Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Detectie in cybersecurity

Wat is het, waarom is het belangrijk en waar begin ik

Inleiding

Ongeveer één op de vijf organisaties krijgt jaarlijks te maken met een cyberincident. Deze incidenten komen niet uit de lucht vallen. Door detectie ontstaat er een duidelijk beeld van (mogelijke) aanvallen en dreigingen, waardoor je gepaste maatregelen kunt treffen. Detectie is het met technische middelen zichtbaar maken van gerichte (aanvallen), onbedoelde schadelijke activiteiten en verdacht gedrag om deze vroegtijdig te identificeren en mogelijk te stoppen.

Doelgroep

Chief Information Officers, Chief Information Security Officers en bestuurders

Inhoud

Achtergrond

Cyberincidenten zijn aan de orde van de dag en hebben meestal een grote impact op de bedrijfscontinuïteit of reputatie van de getroffen organisatie. Detectie maakt het mogelijk om een aanval tijdig te herkennen en daarop te reageren. Detectie is namelijk geen doel op zich maar opvolging wel.

Cyberincidenten worden veelal veroorzaakt door kwaadwillende actoren, denk bijvoorbeeld aan opportunistische criminelen, (niet) kwaadwillende insiders of statelijke actoren die (gerichte) cyberaanvallen uitvoeren. Volgens de Lockheed Martin Cyber Kill Chain start een aanval met het in kaart brengen van de infrastructuur, componenten, data en mogelijke doelen (reconaissance). In de daaropvolgende fasen (weaponization, delivery, exploitation, installation) zal een aanvaller proberen in te breken op het netwerk. Daarbij stuurt de aanvaller bijvoorbeeld een gerichte phishingmail aan een medewerker met daaraan vast een exploit voor een kwetsbaarheid. Nadat de exploit is geslaagd, start communicatie met een zogenoemd Command & Control-systeem (C2) van de aanvaller. De aansturing via deze weg resulteert uiteindelijk in acties (“Actions”) zoals het ontvreemden van gevoelige documenten of het vastleggen van toetsaanslagen. Tijdens iedere fase is het mogelijk om bepaalde activiteiten van de kwaadwillende zichtbaar te maken door de juiste toepassing van detectiemaatregelen. Hierdoor kun je extra beveiligingsmaatregelen nemen en beperk je de potentiële schade van een aanval. Het doel is om niet enkel een goed slot en een camera bij de voordeur te hebben, maar in het gehele huis te speuren naar activiteiten van kwaadwillenden.

Wat detectie precies inhoudt en hoe je het opzet, dat lees je in dit basisboek. We gaan in op wat detectie is en hoe je het organisatorisch in kan richten in je organisatie.

Wat is detectie?

Onder detectie verstaan we alle activiteiten die erop gericht zijn om (potentiële) incidenten vroegtijdig te identificeren. In dit basisboek bedoelen we daarmee de ontdekking van malafide gebruikers/hackers/software/applicaties in een netwerk of op een systeem, waarna je actie wilt ondernemen, met als doel om tijdig te kunnen reageren op incidenten en daarmee de schade van die incidenten te verminderen.

Aanvallen kunnen op verschillende manieren geautomatiseerd gedetecteerd worden. Bekende vormen zijn:

Antivirussoftware

EDR/NDR/XDR (Endpoint/ Network/ Complex Detection and Respons)

Log analyse (SIEM/SOC)

HIDS/NIDS (network and endpoint detection, zonder response)

Antivirussoftware scant je bestanden op de aanwezigheid van kwaadaardige bestanden en rapporteert de bevindingen. EDR/NDR/XDR zijn tools die het gehele netwerk, of een specifiek deel monitoren, op zoek naar bewijs van de aanwezigheid van dreigingen om vervolgens automatisch acties uit te voeren om deze dreigingen te mitigeren.[1]

Het Amerikaanse National Institute of Standards and Technology (NIST) hanteert in het Cybersecurity Framework twee hoofdtaken bij detectie:

Continue monitoring:

assets worden continu gemonitord om afwijkingen en verdachte activiteiten te kunnen waarnemen.

