



Rijksoverheid

Joint SOC Best Practice



Datum : Dinsdag 23 december 2025

Versie : 3.1

Status : Definitief

TLP : **TLP: CLEAR**



Colofon

Contactpersoon: J-SOC / info@jsoc.nl

Auteurs :	Rob van Os	Argos CSA
	Karl Lovink	Belastingdienst
	Michiel Moermans	DICTU
	Martijn Peijer	DICTU
	Matthijs Goofers	Rijkswaterstaat
	Mark van Uffelen	SSC-ICT
	Paul van de Luitgaarden	MinJenV
	Geert Wijers	DUO
	Willem Katoen	MinDef



Inhoudsopgave

DOCUMENTEIGENSCHAPPEN	6
DOCUMENTHISTORIE	6
AUTEURS	6
GOEDKEURDERS	6
REVIEWERS.....	6
1 MANAGEMENTSAMENVATTING.....	7
2 INLEIDING	8
2.1 ACHTERGROND.....	8
2.2 DEFINITIE	8
2.3 UITGANGSPUNTEN	8
2.4 DOELSTELLINGEN BEST PRACTICE	8
2.5 DOELGROEP	9
2.6 STRUCTUUR VAN HET DOCUMENT.....	9
3 SECURITY FUNDAMENT	10
3.1 SOC-FUNCTIE BINNEN DE ORGANISATIE	11
3.2 SECURITY FUNDAMENT VOOR HET SOC	11
4 J-SOC BEST PRACTICE	12
5 BUSINESS DOMEIN	13
5.1 BUSINESS DRIVERS.....	13
5.2 DIENSTAFNEMERS EN BELANGHEBBENDEN	14
5.3 CHARTER.....	15
5.4 GOVERNANCE	16
5.4.1 Organisatorische positionering van het SOC.....	16
5.4.2 Verschijningsvormen.....	17
5.4.3 Relatie tot andere security entiteiten	18
5.4.4 Governance meetings	18
5.4.5 Kostenbeheersing.....	19
5.4.6 Gebruikte frameworks en Best Practices	20
5.5 PRIVACY, BELEID, WETGEVING EN JURIDISCHE KADERS	21
5.5.1 Privacy.....	21
5.5.2 Beleid	21
5.5.3 Wetgeving en Juridische kaders.....	23
6 PEOPLE DOMEIN	24
6.1 MEDEWERKERS	24
6.1.1 Aantrekken talent	24
6.1.2 Behouden talent.....	24
6.1.3 Veilige werkomgeving.....	24
6.2 ROLLEN EN HIËRARCHIE	25
6.2.1 Teamstructuur	25
6.2.2 Rollen	27
6.2.3 Tiers.....	30
6.3 PEOPLEMANAGEMENT	35
6.4 KENNISMANAGEMENT.....	37
6.5 TRAINING EN CERTIFICERING.....	38
7 PROCESS DOMEIN	40
7.1 SOC-MANAGEMENT.....	40
7.1.1 Continuous improvement.....	41
7.1.2 Quality assurance	42



7.2	SOC-OPERATIONS EN FACILITEITEN	43
7.2.1	<i>Openingstijden en bereikbaarheid</i>	43
7.2.2	<i>Standaardisering</i>	45
7.2.3	<i>Oefeningen</i>	45
7.2.4	<i>SOC Operations - Faciliteiten</i>	46
7.3	RAPPORTAGE EN COMMUNICATIE	46
7.3.1	<i>Metrics</i>	47
7.3.2	<i>Communicatie</i>	47
7.4	USE CASE MANAGEMENT	48
7.4.1	<i>MITRE ATT&CK toepassing</i>	49
7.4.2	<i>RACI</i>	50
7.5	DETECTION ENGINEERING	51
7.5.1	<i>Detectie validatie</i>	51
7.6	AUTOMATION ENGINEERING	52
8	TECHNOLOGY DOMEIN	54
8.1	SIEM	56
8.1.1	<i>Eigenaarschap</i>	56
8.1.2	<i>Beheer en onderhoud</i>	56
8.1.3	<i>Data retentie</i>	57
8.1.4	<i>RACI</i>	57
8.2	EDR	57
8.2.1	<i>Eigenaarschap</i>	57
8.2.2	<i>Data retentie</i>	58
8.2.3	<i>Beheer en onderhoud</i>	58
8.2.4	<i>RACI</i>	58
8.3	NDR	58
8.3.1	<i>Eigenaarschap</i>	59
8.3.2	<i>Beheer en onderhoud</i>	59
8.3.3	<i>Data retentie</i>	59
8.3.4	<i>RACI</i>	59
8.4	SOAR	59
8.4.1	<i>Eigenaarschap</i>	60
8.4.2	<i>Beheer en onderhoud</i>	60
8.4.3	<i>RACI</i>	60
8.5	OVERIGE TECHNOLOGIE	60
8.6	TOEKOMSTIGE TECHNOLOGIE	61
8.7	BEST PRACTICES VOOR HET TECHNOLOGY DOMEIN	62
9	SERVICE DOMEIN	63
9.1	SERVICE ARCHITECTUUR	63
9.1.1	<i>Servicelevels en KPI's</i>	64
9.1.2	<i>Service RACI</i>	64
9.1.3	<i>Service onboarding</i>	65
9.1.4	<i>Procesarchitectuur</i>	65
9.1.5	<i>Best Practices voor security monitoring</i>	66
9.2	SECURITY INCIDENT MANAGEMENT	67
9.2.1	<i>Servicelevels en KPI's</i>	67
9.2.2	<i>Service RACI</i>	67
9.2.3	<i>Service onboarding</i>	67
9.2.4	<i>Procesarchitectuur</i>	68
9.2.5	<i>Best Practices voor security incident management</i>	68
9.3	SECURITY ANALYSIS & FORENSICS	71
9.3.1	<i>Servicelevels en KPI's</i>	71
9.3.2	<i>Service RACI</i>	72
9.3.3	<i>Service onboarding</i>	72



9.3.4	Procesarchitectuur	72
9.3.5	Best Practices voor security analysis & forensics	72
9.4	CYBER THREAT INTELLIGENCE	73
9.4.1	Servicelevels en KPI's	75
9.4.2	Service onboarding	75
9.4.3	Service RACI	75
9.4.4	Procesarchitectuur	75
9.4.5	Best Practices voor threat intelligence	76
9.5	THREAT HUNTING	76
9.5.1	Servicelevels en KPI's	77
9.5.2	Service onboarding	77
9.5.3	Service RACI	77
9.5.4	Procesarchitectuur	78
9.5.5	Best Practices voor threat hunting	78
9.6	VULNERABILITY MANAGEMENT	78
9.6.1	Servicelevels en KPI's	79
9.6.2	Service onboarding	79
9.6.3	Service RACI	79
9.6.4	Procesarchitectuur	80
9.6.5	Overige activiteiten	80
9.6.6	Best Practices voor vulnerability management	81
9.7	OVERIGE SOC-DIENSTEN	82
10	CONCLUSIE	83
	ANNEX A: LIJST MET GEBRUIKTE TERMEN EN AFKORTINGEN	84
	ANNEX B: NIST CSF MAPPING	85
	ANNEX C: TRAININGSPLAN	87
C.1	OPLEIDINGSPLAN	88
C.2	LEERLIJN	89
C2.1	Tier 1 – Security Analyst	89
C2.2	Doorgroei binnen de functie (van tier 1 -> tier 2)	90
C2.3	Tier 2 Security Analyst	91
C2.4	Doorgroei binnen de functie (van tier 2 -> tier 3)	92
	ANNEX D - JURIDISCHE KADERS	93



Documentgegevens

Documenteigenschappen

Filenaam	Joint SOC Best Practice v3.1
Laatste wijziging	dinsdag 23 december 2025
Aantal pagina's	94
Huidige status	Definitief
Versienummer	3.1
Revisiefrequentie	Jaarlijks
TLP	TLP: CLEAR

Documenthistorie

Versie	Status	Datum	Omschrijving
2.1	Concept	12-03-2024	Document kapstok ter verificatie
2.2	Concept	21-08-2024	Volledig document uitgeschreven ter review
2.97	Concept	14-02-2025	Commentaar 2 interne review sessies verwerkt
2.98	Review	01-09-2025	Review verwerkt J-SOC
2.99	Review	20-09-2025	Review versie t.b.v. RijksISAC
3.0	Definitief	15-12-2025	
3.1	Definitief	23-12-2025	Interne links naar intranet verwijderd en TLP: AMBER+STRICT gewijzigd naar TLP: CLEAR in bijlagen.

Auteurs

Naam	Organisatie
Rob van Os	Argos CSA (extern)
Karl Lovink	Belastingdienst
Michiel Moermans	DICTU
Martijn Peijer	DICTU
Matthijs Goofers	Rijkswaterstaat
Mark van Uffelen	SSC-ICT
Paul van de Luitgaarden	MinJenV
Geert Weijers	DUO
Willem Katoen	MinDef

Goedkeurders

Naam	Functie	Organisatie
Jan Willem Beunk	Manager SOC	Belastingdienst
Mark van Uffelen	Manager SOC	SSC-ICT
Milo Mooij	Manager SOC	Rijkswaterstaat
Martijn Peijer	CTI Coördinator & Programmamanager SOC doorontwikkeling	DICTU
Paul van de Luitgaarden	Manager SOC	MinJenV
Erik Douwes	Manager SOC	DUO
Sander Mallon	Manager DCSC	MinDef

Reviewers

Naam	Functie	Organisatieonderdeel
		VSSR
		RijksISAC



1 Managementsamenvatting

Dit document is bedoeld als Best Practice voor de inrichting en uitvoering van een Security Operations Center binnen het Joint SOC samenwerkingsverband. Het document kan zowel gebruikt worden als leidraad voor het inrichten van een SOC, als het verbeteren van bestaande security operations. Ook kan het document ter inspiratie dienen voor organisaties die geen deelnemer van het J-SOC zijn. Tenslotte kan het document ook gebruikt worden om regie te voeren op uitbestede SOC-dienstverlening.

Het document is gestructureerd conform het SOC Capability Maturity Model (SOC-CMM). Het SOC-CMM is een de facto standaard voor volwassenheidsbepaling in security operations en beschrijft het SOC in 5 domeinen (Business, People, Process, Technology en Services) en daaronder gepositioneerde 26 aspecten.

2 Inleiding

2.1 Achtergrond

Deze Best Practice is een vernieuwing van de bestaande Best Practice binnen het Joint SOC. De Best Practice is bedoeld als algemeen document met praktische richtlijnen voor het inrichten van Security Operations Centers. Het document wordt binnen de J-SOC leden gebruikt als basis voor hun security operations activiteiten.

2.2 Definitie

Binnen de Best Practice wordt de volgende definitie voor een SOC gehanteerd:

"Een Security Operations Center is een gecentraliseerde functie binnen een organisatie die mensen, processen en techniek inzet om de cyberweerbaarheid te verhogen middels detectie, analyse en respons op cybersecurity incidenten."

Binnen dit document wordt uitsluitend de term 'SOC' of de volledig uitgeschreven vorm daarvan gebruikt. Andere termen die in het vakgebied gebruikt worden, zoals Cyber SOC en Cyber Defense Center, vallen ook onder deze term.

2.3 Uitgangspunten

De volgende uitgangspunten zijn meegenomen in het opstellen van deze Best Practice:

- Het SOC-CMM is gebruikt als basis voor het structureren van het document. Waar nodig zijn enkele uitzonderingen gemaakt om deze structuur passend te maken voor het doel van de Best Practice.
- Binnen de Best Practice wordt zoveel mogelijk gerefereerd aan open standaarden op het gebied van security operations.
- De Best Practice is op basis van een generalisering voor security operations. Elke aangesloten SOC bij het J-SOC zal een eigen uitwerking van de Best Practice moeten maken om de inrichting aan te laten sluiten bij de eigen organisatie.
- SOC-processen en technologie sluiten zoveel mogelijk aan op bestaande processen. Alleen daar waar processen niet bestaan of niet voldoende aansluiten op de behoeftes van het SOC worden eigen processen ingericht.

2.4 Doelstellingen Best Practice

De doelstellingen van de Best Practice zijn de volgende:

- Om kennis en kunde van de J-SOC leden te bundelen en beschikbaar te maken voor alle leden van het J-SOC en daarbuiten;
- Om gebruikt te kunnen worden als basis voor inrichting en operatie van een SOC, zowel binnen het J-SOC als daarbuiten;
- Om uniformiteit van de inrichting en uitvoering van security operations binnen de J-SOC leden te ondersteunen;
- Om te dienen als strategisch naslagwerk voor het SOC.

Dit document is expliciet geen visiedocument, maar een document gebaseerd op bestaande en bewezen toepassingen binnen het SOC.



2.5

Doelgroep

Dit document is bedoeld voor de volgende doelgroep:

- SOC Managers die hun SOC willen inrichten en draaien op een wijze die gebaseerd is op standaarden en Best Practices;
- SOC-analisten, engineers en andere operationele medewerkers die meer beeld willen krijgen bij het SOC in de bredere context;
- CISO's die meer kennis willen nemen van security operations, zowel op operationeel als tactisch en strategisch niveau;
- SOC-adviseurs, die SOC-inrichting en volwassenheids groei op basis van Best Practices conform het SOC-CMM willen uitdragen.

2.6

Structuur van het document

Dit document is als volgt gestructureerd:

- Hoofdstuk 3 beschrijft het fundament voor security operations. Dit is de basis die nodig is voor het inrichting en succesvolle operatie van een SOC;
- Hoofdstuk 4 is de introductie voor de Best Practice. In dit hoofdstuk worden de elementen en domeinen van het SOC-CMM kort toegelicht;
- Hoofdstukken 5 t/m 9 beschrijven de daadwerkelijke Best Practice en geven een concrete uitwerking van alle aspecten binnen de 5 domeinen van het SOC-CMM;

Hiernaast bevat het document nog vier annexen, te weten een lijst met gebruikte termen en afkortingen, een mapping tussen NIST CSF en de Best Practice, een trainingsplan en de juridische kaders.



3 Security fundament

Het SOC levert security capabilities aan de organisatie in de vorm van diensten en ondersteunt daarmee de cyberweerbaarheid. Deze security capabilities moeten gezien worden in een bredere aanpak van cyber security. Voor deze bredere aanpak wordt in deze Best Practice het [NIST Cyber Security Framework \(CSF\) 2.0](#) gehanteerd. Dit model bestaat uit 6 fasen: govern, identify, protect, detect, respond en recover en in totaal 22 elementen.

De elementen uit het NIST CSF raamwerk zijn onderdelen van de bredere cybersecuritystrategie. Bij een aantal van deze elementen speelt het SOC een belangrijke rol in de realisatie. Bij andere elementen is de rol van het SOC beperkt of is er helemaal geen rol. Onderstaande overzicht geeft als voorbeeld inzicht in de rol van het SOC in de verschillende elementen van het NIST CSF. Dit kan uiteraard per SOC anders zijn. Daarbij is te zien dat het zwaartepunt van SOC-activiteiten te vinden is in de Detect en Respond fasen.

Functie	Categorie	Categorie ID	Rol van het SOC
Govern (GV)	Organizational Context	GV.OC	Gemiddeld
	Risk Management Strategy	GV.RM	Klein
	Roles, Responsibilities, and Authorities	GV.RR	Gemiddeld
	Policy	GV.PO	Klein
	Oversight	GV.OV	Klein
	Cybersecurity Supply Chain Risk Management	GV.SC	Klein
Identify (ID)	Asset Management	ID.AM	Klein
	Risk Assessment	ID.RA	Gemiddeld
	Improvement	ID.IM	Gemiddeld
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA	Klein
	Awareness and Training	PR.AT	Klein
	Data Security	PR.DS	Gemiddeld
	Platform Security	PR.PS	Klein
	Technology Infrastructure Resilience	PR.IR	Gemiddeld
Detect (DE)	Continuous Monitoring	DE.CM	Groot
	Adverse Event Analysis	DE.AE	Groot
Respond (RS)	Incident Management	RS.MA	Groot
	Incident Analysis	RS.AN	Groot
	Incident Response Reporting and Communication	RS.CO	Groot
	Incident Mitigation	RS.MI	Groot
Recover (RC)	Incident Recovery Plan Execution	RC.RP	Klein
	Incident Recovery Communication	RC.CO	Klein

Een meer gedetailleerde koppeling tussen het NIST CSF en de elementen uit de Best Practice wordt in Annex B getoond.

3.1 SOC-functie binnen de organisatie

Het SOC geeft uitvoering aan een deel van het securitybeleid en is daarmee een belangrijke interne speler voor security. Het SOC is echter geen eigenaar van operationele security binnen een organisatie. Alle operationele teams zijn verantwoordelijk voor de beveiliging van hun eigen systemen en applicaties. Het *security by design* principe is daarbij leidend. Het SOC houdt het centrale beeld, monitort, en rapporteert.

Het is van belang om de andere spelers op het gebied van security binnen de organisatie te identificeren. Daarbij is het belangrijk om de rol van deze spelers te onderkennen, en ook vast te stellen welke interfaces en/of afhankelijkheden er bestaan ten aanzien van deze spelers.

Tenslotte is het ook van belang om goed af te kaderen welke verantwoordelijkheden waar liggen. Een RACI-tabel is daarbij een handig middel. In een dergelijke tabel staat aangegeven:

- **R: responsible.** De entiteit die verantwoordelijk is voor de taak
- **A: accountable.** De entiteit die eindverantwoordelijk is voor de taak
- **C: consulted.** De entiteit waar advies ingewonnen kan worden over de taak
- **I: informed.** De entiteit die geïnformeerd wordt over de taak

3.2 Security fundament voor het SOC

Het goed functioneren van het SOC is afhankelijk van het goed functioneren van de bredere securitystrategie. Het is daarom belangrijk dat er al een securitybasis aanwezig is voordat een organisatie een SOC gaat inrichten. Een dergelijk fundament kan bijvoorbeeld bestaan uit:

- **Kennis van de assets die in het netwerk staan.** Om monitoring uit te kunnen voeren is het allereerst noodzakelijk dat in kaart is welke systemen er bestaan binnen de IT/OT omgeving en wie hiervan de eigenaar is. Het SOC kan nieuwe assets identificeren, maar heeft een basis nodig om vanuit te werken.
- **Informatiebeveiligingsbeleid.** Informatiebeveiligingsbeleid is ondersteunend voor SOC-werkzaamheden. In het business domein wordt verder ingegaan op de beleidstukken die noodzakelijk zijn voor het SOC om goed te kunnen functioneren.
- **Een Information Security Management Systeem (ISMS).** Een ISMS is het fundament voor organisatie en continue verbetering van de informatiebeveiliging strategie, hierin is onder andere vastgelegd welke maatregelen worden afgedekt met een SOC.
- **Security configuratie van de IT/OT componenten (hardening baseline).** De operationele toepassing van beleid in de systemen is geen verantwoordelijkheid van het SOC. Het SOC kan wel ondersteunen in het opstellen van hardening baselines en kan de correcte implementatie van de baseline controleren met behulp van specifieke tooling.
- **Basis IT Processen.** Tot deze processen behoren een log managementproces, incident managementproces en asset managementproces. Het SOC kan alleen effectief opereren als deze processen reeds zijn vormgegeven.
- **Aansluiting op leveranciers.** Leveranciers vormen een integraal onderdeel van het volledige IT-landschap binnen organisatie. Het is belangrijk om afspraken te maken met deze leveranciers over security in het bijzonder over escalaties en samenwerking bij security incident respons.

Een SOC kan helpen om het bestaande security fundament verder te versterken, maar heeft wel een fundament nodig om effectief te kunnen zijn. Het bouwen van een SOC kan daarom nooit de eerste stap zijn in het toepassen van een securitystrategie.

De J-SOC Best Practice is opgezet conform de structuur van het SOC-CMM; een standaard voor het doormeten van volwassenheid en capability binnen een SOC. Deze standaard wordt gebruikt door alle leden van het Joint SOC (J-SOC), een samenwerkingsverband tussen verschillende SOC's binnen de Rijksoverheid.

Het SOC-CMM kent een aantal assen (domeinen) waarlangs de inrichting en operatie van een SOC vormgegeven kan worden. Elk van de domeinen bevat vervolgens een aantal aspecten. De volgende domeinen zijn onderdeel van deze Best Practice:

- **Business domein.** In het business domein ligt de focus op de aansluiting van het SOC bij de bedrijfsvoering, het begrip van de afnemers/belanghebbenden van het SOC, de manier waarop governance ingevuld wordt voor het SOC. Tenslotte komen ook zaken als beleid en privacy binnen het SOC aan bod.
- **People domein.** Het people domein gaat in op een aantal aspecten rondom de bemensing van het SOC. Dat betreft onder andere capaciteit en het aantrekken en behouden van talent, maar ook de manier waarop structuur gegeven wordt aan het SOC-team en hoe zaken als kennismanagement en training en certificering vormgegeven zijn.
- **Process domein.** Het process domein beschrijft een aantal algemene, intern gerichte of overkoepelende processen die van toepassing zijn binnen het SOC. Tot deze processen horen het SOC-managementproces, de reguliere SOC-operatie, rapportages en zaken als Use Case Management en detection & Automation Engineering.
- **Technology domein.** Het technology domein richt zich op de kerntechnologieën zoals gedefinieerd in het SOC-CMM, aangevuld met overige technologieën die toegepast worden in het organisatie SOC.
- **Service domein.** Het service domein beschrijft de diensten van het SOC. Dit zijn naar buiten gerichte processen van het SOC waar duidelijke afnemers en gedefinieerde interacties voor zijn. Het service domein in deze Best Practice is in meerdere delen opgesplitst en benoemt ook diensten die niet door het SOC geleverd worden, maar die wel aansluiten op SOC-diensten.

Elk van de domeinen wordt hierna in een separaat hoofdstuk uitgewerkt.

5 Business domein

Het business domein van het SOC-CMM beschrijft op welke manier het SOC in lijn is gebracht met de business van de organisatie. De praktijk leert dat Security Operations Centers vaak voornamelijk IT-gericht zijn, en daardoor vaak ook onvoldoende aansluiten bij de wensen van de business. Binnen dit domein is een aantal aspecten te vinden wat zorgdraagt voor goede aansluiting op de business, het behoud van deze aansluiting, en de kaders die gelden binnen de organisatie.

De volgende elementen van het business domein worden hierna uitgewerkt:

- Business drivers
- Dienstafnemers en belanghebbenden
- Charter
- Governance
- Privacy, beleid, wetgeving en juridische kaders

Elk van deze onderwerpen wordt hierna in detail toegelicht.

5.1 Business drivers

Business drivers beschrijven de aansluiting van het SOC op de bedrijfsvoering van de organisatie. Primair daarbij is de aansluiting van het SOC op de informatiestrategie.

Business waarde komt met name voort uit de aansluiting van het SOC op de strategische doelen. Een goed functionerend SOC ondersteunt en versterkt de cyberweerbaarheid van de organisatie, en voegt daarmee waarde toe aan de bedrijfsvoering. Deze waarde vertaalt zich vooral naar het borgen van de continuïteit en betrouwbaarheid van de organisatie.

Voorbeelden van mogelijk interessante business drivers:

- **Risicoreductie.** De diensten van het SOC omvatten een set aan mitigerende maatregelen om cyber risico's binnen de organisatie terug te dringen.
- **Versterken van de cyber weerbaarheid.** Met de diensten van het SOC kan de weerbaarheid van de organisatie tegen cyberaanvallen in kaart gebracht worden. Deze informatie kan gebruikt worden om deze weerbaarheid vervolgens te versterken.
- **Compliance.** Het hebben van een Security Operations Center kan nodig zijn om te voldoen aan wet- en regelgeving; in het geval van de Rijksoverheid is dat de BIO. Tevens kan het SOC ook optreden om interne compliance (voldoen aan intern beleid) te ondersteunen door het identificeren van gedragingen die afwijken van beleid (insider threat).

Best Practices voor inrichting

Tijdens de inrichting van het SOC is het met name belangrijk om in kaart te brengen op welke manier het SOC-waarde toevoegt aan de organisatie en hoe het SOC het beste kan aansluiten bij de bedrijfsvoering. Dat is geen IT-vraagstuk, maar een vraagstuk wat beantwoord wordt door relevante belanghebbenden uit de bedrijfsvoering. Een CISO kan hier ook een belangrijke rol in spelen, als vertegenwoordiger van de bedrijfsvoering. Het is tevens van belang dat de inrichting van het SOC rekening wordt gehouden met de andere verantwoordelijken voor security binnen de organisatie. Het moet duidelijk zijn welke verantwoordelijkheden waar liggen.

Best Practices voor uitvoering

Voor de uitvoering is het met name van belang om de aansluiting van het SOC op de bedrijfsvoering in stand te houden. Daarvoor is het nodig om goed in contact te blijven met relevante belanghebbenden, en de belangrijke veranderingen in de bedrijfsvoering nauwgezet te volgen. Een voorbeeld van een verandering is cloud adoptie. Het SOC dient een proactieve houding aan te nemen in een dergelijke transitie. Helderheid verschaffen over de rol van het SOC is daarbij belangrijk, alsmede het overbrengen van de belangen (requirements) van het SOC.

5.2 Dienstafnemers en belanghebbenden

Het SOC staat in dienst van de organisatie. Het is om die reden belangrijk om eenduidig vast te stellen welke dienstafnemers en belanghebbenden er zijn zodat een goede afstemming plaats kan vinden. Daarbij dient onderscheid gemaakt te worden tussen

1. **Dienstafnemers.** De dienstafnemers kunnen gezien worden als de traditionele 'klanten' van het SOC. Dienstafnemers maken gebruik van de diensten en ontvangen output van de diensten. Output is bijvoorbeeld een rapportage, maar kan ook een notificatie zijn. Dat is verschillend per dienst en per geval. In sommige gevallen zijn dienstafnemers ook afhankelijk van hun compliance door het gebruik van de SOC-diensten. Het is daarom van groot belang dat de diensten van het SOC zoveel mogelijk aansluiten bij de wensen van de dienstafnemers.
2. **Interne belanghebbenden.** Interne belanghebbenden zijn belanghebbenden binnen de organisatie. Daarbij wordt verder onderscheid gemaakt in 2 typen belanghebbenden:
 - a. **Primaire interne belanghebbenden** zijn belangrijke entiteiten of functies binnen de organisatie die meegenomen worden in- of actief onderdeel zijn van- de besluitvorming binnen het SOC. Deze belanghebbenden zijn daarmee ook een actief onderdeel van de governance binnen het SOC, en bepalen mede de strategische richting van het SOC. Voorbeelden van primaire belanghebbenden zijn de CISO, COO en de CTO.
 - b. **Secundaire interne belanghebbenden** zijn niet actief betrokken in de besluitvorming en strategische richting van het SOC. Wel wordt een actieve relatie mee onderhouden. Voorbeelden van secundaire interne belanghebbenden zijn privacy officers, legal afdelingen, interne compliance, enzovoorts.
3. **Externe belanghebbenden.** Externe belanghebbenden zijn belanghebbenden buiten de organisatie en aanpalende diensten waarmee een actieve samenwerking gevoerd wordt. Externe belanghebbenden hebben geen directe invloed op de besluitvorming binnen het SOC, maar worden gezien als belangrijke partners.

Best Practices voor inrichting

Allereerst is het van belang om in kaart te brengen welke (beoogde) dienstafnemers en belanghebbenden bestaan, zowel binnen de organisatie als daarbuiten. Dit geschiedt veelal door middel van een stakeholder analyse. Naast het in kaart brengen van de belanghebbenden is het tevens belangrijk om hun informatiebehoeften en wensen te kennen. Dit kan meegenomen worden in het ontwerp van de diensten en de inrichting van dienstrapportages.

Voor externe belanghebbenden is het tevens belangrijk om vast te leggen op welke manier gecommuniceerd wordt. Veilige transmissie van communicatie is uiteraard een belangrijk onderdeel daarbij, maar ook het correct toepassen van het FIRST Traffic Light Protocol (TLP) versie 2 ^[1] en het VIRBI 2013 ^[2] is essentieel.

Best Practices voor uitvoering

Gedurende de operatie van het SOC is het met name van belang dat regelmatig overleg met dienstafnemers en belanghebbenden plaatsvindt en dat deze overleggen onderdeel zijn van het continu verbeteren binnen het SOC. De overlegstructuur zelf is onderdeel van het SOC-CMM element *governance*.

5.3

Charter

Een charter is een strategisch document dat als doel heeft om helderheid te geven over de missie en visie van het SOC, alsook de geleverde diensten en de taken en verantwoordelijkheden die daarbij horen. Het charter dient als separaat document opgesteld te worden, omdat het een functie heeft als communicatiedocument naar de organisatie.

Het charter document dient bekrachtigd te worden op senior managementniveau, zodat draagvlak ontstaat voor de uitvoering van de SOC-diensten.

Best Practices voor inrichting

Bij de initiële inrichting van een SOC zal het charter fungeren als high-level design. Het opstellen van een charter is daarmee de eerste concretisering van hoe het SOC ingericht gaat worden.

Bij het opstellen van het charter dienen de volgende elementen geadresseerd te worden:

- **Missie.** De missie beschrijft waarom het SOC bestaat.
- **Visie.** De visie beschrijft waar het SOC naar toe wil werken.
- **Doelstellingen.** Naast missie en visie is het ook van belang om vast te stellen naar welke doelen het SOC streeft. Deze doelen worden meegenomen in de strategie.
- **Strategie.** De strategie beschrijft op welke manier het SOC toewerkt naar het realiseren van de missie, visie en doelstellingen.
- **Dienstencatalogus.** In de dienstencatalogus wordt beschreven welke diensten het SOC levert aan de organisatie, in het charter moet worden verwezen worden naar de dienstencatalogus.
- **Producten.** De producten geven aan welke output uit de diensten verwacht kan worden. Producten omvatten bijvoorbeeld rapportages, notificaties, advisories, incidentmeldingen, enzovoorts.
- **Taken en verantwoordelijkheden.** De taken van verantwoordelijkheden van het SOC worden in RACI-tabel formaat opgesteld, zodat het duidelijk is welke taken en verantwoordelijkheden bij het SOC liggen en welke bij andere onderdelen van de organisatie belegd zijn. RACI-tabellen worden opgesteld per dienst die het SOC levert.
- **Operationele uren en bereikbaarheid.** Hier wordt beschreven op welke momenten en op welke manieren het SOC bereikbaar is.
- **Belanghebbenden.** De stakeholder analyse, zoals beschreven in het vorige onderdeel, wordt opgenomen in het charter.
- **Statement of success.** Een laatste element in het charter is een *statement of success*, waarmee het SOC duidelijk maakt wanneer het succesvol is in haar doelstellingen.

¹ <https://www.first.org/tlp/>

² <https://wetten.overheid.nl/BWBR0033507/2013-06-01>



Best Practices voor uitvoering

Voor het SOC Charter is het met name belangrijk om het document met regelmaat te beoordelen om vast te stellen of deze nog een goede afspiegeling van de SOC-inrichting is. Met name in SOC's die nog een opstartende fase zijn, zal het document sneller gedateerd raken en is een hogere update frequentie aan te raden. Bij elke grote wijziging (met name: veranderingen in verantwoordelijkheden) is het noodzakelijk om het document opnieuw te laten bekrachtigen. Daarnaast is het advies om het document jaarlijks opnieuw te beoordelen.

Het opstellen van een presentatie waarin de kernpunten van het charter uiteengezet zijn is vaak een effectieve manier om de inhoud van het charter buiten het SOC uit te dragen. Dit kan bijdragen aan meer begrip en waardering voor de SOC-functie. Dit kan dan weer ondersteunend werken om organisatieonderdelen en afdelingen aan te laten sluiten op de SOC-diensten.

5.4

Governance

Governance beschrijft de beheersing van SOC-processen, output en performance. Voor SOC governance is een aantal onderwerpen van belang:

- Organisatorische positionering van het SOC
- Relatie tot andere security entiteiten
- Governance meetings
- Kostenbeheersing
- Toepassing frameworks en Best Practices

Deze onderwerpen worden hierna in detail uitgewerkt.

5.4.1

Organisatorische positionering van het SOC

Een belangrijke inrichtingsbeslissing om te nemen is waar het SOC in de organisatie gepositioneerd worden. Er is geen specifieke voorkeur voor het positioneren van het SOC in de organisatie. Belangrijk is dat het SOC goed kan functioneren van die positie. Elke positie kent zijn eigen voor- en nadelen. Positionering en aansturing vanuit de lijn geven een bepaalde focus aan de doelstellingen van het SOC, waar rekening mee gehouden moet worden. Zo zal een SOC wat geplaatst wordt binnen IT (of direct onder de CTO) een sterker focus hebben op de aansluiting met andere IT-teams, en minder met business teams. Een ophanging onder de CISO zal een betere aansluiting vinden met beleid, maar minder met de operationele implementatie van dat beleid.

