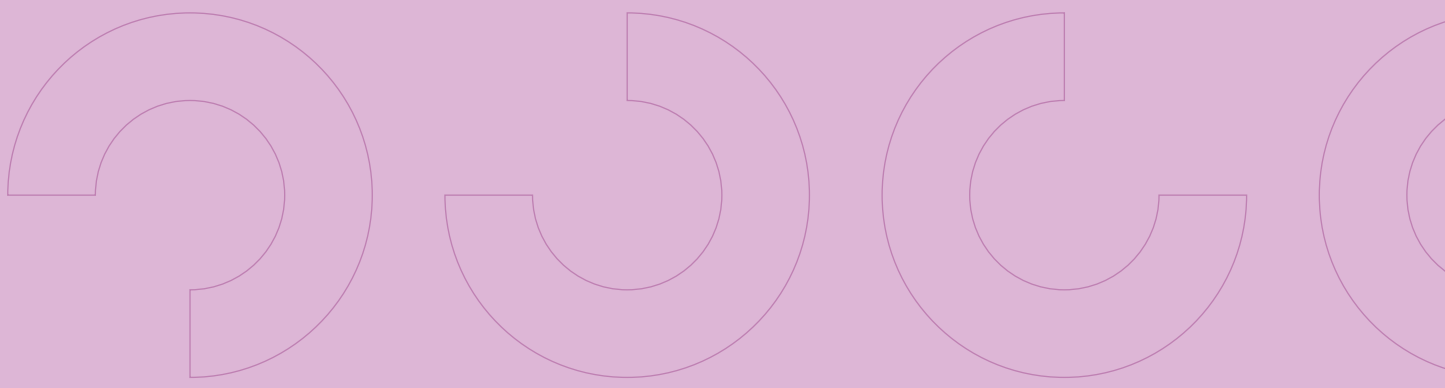
Whitepaper

De 3 fasen van een SOC-implementatie

We see risks
before they hurt

Digitale transformatie voltrekt zich in iedere sector en organisatie. Steeds meer processen worden geautomatiseerd en op een netwerk aangesloten, met als gevolg dat ineens heel nieuwe veiligheidsrisico's ontstaan. Denk aan het stilvallen van de operationele processen of het lekken van data. Daarnaast vereist nieuwe wet- en regelgeving meer inzicht in het niveau van de IT-security.
Het inrichten van een Security Operations Center (SOC) is een goede manier om zicht te krijgen op de risico's en de effectiviteit van de maatregelen. Het helpt u ook om snel te handelen als er een incident plaatsvindt. Bovendien geeft een SOC inzicht in het actuele beveiligingsniveau van uw IT-omgeving. Tevens voldoet het aan belangrijke normen als de ISO 27001 of NEN 7510. Maar hoe zet u een goed SOC op? In deze whitepaper tonen we de belangrijkste stappen.



Uitdagingen en pijnpunten

Hoewel cybersecurity steeds hoger op de agenda staat bij een groeiend aantal organisaties, zijn er nog steeds uitdagingen en pijnpunten op het gebied van monitoring die vaak terugkomen. Een kort overzicht:

- Organisaties hebben moeite om vast te stellen op welke risico's ze precies gaan monitoren. Geen onderscheid maken tussen ernstige en minder prominente dreigingen kan leiden tot een stortvloed aan false positives en 'alert fatigue', waardoor de kans groeit dat u op termijn iets belangrijks mist.
- De logging is niet goed beschikbaar of fout ingesteld.
- Er is geen duidelijke controle over de locaties waar belangrijke data staan. Het overzicht over welke apparaten en gebruikers toegang hebben tot bepaalde data en netwerkonderdelen ontbreekt.
- Cloudoplossingen als Teams worden te snel en zonder goed beleid uitgerold. De coronapandemie heeft dit probleem vergroot.
- Security is vaak het vijfde wiel aan de wagen bij het inrichten van de IT-infrastructuur. Security by design zou namelijk de norm moeten zijn.

Strategische en operationele taken van een SOC

Met een SOC lost u de bovengenoemde problemen op en tilt u uw security naar een hoger niveau. Maar wat is en doet een SOC precies? Een SOC is de combinatie van een toegewijd team van security-experts en securitytools die u helpt om cyberrisico's sneller en beter te ondervangen. Het kan een afdeling binnen uw bedrijf zijn, maar ook een externe dienstverlener (SOC-as-a-service).