Verdacht gedrag-analyse:

de afwijkende gebeurtenissen die waargenomen zijn tijdens het monitoren worden geanalyseerd om deze gebeurtenissen te karakteriseren om cybersecurity-aanvallen te detecteren.

Het is aan te raden om continue monitoring toe te passen naar aanleiding van een risicoanalyse.

[1] What Is an Endpoint? | Microsoft Security
What Is EDR? Endpoint Detection and Response | Microsoft Security

Vervolgens kan afwijkend gedrag geanalyseerd worden om zo tijdig aanvallen op te sporen. Daaropvolgend kan je als organisatie ingrijpen door de vereiste maatregelen te treffen. Denk aan het in quarantaine zetten van kwaadaardige bestanden of software, het blokkeren van een account of specifieke gebruiker.

Monitoren, detecteren & respons

Monitoren is het systematisch en periodiek verzamelen van informatie afkomstig uit logs. **Detecteren** is het analyseren van deze gebeurtenissen om ze te karakteriseren. Zodoende kunnen aanvallen gedecteerd worden om vervolgens op te kunnen reageren. Detectie is namelijk geen doel op zich maar opvolging (**respons**) wel.

Waarom detecteren?

Als detectiemaatregelen in jouw organisatie ontbreken, is de kans groot dat je cyberincidenten niet herkent. Goed ingerichte detectieoplossingen in combinatie met een responseproces kan veel schade voorkomen en de impact van een aanval beperken. Zonder opvolging is detectie niet effectief.

Preventie of Detectie?

Bij **preventie** ligt de focus van maatregelen op het buiten de deuren houden van de aanvaller. Denk aan maatregelen zoals Identity and Access Management (IAM), patchen, multifactorauthenticatie en Virtual Private Networks (VPN's).[2]
Detectiemaatregelen hebben twee andere doelen:

- Het identificeren van verdachte activiteiten van bijvoorbeeld een aanvaller.
- Ervoor zorgen dat we, wanneer de aanvaller toch langs de preventieve maatregelen is gekomen, de activiteiten van de kwaadwillende binnen het netwerk kunnen waarnemen en volgen.

Hoe werkt detectie?

In deze paragraaf worden twee veelvoorkomende vormen van detectie en wat je ervoor nodig hebt, uitgelegd. Namelijk het detecteren op kenmerken en het detecteren op anomalieën (afwijkingen).

Informatiebronnen voor detectie

Wanneer er op zowel applicatie-, systeem- als netwerkniveau informatie verzameld wordt die voor detectie gebruikt kan worden, krijg je het meeste zicht op de infrastructuur. Afhankelijk van het type dreiging en de informatie over de dreiging zijn hiervoor verschillende informatiebronnen nodig, bijvoorbeeld:

- log-informatie van een proxy-, mail- of DNS-server;
- netflow-data;
- Windows event-logging;
- log-informatie van antivirus-software of EDR op servers en werkstations;
- IAM-servers.

De hoeveelheid en kwaliteit van de beschikbare log-informatie wordt bepaald door de grootte van een organisatie, de beschikbare middelen, en de grootte en volwassenheid van het securityteam en hoeveel en welke log-informatie beschikbaar is. De informatiebehoefte verschilt per organisatie en is afhankelijk van de kwetsbaarheden, dreigingen en risico's die naar voren zijn gekomen tijdens de risicoanalyse van de te beschermen belangen (kroonjuwelen) en processen.

