PvIB Expertbrief – Mei 2017
ISSN 1872-4876, jaargang 13 – Nr. 1

Een proactief business Cyber Security Operations Center

Een wendbaar SOC is mensenwerk

Renato Kuiper

Sandra Kagie (redactie)

Kelvin Rorive

Charlotte Rugers

André Smulders

Ben van Zuijlen

Rob van Os

De afgelopen jaren hebben veel organisaties een Security Operations Center (SOC) ingericht of als dienst ingekocht. Organisaties werden hierbij veelal gedreven vanuit strenger wordende wet- en regelgeving (compliance-driven) en vanuit de wens om (potentiële) dreigingen in een vroegtijdiger stadium te ontdekken. SIEM (Security Information & Event Management) neemt binnen een traditioneel SOC een centrale plaats in. Dit maakt een traditioneel SOC bij uitstek reactief. Een probleem wordt gedetecteerd, dit wordt gerapporteerd en er wordt actie ondernomen. Terwijl de snelle veranderingen in de wereld om ons heen, en de cyberwereld in het bijzonder, vragen om een proactief SOC. Wat is er nu nodig om van een traditioneel reactief SOC (r-SOC) te groeien naar een modern proactief SOC (p-SOC)? Hoe ziet een hedendaags p-SOC eruit dat is voorbereid op de toekomst?

Pagina

2

EEN WENDBAAR SOC IS MENSENWERK

MANAGEMENTSAMENVATTING

In een traditioneel Security Operations Center (SOC) nam SIEM (Security Information & Event Management) een centrale plaats in. Dit maakte een traditioneel SOC bij uitstek reactief. Terwijl de snelle veranderingen in de wereld om ons heen, en de cyberwereld in het bijzonder, vragen om een proactief SOC.
We kunnen ons daarom voorstellen dat veel organisaties en daarbinnen de SOC-verantwoordelijken zich afvragen wat er nodig is om van een traditioneel reactief SOC (r-SOC) te groeien naar een modern proactief SOC (p-SOC).
Wat ons betreft is het antwoord relatief eenvoudig: de juiste mensen. Een modern wendbaar SOC is namelijk bij uitstek mensenwerk. Het is en blijft immers de mens die uiteindelijk besluit een alarm op te volgen. Daarbij is het aan de mens, ondersteund door allerhande techniek, om de bredere context van een alarm te zien.

Focus essentieel
Belangrijk bij het vaststellen van de doelstellingen en ambities van een modern SOC is bovendien het besef dat je binnen een SOC niet alles kunt doen. Focus in het bepalen van je Incident en Response capabilities is daarom essentieel.
Er bestaat in het vaststellen van deze doelstellingen geen ‘one size fits all’-keuze. Dit is volledig afhankelijk van je ambitieniveau en het risicoprofiel van je organisatie. Waarbij het kenmerk van een modern p-SOC is dat het zelf het voortouw neemt en speerpunten op de agenda zet. Ga als SOC bijvoorbeeld actief op zoek naar nieuwe dreigingen op basis van threat hunting. Neem hierbij de business, maar ook de ‘beslissers’ bij de hand en laat ze zien wat een p-SOC voor hun organisatie kan betekenen.
De focus verschuift zo van het reageren op bekende dreigingen naar het zoeken naar onbekende dreigingen en afwijkingen (anomaly detection). Naast de verschuiving van reactief naar proactief zie je binnen een p-SOC dus ook de verschuiving van bekend naar onbekend (van rules naar anomalies).

De juiste mensen
Een modern p-SOC is bij uitstek dynamisch. De mate van wendbaarheid in een continu veranderende omgeving bepaalt immers de kracht van zo’n SOC. Juist met deze factor wendbaarheid moet je bij de keuze voor je mensen binnen een SOC rekening houden.
De match tussen de juiste mensen bij specifieke capabilities is van cruciaal belang in de organisatie van een SOC. Om communicatie tussen het SOC en de business soepel te laten verlopen, kun je er binnen een organisatie voor kiezen om vice versa te zorgen voor ambassadeurs. Mensen die vanuit het SOC een rol krijgen in de business en andersom. Om zo wederzijds begrip en draagvlak te creëren.
Een heel belangrijke les bij het kiezen van de juiste mensen voor een SOC is ‘het gaat niet om kwantiteit, maar om kwaliteit’. Wanneer je in de gelukkige omstandigheid bent dat je de juiste mensen hebt weten samen te brengen, is het de volgende stap deze mensen te behouden. Schrik echter niet wanneer specialisten binnen een SOC na vijf jaar daarbuiten op zoek gaan naar een andere uitdaging. SOC-werk kan voor sommige capabilities namelijk

een sleur worden. Om goede mensen in elk geval vijf jaar te behouden moet je ze daarom uitdagingen blijven bieden.
Denk in het kader van voldoende uitdaging bijvoorbeeld aan een koppeling van steeds weer terugkerende activiteiten van monitoring & response aan activiteiten als attack simulation & hunting threats. De kans dat je goede mensen op deze manier langer vast kunt houden, is groot.

Invloed Big Data
Natuurlijk is ook in een p-SOC nog altijd techniek aanwezig uit een r-SOC, zoals een SIEM of loginformatie vanuit applicaties of security devices zoals firewalls, Intrusion Detection System (IDS), Data Loss Prevention (DLP) et cetera.
Gezien de steeds groter wordende hoeveelheid data (Big Data) en bedreigingen waarmee SOC's te maken krijgen, is verdere automatisering van de workload voor het detecteren, analyseren en afhandelen van incidenten noodzakelijk. Denk aan technieken als 'Machine Learning'(ML), 'Artificial Intelligence'(AI) en 'Deep Learning'(DL). Meer mensen is in deze in elk geval niet de oplossing. De stroom data zal namelijk alleen maar groeien en je kunt een SOC-team niet maar uit blijven breiden. Wel vraagt Big Data om specifieke nieuwe specialisten en technieken op het gebied van data science. Een aanvulling op een wendbaar, modern SOC-team.

Op weg naar tactical SOC
Concluderend kun je stellen dat binnen een modern p-SOC in tegenstelling tot een traditioneel r-SOC niet meer de techniek, maar de mens leidend is. Een modern p-SOC is niet langer een opeenstapeling van technische oplossingen en een SOC anno 2017 staat zeker niet meer gelijk aan een SIEM.
De menselijke factor is uiteindelijk bepalend voor het succesvol zijn van een modern p-SOC En dit succes wordt uiteindelijk bepaald door het al dan niet mee kunnen bewegen met de in sneltreinvaart veranderende samenleving om ons heen. De p-SOC is wat ons betreft allesbehalve een eindpunt. SOC's zullen verder blijven ontwikkelen. In onze ogen tot t-SOC's, tactical SOC's. Waarbinnen wendbaarheid in combinatie met mensenwerk keywords blijven. Zo'n t-SOC schuift verder richting een proactieve en voorspellende focus aangevuld met radicaal geautomatiseerde response. Zo'n t-SOC leunt wat ons betreft op een hybride team van medewerkers dat infrastructurele, applicatieve, security, Big Data en data science expertises samenbrengt in dienst van de business.

1.De probleemstelling van deze expertbrief luidt:

Hoe ziet een modern SOC eruit dat is voorbereid op de toekomst met als bijzonder aspect de mens.

In deze expertbrief bundelen verschillende deskundigen hun visie en ervaringen om gezamenlijk tot een advies te komen over de inrichting van een modern p-SOC. Een SOC dat bestaande en nieuwe dreigingen het hoofd kan bieden.

De deskundigen hebben er hierbij voor gekozen de mens centraal te stellen. Ondanks alle techniek is de menselijke factor binnen een SOC namelijk bepalend voor succes. Het is en blijft immers de mens die uiteindelijk besluit een alarm op te volgen. Daarbij is het aan de mens, ondersteund door allerhande techniek, om de bredere context van een alarm te zien.

Afbeelding 1: Opstellers SOC expertbrief.

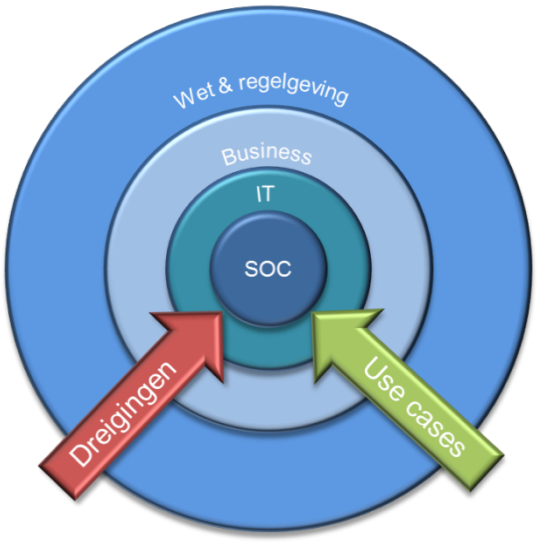
Vlnr: André Smulders, Kelvin Rorive, Charlotte Rugers, Renato Kuiper, Rob van Os en Ben van Zuijlen.