Best Practices voor inrichting

De positionering van het SOC moet een gedragen besluit zijn door de SOC Manager en de primaire belanghebbenden. Voordat een definitieve beslissing wordt genomen is het van belang om een goed beeld te hebben van de voor- en nadelen. De geïdentificeerde nadelen dienen zo goed mogelijk geadresseerd te worden in de uiteindelijke beslissing.

Best Practices voor uitvoering

Best Practices voor uitvoering is dat de positionering van het SOC het best tot zijn recht komt onder de CTO of COO om een sterke band te garanderen op het gebied van beleid en uitvoering.

5.4.2 Verschijningsvormen

Er zijn verschillende verschijningsvormen binnen het SOC. Het document "11 Strategies of a World-Class CyberSOC" [3] onderkent de volgende typen:

- **Ad-hoc security response.** Alleen een security respons wanneer er incidenten zijn. Dit is geen echte SOC-vorm.
- **Security as an additional duty.** Een persoon waarbij security niet de kerntaak is. Bijvoorbeeld een beheerder die ook verantwoordelijk is voor security. Dit is geen echte SOC-vorm
- **Distributed SOC.** Een virtueel SOC-team met experts door de organisatie. Dit begint de contouren te krijgen van een SOC.
- **Centralised SOC.** De meest voorkomende SOC-vorm: één enkel SOC op één enkele locatie
- **Federated SOC.** Een SOC-vorm waarin verschillende SOC's samenwerken, bijvoorbeeld conform een follow-the-sun principe om 24/7 dienstverlening te kunnen aanbieden.
- **Coordinating SOC.** Een SOC wat zelf geen operationele taken heeft, maar andere SOC's aanstuurt en zorgt voor een gelijkaardige werkwijze.
- **Hierarchical SOC.** Een SOC wat zelf operationele taken heeft en daarnaast ook andere SOC's aanstuurt.
- **National SOC.** Een SOC wat acteert op nationaal niveau en afstemt met andere nationale SOC's en SOC's binnen het eigen land.
- **MSSP.** Niet zozeer een SOC type, maar een SOC als dienstverlening. In dit geval is er dan sprake van een outsourced SOC.

Overige vormen die niet in document terugkomen:

- **Hybride SOC:** Het hybride SOC ontstaat wanneer een SOC kiest voor gedeeltelijk outsourcing bij een Managed Security Service Provider (MSSP).
- **Tiering** (zie [paragraaf 6.2.3](#)). Veelvoorkomend is dat tier-1, of zowel tier-1 als tier-2 door een dienstverlener gedaan worden.
- **Specifiek vs generiek.** Bij deze vorm wordt de generieke monitoring uitgevoerd door een dienstverlener die een geoptimaliseerde ruleset heeft hiervoor. Organisatie-specifieke monitoring wordt opgepakt door het eigen SOC.
- **Splitsing op basis van tijden.** In dit geval wordt een splitsing gemaakt op basis van openingstijden. De outsourcing partij neemt de monitoring buiten kantooruren over om 24/7 dienstverlening te kunnen realiseren. Veelal worden hierbij de monitoring infrastructuur en de processen van het eigen SOC gehanteerd. Specifieke afspraken over escalatie buiten kantooruren zijn hierbij noodzakelijk.
- **Technologie.** In het laatste geval is het ook mogelijk om bepaalde onderdelen van de infrastructuur te laten monitoren door een leverancier. Zo kan het eigen SOC verantwoordelijk zijn voor de gehele eigen ICT-omgeving, en de leverancier invulling geeft aan cloud monitoring.

³ <https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf>

Best Practices voor inrichting

De meest passende verschijningsvorm voor een SOC is afhankelijk van de doelstellingen en ambities van de organisatie ten aanzien van security operations. Daarbij moet rekening gehouden worden met de complexiteit die sommige verschijningsvormen met zich meebrengen. Vooral de vormen *federated*, *coordinating* of *hierarchical* vereisen een hoge mate van volwassen governance om te onderhouden. Het hybride SOC is daarentegen een verschijningsvorm die steeds vaker voorkomt in verschillende opzet. Wanneer een organisatie kiest voor gedeeltelijke outsourcing is het met name van belang om te bepalen welke delen geoutsourcet worden en welke delen bij de organisatie zelf blijven en wat de *business* reden daarvoor is zodat een consistente inrichting behaald kan worden.

Best Practices voor uitvoering

Binnen het Joint SOC wordt de voorkeur gegeven aan een intern gecentraliseerd SOC, waarbij de behoefte van de organisatie zo veel mogelijk beantwoord wordt. Indien het SOC gekozen heeft voor een volledig outsourcet of een hybride opzet is het wel belangrijk bijzondere aandacht uit te laten gaan naar de inrichting van governance. Deze governance dient zich vooral te richten op sturing op de kwaliteit van de dienstverlening. Voor hybride SOC's is het van bijzonder belang dat de interfaces tussen beide delen van het SOC goed gedefinieerd zijn en goed beheerst worden.

5.4.3 *Relatie tot andere security entiteiten*

Het SOC is niet de eigenaar van alle operationele securityactiviteiten, maar heeft een specifieke taakstelling. Voor governance binnen het SOC is het daarom belangrijk om de positionering van het SOC als security entiteit binnen de organisatie vast te stellen. Daarnaast is van het belang om de relatie tot andere security entiteiten en taken vast te stellen.

Voorbeelden van relevante security entiteiten zijn: CISO, IT-operations, IT-audit, operational (IT) risk management. Elk van deze entiteiten heeft een specifieke functie. Het is essentieel om deze functies goed te begrijpen om het security speelveld goed in kaart te brengen.

Best Practices voor inrichting

Tijdens de inrichting moet de SOC-functie in relatie tot de andere securityfuncties gedefinieerd en bekrachtigd worden. Dit gebeurt onder andere door het uiteenzetten van de taken en verantwoordelijkheden in de RACI-tabellen behorende bij het charter.

Best Practices voor uitvoering

Best Practices voor uitvoering zijn niet relevant voor dit onderwerp omdat de relatie tot andere security entiteiten in het algemeen statisch is.

5.4.4 *Governance meetings*

De governance meetings van het SOC vinden plaats op verschillende niveaus: operationeel, tactisch en strategisch:

- **Operationele governance.** Operationele governance is gericht op dagelijkse aansturing van het SOC. Meetings zoals daily stand-ups, planning sessies, zijn daar onderdeel van.
- **Tactische governance.** Tactische governance is veelal gericht op het verbeteren van de operationele performance van het SOC. Onderwerpen als rapportage, meetbaarheid, kwaliteitsmanagement en continue verbetering horen daarbij.
- **Strategische governance.** Strategische governance is met name gericht op de richting van het SOC en de aansluiting bij de rest van de organisatie. Stuurgroep meetings, kwartaalsessies en maandelijkse review sessies

Best Practices voor inrichting

Governance meetings worden gedefinieerd op verschillende niveaus: operationeel, tactisch en strategisch. Voor elk van de meeting moet vastgesteld worden wie de deelnemers van de meetings zijn, wat de doelstellingen van de meetings zijn en welke input (rapportage, metrics, etc.) en output er verwacht kan worden van de meeting. Dit kan formeel vastgelegd worden in een *Terms of Reference (ToR)* document.

Tijdens de inrichting van het SOC is het aan te raden om een stuurgroep in het leven te roepen. Deze stuurgroep bewaakt de voortgang van de implementatie van het SOC en stuurt bij indien nodig. Als het SOC operationeel is, kan deze stuurgroep in stand gehouden worden. Het is echter ook mogelijk om de stuurgroep op te heffen en sturingselementen onder te brengen in de nieuwe governance structuur.

Best Practices voor uitvoering

De effectiviteit van de governance structuur dient met regelmaat geëvalueerd worden. Waar nodig worden wijzigingen doorgevoerd om de effectiviteit van de governance meetings te maximaliseren. Een voorbeeld van een wijziging is het toevoegen of verwijderen van deelnemers, of het wijzigen van de input. Indien er ToR documenten gehanteerd worden, worden deze ook geüpdatet om overeen te komen met de wijzigingen.

5.4.5***Kostenbeheersing***

Kostenbeheersing is een belangrijk onderwerp omdat de investering in security in het algemeen en security operations in het bijzonder kloppend moet zijn binnen het totaalbudget. De uitgaven voor security moeten in lijn zijn met het risico wat de organisatie loopt op dit gebied, zodat security niet alleen effectief is, maar ook kosten-efficiënt. Het kwantificeren van risico, bijvoorbeeld de FAIR™ [4] methodologie kan daarbij een goed instrument zijn.

Best Practices voor inrichting

Voor inrichting van kostenmanagement is het met name van belang om de verschillende typen kosten en de hoogte van deze kosten in kaart te brengen. De typen kosten kunnen omvatten:

- Personeelskosten, inclusief kosten voor kennisontwikkeling (training, certificering, opleiding, etc.).
- Kosten geassocieerd met SOC-processen. Omvat bijvoorbeeld kosten voor het uitvoeren van oefeningen.
- Technologiekosten, inclusief licenties.
- Kosten geassocieerd met dienstverlening. Dat kunnen bijvoorbeeld pentesting kosten zijn indien het SOC pentesting uitbesteed, of kosten van een bug bounty programma indien dat gevoerd wordt.
- Kosten van fysieke faciliteiten, waaronder huisvesting.
- Kosten behorende bij ontwikkeling en innovatie.

De verschillende typen kosten worden niet altijd doorberekend aan het SOC. Het is belangrijk om bij de inrichting vast te stellen welke kosten wel en niet doorberekend worden.

Best Practices voor uitvoering

Om een goede beheersing van kosten te realiseren is het van belang om continu goed inzicht te hebben in de budgetten en de benutting daarvan. Daarnaast is het belangrijk om forecasting te doen voor verwachte benutting. Met deze informatie kan gestuurd worden zodat benutten van budgetten optimaal is en de grenzen niet overschrijdt. Tenslotte is het ook van belang om mogelijk groei in budgetten (met name operationele kosten) te identificeren en goed te laten keuren voor de volgende budgetcyclus.

⁴ [The Importance and Effectiveness of Quantifying Cyber Risk \(fairinstitute.org\)](https://www.fairinstitute.org/)



5.4.6 *Gebruikte frameworks en Best Practices*

Het SOC moet vastleggen welke frameworks en Best Practices toegepast worden binnen het SOC.

Best Practices voor inrichting

Tijdens de inrichting van het SOC worden Best Practices en frameworks op verschillende niveaus geselecteerd, vastgelegd en toegepast. De volgende Best Practices, methodologieën en frameworks vormen daarbij een basis set:

- Voor toetsing van de volwassenheid van het SOC wordt het [SOC-CMM maturity assessment](#) toegepast. Waar mogelijk wordt benchmarking toegepast om het eigen SOC te vergelijken met andere SOC's in dezelfde sector. Het doel hiervan is om te leren van elkaars inrichting. Een SOC-CMM assessment wordt jaarlijks uitgevoerd om de groei van het SOC accuraat te kunnen monitoren.
- Voor meting van dienstverlening worden de [SOC-CMM metrics](#) gebruikt. Een selectie aan relevante metrics is daarbij noodzakelijk. Het document beschrijft op welke manier een selectie gemaakt kan worden. Het meest relevant daarbij is het selecteren van metrics die gebruikt kunnen worden om zwakkere onderdelen van het SOC te ondersteunen. Er is daarmee een koppeling tussen het meten van volwassenheid en het toepassen van metrics.
- Voor inrichting van de rollen en daarbij behorende verantwoordelijkheden worden het [NIST NICE framework](#) gebruikt.
- Voor de inrichting van een bredere cyber security strategie wordt het [NIST Cyber Security Framework](#) gehanteerd. Voor het SOC zijn met name de functies Detect en Respond belangrijk.
- Voor de inrichting van Use Case Management wordt het [MaGMa Use Case Framework](#) gehanteerd.
- Voor het monitoren en verbeteren van de coverage ten opzichte van bekende aanvalstechnieken wordt [MITRE ATT&CK®](#) gebruikt. De coverage ten opzichte van MITRE ATT&CK® wordt maandelijks gemeten. Voor het in kaart brengen van visibility ten opzichte van MITRE ATT&CK® op basis van bestaande log bronnen wordt de [DeTT&CT](#) tooling gebruikt. De visibility status wordt maandelijks gemeten. Tenslotte wordt het [MITRE D3FEND™](#) framework gebruikt om in kaart te brengen welke preventieve controls ingericht zijn om bepaald aanvalstechnieken te kunnen weerstaan.
- Voor de uitvoering van threat intelligence wordt het threat intelligence life cycle proces uit het [Threat Intelligence Handbook](#) van Recorded Future gebruikt, gebaseerd op de US DoD intelligence lifecycle.
- Voor de zichtbaarheid van het SOC in de infrastructuur wordt de [Gartner visibility triad](#) gebruikt.
- Voor het ontwikkelen van security incident capabilities wordt het [RE&CT](#) framework gebruikt.
- Voor het uitvoeren van threat hunting onderzoeken wordt de [TaHiTI threat hunting methodologie](#) en/of de [PEAK methodologie](#) toegepast.
- Voor algemene Best Practices in het SOC wordt het document [MITRE 11 Strategies of a World-Class Cybersecurity Operations Center](#) gebruikt.

Best Practices voor uitvoering

De set aan frameworks wordt met regelmaat geëvalueerd, om zeker te zijn dat het SOC de trends en voortschrijdende inzichten op het gebied van security operations blijft volgen.

5.5 Privacy, beleid, wetgeving en juridische kaders

5.5.1 Privacy

Privacy is een belangrijk onderwerp binnen het SOC, vanwege het centraal verwerken van gegevens en de aard van de informatie. Voor een deel van de gegevens is een Data Privacy Impact Assessment (DPIA) verplicht. Dit geldt in ieder geval voor dataverwerking in het kader van monitoren van gebruikershandelingen. In een DPIA worden risico's geïdentificeerd en maatregelen benoemd. Deze maatregelen worden vervolgens opgevolgd door het SOC middels de bestaande mechanismen voor continue verbetering. Wanneer er door security en privacy tegenstrijdige maatregelen worden voorgesteld moet er op de juiste plek binnen de organisatie een besluit worden genomen met betrekking tot deze tegenstrijdige maatregelen. Voor het SOC is het genomen besluit input en is zij (enkel) uitvoerend.

Best Practices voor inrichting

Bij de inrichting van het SOC is het van belang om privacy vereisten voor SOC-services goed in kaart te brengen. Een samenwerking met een Functionaris Gegevensbescherming (FG) of vergelijkbaar, is daarbij een krachtig hulpmiddel. Deze requirements kunnen vervolgens gebruikt worden om maatregelen te nemen die in overeenstemming zijn met privacyregels. Proportionaliteit en doelbinding zijn daarbij belangrijke principes. Tevens kunnen de uitgangspunten voor het behouden van privacy op de werkplek opgenomen worden in een SOC-beleid.

Best Practices voor uitvoering

Gezien de dynamiek van monitoring door het SOC, bijvoorbeeld op het gebied van nieuwe tooling, nieuwe processen en nieuwe werkwijzen, wordt een DPIA op security monitoring elke drie jaar opnieuw uitgevoerd. Uiteraard is de frequentie afhankelijk van de risk appetite van de organisatie. Daarnaast worden operationele procedures die impact hebben op privacy met regelmaat getoetst.

5.5.2 Beleid

Voor de correcte werking van het SOC is het van belang dat beleid op het gebied van security aanwezig is binnen de organisatie. Het beleid geeft mandaat aan het SOC om acties te ondernemen. Relevant beleid omvat in ieder geval:

- **Auditing en logging beleid.** Dit beleid beschrijft dat audit logging voor systemen aan dient te staan en dat logging naar een centrale log omgeving verstuurd moet worden. Ook het loglevel en de benodigde loginformatie (voor intern ontwikkelde applicaties) dienen hierin te staan. Het auditing en logging beleid draagt daarmee bij aan de basis voor log-gebaseerde monitoring technieken zoals SIEM.
- **Incident management-beleid.** In dit beleid worden de activiteiten en escalaties op het gebied van incidenten beschreven. Het is van belang dat het security incident managementproces aansluit op bestaande incident managementprocessen binnen de organisatie, met de daarbij behorende escalatie lijnen en vastgestelde verantwoordelijkheden. Tenslotte moet hier ook het mandaat van het SOC om respons acties uit te mogen voeren vastgelegd zijn. Dit dient zowel kleine respons acties (het isoleren van een werkstation) tot grote respons acties (het afsluiten van de internetverbinding) te omvatten. Dergelijk acties hebben waarschijnlijk een impact op de bedrijfsvoering. De spelregels voor het uitvoeren van deze acties moeten daarom helder zijn, inclusief het achteraf afleggen van verantwoordelijkheid over de genomen beslissingen. Belangrijk daarbij is dat, achteraf gebleken, verkeerde beslissingen geen persoonlijke consequenties mogen hebben voor de medewerker in kwestie. Voor het melden van security incidenten wordt een procedure opgesteld, zodat duidelijk is wanneer en waar een incident gemeld kan worden.



- **Vulnerability Management-beleid.** Met dit beleid wordt een fundament gelegd voor het omgaan met kwetsbaarheden binnen de organisatie. Het beleid moet onder andere duidelijk maken binnen welke tijd opvolging gedaan moet worden en welke verantwoordelijkheden daarbij horen. Een Coordinated Vulnerability Disclosure (CVD) beleid, als toevoeging op het vulnerability management-beleid, is relevant voor organisaties die een CVD-beleid voeren.
- **Beleid voor veilige applicatieontwikkeling.** Dit beleid beschrijft op welke manier zorggedragen wordt dat applicaties binnen de organisatie op een veilige manier ontwikkeld worden. De SOC requirements zijn daarbij ook van belang. Het gaat daarbij om requirements op het gebied van logging, maar ook op aansluiting bij bestaande securityprocessen en diensten, zowel binnen het SOC als daarbuiten. Indien het SOC ook pentesting uitvoert en/of coördineert, is een grotere rol voor het SOC in applicatieontwikkeling voorzien.

Hiernaast kan ook een SOC beleid worden opgesteld. Dit is een document waarin de werkwijze, afspraken en regels die gelden binnen het SOC uiteen worden gezet.

Best Practices voor inrichting

Bij het inrichten van het Security Operations Center moet vastgesteld worden of het bestaande beleid het SOC voldoende ondersteunt in de werkzaamheden. Waar dit niet het geval is, dient additioneel beleid te worden opgesteld, of dient bestaand beleid te worden aangepast. Ook is het belangrijk om een goede aansluiting bij beleid te vinden. Het beleid wordt daarbij gebruikt om processen en diensten te ontwerpen. De taak van het SOC in het operationaliseren van beleid in techniek en processen moet daarbij helder zijn.

Tenslotte is het van belang een SOC-beleid op te stellen met de volgende elementen:

- Gedragsregels. De attitude van SOC medewerkers kan heel bepalend zijn voor de security cultuur in de organisatie.
- Rules of Engagement (RoE). Hierin wordt uiteengezet wat wel en niet gedaan mag worden door medewerkers in geval van een (mogelijke) dreiging of incident.
- Verantwoordelijkheden. Het betreft algemene verantwoordelijkheden. Rol-specifieke verantwoordelijkheden zijn verder uiteengezet in rolbeschrijvingen.
- Afspraken over het bijhouden van documentatie (review frequentie).
- SOC assessment frequentie en type (self-assessment, 3rd-party assessment).
- Kennisuitwisseling.
- Frequentie van oefeningen binnen het SOC.
- Gebruik van het Traffic Light Protocol (TLP).
- Overige werkafspraken.

Voor gedragsregels kunnen zaken als het personeelsreglement of een formele gedragscode als input worden gebruikt.

Best Practices voor uitvoering

Aansluiting op beleid is vooral een taak van inrichting, omdat beleid in het algemeen niet heel sterk wijzigt. Voor operatie is het met name van belang dat wijzigingen in beleid gevolgd worden door wijzigingen in inrichting van techniek en processen.

5.5.3

Wetgeving en Juridische kaders

Het SOC moet zich bewegen binnen de geldende wettelijke kaders. Kaders verschillen per type organisatie, en kunnen omvatten:

- **Aanbestedingsplicht.** Indien sprake is van een aanbestedingsplicht moet nieuwe technologie binnen het SOC via een Europese aanbesteding verkregen worden. De aanbestedingsregels zijn daarbij van toepassing om te bepalen of een aanbesteding wel of niet noodzakelijk is. Het SOC dient te voldoen aan dezelfde regels met betrekking tot inkoop van middelen als de rest van de organisatie.
- **Zorgplicht.** Uit de NIS2 regelgeving vloeit een zorgplicht voor het vaststellen van risico's en het nemen van maatregelen. Alhoewel de risico assessment geen activiteit is van het SOC, kan het SOC wel betrokken worden hierbij. Het SOC zelf, en de diensten die geleverd worden, vallen onder de maatregelen.
- **Meldplicht.** Het SOC heeft een meldplicht, die door verschillende richtlijnen worden afgedwongen:
 - Meldplicht voor incidenten met betrekking tot persoonsgegevens bij de Autoriteit Persoonsgegevens (AP), voortvloeiend uit de Algemene Verordening Gegevensbescherming (AVG). Het SOC is in dit geval niet altijd de melder, maar levert wel de benodigde informatie voor de melding aan.
 - Meldplicht voor het melden van grote security incidenten bij het NCSC of bij een sectoraal CERT, voortvloeiend uit de NIS2 regelgeving.
 - Meldplicht voor het melden van grote security incidenten bij de toezichthouder, voortvloeiend uit de NIS2 regelgeving.N.B. Aangifte doen bij de Politie bij aanvallen is geen verplichting, maar wordt bij voorkeur wel gedaan. Zorg er voor dat het duidelijk is wie binnen de organisatie gemachtigd is om aangifte te doen namens de organisatie. Dit kan een SOC medewerker zijn maar kan ook elder belegd worden binnen de organisatie.
- **Vrijwaring.** Bij sommige activiteiten (zoals pentesting en sommige typen oefeningen) kan het noodzakelijk zijn de organisatie te vrijwaren voor eventuele gevolgschade. De organisatie moet anderen ook vrijwaren wanneer dit noodzakelijk is.

Daarnaast moet het SOC ook voldoen aan algemene wetgeving (zoals de AVG) en aanvullende wetgeving voor een sector (zoals BIO voor de Rijksoverheid)

Voor ondersteuning bij deze vraagstukken kan het SOC vaak terecht bij interne juridische afdeling.

Best Practices voor inrichting

Net als beleid geldt ook voor wetgeving en juridische kaders dat deze in het algemeen vrij statisch zijn. Het is dus vooral van belang om bij de inrichting van het SOC en het ontwerpen van relevante processen rekening te houden met de hierboven beschreven kaders. In bijlage C is aanvullende informatie opgenomen welke gebruikt kan worden in de inrichting.

Best Practices voor uitvoering

Het correct toepassen van wetten en regels is de belangrijkste taak tijdens de operatie. Dit kan geborgd worden door vastleggen in processen en procedures tijdens de inrichting. Het is daarbij ook van belang dat er awareness is binnen het SOC van geldende wetten en regels zodat het belang van correcte toepassing ook gezien wordt.

Daarnaast is het bijhouden van wijzigingen ook relevant. Alhoewel een juridische afdeling hier leidend in hoort te zijn, heeft het SOC een plicht om te (blijven) voldoen aan de voor hun geldende wetten en regels, ook wanneer deze wijzigen.

6 People domein

6.1 Medewerkers

Het element medewerkers van het SOC-CMM gaat in op het hebben en behouden van de juiste aantallen FTE's binnen het SOC. Het aantrekken en behouden van gekwalificeerd personeel is een belangrijke strategische pijler voor het SOC. Dit omdat de kwaliteit van de output van het SOC in belangrijke mate afhankelijk is van de medewerkers. Daarnaast is een veilige werkomgeving van groot belang voor het optimaal functioneren van het team.

6.1.1 *Aantrekken talent*

Het aantrekken van talent is een lastige opgave in de vanwege de aanhouden schaarste. Omwille van de continuïteit van het SOC is het echter wel zeer belangrijk om dit te doen. Daarbij gaat het om aantrekken van talent op verschillende niveaus. Concreet betekent dit dat de organisatie moet inzetten op het aantrekken van getalenteerd senior personeel, maar ook het aantrekken en door ontwikkelen van nieuw talent ("high potentials"). Dat kan door samenwerkingen aan te gaan met onderwijsinstellingen, of wervingsevents te organiseren.

6.1.2 *Behouden talent*

Naast aantrekken van nieuw talent is het behouden van bestaand personeel ook essentieel. Dit vanwege de kennis die medewerkers op hebben gedaan van de organisatie en de processen binnen de organisatie. Voorbeelden van initiatieven voor het behouden van talent zijn:

- Ruimte geven voor groei en persoonlijke ontwikkeling;
- Ruimte geven voor vaktechnische groei door middel van training en certificering;
- Stimuleren van een cultuur waarbij samen werken aan strategische doelen belangrijk is (zingeving in het werk);
- Autonomie bewerkstelligen voor personeel van het SOC om beslissingen te mogen nemen en het eigen werk zelf beter te maken;
- Voeren van een beloningsbeleid wat kans geeft op verder doorgroeien in de techniek. Hiermee wordt bedoeld dat hogere schalen niet alleen mogelijk zijn voor aansturende (management) rollen;
- Voeren van een beloningsbeleid binnen het SOC wat gelijkwaardig is met andere SOC's binnen dezelfde sector en/of regio.

6.1.3 *Veilige werkomgeving*

Het is van belang om een psychologisch veilige werkomgeving te creëren voor alle teamleden. Dit leidt tot meer tevredenheid bij medewerkers en tot betere teamprestaties. Kernwoorden daarbij zijn respectvol, integer, vertrouwen, open en inclusief. Dit geldt uiteraard ook voor het SOC, waarbij het uitgangspunt is dat alles besproken moet kunnen worden en ieders mening even waardevol is. Het is de verantwoordelijkheid van de SOC Manager om deze veilige werkomgeving te realiseren en te bewaken. Dit moet ook de SOC medewerker uitdragen richting de organisatie. Als de SOC medewerker laat zien integer te handelen straalt dat uit naar de organisatie en zijn collega's binnen de organisatie ook eerder bereid security risico's te delen. Een SOC medewerker heeft een voorbeeld functie met betrekking tot security, integriteit en privacy.

Best Practices voor inrichting

Tijdens de inrichting is het met name van belang dat een aantal faciliteiten geregeld worden die zorgdragen voor het aantrekken van talent, zoals het bieden van stageplekken, het samenwerken met hogescholen en universiteiten en het hebben van een goed trainingsprogramma (traineeship) voor het versneld door ontwikkelen van talent. Waar mogelijk wordt aangesloten bij bestaande initiatieven voor talentontwikkeling binnen de organisatie en/of de Rijksoverheid.

Voor het aantrekken van ervaren medewerkers is het met name van belang dat het SOC een uitdagende en afwisselende plek is om te werken, waar ook ervaren medewerkers zich nog verder kunnen ontwikkelen, zowel in soft als in hard skills.

Wat betreft het behoud van talent geldt dat (een selectie) van de genoemde elementen ingericht moeten worden. Daarbij moet rekening gehouden worden met het feit dat een zeker verloop (tot 10% over een jaar) van medewerkers gezond is en zorgt voor instroom van nieuwe kennis en kunde.

De veilige werkomgeving ontstaat uit een open cultuur binnen het SOC. Tijdens de inrichting is het belangrijk om ook vertrouwenspersonen binnen de organisatie (maar buiten het SOC) aan te wijzen, zodat escalatie mogelijk is wanneer de SOC Manager zelf onderdeel is van een onveilige werkomgeving. Het management onderstreept dat een SOC medewerker te allen tijde vrij hun werk zouden moeten kunnen doen.

Tenslotte is het belangrijk om bij de inrichting van deze zaken goed samen te werken met het HR-team (indien voorhanden) en inrichting conform HR-beleid te doen.

Best Practices voor uitvoering

Tijdens de operatie is het van belang om een goed beeld te hebben van de hoeveelheid FTE die noodzakelijk is voor het SOC om efficiënt te kunnen draaien. Het is daarbij belangrijk om ook capaciteit voor verandering (*capacity for change*) mee te rekenen (zie het onderwerp [Continuous Improvement](#)). Daarnaast is het belangrijk om deze hoeveelheid FTE af te stemmen met de groeiambities van het SOC. Hier speelt ook kostenbeheersing (zie [paragraaf 5.4.4](#)) een rol.

Voor het behouden van medewerkers en talent is het belangrijk om de medewerkerstevredenheid te meten. Dit geeft het SOC een peilstok om vast te stellen of de ingevoerde maatregelen voor het behoud van medewerkers afdoende zijn. Transparant zijn over de resultaten en actief sturen op verbetering op basis van de output van deze onderzoeken is daarbij zeer belangrijk.

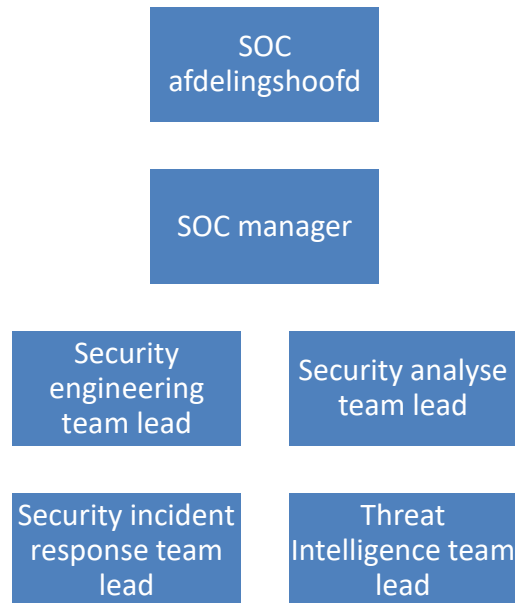
6.2 Rollen en hiërarchie

Het element rollen en hiërarchie gaat in op onderwerpen als rollen binnen het SOC, teamstructuur en *tiers*. De essentie van dit element is bepalen of de huidige personele opzet van het SOC efficiënt is, en of de rollen die binnen het SOC vastgesteld zijn ook goed vastgelegd zijn en goed begrepen worden.

6.2.1 Teamstructuur

Wat betreft teamstructuur is geen vaste formule die in ieder geval zal werken. De twee uitersten zijn:

- Een 'platte' organisatie, waarin er geen structuur is, buiten dat het team een manager heeft.
- Een meer hiërarchische organisatie met verschillende teams, team leads en management lagen ertussen, zoals weergegeven in onderstaande figuur (geschikt voor grotere organisaties).



Uiteraard zijn er vele tussenvormen die voor een team kunnen werken. Vaak zal een team een groeipad doormaken van een platte organisatie naar een meer gestructureerde organisatie, naarmate het aantal medewerkers binnen het SOC groeit. De belangrijkste drijfveer daarbij is *span of control*, ofwel het aantal mensen en management lagen wat redelijkerwijs nog aan te sturen is door 1 manager.

Best Practices voor inrichting

Tijdens de inrichting moet de span of control bepaald worden, omdat deze bepalend is voor het opdelen van het team. Afhankelijk van het niveau van de medewerkers, en met name de autonomie kan span of control tussen 5 en 15 personen zijn. Daarnaast is span of control afhankelijk van het type leiderschap wat past bij de manager ^[5]. Tenslotte speelt volwassenheid van het SOC ook een rol. Een meer volwassen en gestandaardiseerd SOC is eenvoudiger aan te sturen dan een minder volwassen SOC. Bij inrichting van een nieuw SOC is het daarom raadzaam om met een klein aantal medewerkers te beginnen ^[6]. Het SOC kan vanuit die positie groeien naar een ander aansturingsmodel. Wanneer dit niet mogelijk is, is een meer informele aansturing (via team leads) een goede optie omdat de hiërarchische aansturing dan bij de manager blijft, terwijl de inhoudelijke aansturing bij de teamlead ligt. De grootte en complexiteit van de organisatie speelt een rol bij hoeveel mensen er nodig zijn voor een goed functionerende SOC.

Best Practices voor uitvoering

Tijdens de operatie is het van belang om regelmatig te evalueren of de huidige inrichting nog het meest passend is. Een goed moment daarvoor is gedurende de uitvoer van het jaarlijkse *maturity assessment* of tijdens de HR-cycli van de organisatie. Groei in aantallen FTE en groei in volwassenheid kunnen ervoor zorgen dat de teamstructuur niet meer optimaal functioneert. In de dagelijkse operatie valt dit veelal niet direct op. Bij de evaluatie kan zowel gevonden worden dat de huidige span of control te groot is (meer structuur is noodzakelijk), maar ook dat de span of control te klein is (minder structuur is noodzakelijk). In het laatste geval zou dat kunnen betekenen dat een aantal teams samengevoegd wordt.

⁵ <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/how-to-identify-the-right-spans-of-control-for-your-organization>

⁶ <https://www.ncsc.nl/documenten/factsheets/2019/juni/01/soc-inrichten>



6.2.2

Rollen

Binnen het SOC kunnen verschillende rollen bestaan. Het startpunt van het vaststellen van de benodigde rollen zijn de diensten die geleverd worden en de processen die binnen het SOC bestaan.

