TLP:GREEN

RISICOGESTUURDE SOC-PLANNING

Monitoring & Detectie – Readiness Assistance

Factsheet versie 1.4

Complexiteit document
Gemiddeld

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot netwerken, systemen en (gevoelige) informatie.

Monitoring- en detectiediensten zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring- en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om monitoring- en detectiediensten effectief in te kunnen zetten, is het essentieel om te kijken naar de bredere context van de organisatie en haar risico's. In deze context is het aan te bevelen een Security Operations Center risicogestuurd in te richten. Dit document "Risicogestuurde SOC planning" geeft houvast bij het risicogestuurd inrichten van de detectie voor een SOC binnen uw organisatie.

Achtergrond

VSSR levert verschillende kennisproducten die aansluiten bij de SOC Readiness Quickscan. In dit document worden handvatten geboden voor Security Operations, aansluitend bij de vragen op strategisch en tactisch niveau in de SOC Readiness Quickscan.

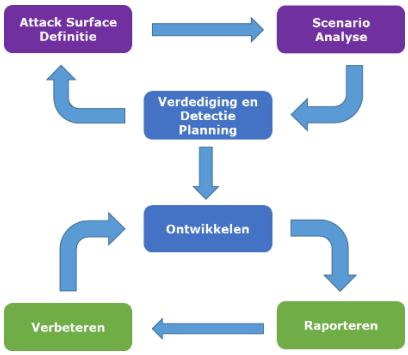
Doelgroep

De Versterken SOC-Stelsel Rijk (VSSR) voorziening biedt met dit document handvatten voor midden- tot hoogvolwassen SOC-organisatie om het SOC te optimaliseren op basis van realistische dreigingen voor de organisatie.

Management Samenvatting

Informatiebeveiliging is in essentie onderdeel van een breder risicobeheersingsbeleid binnen een organisatie. Om te bepalen hoe risico's het beste kunnen worden beheerst, dient in eerste instantie gekeken te worden naar de organisatie en de belangrijkste risico's voor de organisatie zodat op basis daarvan cyberdreigingsscenario's kunnen worden ontwikkeld binnen de context van de organisatie. In dit document worden cyberdreigingen en aanvalsoppervlak als uitgangspunt genomen om te bekijken hoe een Security Operations Center (SOC) detectie en monitoring het meest efficiënt kan inrichten met als doel bij te dragen aan het totaal van risicobeheersing binnen de organisatie.

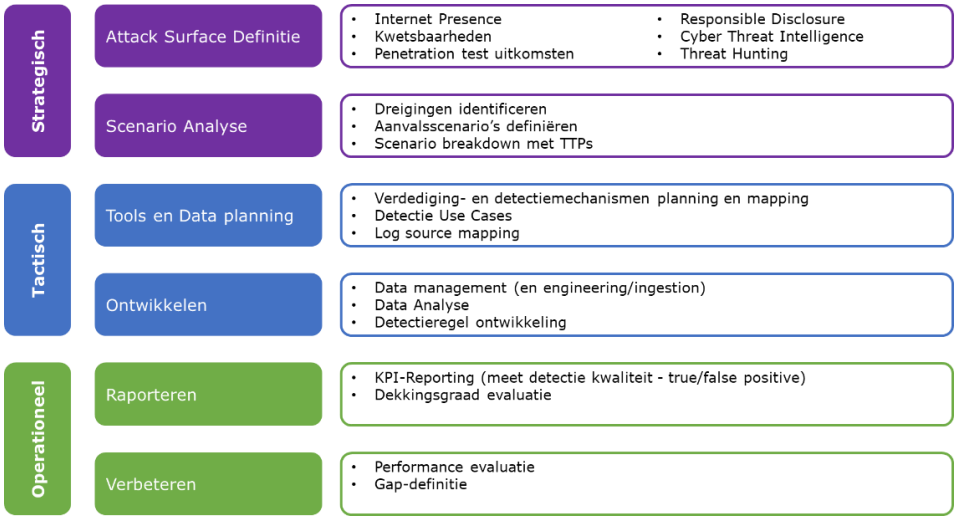
Het plannen en uitwerken van de verdedigings- en detectiestrategie voor een SOC kan procesmatig worden aangepakt. Een voorbeeld van een proces op hoofdlijnen, is weergegeven in Figuur 1 Risicogestuurd ontwikkelproces. De verschillende onderdelen binnen het proces zijn in meer detail onder te verdelen in strategische, tactische en operationele onderdelen met detailstappen zoals weergegeven in Figuur 2: Procesdecompositie.



Figuur 1 Risicogestuurd ontwikkelproces

Op strategisch vlak is het van belang om het aanvalsoppervlak goed in kaart te brengen zodat de bijbehorende risico's en dreigingen met mogelijk aanvalspaden gestructureerd vast kunnen worden gelegd. Met dit vertrekpunt kan de verdediging en detectie worden gepland. De eerste keer zal de inrichting van de procesonderdelen de nodige tijd in beslag nemen, maar als het eenmaal goed is gedaan, is de revisie (bijvoorbeeld jaarlijks) veel minder werk en dient deze vooral aangepast te worden op grote context wijzigingen binnen de organisatie of in het dreigingslandschap.

