Beleid
Techniek
Mens

Datasheet

Pinewood Security Operations Center (SOC)

Door hoge mate van digitalisering worden organisaties steeds meer afhankelijk van de IT-omgeving voor het uitvoeren van de dagelijkse operatie. Het lekken van gevoelige data door verschillende cyberdreigingen is een dagelijks risico. Door de nieuwe wet- en regelgeving wordt meer inzicht in het niveau van de IT security vereist.

Het verkrijgen van voldoende inzicht binnen de complexer wordende infrastructuur is voor veel organisaties een te grote dagtaak geworden. Hierdoor is men kwetsbaarder voor cyberaanvallen op de bedrijfskritische informatie en systemen met alle risico's van dien. Bijvoorbeeld het stilvallen van de operationele processen of het lekken van data wat mogelijk leidt tot financiële schade, boetes en imagoschade

Wat is een SOC?

Het Nationaal Cyber Security Centrum (NCSC) omschrijft een Security Operations Center (SOC) als een middel om zicht en grip op de informatiebeveiliging van een organisatie te krijgen. Inzicht krijgen is hierbij een sleutelwoord. "Meten is weten" wordt steeds belangrijker om keuzes op het gebied van informatiebeveiliging te maken.
Informatiebeveiliging is het geheel van maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie binnen een organisatie garanderen.
Dit betekent dat een SOC moet zorgen voor inzicht in en grip op de beschikbaarheid, integriteit en vertrouwelijkheid van data.

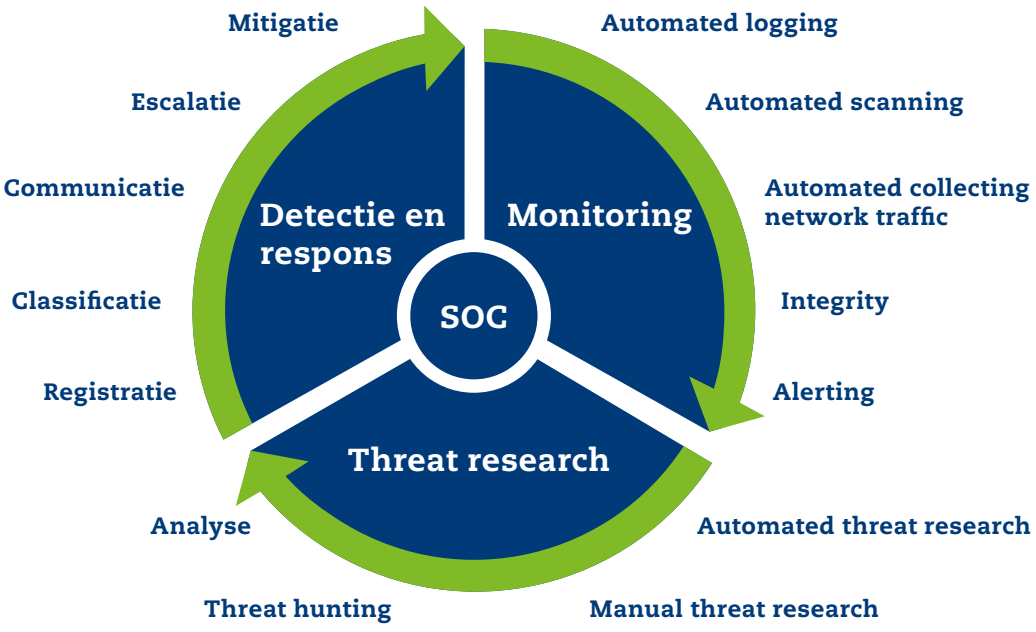
- **Beschikbaarheid:** "Is de informatie continu toegankelijk?"
- **Integriteit:** "Is de informatie correct en onveranderd door onbevoegden?"
- **Vertrouwelijkheid:** "Hebben de juiste personen toegang tot de gewenste informatie?"

De Pinewood SOC dienst heeft informatiebeveiliging als uitgangspunt en beschikt over unieke sensoren waarmee deze doelen bereikt worden.

Hoe werkt het Security Operations Center?