Met het formeel definiëren van een rol wordt duidelijkheid geschept over zaken als taken, verantwoordelijkheden, kennisontwikkeling, training en groei. Het definiëren en toekennen van rollen past bij een meer volwassen SOC.

Belangrijk om te realiseren is dat rollen en functies niet hetzelfde zijn. Iemand in een functie kan meerdere rollen hebben. Zo is het bijvoorbeeld mogelijk dat een security analyst (functie) zowel de rol van security analyst heeft als de rol van vulnerability analyst, of dat een senior security analyst (functie) zowel security analyst is, als team lead security analyse is.

Mogelijke SOC rollen vanuit het NIST NICE Framework zijn:

NIST NICE Rol	Omschrijving	Gerelateerde terminologie
Infrastructure support	Verantwoordelijk voor het bijhouden en optimaliseren van de SOC-infrastructuur.	Systems engineer
Defensive Cybersecurity	Verantwoordelijk voor het analyseren van security events uit de security tooling.	Security Analyst
Digital Forensics	Verantwoordelijk voor het uitvoeren van forensische onderzoeken.	Forensics analyst
Incident Response	Verantwoordelijk voor het uitvoeren van security incident respons handelingen.	Security incident responder
Threat Analysis	Verantwoordelijk voor het analyseren van dreigingsinformatie en het adviseren van de organisatie.	Threat analyst Intelligence
Vulnerability Analysis	Verantwoordelijk voor het analyseren van kwetsbaarheden en de potentiële impact op de organisatie.	Vulnerability analyst
Cybersecurity Architecture	Verantwoordelijk voor het opstellen en bijhouden van een security architectuur voor het SOC.	Security architecture
Data analysis	Verantwoordelijk voor analyseren van grote hoeveelheden data en het detecteren van patronen door middel van de inzet van algoritmen.	Data scientist

Naast deze rollen vanuit het NICE framework kunnen de volgende rollen ook binnen het SOC gevonden worden:



Rolnaam	Omschrijving
SOC Manager	Eindverantwoordelijk voor het SOC en de output van het SOC.
SOC Lead	Verantwoordelijk voor inhoudelijke aansturing van één of meerdere teams binnen het SOC.
Coördinator	Verantwoordelijk voor de operationele aansturing van één of meerdere activiteiten binnen het SOC
Shift lead	Verantwoordelijk voor de coördinatie van operationele activiteiten binnen een shift
Detection engineer	Verantwoordelijk voor het technisch realiseren en verbeteren van security monitoring regels.
Automation engineer	Verantwoordelijk voor het toepassen van automatisering (al dan niet gebruik makend van SOAR-technologie) binnen het SOC.
Threat hunter	Verantwoordelijk voor het uitvoeren van threat hunting onderzoeken en het rapporteren van de uitkomsten van dergelijke onderzoeken.

6.2.2.1

Roldocumentatie

Elk van de rollen in het SOC moet voldoende gedocumenteerd zijn. De volgende elementen zijn van belang voor een goede rolbeschrijving:

- **Rol beschrijving.** Een samenvatting van de rol en de doelstellingen die horen bij deze rol.
- **Rol taken.** De taken die uitgevoerd moeten worden binnen deze rol.
- **Rol verantwoordelijkheden.** De verantwoordelijkheden (veelal gekoppeld aan de taken) die horen bij de rol.
- **Rol verwachtingen.** De verwachtingen die de SOC Manager en de organisatie hebben bij de invulling van de rol.
- **Benodigde technische vaardigheden.** De technische vaardigheden (hard skills) die noodzakelijk zijn om de taken die horen bij de rol uit te kunnen voeren.
- **Benodigde soft skills.** De soft skills (zoals communicatie, presentatie, etc.) die behoren bij de rol.
- **Benodigde opleidingsniveau.** Het opleidingsniveau wat noodzakelijk is voor het uitvoeren van de rol. In organisaties waar opleidingsniveau minder relevant is kan ook gewerkt worden met denkniveau. Belangrijk om hierbij op te merken is dat Rijksorganisaties niet meer aan diploma-eisen mogen doen en er alleen om toepasselijk werk- en denkniveau mag worden gevraagd.
- **Benodigde of geprefereerde certificeringen.** De trainingen en bijbehorende certificeringen die doorlopen moeten worden voor een rol. Voor bepaalde rollen kan een afgeronde certificering een voorwaarde zijn. Deze informatie dient gekoppeld te zijn aan het training- en certificeringprogramma.

Best Practices voor inrichting

Tijdens de inrichting is het met name van belang om een initieel rolmodel te kiezen wat passend is voor de grootte van het team, de teamstructuur en de diensten die het SOC gaat verlenen. Bij een kleiner team kan gewerkt worden met meer algemene rollen zoals 'analist' en 'engineer'. Deze rollen kunnen in een later stadium van het SOC verbijzonderd worden naar respectievelijk 'threat analyst, security analyst, vulnerability analyst, etc.' en 'security engineer, detection engineer, automation engineer, etc.'. Belangrijk is dat de rollen passend zijn binnen het functiehuis van de organisatie (bijvoorbeeld: functiegebouw Rijk) en dat voor elk van de rollen een goede beschrijving beschikbaar is. Er moet een gezonde verhouding zijn tussen de aantallen senior, medior en junior medewerkers. Doel is wel om minimaal één senior per aandachtsgebied te hebben. Bij een klein SOC kan een senior medewerker werkzaam binnen één of meer aandachtsgebieden.

Rol	Functiegebouw Rijk	
SOC Manager	Operationeel manager [7]	Manager
SOC Lead	Expert IV [8]	Senior Adviseur Bedrijfsvoering
Tier 3 Security Analyst	Expert IV	Senior Adviseur Bedrijfsvoering
Level 2 Security Analyst	Senior medewerker IV [9]	Adviseur Bedrijfsvoering
Level 1 Security Analyst	Senior medewerker IV	Adviseur Bedrijfsvoering

Best Practices voor uitvoering

Tijdens de operatie is het met name van belang om met regelmaat te kijken of de gedefinieerde rollen nog passen binnen de werkwijze, de dienstencatalogus en de teamstructuur van het SOC. Door veranderingen in deze zaken kan het nodig zijn additionele rollen te definiëren. Daarnaast is het ook mogelijk te versimpelen door bepaalde rollen samen te voegen wanneer taken en verantwoordelijkheden te veel overlappen. Tenslotte is het ook van belang om zorg te dragen dat rolbeschrijvingen actueel blijven.

⁷ <https://www.functiegebouwwijksoverheid.nl/functiegebouw-html/functiegroep/511>

⁸ <https://www.functiegebouwwijksoverheid.nl/functiegebouw-html/functiegroep/560>

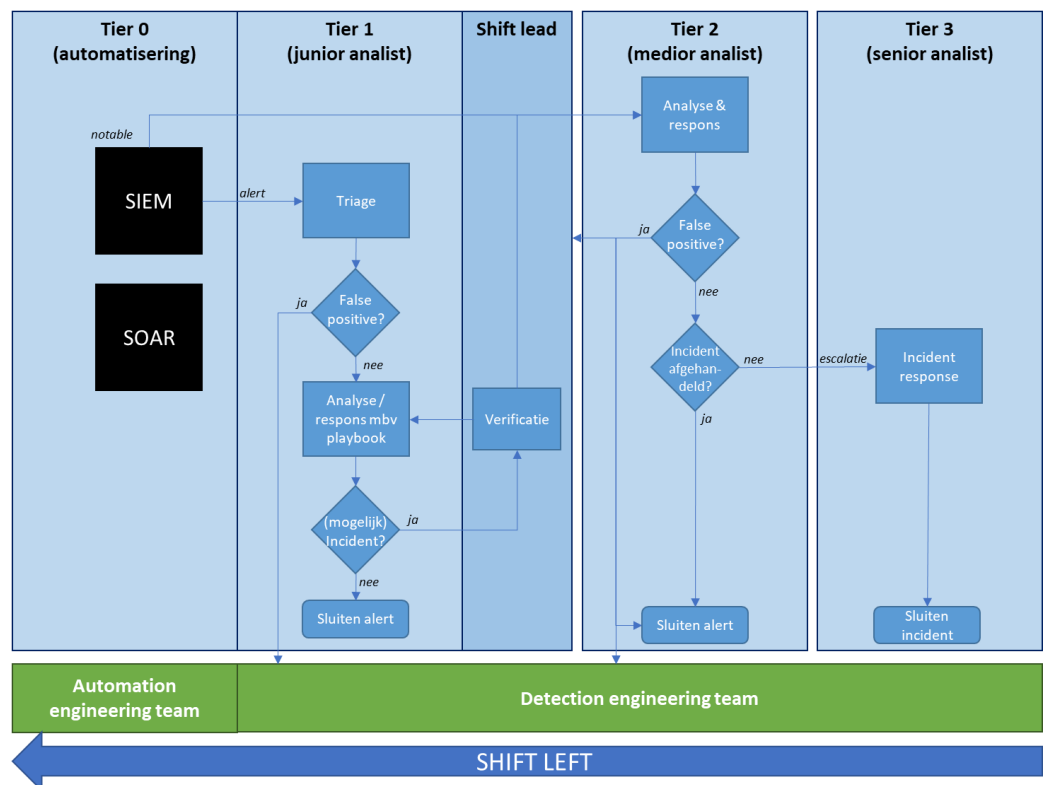
⁹ <https://www.functiegebouwwijksoverheid.nl/functiegebouw-html/functiegroep/559>

6.2.3

Tiers

Tiering is een werkvorm waarbij taken binnen eenzelfde proces over verschillende niveaus worden verdeeld. Binnen Security Operations Centers wordt in sommige situaties tiering toegepast in de security monitoring. Concreet houdt dit in dat er een scheiding is tussen de triage van alerts, de analyse van deze alerts en de opvolging in de incidenten. Onderstaand tabel geeft een aantal belangrijke nadelen en voordelen van tiering weer.

Voordelen tiering	Nadelen tiering
Duidelijke scheiding van taken/ verantwoordelijkheden	Medewerkers meer gelimiteerd door scheiding in taken/ verantwoordelijkheden
Eenvoudigere bezetting van de dagelijkse operatie	Minder eenvoudig doorgroeien in de rol
Geen eenvoudige taken bij ervaren personeel	Minder dynamisch werk voor de medewerkers binnen de tiers
Hybride opzet mogelijk met serviceprovider (uitbesteding 1 ^e lijn)	Minder interessant als werkgever





Tier-1 Security Analyst

De Tier 1 Security Analyst, veelal een junior analist, registreert standaard security meldingen –requests of –incidenten. Deze meldingen worden geïdentificeerd, bekeken of dit een standaardoplossing is waarvoor een werkinstructie voorhanden is. De Tier 1 Security Analyst handelt vervolgens de melding af aan de hand van de werkinstructie. Mocht dit niet mogelijk zijn dan wordt de melding doorgezet naar de Level 2 Security Analyst.

De dagelijkse werkzaamheden van een Tier 1 Security Analyst bestaan uit:

- Het monitoren van Security Events met behulp van tooling en werkinstructies (SIEM/IDS systeem).
- Het registreren en doorzetten van securitymeldingen en incidenten.
- Het opvolgen en registreren van securitymeldingen vanuit standaard werkinstructies en op basis van voor gedefinieerde dashboards en scripts.
- Identificeert false positives en meldt deze bij Detection Engineering.
- Voert de handelingen in runbooks uit om het alert te kunnen afhandelen.
- Identificeert tekortkomingen in runbooks en meldt deze bij Detection Engineering.

Het uitgangspunt is dat Tier 1 activiteiten op termijn geheel, of tenminste voor het overgrote deel geautomatiseerd afgehandeld worden. Getalenteerde Tier 1 Security Analisten worden geselecteerd om verder door te groeien binnen het SOC.

Input:

- Beheerrapportage uit de SOC-Mailbox.
- Externe bronnen zoals NCSC, beveiligingsupdate, (AV-)vendors etc.
- Security meldingen, -requests of incidenten uit call management.
- Security events, dashboards, scans, rapportages, werkinstructies van Tier 2 Security Analyst.
- Geregistreerde security incidenten vanuit de IT Service Management tooling.

Acties:

- Het monitoren van het SIEM en IDS systeem.
- Het afhandelen van security events naar securityincidenten op basis van vooraf gedefinieerde dashboards en scripts. Een Tier 1 Security Analyst werkt voornamelijk met werkinstructies en standaardoplossingen. Afwijkingen hierop worden doorgezet naar de Tier 2 Security Analyst.
- Terugkoppeling naar Tier 2 Security Analisten bij onvolledigheid van de werkinstructies.

Tier-2 Security Analyst

De primaire werkzaamheden van een Tier 2 Security Analyst bestaan uit een aantal onderdelen:

- Het identificeren van dreigingen voor de organisatie.
- Het maken van werkinstructies voor de Tier 1 Security Analyst.
- Het opvolgen van meldingen en security incidenten waarvoor geen standaardoplossing voorhanden is.
- Het adviseren van securitymanagement (via de SOC Lead).
- Het implementeren van logica in de SIEM tooling op basis van Use Cases.
- Het vaststellen van maatregelen om incidenten te kunnen isoleren.
- Identificeert mogelijkheden tot standaardisatie en nieuwe runbooks en belegt deze bij het juiste team.
- Uitvoeren van housekeeping taken.
- Beheer en onderhoud van de SOC-platformen waarbij nauw contact met de beherende partij is.



- Aansluiten en monitoring van logbronnen op SOC-platformen.
- Monitoring SOC-applicaties op verstoringen.
- Ontwikkeling van custom signatures en logconnectoren.
- Scripten en automatiseren van SOC-platformen.

De secundaire werkzaamheden van een Tier 2 Security Analyst bestaan uit een aantal onderdelen:

- Het ontwerpen en uitvoeren van kwetsbaarhedenanalyses (regelmatig).
- Het uitvoeren van penetratietesten (periodiek).

Primaire werkzaamheden

- Identificeren van dreigingen:
De Tier 2 Security Analyst richt zich op specifieke dreigingen die relevant zijn voor de gebruikersorganisatie. Deze dreigingen komen voort uit rapportages van externe partijen zoals CERT-diensten (NCSC), (AV-)vendoren en media. Maar ook van interne rapportages van beheerteams en securitymanagement. Een dreiging kan alles zijn wat de integriteit beschikbaarheid of vertrouwelijkheid van gegevens kan schaden, voornamelijk kwetsbaarheden en malware. De analyse van deze dreigingen vormt het dreigingsbeeld voor de organisatie. Het dreigingsbeeld levert input waarop gemonitord kan worden in de detectiesystemen in de organisatie. Dit komt te staan in de knowledge base van een SOC.
- Security incidenten en security meldingen:
De Tier 2 Security Analyst volgt securitymeldingen en security incidenten op die niet m.b.v. een werkinstructie door de Tier 1 Security Analyst kan worden opgelost. De Tier 2 Security Analyst onderzoekt de securitymelding/incident met behulp van het veiliggestelde materiaal. Het veiliggestelde materiaal kan van alles zijn. Dit materiaal bestaat vaak uit logfiles of malware. Met behulp van het dreigingsbeeld en het veiliggestelde materiaal kunnen zij de oorzaak onderzoeken en een impactanalyse bepalen. Vervolgens geven zij advies over de te nemen stappen aan de SOC Lead. De bevindingen worden gedocumenteerd en bijgehouden in een knowledge base.
- Actueel houden van de SIEM tooling op basis van dreigingsanalyses:
De Tier 2 Security Analyst draag zorg dat de SIEM tooling actueel blijft op basis van het dreigingsbeeld. Dit leidt bijvoorbeeld tot nieuwe dashboards binnen de SIEM tooling en verbeterde werkinstructies.

Input:

- SOC-management.
- Beheerrapportage uit de SOC-mailbox.
- Externe bronnen zoals NCSC, beveiligingsupdates, (AV-)vendors etc.
- Security meldingen, -requests of incidenten uit call management.

Acties:

- Het leveren van werkinstructies voor de Tier 1 Security Analyst.
- Het onderzoeken van securitymeldingen en security incidenten.
- De Tier 2 Security Analyst verzamelt en analyseert bewijsmateriaal om de oorzaak, reikwijdte en impact bepalen (quick-scan) van een security incident.
- De Tier 2 Security Analyst houdt het operationele contact met externe diensten, beheerteams en de melder.

Output:

- Een opgelost security melding of security incident.
- Een advies aan securitymanagement via de SOC Lead.
- SIEM monitoring content aansluitend bij dreigingen organisatie.
- Een analyse en bevindingen voor de knowledge-base.



- Gevraagd en ongevraagd advies aan de organisatie (via SOC Lead).
- Supervisie / ondersteuning van de Tier 1 Security Analyst.
- End-of-Week rapportage opleveren aan de SOC Lead ten behoeve van de interne organisatie.

Secundaire werkzaamheden

- Onderhoud van SOC applicatie- en systeembeheer en onderhoud van een of meerdere SOC-applicaties op de volgende gebieden:
 - health checks;
 - applicatie back-ups;
 - onderhoud certificaten;
 - installatie en updates van applicaties;
 - user beheer;
 - sensor tuning en onderhoud;
 - ontwikkeling van custom signatures en logconnectoren;
 - scripten en automatiseren van SOC-platformen;
 - aansluiten van logbronnen op SOC-platformen.
 - uitvoeren en analyseren van kwetsbaarhedenanalyses en penetratietesten.

De Tier 2 Security Analyst zoekt periodiek diep in de infrastructuur naar technische zwakheden. Zij maken hiervoor gebruik van kwetsbaarhedenanalyses en penetratietesten. Het doel van deze scans en testen is het rapporteren van kwetsbaarheden om te mitigeren zodat er een robuust systeem of infrastructuur ontstaat. Deze resultaten worden vervolgens door de Tier 2 Security Analyst geanalyseerd en omgezet in security problems, -meldingen of -incidenten.

Input:

- Beheerrapportage uit de SOC-mailbox.
- Externe bronnen NCSC, beveiligingsupdates, (AV-)vendors etc.
- Security meldingen, -requests of incidenten uit call management.
- Huidig dreigingsbeeld.
- Eigen onderzoek.

Acties:

- Richtlijnen geven aan de Tier 1 Security Analisten d.m.v. werkinstructies.
- Uitvoeren van maandelijkse kwetsbaarhedenanalyses.
- Uitvoeren van periodieke penetratietesten.
- Het implementeren van logica in de SIEM tooling op basis van vastgestelde use cases.
- Het veiligstellen van onderzoeksmateriaal.

Output:

- Rapportages van penetratietesten en kwetsbaarhedenanalyses.
- Werkinstructies en dashboards voor het monitoren op security issues voor de Tier 1 Security Analyst.
- Een analyse en bevindingen voor de knowledge base.
- Gevraagd en ongevraagd advies aan de organisatie (via SOC Lead).

Tier-3 Security Analyst

De Tier 3 Security Analyst is een rol welke verdieping geeft op de Level 2 Security Analyst. Een Tier 3 Security Analyst is kennishouder van één of meerdere producten en processen binnen een SOC. Hij is richtinggevend en stemt dit af met de SOC Lead. De dagelijkse werkzaamheden van een Tier 3 Security Analyst bestaat uit o.a.:

- Het opvolgen van meldingen en security incidenten.
- Begeleiden en geven van richtlijnen aan A&P testen.



- Het begeleiden en uitvoeren van forensisch digitaal onderzoek.
- Dreigingsbeeld voor de organisatie vertalen naar nieuwe use cases.
- Gevraagd en ongevraagd advies aan SOC Lead.
- Op verzoek van bevoegd gezag ondersteunen van integriteitsonderzoeken.
- Meewerken aan organisatie overstijgende expertgroepen.
- Het aansturen van externe partijen t.b.v. onderzoek.

Input:

- Security events, logfiles.
- Monitoring tool SIEM.
- Huidige dreigingsbeeld.
- Eigen onderzoek.

Acties:

- Het bepalen van het actuele dreigingsbeeld voor de organisatie.
- Modeleren van de te beschermen infrastructuur.
- Onderzoek verbeteringen SOC-platformen.
- Organiseren van use case workshops.

Output:

- Een dreigingsbeeld voor de organisatie.
- Gevraagd en ongevraagd advies aan SOC Lead.
- Supervisie/Ondersteuning van Level 2 Security Analyst.
- Product-, proces- en functie-ontwikkeling binnen zijn kennisgebied.
- Nieuwe use cases voor de monitoringplatformen van een SOC.

Primaire werkzaamheden

- Advies implementaties van BIR/VIRBI;
De Tier 3 Security Analyst geeft gevraagd en ongevraagd advies aan de organisatie over de (technische) implementatie van Baseline Informatiebeveiliging Rijksdienst TNK/OB, VIR-BI en ISO-normen (ISO27001/27002) op basis van het dreigingsbeeld voor de organisatie. Dit advies loopt via de SOC Lead.
- Begeleiden van forensisch onderzoek;
Deze functie wordt ingezet bij een groot security incident waarbij verregaand onderzoek noodzakelijk is. Denk hierbij aan langdurige diepe infiltratie in het netwerk. Hierbij wordt altijd een opsporingsambtenaar ingeschakeld en of een (externe) derde partij waar de Tier 3 Security Analyst mee samenwerkt. Zij vergaren het bewijsmateriaal en geven dit af aan de onderzoek partij. Ook kan deze functie worden ingezet om Indicators of Compromise (IoC's) te onderzoeken van kwaadaardige software binnen het netwerk om hiermee logica te ontwikkelen voor het SIEM middels het Threat Intelligence Platform (TIP).
- Deelname aan CSIRT;
Level 3 Security Analisten maken deel uit van het CSIRT bij een security incident met hoge impact. Daarbij maken zij gebruik van Level 2 Security Analisten waar nodig.
- Ontwikkeling SOC;
Uitbouwen van de informele contacten van een SOC (intern, departementaal of interdepartementaal of extern). Kennisuitwisseling onderhouden tussen interne, departementaal of interdepartementaal of externe partijen.
- Bepalen van dreigingsbeeld;
Identificeren van dreigingen die van toepassing zijn op de organisatie. Participeren in projecten om het actuele dreigingsbeeld in te brengen als adviseur als dit noodzakelijk is. SOC-medewerkers zijn geen vaste projectmedewerkers om security by design in te richten.
- Invulling van expert rol;



In dit geval is de Tier 3 Security Analyst een expert in SOC-kennisgebied. De expert is de sparringpartner binnen het SOC voor alle andere Security Analysten. De expert zorgt ervoor dat zijn kennis m.b.t. het kennisgebied up-to-date blijft.

Naast de tiers zijn in de figuur ook de Detection Engineering en Automation Engineering rollen weergegeven. Deze hebben een bijzondere rol in het tiering-systeem.

Detection Engineering:

- Ontvangt feedback van de verschillende tiers over usecases (detecties) Standard Operating Procedures (SOP's) en gebruikt de feedback om verbeteringen door te voeren.
- Ontwikkelt nieuwe use cases en SOP's en houdt deze actueel.
- Communiceert wijzigingen aan detectieregels en implementatie van nieuwe detectieregels aan de analisten.

Automation Engineering:

- Analyseert en identificeert mogelijkheden voor automatisering.
- Zet SOP's om in automation playbooks, met daarbij behorende automatisering.
- Automatiseert playbooks en alert afhandeling. De triggers voor automatiseren van playbooks zijn: veelgebruikte niet-geautomatiseerde playbooks, playbooks reviewen, nieuwe SOP's.

Best Practices voor inrichting

Bij de inrichting van tiering gelden de volgende principes en uitgangspunten:

- Er wordt zoveel mogelijk afgehandeld door middel van **automatisering** (tier-0) en **playbooks** binnen tier-1. Op deze manier kan een hoge efficiëntie binnen het SOC bereikt worden.
- **Shift left** is van toepassing: waar mogelijk worden werkzaamheden overgedragen van hogere naar lagere tiers. Dit gebeurt via standaardisatie, nieuwe en uitgebreide SOP's en toepassen van automatisering.
- De **shift lead** is verantwoordelijk voor de beslissingen binnen tier-1. De shift lead wordt geleverd uit tier-2 (medior analisten). De shift lead is ook het aanspreekpunt vanuit tier-2 en tier-3 wanneer het gaat om de inhoud van in tier-1 gedane analyses.
- **Escalatie en verificatie** naar hoger gelegen tiers vanuit tier-0 geschiedt via de shift lead.
- **Events met hoge prioriteit** gaan direct naar tier-2 voor verdere analyse en opvolging. Welke events dat exact zijn moet vastgesteld bij de voortbrenging van de use case.

Best Practices voor uitvoering

Voor de operatie is het van belang om zorg te dragen dat *shift left* en het bijbehorende feedbackmechanisme goed werkt. Dit kan gecontroleerd worden door te kijken naar het proces van [continue verbetering](#) wat geoperationaliseerd is binnen het SOC. Binnen dit proces behoren activiteiten te zijn die zorg dragen voor automatisering, standaardisering en afhandeling van events in lagere tiers.

6.3

Peoplemanagement

Het doel van People management is zorgdragen dat medewerkers van het SOC zo goed mogelijk kunnen functioneren binnen het SOC. Dit gedeelte van het SOC-CMM kent een grote overlap met bestaande HR-processen. In veel gevallen is er sprake van een implementatie van deze standaard processen binnen het SOC.

Daarbij dient de aandacht uit te gaan naar de volgende zaken.



- Het creëren van een veilige cultuur voor medewerkers waar men op een transparante en respectvolle manier met elkaar omgaat.
- Het vaststellen van diversiteitsdoelstelling. Deze diversiteitsdoelstellingen kunnen op verschillende manieren vormgegeven worden. Genderdiversiteit, etnische en culturele diversiteit en neurodiversiteit zijn daar voorbeelden van;
- Screening van nieuwe personeelsleden en het hebben van een vast proces voor het inwerken en begeleiden van nieuwe personeelsleden.
- Het vaststellen van doelstellingen voor het team. Daarbij geldt dat deze teamdoelstellingen aanvullend zijn op de persoonlijke doelstellingen. De teamdoelstellingen laten medewerkers bijdragen aan het grotere geheel en bevorderen de samenwerking binnen het SOC.
- Het meten en verbeteren van tevredenheid voor het SOC-medewerkers. Dit is een belangrijk onderdeel van het behoud van personeel, alsmede het identificeren van tekortkomingen in verantwoordelijkheden, processen en procedures.
- *Job rotation* kan toegepast worden binnen het SOC om medewerkers kennis te laten vergaren van de verschillende aspecten binnen het SOC. Het kan daarmee een middel zijn om tekortkomingen in de kennismatrix te verminderen. Daarbij moet rekening gehouden worden met het feit dat *job rotation* in eerste instantie voor een lagere productiviteit van het team zal zorgen. In een tiered model kan dit problemen opleveren.
- In sommige gevallen kan sprake zijn van een multi-team systeem. Bijvoorbeeld wanneer de organisatie een separaat SOC en CSIRT-team kent. In een dergelijk geval is het van belang om oefeningen en teambuilding over het gehele multi-team systeem te organiseren zodat samenwerking tussen de teams geoptimaliseerd wordt.

Best Practices voor inrichting

Bij de inrichting van Peoplemanagement binnen het SOC is het met name van belang zoveel mogelijk gebruik te maken van de middelen die al bestaan binnen het reguliere HR-proces in de organisatie. Uiteraard kan afgeweken worden van de reguliere processen indien deze in de ogen van het SOC onvoldoende effectief zijn om personeelsleden te behouden en verder te laten groeien.



Best Practices voor uitvoering

Voor de operatie is het met name van belang dat de effectiviteit van de HR-processen gemonitord wordt. De medewerkerstevredenheid is daarbij een goed meetinstrument, maar ook het gemiddeld personeelsverloop geeft een goede indicatie van hoe de organisatie, en in het bijzonder het SOC, het doet als werkgever.

6.4 Kennismanagement

Kennismanagement is een belangrijk onderwerp binnen het SOC. Goede uitwisseling en opbouw van kennis is essentieel voor kwalitatief hoogwaardige dienstverlening. Daarnaast is het opbouwen en uitwisselen ook onderdeel van het behoud van medewerkers. Het doel van SOC rondom kennismanagement gaat verder dan alleen het implementeren van een proces met technologie. De doelstelling moet zijn om een cultuur van actieve kennisuitwisseling te creëren. Daarbij hoort ook dat medewerkers actief van elkaar leren tijdens de dagelijkse werkzaamheden.

6.4.1.1 Kennissessies

Om kennisuitwisseling te faciliteren en te stimuleren zijn verschillende sessies mogelijk voor het SOC:

- **Weekstart**, waarin een vooruitzicht voor de komende week gegeven wordt
- **Dagelijkse stand-ups** waarin de laatste inzichten en dreigingen besproken worden.
- **Security topics**. Kennismeetings waarin een bepaald onderwerp uitgelicht wordt. Dat kan een actueel security onderwerp zijn, maar ook meer gericht op de toekomst. Door deze sessies te combineren met een lunch kan een wat meer informeel karakter verkregen worden. Tegelijkertijd zijn dit soort sessies ondersteunend voor het teamgevoel.
- **Lessons-learned events**. Dit zijn kennissessies waarin inzichten uit incidenten en analyses gedeeld worden.
- **Post-training events**. Dit zijn kennissessies waarin een medewerker die een training afgerond de belangrijkste zaken uit de training, workshops of conferentie aan het team meegeeft.

Buiten deze georganiseerde sessies zijn ook kleinschalige sessies, bijvoorbeeld binnen een team, mogelijk. Het initiatief daarvoor kan binnen het team liggen. Dat moet ook zoveel mogelijk gestimuleerd worden.

6.4.1.2 Techniek

Kennis wordt zoveel mogelijk vastgelegd in documenten of als toevoegingen aan de kennisbankomgeving van het SOC. Voorbeelden van kennisdocumenten zijn de SOC-processen, werkinstructies en SOP's. In veel SOC's die op een agile manier werken wordt kennis vastgelegd in een kennissysteem (wiki). Een dergelijk systeem is meer dynamisch dan een filescharing omgeving met documenten.

6.4.1.3 Matrices

Voor het vastleggen van kennis worden kennis- en kundematrices gebruikt. In deze matrices wordt vastgelegd welke kennis en kunde noodzakelijk is voor het SOC om op goede wijze te kunnen functioneren. Daarnaast wordt in kaart gebracht welke medewerkers beschikken over deze kennis en kunde en op welk niveau (beginner, gemiddeld, expert). Op deze manier heeft het SOC een actueel inzicht in de verdeling van de kennis en kunnen plekken waar kennis niet goed verdeeld is actief aangepakt worden. Zo kunnen single points of knowledge vermeden en geadresseerd worden en de continuïteit van het SOC geborgd blijven.

Naast interne kennisuitwisseling kan ook sprake zijn van kennisuitwisseling tussen de organisatie en externe partners. Deze kennisuitwisseling staat meestal in het teken



van uitwisseling rondom incidenten en dreigingen en is daarmee onderdeel van de threat intelligence functie van het SOC. De correcte toepassing van het Traffic Light Protocol is essentieel bij kennisuitwisseling met externe partners.

Best Practices voor inrichting

Bij de inrichting van het kennismanagementproces is het met name van belang de afwegingen te maken die leiden tot het realiseren van de gewenste cultuur rondom kennisuitwisseling. Daar is eigen initiatief van medewerkers op dit gebied een belangrijk onderdeel van. Dat kan gestimuleerd worden door het bieden van een goede structuur (regelmaat van sessies), het maken van afspraken en het toekennen van verantwoordelijkheden binnen het team op het gebied van kennismanagement.

Wat betreft het inrichten van het platform is het van belang een goede structuur aan te brengen voor de documentatie. Het is hierbij mogelijk om de structuur van het SOC-CMM model aan te houden en per onderdeel de juiste documentatie te verzamelen.

Best Practices voor uitvoering

Voor de operatie is belangrijk om zorg te dragen dat de sessies consistent worden uitgevoerd. Omdat kennismanagement geen primaire taak is van het SOC, kan het zijn dat de sessies minder prioriteit krijgen dan andere operationele taken. Om continuïteit in kennisuitwisseling te behouden is het daarom essentieel om voldoende prioriteit aan deze sessies toe te kennen.

Indien een dynamisch kennismanagement platform gebruikt wordt (zoals een wiki) is het van belang te waken dat de beschrijving van de processen niet langzaam steeds verder afwijkt van het goedgekeurde proces.

6.5 Training en certificering

Sterk gelieerd aan kennismanagement is het opbouwen en verder ontwikkelen van kennis en kunde van medewerkers van het SOC. Training en certificering spelen daarbij een belangrijke rol. Trainingen kunnen gebruikt worden om geïdentificeerde tekortkomingen in kennis actief te adresseren. Trainingen dragen ook bij aan behoud van personeel, omdat SOC-medewerkers zich op deze manier verder kunnen ontwikkelen. Certificering is, als aanvulling op training, ook belangrijk omdat het een zeker niveau van kennis en kunde bij het personeel onafhankelijk aantoonbaar maakt.