Vanuit de tactische planning kan het continue ontwikkelproces binnen het SOC worden aangestuurd om kort-cyclisch data- en detectieregels uit te breiden. Vervolgens worden rapportages gebuikt om continu operationele verbeteringen door te voeren, terwijl de strategische planning het ontwikkelproces blijft voeden (binnen de context van de strategische risicobeheersing). Daarnaast kunnen de verdedigingslinies periodiek worden geëvalueerd om in project vorm nieuwe middelen uit te rollen en oude uit te faseren.



Figuur 2: Procesdecompositie

De verschillende onderdelen worden binnen dit document verder toegelicht zodat een SOC-manager zijn strategie risico gestuurd kan opstellen. Op basis van deze strategie wordt vervolgens de operationele planning via een continu verbeterproces ingericht. Dit alles legt een goede basis voor een hoog-volwassen SOC.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	15-12-2023	Initiële versie
V1.1	29-2-2024	Weergave document complexiteit opgenomen
V1.2	08-4-2024	Fout correctie verwijzing naar VSSR DUCK portaal
V1.3	12-9-2024	TLP Markering opgenomen
V1.4	9-6-2026	Referenties geactualiseerd

1.2 Referenties

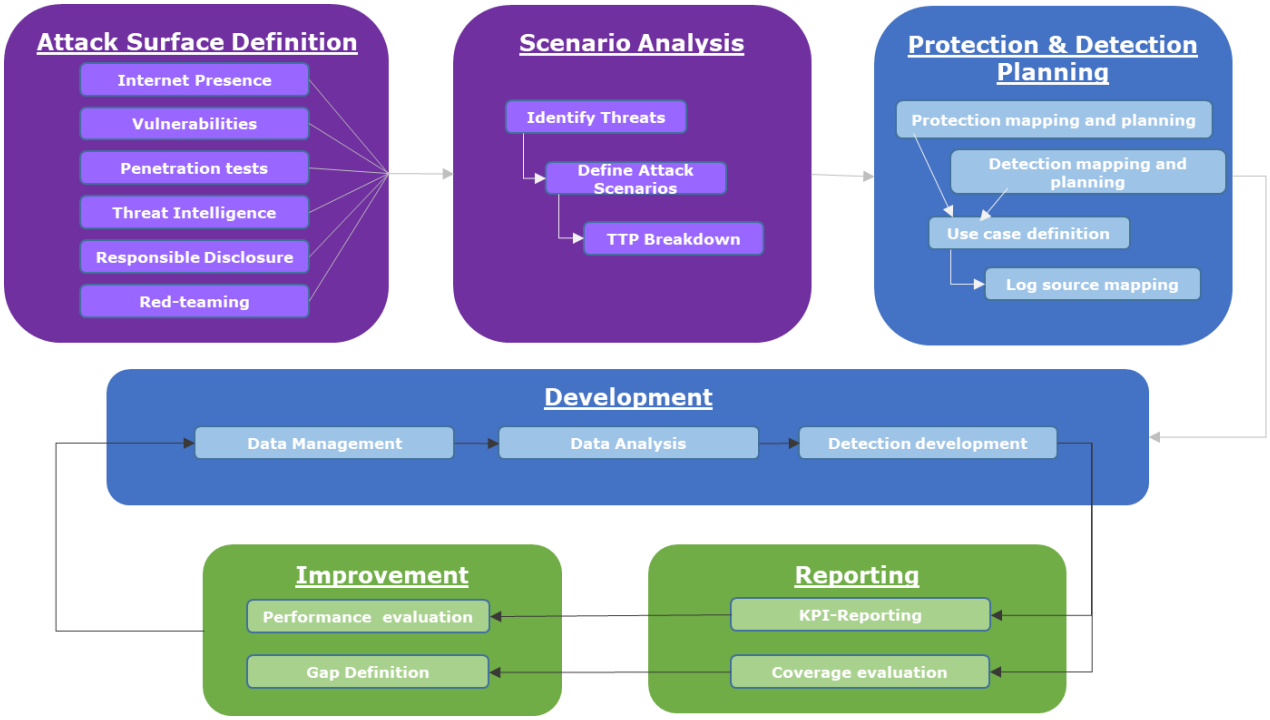
Document	Link
MITRE ATT&CK	MITRE ATT&CK®
MITRE D3FEND	D3FEND Matrix | MITRE D3FEND™
SIGMA	Home · SigmaHQ/sigma Wiki · GitHub
SOC Strategische Aanbevelingen	https://vssr.rijksapplicaties.nl/link?l=DOC-VSSR-MD-RA-SOC_Strategische_Aanbevelingen
Detectietechnieken en Use Case Kennisbank	Detectietechnieken en Use Case Kennisbank (DUCK)
VSSR-kennisdocumenten	VSSR (rijksapplicaties.nl)

1.3 Definities

Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Risicogestuurde SOC- Planning

Informatiebeveiliging in zijn geheel, kan in de kern worden teruggevoerd naar risicobeheersing. Ook voor Security Operations is het verstandig om risicogestuurd te werken. Hiermee kan altijd worden vastgesteld of het SOC binnen de context van de organisatie en een breder informatiebeveiligingsplan met de juiste dingen bezig is. Om dit gericht te kunnen doen is in Figuur 3: Risicogestuurd SOC-proces op hoofdlijnen uitgewerkt hoe dit in praktijk gebracht kan worden. De verschillende stappen zullen in de vervolgparagrafen verder worden toegelicht.



