

KMD SIEM

Med det rigtige værktøj opnår du en intelligent styring og overvågning af din organisations systemer samt den nødvendige indsigt til at opdage uregelmæssigheder og reagere på disse. Med viden og indsigt fra logs fra hele din organisations systemer og applikationer sikres et analysegrundlag, der tillader, at du kan reagere smart, hurtigt og effektivt.

Du opnår en effektiv udnyttelse af IT-ressourcer samtidig med, at du øger IT-sikkerheden, forbedrer driften og overholder lovgivningskrav for logning og indsigt.



KMD SIEM

Med en stødt stigende trussel med flere cyberkriminelle og øget sårbarhed grundet kompleksiteten i netværket samt fortsat stigende afhængighed af IT er der en større risiko end nogensinde for at blive udsat for kriminelle handlinger. Ydermere indføres regulativer med krav til indsigt i håndteringen af data, eksempelvis EU persondataforordningen.

Få indsigt til at opdage indbrud og indblik i uregelmæssigheder

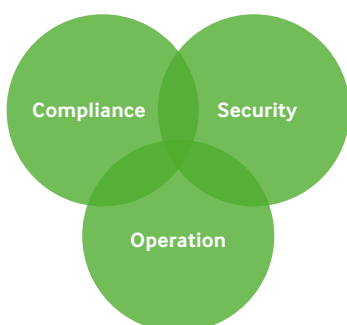
Med stigende risiko og lovmæssige krav til rapportering og håndtering af data øges presset på organisationer til at udnytte IT-ressourcer bedst muligt og forbedre netværksikkerheden og synligheden omkring applikationer.

SIEM giver dig mulighed for at overvåge og styre driften og IT-sikkerheden i din organisation med et højt niveau af overblik og indsigt i netværk, systemer og applikationer. Det giver din organisation de bedst mulige betingelser for at opdage uregelmæssigheder samt at reagere og rapportere på disse.

Konsolidering af hændelseslogs muliggør, at du kan håndtere krav og sårbarheder

IT-revisionen stiller krav, ligesom chefen og forretningen: Sikring af lovmæssig overholdelse af reglerne for håndtering af personfølsomme data, optimering og rapportering af drift samt IT-sikkerhedshændelser og beskyttelse af forretningens data. SIEM kan hjælpe dig med at:

- _ Opfylde en række compliancekrav fra EU data-forordningen, ISO 2700x, PCI DSS o.l.
- _ Øge IT-sikkerheden ved at detektere, analysere og reagere på sikkerhedsbrud.
- _ Reducere tiden, det tager at opdage og reagere på sikkerhedsbrud.
- _ Reducere nedetiden og sikre bedre performance af driften på din infrastruktur.
- _ Rapportere til eget brug eller til ledelsen, revisionen og forretningen.



Hvad kan produktet?

SIEM opfylder disse punkter med en platform, der er agil og brugervenlig, og som tilbyder en avanceret søgningsmotor, hvorfra der genereres dashboards, rapporter og regler til alarmer. Ydermere ligger et stort katalog af use-cases klar out-of-the-box til brugeren, så denne kommer sikkert og hurtigt i gang.

SIEM giver jer:

- _ Sikker, separat og konsolideret logopbevaring.
- _ Indsamling af logs fra systemer og applikationer til brug i rapportering, dashboards og/eller alarmering.
- _ Realtidssporing og alarmering af kompromitteringer af sårbarheder i netværket.
- _ Interface til analyse af hændelser for efterfølgende at kunne reagere på disse.
- _ Monitorering af it-services mhp. bedre performance, mindre nedetid og således mere stabil drift.
- _ Out-of-the-box dashboards, compliance-rapporter og regler til alarmering.

Hvorfor KMD?

Der er flere fordele ved at vælge KMD som sikkerhedspartner:

- _ KMD kan understøtte den måde, du ønsker at komme i gang på, hvad end det er
 - on-premise, hosted eller as-a-service løsning.
 - En løsning, hvor KMD overvåger din løsning evt. med integration til din incident-management proces.
- _ KMDs data er opbevaret i Danmark – håndteret og beskyttet af +100 danske sikkerhedsspecialister, som er klar til at bistå i forbedringen af din it-sikkerhed.
- _ KMD har mere end 200 private og offentlige sikkerhedskunder.
- _ Samler og analyserer dagligt 20 millioner logs.
- _ ISO 2700x certificeret.

Kontakt

Få en uforpligtende snak med en af vores sikkerhedsspecialister om, hvordan KMD kan hjælpe med at reducere dine risici. Skriv til os på: security-sales@kmd.dk