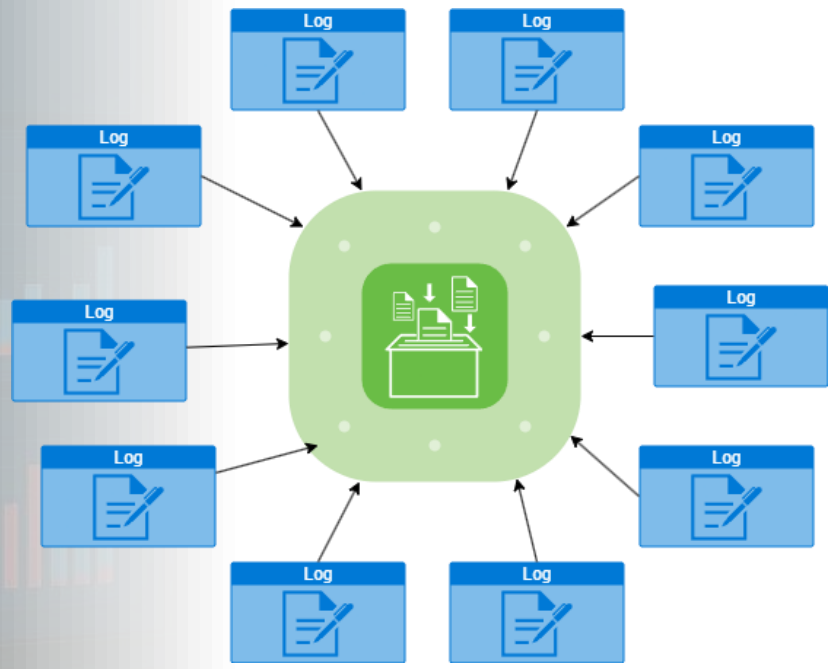
HORTEN
KOMMUNE



HORTEN
KOMMUNE

Sentralisert logging

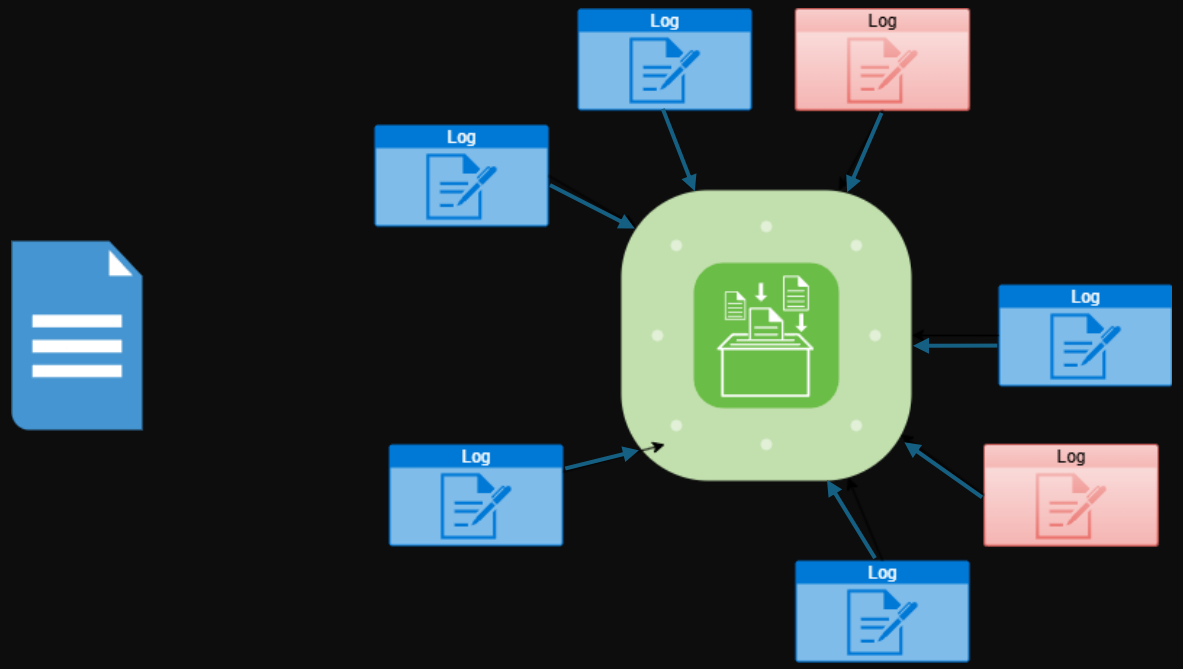
- Sender alle logger til ett sted

