# Handreiking voor implementatie van detectie-oplossingen

Praktische informatie voor een succesvolle implementatie

# Inhoud

# 1 Inleiding

Tegenwoordig is een werksituatie nauwelijks meer voor te stellen zonder computers en internet. Veel bedrijfsprocessen zijn geautomatiseerd, er is veel uitwisseling van informatie waarbij er vele koppelingen met de buitenwereld bestaan. Omdat dit risico's met zich meebrengt zijn bij veel organisaties reeds preventieve informatiebeveiligingsmaatregelen geïmplementeerd. Firewalls, antivirus oplossingen en versleutelde harde schijven en USB-sticks zijn hier voorbeelden van. Maar hoe detecteer en bewijs een organisatie dat deze maatregelen werken? Hoe kan men incidenten detecteren die ondanks getroffen maatregelen zich toch voordoen en hoe bewijst een organisatie dat zij compliant is aan bepaalde normen en standaarden?

## 1.1 Wat is detectie?

Detectie is het ontdekken of opmerken van een incident in de monitoringfase. In deze handreiking wordt daarmee bedoeld de ontdekking van een malafide gebruiker/hackers/applicatie in een netwerk of op een systeem waarna actie ondernomen kan worden. In deze handreiking worden de volgende oplossingen hiervoor verder besproken en uitgediept:

- **Intrusion Detection System** (IDS), een type systeem dat in staat is om malafide acties op een netwerk of systeem te detecteren en hierover te alerteren.
- **Intrusion Prevention System** (IPS), een type systeem dat niet alleen malafide acties kan detecteren, maar ook blokkeren.
- **Security Information and Event Management** (SIEM), oplossingen waarbij één systeem logging-informatie vanuit allerlei componenten in het netwerk verzamelt om deze informatie vervolgens te normaliseren, te correleren en te aggregeren teneinde alerts en andere rapportages beschikbaar te kunnen maken.

## 1.2 Waarom dit document?

Het Nationaal Cyber Security Centrum (NCSC) van de Nationaal Coördinator voor Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) bieden met dit document handvatten voor Information Security Officers en technisch specialisten, opererend op de tactische en operationele laag binnen een organisatie. Dit document biedt basisinformatie over nut en noodzaak van detectie, tools en technieken, en best practices om detectie-oplossingen op werking te testen.

## 1.3 Preventie

Hoewel dit document ingaat op het monitoren van verkeer en processen om incidenten te detecteren, is het belangrijk te beseffen dat deze activiteiten geen alles oplossend antwoord geven op alle beveiligingsproblemen. Het is en blijft van belang om het grotere geheel te zien. Dit betekent dat preventieve maatregelen zoals het versleutelen van data, het beveiligen van verbindingen en het creëren van bewustzijn over risico's bij gebruikers nog altijd net zo belangrijk zijn. Het gebruik van preventieve- en detectieve maatregelen, dekken dus een groter geheel af.

Zoals gezegd kunnen veel van de beveiligingsrisico's worden verlaagd door gebruikers goed te informeren en dus bewustzijn te creëren. Dit kan door het verplicht laten volgen van een security training of een "gamification" (spelenderwijs bewust worden) programma met bijvoorbeeld een "social engineering test" of een "mysterie visit" waarbij op onschuldige wijze de gebruikers bewust worden gemaakt van het gemak

dat indringers informatie naar boven kunnen halen. Het Verizon rapport van 2015 laat zien dat "phishing" mails in het eerste uur al door 50% van de gebruikers worden geopend[1]. Dit impliceert dat als een gebruiker zich bewust is van het bestaan van dit soort aanvallen, hij een aanval sneller zal herkennen en daar melding van zal maken om andere gebruikers ook te behoeden van deze aanval.

## 1.4 Waarom detectie naast preventie?

Als preventie en bewustwording een goede kans bieden een aanval in de beginfase te kunnen blokkeren, waarom dan toch starten met detectie? Hiervoor is een aantal redenen aan te wijzen:

- Allereerst is er een verandering in het dreigingsbeeld waar te nemen. Bedrijfsspionage en aanvallen van georganiseerde misdaad, terreurgroepen en diverse buitenlandse inlichtingendiensten vormen een serieuze dreiging. Bij dergelijke dreigingen, die ook wel bekend staan als Advanced Persistent Threats (APT's), beschikken de actoren over voldoende geld, middelen en tijd om een aanval met geavanceerde middelen uit te voeren en kunnen zij deze gedurende een langere periode volhouden.

- De keuzes met betrekking tot de wijze waarop technologische wijzigingen worden geadopteerd, vragen aanpassingen aan de huidige architectuur waardoor nieuwe risico's worden geïntroduceerd. Voorbeelden van dergelijke technologische wijzigingen zijn samenwerkingsplatformen die toegang moeten bieden aan derden, plaats en tijd onafhankelijk werken, cloud-oplossingen en "Bring Your Own Device" (BYOD). Deze aanpassingen introduceren nieuwe risico's die niet afgedekt kunnen worden met slechts preventieve maatregelen. Ook de snelheid waarmee gebruikers technologische wijzigingen adopteren spelen mee. Tablets en smartphones bestaan nog niet zo heel lang, zijn algemeen geaccepteerd in het bedrijfsleven (zonder een dergelijk device "hoort men er niet meer bij"), maar de beveiliging van tablets en smartphones loopt nog wel achter. Dreigingsactoren kunnen hierdoor in sommige gevallen onopgemerkt hun gang gaan. Deze afbrokkeling van het huidige 'corporate netwerk' en het zogenaamde 'system high model' (waarbij het merendeel van de beveiligingsmaatregelen aan de rand(en) van het netwerk of het informatie systeem worden toegepast) creëert de noodzaak de vervolgstap te maken om naast preventieve maatregelen ook detectie en monitoring toe te passen binnen de informatiebeveiliging. Deze vervolgstap is tevens zichtbaar in de visie van de Nederlandse overheid zoals deze te vinden is in de Nationale Cybersecurity Strategie 2.

Door detectie- en monitoringoplossingen te implementeren naast preventieve maatregelen verkleint men de kans op langdurige aanvallen en verkleint men de impact van aanvallen op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen). Hier moet men denken aan misbruik door gebruikers van informatiesystemen (outsider en insider threats).

Detectie helpt tevens bij aanvallen die hun oorzaak niet vinden in cybergerelateerde aanvallen zoals:

- het niet (tijdig) opmerken van falende componenten en relevante kritieke meldingen van systemen waarop belangrijke assets te vinden zijn;
- onderbrekingen van dienstverlening als gevolg van gebruikersfouten of configuratiefouten.

[1] Verizon -2015 *Data Breach Investigations Report.* Beschikbaar via http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigationreport- 2015_en_xg.pdf (Opgehaald op 2015-04-28)