2. AMBITIES EN DOELEN VAN EEN MODERN SOC

In zijn algemeenheid zijn de ambities en doelen van een modern p-SOC tweeledig:

1. Inzicht krijgen in Situational Awareness.
2. Incident & Response meer gericht op business belang.

Situational Awareness (SA) staat voor het inzicht in wat een organisatie bedreigt. Dit kan van alles zijn: een datalek, niet voldoen aan nieuwe wet- en regelgeving, Internet of Things (IoT), een Distributed Denial of Service (DdoS)- of Advanced Persistent Threat (APT)-aanval, Bring your Own Device (BYOD), een blind vertrouwen in het eigen kunnen, et cetera.
SA houdt in dat je van deze risicofactoren op de hoogte bent, dat je ze meet en weet. Maar ook dat je vervolgens bepaalt of er iets moet worden gedaan aan deze risico's. En zo ja, wat er moet worden gedaan.
SA gaat daarmee verder dan Risico Management (de strategie) en Security Incident Management (de operatie/inrichting). SA verbindt deze twee en vormt zo de ruggengraat van een SOC. Heb je inzicht in je SA dan weet je niet alleen wat je als organisatie moet kunnen om dreigingen het hoofd te bieden (je capabilities), maar dan weet je ook of de manier waarop je organisatie is ingericht afdoende functioneert om dit te kunnen doen. Dit integraal en centraal inzicht in je organisatie door het continu combineren van verschillende informatiebronnen kan alleen middels een SOC. Dit zeker in een continu veranderende wereld waarin je te maken hebt met een explosie aan informatie, steeds weer nieuwe dreigingen, nieuwe wet- en regelgeving en een continu veranderende interne organisatie.



Afbeelding 2: De plek van een SOC in een continu veranderende omgeving (Rob van OS).

Inzicht in je SA is zo belangrijk om als SOC risico-gebaseerde én kosteneffectieve beslissingen te kunnen nemen waarmee je primaire doelstellingen en bedrijfsprocessen daadwerkelijk ondersteunt.

Belangrijk bij het vaststellen van je doelstellingen en ambities is het besef dat je binnen een SOC niet alles kunt doen. Focus in het bepalen van je Incident en Response capabilities is

daarom essentieel. Overleg met je stakeholders: wat zijn hun verwachtingen? Stem hier je ambities op af. Stel vast welke capabilities essentieel zijn voor de continuïteit van je business en ontwikkel deze capabilities of koop ze in. Je kunt hierbij ook kiezen voor een hybride oplossing, een combinatie van interne en externe kennis en kunde.

Er bestaat in het vaststellen van je doelstellingen bij een SOC geen 'one size fits all'-keuze. Dit is volledig afhankelijk van je ambitieniveau en het risicoprofiel van je organisatie. Waarbij je momenteel een verschuiving van ambitieniveau ziet in de richting van een p-SOC. Binnen een r-SOC werd nog veelal gewacht op beleidsmakers om vervolgens actie te ondernemen. Een p-SOC kiest er steeds vaker voor zelf het voortouw te nemen en speerpunten zelf op de agenda te zetten.
Communicatie is hierbij heel belangrijk. Neem de business, maar ook de 'beslissers' bij de hand en laat ze zien wat een SOC voor hun organisatie kan betekenen.

De focus verschuift zo van het reageren op bekende dreigingen naar het zoeken naar onbekende dreigingen en afwijkingen (anomaly detection). Naast de verschuiving van reactief naar pro-actief zie je binnen een p-SOC dus ook de verschuiving van bekend naar onbekend (van rules naar anomalies).

Nb. Een puur compliance georiënteerd SOC biedt organisaties anno 2017 volgens de deskundigen weinig meerwaarde. Het getuigt bovendien niet van een modern ambitieniveau waarbinnen omgaan met veranderingen om ons heen (dreigingen, business, IT en wetgeving) centraal staat. De kern van een p-SOC is immers steeds weer in kunnen spelen op deze veranderingen en zo bij te dragen aan de continuïteit van de business.

Het vaststellen van je ambitieniveau hangt nauw samen met het mandaat dat je als SOC krijgt. In hoeverre kun je als SOC eisen van belanghebbenden/de business dat ze na de detectie van een probleem de benodigde maatregelen nemen? Dit mandaat kent grofweg 3 niveaus:

1. Geen mandaat. Het SOC is puur adviserend, maar advies hoeft niet te worden opgevolgd door bijv. CIO's, CISO's, CEO's of systeem-eigenaren.
2. Gedeeld mandaat. Het SOC kan aanbevelingen doen. Deze aanbevelingen worden gewogen. Het SOC heeft een stem, maar niet de finale stem.
3. Volledig mandaat. Het SOC kan maatregelen afdwingen zonder toestemming van hogerhand.

(Bron: - Ten Strategies of a World-Class Cybersecurity Operations Center. P. 17)

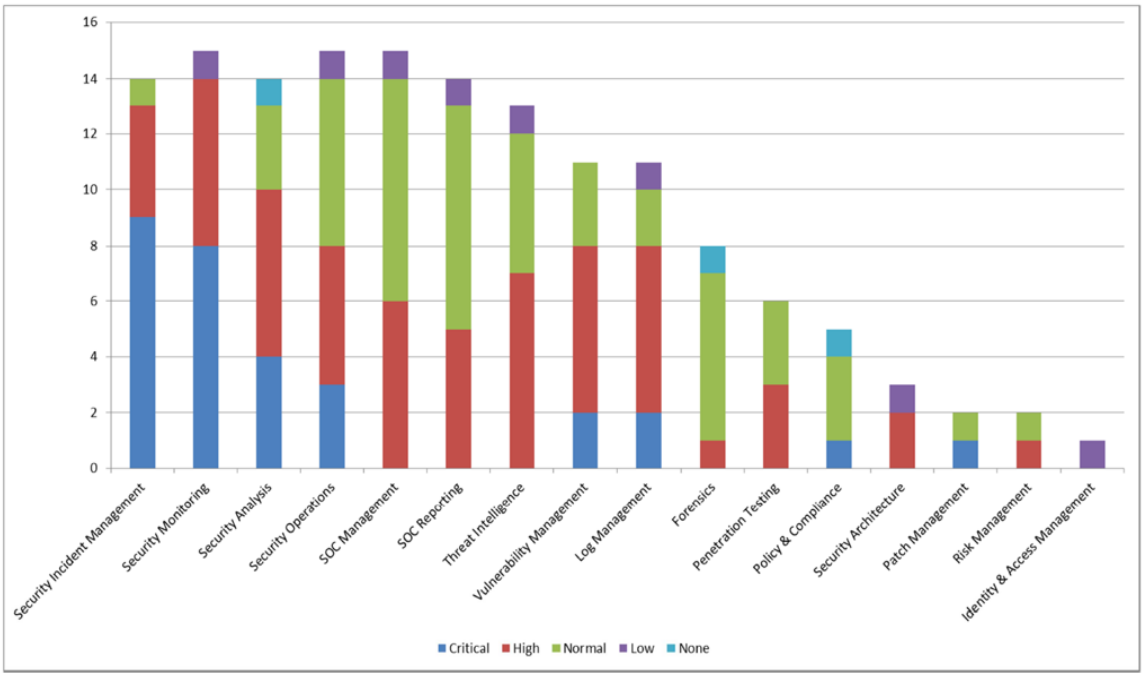
"Geef een SOC het mandaat om zijn werk te kunnen doen"

De inrichting van een SOC gebeurt op basis van het ambitieniveau in combinatie met het mandaat dat een SOC krijgt. Dit doorgaans over vijf assen: capabilities, organisatie, mensen, processen en techniek. Deze vijf assen diepen we in de komende vijf subhoofdstukken verder uit.

3. INRICHTING SOC

3.1 Capabilities

Welke capabilities je met een SOC nastreeft, is zoals in het vorige hoofdstuk benoemd afhankelijk van je ambitieniveau. De volgende figuur geeft een overzicht van de set aan capabilities waar je je als SOC op kunt richten. Waarbij we nogmaals benadrukken dat focus essentieel is.



Afbeelding 3: 'SOC-processes in use' geeft een overzicht van mogelijke capabilities waarop je kunt focussen (bron: Rob van Os, SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers).

