# Vi beskytter din infrastruktur
- døgnet rundt

# Er du en SMV virksomhed?

Beskyttelse af data bliver en mere og mere kompleks opgave, som er både omkostningstung, ressource- og tidskrævende. Vi har udviklet et servicekoncept, som hjælper din virksomhed med at øge sikkerheden i din infrastruktur.  Du får optimal beskyttelse mod sikkerhedsbrud uden brug af ekstra ressourcer.

## SentinelOne Endpoint protection

CapMons Managed Service koncept er designet til dig, der har brug for optimal beskyttelse og sikkerhedsovervågning  af din infrastrukkur  til en pris der ikke overstiger kr. 50.000 for helt op til 50 it-enheder (pc, server etc.).

I vores Managed Service koncept benytter vi teknologier fra SentinelOne, som er ny på danske marked, hvor vi er MSSP (Managed Security Service Provider) .

## Automatiserede processer

SentinelOne bygger på en teknologi, der hedder Active EDR (Endpoint Detection and Response). Der benyttes bl.a. signaturbaserede detekteringsteknikker i forbindelse med sikkerheds- overvågning af virksomhedens klienter. Teknikken benyttes til at identificere, om en given fil eller applikation er malicious (ondsindet) eller suspicious (mistænkelig).

Automatiserede processer  sørger for karantæne af infcerede filer, hurtig eskalering af hændelser til efterfølgende analysering og genskabelse af en inficeret pc.

## En Managed Service aftale giver jer:

- Awareness træning af jeres medarbejdere
- Undersøgelse af mistænkelige mails
- Dansk Support 08:30 - 16:00 med mulighed for tilkøb af 24/7 service og eskalering til 3rd level support.
- Overvågning med proaktiv assistance:
  - Identificere om signaturer er gode eller dårlige
  - Malicious detection
  - Suspicious detection
  - 3. parts forensics analyse
  - Analyse af karantæneramte filer i sandbox miljø
- Automatisk genskabelse af inficeret pc

CapMon A/S | Lyskær 9 | 2730 Herlev | Denmark | Tel.: +45 4485 5060 | www.capmon.dk | E-mail: salg@capmon.dk

| Managed services | Guld | Sølv<br>Mest solgte | Bronze |
|---|---|---|---|
| Awareness træning af medarbejdere - opstart på aftale | ★ | ★ | |
| Implementering og opsætning herunder black og white listning af diverse applikationer | ★ | ★ | ★ |
| Mail investigation | ★ | ★ | ★ |
| Dansk Support 08:30 til 16:00 på alle hverdage med eskalering til 3. level support | ★ | ★ | ★ |
| Overvågning med proaktiv assistance, herunder<br>- Identificere, om signaturer er gode eller dårlige<br>- Malicious detection<br>- Suspicious detection<br>- 3. parts Forensics Analyse på suspicious detection<br>- Analyse af karantæneramte filer i sandbox miljø<br>- Analyse af karantæneramte filer i sandbox miljø - on request<br>- Incident reporting | ★ | ★ | |
| Klient opgradering | ★ | ★ | |
| Managed Detection and Response | ★ | ★ | |
| Customer reporting 1 gang pr. måned | ★ | ★ | |
| 24/7 overvågning med proaktiv assistance og hurtige svar-tider, med eskalering til 3. level support.<br>- Identificere, om signaturer er gode eller dårlige<br>- Malicious detection<br>- Suspicious detection<br>- 3. parts Forensics Analyse på suspicious detection<br>- Analyse af karantæneramte filer i sandbox miljø<br>- Analyse af karantæneramte filer i sandbox miljø - on request<br>- Incident reporting | ★ | | |
| Cyber Security Advisor | ★ | | |

**Awareness træning af medarbejdere**
Træning af medarbejdere er altafgørende, da de i langt de fleste tilfælde er årsagen til et sikkerheds-brud. Som opstart har du mulighed for Awareness træning via et Cyber Security foredrag på ca. 1 time for jeres medarbejdere for at øge bevidstheden omkring Cyber Security.

**Implementering og opsætning**
**Bronze, Sølv, Guld**
CapMon hjælper dig med at installere SentinelOne. Dette kræver, at virksomhedens gamle antivirusklient bliver fjernet, før SentinelOne klienten bliver instal-leret - en ret nem hurtig operation.