## 1.5 Leeswijzer

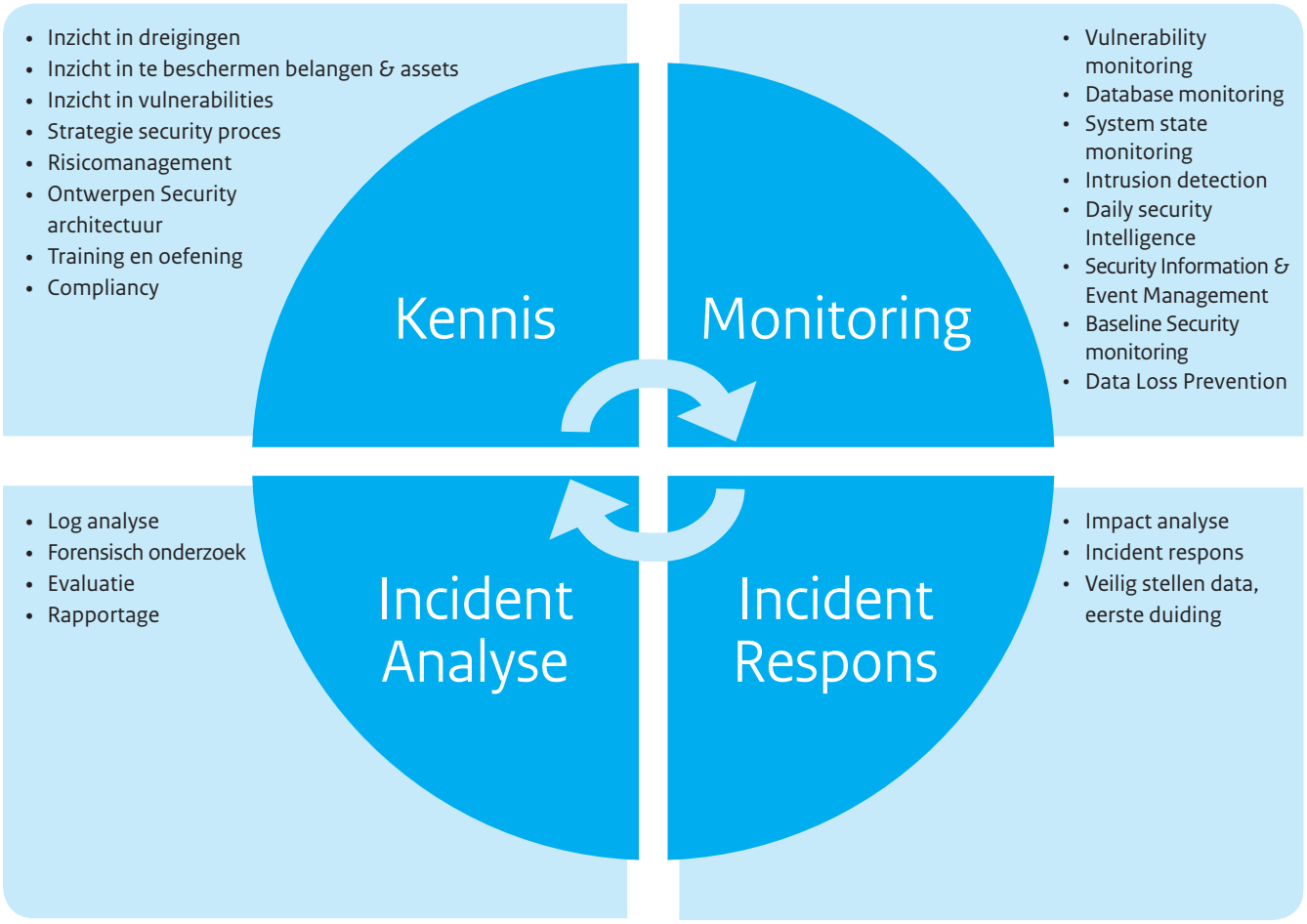
Er is in dit document onderscheid gemaakt tussen organisatorische/procesmatige informatie en technische informatie. Het document beschrijft in hoofdstuk 2 de aanleiding tot detectie en de verschillende proces-stappen. Vervolgens geeft het document in hoofdstuk 3 een technische beschrijving van verschillende detectietechnieken die beschikbaar zijn en biedt het vervolgens in hoofdstuk 4 een aantal handvatten aan de hand van best practices gericht op detectie en monitoring. Deze handvatten zijn gebaseerd op bestaande richtlijnen en normen zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), PCI-DSS 3.0, maar ook de SANS 20 Critical Security controls, de “Good Practice Guide 13”, aangevuld met toevoegingen van het NBV en het NCSC. Hiermee kan een detectie-oplossing ingericht en verbeterd worden.

# 2 Taken en processen

Detectie kan een positieve invloed hebben op de beveiliging van een infrastructuur. Het is wel zo dat detectie-oplossingen niet efficiënt en effectief uitgenut kunnen worden wanneer aanpalende processen en taken deze oplossingen niet maximaal versterken. Zo kan monitoring bijvoorbeeld slechts beperkt succesvol zijn als het de organisatie aan kennis ontbreekt over *wat* men wil monitoren, *waarvoor* men wil monitoren, of wanneer er geen proces is ingericht om opvolging te geven aan constateringen vanuit monitoring. Daarom is het van belang om, voordat men in de details van detectie duikt, eerst de context te beschouwen waarbinnen deze activiteiten moeten gaan plaatsvinden.

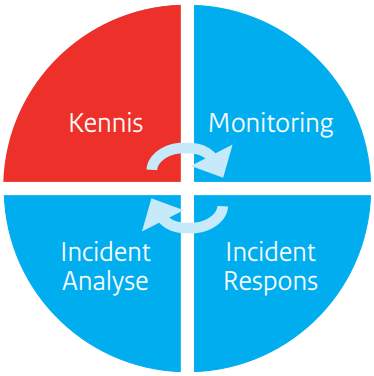
## 2.1 Processen

De mate waarin detectie bijdraagt aan het beveiligingsniveau van de organisatie, is afhankelijk van een viertal factoren: kennis, monitoring, incident respons en incident analyse. Figuur 1 toont deze vier factoren in de vorm van vier kwadranten. Indien één van deze vier factoren niet of onvoldoende is ingericht, heeft dit direct impact op de effectiviteit van detectie als maatregel. Hieronder worden deze vier factoren verder uiteen gezet.



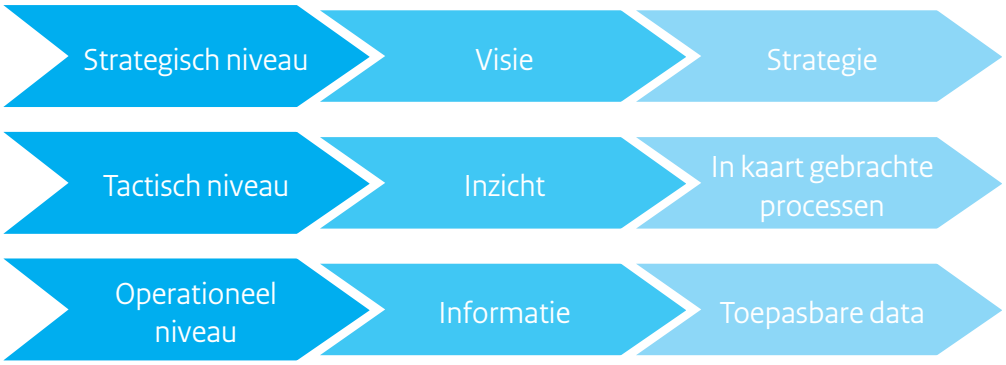

*Figuur 1. Detectie implementatierichtlijn*

## 2.2 Kennis




Detectie is geen oplossing die een organisatie op een specifiek moment aanzet en automatisch een aantal problemen oplost. Sterker nog, het levert misschien juist problemen op! Een effectieve detectie-implementatie kost veel capaciteit, inspanning en kennis, en vereist een brede commitment binnen de organisatie (en dus niet alleen de ICT-afdeling).

Afhankelijk van het doel dat de organisatie nastreeft met detectie (inzage, compliancy, etc.), ligt het zwaartepunt bijvoorbeeld op bepaalde focusgebieden. Dit bepaalt de intensiteit waarmee er detectie plaatsvindt en de mate waarin er processen rondom detectie zijn ingericht. Kennis valt onder te verdelen in drie groepen die ieder ook op een ander niveau toepasbaar zijn:




*Figuur 2. Waar bestaat kennis uit?*

Het is essentieel eerst te duiden ten opzichte van welke systemen en informatie detectie wordt ingezet (bepalen van de te beschermen belangen, stap 1). Ook is het van belang te bepalen ten behoeve van welke dreigingen en dreigingsscenario's detectie zal worden ingezet (stap 2).
Indien je deze zaken niet vooraf bepaalt, loopt de organisatie de kans veel informatie te verzamelen zonder dat hier direct inzicht en prioriteit aan gegeven kan worden (zie de Best practices in hoofdstuk 4).

Het kenniskwadrant in dit model heeft betrekking op deze problematiek.

*Stap 1. Voorbereiding "Wat proberen we nu eigenlijk te detecteren?"*
Om te bepalen in welke mate detectie bijdraagt aan het beveiligingsniveau moet eerst duidelijk zijn ten opzichte van welk systeem of (nog beter) welke informatie of te beschermen belangen dit dan is. Voer een risico- en impactanalyse uit om de assets te identificeren en te classificeren.

Detectie kan meerdere doelen dienen en betrekking hebben op meerdere te beschermen belangen, sterker nog, dit is over het algemeen het geval; echter, als men de vraag stelt in welke mate het bijdraagt aan het beveiligingsniveau dan is ten opzichte van *wat* essentieel.

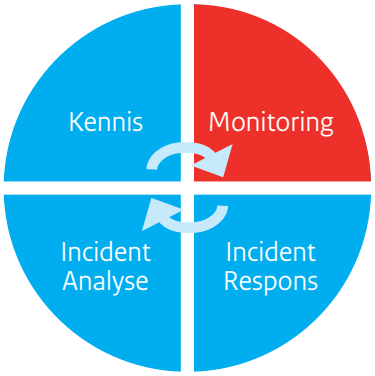
*Stap 2. Analyse en ontwerp "Wie of wat proberen we te detecteren?"*
Detectie kan meerdere doelen dienen waaronder compliance en threat management. Is het van belang dat, in geval van een incident, slechts aangetoond hoeft te worden dat de organisatie op dat moment compliant was, dan vereist dit een minder intensieve implementatie dan wanneer een organisatie zich tegen APT's wil beschermen. De ene implementatie vraagt dan ook om andere informatie als input voor detectie dan een andere.

Voordat detectie als maatregel effectief ingezet kan worden is het noodzakelijk eerst te bepalen ten opzichte van welke dreiging detectie wordt ingezet.

Waar het gaat om het prioriteren van risico/dreigingsscenario's is het van belang om hier zicht op te hebben. Dit kan onder andere op basis van informatie uit de eigen organisatie (aantal incidenten in het afgelopen jaar binnen een bepaald scenario) en informatie van derden zoals de AIVD en het NCSC.