Detecteren op kenmerken

Vaak hebben aanvallen herkenbare elementen die je na analyse waarneemt en met deze aanval in verband kan worden gebracht. Deze kenmerken worden ook wel *Indicators of Compromise* (IoC) of *signatures* genoemd. Voorbeelden hiervan zijn:

- Een bepaald aantal e-mailadressen van afzenders van e-mailberichten met malware;
- Specifieke domeinnamen/ip-adressen waar kwaadaardige software verbinding mee maakt (C2);

[2] Woordenboek - Cyberveilig Nederland

- Kenmerken zoals hashes, pakketvolume, tijdstippen of andere herkenbare elementen van bepaalde malwarebestanden of gedragingen.

Met kenmerkgebaseerde detectie worden bekende kenmerken getoetst op de eerdergenoemde informatiebronnen om te detecteren of, en zo ja, waar en wanneer, deze kenmerken zijn waargenomen. Bronnen voor dit soort kenmerken kunnen door het securityteam zelf geïdentificeerd of worden verkregen bij CTI Cyber Threat Intel (CTI)-aanbieders of open bronnen.

Anomalie-detectie

Naast het monitoren op kenmerken kan een organisatie ook monitoren op patronen en/of gedragingen die afwijken van het normbeeld, bijvoorbeeld op:

- werkstations die midden in de nacht verdachte of kwaadaardige activiteiten buiten de vastgestelde baseline vertonen;
- gebruikersaccount die opeens vanaf een niet bij de organisatie bekende locatie inloggen;
- gebruikersaccounts die opeens gebruikt worden voor pogingen om bij afgeschermde informatie of systemen te komen;
- gebruik van tooling om *'laterale bewegingen'*[3] uit te voeren binnen het netwerk.

Voor waarneming van zulke activiteiten moet een organisatie ervoor zorgen dat de log-informatie gecontroleerd wordt op deze gedragingen. Ook moet een organisatie zelf in kaart brengen wat het normbeeld is voor activiteiten binnen de organisatie. Deze geavanceerdere methode van detectie goed opzetten en volgen kost meer inspanning.

Opvolging cruciaal

Detectieoplossingen binnen de organisatie werken alleen als er ook opvolging gegeven wordt aan de meldingen. Zorg dan ook dat dit goed geborgd is binnen de organisatie voordat detectieoplossingen geïntroduceerd worden.

[3] Het gebruik maken van technieken om eenmaal na de initial access dieper het netwerk en systemen in te komen en te bewegen naar waardevolle informatie en assets.

Detectie is namelijk geen doel op zich maar opvolging wel.

Hoe richt ik detectie in?

Om detectie in een organisatie voor de eerste keer te kunnen implementeren, is het noodzakelijk een drietal vragen te beantwoorden:

- Op welke punten in het netwerk en op endpoints willen we zicht krijgen?
- Welke detectiemethode ga ik gebruiken?
- Hoe/waar/met wie ga ik de detectieinformatie verwerken?

Stap 1: Risicoanalyse en assetinventarisatie

Identificeer de belangrijke of kwetsbare (public-facing) punten in het netwerk waar veel informatie van andere systemen naar toe en/of doorheen gaan. Bijvoorbeeld de AD-servers, firewalls, proxy-servers en DNS-servers maar ook de endpoints. Endpoints zijn apparaten die verbinding maken met een netwerk. Voorbeelden hiervan zijn servers, mobiele apparaten, desktops en slimme apparaten. Deze netwerkpunten vormen een goed begin voor een overzicht van je ICT-netwerk en vormen de juiste bronnen om log-informatie uit te halen.

Bepaal daarnaast welke netwerkonderdelen vitaal zijn voor de kernprocessen van je organisatie en neem dat mee in de prioriteitsweging. Dit doe je door de belangrijkste knooppunten of assets in het netwerk in kaart te brengen op basis van de mogelijke impact op de continuïteit van de belangrijkste bedrijfsprocessen.

Zelf doen of uitbesteden?