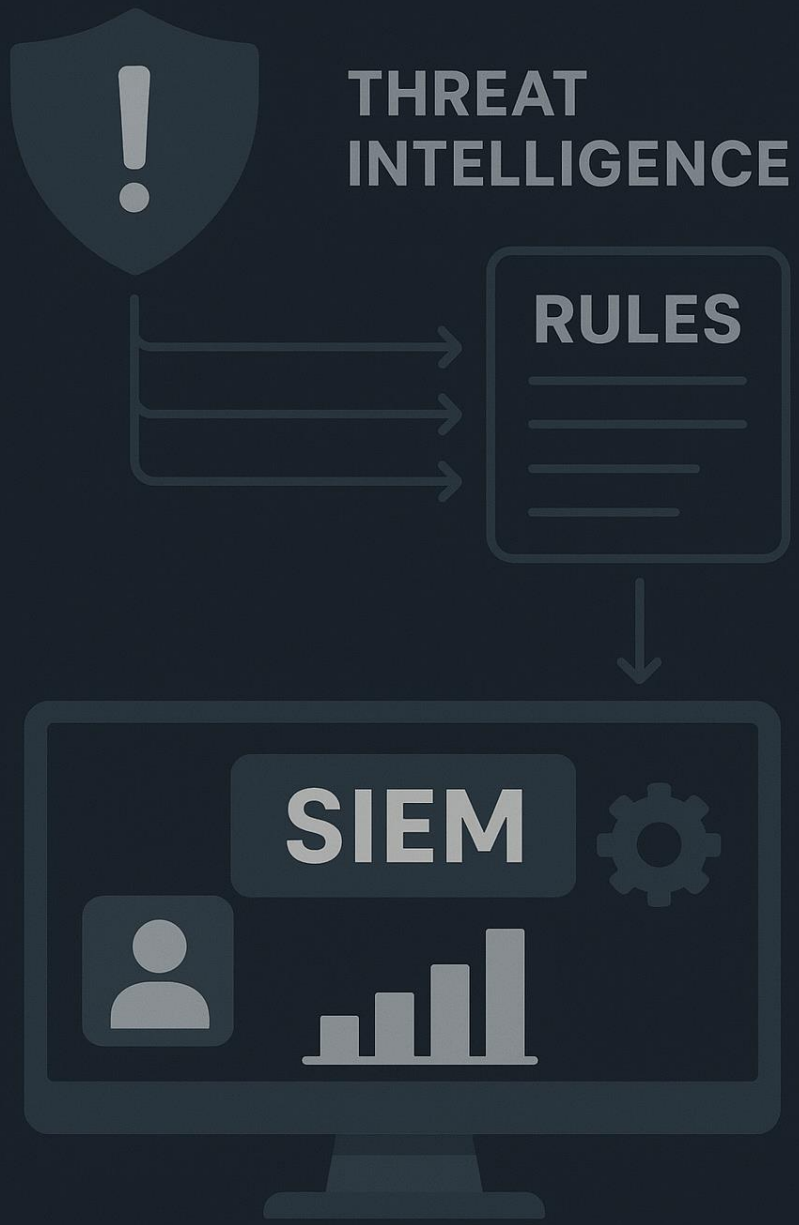


HORTEN
KOMMUNE

Sentralisert logging

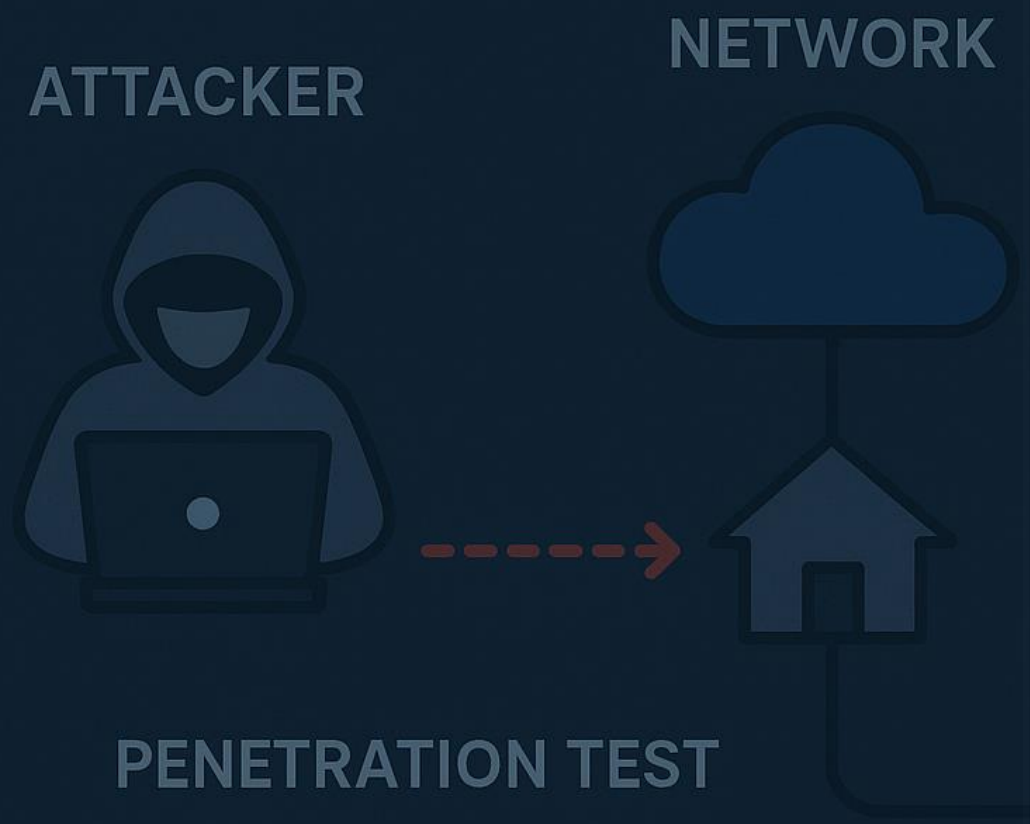
- Trussel → mangler logger → nye loggkilder