De kolommen in bovenstaande figuur geven de relevantie aan van de SOC-processen die uitgevoerd worden. Hierbij is in blauw, rood, groen, paars en lichtblauw aangegeven hoe kritisch ze zijn. 'Blauw' staat voor kritisch (moeten altijd aanwezig zijn), 'rood' wordt als zeer belangrijk ervaren, 'groen' wordt als normaal aanwezig geacht, 'paars' wordt als zelden aanwezig geacht en 'lichtblauw' wordt als niet aanwezig geacht.
Nb. De relevantie is bepaald op basis van een survey onder 16 deelnemers. De waarde in de Y-as is het aantal deelnemers dat heeft aangegeven die dienst te verlenen.

Capabilities van een SOC zijn volgens de standaarden van het National Institute of Standards and Technology (NIST - www.nist.gov/cyberframework) in hoofdlijnen onder te verdelen in verschillende fases en daarbij behorende hoofdprocessen:

- Phase: Identify – Service: Threat Intelligence.
- Phase: Protect – Service: Vulnerability Management / Penetration Testing.
- Phase: Detect – Services: Security Monitoring, Security Analysis en Log Management.
- Phase: Respond – Services: Security Incident Management.
- Phase: Recover – Services: Recovery after a security incident, Back-up & Restore

Schematisch ziet dit er als volgt uit:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Source: Cybersecurity Framework 1.0

Afbeelding 4: Capabilities van een SOC volgens de standaarden van het National Institute of Standards and Technology (Bron: NIST - www.nist.gov/cyberframework)

De eindverantwoordelijken van een SOC bepalen op welke services de nadruk binnen een SOC ligt. Dit afhankelijk van wat stakeholders wensen, leidende wet- en regelgeving en beschikbare middelen. Bepaal op basis hiervan de kritische factoren van jouw SOC en focus daarop. Deze eindverantwoordelijkheid ligt altijd bij de organisatie en kan niet belegd worden bij bijvoorbeeld een extern SOC.

“Maak binnen een SOC keuzes. Focus en prioritering is essentieel voor succes.”

De lijst van mogelijke services is enorm. Zie bijvoorbeeld *Table 1. SOC Capabilities - Ten Strategies of a World-Class Cybersecurity Operations Center p. 19-24*. Bedenk daarbij dat geen enkel SOC al deze capabilities in zich zal hebben.

3.2 De organisatie van een SOC

Een SOC kan op meerdere manieren gepositioneerd zijn in een organisatie. Dat is bepalend voor de wijze van governance. Daarnaast is de rol van een SOC ook van invloed op de governance. Besteed je een SOC uit dan krijg je te maken met een regiemodel waardoor afspraken een formeler karakter krijgen ten opzichte van een intern SOC dat alles zelf doet. Een SOC dat intern dienstverlenend is, heeft overwegend meer flexibiliteit en kan daardoor sneller reageren op veranderende dreigingen.
Aspecten die van belang zijn bij governance van een SOC zijn onder andere volwassenheid, verantwoording over de effectiviteit van een SOC en ook de financiële verantwoording.

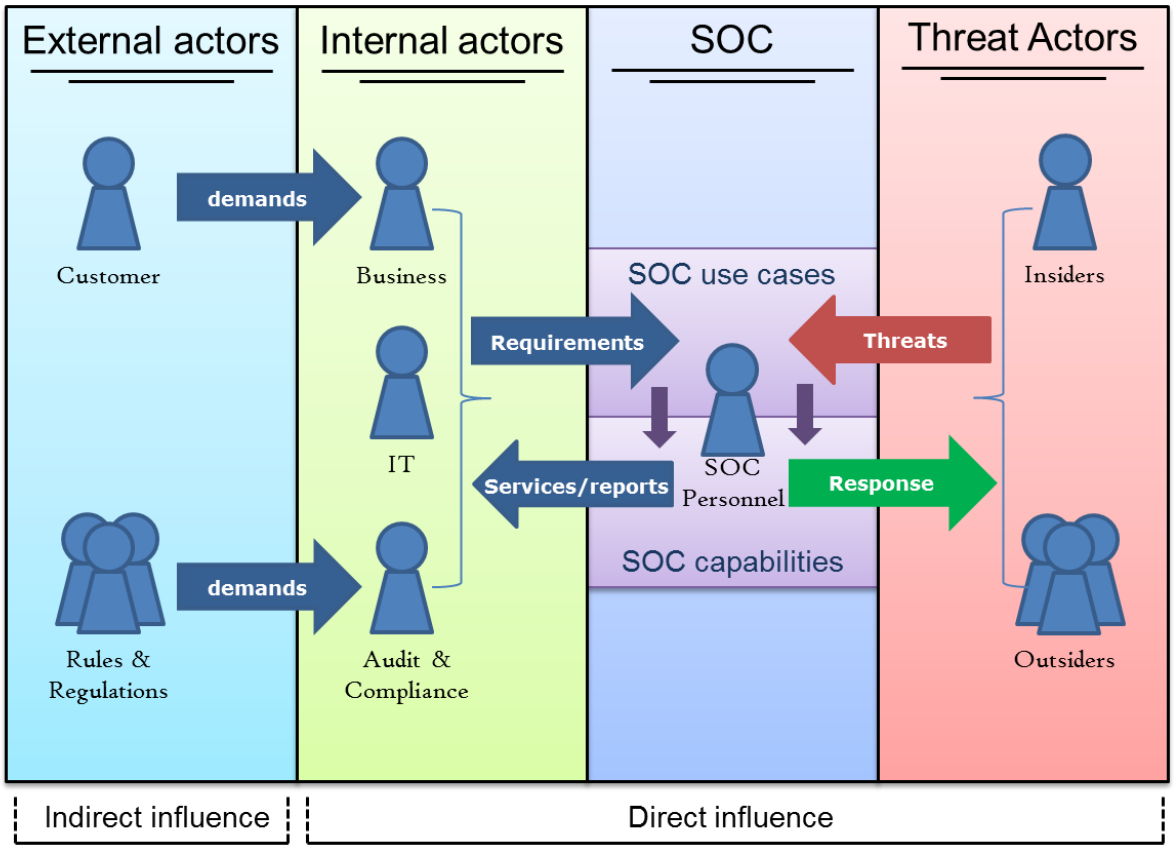
Binnen de organisatie van een SOC zijn mensen leidend. Zij bepalen uiteindelijk welke kennis, kunde en ervaring binnen een SOC aanwezig is. Mis je als leidinggevende binnen een SOC specifieke menskracht voor bepaalde capabilities bekijk dan hoe je dit het beste kunt oplossen: intern door opleiding of door externe krachten binnen te halen. Een trend die in deze gaande is, is die van hybrid staffing.

“Benut binnen een SOC de mogelijkheid van hybrid staffing.”

Een modern p-SOC is bij uitstek dynamisch. De mate van wendbaarheid in een continu veranderende omgeving bepaalt immers de kracht van zo’n SOC. Juist met deze factor wendbaarheid moet je bij de keuze voor je mensen binnen een SOC rekening houden.

De match tussen de juiste mensen bij specifieke capabilities is van cruciaal belang in de organisatie van een SOC. Ditzelfde geldt voor de keuze van mensen die om kunnen gaan met verandering. Hierover later meer in het hoofdstuk ‘mensen’.

In een traditioneel r-SOC is de IT manager de belangrijkste stakeholder. Hij is verantwoordelijkheid voor een betrouwbare infrastructuur. Daarnaast speelt binnen dit traditioneel r-SOC de compliance officer een belangrijke rol.
Je ziet dat in een modern p-SOC - waarbinnen het totale security(dreigings)beeld van een organisatie wordt geanalyseerd onder meer op basis van een actueel, operationeel dreigingsbeeld - ook de business stakeholder wordt van een SOC. De business wil graag inzicht hebben in de kwaliteit van de geleverde IT diensten en de veiligheid daarvan (ze zijn op zoek naar een dashboard). Risicoreductie is voor hen een belangrijke business driver.



Afbeelding 5: Geeft schematisch weer welke rollen/ actoren een modern p-SOC beïnvloeden (Rob van Os op basis van *'Figure 1' p.14 - Ten Strategies of a World-Class Cybersecurity Operations Center*).

Een belangrijke vraag die in een modern p-SOC beantwoord moet worden, is wie er de lead heeft in de opleiding van de business als het gaat om IT en security. Welke kennis moeten zij in deze hebben? Belangrijk voor zowel de business als het SOC om optimaal te kunnen presteren. Immers bij een incident kan het SOC niet alles afhandelen, de business moet zelf ook acties ondernemen.
Om communicatie tussen het SOC en de business soepel te laten verlopen, kun je er binnen een organisatie voor kiezen om vice versa te zorgen voor ambassadeurs. Mensen die vanuit het SOC een rol krijgen in de business en andersom. Om zo wederzijds begrip en draagvlak voor verandering te creëren.