Figuur 3: Risicogestuurd SOC-proces

Risicobeheersing betekent in essentie[1]:

1) Contextbepaling: Vaststellen risicobereidheid en strategiebepaling.
2) Evalueren:
   a. Identificeren van dreigingen en kwetsbaarheden.
   b. Prioriteren op basis van waarschijnlijkheid, belangrijkheid en impact
3) Reageren: Voorkomen, mitigeren, accepteren, etc.
4) Monitor & bijstellen: Continue verbetering.

Het proces in Figuur 3: Risicogestuurd SOC-proces is opgedeeld in zes hoofdonderdelen en drie kleuren. Logischerwijs kan deze opdeling worden gerelateerd aan risicobeheersing (Tabel 1: Risicobeheersing en Security Operations planning) waarbij de "Contextbepaling" vooraf al is gedaan en in deze stappen (en dit document) verder niet terugkomt[2]:

	Risk Management	Security Operations Planning
	Evalueren	Aanvalsoppervlakbeheer
		Scenario Analyse
	Reageren	Beschermings- en Detectieplanning
		Ontwikkeling
	Monitoren & Bijstellen	Rapportage
		Verbeterplan

Tabel 1: Risicobeheersing en Security Operations planning

[1] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
[2] VSSR kennisdocument: SOC Strategische Aanbevelingen

De paragraafindeling in het verdere document is volgens dezelfde structuur opgezet. Het inrichten van het volledige proces zal de nodige tijd in beslag nemen en is veelal weggelegd voor meer volwassen SOC-omgevingen waar verschillende van de gebruikte competenties al aanwezig zijn. Tegelijkertijd is het niet strikt noodzakelijk om het SOC direct op basis van alle onderdelen in te richten. De verschillende paragrafen kunnen ook als afzonderlijke componenten worden gezien waarbij de introductie van een afzonderlijk component al kan bijdragen aan een volgende stap naar volwassenheid van het SOC. Een aantal voorbeelden van kleine verbeteringen zijn:

- Een bestaand SOC kan een nieuwe tool kunnen introduceren om het extern aanvalsoppervlakbeheer beter onder controle te krijgen. Op basis van de eerste scanresultaten kan worden besloten om een aantal bevindingen te mitigeren en voor anderen voorlopig detectie te bouwen.
- Een startpunt voor een nieuw op te zetten SOC (of voor uitbesteding) kan zijn om een dreigingsanalyse uit te voeren waar een eerste set aan use-cases uit wordt gedestilleerd.
- Een bestaand SOC zou samen met de organisatie kunnen inventariseren wat de belangrijkste IT-componenten binnen het landschap zijn (de kroonjuwelen) om deze dan als eerst op kwetsbaarheden te scannen en om detectie op in te richten.

Verder kan worden overwogen om eerst scenarioanalyse te doen en pas daarna te gaan kijken naar het aanvalsoppervlak. Op deze manier wordt eerst gekeken naar theoretische dreigingen en bijbehorende scenario's en pas daarna naar de bijbehorende effectieve risico's op basis van de feitelijke IT-infrastructuur en bijbehorende kwetsbaarheden.

2.1 Evalueren

2.1.1 Aanvalsoppervlakbeheer

Het aanvalsoppervlak, of Attack Surface, is het totaal van alle mogelijke digitale objecten die kunnen worden aangevallen door kwaadwillende derden of internen (Insider Threat). Het aanvalsoppervlak bestaat uit verschillende onderdelen zoals: alle koppelvlakken die direct via internet beschikbaar zijn, alle koppelvlakken naar derde partijen, componenten die direct op het Internet zijn uitgerold met behulp van bijvoorbeeld cloud-toepassingen. Via het aanvalsoppervlak worden eventuele kwetsbaarheden blootgesteld aan aanvallers. Door het uitbuiten van kwetsbaarheden of incorrecte configuratie krijgt een aanvaller daadwerkelijk toegang tot IT-componenten die van belang zijn voor de organisatie. Het is dus essentieel om voor het aanvalsoppervlak de verschillende kwetsbaarheden goed in kaart te hebben.

Attack Surface Management (ASM) is de competentie die zich richt op het in kaart brengen van dit aanvalsoppervlak met bijbehorende kwetsbaarheden. ASM is erg in opkomst (anno 2021[3]) waarbij er ook steeds meer tooling beschikbaar komt om dit te faciliteren. Binnen ASM zou de aandacht op zowel intern als extern aanvalsoppervlak moeten liggen. Veel tooling richt zich, echter, voornamelijk op blootstelling richting het Internet. Om compleet te zijn is het van belang om ook alle intern beschikbare infrastructuur en applicaties (asset database) mee te nemen. Hiervoor kan reguliere software voor het scannen op kwetsbaarheden worden gebruikt.

Naast het automatisch identificeren van het aanvalsoppervlak en bijbehorende kwetsbaarheden zijn ook processen als responsible disclosure, software penetratietesting en code-reviews op software van essentieel belang. Deze processen richten zich op de onderdelen die niet goed kunnen worden afgevangen met geautomatiseerd scannen. Geautomatiseerd scannen concentreert zich op bekende en gepubliceerde software kwetsbaarheden[4] [5] maar biedt geen, of weinig, inzicht in kwetsbaarheden of logicafouten binnen specifieke applicaties die voor een organisatie zijn gemaakt.