HORTEN
KOMMUNE

Sentralisert logging

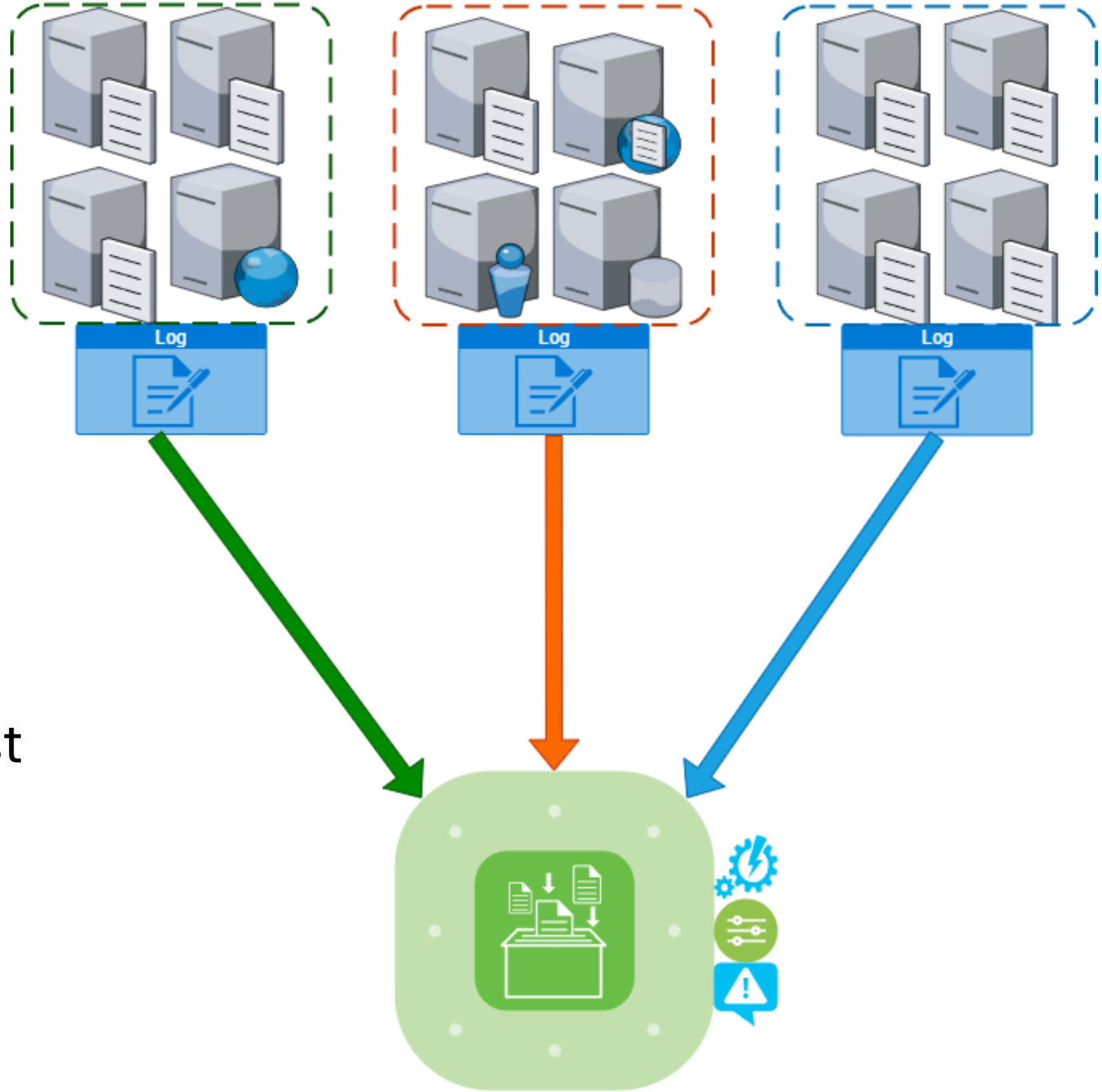


HORTEN
KOMMUNE

SIEM

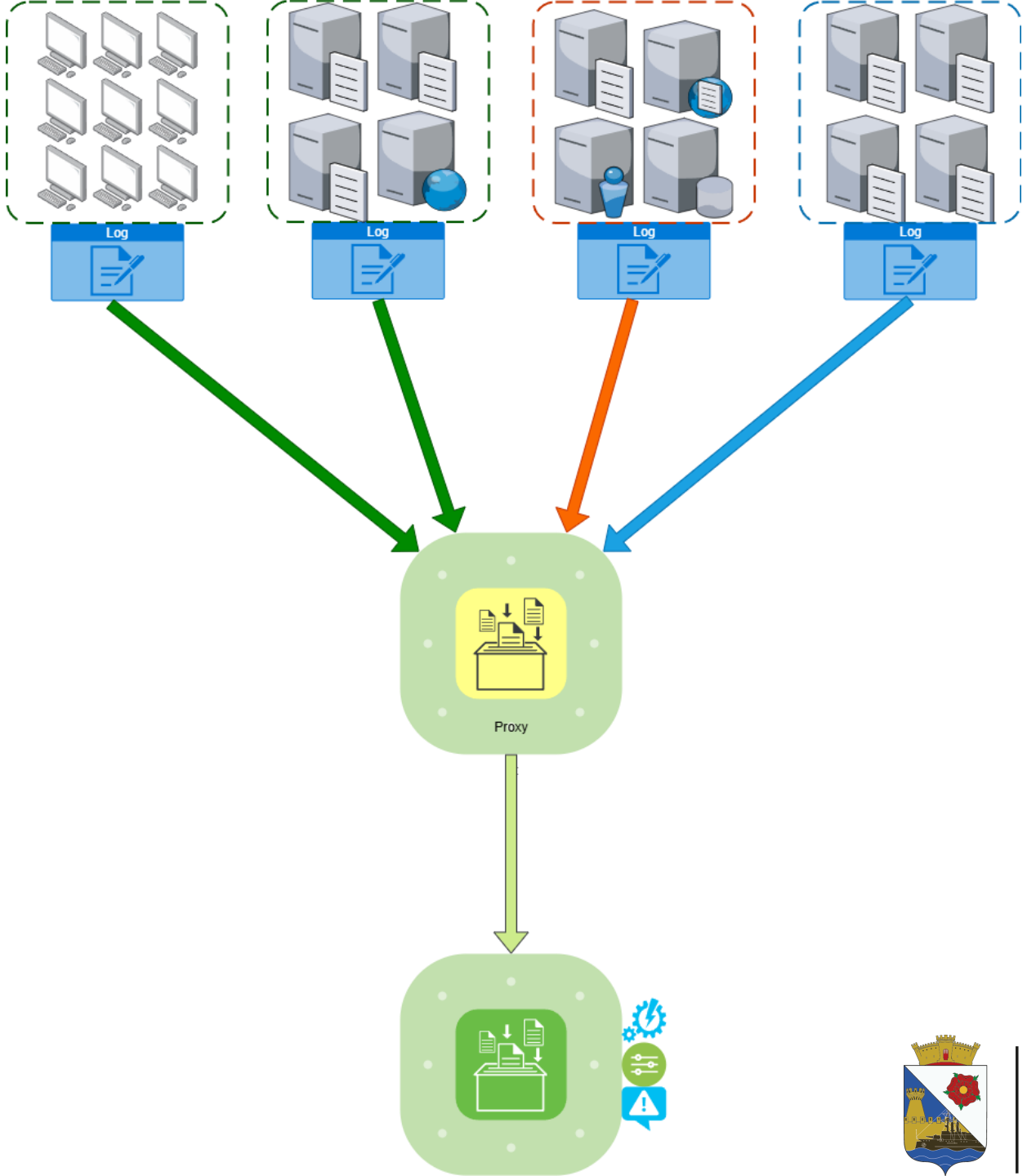
Security and Incident Event Management

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



SIEM

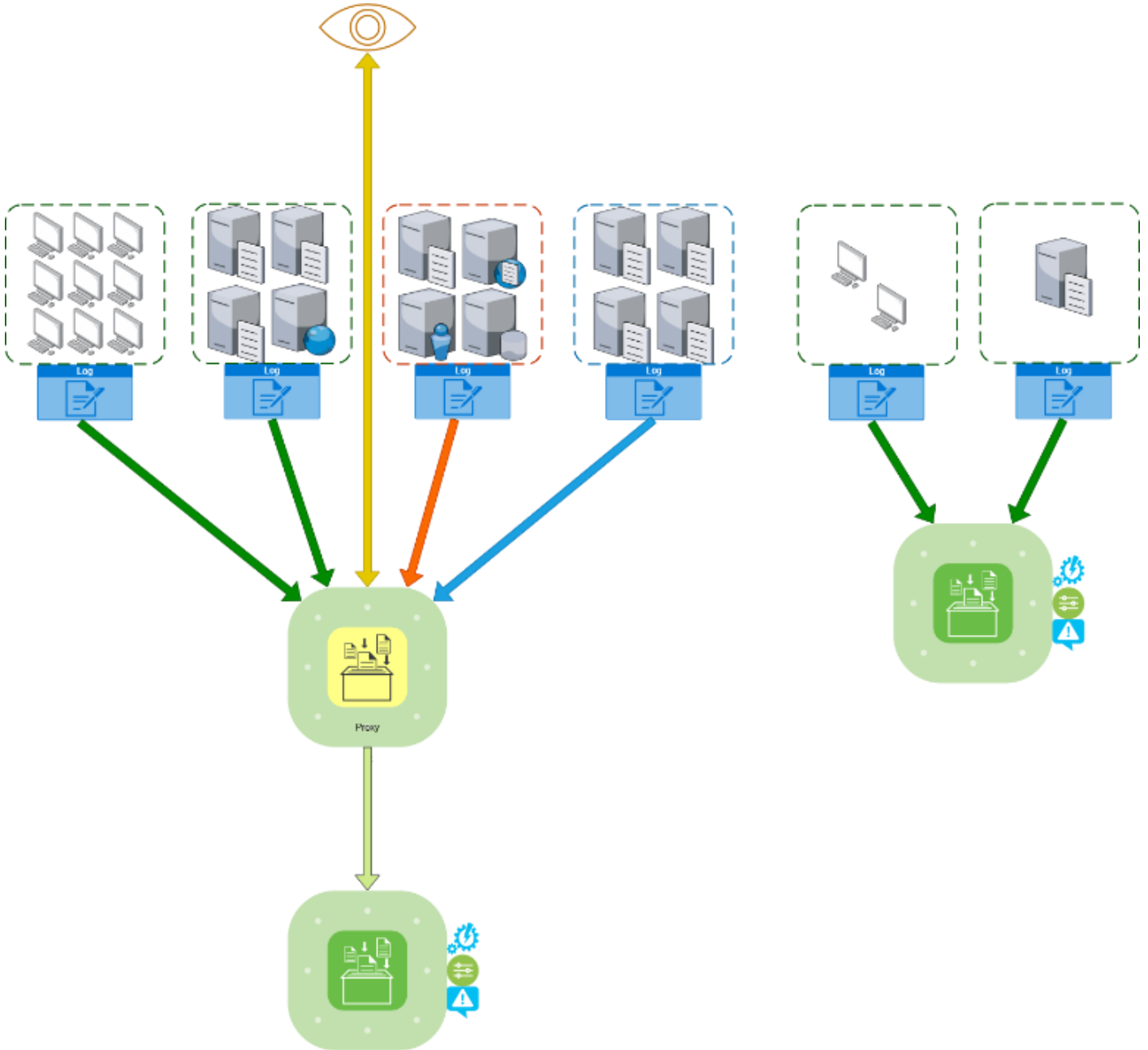
