CapMon SOC

Overblik

CapMons Security Operations Center (SOC) er en central enhed, som kan håndtere din virksomheds sikkeheds issues både på et organisatorisk og teknisk niveau.

Vi håndterer Incident management for din virksomhed.

Vi sikrer, at alle sikkerheds-angreb, malware, spyware og andrer hændelser for virksomheden bliver korrekt identificeret, analyseret, kommunikeret, elimineret, dokumenteret og rapporteret.

Fordele

Vi holder øje med dine kritiske aktiver og eliminerer eventuelle risici, før der opstår komplikationer, der kan skade din virksomhed.

Vi sørger for, at it-sikkerheden konstant er i fokus. Det giver dig mere tid til at koncentrere dig om din forretning.

Elastic SIEM

Forøg it-sikkerheden i din organisation

Det moderne samfund er stærkt afhængigt af informations- og kommunikations-teknologi. Et væsentligt mål indenfor informationssikkerhed som en disciplin og som profession er derfor også at beskytte værdifulde aktiver i virksomheden.

Hvad er Elastic SIEM

Vores SIEM er en enterprise løsning til log management af hele din infrastruktur, hvilket øger sikkerheden på tværs af organisationen.

Du får et realtidsbillede af hele it-infrastrukturen med registrering af eventuelle trusler. Du kan monitorere hele vejen ned til applikationslaget og derved være i stand til at identificere mulige cyber-angreb eller andre hændelser og få verificeret, om det er en reel, ondsindet trussel (hændelse), om det har konsekvenser for forretningen - og i givet fald hvilke.

Udvalgte data kan vises på dashbords. Det giver dig mulighed for at få et samlet overblik over dine vigtigste overvågningsdata.

Effektiv incident management

Løsningen er skalerbar, enkel og er et særdeles kraftfuldt værktøj, til korrelering og aggregering af logs. Der er ingen installation af ekstra agenter. Kun konfigurering af log sources er nødvendig for at opsamle loginformationer. Du får lynhurtig opsamling og visning af data på dit dashboard til brug for den efterfølgende analyse, dokumentation og rapportering. Du har mulighed for historisk lagring af data samt filtrering af dine logfiler for reducering af "False Positives" - alle funktionaliteter, som bidrager til hurtig, effektiv og korrekt incident management.

Elastic versus andre SIEM teknologier

- Du får et skalerbart værktøj, som er hurtigere end andre logningssystemer, hvilket er en væsentlig tidsbesparende faktor.
- Det er ikke nødvendigt at installere ekstra agenter i din it-infrastruktur. Det eneste du behøver er at konfigurere log sources for at opsamle loginformationerne.
- Understøtter alle logformater
- Logningen foregår centralt fra en enkelt lokation
- Fortager lynhurtig korrelering og lagring af store mængder data (Big data) på ganske få minutter
- Særdeles omkostningsbesparende sammenlignet med andre tilsvarende løsninger

SIEM log services

Log Analysis & log management

Realtidssøgning, opsamling, analysering og lagring af events fra relevante datakilder for detektering og digital analyse af sikkerhedsincidents.Opsamling af logs fra dine sikkerhedskontroller og netværksenheder

Fordele

Korrelering af alle logbeskeder i din it-infrastruktur. Let og hurtig identificering af potentiel skadelig aktivitet.
Realtidssøgning og historisk lagring af konsoliderede data.

Forensics analysis (critical assests)

Gennemgribende digital undersøgelse inkl. udførlig og dybdegående analyse af systemerne.

Fordele

Detektering af svindel, spild og misbrug. Finder årsager og foretager preventive tiltag, for derved at sikre fokus på kritiske aktiver og omkostninger for forretningen. Gearing af oplysninger i dataarkiver.

Fine tuning

Reducering og filtrering af "False Positive" alarmer, som ofte koster tid og manpower.

Fordele

Giver dine sikkerhedsmedarbejdere bedre tid til at beskæftige sig med de alvorlige trusler.

Reporting & documentation

Ugentlig rapportering og teknisk dokumentation. Der foretages incident management for hver hændelse.

Fordele

Du får dokumentation til brug for revision og compliance. Du får en vurdering af sikkerhedsniveauet og eskalering til "response teams" via et Ticket system.

Maintainance of log sources

Tilføjelser af nye/fjernelse af inaktive aktiver i SIEM miljøet.

Fordele

Reducerer netværkstrafikken og sikrer, at der udelukkende er fokus på aktive og kritiske aktiver.

Proactive monitoring

Find usædvanlige logaktiviteter i netværket. Identificér og ret små problemer tidligt, før de har en chance for at udvikle sig til større problemer. CapStash kan foretage central log monitorering

Fordele

Korrekt proaktiv vedligeholdelse af et netværk vil forbedre din produktivitet, øge pålideligheden af systemerne, og reducere dine it-supportomkostninger.

SIEM security services

Security Awareness

Etablering og implementering af security awareness program i virksomheden for at øge forståelsen for it-sikkerhed i organisationen.

Fordele

Reducerer forekomst af datalækager malware, spyware og virusangreb gennem forståelse hos medarbejderne for korrekt brug af it samt vigtigheden af at kunne detektere og rapportere sikkerhedsincidents.

Penetration testing & risk assessment

Ved hjælp af plugins, log analyser og sniffing værktøjer scannes, evalueres, og risikovurderes sikkerheden i din it-infrastruktur.
Du identificerer trusler og sårbarheder, og om de er kritiske/mindre kritiske eller blot er "false positives"

Fordele

Imødegår regulatoriske krav og undgå bøder. Letter arbejdet med eventuel efterfølgende etablering af en beredskabsplan, som giver mulighed for en mere effektiv tildeling af dine sikkerhedsressourcer.