[3] Gartner® Report: Hype Cycle™ for Security Operations, 2022
[4] Home | CVE
[5] CVE - CVE (mitre.org)

Bedenk bij het in kaart brengen van het aanvalsoppervlak dat alles in één keer waarschijnlijk te veel is. Kijk waar de belangrijkste risico's liggen en begin dan daar met inventariseren en verbeteren. Een mogelijke volgorde kan zijn:

1. Extern aanvalsoppervlak;
2. Kroonjuwelen;
3. Legacy systemen;
4. Andere belangrijke data-dragende systemen;
5. Werkplekken;
6. Koppelingen met 3e partijen/leveranciers;
7. Overige IT-componenten.

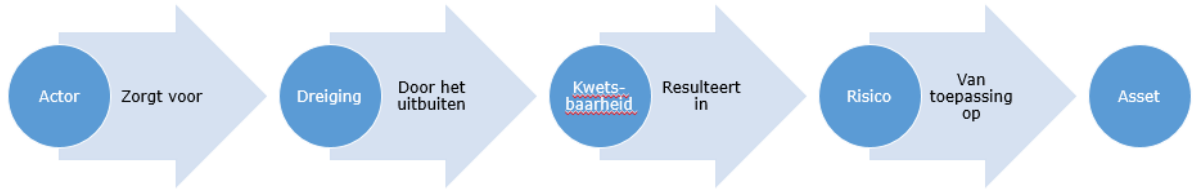
2.1.2 Scenario Analyse

Als het aanvalsoppervlak met bijbehorende kwetsbaarheden en gerelateerde risico's bekend zijn, kan systematisch in kaart worden gebracht wat de meest voordehand liggende aanvalsscenario's zijn. Een scenario beschrijft een doel (bijv. kroonjuweel), wie de meest voor de hand liggende aanvaller zou kunnen zijn (m.a.w. waar de dreiging vandaan zou kunnen komen) en wat het aanval pad zou zijn om het doel te bereiken.

Scenario-analyse is een meer moderne en dynamische variant van risicobeheersing waarbij vooral wordt gekeken naar de negatieve effecten van een aaneenschakeling van gebeurtenissen (tegenoverstaande de meer traditionele manier van *black-swan risicobeheersing* waarbij vooral wordt gekeken naar de meest onwaarschijnlijke, opzichzelfstaande gebeurtenissen met zeer grote gevolgen). Vooral de aaneenschakeling van verschillende gebeurtenissen, of aanvalsstappen, is hier van essentieel belang. Dit is voornamelijk omdat een aanval in de meeste gevallen niet bestaat uit een enkele gebeurtenis en de verschillende individuele stappen in de aaneenschakeling van gebeurtenissen op zichzelf vaak van beperkte impact zijn. Het totaal van de kleinere stappen resulteren, daarentegen, vaak wel in grote schade.

Voordat de aanvalsstappen in een scenario kunnen worden uiteengezet, is er eerst additionele informatie nodig. Eerst dienen mogelijke einddoelen voor de verschillende scenario's te worden geïnventariseerd. Dit gaat vaak om kritische data, systemen en processen (vaak samen te vatten als de kroonjuwelen of het te beschermen belang). Denk hierbij ook in termen van de mensen binnen de organisatie. De mailbox van een directeur is mogelijk belangrijker dan van een andere medewerker. Een IT-beheerder heeft vaak meer rechten en meer toegang binnen het IT-landschap dan andere gebruikers en is daarom een gewild doelwit.

Vervolgens is het van belang om te kijken naar mogelijke actoren om zo een inschatting te maken over wie de mogelijke aanvaller is en hoe deze is uitgerust. Een belangrijk kenmerk van statelijke actoren is bijvoorbeeld dat deze vaak veel tijd en middelen hebben om een goede aanval op te zetten. De scenario's en doelwitten waar dit op van toepassing is, verdienen dus extra aandacht. Om deze analyse verder kracht bij te zetten, is het goed om ook naar actuele dreigingen te kijken. Ransomware is bijvoorbeeld in toenemende maten een grote uitdaging voor veel organisaties en de frequentie van optreden lijkt als maar toe te nemen. Hier wil je je als organisatie tegen wapenen met de belangrijkste data voorop. In de markt is veel informatie beschikbaar over trends in dreigingen waarbij vaak meer lokaal toegespitste analyses[6]



Per scenario dient de verzamelde informatie te worden vastgelegd.

Scenario	
Dreiging	Ransomware-aanval

[6] Cybersecuritybeeld Nederland | Nationaal Cyber Security Centrum (ncsc.nl)

Scenario	
Beschrijving	Een criminele organisatie poogt bedrijf kritische informatie te gijzelen en vraagt geld om deze data weer vrij te geven. Als niet wordt betaald wordt de data publiek gemaakt en/of vernietigd.
Actor	Criminele Organisaties
Aanvalsoppervlak	Endpoint via email
Tactiek	Phishing
Doelwit	Bedrijf kritische informatie
	Eenvoudig: Het uitvoeren van een phishing campagne en bijbehorende ransomware aanval zijn vrij eenvoudig uit te voeren en kunnen zelfs als dienst worden ingekocht.
	Hoog: Ransomware aanvallen zijn al een geruime tijd erg in opkomst bij criminele organisaties vanwege de eenvoud en doeltreffendheid van uitvoering.
Gevolg/impact	Openbaar worden en/of vernietiging van gevoelige of bedrijfskritische informatie.
Stappen	1. Crimineel stuurt phishing email. 2. Gebruiker opent email, klikt op link. 3. Ransomware software installeert zich op de eerste machine. 4. Ransomware verspreidt zich door het netwerk. 5. Ransomware vernietigt backups 6. Ransomware versleutelt data.