- Klienter
- Proxy



HORTEN
KOMMUNE

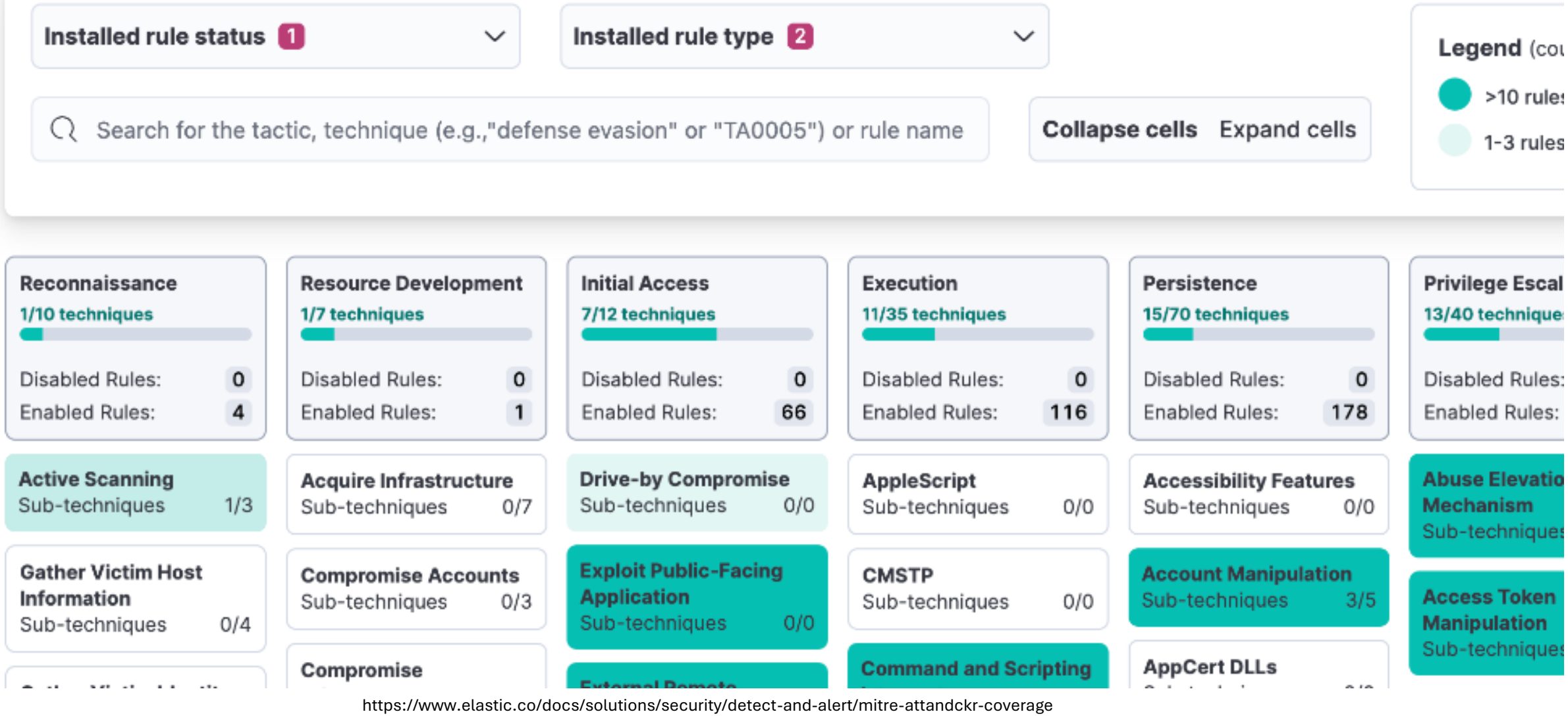
SIEM

- SOC
- Testmiljø
- Herding



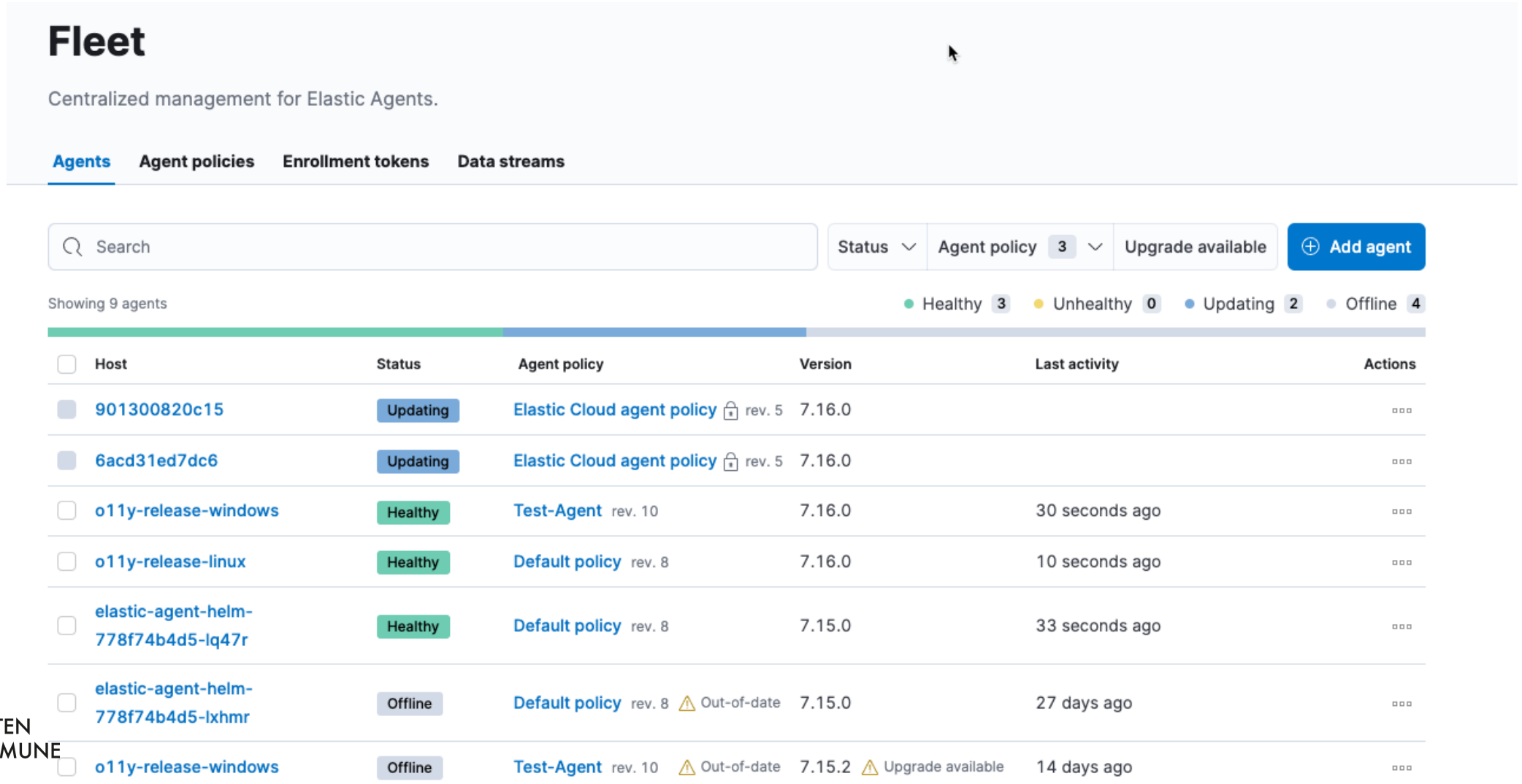
MITRE ATT&CK® coverage

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. Ru
framework to be displayed. Learn more.



https://www.elastic.co/docs/solutions/security/detect-and-alert/mitre-attandckr-coverage

Flåtestyring



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	NOT Lokaltrafikk
Custom query	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"
Custom query language	KQL
Rule type	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 | Updated 3 seconds ago | On

Rule	Risk s...	Severity	Last run	Last response	Last updated	Notify	Enabled
SMB Data exfiltration	47	Medium	1 minute ago	Succeeded	May 13, 2025 @ 10:05:19.964		