*Stap 3. Implementatie "Hoe Detectie gericht als maatregel in te zetten?"*
Nu duidelijk is "wat" er beveiligd moet worden tegen "wie of wat", dan kan de detectie gericht als maatregel worden geïmplementeerd. Er moet immers voorkomen worden dat een hele grote hoeveelheid logs naar een "Security Information and Event Management" (zie 3.2 voor uitleg over SIEM) systeem geforward worden en dat niets met deze informatie gedaan kan worden omdat men niet weet waar te beginnen.

## 2.3 Monitoring




Een organisatie kan monitoring voor diverse doeleinden inzetten. De belangrijkste reden voor het inzetten van monitoring is zeer waarschijnlijk het beter kunnen detecteren en eventueel blokkeren van digitale aanvallen op de infrastructuur. Intrusion detectie en preventie is bijvoorbeeld een belangrijk onderdeel van de door Lockheed Martin opgestelde "cyber kill chain"[2]. De cyber kill chain beschrijft de verschillende fasen van een gerichte digitale aanval waarbij in elke fase de aanval op verschillende manieren kan worden gedetecteerd (en zo geblokkeerd kan worden in de fase "Incident Respons"). Figuur 3 beschrijft de verschillende fasen uit dit model van "reconaissance" tot aan "actions".


*Figuur 3. De cyber kill chain (bron: Lockheed Martin)*

Volgens het model van Figuur 3 start een gerichte 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 verstuurt de aanvaller bijvoorbeeld een gerichte phishingmail aan een medewerker met daaraan vast een exploit voor een kwetsbaarheid, of valt de aanvaller via een strategic web compromise, zoals een wateringhole aanval, de browser van een eindgebruiker aan. Nadat de exploit is geslaagd, en één of meerdere systemen succesvol zijn overgenomen door de kwaadwillende, start communicatie met een zogenoemd "Command & Control"-systeem (C2) van de aanvaller waarmee deze aanvaller allerlei commando's aan het geïnfecteerde systeem kan doorgeven. Deze commando's resulteren uiteindelijk in acties ("Actions") zoals het ontvreemden van gevoelige documenten of het vastleggen van toetsaanslagen.

Figuur 3 toont, naast de verschillende fasen van het model, ook dat detectie van een aanval in verschillende fasen mogelijk is. Zo zijn netwerk-gebaseerde Intrusiondetectiesystemen (NIDS) in staat om binnen de fasen "weaponization" en "C2" malafide acties te detecteren en kunnen host-gebaseerde Intrusiondetectiesystemen (HIDS) dit doen binnen de fasen "exploitation" en "installation".

Een organisatie kan aan de hand van het model van Lockheed Martin kiezen voor monitoring om uiteindelijk een digitale aanval zo vroeg als mogelijk (aan de linkerkant van het model) te detecteren en onschadelijk te maken. In meer pro-actieve zin kan detectie helpen om eventuele kwetsbaarheden in de infrastructuur in een vroeg stadium op te sporen door het uitvoeren van kwetsbaarhedenscans en penetratietesten.

[2] http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

Het type monitoring waar dit document echter de nadruk op legt, is (reactieve) monitoring op aanvallen waarmee de infrastructuur op een specifiek moment te maken heeft. Bij deze wijze van monitoring controleert een systeem netwerkverkeer en systeemactiviteiten om op die manier (potentieel) malafide activiteiten te kunnen detecteren. Het herkennen van deze malafide activiteiten kan hierbij zowel gebeuren op basis van bekend ongewenst gedrag (signatures) als op basis van afwijkingen op gebruikelijke patronen (anomaliedetectie). Het correleren van de verschillende soorten informatie voortkomend uit de analyse op deze patronen, maakt het mogelijk om nieuwe aanvallen waar te nemen en/of een inschatting te maken van de aannemelijkheid van een aanval.

Naast het inzetten van detectie-oplossingen voor het herkennen en blokkeren van aanvallen, kunnen er ook nog andere redenen bestaan om te kiezen voor een dergelijke oplossing. In het vervolg van deze paragraaf zullen we deze redenen kort aan bod laten komen.

### 2.3.1 Inzicht in het netwerk

De inzet van netwerkdetectie kan leiden tot een beter inzicht in hoe een netwerk functioneert en welke toepassingen hierop actief zijn. Aangezien een Intrusion Detection System (IDS) en een Intrusion Prevention System (IPS) zeer veel overeenkomsten hebben, gebruiken we in dit document de term *Intrusion Detection & Prevention System* (IDPS) om naar dit soort systemen te verwijzen. Op het moment dat een organisatie start met een IDPS, levert dit mogelijk veel alerts op die hun oorsprong vinden in bijzonder – maar bonafide – gedrag van applicaties en systemen. Dit is voornamelijk een probleem met netwerkmonitoring en een oorzaak kan gevonden worden in kwaliteit van signatures, kwaliteit van rules, en ongetrainde anomaliedetectie.

Een IDPS kan daarnaast bijvoorbeeld inzicht verschaffen in de applicaties die op het netwerk in gebruik zijn en alerteren wanneer een nieuwe applicatie (bonafide danwel malafide) zijn intrede doet op het netwerk.

### 2.3.2 Altijd patchen, maar wat als dat niet mogelijk is?

Om succesvol misbruik van kwetsbaarheden te voorkomen is het van groot belang om patches en updates van leveranciers zo snel als mogelijk te installeren, mits eerst getest in een testomgeving alvorens de uitrol in productie. Diverse omstandigheden kunnen er echter toe leiden dat het installeren van een dergelijke patch niet mogelijk is:

- Er is simpelweg (nog) geen patch voorhanden. Dit is bijvoorbeeld het geval bij zogenoemde zero-days waarbij details over een kwetsbaarheid verschijnen voordat de leverancier een patch heeft kunnen ontwikkelen.

- Het is niet mogelijk om de patch direct te installeren omdat het de stabiliteit van een kritiek systeem in gevaar kan brengen of omdat het uitrollen van patches alleen mag plaatsvinden binnen een afgesproken onderhoudswindow.

- Er zal geen patch voor de kwetsbaarheid beschikbaar komen omdat de leverancier de betreffende software niet langer meer ondersteunt.

- Andere software op de machine verhindert de installatie (incompabiliteit of unsupported combinatie). De keuze is dan een gepatched systeem wat unsupported is, of een niet gepatched systeem wat supported is.

Om in dit soort gevallen toch bescherming te bieden tegen aanvallen, kan een IDPS misbruik van deze kwetsbaarheden herkennen en blokkeren. Men spreekt in dit kader ook wel over virtueel patchen waarbij niet de daadwerkelijke patch wordt geïnstalleerd maar wel bescherming tegen de kwetsbaarheid wordt geboden. Hoewel heel waardevol neemt dit niet de noodzaak weg om de patch alsnog uit te rollen. De virtuele patch beschermt immers wel tegen een set aan aanvallen op de kwetsbaarheid, maar omdat de kwetsbaarheid zelf niet wordt weg genomen, bestaat altijd de kans dat het IDPS een bepaalde aanvalsvariant toch niet herkent of blokkeert. Als alternatief op virtueel patchen (of als dit niet kan in een situatie) is het tijdelijk blokkeren of uitzetten van functionaliteit een mogelijkheid (afhankelijk van de impact en het te lopen risico). Bijvoorbeeld tijdelijk bepaalde attachment types blokkeren bij een mail-kwetsbaarheid, totdat de patch of virtuele patch beschikbaar is.

### 2.3.3 Onbekende dreigingen tegengaan

Veel beveiligingsoplossingen zijn in staat om bekende dreigingen te detecteren en te blokkeren op basis van statische indicatoren ook wel signatures. Zo kan een virusscanner op basis van hashes van bekende virussen malafide bestanden herkennen en kan een firewall toegang tot bekende malafide IP-adressen blokkeren. Maar naast de bekende bedreigingen bestaan er nog veel meer onbekende dreigingen waarvan indicatoren zoals hashes en IP-adressen niet beschikbaar zijn. Om dit soort dreigingen tegen te kunnen gaan is een oplossing vereist die op basis van gedrag of anomalieën malafide activiteiten binnen het netwerk of op de host kan herkennen. Een IDPS is in veel gevallen in staat om hieraan een invulling te geven.