Het securitybeleid is altijd een afgeleide van het organisatiebeleid. Het management van een organisatie moet bepalen wat het ambitieniveau voor security is en welke risico's prioriteit krijgen. Ook de externe omgeving speelt een rol: welke bedreigingen doen zich in onze sector veel voor? En waar zitten specifieke risico's? Al deze factoren samen bepalen de invulling van het securitybeleid.

Daarnaast vervult het SOC een operationele functie: het detecteren van risico's en hier snel op inspelen. Hierin spelen techniek en mens een even belangrijke rol. Uiteraard is technologie nodig om de ICT-omgeving voortdurend te monitoren en dreigingen vroegtijdig te detecteren. Maar het zijn vervolgens wel de mensen die tot actie moeten overgaan. Waar een traditioneel SOC reactief te werk gaat, is een modern SOC proactief en wendbaar. Het SOC moet bovendien voortdurend aansluiting

Implementatie SOC: 3 fasen

De technische implementatie van een SOC bestaat in de kern uit het plaatsen van logsensoren en netwerksensoren op alle relevante componenten van de infrastructuur. De logsensoren verzamelen gegevens over events, bijvoorbeeld de events die security-oplossingen detecteren. En de netwerksensor detecteert dreigingen in het netwerkverkeer. Maar implementeren is meer dan techniek alleen. De gehele implementatie van een SOC bestaat uit 3 fasen:

Fase 1: Inventarisatie

- Een SOC is geen generieke dienst, het is maatwerk. Een SOC moet inspelen op de veiligheidssituatie binnen een organisatie, de dreigingen waar de organisatie aan blootstaat en de impact die eventuele incidenten hebben. De inventarisatie bestaat daarom uit verschillende onderdelen:
- Interviews met diverse betrokkenen, waaronder de security officer, medewerkers uit het infrateam en het applicatieteam. Maar uiteraard ook met de IT-manager en de functionaris gegevensbescherming.
- Een analyse van de architectuur. Denk hierbij aan netwerktekeningen, systemen, procesbeschrijvingen en de datastromen tussen de verschillende onderdelen van uw IT-landschap.

Fase 2: Technische en organisatorische voorbereidingen

De **technische voorbereidingen** hebben vooral betrekking op het plaatsen van de log- en netwerksensoren Hiervoor wordt een detailontwerp gemaakt dat u baseert op de informatie die uit de inventarisatie naar voren is gekomen. De netwerksensor ontvangt een kopie van het relevante netwerkverkeer en doet daar een analyse op. De logsensor ontvangt de log- en eventdata van alle logbronnen, zoals de firewall, endpointbescherming, anti-malware en intrusion prevention-systemen.

De **organisatorische voorbereidingen** zijn vooral gericht op de samenwerking tussen het interne of externe SOC en de rest van de organisatie. Denk bijvoorbeeld aan de manier waarop het SOC bedreigingen en incidenten communiceert naar directieleden, managers en mensen op de werkvloer en aan de wijze waarop medewerkers binnen de organisatie omgaan met de adviezen en bevindingen van het SOC. We kunnen hierin onderscheid maken tussen tactisch-strategische collaboratie en operationele samenwerking.

De operationele samenwerking houdt zich vooral bezig met het afstemmen van het incidentmanagement en de rapportage. Welke procedure volgt u voor het melden van een incident? Hoe lopen de escalatiepaden? Wie zijn de contactpersonen en wat is hun verantwoordelijkheid? Hoe classificeren we incidenten? Wat is de vorm, inhoud en frequentie van rapportages? Op strategisch niveau denkt een SOC mee over vraagstukken als:

- Wat is de impact van de AVG en andere wet- en regelgeving op onze organisatie?
- Op welke terreinen voldoen onze maatregelen en op welke gebieden is er nog werk aan de winkel?
- Wat is de security-impact van een bepaalde digitale toepassing?
- Wat moet ik aanpassen om die toepassing veilig te maken?
- Welke medewerkers hebben welke training(en) nodig om hun security awareness op het juiste niveau te brengen?

Een SOC maakt de vertaalslag van security naar de alledaagse praktijk in een organisatie en adviseert de security officer welke organisatorische maatregelen nodig zijn om de informatiebeveiliging naar een hoger niveau te krijgen.