Training en certificering kan objectief bijdragen aan kennisontwikkeling, de persoonlijke doelstelling van een medewerker en zijn of haar carrière pad. Training en certificering is daarmee gekoppeld aan de volgende aspecten van het SOC-CMM:

- **Medewerkers.** Het kunnen volgen van training geeft voldoening en draagt daarom bij aan het aantrekken en behouden van talent.
- **Rollen & hiërarchie.** Rolbeschrijvingen dienen verplichte en optionele trainingen te omvatten.
- **Peoplemanagement.** Trainingen dragen bij aan de ontwikkeling van de medewerker.
- **Kennismanagement.** Training is onderdeel van kennisontwikkeling, en kan ook gericht gebruikt worden om tekortkomingen in de kennismatrix te adresseren

Naast inhoudelijke trainingen is het ook belangrijk om aandacht voor de persoonlijke vaardigheden van SOC-medewerkers (soft skills) te hebben. Soft skills zijn onderdeel van de kennis- en kunde matrices en worden ook meegenomen in het trainingsprogramma.



Best Practices voor inrichting

Tijdens de inrichting van het SOC wordt een training en certificering programma ingericht. Deze programma's worden gebaseerd op een analyse van de benodigde kennis en kunde binnen het SOC. Dat komt dan weer voort uit de beoogde dienstencatalogus, die opgesteld is als onderdeel van het SOC Charter. Daarbij worden verplichte training en optionele trainingen onderscheiden. Belangrijk daarbij is een evenwichtige verdeling van trainingen voor de verschillende rollen die binnen het SOC gevoerd worden. Daarnaast dient een goed aanbod van trainingen op inhoudelijke kennis en training voor de ontwikkeling van vaardigheden (*soft skills*) onderdeel zijn van het programma. Tenslotte is onderdeel van de inrichting en bepalen en reserveren van voldoende budget en uren voor training en (voorbereiding op) certificering bovenop het centrale opleidingsbudget van de organisatie. In Annex C: Trainingsplan staat een voorbeeld van een opleidingsplan.

Best Practices voor uitvoering

Tijdens de operatie moet met regelmaat geëvalueerd worden of het aanbod van trainingen en certificeringen nog passend is voor het SOC. Daarbij moet ook gekeken worden of de optionele trainingen nog steeds als optioneel worden gezien, of dat deze inmiddels als verplicht worden ervaren. Tenslotte moet het aanbod van trainingen doorlopen worden om te zien of nieuwe trainingen beschikbaar zijn die van toegevoegde waarde kunnen zijn voor het SOC. Belangrijk is dat de trainingen worden gebruikt voor ontwikkeling van het personeel, maar ook om actief tekortkomingen in de kennismatrix te dichten.

7 Process domein

Het procesdomein beschrijft een aantal generieke processen die ondersteunend zijn aan de diensten van het SOC.

7.1 SOC-management

Onder SOC-management wordt verstaan: de activiteiten die worden uitgevoerd om het SOC zelf en het ecosysteem waar het SOC in functioneert te beheersen. Deze activiteit heeft een relatie met SOC governance, maar is specifiek gericht op activiteiten binnen het SOC.

Onderstaande tabel is een weergave van de elementen uit het SOC-CMM die benoemd zijn voor SOC-management en hoe dit geïmplementeerd is in het SOC.

Element	Toelichting
Intern relatiemanagement	Intern relatiemanagement is het opbouwen en uitbouwen van relaties binnen de organisatie. Dit is met name van belang in grotere organisaties. Deze relaties zijn onder andere van belang voor het kunnen maken van goede afspraken, soepele uitrol van diensten over de organisatie, goede escalatie, sturing op performance, etc.
Extern relatiemanagement	Extern relatiemanagement is het opbouwen en uitbouwen van relaties buiten de organisaties. Dat kunnen andere SOC's zijn waarmee samengewerkt wordt, Het Nationaal Cyber Security Center (NCSC) een community voor het uitwisselen van threat intelligence en Best Practices, en andere externe initiatieven voor samenwerking.
Vendormanagement	Vendormanagement is het actief aangaan van relaties met partijen die software, hardware, of licenties leveren waar SOC-technologie en de daaraan gekoppelde dienstverlening mee gerealiseerd wordt. Dit is belangrijk, zodat het SOC goed in staat is om mee te bewegen met de technologische trends.
Project methodologie	Het hebben van een project methodologie is essentieel om grotere projecten binnen het SOC (zoals het implementeren van een nieuwe technologie) succesvol te laten verlopen. De gekozen methodologie moet aansluiten bij de rest van de organisatie.
Procesdocumentatie en diagrammen	Het SOC omvat vele procesbeschrijvingen en andere vormen van documentatie en diagrammen. Het is noodzakelijk om deze documentatie accuraat en up-to-date te houden. Dat vereist actief documentation management en goede afspraken binnen het SOC.



Element	Toelichting
RACI-tabel	Binnen SOC-management valt het opstellen en beheren van de RACI-tabel. Hierin wordt aangegeven welke verantwoordelijkheden bestaan voor het SOC en voor de rest van de organisatie. De RACI-tabel kan ook opgenomen worden in het charter, zodat het direct op het hogere managementniveau bekrachtigd kan worden. In de praktijk zullen meerdere matrices gebruikt worden binnen het SOC: een RACI-tabel op hoog niveau, en gedetailleerde matrices op het niveau van technologie en diensten. RACI-tabellen zijn met name belangrijk waar teams samen werken om tot een resultaat te komen. Dat kan bijvoorbeeld het geval zijn bij beheer en optimalisatie van tooling, of bij een proces waar meerdere teams bij betrokken zijn zoals vulnerability management.
Dienstencatalogus	De dienstencatalogus is een communicatiemiddel naar de organisatie waarin uitgewerkt wordt wat men van het SOC mag verwachten. De dienstencatalogus kan in versimpelde vorm onderdeel zijn van het charter.
Onboarding procedure	Onboarding procedures zijn belangrijk om zorg te dragen dat teams en afdelingen goed aangesloten kunnen worden op de diensten van het SOC. Of dat het nieuwe SOC-dienst goed uitgerold kan worden binnen de organisatie.
Off-loading procedure	Service off-loading (of off-boarding) is met name van belang in de MSSP-context, om zorg te dragen dat een klant die weggaat goed uit de processen en systemen verwijderd wordt. Bij een intern SOC is dit niet zo van belang.
<i>Continuous improvement</i>	Continue verbeteren heeft als doel om zorg te dragen dat de dienstverlening van het SOC steeds verder verbeterd en geoptimaliseerd wordt. Dit onderwerp wordt hierna in meer detail beschreven.
Kwaliteitscontrole	Kwaliteitscontrole heeft als doel om zorg te dragen dat de kwaliteit van de output van het SOC gemonitord en geborgd wordt. Dit onderwerp wordt hierna in meer detail beschreven.

7.1.1

Continuous improvement

Om te zorgen dat het SOC Security Operations op een moderne manier uitvoert is continue verbeteren, optimaliseren en innoveren van groot belang. Belangrijke punten hierbij zijn:

- **Continuous tuning.** Dit is het proces van continu werken aan het optimaliseren van de set aan detectie regels die het SOC heeft (monitoring ruleset).
- **Continuous automation.** Om de groeiende hoeveelheid werk het hoofd te kunnen bieden en tegelijkertijd het werk interessant te houden voor de medewerkers van het SOC wordt *continuous automation* toegepast. Slimme toepassing van automatisering wil zeggen dat automatisering daar toegepast wordt waar de baten het hoogst zijn en in verhouding zijn tot de kosten (benodigde tijd). Deze verbeteringen kunnen inzichtelijk gemaakt worden door per uitgevoerde automatisering te meten hoeveel tijd daarmee bespaard is.

- **Continuous measurement.** De performance van het SOC wordt op een aantal punten continu gemeten. Deze informatie wordt gebruikt om de dienstverlening en de toewijzing van resources te optimaliseren. Voor deze metingen zijn Key Performance Indicators (KPIs) gedefinieerd en vastgelegd.
- **Capacity for change.** Belangrijk bij continu verbeteren is het reserveren van *capacity for change*; personele capaciteit om te werken aan verbeteringen en veranderingen. Door het verbeteren te prioriteren naast het reguliere werk kan zorggedragen worden dat er ook echt een continue cyclus van verbeteringen ontstaat. Het is dus belangrijk om een vaste hoeveelheid capaciteit te reserveren. Deze capaciteit moet realistisch zijn. Dat wil zeggen: de capaciteit moet ook daadwerkelijk benut kunnen worden. Wanneer een SOC meer werk heeft dan het aankan, is er eigenlijk geen ruimte voor verbetering. Door in zulke gevallen toch een vaste hoeveelheid tijd te reserveren voor verbetering, kan gewerkt worden aan structurele oplossingen voor het probleem. Daarbij zullen keuzes gemaakt moeten worden omdat niet al het operationele werk meer opgepakt kan worden.

Een Continuous Improvement aanpak is meestal gestoeld op een agile werkwijze, bijvoorbeeld met een Kanban-methodiek. Welke werkwijze exact wordt toegepast is van minder groot belang. Deze methodiek kenmerkt zich als volgt:

- **Minimale overhead.** Het proces is zo ingericht dat de overhead van agile werken minimaal is. De essentiële activiteiten (planning en *refinement*) vinden plaats op een geoptimaliseerde manier.
- **Duidelijke taken.** Taken worden pas opgepakt als voor de teamleden duidelijk is wat het beoogde resultaat is en wanneer het resultaat behaald is. Daarvoor worden een *definition of ready* en een *definition of done* gehanteerd.
- **Dagelijkse sturing.** Dagelijks wordt bekeken wat de voortgang is van de items. Blokkerende problemen of hulpvragen worden daar behandeld.
- **Transparantie.** Iedereen binnen het team weet waar de ander aan werkt.
- **Eigenaarschap.** Ieder teamlid dat een taak oppakt neemt eigenaarschap voor de taak en zorgt voor een tijdige en kwalitatief goede afronding van de taak. Waar nodig kan de taak worden overgedragen aan een teamlid.
- **Alignment met de organisatie.** Er wordt gezocht naar een goede alignment met Continuous Improvement initiatieven elders in de organisatie.
- **Gebruik van KPI's voor sturing.** KPI's worden gebruikt om de performance binnen het agile proces te meten en te verhogen (*velocity*).

7.1.2

Quality assurance

Voor het SOC is het van groot belang om de kwaliteit van de dienstverlening goed te borgen. Deze kwaliteit wordt op de volgende manier bewaakt:

- **Door middel van KPI's.** Een aantal KPI's is gedefinieerd om de kwaliteit van de verschillende diensten in kaart te brengen. Daarnaast worden KPI's ook gebruikt om prioritering te geven aan verbeterinitiatieven. Wanneer doelwaarden voor KPI's niet gehaald worden vindt altijd een analyse plaats om vast te stellen waarom het doelwaarde niet gehaald is, en wat er gedaan kan worden om de waarde wel te halen. De analyse komt als verbeterinitiatief terug in de agile methodiek. Belangrijk is ook dat nu afronding van de verbetering nagegaan wordt dat deze inderdaad het gewenste effect heeft gehad.
- **Door middel van peer review.** Opgeleverde producten (documentatie, use cases, etc.) worden door middel van peer review gecontroleerd. Zo worden fouten zoveel mogelijk voorkomen.
- **Door middel van reguliere controle.** Opgeleverde producten (documentatie, use cases, etc.) verouderen en dienen met regelmaat opnieuw beoordeeld te worden zodat deze actueel blijven.

- **Door middel van steekproeven.** Een deel van de alerts wordt door senior analisten gecontroleerd om vast te stellen of deze goed beoordeeld zijn. Hierin vindt ook een stuk kennisoverdracht plaats.
- **Door middel van laagdrempelig collegiaal overleg.** Bij twijfel over te nemen beslissingen kan collegiaal overleg plaatsvinden. Dan kan in samenspraak de juiste vervolgactie ingezet worden.
- **Voldoende tijd** om de beoogde kwaliteit te kunnen leveren. Monitoring hierop zou je ook vanuit continuous improvement willen doen).
- **(Ruimte voor) plezier** in het werk met collega's. Werkplezier draagt bij aan de intrinsieke motivatie om het werk (goed) te doen en er te zijn wanneer het nodig is.

De output van het *quality assurance* proces wordt gebruikt om verbeteringen door te voeren. Veelal zullen dit verbeteringen binnen het SOC zijn, maar het kan ook verbeteringen betreffen in procesinterfaces tussen het SOC en andere teams.

Best Practices voor inrichting

SOC-managementomvat een groot aantal onderwerpen. Bij het inrichten van het SOC is het belangrijk om na te gaan welke onderwerpen in eerste instantie relevant zijn voor het SOC. Deze onderwerpen worden als eerste ingericht. Andere onderwerpen volgen daarna zodra deze zich aandienen. De belangrijkste onderwerpen voor een startend SOC zijn:

- Het afbakenen van verantwoordelijkheden met RACI-matrices.
- Het definiëren van diensten met een dienstencatalogus.
- Het inrichten van *Continuous Improvement* als drijvende kracht voor verbetering en verhoging van volwassenheid.
- Het inrichten van *quality assurance* om zorg te dragen dat de diensten die geleverd worden ook van voldoende kwaliteit zijn.

Best Practices voor uitvoering

Tijdens de operatie is het belangrijk om met regelmaat de performance van de verschillende sub-processen binnen SOC-management te evalueren. Daarbij wordt gebruikt gemaakt van metingen en gedefinieerde KPI's. Deze informatie kan gebruikt worden om de processen verder te optimaliseren.

7.2 SOC-operations en faciliteiten

Het onderwerp SOC-operations en faciliteiten behandelt de zaken die ingericht zijn rondom het draaien en optimaliseren van de operatie en de fysieke faciliteiten die beschikbaar zijn voor het SOC om de werkzaamheden uit te voeren.

7.2.1 Openingstijden en bereikbaarheid

Het moet voor de organisatie duidelijk zijn wat men van het SOC kan verwachten wat betreft openingstijden, en bereikbaarheid. Ook de reactietijden van het SOC moeten duidelijk zijn voor de organisatie.

Bereikbaarheid kan op verschillende manieren ingericht worden:

- Door 24/7 aanwezig te zijn op het SOC
- Door tijdens kantooruren aanwezig te zijn en daar buiten stand-by te zijn
- Door alleen tijdens kantooruren aanwezig te zijn

Welke vorm het meest passend is voor het SOC, is onder andere afhankelijk van ambities, strategie en verwachtingen van de organisatie en het huidige dreigingsbeeld. Veel organisaties kiezen voor een oplossing met bezetting op kantooortijden en stand-by buiten kantooortijden. Deze oplossing zorgt wel voor 24/7 monitoring, zonder de kosten en personele impact die een volledige 24/7 bezetting met zich meeneemt. Het is wel belangrijk om 24/7 binnen kritieke delen van de gehele organisatie te hebben, zodat de juiste medewerkers (beheerders, managers, etc.) ook



beschikbaar zijn om escalaties op te volgen buiten kantoortijden. Hierbij moet ook rekening gehouden worden met de geldende ARBO-wetgeving.

7.2.1.1 Fysieke aanwezigheid

Fysieke aanwezigheid op locatie is niet noodzakelijk om bereikbaar te zijn. Indien dat wel het geval is, is het nodig om een rooster op te stellen zodat altijd er een bezetting op het SOC is. Hierbij moet uiteraard rekening gehouden worden met interne reglementen.

7.2.1.2 Shifts en stand-by

Afhankelijk van de keuzes die gemaakt worden voor openingstijden en stand-by kunnen *shifts* noodzakelijk zijn in het SOC. Het doel van een *shift* is om zorg te dragen voor continuïteit van de 1^e-lijns operationele werkzaamheden. Voorbeelden van die werkzaamheden zijn:

- Het afhandelen van tickets
- Het afhandelen van e-mails en verzoeken
- Het uitvoeren van triage en doorzetten van potentiële incidenten
- Het uitvoeren van controles of andere herhalende taken

Het is daarbij wel noodzakelijk dat er ook escalatie mogelijkheden zijn naar de 2^e en 3^e lijn, en zo nodig SOC-management.

Aan het einde van een *shift* wordt altijd een overdracht uitgevoerd. Daarbij worden openstaande zaken en bijzonderheden overgedragen zodat deze verder opgevolgd of afgehandeld kunnen worden. Het vastleggen van deze bijzonderheden in een *shift log* zorgt ervoor dat op een gestructureerde manier gewerkt wordt en geen zaken over het hoofd worden gezien.

Ook bij stand-by is het noodzakelijk om *shifts* te gebruiken. Op deze manier wordt de stand-by medewerker goed geïnformeerd over de lopende zaken binnen het SOC. Ook wordt de *shift* van de volgende dag weer geïnformeerd door de stand-by medewerker over bijzonderheden buiten kantoortijden. Het spreekt voor zich dat de stand-by zich niet bezighoudt met operationele werkzaamheden met lage prioriteit, maar dat deze alleen de afhandeling van belangrijke alerts op zich neemt.

Het inrichten van een stand-by moet altijd gedaan worden in overeenstemming met wettelijke kaders en interne reglementen. Denk daarbij ook aan afstemming met de Ondernemingsraad. Belangrijk daarbij is dat duidelijk is wat de verwachtingen zijn aan de medewerker die stand-by loopt en dat de belasting van de stand-by binnen acceptabele grenzen is. Onderdeel daarvan is goed onderbouwde keuzes maken over welke alerts voldoende belangrijk zijn om buiten werktijden direct op te laten volgen. Daarnaast is het belangrijk om afspraken te maken over werktijden tijdens een stand-by week. Een voorbeeld van een dergelijke afspraak is dat de medewerker, als deze in de nacht werkzaamheden heeft moeten verrichten, later kan beginnen. Tenslotte is het ook mogelijk om een dubbele stand-by in te regelen. In een dergelijk geval is er een senior medewerker als tweede stand-by die ondersteuning kan bieden indien de eerste stand-by een escalatiemogelijkheid nodig heeft. Met een dubbele stand-by kan gezorgd worden dat altijd voldoende senioriteit en kennis van verschillende disciplines binnen het SOC aanwezig is.

Tenslotte is het voor stand-by belangrijk om een betrouwbaar notificatie systeem in te richten. Het systeem moet kunnen garanderen dat een bericht afgeleverd is, bij voorkeur met een ontvangstbevestiging door de medewerker die stand-by loopt, wanneer meerdere medewerkers stand-by loopt maak dan een keuze wie de ontvangstbevestiging verstuurd.

7.2.2

Standaardisering

Voor het verhogen van de efficiëntie binnen het SOC is het noodzakelijk om werkzaamheden te standaardiseren. Dat kan bijvoorbeeld door het toepassen van workflows of Standard Operating Procedures. Op deze manier kan gezorgd worden dat het resultaat van de werkzaamheden voorspelbaar en betrouwbaar is. Standaardisering is daarmee onderdeel van kwaliteitsmanagement binnen het SOC. Ook is standaardisering de basis die nodig is voor automatisering van dergelijke taken en handelingen.

Een ander onderdeel van standaardisering is het uitvoeren van dagelijkse stand-ups. In veel gevallen wordt daarvoor een dagstart gebruikt. Andere SOC's hanteren een dageinde, of zelfs beide. Deze stand-ups worden ook gestandaardiseerd met een vaste agenda, en ook een vaste hoeveelheid tijd die gebruikt mag worden. Op deze manier wordt voorkomen dat stand-ups steeds langer duren. De overdracht van een shift kan samenvallen met de stand-up, maar dit is niet noodzakelijk dit kan ook middels een shift-log.

7.2.3

Oefeningen

Oefeningen zijn noodzakelijk om de medewerkers binnen het SOC scherp te houden en voor te bereiden op daadwerkelijke incidenten. Daarvoor kunnen verschillende typen oefeningen ingezet worden, waaronder:

- **Table topoefeningen.** Hierbij wordt een scenario op papier doorlopen om vast te stellen of incident respons op een juiste manier verloopt.
- **Cyber ranges.** Hierbij wordt een simulatie uitgevoerd waarbij in een technische omgeving een incident wordt nagebootst. Het is mogelijk om daarbij een generieke simulatie te gebruiken, of een simulatie die is geconfigureerd conform die eigen infrastructuur.
- **Capture the flag (CTF) events.** Dit zijn oefeningen waarbij er met name gewerkt wordt aan hunting en analyse skills binnen het SOC. Ze bevatten vaak diverse challenges, behorend tot verschillende categorieën, zoals Forensics, Malware, Hacking of OSINT.
- **Red team oefeningen.** Bij red team oefeningen wordt een aanval uitgevoerd op de organisatie, waarbij het aanvallende team (red team) ook daadwerkelijk probeert in te breken en een aantal activiteiten (red flags) uit te voeren, zoals het overnemen van een domain admin account. Bij een red team oefening worden preventie, detectie en respons getest op een zo realistisch mogelijke manier. Hierbij kan gebruik gemaakt worden van standaard methodologieën, zoals ART (Advanced Red Teaming) ^[10] en TIBER (Threat Intel Based Ethical Redteaming) ^[11].

Oefeningen kunnen intern georganiseerd worden. Het is echter ook mogelijk om te participeren in publieke oefeningen, waarin samen met andere organisaties geoefend wordt. Bij dergelijke oefeningen kan ook van andere organisaties geleerd worden. Een aantal van deze oefeningen en/of testen kunnen ook als purple teaming sessie worden uitgevoerd.

De organisatie moet een keuze maken over de frequentie van oefenen, het type oefeningen en of wel of niet geparticipeerd wordt in publieke oefeningen. Deze keuzes resulteren in een oefenkalender voor het SOC waarin de planning voor oefeningen in dat jaar vastgelegd wordt.

¹⁰ <https://www.dnb.nl/en/sector-information/cash-and-payment-systems/dnb-oversees-cyber-resilience-tests/advanced-red-teaming-art/>

¹¹ <https://www.dnb.nl/voor-de-sector/betalingsverkeer/begeleiding-cyberweerbaarheidstesten-door-dnb/threat-intelligence-based-ethical-red-teaming-tiber/>



Tenslotte is het belangrijk dat oefeningen goed opgevolgd worden. Elke oefening zal waardevolle bevindingen opleveren voor het verder verbeteren van het SOC. Deze bevindingen moeten gestructureerd opgevolgd worden binnen het *Continuous Improvement* proces.

7.2.4 SOC Operations - Faciliteiten

Fysieke faciliteiten in het SOC zijn noodzakelijk om SOC-medewerkers op een efficiënte manier te laten werken. Tot de fysieke faciliteiten van het SOC kunnen behoren:

- Een fysieke ruimte met werkstations. Deze werkstations zijn voorzien van grote schermen waar analisten hun analyse werk kunnen uitvoeren.
- Een *videowall* met schermen waarop relevante en actuele informatie getoond wordt.
- Een aparte vergaderruimte voorzien van teleconferencing mogelijkheden voor het houden van vergaderingen. Deze ruimte kan ook fungeren als *war room* in geval van grote incidenten.
- Een aparte lab ruimte waar onderzoeken kunnen plaatsvinden. Deze ruimte wordt tevens gebruikt voor opslag van systemen, zoals forensische hardware.
- Een kaartlezer gecombineerd met biometrie, eventueel een tourniquet om *tailgating* te voorkomen die zorg draagt dat alleen geautoriseerde personen toegang kunnen krijgen tot het SOC.
- Een SOC-infrastructuur waar het SOC een eigen deel van het netwerk heeft voor de eigen systemen en applicaties. Separate autonome infrastructuur voor het SOC die ervoor zorgdraagt dat in het geval van een incident, het SOC door kan blijven werken.

Medewerkers van het SOC dienen ook vanuit huis op een veilige manier te kunnen werken. Daar worden de faciliteiten van de organisatie voor remote werken voor gebruikt. Op basis van een risicoanalyse kan er bepaald worden of SOC-medewerkers wel of niet thuis.

Best Practices voor inrichting

Voor de inrichting van operations en faciliteiten is het van belang om te starten met wat minimaal noodzakelijk is voor het SOC. In de basis betekent dit keuzes maken voor openingstijden, zorgdragen dat er voldoende bezetting is en dat het werk op een gestandaardiseerde manier wordt uitgevoerd. Zaken als oefeningen en stand-by worden daar later aan toegevoegd.

Best Practices voor uitvoering

Feitelijk is operations & facilities de basis voor het SOC. Voor de operatie geldt voor dit element vooral dat het noodzakelijk is dat zaken efficiënt en effectief uitgevoerd worden. De focus voor de operatie is zorgdragen dat de efficiënte en effectiviteit gewaarborgd wordt (middels kwaliteitsmanagement) en dat deze waar mogelijk verbeterd wordt (middels *Continuous Improvement*).

7.3 Rapportage en communicatie

Voor het SOC is het van groot belang om transparant te zijn over haar dienstverlening. Dit helpt bij acceptatie van de SOC-werkzaamheden binnen de organisatie en toont ook de toegevoegde waarde van het SOC aan belanghebbenden. Duidelijke rapportage is onderdeel van deze transparantie. Rapportages worden gebruikt als input voor governance meetings (zie 3.1.4), en om de kwaliteit van de dienstverlening en de performance van het SOC te meten en continu te verbeteren.

Het SOC kan verschillende rapportages uitbrengen:

- **Dienstrapportages.** De dienstrapportages worden gebruikt om inzicht te geven in de performance van de SOC-diensten en worden maandelijks



opgeleverd. De dienstrapportages worden gebruikt in SOC governance meetings, en gecommuniceerd naar primaire belanghebbenden. De inhoud van de rapportages is afgestemd met de ontvangende partijen.

- **Incidentrapportages.** Vanuit de dienst [Incident Management](#) worden incident rapportages uitgebracht waarin incidenten in detail beschreven worden. Tot de incident beschrijving behoort: scope, impact, oorzaak, en aanbevelingen voor verbeteringen. Deze verbeteringen kunnen van toepassing zijn op het SOC, maar ook daarbuiten. Ook hier geldt dat opvolging van deze aanbevelingen op een gestructureerde manier opgepakt moeten worden, zowel binnen als buiten het SOC.
- **Vulnerability-rapportages.** Vanuit de dienst [Vulnerability Management](#) worden rapportages geleverd over kwetsbaarheden binnen de infrastructuur. Deze rapportages worden geleverd aan de relevante teams en bevatten advies voor opvolging. Zodoende kunnen de teams actieve opvolging geven aan de rapportages.
- **CTI-rapportages.** Vanuit de dienst [Threat Intelligence](#) wordt continue informatie verzameld over relevante dreigingen. Waar nodig worden uitgebreide analyses uitgevoerd en worden de resultaten daarvan met de belanghebbenden gedeeld binnen en buiten de organisatie. Belangrijk daarbij is dat de rapportages 'actionable' zijn, wat betekent dat de rapportages duidelijke informatie geven over te nemen vervolgstappen. CTI-rapportages worden periodiek of ad-hoc uitgebracht voor relevante dreigingen.

Voor alle typen rapportages geldt dat deze zoveel mogelijk automatisch worden gegenereerd. Analyses en inzichten worden handmatig toegevoegd aan de rapportage.

Naast de gestandaardiseerde rapportages kan het SOC ook voorzien in ad-hoc rapportages voor gespecificeerde gevallen. Zo kan het SOC op verzoek rapportages opleveren aan andere teams, interne audit of de toezichthouder.

7.3.1

Metrics

Metrics liggen aan de basis van de rapportages. Het SOC kan echter meer metrics hebben dan wat in de rapportages terugkomt. Zo kunnen metrics ook gebruikt worden als interne sturingsinformatie binnen het SOC. Het SOC dient een set aan metrics te selecteren. Deze metrics worden gekozen op basis van:

- Noodzaak voor het kunnen rapporteren over SOC-activiteiten (op verzoek van dienstafnemers).
- Noodzaak voor het kunnen aantonen van de effectiviteit van het SOC (op verzoek van belanghebbenden).
- Verbetering van zwakkere elementen binnen het SOC.

Voor de inrichting van metrics binnen het SOC is het goed om te starten met een selectie van essentiële set aan metrics, om deze later uit te bouwen. Als startpunt voor metrics kan de SOC-CMM metrics suite ^[12] gebruikt worden, die metrics op verschillende implementatieniveaus beschrijft en een aantal Best Practices voor de inrichting van een metrics programma bevat.

7.3.2

Communicatie

Ook op het gebied van communicatie vanuit het SOC is het belangrijke duidelijke afspraken te maken. Een algemene afspraak is dat algemene communicatie vanuit het SOC zoveel mogelijk vanuit de algemene mailbox gedaan wordt. Op die manier kunnen antwoorden vanuit de het team opgepakt worden en is de continuïteit van beantwoording gegarandeerd. Waar mogelijk worden referenties gebruikt, bijvoorbeeld naar een casenummer of een alert ID, zodat de communicatie overdraagbaar is binnen de shift en naar de volgende shift.

¹² <https://www.soc-cmm.com/products/metrics/>

Voor communicatie bij grotere incidenten moet duidelijk zijn waar de verantwoordelijkheden liggen. Ook moet in de respons plannen staan met welke frequentie de belanghebbenden geïnformeerd moeten worden. Het gebruik van communicatietemplates voor eenduidige en consistente communicatie is hierbij een goed hulpmiddel.

Best Practices voor inrichting

Voor de inrichting van rapportages is het belangrijk om de informatiebehoefte van de belanghebbenden en dienstafnemers helder te hebben. Deze informatiebehoefte vormt de basis voor rapportage en transparantie over de dienstverlening. Daarnaast moet het SOC in kaart brengen welke informatie het zelf nodig heeft om sturing te kunnen geven aan de operatie. De combinatie van deze zaken wordt gebruikt om de juiste metrics te selecteren en in te richten.

Best Practices voor uitvoering

Ook voor rapportages geldt dat het van belang is om met regelmaat te evalueren of de rapportages nog goed aansluiten bij de belanghebbenden. Het SOC moet zich daarbij ook afvragen of de boodschap die het SOC over wil brengen nog effectief overgedragen wordt aan de ontvangers. Het wijzigen van de vorm en inhoud van de rapportage kan helpend zijn om een nieuw perspectief te bieden. Ook moet het SOC regelmatig de set aan interne metrics evalueren. Doel daarbij is de metrics af te stemmen op de benodigde verbeteringen binnen het SOC.

7.4**Use Case Management**

Security Monitoring use cases beschrijven een risico voor de organisatie wat met security monitoring verkleind kan worden. Het security monitoring proces kan daarbij gezien worden als een mitigerende maatregel. Om security monitoring goed te laten aansluiten op de risico's binnen de organisatie is het belangrijk om een gedegen proces te hebben voor het beheersen van use cases gedurende de levenscyclus.

Binnen Use Case Management wordt onderscheid gemaakt in twee typen use cases:

1. Generieke use cases.
2. Maatwerk use cases

Generieke use cases

Generieke use cases worden ontwikkeld op basis van standaard frameworks, met name MITRE ATT&CK®. Generieke use cases worden autonoom door het SOC gebouwd. Het beheer en onderhoud van deze use cases ligt volledig bij het SOC. In de volgende paragraaf wordt de toepassing van MITRE ATT&CK® binnen het SOC verder uitgewerkt.

Maatwerk use cases

Maatwerk use cases worden op aanvraag van een systeem- of applicatie eigenaar in samenspraak tussen het SOC en het betreffende team ontwikkeld. Ook andere rollen zoals security officers en riskmanagers kunnen daarbij betrokken worden. Het ontwikkelen van maatwerk use cases begint bij de identificatie van het risico en de mogelijkheid om met monitoring dit risico te verkleinen. Deze identificatie ligt bij de eigenaar van het systeem of de applicatie. Alle teams dienen na te denken over mogelijke risico's binnen de opgeleverde applicatie of infrastructuur (in IRAM-sessies of BIO-gap analyses) om vast te stellen of het implementeren van use cases van toegevoegde waarde is. Het SOC kan daarbij op aanvraag ondersteunend optreden. Voor DevOps teams kan dit opgenomen worden in de '*definition of ready*'. Indien een use case wordt geïdentificeerd wordt deze in gezamenlijkheid tussen het SOC en de aanvrager uitgewerkt en geïmplementeerd. Ook maatwerk use cases hebben een mapping naar MITRE ATT&CK®.

Use Case Management

Om zorg te dragen dat use cases actueel en relevant zijn en blijven is een Use Case Managementproces noodzakelijk. Voor Use Case Management wordt gebruik gemaakt van het MaGMA use case framework. Concreet betekent dit dat:

- Use cases **uitgewerkt en beschreven** worden, van risico's tot low-level implementatie in de security monitoring tooling.
- Use cases onderhouden worden gedurende de gehele **lifecycle**. Dat betekent dat use cases onderhevig zijn aan review, en regelmatig beoordeeld worden op relevantie en actualiteit. Inzichten uit andere SOC-processen, waaronder security incident respons, threat hunting en threat intelligence, en inzichten uit operationele processen buiten het SOC (zoals pentesting en red teaming) worden gebruikt om use cases te tunen en nieuwe use cases te ontwikkelen.
- Use cases actief **gemeten** worden, om de performance van de use case vast te stellen. Op deze manier wordt zorggedragen voor een hogere performance van de rule set, door het verminderen van false-positives, het verbeteren van dekking, en het toepassen van automatisering voor het verbeteren van context en afhandeling.