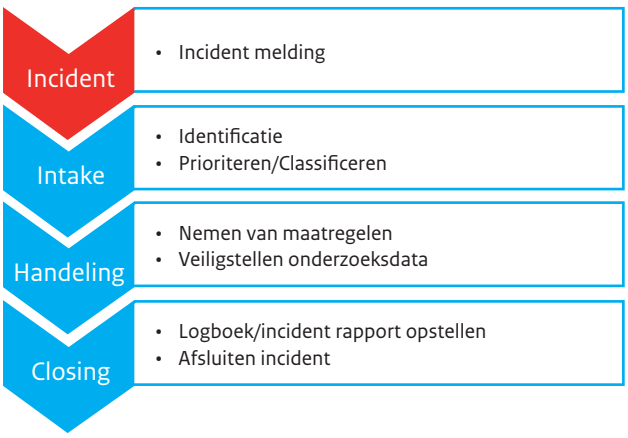
### 2.3.4 BYOD

Bring Your Own Device (BYOD) is het beleid om medewerkers, zakelijke partners en andere gebruikers toe te staan om persoonlijk geselecteerde en gekochte (computer)apparatuur - zoals smartphones, tablets en laptops - op de werkplek te gebruiken en met het bedrijfsnetwerk te verbinden[3]. Het toestaan van BYOD betekent dus dat deze devices, die niet in beheer zijn bij de ICT-afdeling van de organisatie, verbinden met het interne netwerk en toegang krijgen tot delen van de infrastructuur van de organisatie. Het gaat daarbij vrijwel altijd om een draadloos netwerk van de organisatie.

Beleid zal veelal voorschrijven dat de beheerorganisatie geen toegang heeft tot BYOD vanwege privacy issues. Daarnaast is er ook nog een ander probleem omdat er niet altijd voor elk platform de juiste software en kennis bij de beheerders aanwezig zal zijn.
Hierdoor is het onder andere niet mogelijk om op deze devices software zoals anti-virusscanners uit te rollen voor het afweren van digitale aanvallen. Een beveiligingsprobleem met een aangesloten device kan echter ook tot problemen leiden voor de organisatie, bijvoorbeeld als een geïnfecteerd device zelf aanvallen uitvoert op systemen van andere organisaties. Door inzet van een IDPS kan een organisatie grip krijgen op BYOD, bijvoorbeeld door het inzetten van een IDPS op het draadloze netwerk (een wireless IDPS) waarop devices aansluiten. Maar echte end-point detectie kan enkel op de hosts zelf. Dus malafide versleuteld verkeer zal niet door de wireless IDPS worden gedetecteerd.

## 2.4 Incident respons

Om de impact van een aanval te beperken dient deze geanalyseerd te worden. Vervolgens kan er na het stellen van prioriteiten actie worden ondernomen. Dit laatste laat zich omschrijven als incident respons. Hierbij horen activiteiten als het isoleren van systemen, het aanscherpen van de beveiligingssystemen of het opschonen van malware.


[3] Definitie overgenomen uit het NCSC Whitepaper "Consumerization en security" (zie https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/consumerization--security.html).

### 2.4.1 Incident

Het daadwerkelijk detecteren uit zich in een incidentmelding en is het resultaat van de monitorings-activiteiten. Indien een incident zich voordoet zal er een vorm van incident respons plaats moeten vinden. Incident respons valt in een drietal stappen uiteen te zetten:

1. *Intake*

Voordat er actie ondernomen kan worden moet eerst duidelijk zijn om wat voor incident het gaat. Wat is de omvang van het incident, welke assets zijn betrokken, welke worden er bedreigd en wat is de impact ten aanzien van deze assets. De impact kan worden bepaald aan de hand van de resultaten in stap 1 onder Kennis.

Indien dit beeld duidelijk is kunnen de te nemen stappen worden geprioriteerd. Ook kan intake worden gebruikt voor het prioriteren van incidenten onderling op het moment dat er meerdere incidenten gelijktijdig plaats vinden.

2. *Handeling*

Het nemen van actie zoals het dichtzetten van een firewall of netwerkpoort, het elimineren van een geïnfecteerde machine of het aanpassen van een IDPS-ruleset zijn voorbeelden van maatregelen die bij deze stap thuis horen. De acties hebben allen het doel om de schade te beperken voortkomend uit het incident. Indien meer duiding noodzakelijk is om over te gaan tot actie wordt er eerst informatie verzameld, bijvoorbeeld door het uitvoeren van gericht forensisch onderzoek.

Er kan ook een bewuste keuze gemaakt worden om niet direct te handelen. Hierdoor kan er informatie verzameld worden over de aanval en de aanvaller. Deze informatie kan vervolgens gebruikt worden om intelligente tegenmaatregelen te treffen om een aanvaller te misleiden. Deze vorm van verdediging heet *Active Defense*.

Onderzoeksdata en informatie is input voor het Incident Analyse proces. Het is van belang dat dergelijke informatie tijdig en integer wordt verzameld en bewaard. Zeker waar het gaat om incidenten met een mogelijk strafrechtelijk vervolg is het van belang dat er aandacht is voor de *Chain of Custody*.

3. *Closing*

Er wordt een kort verslag opgemaakt waarin het intake- en handelingsproces uiteen worden gezet. Hierbij wordt ook de veiliggestelde data in perspectief gezet. Ook is dit verslag input voor het Incident Analyse proces.

### 2.4.2 Taken en verantwoordelijkheden

Zodra het gaat om taken en verantwoordelijkheden moet er onder andere stil worden gestaan bij de volgende vragen:

- Wie zoekt de oorzaak?
- Wie is de eindverantwoordelijke?
- Wie mag beslissingen nemen?
- Wie voert de regie, zowel proces technisch als op operationeel niveau?
- Wie gaat de vervolgstappen ondernemen om het voorval op te lossen?
- Zijn er wettelijke beperkingen waar een organisatie rekening mee moet houden?
- Welke externe partijen zijn er allemaal bij betrokken, wie zijn daar de aanspreekpunten en wie mogen daar beslissingen nemen?

Het is aan te raden om gebruik te maken van een informatiebeveiligingsstandaard zoals ISO 27001 om processen en richtlijnen te implementeren om deze verantwoordelijkheden en taken vast te leggen en te borgen. Ook wanneer de organisatie zelf niet de ambitie heeft om gecertificeerd te worden.

## 2.5 Incident Analyse


Incident analyse is het uitvoeren van een evaluatie naar aanleiding van het incident zodat de organisatie hier lessen uit kan trekken. Verder kan deze analyse leiden tot aanpassingen rondom beveiligingsmaatregelen.

### 2.5.1 Forensisch onderzoek

Ondanks alle maatregelen die een organisatie neemt, gebeurt het toch dat een succesvolle aanval het netwerk van deze organisatie treft. Een goed ingericht incident analyse proces is dan essentieel om de schade als gevolg van deze aanval te beperken. Een onderdeel van een dergelijk proces is het uitvoeren van forensisch onderzoek waarbij onderzoekers bijvoorbeeld bekijken hoe de aanvaller te werk is gegaan, welke systemen zijn geraakt en welke informatie mogelijk is gelekt.

Het incident analyse proces kan in een tweetal stappen worden onderverdeeld.

1. *Analyseren van het incident*

Afhankelijk van het incident zal er uitgebreid forensisch onderzoek worden uitgevoerd. Forensisch onderzoek is erg tijd rovend en vereist specifieke expertise. Tijdens het uitgebreide onderzoek, waarin de organisatie verder kijkt dan alleen naar de essentiële gegevens voor het afhandelen van het incident, bekijken de onderzoekers of er nadere aandachts- en verbeterpunten uit het onderzoek kunnen worden getrokken. Aangezien het onderzoek zich niet direct richt op het beperken van de impact of het vinden van dadersporen, hoort dit uitgebreide forensische onderzoek (in tegenstelling tot het standaard forensische onderzoek) niet bij incident respons thuis.

2. *Trekken van conclusies*

Het resultaat van de analyse manifesteert zicht als een set aan conclusies. Het doel van deze conclusies is het komen tot verbetervoorstellen en het doorvoeren van aanpassingen om processen verder te optimaliseren en de weerbaarheid van de organisatie te verhogen.

Je kunt hierbij denken aan technische zaken als bijvoorbeeld een nieuw waargenomen Indicator of Compromise die vertaald kan worden naar een set aan nieuwe signatures. Ook kan gedacht worden aan minder technische zaken als aanpassingen op gebied van communicatie of in de prioritering van potentiële incident meldingen om zo het proces te optimaliseren.

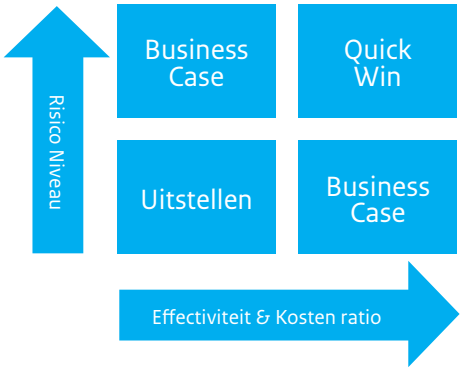
Niet alle conclusies zijn even belangrijk. De meeste aandacht zou uit moeten gaan naar identificatie van nieuwe risico's of naar de "quick wins". De laatse categorie zijn maatregelen die risico's tegen een lage inspanning, belasting en kosten kunnen verminderen. Afwegingen moeten gemaakt worden aan de hand van de resultaten van het kennisproces.