De risicoanalyse maakt inzichtelijk waar je kunt beginnen met detectie. Bijvoorbeeld belangrijke componenten zoals een firewall, de webserver of de endpoints van de organisatie. Begin bij deze componenten met monitoren van het netwerkverkeer en bijvoorbeeld het detecteren op

signaturen of afwijkingen. Vervolgens kun je de observaties melden bij de ICT-beheerorganisatie. Langzaam maar zeker kun je de detectiecapaciteiten gaan uitbouwen over verschillende systemen en processen. Neem de tijd om de gekozen maatregelen goed te begrijpen voordat je meer maatregelen toevoegt.

Detectie zelf inrichten

Je kunt ervoor kiezen om zelf te beginnen met detectie. Dit is arbeidsintensief en vraagt om de aanschaf van middelen. Het voordeel is dat je hierbij wel de volledige regie hebt over de inrichting en uitvoering van de detectie. Begin hier dus ook alleen mee als je van plan bent echt een eigen detectie-centrum op te bouwen zoals een Security Operations Centre. Hiervoor kun je ook de factsheet 'SOC inrichten: begin klein' van het NCSC raadplegen.

Denk goed na of je de hiervoor genoemde werkzaamheden binnen of buiten de eigen organisatie wil beleggen, daar waar het specialistisch werk betreft.

Hybride model

Bij het zelf inrichten van detectie kan ook overwogen worden marktpartijen om advies en hulp te vragen. Op deze manier kan hun kennis geraadpleegd worden bij het aanschaffen van detectieoplossingen. Daarnaast is het mogelijk om een deel van de monitoring en responsewerkzaamheden uit te besteden en een deel bij de organisatie zelf te beleggen.

Detectie uitbesteden

Het inrichten, implementeren en onderhouden van een eigen detectiearchitectuur kan veel capaciteit en middelen kosten. Daarom is het uitbesteden van detectie een veel gekozen optie. Hierbij heb je niet de volledige regie over de detectie en opvolging. Wees goed voorbereid als je overweegt om deze diensten extern in te kopen. Stel je belangrijkste bedrijfsprocessen vast en bepaal de risicobereidheid. Op basis van de asset-inventarisatie en de risicoanalyse stel je vast op welke systeemonderdelen detectie het risico op incidenten kan verkleinen en dus van meerwaarde kan zijn. Ten slotte vergt de opvolging na implementatie altijd nog inspanning van de organisatie en de leverancier. Een goed proces om dit mogelijk te maken is essentieel, inclusief de juiste communicatieafspraken met de gekozen leverancier.

Stap 2: Methode selectie

Maak vervolgens een keuze voor een detectiemethode. Bijvoorbeeld de hierboven genoemde signatuur-gebaseerde of anomalie-gebaseerde methode.

Voor detectie is dreigingsinformatie waardevol. Dreigingsinformatie bestaat vaak uit signaturen (IoC's) en tactieken, technieken en processen die een aanvaller gebruikt: (TTP's) die gebruikt kunnen worden om aanvallen te herkennen.[4] Het verschilt per organisatie welke informatie relevant voor je is. Er zijn verschillende methodes waarop informatie verzameld kan worden:

- open bronnen raadplegen;
- het eigen incidentresponsproces gebruiken;
- dreigingsinformatie uitwisselen met andere organisaties;
- commerciële dreigingsinformatie inkopen.

Als organisatie moet je investeren om te zorgen dat de kwaliteit van dreigingsinformatie goed is. Ook het securityteam moet voldoende kennis hebben om relevante vragen te stellen en tooling in te zetten voor oplossingen. Leveranciers van detectiemaatregelen maken zelf ook gebruik van dreigingsinformatie om hun detectieoplossingen up-to-date te houden.

Stap 3: Verwerking

Bedenk vervolgens waar je de log-informatie gaat verwerken en bewaren. Verwerken kan bijvoorbeeld met SIEM-software. Houd rekening met beschikbare opslagruimte, hoe lang de informatie opgeslagen wordt en de Algemene verordening gegevensbescherming (AVG).