3.3 De factor mens binnen een SOC

We hebben er al vaker aan gerefereerd dat wat ons betreft de factor mens het succes van een modern SOC bepaalt. Uiteindelijk is het de volwassenheid van je mensen die bepaalt of je met je huidige processen en de beschikbare technieken een bepaald plafond kunt halen.

Een heel belangrijke les bij het kiezen van de juiste mensen voor een SOC is 'het gaat niet om kwantiteit, maar om kwaliteit'. Met de juiste tools kan één goede analist het werk doen van honderd gemiddelde analisten. In het boek *Ten Strategies of a World-Class Cyber Security Operations Center* wordt dit als volgt omschreven: *"Analysts can be trained to use a*

tool in a rudimentary manner, they cannot be trained in the mind-set or critical thinking skills needed to master the tool." Een goede analist doorgrondt de output van een tool; hij/zij kent de vorming van de output en de context waarin deze is ontstaan.

"Analyst quality is vastly more important than analyst quantity"

In datzelfde *Ten Strategies of a World-Class Cyber Security Operations Center* wordt de zoektocht naar de juiste mensen voor een SOC ook als volgt omschreven:
"Perhaps the number one quality to look for in any potential hires to the SOC is their passion for the job, regardless of the position. Intrusion monitoring and response is not just "a job" where people put in their eight- or 12-hour shift, collect a paycheck, and then leave. When it comes to "cyber," we're looking for enthusiasm, curiosity, and a thirst for knowledge. This passion is what will keep them coming back to the job, day after day, despite the stress and challenges inherent in operations. This passion, along with intellect and other soft skills, is what propels fresh recruits into becoming what we will call "rock-star analysts."

Wanneer je in de gelukkige omstandigheid bent dat je de juiste mensen hebt weten samen te brengen, is het de volgende stap deze mensen te behouden. Hierbij is ook een belangrijke rol weggelegd voor HR. Maar wat je zelf zeker in de gaten moet houden, is mensen uitdaging blijven bieden. SOC-werk kan voor sommige capabilities een sleur worden.

Denk bij het bieden van voldoende uitdaging aan de diamanten in je team bijvoorbeeld aan het koppelen van steeds weer terugkerende activiteiten in het kader van monitoring & response, aan activiteiten als attack simulation & hunting threats. Je zou zelfs kunnen denken aan een (inter)nationale competitie op dit vlak tussen SOC's onderling.

De kans dat je goede mensen op deze manier langer vast kunt houden, is groot. Zeker wanneer je dit combineert met een op maat ontwikkelplan. Wat je echter niet moet vergeten is dat je veel mensen na zo'n vijf jaar sowieso kwijt kunt raken. Dan hebben ze alles wel een keer meegemaakt, is de ervaring. Gezond verloop zorgt echter voor een juiste dynamiek binnen een SOC. Nieuwe mensen met nieuwe opleiding skills, zoals data-analisten, leveren immers weer nieuwe inzichten op.
Waar binnen organisaties nog te weinig aandacht voor is, is de doorstroom en ontwikkeling van SOC-mensen elders in de organisatie. Terwijl zij juist daar de ambassadeursrol voor het SOC op zich kunnen nemen. Een belangrijk aandachtspunt waarin ook weer HR een rol kan of moet spelen. Job rotation is in deze een veelgehoorde term, maar in de praktijk komt het maar weinig voor.

Nb. In zijn algemeenheid wordt gesteld dat gezien de snelle ontwikkelingen die momenteel op SOC's afkomen het niet eenvoudig is geschikte kandidaten van een opleiding te pikken. Dat geldt bijvoorbeeld niet voor de noodzakelijke 'blauwe' mensen die voor structuur zorgen binnen een SOC-team, maar zeker wel voor de 'gele' extraverte creatievelingen die zorgen voor de nodige balans in een team én zeker in de huidige tijd voor toekomstbestendigheid. Het zijn immers juist die creatievelingen die vaak het gewenste aanpassingsvermogen aan de dag leggen om mee te kunnen gaan in de huidige 'evolving' wereld waarin een SOC opereert.

3.4 Processen binnen een SOC

Vanuit een SOC-perspectief wordt volgens ons invulling gegeven aan vier hoofdprocessen binnen een SOC:

- Threat Intelligence: het inzicht krijgen in wat er gebeurt in onze omgeving en de wereld om ons heen.
- Vulnerability Management: het testen, bewaken en verhelpen van de kwetsbaarheden in de informatiesystemen.
- Security Monitoring: Het 24/7 monitoren op afwijkingen en aanvallen.
- Incident Response: het proces voor het afhandelen van verstoringen en aanvallen vanuit het SOC met de organisatie.

De processen die spelen binnen een SOC hangen uiteraard nauw samen met de twee doelen die veel SOC's hebben:

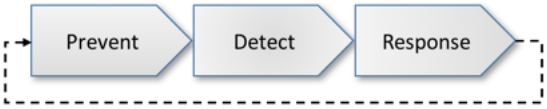
1. Inzicht krijgen in Situational Awareness.
2. Incident & Response gericht op business belang.

Het threat intelligence proces in het kader van het verkrijgen van SA ziet er in hoofdlijnen als volgt uit:

1. **Verzamelen van data**
   Het bij elkaar brengen van informatie uit diverse interne en externe bronnen en deze waar nodig verrijken met interne informatie, zoals een configuratie database en threat intelligence bronnen.
2. **Triage en omzetten in actionable items**
   Het gestructureerd beoordelen en analyseren van ruwe data op relevantie voor de eigen situatie. Waaronder bijvoorbeeld een diepere analyse van de gevonden data of het vergaren van aanvullende data om een betere analyse te kunnen maken. Bepaalde informatie kan direct omgezet worden in acties, zoals het patchen van systemen, het aanpassen van detectie regels in SIEM's, controleren op IOC's (Indicators of Compromise), et cetera.
3. **Communicatie en delen met anderen**
   Afhankelijk van onder andere de positionering van het SOC en de mate van betrokkenheid bij verschillende communities, zoals ISAC's en threat intelligence security leveranciers, kan het wenselijk of zelfs noodzakelijk zijn (delen van) de analyse te delen met derden. Hierbij is het van belang om vast te stellen welke informatie om wat voor reden met deze partijen gedeeld kan en/of moet worden. Afhankelijk van het soort community kan het zelfs noodzakelijk zijn om een bepaalde bijdrage te leveren door zelf de bron van threat intelligence te zijn voor andere partijen.
4. **Maken van een dreigingsbeeld en rapportage**
   Belangrijk in dit proces is een (real time) beeld of rapport creëren over de weerbaarheid van de organisatie op basis van diverse threat intelligence informatie.

Dit beeld kan ook de business voorzien van de nodige waakzaamheid bij het uitvoeren van de bedrijfsprocessen.

In het kader van Incident & Response zijn de lopende processen vrij eenvoudig schematisch weer te geven. Je hebt het hier namelijk over de continue Prevent-Detect-Response cyclus. Deze cyclus volgt steeds op het Identify-proces:



Afbeelding 6: De continue Prevent-Detect-Response cyclus (Bron: pag. 3 The Next SecOps Fundamentals)

Waarbij je response nog kunt uitsplitsen in de processen: repression (schadebeperking) en recovery (herstel van schade).

Belangrijk binnen deze cyclus is ook het proces van reporting. Wie controleert of geautomatiseerde beslissingen en/of acties goed zijn? Dit is een belangrijk aandachtspunt voor de effectiviteit en betrouwbaarheid van het SOC.

Voor zowel het inzicht krijgen in Situational Awareness als voor het vergroten van de Incident & Response capability geldt dat de processen om deze doelen te verwezenlijken op twee manieren kunnen worden ingericht: ‘mode 1’ en ‘mode 2’. Waarbij ‘mode 1’ staat voor de ‘solid as a rock’ oude legacy systemen terwijl ‘mode 2’ staat voor een veel dynamischer, agile aanpak. Hierbij gaan we uit van de ‘mode 1’ en ‘mode 2’ definities van Gartner.

