Wat doet ons SOC voor U

De vijf basisfuncties van het SOC worden hieronder nader toegelicht:

- *Intelligence-functie*

  Een SOC heeft een kern van ervaren analisten nodig die zich richten op de specifieke dreigingen die relevant zijn voor de gebruikersorganisaties. Zij analyseren en geven richtlijnen aan de andere functies binnen het SOC, aan de beheerders, aan degenen die werkzaam zijn binnen systeemontwikkeling en aan de gebruikersorganisaties. Bij een nieuwe threat bepalen deze analisten tevens de signatures voor de SIEM en IDS's, welke scans moeten worden gedraaid, welke pentesten moeten worden uitgevoerd etc. De intelligence-functie is de kern van het SOC. De intelligence-functie richt zich enerzijds op dreigingen gericht op de bedrijfsprocessen van de gebruikersorganisatie. Een sterke band moet aanwezig zijn met de betreffende gebruikersorganisatie en het SOC moet goed inzicht hebben in de te beschermen gebruikersbelangen en de relevante dreigingen waaraan gebruikers bloot (kunnen) worden gesteld. Die kunnen voor verschillende gebruikers(groepen) geheel verschillend zijn. De intelligence-functie richt zich anderzijds op bepaalde IT-domeinen met hun eigen functioneel en technisch beheer. In dit kader is samenwerking alleen mogelijk indien een nauwe band kan worden opgebouwd met de betreffende beheerorganisatie.

- *Baseline Security-functie*

  Een SOC ziet toe op de technische aspecten van de uitrol van security baselines zoals BIR, ISO 27001, CSA Cloud Controls, OWASP, SANS, NCSC-richtlijnen webapplicaties, etc. Hieronder vallen vaak no brainers en immediate high-value actions zoals hardening van technische componenten en patchmanagement. Baselines worden door de systeemontwikkelaars en beheerders geïmplementeerd. Na implementatie van de baselines worden vulnerability- en compliance-scans uitgevoerd. Afwijkingen worden gerapporteerd aan de ontwikkelaars en beheerders. Management ziet toe op het oplossen van de afwijkingen.

- *Monitoring-functie*

  Een SOC bewaakt netwerkverkeersstromen en netwerkcomponenten en probeert op basis van patroon- en anomalie-herkenning, data-aggregatie en datacorrelatie (potentiële) cyberaanvallen te detecteren. Hierbij worden grote volumes aan signalen verzameld en geanalyseerd via filtering en het leggen van correlaties met als doel de werkelijk relevante signalen te kunnen oppikken. Het kernprobleem bij het gebruik van een SIEM is de rule-sets zo in te regelen dat de werkelijk belangrijke alerts of events worden gefilterd uit deze omvangrijke stroom. Slechts enkele alerts of events per dag zijn kandidaat voor het initiëren van een verder onderzoek. De effectiviteit van dit proces wordt grotendeels bepaald door de competenties en gedrevenheid van de betrokken analisten, oftewel dit is mensenwerk waarvoor (zeer) goede analisten nodig zijn. Die goede analisten zijn schaars.

- *Pentest-functie*

  Zowel tijdens systeemontwikkeling als herhalend tijdens exploitatie & beheer worden pentesten uitgevoerd. Deze tests zijn met name gericht op de door de intelligence-functie aangegeven aandachtspunten. Het doel is robuustheid te creëren. De pentesten in de productieomgeving zijn bedoeld als een noodzakelijk aanvulling op de baseline security functie van het SOC en de bijbehorende vulnerability- en compliance-scans. Via deze scans worden beveiligingsmaatregelen

routinematig nagelopen en afwijkingen gesignaleerd. Via de pentests wordt gecontroleerd of er omwegen zijn naar belangrijke functionaliteit of gegevens die door kwaad willende kunnen worden misbruikt. Populair gesproken, via de scans wordt gekeken of de voordeur dicht is, bij de pentest wordt flink aan de deur gerammeld om te kijken of deze niet uit de schoot springt en ook wordt nagegaan of langs de regenpijp omhoog geklommen kan worden naar een open dakraam. De werkzaamheden vereisen een hackers-perspectief. Pentesters dienen hun skills en inzichten dag in dag uit bij te houden. De effectiviteit van een pentest wordt vooral bepaald door de pentester en niet zozeer door zijn of haar ter beschikking staand gereedschap (hacking tools). Daarom dat actief geïnvesteerd dient te worden in bijvoorbeeld zelfstudie en red team/blue team exercises (ethical hacking wedstrijden). Tevens is het van zeer groot belang om in te zien dat pentesting in een productieomgeving als een zeer kritische activiteit moet worden beschouwd. Formele toestemming of een expliciete opdracht van systeemeigenaren dient verkregen te worden en voorzorgsmaatregelen moeten genomen worden om elke verstoring van de business operations te voorkomen.

- *Forensische functie*

  Het SOC assisteert forensische onderzoekers bij het verzamelen en analyseren van bewijsmateriaal. Veelal ligt de leiding van dit soort onderzoeken bij functionarissen die een formele opsporingsbevoegdheid hebben. De medewerkers van het SOC zijn uitvoerend op het technische vlak. Hieronder vallen bijvoorbeeld activiteiten zoals het veilig stellen van computers en storage en het analyseren van harde schijven, logbestanden, mails etc., waarbij veel aandacht nodig is voor een zorgvuldige ‘chain of evidence’ en ‘chain of custody’ tijdens het behandelen van bewijsmateriaal.