[4] Woordenboek - Cyberveilig Nederland

Stap 4: opvolging

Op basis van de voorgaande stappen maak je een weloverwogen keuze voor het implementeren van een detectieoplossing. Het is cruciaal dat er naast detectieoplossingen opvolging gegeven wordt aan incidenten met responsprocessen. Detectie voorkomt geen incidenten. Neem ook altijd voldoende preventieve maatregelen.

NIS2

De NIS2-richtlijn in Nederland, bekend als de cyberbeveiligingswet, richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van de richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties. De NIS2 is de opvolger van de eerste NIS-richtlijn, ook wel bekend als de NIB, die in Nederland in 2016 is opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

Binnen de NIS2-richtlijn bestaat er een zorgplicht waar NIS2-bedrijven aan moeten voldoen. Het hebben van detectieoplossingen draagt bij aan het realiseren van deze zorgplichtmaatregelen binnen je organisatie, in bijzonder richtlijnen 4 en 6. [5]

Detectie als cyclisch proces

Er is geen magische oplossing voor detectie. Elke organisatie is anders en heeft andere overwegingen bij het starten van detectie. De te treffen detectiemaatregelen verschillen dan ook per organisatie. Goede detectie is een cyclisch proces.[6] Dat bestaat uit de volgende stappen:

1. *Draagvlak*

Het is essentieel dat de organisatie vaststelt waarom detectiemaatregelen geïntroduceerd moeten worden. Welk doel dienen de maatregelen en hoe is het doel tot stand gekomen? Bijvoorbeeld door beleid of wet- en regelgeving. Het is essentieel dit inzichtelijk te hebben voor de borging van bestuurlijk draagvlak, de genomen keuzes en het budget.

2. *Asset management*

Het inventariseren van de assets binnen de organisatie is noodzakelijk voor een goed overzicht welke assets er binnen de organisatie-infrastructuur draaien. Als er geen goed beeld is van de assets binnen de organisatie dan zie je gemakkelijk cruciale componenten en mogelijke kwetsbaarheden over het hoofd. Begin met het in kaart brengen van deze te beschermen belangen en de onderliggende afhankelijkheden. Vervolgens kun je deze belangen prioriteren.

3. *Risicoanalyse*

Voer een risicoanalyse uit voordat detectiemaatregelen worden ingericht. Door een risicoanalyse uit te voeren ontstaat een goed beeld welke belangen de organisatie heeft en welke processen, infrastructuur, systemen en informatie die belangen ondersteunen.

4. *Dreigingsanalyse*

Op basis van de in kaart gebrachte belangen kijk je naar de dreigingen die relevant zijn voor deze ondersteunende processen en de daar bijhorende infrastructuur, systemen en informatie. Hiervoor kun je per proces een dreigingsanalyse uitvoeren .

Begin simpel

Vaak neem je als organisatie al IT-diensten af, kijk of het mogelijk is om bij deze IT-leverancier ook detectie af te nemen. Voorbeelden hiervan zijn onder andere het aanzetten van een firewall of een antivirusprogramma. Vergeet daarbij niet om ook logging aan te zetten. Om de genoemde activiteiten uit te voeren kan de interne ICT-beheerder hier een specifieke cursus voor volgen.

[5] Richtlijn - 2022/2555 - EN - EUR-Lex (europa.eu)

[6] Projecten - Informatiebeveiligingsdienst module 2

Investeer in de mens

Detectie is niet alleen technisch. Medewerkers spelen een cruciale rol in het detectieproces. Zo kan een medewerker afwijkend gedrag of verdachte mailtjes opmerken. Daarnaast moeten zij ook de juiste conclusies verbinden aan wat zij detecteren. Inversteer dan ook in hun kunde om dit goed te kunnen doen, bijvoorbeeld met een awarenesstraining.