- In de ‘mode 1’ werken we in een omgeving die vrij stabiel is, erg oude systemen heeft waar niet veel wijzigt in functionaliteit. Security monitoring wordt mogelijk eenvoudig omdat we vrij snel kunnen vaststellen wat het normale en dus ook het abnormale gedrag in de systemen is. Daarnaast kunnen we vulnerability management eenvoudig uitvoeren: we weten immers welke systemen we hebben. Ze zijn deels verouderd, maar er verandert niet veel. Als we inzichtelijk hebben welke systemen dat zijn, inclusief hun operating systemen, versies en patch niveaus, dan kunnen we een nieuwe CVE eenvoudig mappen op relevantie. We lopen hierbij wel het risico dat er voor oude systemen geen security patches worden uitgebracht. In dat geval is vulnerability management nagenoeg onmogelijk en moeten we virtueel gaan patchen of andere security maatregelen kunnen implementeren.
- In een ‘mode 2’ omgeving - veel dynamischer zowel qua gebruikers, als systemen en functionaliteit - moeten we veel meer energie steken in het goed inbedden van zaken als security monitoring en vulnerability management. Het vraagt een snelle wijze van schakelen op veranderingen en bewaking van nieuwe kwetsbaarheden. Het mappen van nieuwe CVE is dan ook al een stuk lastiger. Het security monitoren wordt ook lastiger, we moeten ons instellen op een omgeving waarin het abnormale gedrag en afwijkingen daarop veel moeilijker vast te stellen zijn. Het normale gedrag is immers al amper te volgen en te bepalen. Als organisatie moet je steeds meer

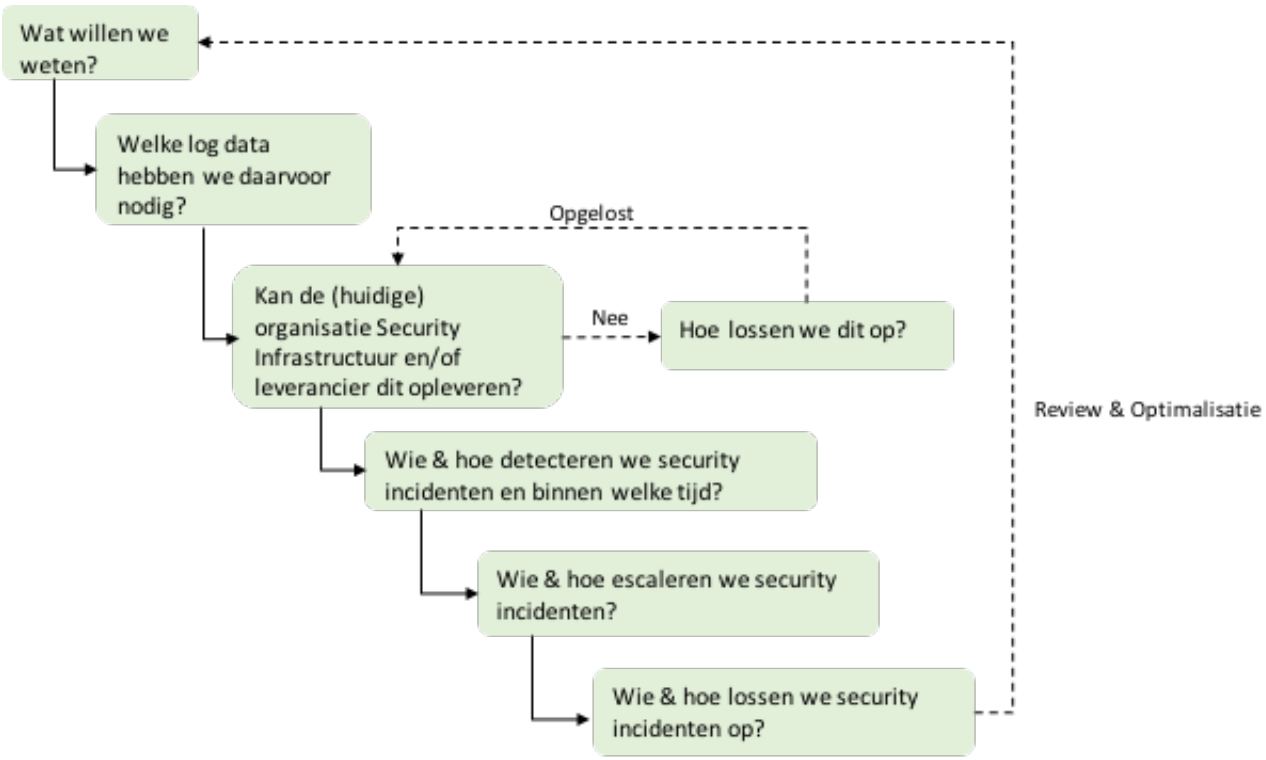
ontwikkelen naar deze ‘mode 2’ omgeving. Dit om snel en wendbaar in te kunnen spelen op veranderingen. Dit vraagt niet alleen een andere benadering van de SOC hoofdprocessen, maar ook iets van de andere vier assen: capabilities, organisatie, mensen en techniek.

3.5 Use cases

Op deze plek willen we ook aandacht besteden aan het ontwikkelen van een use case voor het SOC. Een activiteit die vanuit een dreigingsgedachte opgezet moet worden. Hierbij moet antwoord gezocht worden op vragen als: Waar zijn we bang voor? Welke dreigingen vormen risico’s voor ons en de business? Welke risico’s willen we mitigeren? Wat willen we weten? Hoe gaan we dat vaststellen? Welke informatie hebben we daarvoor nodig? Is die informatie beschikbaar is het bestaande applicatielandschap? Welke signalen zijn van belang om op te reageren? En wie gaat er wat en wanneer doen?

Het verkrijgen van informatie uit een bestaande omgeving kan leiden tot het plaatsen van security sensoren in het netwerk (firewalls, Intrusion Detection Systemen (IDS) / Intrusion Prevention Systemen (IPS) / Data Loss Prevention (DLP) software of agents op servers. Eventueel moeten er applicaties aangepast worden zodat de benodigde loginformatie daadwerkelijk door de applicatie kan worden geproduceerd.

Het proces zoals hierboven beschreven, is weergegeven in Afbeelding 7:



Afbeelding 7: Use case ontwikkelproces (Renato Kuiper, met dank aan Wilco van Ginkel).

Het opzetten van de use case geeft ook meteen antwoord op de vraag wie gaat wat wanneer doen. Dit helpt zeker in het geval er gekozen wordt voor een MSSP (Managed Security Service Provider) die de SOC-dienstverlening gaat leveren, de SOC-governance op tactisch en operationeel niveau is dan al beschreven voor die use cases.

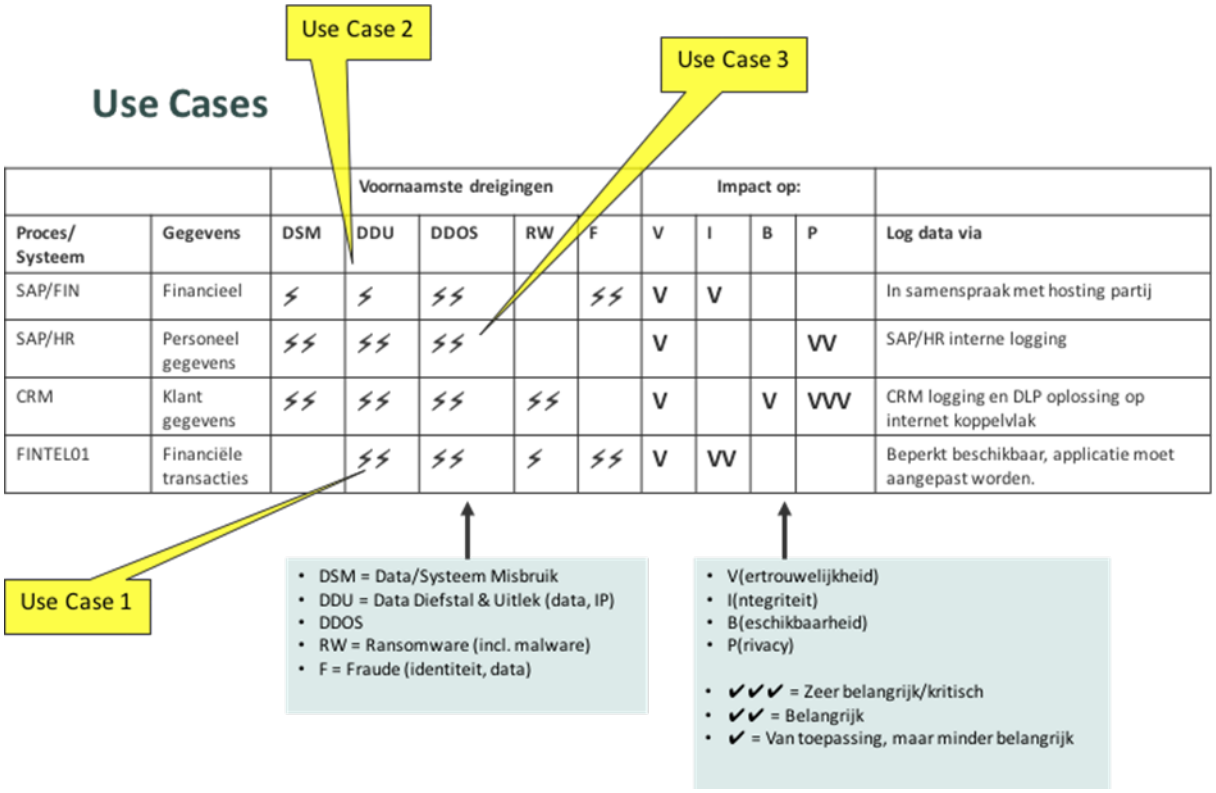
Elke use case gaat dus uit van een mogelijk scenario dat kan optreden. Dit scenario wordt beschreven, zie afbeelding 8, en gemapped op de infrastructuur en/of applicatie waar deze kan optreden.