Tabel 2: Voorbeeld dreigingsscenario

Als de verschillende scenario's op hoofdlijnen uiteen zijn gezet, wordt in de volgende stap een verdere detaillering naar aanvalstechnieken gedaan. Deze uiteenzetting beschrijft het aanvalsdraaiboek voor een specifiek scenario met behulp van aanvalstechnieken. Om dit goed en gedetailleerd doen, is het verstandig om hiervoor cyberspecialisten in te zetten die zijn opgeleid in het uitvoeren van red-team aanvallen of met een achtergrond in threat intelligence (een team met beide disciplines is vanzelfsprekend constructiever). Voor de uiteenzetting is het verstandig om een bekend raamwerk te gebruiken zoals MITRE ATT&CK™ [7]. Binnen dit raamwerk worden aanvalstechnieken, tactieken en procedures op een gestandaardiseerde manier uiteengezet, veelal ook in security tool geïntegreerd om zo op een uniforme wijze te kunnen werken.

De vastlegging van een deel van een scenario is in Tabel 3: Scenario vastlegging weergegeven.

Tactiek	Doelwit	ID	Techniek	Mitigatie	Detectie
Initial Access	Eindgebruiker	T1566	Phishing	Antiphishingbeveiliging	Geen
Execute	Endpoint	T1204.002	Malicious File	Endpoint Detectie en Repsonse (EDR)	Detecteer ongebruikelijk proces op endpoint
Command & Control	N/A	T1071.001	Web Protocols	Proxyserver	Detecteer ongebruikelijke communicatie via de proxyserver naar Internet
Exfiltration	Kritische data	T2053.001	Exfiltration over USB	USB-poort blokkade	Detecteer pogingen tot gebruik USB-poorten
Etc.					

Tabel 3: Scenario vastlegging

[7] MITRE ATT&CK®

2.2 Reageren

2.2.1 Beschermings- en Detectieplanning

Het Beschermings- en detectieplan gaat over het risicogericht [8]mitigeren van dreigingen, kwetsbaarheden en aanvalstechnieken. Als de verschillende scenario's en bijbehorende aanvalsdraaiboeken zijn uitgewerkt, wordt in eerste instantie gekeken naar de manieren waarop de organisatie zich met security tooling heeft gewapend tegen de verschillende aanvalsstappen. Daarna wordt bepaald welke detectie nodig is.

Om te bepalen tegen welke dreigingen de organisatie wel of niet is gewapend, kan een eenvoudig overzicht worden opgesteld, eventueel per scenario. Voor het opstellen van een overzicht van beschermende maatregelen kan gebruik worden gemaakt van bestaande raamwerken[9] om te onderzoeken welke mogelijke strategieën beschikbaar zijn. Het uiteindelijk doel is om tot een overzicht te komen zoals in Tabel 4: Matrix verdedigingslinies. Op basis van een overzichtsmatrix kan verder worden bepaald welk nog niet aanwezig zaken (rood) mogelijk ingericht moeten gaan worden op basis van een risicoafweging. Zo kan bijvoorbeeld op basis van onderstaand overzicht worden bepaald of, en in welke volgorde, Phishing protection, Application control, EDR, CTI en USB-poort blokkade ingericht moet gaan worden. In de overweging dient rekening gehouden te worden met het aantal en de omvang van de risico's die met een oplossing worden afgevangen. Daarnaast kan rekening worden gehouden maar haalbaarheid, doorlooptijd, eenvoud van implementatie, etc.

Tactiek	Deny	Disrupt	Detect	Contain
Reconnaissance	Firewall	Firewall	NIDS	
Initial Access	Phishing protection	AV	EDR	
Execute	Applicatie patching	Application control	Audit logs	
Command & Control	Web traffic blokkade		CTI	Netwerkzonering
Exfiltration	USB-poort blokkade		Audit logs	Netwerkzonering

Tabel 4: Matrix verdedigingslinies

Als de verdedigingsmechanismen in kaart zijn gebracht, kan een vergelijkbare oefening worden gedaan voor detectie. In veel gevallen zijn de verdedigingsmechanismen ook databron voor detectiesystemen. Het in kaart brengen van de noodzakelijke detectie gaat dan ook niet over applicatieve oplossingen maar meer over detectieregels om de verschillende aanvalsscenarios te kunnen detecteren. Dit bepaalt uiteindelijke wat het SOC-inzicht moet gaan geven in actuele aanvallen. Bij elke detectiemethode dient ook telkens de mogelijke databron te worden opgenomen. Dit geeft inzicht in de beschikbare data voor het SOC en dus de haalbaarheid van detectieonderdelen. Ook geeft het inzicht in welke data met welke prioriteit beschikbaar moet worden gemaakt.
De benodigde detectiemechanismen kunnen per aanvalstechniek worden opgenomen in een detectie scenario (use case) bibliotheek. Als deze stap effectief wordt uitgevoerd is er aan het eind van het proces een bibliotheek met detectieregels beschikbaar. Dit dient als input voor de bouwfase om als kleine brokjes werk te implementeren in de operationele detectie-tooling.