Het op peil houden van de kennis en kunde van het informatiebeveiligingsmedewerkers door middel van goede trainingen en certificeringen is al net zo belangrijk.

Tips bij uitbesteden

Verder zijn er een paar belangrijke zaken waar je op moet letten als je detectie uitbesteedt:

Opvolging van meldingen

- Bepaal welke activiteiten, op basis van intern beleid, bij een leverancier belegd mogen worden;
- Zorg dat je een partij kiest die 24/7 monitort op je systemen zodat je tijdig kunt reageren. Hierbij is het van belang dat iemand de meldingen kan opvolgen.

Logging

- Ga goed na welke logging, dus op welke systemen, voor je organisatie belangrijk is en welk bewaartermijn hierbij passend en vereist is, dit is in sommige gevallen ook wettelijk bepaald.

Leverancier

- Kijk welke mate van afhankelijkheid je wilt hebben van de leverancier wat betreft organisatiecontext. Vaak loopt het mis doordat een SOC-partij de gemonitorde organisatiecontext mist of de organisatie niet snapt;
- Maatwerk en flexibiliteit zijn erg belangrijk. Geen organisatie is hetzelfde dus kies een partij die bij jouw organisatie passende diensten kan aanbieden;
- Maak afspraken over informatieopslag, -deling en -verwerking. Dit in het licht van de AVG en andere wet- en, regelgeving of overeenkomsten.
- Bepaal welke risico's gepaard gaan met het uitbesteden van detectieactiviteiten;
- Zorg voor een goede relatie met de leverancier (is er een klik?);
- Besteed aandacht aan referenties en reputatie van een leverancier;
- Kijk of een leverancier aan informatiebeveiligingsnormen voldoet en daarvoor gecertificeerd is;
- Zorg ervoor dat binnen de eigen organisatie kennis over detectie en monitoring behouden blijft. Zo kan je altijd inhoudelijk in gesprek met de leverancier en identificeer je eventuele blinde vlekken binnen de organisatie;

Voor het effectief betrekken van een leverancier is goed inzicht in de inrichting, ambitie en verantwoordelijkheden van de eigen organisatie van groot belang.

Conclusie

Er zijn veel verschillende detectiemogelijkheden. Het is belangrijk om goed na te gaan welke soorten monitoring, detectie en opvolging voor de organisatie het meest van belang zijn. Op basis hiervan neem je een weloverwogen keuze in het kiezen van een detectieoplossing(en) en de opvolging hierop. Effectieve opvolging is hierbij belangrijker dan alomvattende monitoring en detectie.

Leestips

Als je meer wilt weten over detectie dan staan hier een aantal leestips:

1. Handreiking voor implementatie van detectie-oplossingen | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)
2. SOC-CSIRT-competenties | Onderzoek | Nationaal Cyber Security Centrum (ncsc.nl)
3. E-mail | Digital Trust Center (Min. van EZK)
4. In dit document hebben we het detecteren van aanvallen besproken. Het is echter ook van belang om na het detecteren van een incident goed te kunnen reageren. Dit doe je met een incident response plan.

Gerelateerde publicaties

In deze publicaties verwijzen we naar de volgende publicaties:

Publicatie	URL
SOC inrichten	https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren/soc-inrichten
Hoe breng ik mijn te beschermen belangen in kaart?	https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-breng-ik-mijn-te-beschermen-belangen-in-kaart
Hoe breng ik mijn dreigingen in kaart?	https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-breng-ik-mijn-dreigingen-in-kaart
Hoe breng ik mijn rechtstreekse leveranciers in kaart?	https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-breng-ik-mijn-rechtstreekse-leveranciers-in-kaart
Hoe bepaal ik de meest relevante risico's voor mijn organisatie?	https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-bepaal-ik-de-meest-relevante-risicos

Bekijk ook de digitale versie van deze publicatie op www.ncsc.nl:
https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren/detectie-in-cybersecurity

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Oktober 2024