	Mensen	Technologie	Processen
Wat willen we weten → Is er fraude gepleegd in financieel systeem of door een specifieke medewerker?			
Welke log data hebben we daarvoor nodig?	Corporate Financiële afdeling	SAP Platform	Financiële / betalingsproces
Kan de (huidige) Security Infrastructuur en/of leverancier dit opleveren?		Ja[1]	
Wie & hoe detecteren we security incidenten en binnen welke tijd?	MSSP	Organisatie log data verzameld & geanalyseerd door MSSP platform & MSSP mensen	MSSP
Wie & hoe escaleren we security incidenten?	MSSP naar organisatie contact personen	Email, MSSP security dashboard, ...	MSSP escalatieproces volgens SLA & workflow
Wie & hoe lossen we security incidenten op?	Organisatie, mogelijk met ondersteuning van MSSP	MSSP levert security incident data aan organisatie. Organisatie onderzoekt, mogelijk meer info vanuit organisatie security infrastructuur.	Organisatie incident response proces
Review & optimalisatie: Wat moeten we in de SMLC aanpassen om fraude te voorkomen of sneller/beter te detecteren?	Mogelijke aanpassingen	Mogelijke aanpassingen	Mogelijke aanpassingen

Opmerkingen:
1. Vanwege voorbeeld is er nu 'Ja' ingevuld. Praktijk zal uitwijzen of dit ook zo is.

Afbeelding 8: Beschreven Use case (Renato Kuiper, met dank aan Wilco van Ginkel).

Verschillende mogelijke scenario's kunnen dan beschreven worden, zoals weergegeven in Afbeelding 9.



Afbeelding 9: Use Case (Renato Kuiper, vanuit een praktijk case in Nederland, met dank aan Wilco van Ginkel).

Elke use case moet geëvalueerd worden op de correcte werking en of deze efficiënt is. Wijzigingen in het dreigingsbeeld kunnen leiden tot het aanpassen van een bestaande use cases of het verwijderen van een bestaande use case, danwel opname van een nieuwe use case.
Voor alle use cases geldt: begin simpel met de use cases die kunnen werken. Kies daarom voor de use cases waarvoor de dreiging helder is, het bijhorende risico een eigenaar heeft (bij voorkeur uit de business), waarvoor de manier waarop ernaar gekeken moet worden duidelijk is, maar vooral waarvan de benodigde informatie beschikbaar is. Begin met een beperkt aantal use cases en doe ervaring op. Dit is in Afbeelding 9 weergegeven door slechts drie use cases te selecteren uit de lijst van vijftien use cases.

3.6 Techniek binnen een SOC

Ook in een p-SOC is nog techniek aanwezig uit een r-SOC, zoals een SIEM of loginformatie vanuit security devices zoals firewalls, IDS, DLP, et cetera.
Gezien de steeds groter wordende hoeveelheid data (Big Data) en bedreigingen waarmee SOC's te maken krijgen, is verdere automatisering van de workload noodzakelijk. Denk aan technieken als 'Machine Learning'(ML), 'Artificial Intelligence'(AI) en 'Deep Learning'(DL). Meer mensen is in deze niet de oplossing. De stroom data zal namelijk alleen maar groeien en je kunt een team niet maar uit blijven breiden. Bovendien moet je dit niet willen, want niet- of weinig uitdagend werk dat kan worden geautomatiseerd, moet je niet door mensen laten doen. Een belangrijk aandachtspunt hierbij is wie controleert of geautomatiseerde

beslissingen en acties goed zijn en aan de regels voldoen? Wel vraagt Big Data om specifieke nieuwe specialisten en technieken op het gebied van data science. Een aanvulling op een wendbaar, modern SOC-team.

Een andere ontwikkeling die je ziet, is de opkomst van 'Threat & Security Intelligence'-technieken. Denk aan 'threat hunting' en 'red teaming'. Dit in lijn met de ontwikkeling van reactief naar proactief. Het is geen vervanging van monitoring, maar een aanvulling op. Waarbij het doel van 'threat hunting' is om nog onbekende dreigingen op te sporen. Het doel van 'red teaming' is niet alleen het aantonen van kwetsbaarheden in de infrastructuur of de menselijke factor in de organisatie. 'Red teaming' gaat verder door de dynamiek tussen aanvallers en verdediging (incident response team) te toetsen. 'Red teaming' is daarmee een volledige simulatie van een cyberaanval. Je ziet in deze een verschuiving van de traditionele pen-testen naar 'red teaming'. Advies is om dit 'red teaming' niet zelf te doen, maar hiervoor een externe partij te vragen. Dit voorkomt tunnelvisie.

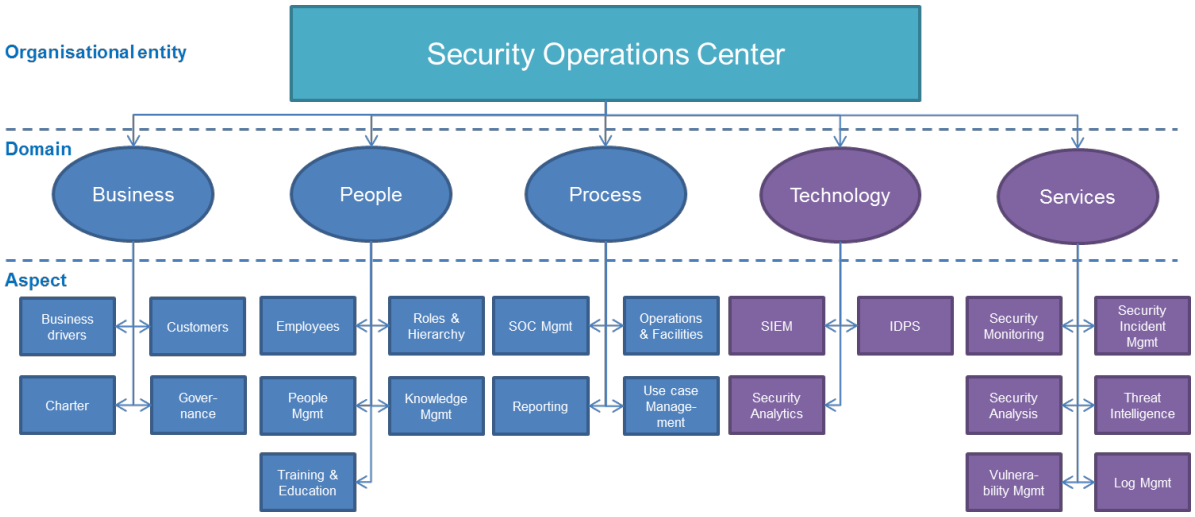
Wel kan een SOC natuurlijk ook zelf in een zogenoemde probeeromgeving allerlei scenario's testen. Zeker een manier om mensen gemotiveerd te houden. Als er weinig incidenten zijn, kun je gecontroleerd incidenten creëren om mensen scherp te houden. Maak hierbij zeker ook gebruik van bijvoorbeeld simulatietechnieken en -experts.

4. VOLWASSENHEID VAN EEN SOC

Wendbaarheid binnen een SOC met behoud van kwaliteit van de dienstverlening vraagt om een zeker mate van volwassenheid. Dit houdt in dat het SOC op een gecontroleerde manier functioneert en gestuurd wordt. Ook blijvende groei en mee kunnen bewegen met de nieuwste ontwikkelingen binnen cybersecurity, zowel op het gebied van dreigingen als technische ontwikkelingen, zijn onderdeel van volwassenheid.

Om het volwassenheidsniveau van een SOC te kunnen bepalen, is het noodzakelijk om met regelmaat metingen uit te voeren. Deze metingen stellen de organisatie in staat om zwakke plekken te identificeren, concrete vervolgstappen te bepalen en uiteindelijk ook de groei in volwassenheid aantoonbaar te maken.

