

# Effektivisering av brannmurrevisjon gjennom logganalyse

	policy_id	policy_name	services	allow_all	unused_ranges
<input type="checkbox"/>	2	52516	SFTP Gateway - Inbound (Sit	PORT 135 TCP,TCP 4976	62553-63166, 144, 160, :
<input type="checkbox"/>	3	93484	HQ - App Proxy Inbound	Port 7077	443
<input type="checkbox"/>	4	13663	SCCM RemoteMgmt - Standa	ALL	8080, 8443
<input type="checkbox"/>	5	81252	Test - VPN Portal Admin	ALL	465, 587
<input type="checkbox"/>	6	47319	Discovery to Dormakaba - DF	MS-SQL UDP	None
<input type="checkbox"/>	7	7882	Elastic Monitoring - Standard	TELNET,RFC4890+ping6	30774-31037, 61575
<input type="checkbox"/>	8	44007	Reporting to SCCM - Edge (M	ALL_ICMP6,PORT 135 TC	24400, 64075
<input type="checkbox"/>	9	40599	HQ - Veeam Telemetry	Veeam_Backup_Window	46939
<input type="checkbox"/>	10	86967	Metasys Reporting - Tempora	CA-tjenester,NTP	17211-17490, 52717, 32
<input type="checkbox"/>	11	51602	Uniflow Monitoring - Standar	TCP 49152-65535,PING	53548
<input type="checkbox"/>	12	83850	LibreNMS Enrollment - Stand	Port 800 TCP,UDP,Port 16	20000, 10201

## Hensikt og mål

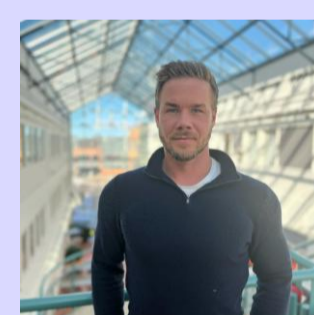
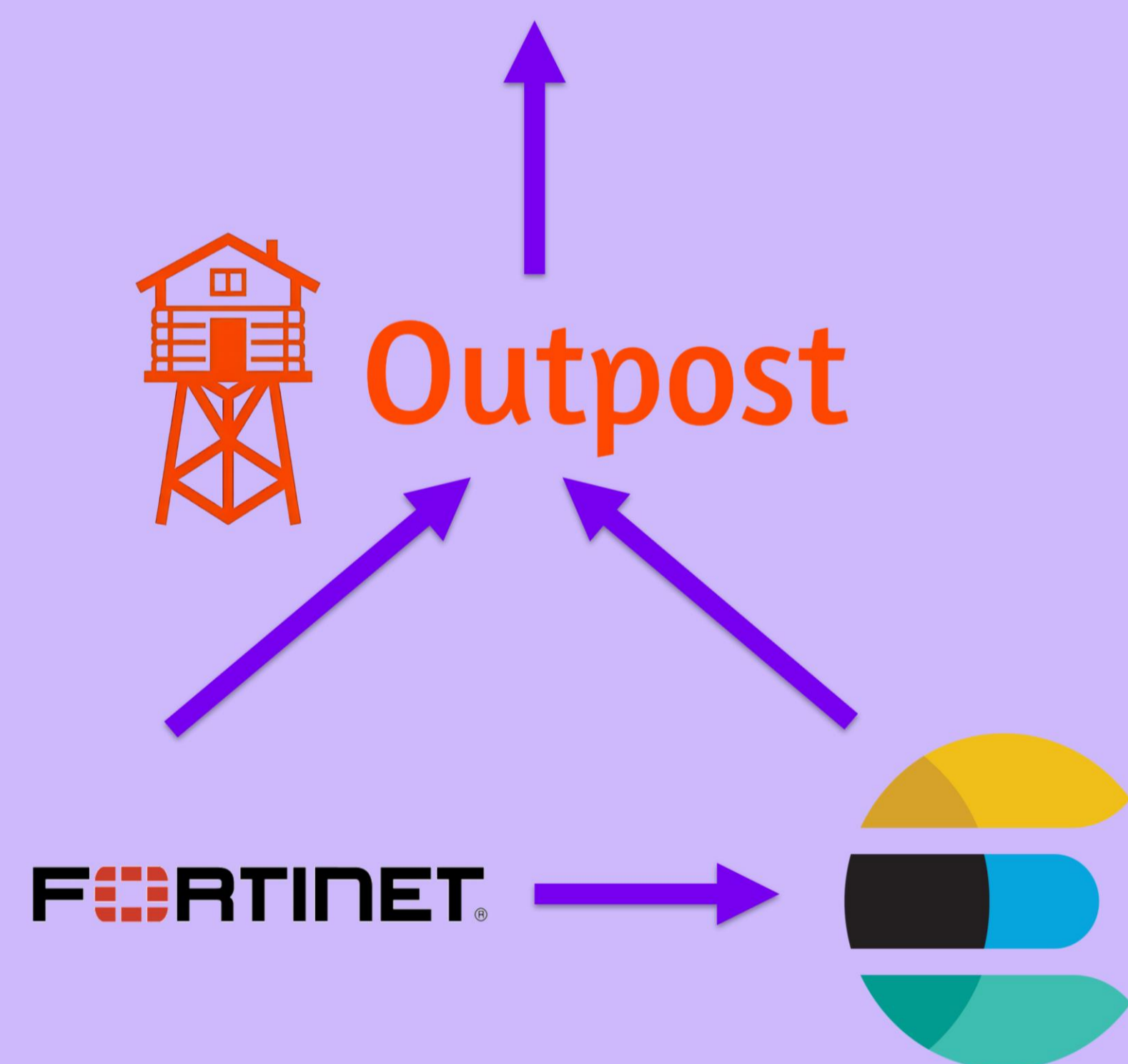
Hensikten med prosjektet går ut på å effektivisere og forenkle sikkerhetsarbeidet til Horten Kommune. Ved å utvikle et brannmurverktøy bidrar analyse av loggdata til en mer effektiv revisjon av kommunens brannmurregler.

## Resultater og sentrale funn

Vi har utviklet et brukervennlig verktøy som gjennom logganalyse gir innsikt over bruken av gjeldene regelsett. Verktøyet identifiserer bl.a.:

- Port- og DNS-aktivitet
- Overlappende og duplikate regler
- Avdekker hvilke brannmurregler som ikke treffes
- Anbefalinger basert på least privilege

Dette gir grunnlaget for et optimalisert sikkerhetsdrift.



Michael Jonassen  
109815@usn.no  
Dataingeniør,  
cybersikkerhet



Hans-Ole  
Rennekvammen  
261659@usn.no  
Dataingeniør,  
cybersikkerhet



William Tinnion-  
Varholm  
260559@usn.no  
Dataingeniør,  
cybersikkerhet



Marco André  
Berg  
258442@usn.no  
Dataingeniør,  
cybersikkerhet

Veileder:  
Raymond Berg Hansen  
raymond.b.hansen@usn.no

Samarbeidspartner:  
Horten Kommune, Sindre Kristoffersen Olsen  
sindre.olsen@horten.kommune.no

