CONSCIA CYBER DEFENSE

Logmanagement as a service

Kravet for dokumentation og compliance vokser

Mange virksomheders IT-revision har øget fokus på loghåndtering fx for at kunne dokumentere et hændelsesforløb men også for at sikre, at regler bliver overholdt, og om en eventuelt kompromittering af data har fundet sted.

Logning eller SIEM

Mange kan have tendens til at forveksle eller sammenligne logmanagement og SIEM-løsninger (Security Information and Event Management).

Kort fortalt er logmanagement en løsning, hvor man gemmer de data, som er relevante for virksomheden. Det kan enten være fordi lovgivningen stiller krav til det eller for at have data, som kan bruges i tilfælde af en sikkerhedshændelse.
I logmanagement-løsningen defineres også, hvor længe data skal være tilgængelig. Hvis data fx. ikke må gemmes mere end 180 dage, er det muligt at definere dette som et regelsæt og modsat, hvis fx. en firewall-log skal være tilgængelig i flere år.

Når data er tilgængelig i logmanagement-løsningen, og man ønsker at søge på tværs af data, eller få alarmer, når bestemte hændelser opstår, kombineres løsningen med et SIEM-system. Dette er også en mulighed med logmanagement-as-a-service fra Conscia.

Med SIEM-overbygningen er det muligt at blive alarmeret hvis der fx:

- Oprettes brugere med for mange rettigheder
- Hvis der er DNS-aktivitet mod servere, som ikke tidligere er set
- RDP- og SSH-sessioner mod internettet og meget mere.

Alarmer fra et SIEM system kan kun være så gode, som det data de baseres på, og derfor anbefaler Conscia at sikre en ordenligt logmanagement-platform.

Simpel og skalerbar logmanagement i skyen

Conscia simplificerer processen omkring logmanagement ved at give adgang til en cloudløsning, der både kan håndtere de logningskrav, som virksomhederne står overfor i dag, og kan skalere til virksomhedens kommende krav.

Logmanagement-løsningen er baseret på Elastic Cloud og håndteres og vedligeholdes af et sikkerhedsteam fra Conscia.

Med logmanagement-løsningen får I:

1. Cloudløsning med dataplacering i EU
2. Ressourcer baseret på jeres krav og mulighed for skalering
3. Normalisering af data fra 50+ leverandører bl.a. Cisco, Palo Alto Networks, Infoblox & Microsoft
4. Mulighed for alarmering på baggrund af events og hændelser
5. Fuld adgang til løsningen

Sundhedstjek

Conscia udører desuden et kontinuerligt sundhedstjek af løsningen, så den altid fungerer optimalt.

Med sundhedstjekket får I:

1. 8x5 overvågning
2. Overvågning af logmodtagelse
3. Database- og dataoptimering
4. Overvågning af at log-opbevaringstiden overholdes
5. Månedsrapportering

Prisen beregnes ud fra logmængden, samt den periode som loggen skal kunne tilgås.

Vil du høre mere om Conscia Cyber Defense?

Kontakt Nikolaj Andersen Wølck, Security Architect
Mail: naw@conscia.com
Mobil: +45 51 80 54 10

conscia