Vi ser dog i nogle tilfælde, at der kan være udford-ringer med dvs. applikationer, som kræver, at man skal ind og enten tillade, at denne applikation er til stede, eller man skal ind i applikationen på klienten og acceptere, at SentinelOne nu er det antivirus program der bliver benyttet. Dette kaldes også, at man black- og whitelister applikationer på klienten.

**Mail investigation**
**Bronze, Sølv, Guld**
CapMon tilbyder, at du kan sende mistænkelige mails til vores specialister, som undersøger mailen og sender dig besked om, hvad du skal foretage dig.

**Dansk support**
**Bronze, Sølv, Guld**
CapMon har et dansk supportteam der sidder klar (hverdage i tidsrummet 08:30 til 16:30). Dette sker enten via mail, telefon eller en remote forbindelse.

**Overvågning med proaktiv assistance**
**Sølv: Hverdage 08:30 til 16:30 - Guld: 24/7**
CapMons support team har over 20 års erfaring. Teamet holder løbende øje med din virksomheds infrastruktur og tilstanden i denne.

Ved hjælp af SentinelOne identificeres, om en fil eller applikation er malicious (ondsindet) eller suspicious (mistænkelig).

Ved malicious detection vil en ondsindet handling blive stoppet med det samme. Filerne vil automatisk blive sat i karantæne, og vores specialister vil undersøge den/de karantæneramte filer.
Ved suspicious detection vil den mistænkelige hæn-delse ikke automatisk blive stoppet, men der vil komme en alarm til vores support team, som vil undersøge, hvorvidt den pågældende hændelse er ondsindet eller ej.

I første omgang ser vi på, om denne type hændelse allerede er kendt eller er set hos nogle af vores andre kunder.  Hvis det viser sig, at den mistænkelige hændelse rent faktisk er en malicious hændelse, vil vi hos alle vores kunder bringe denne viden ind i deres løsning. Denne Forensics Analyse varetages af vores erfarne sikkerhedskonsulenter og udviklere. Vi be-nytter forskellige testmiljøer, og vi tester altid samme hændelse i mindst 3 forskellige testmiljøer for at se, om reaktionen er den samme.

Har du filer der er karantæneramt og som du gerne vil benytte, kan du anmode os om at undersøge den pågældende fil og komme med en risikovurdering,

Så snart der er opstået en malicious hændelse vil der altid blive sendt information til dig om den pågæld-ende hændelse.

**Klient opgradering (hverdage 08:30 til 16:30**
**Sølv & Guld**
CapMons support team vil tilsikre, at alle klienter er blevet opdateret senest 24 timer efter, at en ny SentinelOne release er blevet frigivet. Er der stadig klienter i kundens infrastruktur der ikke er opgra-deret vil kunden blive notificeret om dette.

**Managed Detection and Response**
SentinelOne, som er "second to none" på dette område, er i stand til at detektere en malicious hændelse.  Der kan være flere filer, som er blevet berørt. SentinelOne vil automatisk kunne restore en klient og de tilhørende filer, som klienten har været i berøring med.

**Incident Reporting (Sølv og Guld)**
1 gang pr. måned vil du få en kort rapport over de hændelser der har været den foregående måned, med anbefalinger til mulige forbedringer af virksom-hedens sikkerhed.

**Cyber Security Advisor (Guld)**
CapMon har i de sidste 20 år arbejdet med it-sikker-hed. Vi stiller vores rådgivere til rådighed inden for 3 områder:

*Crisis Management Team* - bør man have - en mindre virksomhed dog med et begrænset antal deltagere. Dette team skal som minimum have en forankring i topledelsen og helst også i bestyrelsen. (Ydelsen afregnes på medgået tid)

*Årlig awareness træning* - udover den awareness træning som foregår i opstarten, tilbydes denne træning som en årlig service

*Ekstern hjælp:* Skulle virksomheden blive udsat for en ransomware-krise, er der ofte behov for ekstern hjælp, Virksomheden har brug for 24/7/365 adgang til en Cyber Security Advisor, der er i stand til at hjælpe dig med at fastholde, genoprette og efterforske angrebet. (Ydelsen afregnes på medgået tid).