7.4.1 MITRE ATT&CK toepassing

Het MITRE ATT&CK framework kan effectief worden ingezet binnen een SOC om de security monitoring en incident response te versterken. Door de gestandaardiseerde taxonomie van aanvalstechnieken te gebruiken, kunnen SOC-teams hun detectieregels gericht opstellen en incidents beter categoriseren. Het framework dient als gemeenschappelijke taal tussen verschillende securityteams en maakt het mogelijk om dreigingen consistent te documenteren en analyseren. Dit verbetert niet alleen de operationele efficiëntie, maar helpt ook bij het identificeren van gaps in detectiecapaciteit en het prioriteren van security investeringen. Door het framework geleidelijk te implementeren en te integreren in bestaande SOC-processen, ontstaat een meer gestructureerde en effectieve aanpak van security monitoring en incident response.

Het ATT&CK® framework is zeer uitgebreid en omvat vele honderden (sub-)aanvalstechnieken. Het is daarom noodzakelijk om onderscheid te maken in welke technieken voor de organisatie het meest relevant zijn. Dit wordt gedaan door het opstellen van een ATT&CK® profiel. Daarbij wordt de volgende informatie gebruikt:

1. **Cyber Threat Intelligence (CTI)**. Met behulp van CTI worden waar mogelijk de relevante actoren in kaart gebracht. Deze actoren worden verder onderzocht om te bepalen welke aanvalstechnieken daarmee het meest relevant worden.
2. **ATT&CK® analyse**. Door analyse van het raamwerk kan bepaald worden welke aanvalstechnieken het vaakst voorkomen onder alle actoren.
3. **Kennis van bestaande maatregelen**. Aanvalstechnieken gericht tegen componenten waar gedegen maatregelen voor geïmplementeerd zijn, kennen een lager risico dan componenten waar weinig of minder effectieve maatregelen van toepassing zijn. MITRE D3FEND™ is hierbij een bruikbaar hulpmiddel, omdat dit een overzicht geeft van defensieve security-maatregelen, gekoppeld aan aanvalstechnieken.
4. **Aanwezigheid van databronnen**. Indien een aanvalstechniek alleen gemonitord kan worden met databronnen die niet beschikbaar zijn voor het SOC, is het zinloos om detectie regels te gaan ontwikkelen. Binnen [Detection Engineering](#) worden databronnen in kaart gebracht en voortdurend verbeterd.

Feitelijk zijn dit verschillende heatmaps boven op het ATT&CK® raamwerk die over elkaar gelegd worden om tot de kern te komen van meest relevante technieken: een heatmap met relevante actoren, een heatmap met meest gebruikte technieken, een

heatmap met bestaande maatregelen en een heatmap met databronnen. De meest relevante technieken zijn die technieken die: gebruikt worden door relevante actoren, geen effectieve preventieve maatregelen kennen en waar de benodigde data voor aanwezig is.

MITRE ATT&CK® wordt daarnaast ook gebruikt voor het labelen van alerts. Op deze manier is het mogelijk om een heatmap te maken van de aanwezigheid van detecties ten opzichte van MITRE ATT&CK®, en ook een heatmap van de daadwerkelijke alerts gegenereerd door het monitoringsysteem ten opzichte van MITRE ATT&CK® in een bepaalde periode. Deze heatmaps kunnen gebruikt worden om de coverage ten opzichte van MITRE ATT&CK® te tonen en te verbeteren.

Ook kan binnen het CTI-proces het MITRE ATT&CK® framework gebruikt in het duiden van analyses van cyberaanvallen. Deze labels kunnen vervolgens gebruikt worden om vast te stellen of er voldoende mogelijkheden zijn voor het detecteren van de aanvallen. Hiermee kan meer context gegeven worden aan intelligence rapporten naar het blue team, maar ook naar samenwerkingspartners buiten het SOC.

7.4.2

RACI

De activiteiten en verantwoordelijkheden binnen het Use Case Managementproces zijn weergegeven in onderstaande RACI-tabel. Dit is een algemene tabel, en kan dienen als basis voor het realiseren van een organisatie-specifieke RACI-tabel. Binnen de tabel wordt onderscheid gemaakt tussen de generieke use cases, ingevuld met MITRE ATT&CK® en specifieke use cases, die ontwikkeld worden vanuit een concrete behoefte binnen de dienstafnemers. Belangrijk daarbij is dat het SOC eigenaar is van de generieke use cases, terwijl het eigenaarschap van de specifieke use cases bij de applicatie- of de systeemeigenaar ligt.

	SOC	IT support teams	Systeem / applicatie eigenaar (business)
Generieke use case			
Identificatie nieuwe use case	RA		
Uitwerken use case	RA	C	
Beschikbaar stellen benodigde logging	CI	R	A
Aansluiten benodigde log bronnen	A	R	I
Borgen continuïteit logstroom	RA		
Implementatie use case in monitoring tooling	RA		
Validatie correcte werking use case	RA		
Bepalen noodzaak tot wijzigen use case	RA		
Periodieke review use case	RA		
Tuning use case	RA		
Ontwikkelen en bijhouden respons plan (playbook)	RA		
Maatwerk use case			
Identificatie nieuwe use case			RA
Uitwerken use case	CI		RA
Beschikbaar stellen benodigde logging	CI	R	A
Aansluiten benodigde log bronnen	A	R	I
Borgen continuïteit logstroom	CI		RA
Implementatie use case in monitoring tooling	RA		I
Validatie correcte werking use case	RA		CI



Bepalen noodzaak tot wijzigen use case (use case LCM)			RA
Periodieke review use case	RA		CI
Tuning use case	RA		CI
Ontwikkelen en bijhouden respons plan	CI		RA

Best Practices voor inrichting

Voor de inrichting van Use Case Management is het belangrijk om te realiseren dat zowel de bottom-up (werken vanaf de aanvalstechnieken) als top-down (werken vanaf de risico's) valide werkwijzen zijn. Met top-down werken zal het langer duren om tot resultaat te komen. Het is daarom belangrijk om allereerst een goede basis te leggen voor de monitoring. Dat kan op basis van de bestaande set aan correlatieregels, aangevuld met detectie regels op aanvalstechnieken. Daarbij kunnen ook publieke bronnen van detectie regels gebruikt worden. De detectieregels kunnen later nog gekoppeld worden aan high-level risico's op het moment dat Use Case Management een meer volwassen proces is.

Best Practices voor uitvoering

Voor de operatie is het van belang om Use Case Management als proces en de detectieregels die daarbij horen continue te blijven ontwikkelen. Door in het begin generiek te starten en een basis voor monitoring neergezet worden is het mogelijk om dit later uit te bouwen door maatwerk use cases te introduceren, het MaGMA use case framework toe te passen, metingen op use cases in te voeren, en meer specifieke focus aan te brengen op monitoring door ATT&CK® profilering uit te voeren.

7.5

Detection Engineering

Detection Engineering heeft als doel om de technische en functionele inrichting van de security monitoring tooling en de daarbij behorende integraties en bronnen te optimaliseren zodat security monitoring maximaal effectief is. Detection Engineering is als proces nauw gelieerd aan Use Case Management en MITRE ATT&CK® toepassing. In sommige gevallen zijn deze zaken samengevoegd tot het takenpakket binnen één enkele SOC-rol.

Detection Engineering houdt zich primair bezig met twee taken:

- Verbeteren van detectiemogelijkheden door het **optimaliseren van databronnen**. De belangrijkste input hierbij komt voort uit het toepassen van DeTT&CT, een tool waarmee inzichtelijk gemaakt kan worden welke aanvalstechnieken gedetecteerd kunnen worden met de aangesloten databronnen. Daarnaast wordt ook actief de dekking van aangesloten bronnen gemeten en verbeterd. Onderdeel van het verbeteren van detectie mogelijkheden is ook het tunen van detectie regels om false positives en false negatives te voorkomen.
- Verbeteren van detectiemogelijkheden door het **optimaliseren van de detectieregels**. De belangrijkste inputs hierbij zijn het vaststellen van tekortkomingen ten aanzien van de generieke en specifieke use cases.

De output van het Detection Engineering proces zijn nieuwe, gewijzigde of verwijderde detectieregels voor de security monitoring tooling. Het use case framework wordt overeenkomstig aan de technische aanpassing bijgewerkt.

7.5.1

Detectie validatie

Naast het optimaliseren van detectieregels en databronnen houdt het Detection Engineering team zich ook bezig met het valideren van bestaande detecties. Dit is noodzakelijk omdat anders detecties ongemerkt niet goed kunnen werken. Hierdoor kunnen incidenten gemist worden, waardoor deze een grotere impact op de organisatie kunnen hebben. Om dit te voorkomen is een strategie van toepassing met meerdere componenten:

1. **Purple teaming.** Door met regelmaat en op een gestructureerde manier red en/of purple teaming oefeningen uit te voeren kan getoetst worden of de geïmplementeerde detectieregels werken. Het SOC kan er dan vanuit gaan dat zij in staat is om aanvallen te signaleren en daar adequaat mee om te gaan.
2. **Regelmatige review van use cases.** Daarbij worden met name de use cases gereviewd die al een tijd lang niet beoordeeld zijn en de detectie regels die al een tijd lang geen alerts meer hebben gegenereerd.
3. **Simulatie van aanvalstechnieken.** Op kleinere schaal dan een red team kan het SOC ook zelf een simulatie uitvoeren van een aanvalstechniek. Termen die hierbij horen zijn Breach & Attack Simulation, Micro Attack Simulations, en Adversary Emulation. Het SOC gebruikt daarbij tooling om aanvalstechnieken te simuleren en te toetsen als onderdeel van de threat hunting-/purple teaming- activiteiten.
4. **Actieve controle van de databron status en format.** Wanneer databronnen geen informatie meer aanleveren, levert dit gaten op in de monitoring. Het is dus zaak om de status van de databronnen goed te monitoren en actief na te gaan waarom een databron geen informatie meer aanlevert. Ook het databron format is belangrijk. Wanneer een log format wijzigt kan dit tot gevolg hebben dat een detectie niet langer werkt. Het is dus ook zaak om hier als SOC scherp op te zijn.
5. **Nieuwe detecties** dienen altijd eerst worden getest in een geschieden omgeving met toegang tot productie-data (acceptatie en test-prod), inclusief backtest en een canary/soak-fase. Dit voorkomt dat validatie direct in productie plaatsvindt en verhoogt de betrouwbaarheid van detecties.

Best Practices voor inrichting

Detection Engineering is een activiteit die specifieke kennis en kunde vereist rondom het ontwikkelen en testen van detectie regels. Duidelijk vastleggen van deze kennis en kunde, en de verwachtingen aan detection engineers is belangrijk voor het goed inrichten van het proces. Tenslotte is het ook belangrijk om na te gaan of Use Case Management, MITRE ATT&CK® toepassing en Detection Engineering als separate activiteiten worden gezien, of als activiteiten behorende bij één enkele rol. Bij de inrichting van het proces moet ook gezorgd worden dat er een goede afstemming is met andere activiteiten binnen het SOC, zoals threat intelligence voor het inrichten van detectie regels, gebaseerd op actuele dreigingsinformatie en het analistenteam (die te maken krijgen met de output van het Detection Engineering proces).

Best Practices voor uitvoering

Detection Engineering bepaalt in grote mate hoe goed de detectie capability van het SOC ontwikkeld wordt. Daarnaast is Detection Engineering ook belangrijk voor het beheersen van de kwaliteit van de alerts en het zorgdragen dat de hoeveelheid alerts die analisten te verwerken krijgen niet te hoog is. Het is daarmee een essentieel proces voor het SOC. Om die reden is het noodzakelijk om goed inzicht te krijgen in de performance van de ruleset en het Detection Engineering proces in zijn geheel. De input van de analisten is daarbij belangrijk om mee te nemen.

7.6

Automation Engineering

Naast de processen benoemd in het SOC-CMM model is Automation Engineering een belangrijk proces binnen het SOC. Automation Engineering heeft als doel de effectiviteit en efficiëntie van SOC-processen en activiteiten te verhogen en daarmee de performance van het SOC te maximaliseren. Daarbij wordt ook het werk interessanter gemaakt voor de SOC-analisten doordat herhaaldelijk werk automatisch wordt afgehandeld of in sterke mate ondersteund wordt door automatisering.



Er worden 2 typen automatisering onderscheiden:

- **Workflow automation.** Het betreft hier het (gedeeltelijk) automatisch afhandelen van alerts. Vaak wordt hier automation tooling voor gebruikt, of wordt gebruik gemaakt van de mogelijkheden die bestaan binnen het security monitoringsysteem.
- **Automatisering van overige taken.** Naast workflow automation kunnen ook andere verzoeken voor automatisering neergelegd worden bij het Automation Engineering team. Daaronder vallen bijvoorbeeld het automatiseren van rapportages of het automatiseren van herhaaldelijke taken.

De belangrijkste input voor Automation Engineering is de identificatie van mogelijkheden tot automatisering. Elke medewerker van het SOC kan mogelijkheden tot automatisering aandragen bij het automation team. Bij het ontwikkelen van automatisering wordt de hoogste prioriteit gegeven aan taken waar de meeste tijdswinst behaald kan worden. Het is daarvoor nodig om deze tijdswinst zo goed mogelijk te kwantificeren. Daarbij moet wel rekening gehouden worden met de hoeveelheid tijd die nodig is voor het ontwikkelen van de automatisering.

Playbook ontwikkeling

Playbook ontwikkeling is onderdeel van het takenpakket van het Automation Engineering team. Playbooks liggen ten grondslag aan workflow automation, en dienen primair om de afhandeling van alerts te standaardiseren. Playbooks kunnen deels geautomatiseerd worden, bijvoorbeeld door extra context op te halen voor verrijking van het incident. Voorbeelden van context zijn Virustotal informatie, IP reputation, dreigingsinformatie, etc. De feedback van analisten wordt gebruikt om de playbooks te automatiseren.

Best Practices voor inrichting

Voor de inrichting van het Automation Engineering proces is het met name belangrijk om de medewerkers met de juiste skills in te zetten. Deze medewerkers dienen programmeer skills te hebben en te kunnen werken met automation tools. Daarbij is het belangrijk om keuzes te maken voor welke programmeertaal als standaard gebruikt wordt binnen het SOC.

Best Practices voor uitvoering

Voor de operatie is het met name van belang om de effectiviteit van het proces inzichtelijk te maken. Dat kan door de hoeveelheid tijd per activiteit te kwantificeren voor en na de automatisering. Op deze manier kan gevalideerd worden dat de automatisering het gewenste effect heeft. Binnen het Joint SOC wordt Python als standaard gehanteerd als programmeertaal voor automatisering.

8 Technology domein

Om diensten te kunnen leveren, maakt het SOC gebruik van meerdere technologieën. Het SOC-CMM kent een viertal kern technologieën, die met name op het gebied van security monitoring en de opvolging van meldingen uit security monitoring te maken hebben: Security Information & Event Management (SIEM), Network Detection & Response (NDR), Endpoint Detection & Response (EDR) en Security Orchestration & Automated Response (SOAR). Deze kerntechnologieën worden in de hiernavolgende paragraaf in meer detail beschreven. Naast deze kern technologieën worden ook andere technologieën gebruikt door het SOC. Techniek is altijd aan verandering onderhevig, dus het is belangrijk voor elk SOC om de technologische ontwikkelingen goed in de gaten te houden.

Met de technologie die gebruikt wordt, wordt onder andere invulling gegeven aan de Gartner SOC visibility triad [¹³]:



Figuur 1: Gartner SOC visibility triad

SOAR speelt geen rol in deze triad, maar helpt om de techniek en processen efficiënter in te zetten. Een Threat Intelligence Platform (TIP) speelt ook geen rol in deze triad, maar geeft met CTI-context aan de technologieën.

Principes

Een Security Operations Center (SOC) is sterk afhankelijk van diverse security tooling voor detectie, monitoring en incident response. Het beheer van deze tooling vereist een doordachte aanpak vanuit zowel technisch als functioneel perspectief.

Juridische en compliance overwegingen spelen een cruciale rol bij de selectie en implementatie van SOC tooling. Organisaties moeten rekening houden met wet- en regelgeving zoals de AVG/GDPR voor gegevensbescherming, specifieke sectorale compliance vereisten, en eventuele geografische beperkingen voor dataopslag en -verwerking. Dit betekent dat tools moeten voldoen aan eisen rondom data retention, logging, encryptie en toegangscontrole.

Het technisch beheer richt zich op het waarborgen van de beschikbaarheid, integriteit en veiligheid van de tooling. Dit omvat:

- Het tijdig doorvoeren van security patches en updates om kwetsbaarheden te mitigeren.
- Het monitoren van de performance en capaciteit van systemen.

¹³ <https://www.gartner.com/en/documents/3904768>

- Het hardenen van de systemen.
- Het beheren van backup en recovery procedures.
- Het onderhouden van integraties met andere security en IT-systemen.
- Het implementeren van secure configuration baselines.
- Het uitvoeren van vulnerability assessments op de tooling zelf.

Het functioneel beheer focust op de effectieve inzet van de tooling binnen SOC-processen:

- Het configureren en optimaliseren van detectieregels en use cases.
- Het beheren van gebruikersaccounts en rechtenstructuren.
- Het afstemmen van rapportages op stakeholderbehoeften.
- Het documenteren van procedures en werkinstructies.
- Het trainen van SOC-analisten in het gebruik van de tools.
- Het evalueren van de effectiviteit van de tooling.

Voor zowel technisch als functioneel beheer is het essentieel om een duidelijke governance structuur te hebben met gedefinieerde rollen, verantwoordelijkheden en escalatieprocedures. Dit moet waarborgen dat wijzigingen gecontroleerd worden doorgevoerd en dat security risico's adequaat worden gemanaged.

Belangrijke principes bij de selectie van tooling zijn:

- Informatie wordt centraal verzameld en aangeboden aan analisten zodat zoveel mogelijk een *single pane of glass* ontstaat.
- Securityinformatie wordt altijd op een veilige manier (volgens de richtlijnen van het NCSC ¹⁴) uitgewisseld tussen de componenten.
- Toegang tot securityinformatie vindt plaats na authenticatie en alleen aan geautoriseerde personen.
- De beschikbaarheid, vertrouwelijkheid en integriteit van securityinformatie wordt geborgd.
- Detectie vindt plaats op verschillende lagen (*defense in depth*).
- De mate waarin de tool aansluit bij de use cases en dreigingsscenario's van de organisatie.
- De mogelijkheid tot integratie met bestaande security en ICT-omgeving.
- De beschikbaarheid van lokale expertise voor beheer en ondersteuning.
- De total cost of ownership, inclusief licenties, beheer en training.
- De volwassenheid en toekomstvastheid van de leverancier.
- De beschikbaarheid van support en updates.
- De mogelijkheden voor automatisering en orkestratie.
- De schaalbaarheid van de oplossing.
- Het moet mogelijk zijn om de SOC-systemen worden bij voorkeur in een aparte autonome omgeving geplaatst.
- Uitgebreide informatie (zoals packet captures en end-point informatie) is noodzakelijk voor gedetailleerd onderzoek. Deze informatie wordt bewaard voor onderzoek. Alleen relevante security events worden doorgestuurd naar centrale monitoring componenten.
- Informatie wordt bij voorkeur niet gedupliceerd. Indien er meerdere toepassingen zijn voor dezelfde data, wordt de toegang tot deze data op een veilige manier ontsloten.
- Securityinformatie wordt niet langer bewaard dan noodzakelijk voor het doel en wettelijk toegestaan

¹⁴ <https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>



Het is belangrijk om regelmatig de effectiviteit van de tooling te evalueren en waar nodig aanpassingen door te voeren in de beheerprocessen. Dit moet gebeuren in nauwe samenwerking tussen technisch beheer, functioneel beheer en de SOC-analisten die dagelijks met de tools werken.

8.1 SIEM

Een Security Information and Event Management (SIEM) systeem is een centrale oplossing die security-gerelateerde data verzamelt en analyseert uit verschillende bronnen binnen een IT-infrastructuur. Het combineert loggegevens van servers, netwerkkapparatuur, security tools en applicaties om potentiële security incidenten te detecteren en hierop te kunnen reageren.

Het SIEM systeem correleert deze events om patronen te herkennen die kunnen wijzen op security dreigingen zoals malware infecties, inbraakpogingen of data-diefstal. Door het normaliseren en analyseren van de data kunnen security analisten verdachte activiteiten sneller identificeren en onderzoeken.

De belangrijkste functies van een SIEM zijn:

- Het verzamelen en centraal opslaan van loggegevens;
- Real-time monitoring en alerting op security events;
- Correlatie van events uit verschillende bronnen;
- Ondersteuning bij incident response en onderzoek;
- Rapportage voor compliance en audit doeleinden.

Een SIEM vormt daarmee een essentieel onderdeel van het security monitoring proces binnen een Security Operations Center (SOC).

8.1.1 *Eigenaarschap*

Het eigenaarschap van de SIEM oplossing dient belegd te worden. Het betreft zowel technisch eigenaarschap als functioneel eigenaarschap. Dit kan in beide gevallen het SOC zijn als het SOC ook de technische implementatie en het onderhoud uitvoert. Er kan echter ook een splitsing zijn in verantwoordelijkheden, waarbij het technisch beheer elders belegd is. Het functioneel beheer zal altijd bij het SOC moeten worden belegd, vanwege de specifieke expertise die noodzakelijk is voor het inrichten van de tooling. Dit eigenaarschap wordt vastgelegd in een RACI.

8.1.2 *Beheer en onderhoud*

Beheer en onderhoud van tooling wordt op een volwassen manier uitgevoerd. Dit betekent dat het SOC zich houdt aan de ITIL-processen die van toepassing zijn binnen de organisatie. Voor patches en upgrades wordt het volgende gehanteerd:

- Een testomgeving is bij voorkeur aanwezig om patches en upgrades te testen, nieuwe detectieregels te ontwikkelen en te testen.
- Patches worden altijd geïnstalleerd conform regulier patch/change management.
- Spoedpatches worden direct uitgerold. Een spoedpatch verhelpt een kritieke kwetsbaarheid in het SIEM systeem.
- Upgrades van de software worden geïnstalleerd volgens het n-1 principe, dat wil zeggen: de voorlaatste versie. Hiervan kan afgeweken worden als de upgrade van het product een probleem verhelpt wat operationele issues veroorzaakt, als een nieuwe functionaliteit geïntroduceerd wordt die essentieel is voor het SOC, of wanneer een kwetsbaarheid wordt opgelost.



8.1.3 *Data retentie*

Het SIEM systeem bevat data uit de gehele infrastructuur. Deze data dient lang genoeg bewaard te worden om historische analyses en threat hunting onderzoeken uit te kunnen voeren. Een vuistregel daarbij is om de informatie een half jaar lang te bewaren. Daar kan van afgeweken worden als daar gerechtvaardigde redenen voor zijn. Langere retentieperiodes brengen hogere kosten met zich mee. De baten daarvan moeten duidelijk gemaakt kunnen worden, zodat het SOC kosten-efficiënt kan draaien.

Naast de data retentie van de gehele omgeving, kunnen ook specifieke eisen zijn aan het bewaren van informatie. Voor de overheid geldt dat data behorende bij een security incident wordt tenminste 3 jaar lang bewaard, conform eis 16.1.7.1 uit de Baseline Informatiebeveiliging Overheid (BIO). Deze informatie dient bewaard te worden in het gebruikte incident registratiesysteem.

8.1.4 *RACI*

Voor alle activiteiten van het SOC is het belangrijk een RACI op te stellen. In de RACI voor SIEM dienen tenminste de volgende activiteiten belegd te worden:

- Beleid / voorschriften voor logging (logrichtlijnen) en aansluiting op de SIEM;
- Technisch beheer & onderhoud tooling (patches, upgrades);
- Technische inrichting tooling (data retentie, indexering, etc.);
- Technisch incident management;
- Functionele inrichting tooling (rapportages, detecties, etc.);
- Technisch aansluiten logbronnen (integraties);
- Functioneel aansluiten logbronnen (parsing, API's);
- Troubleshooting logbronnen die geen informatie meer versturen;
- Vendormanagement SIEM;
- Licentiebeheer SIEM.

8.2 **EDR**

Met Endpoint Detection and Response (EDR) tooling wordt vormgegeven aan monitoring op de endpoints binnen de ICT-omgeving van de organisatie. Deze informatie is van cruciaal belang voor security monitoring, omdat security incidenten veelal beginnen op endpoints, met name endpoints van medewerkers. EDR tooling stelt het SOC in staat om te monitoren op de endpoints (detectie) en ook direct in te grijpen (respons) indien zich daar een mogelijk cybersecurity incident voordoet. Tenslotte biedt de EDR tooling mogelijkheden om analyse op afstand uit te voeren, zodat met meer zekerheid vastgesteld kan worden of een alert ook daadwerkelijk een security incident is.

8.2.1 *Eigenaarschap*

Ook voor EDR-oplossingen moet het technisch eigenaarschap en functioneel eigenaarschap eenduidig belegd worden. De technisch eigenaar is eigenaar van de agent en de implementatie van de agent op de end-points. De functioneel eigenaar is eigenaar van de configuratie van de agent. Deze configuratie bepaalt welke functionaliteiten van de agent aan staan en op welke manier de agent zich gedraagt op het end-point. Denk daarbij bijvoorbeeld aan of de agent wel of niet actief ingrijpt en in welke gevallen. Het functioneel beheer zal altijd bij het SOC moeten worden belegd, vanwege de specifieke expertise die noodzakelijk is voor het inrichten van de tooling.



8.2.2 *Data retentie*

Voor data retentie geldt ook hier dat het logbeleid wordt gevolgd om zo (historische) analyses en threat hunting onderzoeken te ondersteunen.

8.2.3 *Beheer en onderhoud*

Beheer en onderhoud van EDR-agents kan gezien worden als een extensie van regulier beheer van end-points. Om die reden is het technisch beheer van EDR tooling in de regel niet binnen het SOC belegd, maar binnen IT-teams die zich met de end-point configuratie bezighouden. Ook hier geldt dat volwassen beheer en onderhoud praktijken toegepast worden, inclusief change management en een n-1 aanpak voor upgrades.

8.2.4 *RACI*

In de RACI voor EDR dienen tenminste de volgende activiteiten belegd te worden:

- Beleid/voorschrift voor configuratie van EDR-oplossing;
- Uitrol EDR-agents op endpoints;
- Technisch beheer & onderhoud tooling (patches, upgrades);
- Technisch incident management;
- Beheer functionele inrichting tooling (security baseline);
- Vendormanagement EDR;
- Licentiebeheer EDR.

8.3 **NDR**

Met Network Detection and Response (NDR) wordt vormgegeven aan monitoring in het netwerk. Dit systeem is in staat om aanvallen op netwerkniveau te detecteren. Omdat de apparatuur in de meeste gevallen niet in-line staat, maar alleen luistert naar het netwerkverkeer is actief ingrijpen niet direct mogelijk. Wel speelt de tooling in elk geval een rol bij incident respons en onderzoek door het SOC de mogelijkheid tot het uitvoeren van uitgebreide netwerkanalyse (network forensics) te bieden. Het is daarbij helpen om zoveel mogelijk gedetailleerde informatie te hebben. Packet captures hebben daarbij de voorkeur. Waar dit niet mogelijk is, biedt netwerk flow informatie een alternatief. Flow informatie heeft minder details, maar kan nog steeds gebruikt worden om analyses uit te voeren van verkeersstromen. Een Netflow sample rate geeft aan welke fractie van het totale netwerkverkeer wordt gesampled voor analyse. Bijvoorbeeld, bij een sample rate van 1:1000 wordt slechts één pakket van elke 1000 pakketten geanalyseerd. Een hoge sample rate (zoals 1:10000) is minder geschikt voor security monitoring omdat hierbij te veel netwerkverkeer wordt gemist. Dit kan leiden tot het niet detecteren van belangrijke security events, zoals scanning activiteiten, data exfiltratie of command & control verkeer. Vooral kortstondige of low-volume malafide activiteiten kunnen hierdoor onopgemerkt blijven. Voor effectieve security monitoring is een lagere sample rate (zoals 1:100 of 1:10) nodig om voldoende zicht te houden op het netwerkverkeer, al moet dit worden afgewogen tegen de beschikbare verwerkingscapaciteit.

Belangrijk bij netwerk detectie is dat zowel noord-zuid (verkeer van binnen naar buiten en vice versa) als oost-west (verkeer binnen de organisatie) verkeer gemonitord wordt. Op deze manier kunnen malafide inkomende verkeersstromen (waaronder malware) en uitgaande verkeersstromen (waaronder data exfiltratie en command en control verkeer) gedetecteerd worden, alsook laterale beweging. De huidige trend is dat steeds meer netwerkverkeer encrypted is, wat betekent dat dit verkeer niet inzichtelijk is. Hierdoor zal de druk van detectie steeds meer naar het endpoint verschuiven.



8.3.1 *Eigenaarschap*

De technisch eigenaar van de NDR-oplossing is eigenaar van de implementatie van de hardware en software in het netwerk. De functioneel eigenaar is eigenaar van de configuratie van de oplossing. De configuratie van de oplossing omvat de detectieregels en de gedragingen van de tool bij detecties (blokkeren, alerts sturen, etc.). Het functioneel beheer zal altijd bij het SOC moeten worden belegd, vanwege de specifieke expertise die noodzakelijk is voor het inrichten van de tooling.

8.3.2 *Beheer en onderhoud*

Beheer en onderhoud van NDR volgt dezelfde principes als het beheer en onderhoud van SIEM systemen. Het SOC werkt voor NDR-oplossingen samen met netwerk engineers om de verkeersstromen en routing goed door de oplossingen te geleiden.

8.3.3 *Data retentie*

Data retentie is voor NDR-systemen kan hoge opslag eisen met zich meenemen, vooral wanneer packet captures opgeslagen worden. Het SOC zal een kosten-baten analyse moeten maken om vast te stellen welke retentieperiode passend is. Wanneer enkel flow data opgeslagen wordt, is een retentie periode van 3 maanden makkelijker haalbaar.

8.3.4 *RACI*

In de RACI voor NDR dienen tenminste de volgende activiteiten belegd te worden:

- Voorschrift voor configuratie van NDR-oplossing;
- Technische implementatie IDS sensoren;
- Technisch beheer & onderhoud tooling (patches, upgrades);
- Technisch incident management;
- Beheer functionele inrichting tooling (security baseline);
- Vendormanagement NDR;
- Licentiebeheer NDR.

8.4 **SOAR**

Met Security Orchestration and Automated Response (SOAR) wordt vormgegeven aan automatisering binnen de analyse en respons processen van het SOC. Het SOAR-systeem wordt gevoed met informatie vanuit het SIEM systeem, of andere systemen voor verrijking van gegevens (zoals mail systemen). Deze informatie wordt door het SOAR-systeem gebruikt om het juiste playbook te starten. Deze playbooks worden ontwikkeld binnen het Automation Engineering proces.

Binnen het playbook worden handmatige acties in verregaande mate geautomatiseerd. SOAR biedt daarbij de mogelijkheid tot het verrijken van informatie waarbij het gebruik maakt van interne en externe bronnen. De SOAR tooling kent daarmee zowel interfaces naar buiten als naar de infrastructuur zelf. De plaatsing van een SOAR-systeem binnen de infrastructuur is dus cruciaal.

Het SOC kan met gedefinieerde respons playbooks automatisch acties uitzetten in de infrastructuur. Acties kunnen daarbij passief zijn (starten van een on-demand virusscan) of actief ingrijpen (blokkeren account, isoleren systeem). Playbooks met actief ingrijpen worden ontwikkeld door het SOC en goedgekeurd op het juiste niveau. Met deze goedkeuring komt ook het mandaat om de acties te mogen uitvoeren indien de situatie daarom vraagt. In het ontwerp van de playbooks wordt rekening gehouden of de acties worden uitgevoerd op een regulier systeem/gebruiker of op een belangrijk systeem/gebruik (VIP-user, kroonjuweel of anderszins belangrijke applicatie).



8.4.1 *Eigenaarschap*

Technisch eigenaarschap van de SOAR-oplossing omvat het eigenaarschap van de (eventuele) hardware en het systeem wat daarop draait. De functioneel eigenaar is eigenaar van de configuratie van de oplossing. Voor SOAR zijn de belangrijkste functionele elementen de playbooks die gebouwd worden ter ondersteuning van analyse en respons en de integraties in de infrastructuur voor automatisering.

8.4.2 *Beheer en onderhoud*

Beheer en onderhoud volgen dezelfde regels als de SIEM oplossing (paragraaf 8.1.2).