Indien het risiconiveau en de effectiviteit van eventuele maatregelen beiden laag zijn, heeft deze conclusie geen prioriteit.

Waar het gaat om zaken met een hoog risiconiveau of een hoge effectiviteit zullen er afwegingen gemaakt moeten worden. Verdere uitwerking vanuit business case perspectief is dan noodzakelijk.

Zaken met een hoog risiconiveau EN een hoge effectiviteit verdienen het om veel prioriteit te krijgen. Dit zijn de zaken waar met relatief weinig middelen aanzienlijke risico's kunnen worden afgedekt, ook wel bekend als laag hangend fruit.

Prioriteren van Conclusies en Risico Response



# 3 Hulpmiddelen

Om detectie binnen een netwerk in te richten bestaan er diverse hulpmiddelen. In het verleden waren organisaties vooral aangewezen op zogenoemde *Intrusion Detection Systems* (IDS) waarmee het mogelijk is om op systemen en het netwerk op zoek te gaan naar malafide activiteiten. De laatste jaren is een technologie die bekend staat onder de noemer *Security Information Event Management* (SIEM) steeds meer in opkomst. Deze technologie heeft als doel om informatie uit allerlei bronnen zoals firewalls, routers en IDS-en te aggregeren en te correleren om op die manier malafide patronen te ontdekken.

Het is niet zo dat een organisatie bij de keuze voor detectie ook een keuze moet maken tussen een IDS óf een SIEM. Het is zelfs aan te raden beide oplossingen naast elkaar te gebruiken zodat deze tools elkaar kunnen versterken. Zo kan de output van een IDS waardevolle input voor een SIEM vormen. Dit hoofdstuk gaat verder in op beide hulpmiddelen.

## 3.1 Intrusion detection en Intrusion prevention

Intrusion detection heeft als doel om te alerteren zodra een potentieel malafide activiteit plaatsvindt binnen het netwerk van een organisatie. Het is vervolgens aan de beheerder van een systeem om te onderzoeken wat er daadwerkelijk aan de hand is en om gepaste actie te ondernemen. Reageert een beheerder niet op een dergelijke alert, dan zal de aanval ook niet gestopt kunnen worden. Om niet afhankelijk te zijn van menselijk ingrijpen bieden systemen op het gebied van Intrusion detection daarom tegenwoordig ook de mogelijkheid tot het automatisch stoppen van een aanval, zonder tussenkomst van een beheerder. Als een IDS wordt ingezet voor het actief blokkeren van een aanval dan spreekt men over een *Intrusion Prevention System* (IPS).

### 3.1.1 Introductie

Oplossingen op het gebied van Intrusion detection en Intrusion prevention zijn er in vele soorten. Welke oplossing geschikt is voor toepassing binnen een netwerk is geheel afhankelijk van bijvoorbeeld de plaats van het systeem en het doel dat men er mee hoopt te bereiken. Deze paragraaf introduceert de onderscheidende kenmerken die helpen om de diverse oplossingen op het gebied van IDPS van elkaar te kunnen onderscheiden.

Bij het beschrijven van de kenmerken zet deze paragraaf vaak twee kenmerken van een IDPS tegenover elkaar, bijvoorbeeld detectie via signatures versus detectie op basis van anomalieën. Dit is bedoeld om duidelijk de verschillende eigenschappen van een IDPS aan te kunnen geven. Het is niet zo dat de implementatie van een IDPS altijd een exclusieve keuze voor de ene optie of de andere optie vereist. In de praktijk zal een IDPS daarom een mix van kenmerken en functionaliteiten bevatten waarbij de keuzevrijheid bestaat om bepaalde functionaliteiten juist wel of niet in te zetten. Zo ondersteunen veel IDPS-systemen zowel signatures als anomalie-detectie en is het aan de beheerder van het IDPS om te bepalen welke functionaliteit hij waarvoor inzet.

#### 3.1.1.1 *Systeemniveau versus netwerkniveau*

Detectie en preventie kunnen grofweg plaatsvinden op twee plekken binnen een infrastructuur: op het netwerk of op een systeem dat is aangesloten op het netwerk. In productliteratuur duiden leveranciers dit verschil aan met *network-based* of *host-based*.

Detectie en preventie op systeemniveau gaat terug tot de tijd van mainframes en bestaat daarmee het langst. Een IDPS op systeemniveau baseert zich op lokaal beschikbare informatie. Denk daarbij aan informatie over bestanden op het systeem, de inhoud van logbestanden of netwerkverkeer dat de netwerk-kaart op het systeem verwerkt. Op basis van deze informatie bepaalt het IDPS of er zich een beveiligings-probleem op het systeem voordoet of dreigt voor te doen. Een voorbeeld is een virusscanner die, vaak op basis van signatures van bekende bestanden, op systeemniveau bepaalt of er potentieel sprake is van een beveiligingsprobleem.

Een IDPS op netwerkniveau heeft geen kennis van de acties die op afzonderlijke systemen plaatsvinden maar ziet wel het netwerkverkeer dat deze systemen met elkaar uitwisselen. Op basis van de inhoud van dit netwerkverkeer kan een IDPS bepalen of er mogelijk sprake is van malafide communicatie. Wanneer in documenten wordt gesproken over een netwerk gebaseerd IDPS, bedoelt men over het algemeen dat het IDPS detectie of preventie uitvoert op netwerkverkeer dat zich via een kabel verspreidt. Met de opkomst van draadloze netwerken is echter ook een nieuw type IDPS ontstaan dat zich juist richt op draadloze communicatie. Dit type IDPS, een wireless-IDPS, richt zich veelal niet zozeer op de inhoud van de communicatie maar veel meer op de draadloze communicatie zelf. Zo is een wireless-IDPS bijvoorbeeld in staat om WEP-cracking, draadloze (D)DoS-aanvallen en het gebruik van zwakke versleuteling vast te stellen. In een omgeving waarin, naast draad gebonden communicatie, ook draadloze netwerkcommunicatie plaatsvindt, vormen deze twee oplossingen dan ook eerder een aanvulling op elkaar dan dat ze als concurrenten van elkaar fungeren.

Een ander bijzonder type IDPS dat met de toenemende populariteit van virtualisatie ontstaat, is de gevirtualiseerde IDPS. Dit type IDPS heeft als doel om detectie en preventie uit te voeren op de communicatie tussen virtuele systemen onderling. Een traditioneel netwerk-IDPS zal op deze verbindingen niet werken, omdat de communicatie tussen de virtuele systemen niet verloopt via de infrastructuur van het netwerk. Hierdoor zal een traditioneel netwerk-IDPS dit verkeer ook niet kunnen inzien.

#### 3.1.1.2 *Afwegingen*

Een belangrijk voordeel van detectie/preventie op netwerkniveau boven detectie/preventie op systeemniveau is de kosteneffectiviteit. Door bijvoorbeeld detectie op netwerkniveau in te richten, is het mogelijk om in één klap detectie uit te voeren voor alle systemen die op dit netwerk zijn aangesloten. Om eenzelfde resultaat te bereiken met een systeem gebaseerde oplossing, moet elk van de afzonderlijke systemen worden voorzien van een IDPS. Bij detectie op een netwerk met bijvoorbeeld 100 systemen maakt dit het verschil tussen één centrale netwerkimplementatie en 100 afzonderlijke systeemimplementaties. Daarbij komt dat een systeem-implementatie specifiek is en daarom voor elk afzonderlijk platform een platform specifieke oplossing geselecteerd moet worden: bijvoorbeeld een oplossing voor Windows-gebaseerde clients en een oplossing voor Linux-gebaseerde servers. Bestaat er voor het in gebruik zijnde platform geen IDPS, is er sprake van een gesloten systeem (bijvoorbeeld een router of andere appliance) of staat het systeem niet onder beheer van de organisatie (zoals bij BYOD), dan is het niet mogelijk om een systeem-IDPS toe te passen.

Op het gebied van versleuteling heeft een systeem-IDPS duidelijk voordelen omdat het systeem het begin- en eindpunt is van een versleutelde verbinding. Een systeem-IDPS kan dus verkeer inzien voordat het wordt versleuteld of nadat het is ontsleuteld. Een netwerk-IDPS heeft hier uiteraard problemen mee. Is er bijvoorbeeld sprake van een VPN-verbinding dan zal een netwerk-IDPS alleen versleuteld verkeer zien en geen mogelijkheden hebben om vast te stellen of er binnen deze VPN-verbinding malafide communicatie plaatsvindt. Sommige netwerk-IDPS-oplossingen hebben tegenwoordig wel de mogelijkheid om verkeer in te zien wanneer het om TLS-versleuteling gaat. Dit is echter alleen in specifieke gevallen mogelijk en alleen wanneer het IDPS beschikt over de private sleutel waarmee de TLS-verbinding is opgezet. De vraag is overigens of dit laatste vanuit het oogpunt van beveiliging (verspreiding van de private sleutel naar andere systemen) en privacy wenselijk is.