Al deze informatie is ook nodig om een overzicht te krijgen van het huidige beschermingsniveau, wat er nodig is qua detectie en om op basis hiervan een geprioriteerde planning te maken om verdere verbeteringen door te voeren. Tegelijkertijd is hiermee alle informatie voorhanden om zwakke plekken vast te stellen en strategische keuzes te maken. Vervolgens kan met deze informatie in handen ook rapportage worden opgezet om de vorderingen op logdata implementatie en detectie ontwikkeling bij te houden.

2.2.2 Ontwikkeling

Binnen het ontwikkelproces worden detectiescenario's omgezet naar detectieregels in verschillende detectiesystemen. Op hoofdlijnen bestaat de hele ontwikkeling uit de drie hoofdonderdelen: databeheer, data-analyse en detectieregels bouwen. Voor de verschillende onderdelen is het verstandig om processen te definiëren die aansluiten bij de eigen organisatie.

[8] VSSR Detectietechnieken en Use Case Kennisbank (DUCK)
[9] https://d3fend.mitre.org/

In eerste instantie kan binnen deze processen gebruik worden gemaakt van data die voorhanden is. Is de organisatie verder in volwassenheid dan kan ervoor worden gekozen om tijdens het ontwikkelen het red-team in te zetten. Een voor gedefinieerd scenario kan in praktijk worden uitgevoerd door het red-team waardoor de logdata de juiste aanknopingspunten van een aanval bevat en waarmee tekortkomingen in de data direct kunnen worden opgespoord en gecorrigeerd.

2.2.2.1 Databeheer

Databeheer is een continu proces om detectiesystemen te voeden met de juiste data. Het IT-landschap verandert continu dus de logdata verandert mee. Telkens als nieuwe systemen of applicaties in gebruik genomen worden, dient er te worden gekeken naar de relevantie binnen de kaders van detectie en monitoring van de data die kan worden aangeleverd. Tegelijkertijd verdwijnen er ook continu IT-toepassingen waarmee ook de data en bijbehorende configuraties wijzigen. Een ander onderdeel van databeheer betreft het goed verwerken van de data in de monitoring- en detectiesystemen. Bij wijzigingen of upgrades van applicaties kan het bijvoorbeeld zomaar gebeuren dat dataformaten anders zijn waar de detectiesystemen op aangepast horen te worden. Het is aan te bevelen om dit in de ontwerp-, wijzigings- en acceptatieprocedures van ICT-systemen op te nemen. Een ander belangrijk onderdeel dat bij databeheer hoort, is het continu beoordelen van relevantie van data: welke data is nodig voor detectie, hoe lang dient data van de verschillende bronnen te worden opgeslagen, en vooral: wat kan worden genegeerd of weggegooid om onnodige log verwerking en dataopslag te voorkomen?

Per databron of brontype is het van belang om op voorhand een aantal zaken in kaart te brengen om een goede inschatting van datavolumes te maken.

Type	#	Gem. EPS[10]	Piek EPS	Bytes	Retentie hot	Retentie cold
Firewall	5	250	500	200	30 dgn	90 dgn
Windows Srv.	100	50	100	300	60 dgn	180 dgn
Etc.						

Tabel 5: Inschatting datavolumes

2.2.2.2 Data-analyse

In een volgende stap wordt data-analyse gedaan. Hierbij wordt per use case bekeken of de data aanwezig is, of de kwaliteit in orde is (en wat eventueel nodig is om dit op orde te krijgen) en of de use case haalbaar is op basis van de data. De data-analyse fase kan voor een enkele use case soms ook verschillende bronnen beslaan. Let wel op de use case niet te breed is geformuleerd en te veel data beslaat want overmatige complexiteit draagt veelal niet bij aan een goed resultaat.

Bij de data-analyse voor een use case is het essentieel om een aantal zaken goed vast te leggen. De Threat Hunting discipline maakt vaak al gebruik van hypothesestelling voordat een onderzoek wordt gestart. De beschrijving zoals hier weergegeven, maakt ook gebruik van hypothesestelling en nog een aantal andere zaken. Vooraf goed beschrijven waar de data-analyse zich op richt, is belangrijk om focus in het onderzoek te houden en naar een doel toe te werken.

Vooraf:

- Achtergrond: Beschrijving van de context en de aanval waarop de use case betrekking heeft.
- Doel: Wat probeert de analist in de data te detecteren.
- Hypothese: Hoe verwacht de analist het geformuleerde doel te gaan bereiken.
- Scope: Geeft aan op welke data het onderzoek van toepassing is (en mogelijk welke applicatie, organisatieonderdeel, proces, etc.)

Tijdens:

- Onderzoeksstap: geef bij elke afzonderlijk stuk data-onderzoek aan wat er precies onderzocht gaat worden.

[10] EPS: Events per Second – het aantal log events dat per seconden wordt verstuurd/aangeleverd.