AD Enumeration - Computer Object Dump

Definition

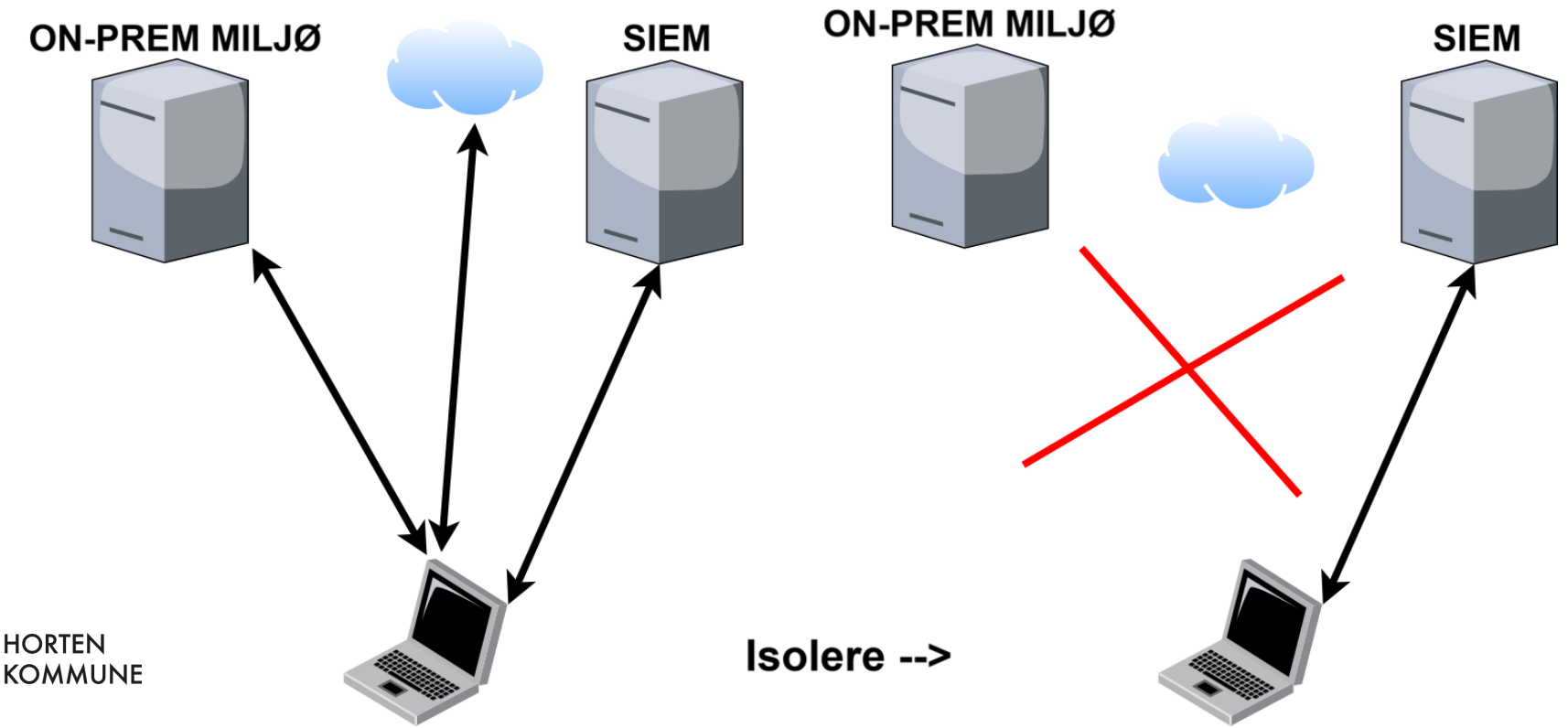
Index patterns	apm-*-transaction* auditbeat-* endgame-* filebeat-* logs-* packetbeat-* traces-apm* winlogbeat-* -*elastic-cloud-logs-*
Custom query	event.code : 4662 and winlog.event_data.ObjectName : [redacted]
Custom query language	KQL
Rule type	Query