Een team van hoog opgeleide securityanalisten (hbo/wo) houdt uw systemen en netwerk 24x7x365 in de gaten. Op basis van de informatie verzameld door sensoren vindt in het SOC een analyse plaats van alle aan security gerelateerde gebeurtenissen in uw netwerk. Dit komt op de volgende drie niveaus tot uiting:

- **Compliancy en wet & regelgeving**
  Vanuit gepersonaliseerde- live dashboards en rapportages (aangepast op de normen die voor uw sector van toepassing zijn, bijvoorbeeld ISO27001 of NEN7510) heeft u direct inzicht in het huidige beveiligingsniveau van uw infrastructuur. In samenwerking met een security officer en analist wordt op basis van geïdentificeerde security incidenten gezocht naar maatregelen om het beveiligingsniveau van uw organisatie doorlopend te verhogen, zowel technisch als beleidsmatig. In periodiek terugkerende overleggen worden de opgeleverde rapportages met u besproken en eventueel bijgestuurd naar uw doelstellingen.
- **Toenemende IT dreigingen**
  De security specialisten van Pinewood hebben de expertise in huis om naast de automatische analyses ook actief op zoek te gaan naar cyberdreigingen, zoals infecties of geavanceerde hackpogingen door middel van “Threat Hunting”.
- **Veranderende en complexer wordende IT omgeving**
  Flexibiliteit en maatwerk is het uitgangspunt van het Pinewood SOC. Samen met u richt Pinewood “uw SOC” in naar uw wensen en behoefte, zodat de dienstverlening past binnen uw (organisatie) doelstellingen. Op basis van de praktijkervaringen passen we de inrichting in overleg aan.



Pinewood maakt hierbij gebruik van de volgende sensoren:

- **Beschikbaarheid** - monitort systemen en applicaties op beschikbaarheid.
- **Integriteit** - monitort bestanden, database tabellen en andere gegevens op geautoriseerde wijzigingen.
- **Vertrouwelijkheid** - monitort logfiles van applicaties, OS en hardware.
- **Kwetsbaarheden** - brengt mogelijke kwetsbaarheden in kaart.
- **Netwerkverkeer** - monitort netwerkverkeersstromen.
- **SCADA** - monitort aansturing van procesautomatiseringssystemen.

Wat levert het Pinewood SOC u op?:

- 24x7x365 detectie van security incidenten in log- en event informatie;
- 24x7x365 incident respons en mitigatieadvies van kritieke incidenten;
- 24x7 toegang tot security dashboard voor inzage in dreigingsniveau en detailinformatie;
- Maandelijkse en kwartaal maatwerkrapportages op technisch en beleidsmatig niveau;
- Security Bulletins met informatie en advies over actuele dreigingen;
- Indien gewenst on-site consultant met informatie en advies over actuele dreigingen;
- Regelmatig overleg op operationeel, tactisch en strategisch niveau;
- Concrete maatregelen zowel technisch als beleidsmatig.

Waarom Pinewood

- Pinewood is een 100% Nederlands bedrijf met datacenter in Nederland en voldoet aan de Nederlandse en Europese wet- en regelgeving. Pinewood kijkt naar informatiebeveiliging in zijn totaliteit en gebruikt verschillende sensoren om de beschikbaarheid, integriteit en vertrouwelijkheid van uw informatie, in welke vorm dan ook, te garanderen.
- De SOC diensten van Pinewood worden per organisatie op maat ingericht, om een zo goed mogelijke aansluiting bij de business verantwoordelijken en de verantwoordelijken voor de informatiebeveiliging tot stand te brengen.
- In het Pinewood SOC werken security analisten, threat hunters en ethical hackers. Zij concentreren zich 24 uur per dag op de monitoring, onderzoek en detectie.
- Bovendien werken de threat hunters met een combinatie van automatisering, artificial intelligence tools aangevuld met onmisbare menselijke analyse en interpretatie.
- Naast de verschillende tools die Pinewood inzet, werkt Pinewood met verschillende threat intelligence feeds uit publieke en commerciële bronnen. Hierdoor krijgt u direct inzicht in de mate waarin u wel/niet beschermd bent tegen nieuwe threat intelligence informatie.

Meer informatie

Bent u geïnteresseerd of wilt u meer informatie, neem dan contact op met ons via info@pinewood.nl of op telefoonnummer 015 251 36 36.

ISO 27001

PINEWOOD
Specialist in informatiebeveiliging

Pinewood bv
Delftechpark 57
2628 XJ Delft
T (015) 251 36 36
info@pinewood.nl
www.pinewood.nl

Beleid
Techniek
Mens