> ***Opmerking:*** het feit dat verkeer via een versleutelde verbinding verloopt, betekent niet automatisch dat een detectiesysteem geen mogelijkheden meer heeft tot het vaststellen van malafide activiteiten. Hoewel het bij een versleutelde verbinding niet meer mogelijk is om in het verkeer te kijken, is het namelijk nog wel steeds mogelijk om andere eigenschappen van het verkeer te bekijken. Op die manier kan bijvoorbeeld nog steeds C2-verkeer worden vastgesteld door detectie uit te voeren op de IP-adressen waarmee interne systemen versleutelde verbindingen opzetten.

Omdat een systeem-IDPS afhankelijk is van het onderliggende systeem kan de integriteit van het systeem een negatieve invloed hebben op de werking van het IDPS. Wanneer er zich bijvoorbeeld een rootkit op het systeem weet te nestelen, dan kan het voorkomen dat het IDPS foutieve informatie te zien krijgt of zelfs informatie mist. Het systeem-IDPS heeft bij een succesvolle infectie dan ook maar één kans om dit te detecteren. Een netwerk-IDPS heeft dit nadeel niet.

Daarnaast kan malware op het systeem controles uitvoeren om te bepalen of er op het systeem een IDPS aanwezig is en, zo ja, welk type dit is. Op basis van herkenning van het IDPS kan een aanvaller ervoor kiezen een andere tactiek te hanteren die door dit specifieke IDPS niet zal worden opgemerkt. Een netwerk-IDPS is veel moeilijker te herkennen voor een aanvaller, zeker als dit IDPS out-of-band geplaatst is (zie volgende paragraaf) en daarom ook moeilijker te omzeilen is.

Tot slot is het voor een netwerk-IDPS vaak moeilijk te bepalen wat de impact van een aanval is. Hoewel een netwerk-IDPS tegenwoordig vaak wel kan vaststellen dat een Windows-exploit naar een Apple-systeem waarschijnlijk niet succesvol zal zijn, is de impact veel moeilijker te bepalen wanneer een Windows-exploit richting een Windows-systeem plaatsvindt. Een systeem-gebaseerd IDPS is hier in het voordeel omdat dit IDPS exact kan zien wat de gevolgen van een aanval zijn; het kan zien welke bestanden veranderen, welke processen nieuw verschijnen en welke configuratiewijzigingen op het systeem plaatsvinden. Dit maakt de impactbepaling van een aanval een stuk eenvoudiger.

#### 3.1.1.3 *Samenvatting*

Tabel 1 – N-IDPS & H-IDPS vat de belangrijkste verschillen die er bestaan tussen een netwerk-IDPS en een systeem-IDPS samen.

| Netwerk-IDPS | Systeem-IDPS |
|---|---|
| Baseert zich op netwerkverkeer | Baseert zich op de inhoud van logbestanden, register-waarden, procestabellen, etc. |
| Sluit aan op draad gebonden netwerken (NIDPS), draadloze netwerken (WIDPS) of gevirtualiseerde systemen (VIDPS) | Wordt geïnstalleerd op bestaande systemen (HIDPS) |
| + Kosteneffectief: één IDPS om meerdere systemen te beschermen | – Kostenineffectief: één IDPS (licentie) per te beschermen systeem |
| + Altijd in te zetten (platform onafhankelijk) | – Afhankelijk van de beschikbaarheid van een IDPS voor het te beschermen platform<br>Niet in te zetten op gesloten systemen zoals routers en switches |
| – Geen of weinig inzicht in versleutelde verbindingen | + Heeft inzicht in het verkeer vóór versleuteling en ná ontsleuteling |
| + Appliance, niet afhankelijk van de integriteit van een onderliggend systeem | – Afhankelijk van de integriteit van het systeem waarop het geïnstalleerd is |
| + Detectie kan moeilijk worden uitgeschakeld door aanvaller. | – Bij vergaring van voldoende rechten op het systeem kan een aanvaller de IDPS uitschakelen. |
| + Niet of moeilijk te herkennen door aanvallers en/of malware | – Mogelijk door aanvallers en/of malware te herkennen |
| – Geen of weinig inzicht in de impact die een aanval heeft | + Volledig inzicht in de impact van een aanval |

*Tabel 1. N-IDPS & H-IDPS*

### 3.1.2 IDS & IPS, de verschillen

IDPS-oplossingen vallen zoals eerder genoemd uiteen in Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS). Een IPS heeft als doel om kwaadaardig verkeer te blokkeren terwijl een IDS dit verkeer alleen wil detecteren (inzichtelijk maken) om hier vervolgens over te alerteren. Een IDS en een IPS maken vaak wel gebruik van dezelfde technieken, waardoor een IPS in feite een IDS is met daarbij de mogelijkheid tot het blokkeren van de gedetecteerde aanvallen. Hoewel in het verleden het verschil tussen een IDS en IPS nog expliciet bestond, is dit verschil tegenwoordig veel minder sterk aanwezig. Standaard is vaak sprake van een IPS, maar door dit IPS anders te configureren, en op een andere manier aan het netwerk te koppelen, functioneert het systeem in feite als een IDS.

#### 3.1.2.1 *Aansluiting*

De aansluiting van een systeem-gebaseerd IDPS is eenvoudig: installatie vindt plaats op het systeem dat via dit IDPS beveiligd moet worden. Bij een netwerk-IDPS ligt dit anders. Om verkeer te kunnen blokkeren wordt een netwerk-IPS vaak inline in het netwerk geplaatst, ook al is dit voor de werking niet strikt noodzakelijk. Bij inline plaatsing moet al het netwerkverkeer door het IPS heen stromen en kan het IPS ingrijpen zodra het verdacht verkeer waarneemt. Een netwerk-gebaseerd IDS plaatst men over het algemeen niet inline maar out-of-band. Daarbij neemt het IDS geen actieve rol in het netwerk in, maar verkrijgt het een volledige of gedeeltelijke kopie van het netwerkverkeer. Deze kopie krijgt het IDS via een speciaal geconfigureerde poort op een netwerkswitch (SPAN[4]-poort), een TAP[5]-aansluiting of een aansluiting op een netwerkhub.

Een netwerk-gebaseerd IDS kan, net als bij een netwerk-gebaseerd IPS, echter ook inline geplaatst zijn, waarbij het systeem geconfigureerd is om verkeer te allen tijde door te laten en alleen detectie – en dus geen preventie – uit te voeren op dit verkeer. In dit geval is sprake van inline bridge mode (versus inline prevention mode bij IPS-aansluitingen).

***Achtergrond***

In grote of complexe netwerken kan men ervoor kiezen een IDPS niet rechtstreeks aan te sluiten op bijvoorbeeld een SPAN-poort maar gebruik te maken van een specifiek device dat het verkeer vanaf het netwerk richting de IDPS-systemen in goede banen leidt. Deze zogenoemde network packet brokers (NPB) plaatst men tussen de input en het IDPS. Ze zijn in staat om allerlei acties uit te voeren op verzameld netwerverkeer zoals het aggregeren van meerdere inputs in één grote input, het load balancen van inputs over meerdere IDPS-systemen, het filteren van irrelevante inputs en deduplicatie van inputs.

Afhankelijk van het detectiescenario waarvoor men kiest, kan detectie ook mogelijk zijn zonder ongefilterde inputs richting het IDS. In dit soort gevallen kan het IDS detectie uitvoeren op basis van bijvoorbeeld logging van systemen en ontstaat een bijzondere vorm van out-of-band-plaatsing. Een bekend voorbeeld hiervan is DNS-gebaseerde detectie waarbij het IDS op basis van logging van de DNS-server, dus zonder toegang tot het "ruwe" DNS-verkeer, kan bepalen of er potentieel schadelijke hostnamen of IP-adressen zijn opgevraagd.

#### 3.1.2.2 *Overwegingen*

Een IPS levert naast detectie ook bescherming tegen potentiële aanvallen aangezien een IPS aanvallen daadwerkelijk kan blokkeren, terwijl een IDS deze alleen kan detecteren en dus geen automatische acties onderneemt om de impact van de aanval te beperken. Zolang het IPS aanvallen terecht blokkeert, vormt het systeem een waardevolle toevoeging op de beveiliging van het netwerk. Wanneer het IPS echter teveel *'false positives'* genereert, zorgt dit ervoor dat het IPS verbindingen, processen of bestanden onterecht blokkeert waardoor er verstoringen binnen de infrastructuur kunnen optreden.

[4] Switched Port Analyzer

[5] Test Access Port

Een voordeel van een inline geplaatst netwerk-gebaseerd IPS is dat het nooit verkeer zal missen. Immers, al het verkeer moet hierbij door het systeem heen gaan. Bij out-of-band plaatsing, zoals bij een netwerk-IDS vaak het geval is, bestaat altijd de kans dat verkeer wordt gemist. Dit gebeurt bijvoorbeeld op het moment dat de belasting op een switch te hoog wordt en de switch daardoor niet al het verkeer meer kopieert naar de SPAN-poort.