Om deze metingen uit te kunnen voeren, is een model ontwikkeld dat kijkt naar een aantal cruciale elementen in de domeinen die in het voorgaande hoofdstuk zijn benoemd. Dit model heet het SOC-CMM en is losjes gebaseerd op het traditionele capability maturity model. Het belangrijkste verschil is dat dit model specifiek is voor SOC's en dat het een organische groei ondersteunt, in plaats van groei in gedefinieerde plateaus. Afbeelding 10 laat zien welke aspecten binnen dit model gemeten worden.



Afbeelding 10: SOC maturity elementen (Rob van Os).

In donkerblauw zijn de domeinen te zien waarin volwassenheid gemeten wordt; in paars zijn de domeinen te zien waarin zowel volwassenheid (maturity) als technische capaciteiten (capability) gemeten worden.

Het vaststellen van het niveau van volwassenheid en capaciteit kan binnen het SOC-CMM door het uitvoeren van een self-assessment. Een template voor deze assessment is vrijelijk verkrijgbaar op de site van het SOC-CMM (https://www.soc-cmm.com/). Met deze self-assessment, bij voorkeur in de vorm van een workshop, kan het SOC in de breedte en diepte worden bekeken. Het voordeel van een self-assessment is dat het eenvoudig en goedkoop uit te voeren is en snel een goed beeld geeft van het SOC, mits de juiste personen aangehaakt zijn bij de workshop. Het nadeel van dergelijk self-assessment is een bepaalde

vorm van subjectiviteit die kan optreden. Het is daarom goed om een onafhankelijke facilitator te hebben die scherp is op objectiviteit en zorgt dat iedereen tijdens de workshop voldoende input kan leveren. Dat kan iemand zijn van binnen de afdeling die zich inhoudelijk niet met de discussie bemoeit, iemand van buiten de afdeling, of iemand van buiten het bedrijf.

Met het afronden van de eerste volwassenheidsmeting (0-meting) wordt bepaald wat het startpunt is van het SOC. Van daaruit kan een groeipad gerealiseerd worden dat past bij het ambitieniveau van het SOC en de context van de organisatie. Het is van belang om de beoogde groei op een gecontroleerde manier te laten verlopen. De aandacht van het SOC moet daarbij gebalanceerd verdeeld worden tussen het blijven draaien van de operatie en het zorgdragen voor innovatie en groei in volwassenheid. Dat betekent dat keuzes gemaakt moeten worden (focus). Het is daarbij gangbaar dat allereerst geïnvesteerd wordt in elementen die het SOC als meest belangrijke ervaart en elementen die het meest achterlopen qua volwassenheid of mogelijk zelfs nog volledig ontbreken. Door de metingen met regelmaat te herhalen kan vast worden gesteld of de gestelde doelen ook bereikt zijn, of dat je op het juiste pad bent. Het is daarom belangrijk om deze doelen na de 0-meting concreet te maken.

Als laatste is het belangrijk om de groei in volwassenheid zo in te richten dat wendbaarheid centraal blijft staan. Het risico bestaat dat door een rigide houding ten opzichte van volwassenheid, vooral op het gebied van regeldruk ten aanzien van het SOC, de wendbaarheid verloren kan gaan. Op de langere termijn kan dit in de weg komen staan van verdere groei en ontwikkeling.

5. TRENDS & ONTWIKKELINGEN

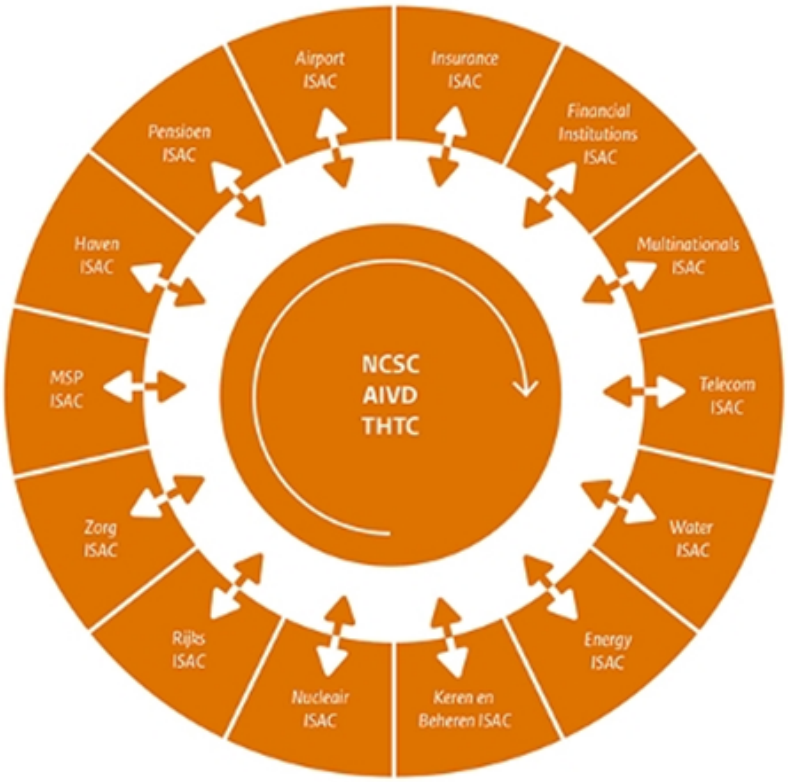
De belangrijkste trends in het kader van de ontwikkeling van een r-SOC naar een p-SOC hebben we reeds benoemd.

- Van reactief naar proactief.
- Van het opsporen van louter bekende dreigingen (r-SOC) naar het tevens zoeken naar onbekende dreigingen (p-SOC). Denk bijv. aan opkomst van threat-hunting.
- Nieuwe methoden als ML (Machine Learning), AI (Artificial Intelligence) en DL(Deep Learning) krijgen hun introductie. Dit nu steeds meer vormen van informatie naar het SOC worden gebracht. Een ontwikkeling die ook goed past in de doelstelling om als SOC steeds meer waarde voor de business te creëren.

Daarbij zie je de ontwikkeling dat een SOC steeds meer bottom-up in plaats van top-down is gestructureerd. Dit hangt samen met de ontwikkeling van reactief naar proactief. Dit betekent dat een SOC juist zelf speerpunten op de agenda zet. Dit vraagt om meer creatieve geesten met gevoel voor de business binnen een team. Creatievelingen die het beste tot hun recht komen in een bottom-up structuur, ook wel team-based structuur genoemd. De rol van de SOC-manager in deze is de balans in zijn team te bewaken om zo het beste uit zijn team te halen.

Een andere belangrijke trend die de deskundigen zien, is de noodzaak tot samenwerken. De kans dat een bepaalde bedreiging ergens anders niet al eerder is gezien, is niet zo heel groot. Je moet het echter wel van elkaar weten. Daarom zijn publiek-private samenwerkingsverbanden zoals bijvoorbeeld ISAC's, Information Sharing and Analysis Centres, zo belangrijk.
Samenwerkingsverbanden waarbinnen deelnemers onderling informatie en ervaringen uitwisselen over cybersecurity. Ook worden analyses gedeeld, met name op tactisch niveau.

We kennen in Nederland de volgende ISAC's:



Afbeelding 11: De bestaande ISAC's (Bron: https://www.ncsc.nl/samenwerking/isacs.html)

Opvallende ontwikkelingen uit het Cybersecuritybeeld Nederland 2016 (http://www.ncsc.nl) die we hier tot slot willen noemen zijn:
(Het rapport werd begin september 2016 gepresenteerd door het NCSC)

- Beroepscriminelen voeren langdurige, hoogwaardige en geavanceerde operaties uit.
- Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk.
- Ransomware is gemeengoed en is nog geavanceerder geworden.
- Advertentienetwerken zijn nog niet in staat gebleken malvertising het hoofd te bieden.

Bevindingen die door staatssecretaris Klaas Dijkhoff van Justitie bij de presentatie van het rapport als 'zorgelijk' werden getypeerd. Reden voor hem om extra in te zetten op 'digitale dijkbewaking', het Nationaal Detectie Netwerk waarmee overheid en bedrijven elkaar informeren over actuele dreigingen.
Bron: www.ncsc.nl

6. REFLECTIE

Concluderend kun je stellen dat binnen een modern p-SOC in tegenstelling tot een traditioneel r-SOC niet meer de techniek, maar de mens leidend is. Een modern p-SOC is niet langer een opeenstapeling van technische oplossingen en een SOC anno 2017 staat zeker niet meer gelijk aan een SIEM.
De menselijke factor is bepalend voor het succesvol zijn van een modern p-SOC. En dit succes wordt uiteindelijk bepaald door het al dan niet mee kunnen bewegen met de in sneltreinvaart veranderende samenleving om ons heen. Het is de mens die aan moet geven waar prioriteiten liggen. En het is uiteindelijk de mens die bepaalt of een alarm wel of niet opgevolgd moet worden. Dit op basis van de context van een alarm.