Timeline template	None

Author	Colin Tortoise
Severity	High
Risk score	73
Max alerts per run	100

HORTEN
KOMMUNE

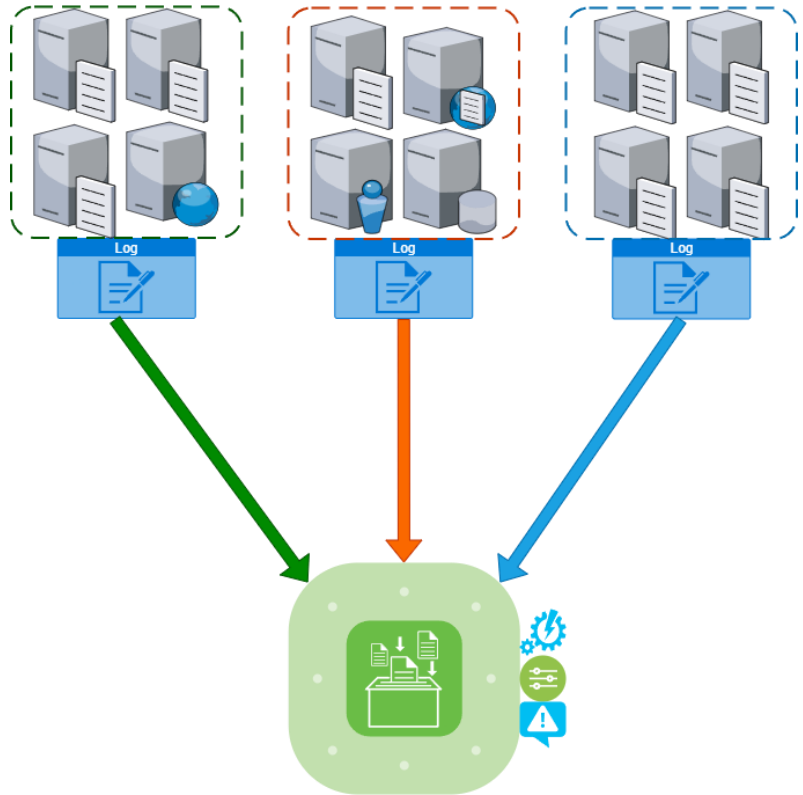
Respons

- 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

HORTEN
KOMMUNE

Sindre Kristoffersen Olsen
IT Sikkerhetsrådgiver

Esben Jørgensen
IT-sikkerhetskonsulent

Spørsmål?