#### 3.1.2.3 *Samenvatting*

Tabel 2 vat de belangrijkste verschillen die er bestaan tussen een IDS en een IPS samen. Mede door het feit dat een IPS in de basis een IDS met blokkademogelijkheden is, blijken deze verschillen in de praktijk redelijk klein.

| IDS | IPS |
|---|---|
| Detecteert (passieve alertering) | Blokkeert / filtert (actieve respons) |
| Netwerk IDS: meestal out-of-band (promiscious) | Netwerk IPS: inline |
| Netwerk IDS werkt met kopieën van netwerkverkeer | Netwerk IPS werkt met live netwerkverkeer |
| + Heeft weinig tot geen invloed op stabiliteit netwerk of het systeem | – Kan stabiliteit netwerk of systeem beïnvloeden |

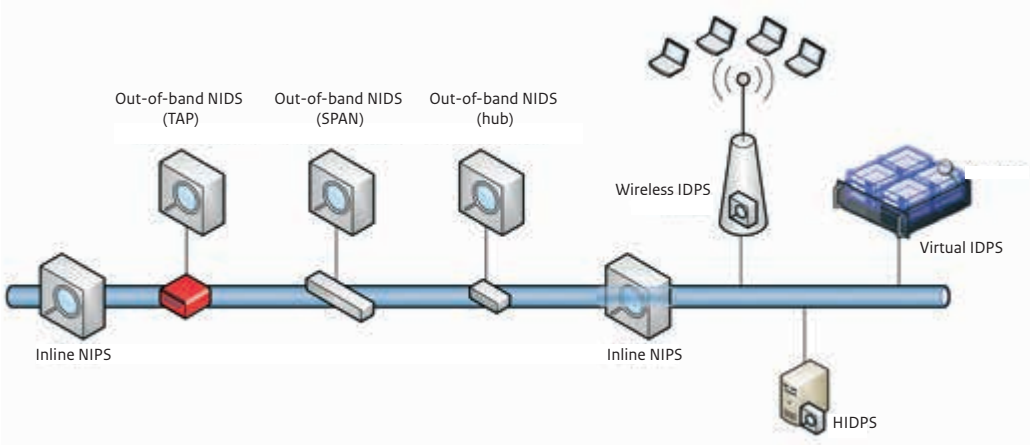
*Tabel 2. IDS & IPS*

### 3.1.3 Systeem/netwerk en IDS/IPS gecombineerd

Door de verschillende typen IDPS-oplossingen uit de vorige paragrafen te combineren, kunnen we uiteindelijk de volgende verschillende typen Intrusion- en detectionplossingen onderscheiden:

| | Detectie (IDS) | Preventie (IPS) |
|---|---|---|
| **Netwerk (bedraad)** | Network Intrusion Detection System (NIDS) | Network Intrustion Prevention System (NIPS) |
| **Netwerk (draadloos)** | Wireless Intrusion Detection System (WIDS) | Wireless Intrusion Prevention System (WIPS) |
| **Gevirtualiseerd** | Virtual Intrusion Detection System (VIDS) | Virtual Intrusion Prevention System (VIPS) |
| **Systeem (host)** | Host-based Intrusion Detection System (HIDS) | Host-based Intrusion Prevention System (HIPS) |

Figuur 4 geeft deze verschillende oplossingen weer, samen met de manier waarop deze oplossingen op een infrastructuur kunnen worden aangesloten.




*Figuur 4. Voorbeeld infrastructuur*

### 3.1.4 Detectiemethoden

Onafhankelijk van het type IDPS bestaan er grofweg twee manieren waarop dit soort systemen detectie uitvoeren op netwerkverkeer of systeemactiviteiten: op basis van handtekeningen of op basis van anomalieën. Maar ongeacht de gebruikte detectiemethode moet elke beheerder aandacht besteden aan twee belangrijke zaken: het minimaliseren van het aantal *false positives* en het minimaliseren van het aantal *false negatives*. De komende paragraaf zal eerst ingaan op deze twee verschijnselen. Daarna gaat dit hoofdstuk verder in op detectie op basis van handtekeningen en anomalieën.

#### 3.1.4.1 *Optimalisatie*

Bij het gebruik van zowel een IDS als een IPS is het van groot belang om het aantal fouten in detectie te minimaliseren. Aan de ene kant is het zaak het aantal *false positives*, ofwel het detecteren van malafide activiteiten terwijl dit niet zo blijkt te zijn, te minimaliseren. Zoals later in dit whitepaper aan de orde zal komen, leidt een slecht geconfigureerd IDS tot een enorme hoeveelheid *false positives* waardoor het voor een beheerder vaak heel moeilijk is om een IDS van toegevoegde waarde te laten zijn. Bij een IPS leiden *false positives* zelfs tot het onbedoeld blokkeren van allerlei activiteiten. Aan de andere kant kunnen ook *false negatives* ontstaan wanneer een IDS of IPS malafide activiteiten niet herkent, en hierop daarom geen actie onderneemt. Voor een goede werking van zowel een IDS als een IPS is het daarom van groot belang om zowel het aantal *true negatives* als het aantal *true positives* zo hoog mogelijk te laten zijn.

| | Positive | Negative |
|---|---|---|
| False | ***False positive:*** het systeem markeert verkeer als malafide terwijl dit bonafide blijkt te zijn. Dit leidt tot het onbedoeld blokkeren van het verkeer (IPS) of tot het genereren van foutieve alerts (IDS). | ***False negative:*** het systeem markeert verkeer als bonafide terwijl dit malafide blijkt te zijn. Dit leidt tot het onbedoeld toestaan van dit malafide verkeer (IPS) of tot het uitblijven van alerts betreffende dit malafide verkeer (IDS). |
| True | ***True positive:*** het systeem markeert verkeer terecht als malafide. | ***True negative:*** het systeem markeert verkeer terecht als bonafide. |

Naast de betrouwbaarheid van een melding speelt ook de potentiële impact of ernst van deze melding een belangrijke rol. Zo vinden bijvoorbeeld netwerkscans vrijwel continu plaats. Wanneer een IDS op het netwerk is aangesloten en over deze netwerkscans rapporteert, is er wel sprake van *true positives*, maar is de potentiële impact ervan laag.

Vaak is het ook van belang om contextuele informatie te hebben bij een melding om de impact ervan vast te kunnen stellen. Zo kan de locatie van de melding binnen het netwerk en het type eindgebruiker dat geraakt is, een grote invloed hebben op de uiteindelijke potentiële impact van de melding. Een malwarebesmetting op het systeem van een netwerkbeheerder heeft bijvoorbeeld mogelijk ernstigere consequenties dan de infectie van een systeem van een gebruiker met zeer beperkte rechten. Op eenzelfde manier is de ernst van een infectie afkomstig uit het netwerk voor gebouwbeveiliging waarschijnlijk een stuk hoger dan eenzelfde infectie afkomstig uit het draadloze netwerk voor BYOD.

Een optimaal werkend systeem genereert daarom een minimaal aantal *false positives* en *false negatives*, een maximum aantal *true positives* en *true negatives* en geeft een automatische indicatie van de ernst van de melding. Dit stelt de beheerders en gebruikers van het detectiesysteem in staat om meldingen zo goed als mogelijk te prioriteren.

> ***Opmerking:*** het hebben van een solide architectuur/netwerkontwerp kan een belangrijke bijdrage leveren aan een optimaal functionerend IDPS. Consequente compartimentering binnen het netwerk kan bijvoorbeeld betekenen dat slechts een subset van signatures op een specifiek gedeelte van het netwerk van toepassing is. Beheerders kunnen dit gebruiken om irrelevante signatures (bijvoorbeeld Linux-gebaseerde signatures in een Windows-compartiment) uit te schakelen en op die manier false positives te minimaliseren. Daarnaast helpt een goed netwerkontwerp ook bij het prioriteren van meldingen, afhankelijk van het onderdeel van het netwerk van waaruit een alertering afkomstig is.

#### 3.1.4.2 *Detectie op basis van handtekeningen*

Van oudsher vindt detectie plaats op basis van digitale handtekeningen (*signatures*). Een handtekening beschrijft een patroon waarmee het mogelijk is malafide activiteiten te herkennen. Dit is een belangrijk verschil met bijvoorbeeld de werking van een firewall. Een firewall staat in principe niets toe en laat alleen gedefinieerde uitzonderingen door. Een IDPS staat juist in de basis alles toe en detecteert (en blokkeert) alleen mogelijk kwaadaardige uitzonderingen.