- Beschrijving: Beschrijf de analyse helder en duidelijk met ondersteuning van visuele representaties van de data.
- Resultaat: Beschrijf de uitkomst van het onderzoek en verbind hier mogelijk conclusies aan.

Na:
- Samenvatting: Maak een korte samenvatting van het onderzoek.
- Conclusie: verbind conclusies aan het onderzoek en beschrijf de haalbaarheid.
- Detectie: Geef een functionele beschrijving van de detectieregel die gemaakt zou kunnen worden. Gebruik hierbij mogelijk een generieke beschrijvingsmethode (SIGMA[11]).

Belangrijke valkuilen bij het uitvoeren van data-analyse kunnen zorgen voor het uitblijven van resultaat of kunnen resulteren in detectieregels die vooral veel ruis genereert (niet uitputtende lijst).

- Focus: Als het onderzoek te breed en diep is opgezet, is de kans groot dat het zal verzanden in zoekwerk in veel data. Beschrijf het doel en verwachte resultaat goed, en blijf scherp bij het onderzoek.
- Sidetracking: Tijdens het onderzoek zullen er mogelijk andere, nieuwe, interessante dingen naar boven komen. Noteer deze voor later, maar zorg dat het onderzoek gericht blijft op het doel.
- Beperkte dataset: Kijk naar data van een aantal weken want gedrag verandert per maand, week, dag en uur van de dag. Als de analist een data set van een uur neemt, kan het zijn dat de uitkomst (toevallig) heel positief is, maar niet representatief.
- Tijdsbesteding: Zet een limiet op de hoeveelheid tijd dat een onderzoek mag kosten. Een specifieke use case kan heel mooi klinken maar als het onderzoek een maand kost dan is je return-on-investment beperkt. Misschien kan een vergelijkbare use case (of cases) ongeveer hetzelfde doen maar zijn ze veel sneller op te leveren.
- Ruis in data: Het kan best zijn dat in een stroom van logevents een event aanwezig is dat onderdeel uitmaakt van een aanval, maar als de hoeveelheid ruis te groot is en een specifiek onderscheidend kenmerk ontbreekt, is het heel lastig om goede detectie te maken. Het is bijvoorbeeld heel lastig om foutieve loginpogingen te gebruiken als indicator omdat elke gebruiker regelmatig foutieve logins produceert.
- Hanlon's razor[12]: Een use case die beschrijft dat een goede login poging na vijf foutieve logins gedetecteerd dient te worden, klinkt leuk, maar in praktijk is dit veelal regulier gebruikersgedrag (zeker op maandag ochtend of na een vakantieperiode). En inderdaad, bij een echte aanval kan dit scenario ook vóórkomen, maar veelal zal het SOC naar uitkomsten van regulier gedrag zitten te kijken en is het verschil tussen normaal en abnormaal heel lastig vast te stellen.

In het begin van de paragraaf is haalbaarheid genoemd; haalbaarheid is niet altijd vanzelfsprekend. Haalbaarheid heeft o.a. te maken met aanwezigheid van data, maar ook met de mogelijkheden van het detectiesysteem. Het detecteren van uitschieters op een statistische normaal-distributie van een bepaald type logevent kan bijvoorbeeld heel mooi klinken als use case, maar als een detectiesysteem dit type statistische analyse niet ondersteunt, dan wordt het lastig om dit te realiseren. Ook performance van het detectiesysteem kan van invloed zijn op de haalbaarheid van bepaalde casussen.

Een ander heel belangrijk onderdeel om rekening mee te houden, is de hoeveelheid output een regel gaat genereren op basis van de analyse. Elke uitgewerkte detectieregel zal in de basis resulteren in een alarm dat door een monitoringteam moet worden geanalyseerd. Elk team heeft een maximumcapaciteit om alarmen op te kunnen pakken en verwerken. Als de hoeveelheid detectieregels zich opstapelt en het aantal alarmen te hoog is, dan zal uiteindelijk veel blijven liggen. Als een SOC te veel alarmen moet verwerken en een groot deel hiervan is vooral ruis, kan dit op termijn resulteren in wat 'Alert Fatigue' wordt genoemd. Het resultaat zal zijn dat onder

[11] Home · SigmaHQ/sigma Wiki · GitHub
[12] Hanlon's razor: "Never attribute to malice that which is adequately explained by stupidity"

hoge werkdruk alarmen te snel worden afgehandeld en dat door het hoge gehalte aan ruis de scherpte uit de analyse zal verdwijnen waardoor belangrijke zaken over het hoofd gaan worden gezien. Bij het evalueren van de hoeveelheid output van een mogelijke detectieregel, dient de context van bestaande detectieregels binnen de operatie altijd mee te worden genomen. De output van één regel is belangrijk, maar de output van alle detectieregels samen is nog belangrijker.

2.2.2.3 Implementatie Detectieregels

Als de data-analyse-fase is afgerond, zouden in principe alle randvoorwaarden aanwezig moeten zijn om (een) detectieregel(s) te bouwen. Voordat een detectieregel wordt gebouwd, is het verstandig om deze eerst functioneel te definiëren. Dit zorgt ervoor dat het SOC een bibliotheek van detecties opbouwt en dat content op een later moment opnieuw kan worden geïnterpreteerd als bijvoorbeeld migratie naar een ander detectiesysteem nodig is. Mogelijk helpt het om content op voorhand vast te leggen in een generieke, meer abstracte taal waardoor implementatie in verschillende technologieën eenvoudiger wordt. Hiervoor zijn bestaande oplossingen beschikbaar die in een brede community worden gedragen, zoals SIGMA.