8.4.3 *RACI*

In de RACI voor SOAR dienen tenminste de volgende activiteiten belegd te worden:

- Technisch beheer & onderhoud tooling (patches, upgrades);
- Technische inrichting tooling (back-ups, indexerend, etc.);
- Functionele inrichting tooling (rapportages, automatisaties, etc.);
- Ontwikkelen externe integraties;
- Opstellen geautomatiseerde respons playbooks;
- Goedkeuren geautomatiseerde respons playbooks;
- Realiseren technische integratie voor geautomatiseerde respons;
- Vendormanagement SOAR;
- Licentiebeheer SOAR.

8.5 **Overige technologie**

Naast de kern technologieën voor monitoring en respons komen de volgende technologieën ook veel voor in security operations teams:

- **Kwetsbaarheidsscanners.** Het SOC gebruikt scanners om kwetsbaarheden in de ICT-omgeving in kaart te brengen. Daarbij wordt gekeken naar het externe aanvalsoppervlak en het interne aanvalsoppervlak, zowel op infrastructureel als applicatie niveau. Het SOC voert ook geauthentiseerde scans uit op servers en applicaties om diepgaander te kunnen kijken naar aanwezige kwetsbaarheden. Daarnaast stelt een geauthentiseerde scan het SOC in staat om de configuratie van het systeem te houden tegen een gedefinieerde baseline.
- **Forensische toolset.** Het betreft hier een toolset waarmee forensics uitgevoerd kan worden op systemen en randapparatuur (geheugen, disk, USB sticks en applicaties) en omvat ook apparatuur voor onderzoek van malware (dynamische en statische malware analyse).
- **Threat Intelligence Platform.** Een Threat Intelligence Platform (TIP) kan gebruikt worden voor collectie, analyse en distributie van threat intelligence. Voor SOC's kan een TIP ondersteunen in het verschaffen van context voor monitoring. Voor SOC's met een meer volwassen CTI capability is een TIP vaak een must-have om de processen te ondersteunen en te optimaliseren.
- **OSINT/CTI tools.** Naast een TIP kan een SOC ook gebruik maken van tools waarmee threat intelligence en open source intelligence (OSINT) onderzoeken en monitoring (zoals social media, datalekmonitoring en darkweb monitoring) uitgevoerd kunnen worden. Ook dit is onderdeel van een meer volwassen toepassing van CTI in het SOC. Onderzoek wel welke OSINT/CTI tools er vanuit externe en interne wet- en regelgeving moeten worden gebruikt, en wat de juridische kaders zijn waarbinnen moet worden gewerkt.

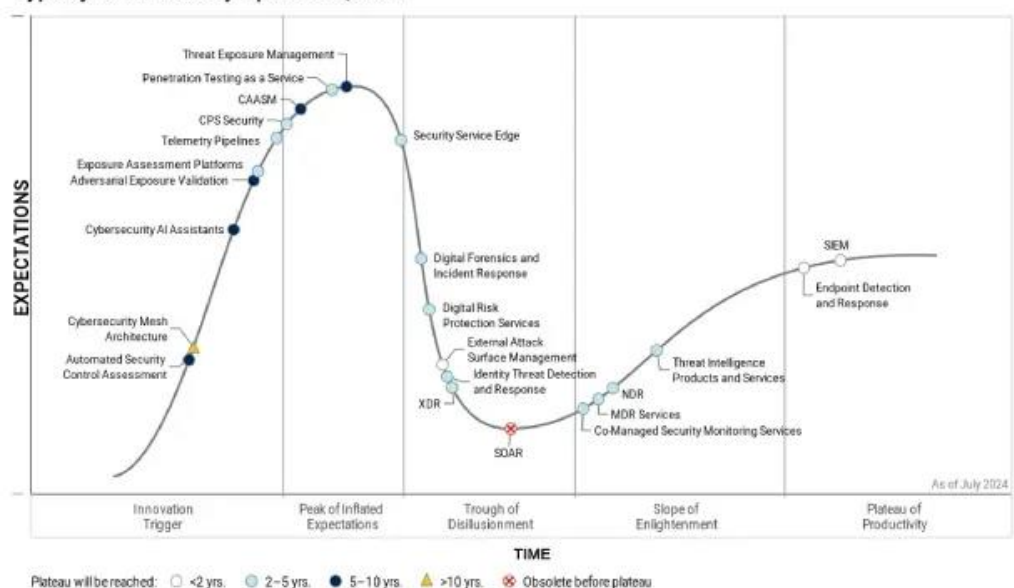
8.6

Toekomstige technologie

De technologieën die in dit hoofdstuk beschreven zijn, zijn standaard technologieën binnen het SOC. Naast deze standaard technologieën (proven technology) is ook sprake van opkomende technologieën. De Gartner hype cycle voor security operations (onderstaande figuur) toont voor verschillende technologieën waar deze op de hype cycle zitten. Hoe verder naar rechts, hoe volwassener het product. Daarnaast geeft de hype cycle ook aan wanneer technologieën tot ware productiviteit kunnen komen. De horizon die daarbij genoemd wordt kan gebruikt worden om het SOC voor te bereiden op die nieuwe technologie.

Bij het implementeren van nieuwe technologieën of tools binnen een SOC moet zorgvuldig worden gekeken naar de toegevoegde waarde. De tool moet aansluiten bij bestaande processen en integreren met de huidige infrastructuur. Daarnaast zijn er belangrijke overwegingen rond compliance en data-privacy, vooral als het gaat om het verzamelen en analyseren van gevoelige gegevens. De beschikbare expertise voor het beheer en gebruik van de nieuwe technologie is cruciaal, evenals de mogelijkheid om de gebruikers en beheerder te trainen. Ook moet worden gekeken naar de schaalbaarheid en onderhoudbaarheid van de oplossing, inclusief de beschikbaarheid van vendor support en updates. De total cost of ownership, waaronder licenties, beheer en trainingskosten, moet passen binnen het beschikbare budget. Tot slot is het belangrijk om de effectiviteit van de nieuwe technologie te kunnen meten en evalueren om de investering te rechtvaardigen.

Hype Cycle for Security Operations, 2024



De hype cycle kan gebruikt worden om vast te stellen wanneer het SOC zich voor moet bereiden voor het implementeren van nieuwe technologie. Het SOC moet zich daarbij afvragen of het een *early adopter* of *smart follower* wil zijn.

Early adopters hebben eerder toegang tot nieuwe technologieën, maar zullen ook moeten investeren in onvolwassen technologie, met het risico dat deze technologie uiteindelijk niet voldoende aanslaat. *Smart followers* wachten tot technologie zichzelf bewezen heeft alvorens deze te adopteren. Belangrijk is dat de technologie toegevoegde waarde biedt voor het SOC, en dat gedegen requirements opgesteld worden alvorens technologie aan te schaffen en te implementeren.

8.7**Best Practices voor het technology domein**

De verschillende technologieën die besproken zijn in dit hoofdstuk kennen dezelfde set aan Best Practices. Deze zijn hierna beschreven.

Best Practices voor inrichting

Voor de aanschaf van nieuwe technologie is het belangrijk om gedegen marktonderzoek uit te voeren. Op basis van het marktonderzoek wordt een set aan requirements opgesteld die gebruikt wordt om tot een goede selectie van product en leverancier te komen. Het opstellen van een business case is daarbij een belangrijk middel.

Voor de inrichting van SOC-technologie is het belangrijk (zoals reeds beschreven) om het eigenaarschap van de tooling goed te beleggen en goede procedures voor onderhoud en beheer af te spreken. Op die manier kan gezorgd worden voor betrouwbare technologie. Om deze betrouwbaarheid te ondersteunen dienen ook KPI's voor beheer, uptime en onderhoud afgesproken en nageleefd te worden. Tenslotte is het van belang dat personeel wat zich bezig houdt met SOC-technologie (zowel technisch als functioneel) getraind is in het gebruik van deze technologie. Dit kan onderdeel zijn van het trainingsprogramma binnen het SOC. Omdat sommige activiteiten ook buiten het SOC uitgevoerd worden, moeten afspraken gemaakt worden over training van deze medewerkers.

Best Practices voor uitvoering

Tijdens de operatie is het vooral belangrijk om de coverage en de functionele inrichting van de detectie oplossingen te optimaliseren.

- **Coverage.** De effectiviteit van monitoring is in belangrijke mate afhankelijk van wat er aangesloten is op de monitoring. Voor EDR betekent dit het aantal aangesloten endpoints, voor NDR betekent dit het aantal aangesloten verkeersstromen, voor SIEM betekent dit het aantal aangesloten databronnen. Het doel moet niet zijn om 100% coverage te realiseren. In plaats daarvan moet het SOC in kaart brengen welke coverage nodig is om effectieve monitoring te kunnen uitvoeren. Door de coverage te meten en te koppelen aan de effectiviteit van monitoring is het mogelijk om kosten-efficiënt en risico-gebaseerd te werken.
- **Functionele inrichting.** Nieuwe functionaliteiten worden met regelmaat ter beschikking gesteld. Deze nieuwe functionaliteiten moeten beoordeeld worden, en geïmplementeerd worden indien deze als waardevol worden gezien. Daarnaast moeten de bestaande functionaliteiten en de benutting daarvan steeds geoptimaliseerd worden en aangepast worden op de veranderende ICT-omgeving.

9 Service domein

In dit hoofdstuk worden de services uit het SOC-CMM besproken:

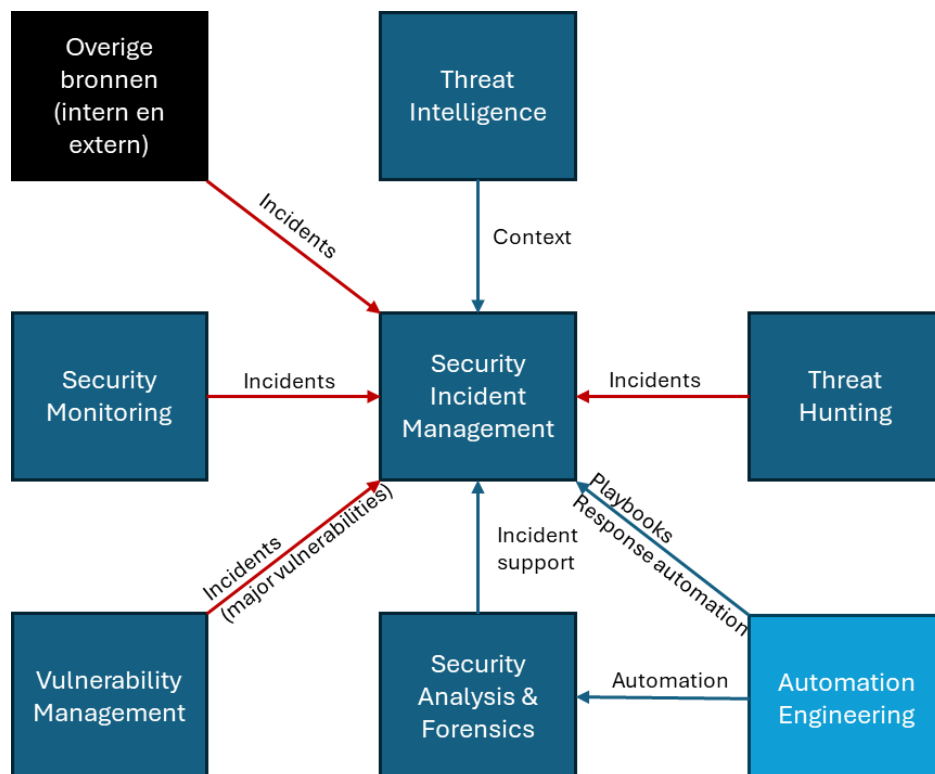
- Security Monitoring
- Security incident respons
- Security Analysis & Forensics
- Threat Intelligence
- Threat Hunting
- Vulnerability Management

De log managementservice uit het SOC-CMM framework is een legacy service, en wordt daarom niet meegenomen in deze Best Practice. De meeste relevante zaken uit de log managementservice worden besproken onder security monitoring.

Belangrijk om te vermelden is dat de dienstencatalogus door het SOC vastgesteld moet worden. Dat betekent dat mogelijk niet alle services die in dit hoofdstuk vermeld worden onderdeel zullen zijn van het SOC dat er diensten geleverd kunnen worden die hier niet in vermeld staan. De dienstencatalogus moet passend zijn voor de wensen van de organisatie.

9.1 Service architectuur

Deze diensten kennen een logische samenhang die de diensten architectuur genoemd wordt. Deze diensten architectuur omvat zowel de primaire diensten (de kern diensten van het SOC), als de ondersteunende processen. Onderstaande figuur toont een generieke dienstenarchitectuur met de samenhang tussen alle diensten en de processen Detection Engineering en Automation Engineering daarin. De rode pijlen geven incident flows aan.



Figuur 2: Security Monitoring



De doelstelling van deze dienst is het identificeren van manifestaties van cyberdreigingen binnen de infrastructuur van de organisatie. Concreet betekent dit dat binnen de dienst security monitoring informatie verzameld wordt uit de gehele infrastructuur. Deze informatie wordt centraal verwerkt om (potentiële) cyberaanvallen in een zo vroeg mogelijk stadium te identificeren. Voorbeelden van databronnen hierbij zijn:

- Logbronnen uit de ICT-omgeving, zowel op infrastructureel als applicatie niveau;
- Databronnen uit cloud omgevingen;
- IOC's uit de TIP (indien aanwezig);
- Security events van endpoint componenten (bijvoorbeeld een EDR-oplossing, of ruwe security logs);
- Security events van network securitycomponenten (bijvoorbeeld een NDR-oplossing, of een NIDS).

Bij afwijkingen worden alerts gegenereerd, die geanalyseerd worden door SOC-medewerkers. Als na analyse een incident wordt vastgesteld, wordt deze opgevolgd in het security incident respons proces.

9.1.1 *Servicelevels en KPI's*

Servicelevels binnen security monitoring hebben met name betrekking op de openingstijden van het SOC. Deze zijn eerder in het document besproken onder openingstijden en bereikbaarheid.

KPI's op security monitoring zijn veelal KPI's die betrekking hebben op de snelheid en accuratesse van het proces. Voorbeelden van dergelijk KPI's zijn:

- Monitoring coverage. De trend van het percentage relevante assets wat informatie aanlevert aan het security monitoringsysteem
- Mean time to pick-up. De tijd die nodig is geweest voordat het alert uit de alert queue opgepakt is.
- Mean time to analyse. De tijd die nodig is geweest voor het analyseren van alerts
- Mean time to escalate. De tijd die nodig is geweest om tot effectieve escalatie van een alert tot een incident te komen.
- Alerts not analysed. De hoeveelheid (of het percentage) alerts wat niet geanalyseerd is.

9.1.2 *Service RACI*

In de RACI voor Security Monitoring dienen tenminste de volgende activiteiten belegd te worden:

- Bepalen beleid/voorschriften voor security monitoring
- Aanvragen aansluiting op security monitoring
- Aansluiten apparatuur op security monitoring
- Uitvoeren security monitoring
- Opstellen rapportage

Het opstellen van use cases valt onder de RACI van Use Case Management, het technisch en functioneel beheer valt onder de RACI van SIEM.

9.1.3 Service onboarding

Voor het *onboarden* in de security monitoring dienstverlening is het noodzakelijk om te voldoen aan de volgende basisvoorwaarden:

- De technische componenten zijn bekend
- Benodigde data is beschikbaar gemaakt
- Technische toegang tot de data is geregeld (netwerk toegang en user access)
- Contact informatie voor incident opvolging is beschikbaar
- Stappen voor incident opvolging zijn gedefinieerd

Daarnaast zijn de volgende additionele voorwaarden van toepassing:

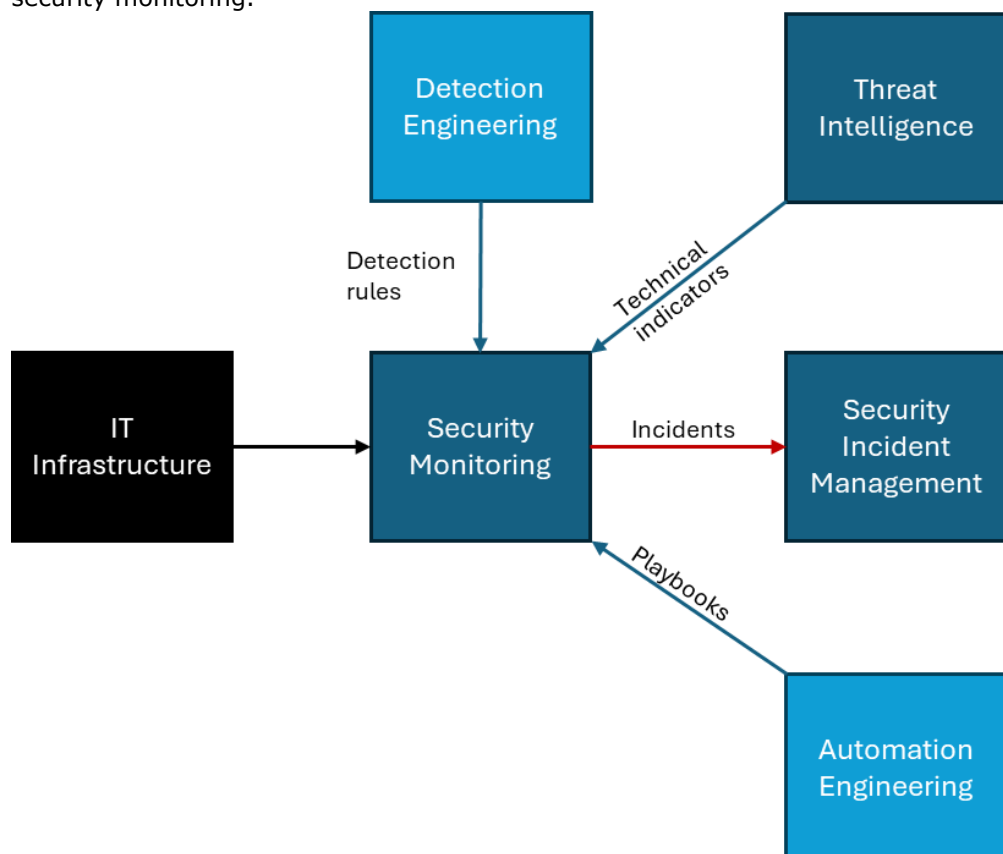
- De risico's voor de aan te sluiten componenten zijn inzichtelijk
- Maatwerk use cases zijn onderkend

Deze voorwaarden zijn geen basisvoorwaarden, maar additionele voorwaarden als er gewerkt wordt met maatwerk use cases voor de aan te sluiten componenten.

Alle teams binnen de organisatie moeten verplicht worden om aan te sluiten op de security monitoring dienstverlening. Dit wordt ondersteund door beleid. Bij voorkeur is er een separaat document welke beschikbaar is met deze aansluitvoorwaarden, om duidelijkheid naar de organisatie te creëren. Logrichtlijnen voor zowel infrastructuur als applicatie moeten aanwezig zijn.

9.1.4 Procesarchitectuur

Onderstaande figuur is een procesarchitectuur voor security monitoring. Het omvat elementen van de totale service architectuur, maar heeft een specifieke focus op security monitoring.



Figuur 3: Security monitoring procesarchitectuur

9.1.5 Best Practices voor security monitoring

Best Practices voor inrichting

Bij de inrichting van het security monitoring proces is het met name belangrijk om de benodigde analyse capaciteit goed in te schatten. De analyse capaciteit moet schaalbaar zijn om de hoeveelheid alerts goed te kunnen behandelen en dient rekening te houden met groei in aantallen alerts als gevolg van het vergroten van de coverage en het verbreden van monitoring door het aantal detectieregels te verhogen. Leg je scope van de security monitoring vast en begin met de coverage van de kroonjuwelen.

Bij de inrichting van security monitoring is een aantal eerder behandelde onderwerpen relevant:

- Openingstijden en bereikbaarheid
- Shifts en stand-by
- Tiering

Om analisten alerts met de juiste prioriteit op te pakken is het belangrijk om alle alerts voorzien van de juiste *severity* (ernst). Deze *severity* wordt gebruikt om de alerts in de juiste volgorde af te handelen. Het SOC dient een methodiek te hebben voor de toekenning van deze prioriteit. Daar kan bijvoorbeeld gebruik gemaakt worden van een matrix met kans en impact. Kans is daarbij waarschijnlijkheid van het alert. Een alert met een hoge waarschijnlijkheid dat het signaal daadwerkelijk een security event is. Onderstaande tabel toont een voorbeeld van een dergelijke matrix voor prioritering van alerts.

Kans/impact	Laag	Midden	Hoog
Hoog	Midden	Hoog	Kritisch
Midden	Laag	Midden	Hoog
Laag	Informatief	Laag	Midden

Belangrijk is dat de prioritering consequent wordt toegepast en is vastgelegd in een begrijpelijk document.

Best Practices voor uitvoering

Tijdens de uitvoering is het met name belangrijk om de kwaliteit van het proces goed te monitoren. Dat kan door te kijken naar het aantal false-positives in de monitoring, het aantal onjuiste escalaties, het aantal niet-geanalyseerde alerts, etc. Deze KPI's geven inzicht in de hoeveelheid alerts die de analisten moeten verwerken, en in hoeverre er sprake kan zijn van *alert fatigue*, een veelvoorkomend verschijnsel waarbij de kwaliteit van de analysis achteruitgaat door een te grote hoeveelheid alerts.

9.2 **Security Incident Management**

De dienst security incident management geeft opvolging aan bevindingen uit de security monitoring dienst. De doelstelling van deze dienst is adequaat en tijdig te reageren op gedetecteerde dreigingen om security incidenten te voorkomen, of deze in een vroegtijdig stadium te mitigeren om de impact van incidenten te minimaliseren. Het is ook mogelijk dat incidenten uit andere hoek komen dan de security monitoring.

Security incidenten worden als volgt gedefinieerd (conform de definitie in ISO27001): *Een security incident is één of meerdere ongewenste of onverwachte gebeurtenissen die een grote kans hebben op het compromitteren van de bedrijfsprocessen en / of een bedreiging vormen voor de Beschikbaarheid, Integriteit en/of Vertrouwelijkheid (BIV) van informatie.*

Security Incident Management ontvangt mogelijke incidenten uit de security monitoring of uit andere bronnen. Deze informatie wordt vervolgens geanalyseerd om vast te stellen of het inderdaad een incident betreft en welke prioriteit dit incident heeft. Het incident wordt vervolgens afgehandeld of intern geëscaleerd indien nodig. Waar nodig wordt de samenwerking gezocht met interne teams om het incident effectief te kunnen afhandelen. Daarbij wordt zoveel mogelijk een aansluiting gerealiseerd op bestaande processen in de organisatie, zoals incident management en crisis managementprocessen.

Onderdeel van security incident management is het evalueren van het incident en het proces. De geleerde lessen hieruit kunnen gebruikt worden om het proces te verbeteren, en om soortgelijke incidenten in de toekomst te voorkomen.

9.2.1 *Servicelevels en KPI's*

Relevante KPI's voor security incident management omvatten bijvoorbeeld:

- Mean time to respond. De tijd die nodig is geweest tussen initiatie van het response proces en daadwerkelijk uitvoeren van incident respons.
- Mean time to contain. De tijd die nodig is om het incident in te perken.
- Mean time to detect. De tijd tussen het starten van het incident (compromittering) en het detecteren daarvan.

9.2.2 *Service RACI*

In de RACI voor security incident management dienen tenminste de volgende activiteiten belegd te worden:

- Bepalen beleid/voorschriften voor security incident respons;
- Uitvoeren van security incident respons activiteiten;
- Escaleren van incidenten;
- Uitvoeren van incident evaluatie;
- Opstellen rapportage op basis van KPI's/duiding;
- Doorvoeren verbeteringen conform incident/problem proces.

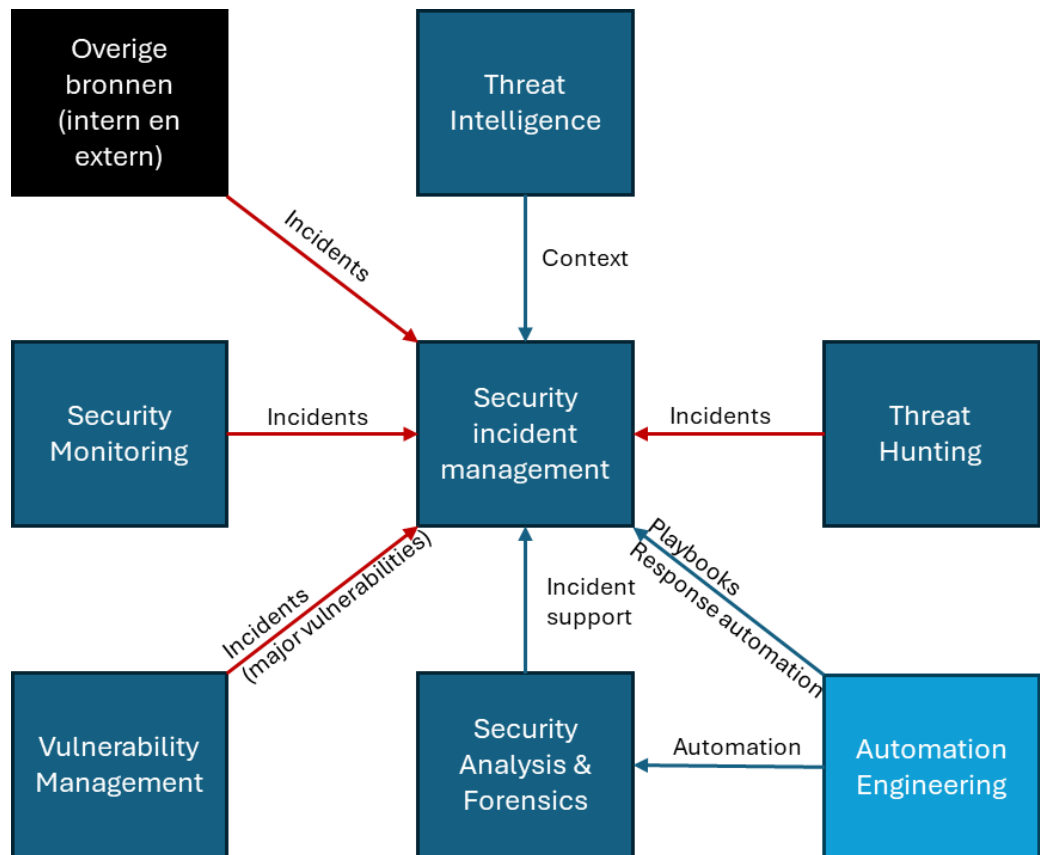
9.2.3 *Service onboarding*

Security incident respons volgt veelal op meldingen uit security monitoring. Security incidenten kunnen ook uit andere bronnen voortkomen, zoals de servicedesk of rechtstreeks van medewerkers. Tenslotte kunnen incidenten ook door externe bronnen gemeld worden.

9.2.4

Procesarchitectuur

Onderstaande figuur is een generieke procesarchitectuur voor security incident management.



Figuur 4: Security incident managementprocesarchitectuur

Kanttekening bij deze figuur: het afhandelen van kwetsbaarheden volgt niet altijd het security incident managementproces, maar wordt soms ook rechtstreeks in regulier incident management of patch management afgehandeld. Dit moet tijdens de inrichting van het vulnerability managementproces besloten worden. Security Incidenten moeten altijd wel vastgelegd zijn in het incident managementproces.

9.2.5

Best Practices voor security incident management

Beste practices voor inrichting

Positionering

Voor de positionering van incident respons in de organisatie is het belangrijk om vast te stellen of het SOC de incident respons functie heeft in de organisatie, of dat er ook sprake is van een CSIRT binnen de organisatie. In het geval een CSIRT-functie naast het SOC ingericht is, is het van groot belang de verantwoordelijkheden af te kaders om overlappende verantwoordelijkheden of niet belegde activiteiten te voorkomen. Ook de samenwerking en overdracht tussen de teams moet in een dergelijk geval uitgewerkt en beschreven worden.

Procesinrichting

Voor de inrichting van het security incident managementproces dient een bestaande standaard gebruikt te worden. De NIST standaard op het gebied van incident response



(NIST SP 800.61r2) wordt daarbij aangeraden. Bijzondere aandacht daarbij dient uit te gaan naar het escalatie proces. Wanneer incidenten leiden tot grootschalige impact op de organisatie, worden deze door het incident response team geëscaleerd. Daarvoor zijn gedefinieerde escalatiepaden noodzakelijk.

Eigenaarschap

Daarnaast is het ook belangrijk om bij de inrichting van het proces een keuze maken wat in hoeverre het eigenaarschap van het proces bij het SOC ligt. Het SOC kan daarbij volledig eigenaar zijn van het security incident managementproces. Het SOC kan er echter ook voor kiezen om geen eigenaar te zijn van het proces, maar alleen van de security incident respons activiteit. Als het SOC alleen security incident respons uitvoert, en geen eigenaar is van het gehele proces moet duidelijk zijn waar dat eigenaarschap dan wel ligt. In veel gevallen zal dat onder het reguliere incident management vallen.

Aansluiting CSIRT communities

Voor incident respons teams is het te overwegen om aan te sluiten op een incident respons community zoals FIRST. Ook een aansluiting op het Nationaal Respons Netwerk (NRN) is een goed middel om samen te werken met andere teams en daarvan te leren. Datzelfde geldt voor het aansluiten op het Operationeel Incident Response Team Overleg (o-IRT-o). Hier werken een aantal grote SOC's en CSIRT's samen vanuit een publiek/private samenwerking.

Toepassing van de VERIS Taxonomie in Incidentregistratie

Het [Vocabulary for Event Recording and Incident Sharing \(VERIS\) framework](#) biedt een gestructureerd raamwerk voor het registreren, classificeren en analyseren van security incidenten. Door de toepassing van deze taxonomie kunnen incidenten efficiënt worden vastgelegd en geanalyseerd, wat bijdraagt aan verbeterd rapporteren en beter inzicht in trends en kwetsbaarheden.

Binnen de VERIS-taxonomie worden de volgende belangrijke componenten vastgelegd in de registratie van incidenten:

- Actor: Wie was de dader van het incident?
- Action: Wat gebeurde er tijdens het incident?
- Asset: Welke systemen of gegevens waren het doelwit van de aanval?
- Attribute: Welk aspect van het incident werd geschaad?

De Actor-categorie maakt onderscheid tussen drie hoofdcategorieën:

- Extern: Actoren van buiten de organisatie, zoals cybercriminelen, statelijke actoren of hacktivisten.
- Intern: Medewerkers, contractors of ander intern personeel.
- Partner: Externe bedrijven of organisaties die verbonden zijn door een samenwerking, bijvoorbeeld leveranciers of klanten.

De Action-categorie omvat zes hoofdcategorieën, die de aard van de actie beschrijven:

- Social: Acties die gericht zijn op social engineering, zoals phishing, scams of spam.
- Malware: Het gebruik van kwaadaardige software om systemen te infecteren.
- Hacking: Directe aanvallen waarbij systemen worden gehackt of beveiligingen worden doorbroken.
- Misuse: Misbruik van interne toegang of bevoegdheden.
- Physical: Fysieke inbreuken op systemen, zoals diefstal van hardware of inbraak in een datacenter.
- Environmental: Incidenten veroorzaakt door natuurlijke of omgevingsfactoren, zoals brand of overstroming.

Binnen de Asset-categorie wordt het getroffen object of systeem geïdentificeerd. De belangrijkste subcategorieën zijn:

- People: Personen die direct getroffen zijn door het incident, bijvoorbeeld door verlies van persoonlijke gegevens.
- Offline-data: Fysieke opslagmedia zoals tapes, flashdrives of harde schijven.
- User devices: Apparaten van gebruikers, zoals laptops of smartphones.
- Networks: Netwerkinfrastructuur, zoals routers of firewalls.
- Servers: Servers die gebruikt worden voor het hosten van data of applicaties.

Tot slot wordt in de Attribute-categorie het specifieke aspect van het incident vastgelegd dat is geschaad volgens de CIA-driehoek:

- Vertrouwelijkheid: Gevoelige informatie wordt onterecht ingezien of gestolen.
- Integriteit: Gegevens worden gewijzigd of gemanipuleerd.
- Beschikbaarheid: Systemen of data worden ontoegankelijk door bijvoorbeeld een DDoS-aanval of systeemstoring.

Door gebruik te maken van de VERIS-taxonomie kunnen security incidenten op een gestandaardiseerde manier worden geregistreerd, wat zorgt voor een gedetailleerd en gestructureerd overzicht van incidenten. Dit helpt bij het snel herkennen van patronen, het verbeteren van de incident response en het versterken van de algehele beveiligingsstrategie.

