Orange
Cyberdefense

Managed Threat Detection [log]

Logsanalyse er vejen til de mest værdifulde sikkerhedsdata, I overhovedet kan få. Men det kræver, at analysearbejdet udføres præcist og nøje tilpasset jeres behov.

Dyb indsigt og kort reaktionstid

Intet sikkerhedssystem er uden sårbarheder. Spørgsmålet er derfor ikke, om jeres netværk bliver angrebet, men hvornår det sker. Jo hurtigere det opdages, jo bedre mulighed for at begrænse skaderne.

I den sammenhæng er real time loganalyse et særdeles effektivt værktøj, men det kræver viden og teknologi, som de fleste virksomheder ikke selv råder over – derfor tilbyder vi tjenesten Managed Threat Detection [log].

Her sørger erfarne sikkerhedseksperter i vores 11 Cyber-SOCs for effektiv overvågning af jeres it-miljø gennem avanceret analyse af udvalgte logdata. Alle vores analytikere har gennemgået omfattende træning, så de kan realisere det fulde sikkerhedspotentiale i jeres loganalyse.

Hvorfor vælge Managed Threat Detection [log]?

- Markant forbedring af jeres mulighed for hurtigt at opdage trusler
- Det er dyrt og tidskrævende at bygge egne SOC- og CSIRT-teams
- Andre udbydere baserer udelukkende deres loganalyse på SIEM-teknologi. Vi kombinerer med konstant research, intelligence-baseret knowhow, velafprøvede analysemetoder og analytikere med et bredt sæt af sikkerhedskompetencer

Kend jeres behov

For at beslutte det næste skridt i jeres trusselsovervågning, er det vigtigt at vide, hvor I står i dag. Fx hvilken risikprofil i ønsker. Hver virksomhed har sine egne unikke sikkerhedsbehov, som bør afspejles i valg af sikkerhedslag, overvågning og beredskab. Det kan måske lyde komplekst – men det behøver det ikke at være.

Threat Detection Framework

Det er også vigtigt at opstille klare målsætninger for, hvad I vil opnå med jeres loganalyse, da det har stor betydning for, hvilke logdata vi skal analysere på. Her kan vores Threat Detection Framework give jer et stærkt beslutningsgrundlag.

Forretningsmæssige fordele

Managed Threat Detection [log] giver jer ikke alene avanceret overvågning. Tjenesten kan også hjælpe jer med at træffe forretningsmæssige beslutninger relateret til jeres sikkerhed.

Vi interfacer med MITRE ATT&CK framework, så I kan følge udvikling tæt.

Vores unikke asset database gør lettere at måle på risiko og angrebsmønstres over tid.

Overvågning kan efter behov udvides med flere data, så I sparer ressoucer i jeres eget sikkerhedsteam.

Se mere om hvordan I kan opdage angreb, før de forretter skade:
orangecyberdefense.com/global/mdr/

De største udfordringer?

- Management og løbende udvikling af jeres platform for overvågning og respons.Staffing a security platform management team with subject matter experts
- Bemanding af eget sikkerhedsteam med det rette mix af kompetencer
- Manglende ressourcer til at drive eget SOC 24/7
- Udvikling af metoder som giver det rette analysegrundlag uden at medføre mange falske positiver
- Trusselsbillede baseret på global intelligence

Hvornår er Managed Threat Detection [log] især relevant?

- Hvis I er underlagt compliance-krav om lagring af logs, og I ønsker dette udført som en service
- Hvis I har brug for hjælp til at udrulle og drive en outcome-based MDR-service baseret på SIEM
- Hvis I har investeret i Microsoft Sentinel, men ikke selv har ressourcerne til at drive løsningen
- Hvis I har brug for managed threat detection 24/7 eller 8/5
- Hvis I har brug for en leverandør med fokus på [the full "SOC triad" stack], og endpoint- / netværksbaseret overvågning understøttet med Cyber Threat Intelligence

Hvad gør vi?

- Vi implementerer vores proprietære Pattern-baserede overvågning på en Splunk-platform, som er en del af tjenesten – ELLER vi bygger samme løsning oven på jeres eksisterende Microsoft Azure Sentinel-platform
- Vi udfører løbende analyse og trusselsprioritering
- Vi overfører relevante data til vores unikke Threat Intelligence Datalake
- Løbende tilpasning af use cases og overvågning
- Performance, Device Health, OS, Log Source, Application and License Monitoring (kun på Splunk)

Hvad får i?

- Real time-analyse af sikkerhedshændelser
- Månedlig rapportering om analysearbejdet og jeres aktuelle trusselsniveau
- Cyber Threat Hunting

Tilvælg Managed Threat Response

Her bruger vi jeres eksisterende sikkerhedsværktøjer til at isolere endpoint involveret i kritiske sikkerhedshændelser.

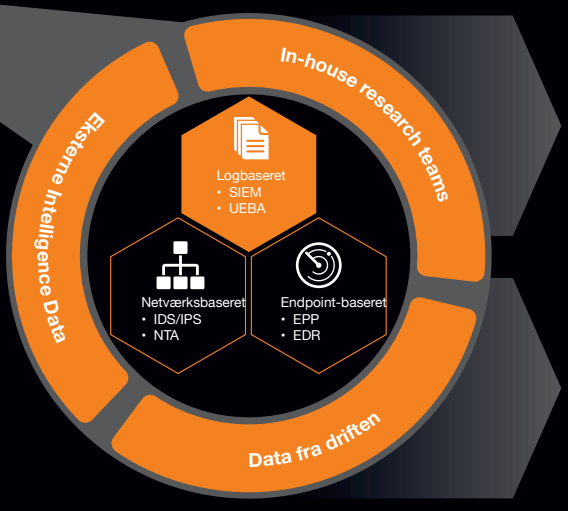
Intelligence-baseret loganalyse – oversigt over de vigtigste fordele

Orange Cyberdefense
Intelligence Backbone

- Intelligence fra MDR, CERT og CSIRT
- Ekstern intelligence
- Samarbejde med myndigheder
- In-house R&D

Internt

- Overvågning af mistænkelige aktiviteter
- Analyse og klassificering af hændelser
- Notifikation og rapportering



Forbedret logbaseret overvågning

- Dyb indsigt i IoC's
- Risikobaseret overvågning med fleksibel adfærdsanalyse
- Klassificering af trusler
- Forvarsling og tidlig identificering af store angreb
- Effektiv bortfiltrering af "støj" og falske positiver
- Mange muligheder for tilpasning
- 24/7 CyberSOC