Natuurlijk moeten we ervoor zorg dat saai, repetitief werk waar mogelijk wordt geautomatiseerd. Maar uiteindelijk leren de systemen van de ‘rockstar-analist’. Ook is het is deze analist die controleert of de geautomatiseerde activiteiten de juiste werking hebben.

Deze rockstar-analisten vinden, blijft een probleem. Deskundigen blijven daarom hameren op de noodzaak van (interne) opleiding. Dit zeker gezien het snel veranderende speelveld waarin een SOC acteert. Vaak logge onderwijsinstituten kunnen moeilijk inspelen op deze snelle veranderingen. Interne opleiding is daarom cruciaal. Dit ook om je mensen gemotiveerd te houden.

7. HOE VERDER?

Ontwikkelingen als Machine Learning, Artificial Intelligence, IoT, Data Science en bijvoorbeeld Automorphing ter ondersteuning van automated defence zullen steeds verder gaan. Hier moet je als modern wendbaar p-SOC op voorbereid zijn. Datzelfde geldt voor de steeds verdere professionalisering van tegenstanders. De p-SOC is dan ook allesbehalve een eindpunt. Wendbaarheid in combinatie met mensenwerk blijven wat ons betreft de key-woorden. Ook wanneer we binnen afzienbare tijd zonder twijfel verder ontwikkelen naar een tactical SOC, een t-SOC.

Kenmerken van een t-SOC:

- t-SOC schuift verder op naar een proactieve en voorspellende focus aangevuld met radicaal geautomatiseerde response.
- t-SOC gaat verder dan alleen de traditionele infrastructuur logging, maar gebruikt Big Data oplossingen om in het diverse applicatielandschap effectieve monitoring te kunnen toepassen.
- t-SOC is in staat om threat hunting uit te voeren in een extreem dynamische omgeving; initieel gevoed door mode 2 IT en later waarschijnlijk ook door automated defence.
- t-SOC leunt op een hybride team van medewerkers dat infrastructurele, applicatieve, security, Big Data expertises en de business belangen bij elkaar brengt.
- Zeer operationele en herhaalbare taken worden steeds verder geautomatiseerd. De vraag is dan ook of het t-SOC nog wel een ‘operationele’ entiteit is. Het is waarschijnlijker dat het SOC die rol ontstijgt en een meer tactische rol binnen de organisatie gaat vervullen. Threat management en SA (beiden gedreven door threat intelligence) zullen hierbij centraal staan.

Conclusie / takeaways

- Het succes van een modern p-SOC wordt bepaald door de juiste mensen. Een modern wendbaar SOC is namelijk bij uitstek mensenwerk. Het is en blijft immers de mens die uiteindelijk besluit een alarm op te volgen. Daarbij is het aan de mens, ondersteund door allerhande techniek, om de bredere context van een alarm te zien. En het is uiteindelijk de mens die controleert of de geautomatiseerde activiteiten de juiste werking hebben.

- Een modern p-SOC is bij uitstek dynamisch. De mate van wendbaarheid in een continu veranderende omgeving bepaalt de kracht van zo’n SOC. Juist met deze factor wendbaarheid moet je bij de keuze voor je mensen binnen een SOC rekening houden. Zorg voor een combinatie van ‘blauwe’ en ‘gele’ mensen die infrastructurele, applicatieve, security, Big Data expertises en business belangen bij elkaar brengen.

- Om deze mensen geboeid te houden, SOC-werk kan in sommige gevallen saai worden, is het essentieel voldoende aandacht te hebben voor het bieden van uitdagingen. Goed people management is hierbij essentieel. Houd er hierbij rekening mee dat gezond verloop goed is. Nieuwe mensen bieden immers frisse, nieuwe inzichten. Onthoud daarbij dat oude collega's in de business ambassadeurs kunnen zijn voor het SOC en vice versa.

- Belangrijk bij het vaststellen van de doelstellingen en ambities van een modern p-SOC is het besef dat je binnen een SOC niet alles kunt doen. Focus in het bepalen van je Incident en Response capabilities is daarom essentieel. Zorg hierbij continu voor afstemming met de business. Er is namelijk geen 'one size fits all'. Kies er ook daarom voor om binnen je organisatie vice versa te zorgen voor ambassadeurs. Mensen die vanuit het SOC een rol krijgen in de business en andersom. Om zo wederzijds begrip en draagvlak te creëren.

BIJLAGE 1: LITERATUURLIJST

De expertgroep beveelt ter aanvulling of ter verdieping van de behandelde onderwerpen de volgende literatuur aan:

Titel	#pagina's	Relevante pagina's	Bestandsnaam	Auteur
Ten Strategies of a World-Class Cybersecurity Operations Center	346	vii (Inhoudsopgave)	01-pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf	MITRE
Ten Strategies of a World-Class Cybersecurity Operations Center	346	81-85		
Cyber Resiliency Engineering Framework	78	Hoofdstukken 3 en 4	02-MITRE-Cyber resilience engineering framework.pdf	MITRE
Cyber security information exchange to gain insight into the effects of cyber threats and incidents	9	Compleet artikel (in ieder geval impact stuk)	03-Artikel - Springer Cyber information exchange to gain insights.pdf	Fransen, Kerkdijk, Smulders
SOC Expertbrief	10	Alle	ExpertBrief - SOC V1.0 definitief.pdf	vorige groep
SOC aantekeningen Ben, kelvin, Renato Andre			Werkdocument SOC XP brief 20140901.doc	Ben, Andre, Kelvin en Renato
On SecOps Maturity	8	Totale paper	Seculior - On-SecOps-Maturity-June-2016.pdf	Wilco van Ginkel
The Next SecOps Fundamentals	8	Totale paper	Seculior - The-Next-SecOps-Fundamentals.pdf	Wilco van Ginkel
Security operations services (rabobank)	2	Beide sheets	Security Operations Services - tbv XP brief SOC.ppt	Kelvin Rorive
SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers				Rob van Os

BIJLAGE 2. INFORMATIE OVER DE DEELNEMERS

Onderstaande deelnemers hebben bijgedragen aan deze expertbrief. Mocht u met een van hen contact willen opnemen dan kan dat via het secretariaat van het PvIB, zie http://www.pvib.nl/contact.

Renato Kuiper

Is security architect bij Verdonck, Klooster en Associates, en richt zich op het snijvlak van informatiebeveiliging, risicomanagement en architectuur. Vanuit die invalshoeken heeft hij veel ervaring opgedaan met Security Operations Centers.

Sandra Kagie

Is freelance tekstschrijver/journalist. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging', het magazine van het PvIB. www.sanscriptproducties.nl / Twitter @SanSanscript.

Kelvin Rorive

Is binnen het Cyber Defence Centre van Rabobank als manager verantwoordelijk met een internationaal team voor global IT threat management, security monitoring en Incident response. Kelvin is daarnaast voorzitter van de activiteitencommissie van het PvIB.

Charlotte Rugers

Is sr. innovation manager bij het Ministerie van Defensie. In het verleden heeft zij gewerkt als plaatsvervangend security officer binnen een SOC.

Andre Smulders

Is Strategisch Adviseur Cyber Security en werkt bij TNO aan security innovaties voor opdrachtgevers uit het private en publieke domein. Daarnaast is hij co-auteur van het boek 'Foundations of Information Security – based on the ISO27001 and 27002'.

Ben van Zuijlen

Is manager van de afdeling Control & Security Center bij de Volksbank en eindverantwoordelijk voor de Security Operations Center-activiteiten. Daarnaast is hij vicevoorzitter van de FI-ISAC.

Rob van Os

Is cyber defense specialist bij de Volksbank en operationeel verantwoordelijk voor het draaien van een Security Operations Center en groei in volwassenheid. Vanuit zijn consultancy rol heeft hij in het verleden veel ervaring opgedaan met SOC-processen en inrichting. Rob is tevens de auteur van het SOC-CMM.

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by/3.0/nl/

Deze pagina ziet er op het moment van schrijven als volgt uit:

28

WORD LID VAN HET PVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN…

Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. Of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Platform voor Informatiebeveiliging kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Platform voor Informatiebeveiliging?
Het PvIB is een open, breed samengesteld platform waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het PvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en IT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

https://www.pvib.nl/abonnementsinformatie