Incident Response retainer

Wanneer het SOC over een volwaardige incident respons capability beschikt, bekend dit dat het team zelfstandig in staat is om security incidenten af te handelen. Dit omvat zowel het managen van het incident zelf als het uitvoeren van forensisch onderzoek ter ondersteuning van het security incident managementproces. Het kan echter nodig zijn om in sommige gevallen terug te kunnen vallen op externe expertise en capaciteit, bijvoorbeeld in de volgende gevallen:

- Bij grootschalige incidenten.
- Bij incidenten waar bijzondere expertise bij noodzakelijk is die niet voorhanden is in het SOC.
- Wanneer het SOC niet over een volwaardige incident response capaciteit beschikt.
- Indien er een onafhankelijk onderzoek van een derde partij nodig is.

Om gebruik te kunnen maken van deze externe expertise kan een retainer afspraak gemaakt worden met één of meerdere leveranciers. In deze retainer wordt vastgelegd wanneer en onder welke voorwaarde een beroep gedaan kan worden op deze additionele incident respons capaciteit en expertise. Regelmatig oefenen met de retainer is daarbij ook belangrijk.

Meldplicht

Het is van belang om voor security incidenten goed te kijken naar de verplichtingen (zoals de Cyber Beveiligings Wet, CBW) [15] die de organisatie heeft voor het melden van incidenten. Ook moet de organisatie keuzes maken voor wanneer aangifte gedaan wordt in geval van incidenten.

¹⁵ <https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN>

Best Practices voor uitvoering*Evaluatie*

Voor de operatie is het met name de evaluatie stap binnen het proces heel belangrijk. Deze stap is essentieel om de weerbaarheid van de organisatie en de effectiviteit van incident response te verbeteren. Na het afsluiten van een incident dient altijd een post-incident analyse plaats te vinden. Bij deze analyse wordt gekeken naar de oorzaak van het incident. Daarnaast wordt een analyse gedaan van het security incident respons proces. De geleerde lessen hieruit worden gebruikt voor:

- **Preventie.** Voorkomen van soortgelijke incidenten in de toekomst door maatregelen aan te passen of in te richten
- **Detectie.** Snellere detectie van soortgelijke incidenten in de toekomst realiseren door het implementeren of wijzigen van monitoring regels
- **Respons.** Efficiëntere en/of effectievere respons op soortgelijke incidenten door het security incident respons proces te optimaliseren.

Optimalisatie

Een relevant raamwerk bij security incident management is het RE&CT framework. Aan de hand van dit raamwerk kan in kaart gebracht worden welke activiteiten door het SOC uitgevoerd (kunnen) worden. Ontbrekende activiteiten kunnen opgebouwd worden via het Continuous Improvement proces. Door gebruik te maken van het RE&CT framework wordt ook direct een koppeling met het MITRE ATT&CK® framework gemaakt.

Oefening

Tenslotte is het van groot belang om regelmatig te oefenen. Daarmee wordt geborgd dat het SOC in staat is om adequaat en effectief te reageren in geval van daadwerkelijke incidenten. Zoals eerder besproken kunnen dit oefeningen zijn binnen de organisatie, of daarbuiten. Indien het respons team onderdeel is van een community kan ook geoefend worden in die community.

9.3 Security Analysis & Forensics

De dienst security analysis & forensics is primair ondersteunend aan incident respons. In deze dienst zit de expertise om forensische onderzoeken uit te voeren op apparatuur, zoals computers, USB-sticks en mobiele telefoons. Daarnaast zit in deze dienst ook de expertise om statische en dynamische analyse te kunnen uitvoeren van malware.

Dit type analyse is vrij specifiek. Niet elk SOC zal voldoende kennis en kunde in huis hebben om deze dienst zelf uit te voeren. In een dergelijk geval is het mogelijk om deze activiteiten extern uit te laten voeren. Ook wanneer een security incident mogelijk kan leiden tot een strafzaak is het noodzakelijk om een externe partij het forensische onderzoek uit te laten voeren. Dit in verband met rechtsgeldigheid en het ontbreken van opsporingsbevoegdheid bij het SOC.

9.3.1 Servicelevels en KPI's

Omdat het een ondersteunende functie betreft zijn servicelevels niet van toepassing op deze dienst.

Wel zijn een aantal relevante KPI's te benoemen:

- Gemiddelde tijd om een forensisch onderzoek af te ronden.
- Gemiddelde tijd om malware analyse uit te voeren.
- Percentage automatisering toegepast op onderzoek. Hiermee kan gezorgd worden voor verder optimalisatie en efficiëntie van het onderzoeksproces. Deze KPI kan gekoppeld worden aan de eerste twee.

9.3.2 Service RACI

In de RACI voor security analysis & forensics dienen tenminste de volgende activiteiten belegd te worden:

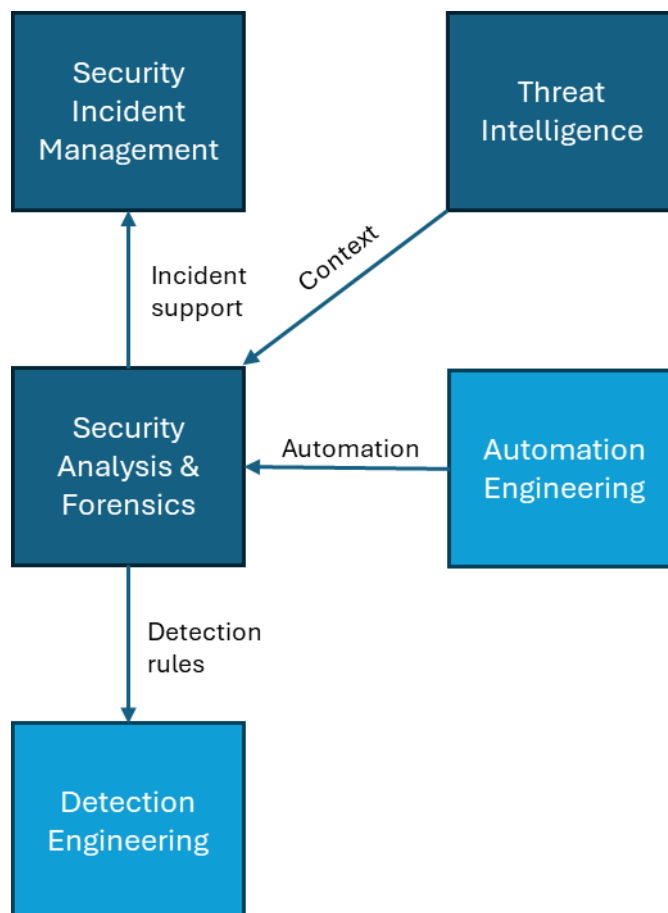
- Bepalen beleid/voorschriften voor security analysis & forensics;
- Uitvoeren van security analysis & forensics onderzoeken;
- Opstellen rapportages.

9.3.3 Service onboarding

Security Analysis & Forensics is een ondersteunend proces voor security incident management. Voor dit proces is geen expliciete onboarding nodig.

9.3.4 Procesarchitectuur

Onderstaande figuur is een generieke procesarchitectuur voor security analysis & forensics.



Figuur 5: Security analysis & forensics procesarchitectuur

9.3.5 Best Practices voor security analysis & forensics

Best Practices voor inrichting

Voor de inrichting is het belangrijk dat de medewerkers voldoende getraind zijn en de beschikking hebben over de juiste apparatuur en procedures (zoals het vastleggen van *Chain of Custody*) om onderzoeken te kunnen uitvoeren. Het is daarbij helpend om forensische apparatuur op een vaste afgesloten locatie (of bijvoorbeeld een koffer) te hebben, zodat deze altijd voorhanden is wanneer deze nodig is. Belangrijk is dat deze koffer regelmatig onderhouden en gecontroleerd wordt. Deze moet verder voor niemand toegankelijk zijn, behalve voor de relevante analisten.



Best Practices voor uitvoering

Voor de uitvoering moet gezorgd worden dat de medewerkers van het SOC die deze onderzoeken uitvoeren dit met regelmaat doen om hun kennis en kunde bij te houden. Verdere trainingen kan ook een manier zijn om de kennis actueel te houden.

Door automatisering toe te passen op het proces wordt de efficiëntie van het proces verhoogd. Tegelijkertijd wordt de kans op fouten geminimaliseerd.

9.4

Cyber Threat Intelligence

De dienst Cyber Threat Intelligence (CTI) heeft als doel het in kaart brengen van het cyber dreigingslandschap en het vroegtijdig identificeren van voorbereidingen voor het aanvallen van de organisatie. Tot het in kaart brengen van het dreigingslandschap behoort het identificeren van relevante dreigingsactoren, het identificeren van relevante aanvalstechnieken en het vaststellen van trends in aanvallen. Deze informatie wordt gebruikt om de weerbaarheid van de organisatie tegen cyberaanvallen te verhogen en actuele aanvallen te kunnen detecteren en afslaan. CTI heeft daarmee een centrale rol in de SOC-processen, en moet sturend zijn in het stellen van prioriteiten.

Binnen het CTI-proces wordt informatie uit verschillende bronnen verzameld. Het betreft hier zowel open bronnen (open source intelligence (OSINT), als gesloten bronnen (waaronder het TIP en informatie vanuit samenwerkingsverbanden). Ook interne bronnen kunnen worden gebruikt, zoals security incidenten, threat hunt bevindingen en waarnemingen vanuit security monitoring binnen het SOC. Deze informatie wordt geanalyseerd en voorzien van duiding (context). Vanuit het CTI-proces gaat belangrijke input richting security monitoring (monitoring op indicatoren van aanvallen/IOC's), Detection Engineering (use cases), threat hunting (hypothesen). Informatie uit het proces kan worden gedeeld binnen of buiten de organisatie.

CTI kan op verschillende niveaus uitgevoerd worden:

- **Strategisch niveau.** Dit is het niveau van CTI waarbij vooral gekeken wordt naar trends, campagnes en dreigingslandschappen.
- **Operationeel niveau.** Dit is het niveau van CTI waarbij vooral een focus is op technische indicatoren;
- **Tactisch niveau.** Dit is het niveau van CTI waarbij vooral Tactics, Techniques en Procedures (TTPs) een belangrijke rol spelen, die in kaart gebracht kunnen worden op bepaalde actoren d.m.v. het MITRE ATT&CK Framework.

Welke niveaus ondersteund worden door het SOC is afhankelijk van de requirements van de organisatie aan de CTI-dienst. Het is ook aan te raden om gebruik te maken van Priority Intelligence Requirements (PIR's) om aan de informatiebehoefte van de organisatie te voldoen.

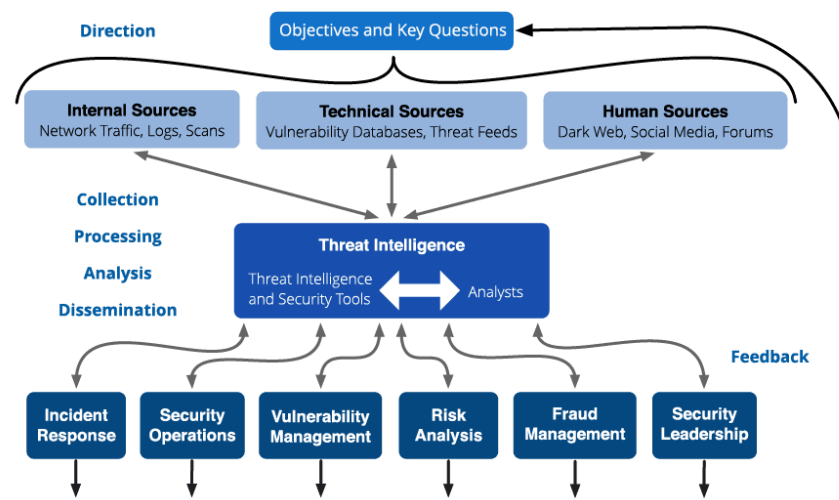
Belangrijk bij CTI is dat rapportages *actionable* zijn. Dat betekent dat er concreet handelsperspectief wordt geboden voor de afnemers van de rapportage. Per type afnemer kan de informatiebehoefte verschillen qua formaat en detail van de aangeboden informatie. Het is van belang dat het CTI-team goed inzicht heeft in deze informatiebehoefte en daarop inspeelt met de inhoud van de rapportage.

CTI-lifecycle

Het uitvoeren van CTI vindt op een gestructureerde manier plaats. Daarvoor wordt een lifecycle toegepast die bestaat uit een aantal stappen:

- **Direction.** In deze fase worden de doelstellingen en strategische richting van threat intelligence bepaald
- **Collection.** In deze fase wordt informatie verzameld uit geselecteerde bronnen. Bronnen worden regelmatig getoetst op toegevoegde waarde en kwaliteit.
- **Processing.** In deze fase worden de verzamelde informatie bij elkaar gebracht.
- **Analysis.** In deze fase vindt de daadwerkelijke analyse plaats. Daarbij wordt gekeken naar de impact van de informatie voor de organisatie en wordt ook het handelingsperspectief (course of action) uiteengezet.
- **Dissemination.** In deze fase wordt de informatie gedeeld met de belanghebbenden. Dit kunnen belanghebbenden zijn binnen het SOC (bijvoorbeeld: Detection Engineering voor het maken van nieuwe detecties op basis van CTI), alsook belanghebbenden binnen de organisatie en daarbuiten. Dissemination vindt op een gestructureerde manier plaats. Technische informatie wordt gedeeld via het threat intelligence platform en/of opgenomen in een rapport.
- **Feedback.** In deze fase wordt feedback verzameld om het proces te verbeteren.

Onderstaande figuur toont de CTI life cycle.



Figuur 6: Threat Intelligence life cycle ^[16]

OSINT

Een activiteit binnen het CTI-domein is het verzamelen en omgaan met open source intelligence (OSINT). Dit is informatie uit openbare bronnen die gebruikt wordt om cyber risico's voor de organisatie in kaart te brengen, indicatoren van een op handen zijnde aanval te ontdekken en alerts en incidenten van meer contextuele informatie te voorzien. Voor OSINT worden verschillende externe bronnen gemonitord, bijvoorbeeld om vast te stellen of interne informatie van de organisatie publiek gemaakt is, of dat mogelijk sprake is van compromitteren van accounts. Dit gebeurt op het reguliere internet, maar ook op het dark web, hackersfora of in (besloten) Telegram-kanalen. Het is daarbij belangrijk om te blijven opereren binnen de

¹⁶ Bron: <https://www.recordedfuture.com/blog/threat-intelligence-lifecycle-phases>

juridische kaders. In [Annex D - Juridische kaders](#) zijn enkele van de kaders voor de Rijksoverheid opgenomen.

9.4.1 *Servicelevels en KPI's*

CTI is vooral een ondersteunende dienst. Daarom zijn er geen servicelevels van toepassing.

Wel kunnen KPI's gedefinieerd worden om de performance van de dienst te monitoren en te verbeteren. Voorbeelden van dergelijke KPI's zijn:

- Aantal CTI rapporten per periode;
- Aantal geduide IOC's gedeeld;
- Gemiddelde tijd benodigd voor CTI-analyse.

9.4.2 *Service onboarding*

Voor threat intelligence bij in-house SOC's is geen expliciete onboarding noodzakelijk.

9.4.3 *Service RACI*

In de RACI voor threat intelligence dienen tenminste de volgende activiteiten belegd te worden:

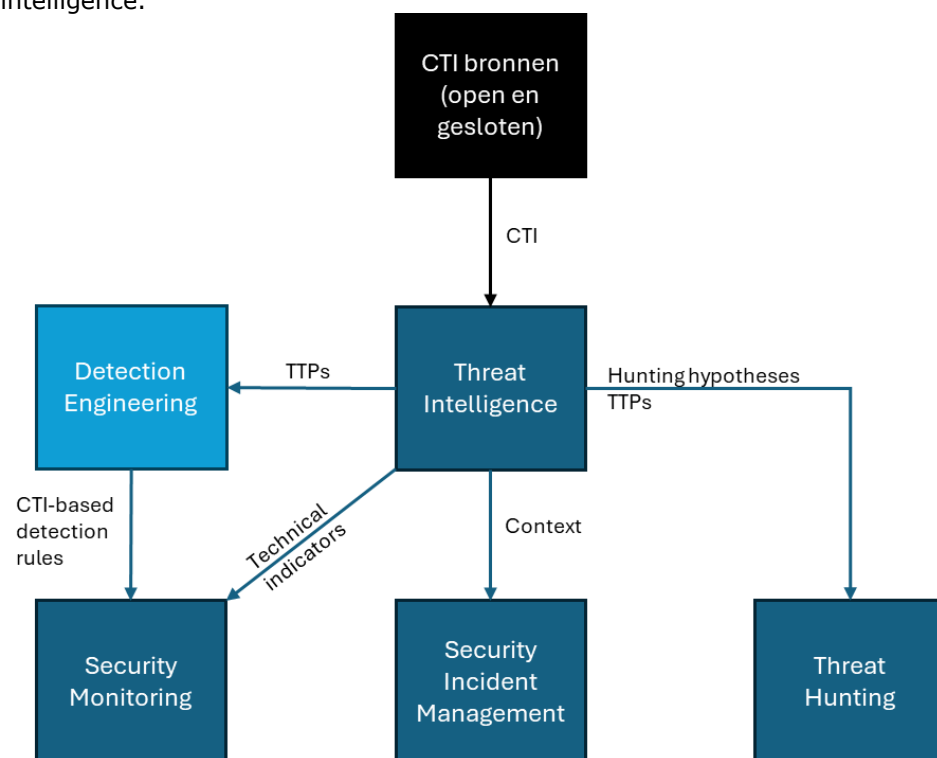
- Verzamelen en analyseren van dreigingsinformatie;
- Beheren van CTI-bronnen;
- Informeren organisatie over cyberdreigingen;
- Opstellen rapportages.

Indien CTI ook op strategisch niveau toegepast wordt, zijn de volgende activiteiten ook van toepassing:

- Opstellen strategisch dreigingslandschap op basis van de scope van de CTI-dienstverlening, in samenwerking met de business/bedrijfsvoering;
- Vertalen dreigingslandschap naar tactisch/operationeel niveau.

9.4.4 *Procesarchitectuur*

Onderstaande figuur is een generieke procesarchitectuur voor cyber threat intelligence.



Figuur 7: : Cyber Threat Intelligence procesarchitectuur



9.4.5 Best Practices voor threat intelligence

Best Practices voor inrichting

Allereerst is het bij de inrichting van de dienst belangrijk om vast te stellen welke niveaus van threat intelligence gehanteerd worden binnen het threat intelligence proces (strategisch, tactisch, operationeel). Het uitgangspunt daarbij is dat er toegevoegde waarde is voor de organisatie voor elk niveau dat geïmplementeerd wordt en dat er ook voldoende capaciteit beschikbaar is om de dienst op een kwalitatief goede wijze te kunnen uitvoeren.

Best Practices voor uitvoering

Voor de uitvoering dient het SOC regelmatig de CTI-bronnen opnieuw te evalueren. Bij deze evaluatie moet gekeken worden of bestaande bronnen nog voldoende toegevoegde waarde hebben en of nieuwe relevante bronnen aangesloten moeten worden.

Daarnaast is het belangrijk om vast te stellen of de rapportages die uitgebracht worden voldoende aansluiten bij de behoefte van de afnemers. Dit kan gedaan worden door samen met de afnemers te evalueren en, indien nodig, verbeteringen door te voeren.

9.5 Threat Hunting

De dienst threat hunting heeft als doel om onopgemerkte dreigingen die aanwezig zijn in de infrastructuur te identificeren. Waar security monitoring vooral reactief is (actie na detectie door de tooling) is threat hunting proactief (actief zoeken naar mogelijke indicatoren van het compromitteren van een IT-asset). Het uitgangspunt daarbij is *assume breach*, ofwel: uitgaan dat de ICT-omgeving al gecompromitteerd is, maar dat dit nog niet opgemerkt is in de monitoring.

Bij threat hunting onderzoeken kan ook Tactieken, Technieken en procedures worden onderzocht om vast te stellen of er afdoende bescherming is tegen het gebruik van de technieken en om vast te stellen welke sporen dit achter laat in de infrastructuur. Door gericht te zoeken naar deze sporen en de karakteristieken daarvan in kaart te brengen is het mogelijk om nieuwe detectie mogelijkheden te ontwikkelen.

Het uitvoeren van een threat hunting onderzoek kan op verschillende manieren:

- **Hypothese-gedreven hunting.** Een threat hunting onderzoek start daarbij met een hypothese. Deze hypothese kan ingegeven zijn door threat intelligence, maar kan ook voortkomen uit andere bronnen zoals historische incidenten en kroonjuweel analyse. Vervolgens wordt de analyse uitgevoerd. Veelal betreft dit een analyse van bestaande data. Het kan ook nodig zijn eerst relevante data te genereren door het draaien van een (hacking) tool in een gecontroleerde omgeving. Uit een threat hunting onderzoek komt altijd een onderzoeksrapport. Daarnaast kan een onderzoek ook incidenten opleveren, kwetsbaarheden of nieuwe detecties voor gebruik in real-time monitoring.
- **Baseline-gedreven hunting.** Hierbij is het uitgangspunt een baseline van regulier gedrag van mensen en systemen. Tijdens de hunt ligt de focus op het vinden van afwijkingen van het reguliere gedrag.
- **Machine Learning-gedreven hunting.** Hierbij wordt op basis van machine learning modellen gezocht naar mogelijke tekenen van incidenten. Deze machine learning werkt ook op basis van baselines, maar kent een hogere mate van automatisering.



Hypothese-gedreven hunting wordt in meer detail beschreven in de Targeted Hunting integrating Threat Intelligence (TaHiTI) methodologie voor threat hunting. Het proces wat daarin uitgewerkt staat is vergelijkbaar met wat in Prepare, Execute, and Act with Knowledge (PEAK) framework^[17] getoond wordt.

9.5.1 *Servicelevels en KPI's*

Threat Hunting diensten in een in-house SOC kennen veelal geen servicelevels, omdat het een ondersteunende dienst is.

Voorbeelden van relevante KPI's voor threat hunting zijn:

- **Aantal gevonden incidenten.** Het aantal incidenten wat gevonden is tijdens het uitvoeren van een threat hunting onderzoek.
- **Aantal nieuwe detectie regels ontwikkeld.** Het aantal nieuwe detectie regels wat ontwikkeld is gedurende threat hunting onderzoeken. Deze regels kunnen overgedragen worden aan de security monitoring dienst voor real-time monitoring.
- **Aantal aanbevelingen voor verbetering.** Tijdens threat hunting onderzoeken kunnen ook andere kwetsbaarheden of mogelijkheden voor verbetering aan het licht komen.
- **Hoeveelheid tijd gespendeerd aan threat hunting.** De totale hoeveelheid tijd die gebruikt is voor threat hunting, zowel in voorbereiding als in uitvoering en rapportage. Deze tijd kan ook uitgezet worden tegen de voorgenomen hoeveelheid tijd voor threat hunting. Op die manier kan gemonitord worden of threat hunting voldoende prioriteit krijgt in het geheel van security operations.

9.5.2 *Service onboarding*

Voor threat hunting bij in-house SOC's is geen expliciete onboarding noodzakelijk. Threat Hunting vindt veelal plaats op de centraal verzamelde informatie (SIEM), maar kan ook uitgevoerd worden op end-points met behulp van EDR of in het netwerk met behulp van NDR.

9.5.3 *Service RACI*

In de RACI voor threat hunting dienen tenminste de volgende activiteiten belegd te worden:

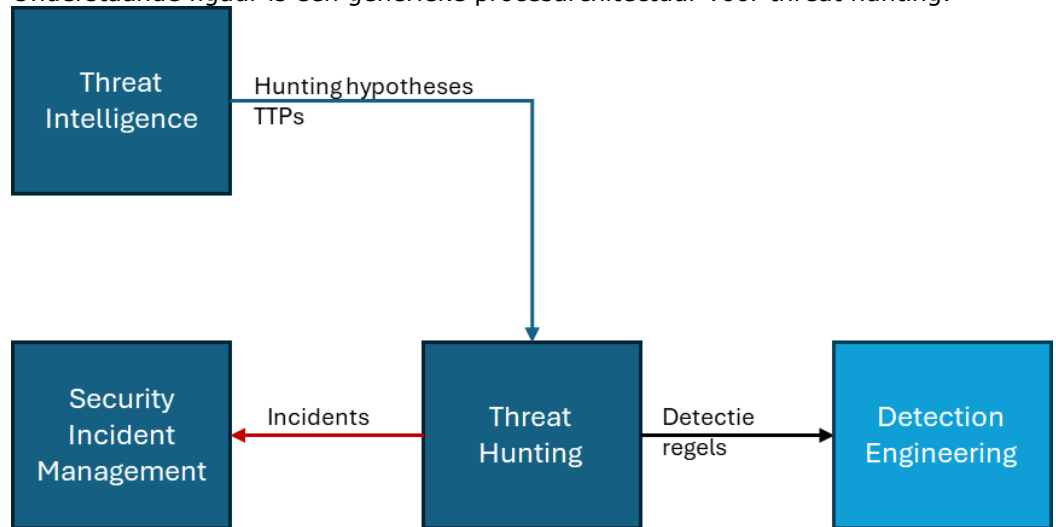
- Opstellen hypotheses;
- Uitvoeren threat hunting onderzoeken;
- Opstellen rapportages;
- Doorvoeren verbeteringen conform incident/problem proces.

¹⁷ https://www.splunk.com/en_us/blog/security/peak-threat-hunting-framework.html

9.5.4

Procesarchitectuur

Onderstaande figuur is een generieke procesarchitectuur voor threat hunting.



Figuur 8: Threat Hunting procesarchitectuur

9.5.5

Best Practices voor threat hunting

Best Practices voor inrichting

Voor het inrichten van Threat Hunting is een gedegen Threat Intelligence basis nodig, op basis van de vergaarde Threat Intelligence kan de hunting backlog opgezet worden. Prioriteer de hunts op basis van Threat Intelligence. Hypothese-gedreven threat hunting op basis van een framework zoals PEAK en TaHiTI is daarbij de basis. De overige vormen van threat hunting kunnen daaraan toegevoegd worden.

Best Practices voor uitvoering

Voor de uitvoering is het met name belangrijk dat zichtbaar wordt gemaakt wat het proces oplevert. Threat Hunting wordt vaak gezien als nevenactiviteit van het SOC, maar biedt belangrijke inzichten die niet uit andere processen naar boven komen. Deze inzichten moeten terugkomen in rapportages en KPI's zodat er een duidelijke aantoonbare toegevoegde waarde van het proces voor de organisatie is.

9.6

Vulnerability Management

De dienst vulnerability management heeft als doel het tijdig identificeren van kwetsbaarheden in de infrastructuur en applicaties van de organisatie. Bevindingen uit vulnerability management (kwetsbaarheden) dienen te worden opgevolgd om misbruik te voorkomen.

Vulnerability Management wordt uitgevoerd door het regulier scannen van de IT-omgeving van binnen en buitenaf, met behulp van geautomatiseerde tooling. Deze tooling stelt mogelijke kwetsbaarheden vast en rapporteert over de gevonden kwetsbaarheden. Vanuit het SOC worden de geïdentificeerde kwetsbaarheden geanalyseerd en voorzien van duiding en advies voor opvolging. De opvolging van de bevindingen wordt gedaan door de IT-teams van de organisatie; dit valt buiten de verantwoordelijkheid van het SOC. Dit zal veelal verlopen via het incident- of probleemproces binnen de organisatie.



9.6.1 *Servicelevels en KPI's*

Aan de vulnerability managementservice kunnen servicelevels toegekend worden. Veel voorkomende servicelevels daarbij zijn:

- Assets aangesloten op het vulnerability managementservice worden periodiek gescand
- Verzoeken tot het uitvoeren van een ad-hoc scan worden binnen een opgestelde SLA periode uitgevoerd.

Daarnaast zijn de volgende KPIs van toepassing:

- **Totaal aantal kwetsbaarheden.** Hiermee kan de trend van kwetsbaarheden over een langere periode gemeten worden. Differentiatie in de ernst van de kwetsbaarheid biedt verder inzicht.
- **Gemiddelde oplostijd van kwetsbaarheden.** De gemiddelde oplostijd van kwetsbaarheden geeft inzicht in hoelang de ICT-omgeving kwetsbaar blijft. Ook hier geeft differentiatie in de ernst van de kwetsbaarheid extra inzicht.
- **Aantal high & critical kwetsbaarheden niet tijdig opgelost.** Voor kwetsbaarheden moeten afspraken gemaakt worden over oplostijden. Kwetsbaarheden die niet tijdig opgelost worden, moeten gemonitord worden.
- **Coverage.** Het verbeteren van de coverage is belangrijk om zichtbaarheid van kwetsbaarheden in de gehele ICT-omgeving te krijgen. De informatie in de CMDB is daarbij leidend.

9.6.2 *Service onboarding*

Voor het onboarden in de vulnerability managementdienstverlening is het noodzakelijk om te voldoen aan de volgende voorwaarden:

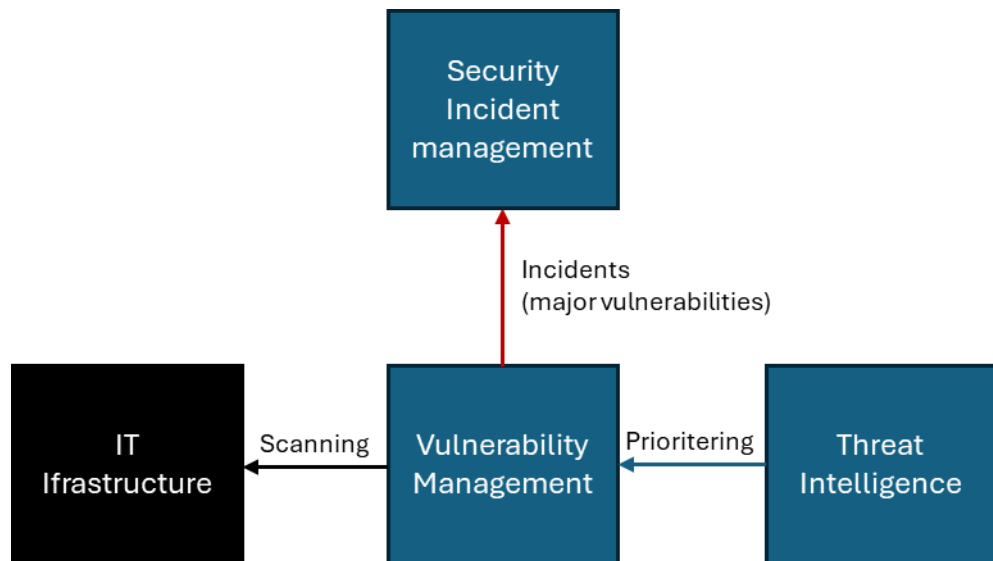
- De technische componenten zijn bekend.
- Toegang tot de componenten vanaf de centrale scanners is geregeld (netwerk toegang en lokale toegang met user accounts).
- Contact informatie voor kwetsbaarheden opvolging (rapportage) is beschikbaar.
- Het is duidelijk welke testen uitgevoerd kunnen worden op de technische componenten, zonder een gevaar voor de continuïteit van de dienstverlening te vormen.
- Alle teams binnen de organisatie zijn verplicht om aan te sluiten op de vulnerability managementdienstverlening. Dit wordt ondersteund door beleid.

9.6.3 *Service RACI*

In de RACI voor vulnerability management dienen tenminste de volgende activiteiten belegd te worden:

- Bepalen beleid/voorschriften voor vulnerability management;
- Aanvragen aansluiting apparatuur op reguliere scanning;
- Aanvragen ad-hoc scan;
- Aansluiten apparatuur op scanning platform;
- Uitvoeren scanning;
- Duiden bevindingen (kwetsbaarheden);
- Rapporteren bevindingen (kwetsbaarheden);
- Adviseren bevindingen (kwetsbaarheden);
- Monitoren tijdige opvolging bevinding (kwetsbaarheden);
- Opstellen rapportages.

9.6.4 Procesarchitectuur



Figuur 9: Vulnerability Management procesarchitectuur

In geval van kwetsbaarheden met een verhoogd risico kan een beroep gedaan worden op het security incident managementproces. Een voorbeeld daarvan is de log4j kwetsbaarheid die wijdverspreid was in componenten binnen elke ICT-omgeving. Onder normale omstandigheden worden kwetsbaarheden binnen reguliere ITIL-processen zoals incident- of problem-management afgehandeld. Binnen het Threat Intelligence proces kan de prioriteit worden vastgesteld welke services het grootste risico lopen en het eerst moeten gescand.

9.6.5 Overige activiteiten

Coordinated Vulnerability Disclosure (CVD)

Een bijzondere activiteit binnen het vulnerability managementproces is Coordinated Vulnerability Disclosure (CVD), voorheen Coordinated Vulnerability Disclosure (CVD)(RD). Iedereen, dus ook collega's, kan een melding maken van een kwetsbaarheid in een organisatie systeem en/of applicaties. Er kan hiervoor gebruik gemaakt worden van de dienstverlening van het SOC of een externe partij. Deze meldingen komen vaak uit bij het SOC. De meldingen worden gevalideerd en het betreffende team wordt geïnformeerd. Hiervoor kunnen direct security incidenten en problemen aangemaakt worden op basis van de gemelde kwetsbaarheden. Het team heeft vervolgens de taak om deze melding op te lossen binnen de daarvoor gestelde tijd conform CVD-beleid. Het SOC of de externe partij verzorgt de communicatie met de melder. De melder kan een waardering ontvangen voor het doen van de melding. De identiteit van de melder wordt in dit proces intern verborgen gehouden. Voor veel Rijksoverheid organisaties wordt is het meldpunt en de eerste triage belegd bij het NCSC.