De meeste SIEM - of andere monitoring tooling - beschikt over standaard usecases, Deze zijn gericht op aanvallen en configuratiefouten welke binnen elke organisatie spelen. Denk bijvoorbeeld aan exploits van vulnerabilities, antimalware meldingen en privilege escalation. Nadat standaard dreigingen, welke onderdeel van de risico analyse zouden moeten zijn, geïdentificeerd en als usecase gedefinieerd zijn volgen de bedrijfsspecifieke usecases. De input van deze usecases komt uit bovenstaande analyse van de bedrijfsprocessen en mensen. Deze usecases worden vanuit het bedrijfsrisico bepaald en vertaald naar de techniek om het te kunnen monitoren. Met het vooraf definiëren van usecases kan op een beheerste wijze gestart worden met het verkrijgen van inzicht en controle op de voornaamste securityrisico's, maar ook op de maatregelen die er genomen zijn. Aan de aan hand van de binnenkomende data en feedback vanuit de organisatie wordt de werking van deze regels gecontroleerd en waar nodig verbeterd.

Fase 3: Pre-productie

Tijdens deze fase worden de eerste stappen tot monitoring gezet. In deze fase verricht het SOC de volgende werkzaamheden.

- **Analyseren data en usecases**. De loginformatie stroomt nu binnen en de verschillende usecases geven alarmen af. Het is nu zaak om de deze output te analyseren en te onderscheiden in 'business as usual' en bedreigingen. Door deze analyse wordt het duidelijk welke informatie 'standaard' is en welke afwijkingen gedetecteerd worden. Er ontstaat een baseline voor de hele organisatie. Afwijkingen van de baseline moeten worden opgenomen in usecases. Dit aanpassen van de baseline is een doorlopend proces, aangezien er voortdurend interne wijzigingen en nieuwe externe dreigingen optreden.
- **Het incidentmanagement inregelen**. In de voorbereidingsperiode zijn afspraken gemaakt over incidentmanagement. De baselineperiode is het moment om deze afspraken in de praktijk te toetsen en eventueel aan te passen. Daarom is in deze periode de communicatie frequentie tussen de verschillende organisatieonderdelen intensiever dan tijdens de productiesituatie.
- **Rapportages inregelen**. Tijdens de voorbereidingsfase zijn ook afspraken gemaakt over de vorm, inhoud en frequentie van rapportages. Tijdens deze periode wordt de haalbaarheid van dergelijke rapportages getoetst. Wellicht ontstaan er tijdens deze periode andere inzichten door de verkregen data, dit zal meegenomen worden in de rapportages.

Deze fase in het proces kan, op kleine schaal, herhaald worden wanneer een verandering in de dienstverlening of risicobeeld, ontstaat. Een dergelijke verandering zouden een herijking van de vastgestelde baseline ten gevolge kunnen hebben.

pinewood

Hoe helpt Pinewood?
Pinewood is een honderd procent Nederlands bedrijf met 25 jaar specialistische ervaring in de informatiebeveiliging. Pinewood heeft een eigen SOC in Delft. Daar werken hoogopgeleide, Nederlandstalige security-analisten. Zij houden 24 uur per dag, zeven dagen per week de systemen en netwerken van klanten nauwlettend in de gaten. De security-analisten van Pinewood slaan een brug tussen techniek en beleid, zodat ze complexe analyses uit de techniek direct kunnen omzetten naar strategische en beleidsmatige maatregelen.

Wij beseffen dat elke klant anders is. Bij ons vindt u geen digitale menukaart die we plichtmatig afvinken, maar maatwerk dat voldoet aan de specifieke bijzonderheden van uw IT-omgeving. Pinewood detecteert en analyseert dus niet alleen, maar speelt tevens een adviserende rol. Bij dit advies staan aspecten als wet- en regelgeving, integriteit en vertrouwelijkheid centraal. We zijn bovendien volledig onafhankelijk en kunnen met technologie van alle vendoren werken

Benieuwd naar de mogelijkheden? Neem dan gerust vrijblijvend contact met ons op. Bel naar 015 251 36 36 of stuur een e-mail naar info@pinewood.nl.

ISO

Pinewood BV.
Delftechpark 57
2628 XJ, Delft

015 251 36 36
info@pinewood.nl
www.pinewood.nl