We protect your infrastructure - 24/7

Managed cyber protection for SMB's

Protection of data is a complex task, which is both costly, resource- and time-consuming. In order to help your company uptimize IT-security, CapMon has developed a Managed Services concept that provides maximum protection against security breaches without any use of extra resources.

SentinelOne Endpoint protection

CapMons Managed Service concept is designed for companies with a need for uptimal protection and monitoring of the IT-security, at a price, not exceeding DKK 50.000 for up to 50 units (pc, server etc.).

In our Managed Service concept, we use technologies from SentinelOne, which is new on the Danish market, and represented by CapMon as MSSP (Managed Security Service Provider).

Automated processes

SentinelOne is builded on a technology called Active EDR (Endpoint Detection and Response). Signature-based detection techniques are used in connection with security monitoring of the company's clients.The technique is used to identify if a specific file or application is malicious or suspicious.

Automated processes ensure quarantine of infected files, fast escalation of incidents for subsequent analysis, and recovery of infected PCs.

Our Managed Service agreement provides:

- Awareness training of your staff
- Investigation of suspicious mails
- Danish support 08:30 – 16:00 with the possibility of 24/7 service and escalation to 3rd level support
- Monitoring incl. proactive assistance:
  - Identify whether signatures are valid or not
  - Malicious detection
  - Suspicious detection
  - 3rd party forensics analysis
  - Analysis af quarantined files in a sandbox environment
- Automatic recovery of infected pc

=> 2

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

Managed services	Gold	Silver Preferred choice	Bronze
Awareness training of staff - by start-up of agreement	★	★	
Implementation and set-up, incl. black/white listing of various applications	★	★	★
Mail investigation	★	★	★
Danish Support 08:30 - 16:00 on workdays - incl. escalation to 3rd level support	★	★	★
Proactive monitoring and service, incl. - Identify whether signatures are valid or not - Malicious detection - Suspicious detection - 3rd party Forensics Analysis on Suspicious Detection Incidents - Analysis of quarantined files in sandbox environment - Analysis of quarantined files in sandbox environment - on request	★	★	
Client upgrade	★	★	
Managed Detection and Response	★	★	
Customer reporting - monthly basis	★	★	
24/7 monitoring with proactive assistance, fast response times, and escalation to 3rd level support. - Identify whether signatures are valid or not - Malicious detection - Suspicious detection - 3rd party Forensics Analysis on Suspicious Detection Incidents - Analysis of quarantined files in sandbox environment - Analysis of quarantined files in sandbox environment - on request - Incident reporting	★		
Cyber Security Advisor	★		