Bug bounty programma

Als onderdeel van het CVD-proces kan een organisatie ook aansluiten op een bug bounty programma. De organisatie komt dan op een platform te staan waarbij security onderzoekers uitgenodigd worden kwetsbaarheden te vinden en te rapporteren. De initiële triage wordt door de het bug bounty programma gedaan. Veelal wordt hier een financiële beloning voor uitgekeerd.



Baseline scanning

Naast scanning op bekende kwetsbaarheden kan ook baseline scanning uitgevoerd worden. Hierbij wordt de configuratie van een systeem vergeleken met de gewenste configuratie (baseline) en worden afwijkingen op deze baseline (non-compliance) gerapporteerd. Veelal kan hier dezelfde tooling voor gebruikt worden. De meeste tooling beschikt over standaard CIS-baselines om tegen te kunnen meten.

Het eigenaarschap van de technische baselines moet goed worden belegd. Wat betreft het proces voor opvolging gelden hierbij dezelfde rollen en verantwoordelijkheden als voor regulier vulnerability management. Baseline scanning is zowel van toepassing op systemen in de eigen datacenters en ICT-omgeving als in de cloud. In het laatste geval wordt bij de baseline uitgegaan van de cloud security policy.

9.6.6

Best Practices voor vulnerability management

Best Practices voor inrichting

Voor de effectiviteit van het vulnerability managementproces is het belangrijk dat escalatielijnen duidelijk zijn. Indien kwetsbaarheden niet tijdig opgelost worden, of in het geheel niet opgelost worden, kan het SOC escaleren. Normaal gezien worden de reguleren escalatie lijnen hiervoor gebruikt.

Risicoacceptatie van kwetsbaarheden kan plaatsvinden. In een dergelijk geval wordt een kwetsbaarheid niet opgelost. Dat kan verschillende redenen hebben. Belangrijk is dat er expliciete risico acceptatie van het gevolg van het niet oplossen van de kwetsbaarheid plaatsvindt. Dat betekent dat er een eigenaar is van het risico en dat het risico met regelmaat opnieuw geëvalueerd wordt.

Best Practices voor uitvoering

De kwaliteit van het vulnerability managementproces is in sterke mate afhankelijk van de kwaliteit van de CMDB, waarin alle assets en configuratie opgenomen dienen te worden. De assets worden gebruikt om vast te stellen wat de coverage is van het proces en deze te optimaliseren; de configuraties worden gebruikt om, in geval van kwetsbaarheden op specifieke libraries of componenten, vast te kunnen stellen wat de scope is van de kwetsbaarheid. De CMDB is voor het SOC de *single source of truth*. Het correct vullen (eventueel geautomatiseerd met behulp van asset discovery) valt niet onder vulnerability management en is niet de verantwoordelijkheid van het SOC.

Voor de effectiviteit van het vulnerability managementproces is het aan te raden zaken te automatiseren, tenminste op de volgende onderdelen:

- Aanmaken problems/incidenten bij eigenaar
- Bepalen van de prioriteit en de daarbij horende afgesproken oplostijd
- Reminders
- Escalatie in de lijn
- Rapportage naar senior management over opvolging

Deze automatisering is belangrijk voor de schaalbaarheid van het proces.



9.7

Overige SOC-diensten

Naast de genoemde diensten komen de volgende diensten ook voor in Security Operations Centers:

- **Purple teaming.** Bij purple teaming wordt er samengewerkt tussen de verdedigers (blue team) en de aanvallers (red team). Het doel is om in gezamenlijkheid te toetsen of bepaalde aanvalstechnieken effectief zijn in de eigen ICT-omgeving, welke sporen deze technieken achterlaten, en of deze goed gedetecteerd kunnen worden. Micro Attack Simulation, en automatische tooling (zoals Breach & Attack Simulation) kunnen daarbij ondersteunend zijn.
- **Pentesting.** Pentesting is het uitvoeren van onderzoeken op applicatie of infrastructureel niveau. Het doel is om vast te stellen of systemen bestand zijn tegen aanvallen. Het pen testing proces levert inzicht in kwetsbaarheden op, die opgevolgd moeten worden. Bij de meeste SOC's wordt pentesting uitgevoerd buiten het SOC maar wordt het SOC wel geïnformeerd. Daarvoor kan het reguliere vulnerability managementproces gebruikt worden. De logging die geproduceert wordt door pentesting is waardevolle input voor Detection Engineering.
- **Security adviesfunctie.** Als expertisecentrum op het gebied van cyber security kan het SOC een security adviesfunctie invullen. Het SOC kan dan gevraagd en ongevraagd advies geven, bijvoorbeeld over de inrichting van bepaalde componenten. Het moet duidelijk zijn over welke onderwerpen het SOC adviseert, vooral als er ook een bredere adviesfunctie informatiebeveiliging onder de CISO valt.



10 Conclusie

Dit document heeft per onderdeel van het SOC-CMM raamwerk de Best Practices beschreven vanuit de Rijksoverheid, zowel voor de inrichting van een SOC als voor het uitvoeren van security operations. Belangrijk hierbij is om de samenhang tussen de verschillende elementen uit het SOC-CMM model te kunnen zien. Om effectieve security operations te kunnen draaien is het noodzakelijk om over alle domeinen van het model zorg te dragen voor voldoende volwassenheid. Kwalitatief goede diensten komen dus niet alleen voort uit het services domein, maar worden geleverd met behulp van goed ingerichte en beheerde technologie (technology domein), ondersteund door volwassen processen (process domein), uitgevoerd door gekwalificeerd personeel (people domein) en sluiten aan op de wensen van de belanghebbenden (business domein). Alle domeinen in het model zijn dus even belangrijk.

Bij het bouwen van een nieuw SOC is het goed om klein te beginnen, en te zorgen voor een brede en solide basis. Vanuit deze basis kan de operatie verder uitgebreid worden door het toevoegen van additionele diensten en het vergroten van de scope van security operations. Belangrijk daarbij is om de kern van de werkzaamheden (monitoring en respons) en de kwaliteit van deze werkzaamheden niet uit het oog te verliezen.

Bij het draaien van een bestaand SOC staat continue verbetering centraal. Dit kan gerealiseerd worden door de juiste metingen uit te voeren, en daar opvolging aan te geven met goed ingerichte governance. Een metrics programma met juiste KPIs, een *quality assurance* proces en regelmatige meting van het SOC in de volle breedte, geven het inzicht wat nodig is om op een effectieve manier te kunnen verbeteren waar dit het meest noodzakelijk is. Tenslotte is het ook noodzakelijk om te testen en te oefenen, zodat het SOC niet alleen op papier van hoge kwaliteit is, maar ook in de praktijk.

Annex A: lijst met gebruikte termen en afkortingen

Onderstaande tabel toont de alfabetische lijst met gebruikte termen en afkortingen binnen dit document.

Afkorting / term	Beschrijving
ATT&CK	Raamwerk wat een beschrijving geeft van technieken, tactics en procedures die gebruikt worden door aanvallers.
CTI	Cyber Threat Intelligence. Dreigingsinformatie over cyber aanvallen en actoren.
D3FEND	Framework met defensieve (mitigerende) maatregelen, gekoppeld aan aanvalstechnieken.
DeTT&CT	Tool voor het in kaart brengen van zichtbaarheid voor het SOC op basis van databronnen.
DPIA	Data Privacy Impact Analyse. Een analyse van de impact op de privacy van personen als gevolg van het implementeren van een proces en/of tool
EDR	Endpoint Detection & Response
FIRST	Forum for Incident Response Security Teams. Een community voor samenwerkende incident respons teams
J-SOC	Joint SOC. Een samenwerkingsverband tussen verschillende SOC's binnen de Nederlandse Rijksoverheid.
MaGMA UCF	MaGMA use case framework. Een raamwerk voor het structureren en doormeten van security monitoring use cases.
NDR	Network Detection & Response
NIST CSF	NIST Cyber Security Framework. Een breed raamwerk voor inrichting van cyber security binnen de organisatie.
NIST NICE	Een raamwerk waarin verschillende rollen binnen het cyber security medewerkersbestand uitgewerkt is in termen van kennis, kunde, competenties, en activiteiten.
NRN	Nationaal Response Netwerk. Een community van samenwerkende security incident respons teams
OSINT	Open Source Intelligence. Het proces van verzamelen van dreigingsinformatie (CTI) op basis van open bronnen.
PEAK	Methodologie voor het uitvoeren van threat hunting onderzoeken, opgesteld door Splunk.
RE&CT	Framework wat reactieve capabilities beschrijft die ingezet kunnen worden tijdens incident response, gekoppeld aan het Mitre ATT&CK® framework.
SIEM	Security Information & Event Management
SOAR	Security Orchestration & Automated Response
SOC	Security operations center
SOC-CMM	Een model en framework voor Security Operations Center, met een aantal producten, waarvan de volwassenheid assessment tool de meest relevante is voor dit document.
TaHiTI	Methodologie voor het uitvoeren van gestructureerde threat hunting op basis van dreigingsinformatie (CTI).
Tier	Een manier om analisten in verschillende niveaus te scheiden op basis van taken en verantwoordelijkheden.
TIP	Threat Intelligence Platform. Een platform voor het geautomatiseerd verwerken van dreigingsinformatie.
UEBA	User & Entity Behaviour Analytics.



Annex B: NIST CSF mapping

Onderstaande tabel toont de SOC-CMM domeinen en de NIST CSF functies waar deze aan gerelateerd zijn. Hierbij wordt alleen gekeken naar de belangrijkste functies en categorieën voor elk element van het SOC-CMM model. Voor de volledig uitgeschreven categorieën, zie [hoofdstuk 3 \(Security fundament\)](#).

SOC-CMM domein	SOC-CMM aspect	NIST CSF functie	NIST CSF categorie
Business	Business drivers	Govern	GV.OC
	Customers	Govern	GV.OC
	Charter	Govern	GV.OC
	Governance	Govern	GV.RM, GV.PO
	Privacy & policy	Govern	GV.PO
People	Employees	Govern	GV.RR
	Roles & hierarchy	Govern	GV.RR, GV.SC
	People management	Govern	GV.RR
	Knowledge management	Protect	PR.AT
	Training & education	Protect	PR.AT
Process	SOC management	Govern	GV.RR
	Operations & facilities	Identify, Protect	ID.IM, ID.AM, PR.IR
	Reporting & communication	Govern Respond	GV.RR RS.CO
	Use Case Management	Identify	ID.RA
	Detection Engineering Detection Engineering & validation	Identify	ID.IM
Technology	SIEM / UEBA	Govern, Protect, Identify, Detect	GV.RR, PR.IR, PR.AT, ID.IM, ID.AM, DE.CM, DE.AE
	NDR	Govern, Protect, Identify, Detect	GV.RR, PR.IR, PR.AT, ID.IM, ID.AM, DE.CM, DE.AE
	EDR	Govern, Protect, Identify, Detect	GV.RR, PR.IR, PR.AT, ID.IM, ID.AM, DE.CM, DE.AE
	SOAR	Govern, Protect, Identify, Detect	GV.RR, PR.IR, PR.AT, ID.IM, ID.AM, DE.CM, DE.AE



SOC-CMM domein	SOC-CMM aspect	NIST CSF functie	NIST CSF categorie
Services	Security Monitoring	Detect	DE.CM, DE.AE
	Security Incident Management	Respond	RS.CO, RS.MI, RS.AN, RS.MA
	Security Analysis & Forensics	Detect, Respond	DE.AE RS.AN
	Threat IntelligenceThreat Intelligence	Identify	ID.RA
	Threat Hunting	Detect	DE.CM, DE.AE
	Vulnerability Management	Identify	ID.RA
	Log management	Protect, Detect	PR.DS, DE.AE



Annex C: Trainingsplan

SOC-medewerkers dienen hun kennis op peil te houden waardoor deze in de gelegenheid moet worden gesteld om trainingen en seminars te volgen. Hierbij moet rekening worden gehouden dat de kosten voor dergelijke securitytrainingen hoger liggen. Het verdient de voorkeur dat de Security Analyst eerst de opleidingen volgt die deel uit maken van de functie op het basisniveau. Deze opleidingen geven een goede start om verdiepingsopleidingen te volgen.

Het is raadzaam om voor de functie security analyst een leerlijn te ontwikkelen passend bij het Functiegebouw rijk en het Kwaliteitsraamwerk Informatievoorziening (KWIV [¹⁸]). Het KWIV beschrijft de competenties en bekwaamheden voor professionals binnen de informatievoorziening.

Voor SOC-analisten betekent dit:

- Ontwikkeling van analytische en technische vaardigheden
- Kennisopbouw over incident response en threat hunting
- Soft skills zoals communicatie en samenwerking binnen multidisciplinaire teams

SOC-functies vallen binnen het functiegebouw Rijk in de functiegroepen Expert IV of (Senior) Adviseur Bedrijfsvoering. Deze functies vereisen een combinatie van:

- (Strategisch) Inzicht in security operations en dreigingslandschap
- Diepgaande technische expertise en threat intelligence
- Adviesvaardigheden voor beleidsvorming en procesoptimalisatie

De volgende pagina's geven een overzicht van een mogelijke leerlijn voor SOC-analisten en bevatten een (beknopt) opleidingsplan dat op basis van de organisatie behoefte aangepast kan worden.

¹⁸ <https://www.functiegebouwrjksoverheid.nl/kwaliteitsraamwerken/kwaliteitsraamwerk-informatievoorziening>



C.1 Opleidingsplan

Hieronder is een beknopt opleidingsplan weergegeven op basis van het SANS trainingscurriculum.

NIST NICE Role	Omschrijving	Gerelateerde terminologie	Level 1	Level 2	Level 3
Infrastructure support	Verantwoordelijk voor het bijhouden en optimaliseren van de SOC infrastructuur.	Platform/Systems/Security engineer			
Level 1	SEC401: Security Essentials		X		
	SEC406: Linux Security for InfoSec Professionals		X		
Level 2	SEC530: Defensible Security Architecture Implementing Zero Trust for the Hybrid Enterprise			X	
	SEC511: Continuous Monitoring and Security Operations			X	
Defensive Cybersecurity	Verantwoordelijk voor het analyseren van security events uit de security tooling.	Security Analyst			
Level 1	SEC450: Blue Team Fundamentals, Security Operations and Analysis		X		
	SEC406: Linux Security for InfoSec Professionals		X		
Level 2	SEC511: Continuous Monitoring and Security Operations			X	
	SEC541: Cloud Security Threat Detection			X	
	SEC504: Hacker Tools, Techniques and Incident Handling			X	
Level 3	SEC503: Network Monitoring and Threat Detection				X
Digital Forensics	Verantwoordelijk voor het uitvoeren van forensische onderzoeken.	Forensics analyst			
Level 1	FOR498: Digital Acquisition and Rapid Triage		X		
	FOR500: Windows Forensic Analysis		X		
Level 2	FOR518: Mac and iOS Forensic Analysis and Incident Response			X	
	FOR585: Smartphone Forensic Analysis In-Depth			X	
Level 3	FOR610: Reverse Engineering Malware: Malware Analysis Tools and Techniques			X	X
	FOR710: Reverse-Engineering and Malware: Advanced Code Analysis				X
Incident Response	Verantwoordelijk voor het uitvoeren van security incident response handelingen.	Security incident responder			
Level 1	SEC504: Hacker Tools, Techniques and Incident Handling		X		
Level 2	FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics			X	
	FOR572: Advanced Network Forensics, Threat Hunting, Analysis and Incident Response			X	
	FOR577: LINUX Incident Response and Threat Hunting			X	
	FOR509: Enterprise Cloud Forensics and Incident Response			X	
Level 3	FOR608: Enterprise-Class Incident Response and Threat Hunting				X
Threat Analysis	Verantwoordelijk voor het analyseren van dreigingsinformatie en het adviseren van de organisatie.	Threat intelligence analyst			
Level 1	Responsible for analyzing data and information from one or multiple sources to conduct preparation of the operational environment, respond to requests for information, and submit intelligence collection and production requirements in support of intelligence planning and operations.				
	SEC497: Practical Open Source Intelligence		X		
	FOR578: Cyber Threat Intelligence		X		
	FOR589: Cybercrime Intelligence		X		
	SEC504: Hacker Tools, Techniques and Incident Handling		X		
Level 2	Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of intelligence collection requirements. Evaluates performance of intelligence collection assets and operations.				
	FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics			X	
	FOR528: Ransomware and Cyber Extortion			X	
	SEC587: Advanced Open Source Intelligence			X	
Level 3	FOR610: Reverse Engineering Malware: Malware Analysis Tools and Techniques			X	X
	FOR710: Reverse-Engineering and Malware: Advanced Code Analysis				X
Vulnerability Analysis	Verantwoordelijk voor het analyseren van kwetsbaarheden en de potentiële impact op de organisatie.	Vulnerability analyst			
Level 1	LDR516: Vulnerability Management		X		
Level 2	SEC560: Enterprise Penetration Testing			X	
	SEC542: Web App Penetration Testing and Ethical Hacking			X	
Level 3	SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking				X
Cybersecurity Architecture	Verantwoordelijk voor het opstellen en bijhouden van een security architectuur voor het SOC.	Security architecture			
Level 2	SEC530: Defensible Security Architecture Implementing Zero Trust for the Hybrid Enterprise			X	
	SEC549: Cloud Security Architecture			X	
SOC Manager	Eindverantwoordelijk voor het SOC en de output van het SOC.				
Level 1	LDR551: Building and Leading Security Operations Centers		X		
SOC Lead	Verantwoordelijk voor inhoudelijke aansturing van een team binnen het SOC.				
Level 1	LDR551: Building and Leading Security Operations Centers		X		
Level 2	SEC511: Continuous Monitoring and Security Operations			X	
Detection Engineer	Verantwoordelijk voor het technisch realiseren en verbeteren van security monitoring regels.				
Level 2	SEC511: Continuous Monitoring and Security Operations			X	
	SEC503: Network Monitoring and Threat Detection			X	
	SEC595: Applied Data Science and AI/ Machine Learning for CyberSecurity Professionals			X	
	SEC541: Cloud Security Threat Detection			X	
Automation Engineer	Verantwoordelijk voor het toepassen van automatisering (al dan niet gebruik makend van SOAR technologie) binnen het SOC.				
Level 1	SEC573: Automating Information Security with Python		X		
Level 2	SEC598: Security Automation for Offense, Defense and Cloud			X	
Level 3	SEC673: Advanced Information Security Automation with Python			X	X
Threat Hunter	Verantwoordelijk voor het uitvoeren van threat hunting onderzoeken en het rapporteren van de uitkomsten van dergelijke onderzoeken.				
Level 1 and 2	FOR589: Cybercrime Intelligence		X	X	
	FOR578: Cyber Threat Intelligence		X	X	
Level 2	FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics			X	
	FOR572: Advanced Network Forensics, Threat Hunting, Analysis and Incident Response			X	
	FOR577: LINUX Incident Response and Threat Hunting			X	
	FOR528: Ransomware and Cyber Extortion			X	
Level 2 and 3	FOR610: Reverse Engineering Malware: Malware Analysis Tools and Techniques			X	X
	FOR608: Enterprise-Class Incident Response and Threat Hunting			X	X
	FOR710: Reverse-Engineering and Malware: Advanced Code Analysis				X



C.2 Leerlijn

C2.1 Tier 1 – Security Analyst

Security analyst	FGR	KWIV beschrijving	Vakinhoudelijke opleidingen	KWIV competenties	Internationale beroepsstandaard
Tier 1	Security analyst (Senior Adviseur Bedrijfsvoering) - Opsomming taken functiebeschrijving FGR competenties - Organisatiesensitiviteit - Analyseren - Overtuigingskracht - Netwerken - Omgevingsbewustzijn - Plannen en organiseren - Creativiteit Voor omschrijving competenties zie competentiewoordenboek FGR: pdf-competentie-gids april-2024.pdf (functiegebouwRijkoverheid.nl)	4.1.1 SECURITY MANAGEMENT IV-securitymanagement (informatiebeveiliging) richt zich op technische maatregelen die ingezet worden voor bescherming/beveiliging van een organisatie en de daarbij behorende medewerkers, klanten/gasten, data, financiën, goederen, et cetera. Het omvat het ontwerpen, implementeren, onderhouden en evalueren van beveiligingsmaatregelen met betrekking tot de IV (hardware en software). Securitymanagement is verantwoordelijk voor de beveiliging van de informatievoorziening (IV). De focus ligt op het beveiligen van de IV wat betreft de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie.	Basis SEC401: Security Essentials SEC406: Linux Security for InfoSec Professionals SEC450: Blue Team Fundamentals, Security Operations and Analysis Verdiepingsmogelijkheden SEC530: Defensible Security Architecture Implementing Zero Trust for the Hybrid Enterprise SEC511: Continuous Monitoring and Security Operations Professionalisering SEC503: Network Monitoring and Threat Detection	KWIV-competenties A.01 Afstemming informatiesysteem en bedrijfsstrategie A.07 Monitoren technologische ontwikkelingen D.01 Strategieontwikkeling informatiebeveiliging D.10 Informatie- en kennismanagement E.03 Risicomanagement E.08 Informatiebeveiligingsmanagement E.09 IT-governance Voor omschrijving competenties zie: Kwaliteitsraamwerk Informatievoorziening (KWIV) (rijksapplicaties.nl)	NICE workrole Cybersecurity Analyst / Engineer ECSF (European Cybersecurity Skills framework)



C2.2 Doorgroei binnen de functie (van tier 1 -> tier 2)

Benodigde ervaring	Benodigde competenties
• Ervaring binnen het Security vakgebied • Naast operationeel ook acteren op tactisch niveau • Grotere mate van zelfstandigheid : in staat om beveiligingsincidenten zelfstandig op te pakken. • Grotere mate van complexiteit van projecten en vraagstukken • Bredere scope van projecten en vraagstukken • Brede focus (op één of meerdere gebieden): weten wat er speelt buiten je eigen gebied en directie en hierop acteren.	Er komt meer nadruk te liggen op: Omgevingsbewustzijn Houdt rekening met relevante externe ontwikkelingen en omstandigheden • Volgt relevante ontwikkelingen buiten de eigen organisatie. • Signaleert ontwikkelingen en omstandigheden die invloed hebben op het eigen werkterrein. • Vertaalt externe ontwikkelingen en omstandigheden naar het eigen werkterrein



C2.3 – Tier 2 Security Analyst

Security analyst	FGR	KWIV beschrijving	Vakinhoudelijke opleidingen	KWIV competenties	Internationale beroepsstandaard
Tier 2	Security analyst (Senior Adviseur Bedrijfsvoering) - Opsomming taken functiebeschrijving FGR competenties - Organisatiesensitiviteit - Analyseren - Overtuigingskracht - Netwerken - Omgevingsbewustzijn - Plannen en organiseren - Creativiteit Voor omschrijving competenties zie competentiewoordenboek FGR: pdf-competentie-gids_april-2024.pdf (functiegebouwRijkoverheid.nl)	4.1.1 SECURITY MANAGEMENT IV-securitymanagement (informatiebeveiliging) richt zich op technische maatregelen die ingezet worden voor bescherming/beveiliging van een organisatie en de daarbij behorende medewerkers, klanten/gasten, data, financiën, goederen, et cetera. Het omvat het ontwerpen, implementeren, onderhouden en evalueren van beveiligingsmaatregelen met betrekking tot de IV (hardware en software). Securitymanagement is verantwoordelijk voor de beveiliging van de informatievoorziening (IV). De focus ligt op het beveiligen van de IV wat betreft de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie.	Basis SEC511: Continuous Monitoring and Security Operations SEC541: Cloud Security Threat Detection SEC504: Hacker Tools, Techniques and Incident Handling Verdiepingsmogelijkheden SEC503: Network Monitoring and Threat Detection SEC530: Defensible Security Architecture Implementing Zero Trust for the Hybrid Enterprise Professionalisering	KWIV-competenties A.01 Afstemming informatiesysteem en bedrijfsstrategie A.07 Monitoren technologische ontwikkelingen D.01 Strategieontwikkeling informatiebeveiliging D.10 Informatie- en kennismanagement E.03 Risicomanagement E.08 Informatiebeveiligingsmanagement E.09 IT-governance Voor omschrijving competenties zie: Kwaliteitsraamwerk Informatievoorziening (KWIV) (rijksapplicaties.nl)	NICE workrole Cybersecurity Analyst / Engineer ECSF (European Cybersecurity Skills framework)



C2.4 Doorgroei binnen de functie (van tier 2 -> tier 3)

Benodigde ervaring	Benodigde competenties
• Naast op operationeel en tactisch niveau ook acteren op strategisch niveau • Op organisatie niveau kunnen meedenken • Vertaling beleidswijzigingen CIO rijk naar huidige organisatie • Deelname aan Policy House overleg (overleg met CISO) • Aansturen van buitenwereld; contacten met BZK en leveranciers onderhouden • Een coördinerende rol voor de IB Specialisten/ inhoudelijk aansturen van IB specialisten	Er komt meer nadruk te liggen op: <u>Omgevingsbewustzijn</u> Houdt rekening met relevante externe ontwikkelingen en omstandigheden • Volgt relevante ontwikkelingen buiten de eigen organisatie. • Signaleert ontwikkelingen en omstandigheden die invloed hebben op het eigen werkterrein. • Vertaalt externe ontwikkelingen en omstandigheden naar het eigen werkterrein. <u>Organisatiesensitiviteit</u> Houdt rekening met de gevolgen van interne ontwikkelingen, beslissingen en acties voor de organisatie. • Kent het beleid, de spelregels, de verhoudingen en belangen in de (internationale) organisatie. • Is op de hoogte van relevante ontwikkelingen binnen de organisatie en bij eventuele ketenpartners. • Herkent gevoeligheden, risico's en kansen en handelt daarnaar. • Houdt bij beslissingen en acties rekening met de gevolgen voor de organisatie. • Gaat bij de juiste personen na of er draagvlak is. <u>Overtuigingskracht</u> Spant zich in om anderen te winnen voor een idee of standpunt. • Gebruikt logische en relevante argumenten. • Stemt argumenten en stijl af op de doelgroep. • Brengt op het juiste moment de juiste argumenten naar voren. • Brengt een voorstel of argumenten met stelligheid en enthousiasme

Annex D - Juridische kaders

De bewegingsvrijheid van een SOC wordt beïnvloed door juridische kaders. In deze paragraaf wordt een overzicht gegeven van de meest relevante regelgeving. Voor een goed begrip wordt de regelgeving onderverdeeld in drie categorieën;

1. het ambtenarenrecht ,
2. het strafrecht
3. het privaatrecht.

Voor een specifieke organisatie kan nog aanvullende wet- en regelgeving van toepassing zijn die voorschrijft wat wel en niet gedaan mag worden en die de samenwerking met andere organisaties beïnvloedt. Elke organisatie moet dit voor zichzelf in kaart brengen.

Ambtenarenrecht

Het ambtenarenrecht behelst de regelgeving die de arbeidsverhouding tussen de ambtenaar en het Rijk beheerst. De arbeidsverhouding wordt primair beheerst door de Ambtenarenwet. In het Algemeen Rijksambtenarenreglement (ARAR) is deze wet nader uitgewerkt voor het Rijk. Daarnaast gelden nog enkele regelingen specifiek voor het Rijk, waaronder de Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT 2016), het Beveiligingsvoorschrift Rijksdienst 2013 (BVR 2013), de gedragsregeling voor de digitale werkomgeving 2016, de Interne Klokkenluidersregeling Rijk, Politie en Defensie, het Normenkader beveiliging Rijkskantoren 2015 (NKBR 2015), het Kader Rijkstoegangsbeleid, het Programma van Eisen PKI Overheid, de Coordinated Vulnerability Disclosure (CVD)procedure voor het Rijk, het Voorschrift Informatiebeveiliging Rijksdienst (VIR2007) en het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI 2013).

Strafrecht

De strafrechtelijke vervolging van een (niet-)ambtenaar en/of de Rijksoverheid zelf vereist dat een overtreding of een misdrijf is gepleegd als beschreven in het wetboek van strafrecht.

Speciale aandacht verdienen de bepalingen:

- Artikel 138ab WvSR – computervredebreuk;
- Artikel 350a/b WvSR – gegevensbeschadiging;
- Artikel 32a Auteurswet – doorbreken beveiligingsmaatregelen in programmatuur.

Privaatrecht

De privaatrechtelijke aansprakelijkheid van een (niet-)ambtenaar en/of de Rijksoverheid zelf moet gebaseerd zijn op een actie uit onrechtmatige daad (artikel 6:162 BW). De basis voor een onrechtmatige daadsactie kan liggen op uiteenlopende terreinen:

Inbreuk op een recht (burgerlijk wetboek) door het doen of nalaten in strijd met een wettelijke plicht uit bijvoorbeeld:

De Algemene Verordening Gegevensbescherming (AVG) – welke gegevens mag het SOC verzamelen en opslaan?

De Auteurswet – welke werken (programmatuur, geschriften, etc.) zijn beschermd tegen kopiëren en/of openbaarmaking

Inbreuk op hetgeen er volgens ongeschreven recht in het maatschappelijk verkeer betamelijk wordt geacht.

Gegevensbeveiliging en recht in het algemeen

Gegevensbeveiliging mag zich verheugen in een aanhoudende brede politieke belangstelling, hetgeen tot uiting komt in internationale wetgevingsactiviteiten (strafvorderlijke gegevensvergaring, computercriminaliteit, aansprakelijkheid voor serviceproviders, etc.) en beleidsvoornemens (nationaal bureau voor cybercrime, code voor informatiebeveiliging, etc.). De organisatie overschrijdende activiteiten vragen om een brede blik op beveiliging en vereisen een flexibel SOC dat kan inspelen op dergelijke ontwikkelingen. Op juridisch gebied kan de Afdeling Juridische zaken van de organisatie hierin een rol spelen.



BIO

Een Security Operations Center (SOC) binnen de Rijksoverheid moet voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO stelt eisen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en is gebaseerd op de internationale ISO 27001- en ISO 27002-normen. Voor een SOC zijn met name de volgende BIO-eisen van belang:

- Risicobeheer: Het SOC moet periodiek een risicoanalyse uitvoeren en passende beheersmaatregelen implementeren om dreigingen te mitigeren.
- Toegangsbeheer: Strikte autorisatie- en authenticatieregels zorgen ervoor dat alleen geautoriseerd personeel toegang heeft tot SOC-systemen en gevoelige informatie.
- Monitoring en logging: Het SOC dient continu netwerk- en systeemactiviteiten te monitoren en logs veilig op te slaan en te analyseren om afwijkingen te detecteren.
- Incidentrespons: Er moeten procedures en protocollen zijn voor het afhandelen van beveiligingsincidenten, inclusief escalatiemechanismen en forensisch onderzoek.
- Continuïteitsbeheer: Het SOC moet waarborgen dat zijn diensten operationeel blijven bij calamiteiten en moet herstelprocedures hebben om snel te kunnen reageren op verstoringen.

NIS2

De NIS2-richtlijn (Network and Information Security Directive 2) is de vernieuwde Europese richtlijn voor cybersecurity en vervangt de oorspronkelijke NIS-richtlijn. NIS2 stelt strengere eisen aan de beveiliging van netwerk- en informatiesystemen binnen essentiële en belangrijke sectoren, waaronder overheidsdiensten, energie, transport en gezondheidszorg.

Voor een Security Operations Center (SOC) heeft NIS2 belangrijke implicaties:

- Uitgebreide reikwijdte: Meer organisaties vallen onder de verplichtingen van NIS2, wat betekent dat SOC's vaker compliance moeten aantonen voor klanten en partners.
- Verhoogde beveiligingseisen: Organisaties moeten robuuste cybersecuritymaatregelen implementeren, zoals risicoanalyse, incidentrespons en beveiligingsmonitoring welke kernactiviteiten van het SOC zijn.
- Strikte rapportageverplichtingen: Incidenten met een significante impact moeten binnen 24 uur worden gemeld aan de bevoegde autoriteiten. Een SOC speelt een cruciale rol in het tijdig detecteren en rapporteren van dergelijke incidenten.
- Ketenverantwoordelijkheid: Organisaties zijn verplicht om cybersecurityrisico's in hun toeleveringsketen te beheren, wat betekent dat SOC's mogelijk de beveiliging van externe partijen moeten monitoren.
- Toezicht en sancties: Lidstaten krijgen strengere handhavingsbevoegdheden en kunnen boetes opleggen bij non-compliance. Dit benadrukt het belang van een goed ingericht SOC dat aantoonbaar voldoet aan de NIS2-vereisten.