Het implementeren zelf zal in de meeste gevallen minder tijd in beslag nemen als het voorwerk goed is gedaan. Als de regel(s) eenmaal zijn gebouwd, is het daarna belangrijk om de content een tijd proef te draaien (tuning-fase) tegen echte data (dit laatste is belangrijk, zeker in een omgeving waar wel een test omgeving wordt gebruikt om te bouwen, maar waar deze testomgeving niet is voorzien van alle productiedata). In een langere periode van proefdraaien komen vaak nog specifieke zaken naar boven die op basis van data-analyse op basis van een kleinere dataset niet altijd aan het licht komen.

Ook bij het bedenken en bouwen van detectie zijn er verschillende valkuilen (niet uitputtende lijst):

- False Positive Ratio: Kijk goed naar de verhouding true vs. false positives. Als uit de analyse komt dat een detectie in principe prima werkt maar de uitkomst in verhouding veel false positives genereert dan is de detectie minder bruikbaar.
- Onderhoudbaarheid: Content dient eenvoudig onderhoudbaar te zijn door analisten van verschillende ervaringsniveaus. Als content te complex wordt, bestaat op termijn zelfs het risico dat bij verloop van analisten bepaalde content niet meer te beheren is.

2.3 Monitoren & Bijstellen

2.3.1 Rapportage

Rapportage met betrekking tot risicogestuurde detectie is te verdelen in twee onderdelen namelijk dekkingsgraad en kwaliteit. De dekkingsgraad heeft betrekking op welk onderdeel van vastgestelde risico's worden afgedekt door detectie en opvolging. Kwaliteit gaat over de toegevoegde waarde van de detectieregels en security-analisten.

Het meten van de dekkingsgraad is van belang omdat tijdens de scenario-analyse fase een gedetailleerde uiteenzetting is gemaakt om de belangrijkste aanvalspaden met betrekking tot de organisatie vast te leggen. Op basis van deze vastlegging en bijbehorende statusrapportage kan de SOC-manager een continue statusvoortgang bijhouden over de vordering van de implementatie. Met deze informatie is het altijd duidelijk wat de vordering is en wat de belangrijkste nog bestaande risicogebieden zijn. Daarnaast kan ook de benuttingsgraad van de gekoppelde data worden bijgehouden.

Als tweede is het van belang om de kwaliteit van de detectieregels te meten om te weten of de inzet van security-analisten op een efficiënte wijze gebeurt. Als een groot deel van de detectieregels alleen maar false positives oplevert dan is de toegevoegde waarde beperkt – t tijd en energie van security analisten wordt verspild aan het onderzoeken en najagen van alarmen die onterecht zijn.

Op basis van het meten van de alarm-volumes per detectieregel, bijbehorende true/false-positive ratio's en de hoeveelheid alarmen die ook echt resulteren in opvolging en incidenten, kan goed worden bepaald wat de effectiviteit van de detectieregels is. Deze informatie kan weer verder

worden gebruikt voor operationele sturing. Zo kan bijvoorbeeld bestaande content verder worden afgesteld om scherpere uitkomst te geven, of kan content die niet (meer) goed werkt, worden afgevoerd.

2.3.2 Verbeterplan

Om het ontwikkelproces verder vorm te geven, is het essentieel om metingen en bijbehorende rapportages om te zetten naar verbeteringen. Dit om de detectie continu mee te laten groeien met wijzigingen in het IT-landschap, IT-trends (e.g. cloud-managed werkplekken) en dreigingen. IT staat niet stil en kwaadwillende factoren buiten de organisatie staan zeker niet stil waarmee continue verandering/verbetering onvermijdelijk is. Gebruik de rapportages om te kijken welke bestaande detectiecomponenten onvoldoende toegevoegde waarde bieden of te veel false positives hebben als basis voor het verbeteren van bestaande detectie. Daarnaast kan dekkingsgraad rapportage worden gebruikt om te bepalen welke belangrijke gaten in de detectie als eerste moeten worden aangepakt.

Een andere belangrijke bron van informatie voor verbetering is het testen van de beveiliging. Voor het testen van de verdedigings- en detectielinies wordt veelal een Red-team oefening gedaan. Het red-team is al eerder genoemd (2.2.2 Ontwikkeling, pag. 10) omdat hier vaak kennis ligt over het aanvalsoppervlak, realistische aanvalsscenario’s en nieuwe of prominente technieken. Naast het meten van detectiekwaliteit en dekkingsgraad kan het red-team worden ingezet om de detectie ook daadwerkelijk te testen. Bevindingen van het red-team kunnen direct worden gebruikt om nieuwe scenario’s te maken, maar kunnen ook resulteren in kleine verbeteringen op bestaande detectie door het toevoegen van nieuwe technieken op bestaande scenario’s. Met al deze informatie in de hand, kan een verbeterplan worden vastgesteld om zo het ontwikkelproces verder te voeden.

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://vssr.rijksapplicaties.nl/

vssr.info@minjenv.nl

December 2023