Stel bijvoorbeeld dat een organisatie een FTP-server aanbiedt via internet waarop gebruikers bestanden kunnen aanbieden. Aangezien gebruikers dit altijd moeten doen via een eigen gebruikersaccount, is er mogelijk sprake van een aanval op het moment dat er getracht wordt verbinding te maken met het 'root'-account. Om dit soort gedrag vast te kunnen stellen is het mogelijk onderstaande simpele *rule* in een Snort IDS op te nemen[6]:

```
alert tcp any any -> any 21 (msg:"FTP ROOT"; content:"USER root"; nocase;)
```

Na het doorvoeren van bovenstaande *rule* zal het IDS een alert met als tekst "FTP ROOT" genereren zodra er FTP-verkeer (21/tcp) plaatsvindt met daarin de tekst "USER root".

#### 3.1.4.3 *Afwegingen bij gebruik van signatures*

Het voordeel van het gebruik van signatures is dat dit weinig *false positives* hoeft op te leveren zolang de signature maar goed geschreven is. Dit is uiteraard voor het grootste gedeelte afhankelijk van de persoon die de signature heeft opgesteld. Had in eerder genoemde *rule* bijvoorbeeld het keyword "root" gemist, dan had de *rule* op elke authenticatiepoging een alert opgeleverd. Uiteraard is dit een simplistisch voorbeeld, maar bij complexe *rules* geldt des te meer dat de *rule* smal genoeg moet zijn om geen *false positives* te veroorzaken, maar daarnaast ook breed genoeg om variaties op de aanval te kunnen detecteren.

De kans dat *false negatives* optreden is relatief groot op het moment dat een signature-schrijver zich bij het maken van een signature richt op bekende exploits die er voor een kwetsbaarheid bestaan. Zodra er dan een soortgelijke, maar toch net andere, aanval plaatsvindt via een andere exploit voor dezelfde kwetsbaarheid, is de kans groot dat het IDPS deze zal missen. Daarnaast betekent deze aanpak dat elke exploit een nieuwe *rule* vereist, wat uiteindelijk zal leiden tot een wildgroei aan signatures. Daarom richten ervaren signature-schrijvers zich bij het opstellen van signatures niet zozeer op de exploit maar veel meer op de kwetsbaarheid waarvan exploits misbruik maken (*vulnerability based signature* versus *exploit based signature*).

Het feit dat signatures in de regel pas beschikbaar komen nadat een aanval al eerder ergens is gezien, heeft zowel voor- als nadelen. Een belangrijk nadeel van signatures is dat de kans om nieuwe (onbekende) dreigingen op te merken vrij klein is. Je moet de aanval, exploit of kwetsbaarheid immers al kennen voordat je de kenmerken eruit kunt filteren. Daartegenover staat dat signatures snel en betrouwbaar kunnen werken en dat alerts vergezeld gaan van een duidelijke context omdat de signature-schrijver bekende details over de aanval aan de alert kan toevoegen.

Omdat aanvallen continu veranderen en nieuwe aanvallen verschijnen is het, bij het gebruik van signatures, wel van groot belang om de signatureset continu up-to-date te houden. Het is daarom belangrijk om een kwalitatief goede dienst hiervoor af te nemen bij een leverancier of om zelf een proces op te zetten om continu nieuwe signatures op te stellen en te verspreiden.

#### 3.1.4.4 *Detectie op basis van anomalieën*

Detectie op basis van signatures richt zich op het herkennen van bekende aanvallen. Daarmee zullen nieuwe, onbekende, aanvallen dus "onder de radar" kunnen blijven. Om dit soort onbekende aanvallen toch op te kunnen merken, kan detectie op basis van afwijkingen ofwel anomalieën worden ingezet. Hierbij kijkt men op basis van slimme mechanismen of verkeersstromen of ander gedrag afwijken van wat normaal gesproken wordt gezien binnen een netwerk of op een systeem.

[6] Overgenomen uit het Snort manual op http://manual.snort.org/node32.html

### 3.1.4.5 *Implementatie van anomaliedetectie*

Anomaliedetectie kan op diverse manieren worden uitgevoerd. Het gaat te ver om al deze verschillende manieren in dit whitepaper te behandelen. Tabel 3 beschrijft enkele voorbeelden van anomaliedetectie om een indruk te schetsen van hoe dit kan werken.

| Type | Omschrijving |
|---|---|
| **Netwerkniveau** | |
| Protocol anomaliedetectie | De opmaak van netwerkpakketten is vastgelegd in protocolstandaarden. Deze protocolstandaarden geven bijvoorbeeld aan hoe communicatie moet zijn opgebouwd, welke informatie kan worden opgenomen in de communicatie, welke sequenties moeten worden doorlopen, et cetera. Door actueel netwerkverkeer te matchen tegen de protocolstandaard is het mogelijk afwijkingen van deze standaard op te merken. Een dergelijke afwijking kan een indicatie vormen dat een aanval plaatsvindt. |
| Flow anomaliedetectie | Informatie over netwerkstromen (in de vorm van NetFlow, Sflow, Jflow en IPFIX) geven inzicht in systemen die met elkaar communiceren, de tijdstippen en frequentie waarop dit gebeurt en de hoeveelheid informatie die zij uitwisselen. Op basis hiervan is het mogelijk om afwijkende c.q. opvallende netwerkstromen (anomalieën) te detecteren. Zo is uitgebreide communicatie met een server in een land waarmee vanuit het netwerk normaal gesproken nooit gecommuniceerd wordt een afwijking die onderzocht zou kunnen worden. |
| Applicatie anomaliedetectie | Door netwerkverkeer binnen een netwerk te bekijken, kan een detectie-oplossing inzicht verschaffen in de applicaties die binnen het netwerk in gebruik zijn. Wanneer plotseling een nieuwe applicatie zichtbaar wordt, kan dit een indicatie zijn van malafide activiteiten. Wanneer voor webverkeer bijvoorbeeld altijd gebruik gemaakt wordt van Internet Explorer en nu webverkeer zichtbaar wordt vanuit een alternatieve browser (bijvoorbeeld Lynx) dan kan dit duiden op een infectie. |
| **Systeemniveau** | |
| System call anomaliedetectie | Applicaties op een systeem maken vaak gebruik van een vaste set aan system calls. Wanneer de applicatie een system call doet die nog niet eerder werd gezien, kan dit betekenen dat via de applicatie een aanval op het systeem is uitgevoerd. |
| Sandboxing | Een relatief nieuwe manier van anomaliedetectie is sandboxing waarbij een beveiligingsoplossing een potentieel malafide bestand opent in een gecontroleerde omgeving om te zien wat hiervan het resultaat is. Vaak vindt daarbij eerst een statische beoordeling van het bestand plaats en wordt het bestand pas dynamisch geanalyseerd nadat het “voldoende verdacht” is bevonden. |

*Tabel 3 - anomaliedetectie*

### 3.1.4.6 *Afwegingen bij anomaliedetectie*

Een belangrijk voordeel van anomaliedetectie is duidelijk dat het de mogelijkheid biedt alerts te genereren zonder kennis vooraf. Er zijn dus geen vooropgestelde patronen vereist om afwijkingen te kunnen detecteren en daarmee ontbreekt ook de eis tot het continu updaten van deze patronen zoals wel het geval is bij signaturedetectie.

Daarnaast is het met anomaliedetectie mogelijk om aanvallen te herkennen die, op basis van signatures, moeilijk of onmogelijk te zien zijn. Denk daarbij bijvoorbeeld aan een aanval waarbij een aanvaller verhoogde rechten weet te verkrijgen. In dergelijke gevallen is er niet altijd sprake van een specifieke aanval of kwetsbaarheid maar voert de aanvaller acties uit die, binnen de context van een beheerder, niet malafide zijn.

Daartegenover bestaat er uiteraard ook een aantal nadelen aan het gebruik van anomaliedetectie. Zo kan anomaliedetectie leiden tot zowel een groot aantal *false positives* als een groot aantal *false negatives*. Vooral aanvallen die over een langere tijd lopen en daarbij minimale afwijkingen veroorzaken (“*low and slow*”) zal men op basis van anomaliedetectie moeilijk kunnen detecteren (*false negatives*). Op netwerken waarop BYOD is toegestaan, is anomaliedetectie mogelijk moeilijk bruikbaar omdat de verscheidenheid aan systemen die hierop aansluiten vrijwel nooit voldoen aan de training set en dus veel *false positives* zullen veroorzaken.

Verder is een grote training set vereist voordat afwijkingen t.o.v. normaal gedrag zichtbaar worden en kunnen aanvallen die plaatsvinden tijdens de training set zorgen voor een verontreinigde set (een aanval als onderdeel van normaal gedrag).

Tot slot kan anomaliedetectie resource-intensief zijn omdat de detectie-oplossing vaak individuele acties moet evalueren tegen een grote set aan "normale" acties.

#### 3.1.4.7 *Signatures versus anomalieën*

Tabel 4 somt de belangrijkste verschillen tussen signaturedetectie en anomaliedetectie op.

| Signature-based | Anomaly-based |
|---|---|
| Werkt op basis van patronen van bekende aanvallen | Werkt op basis van afwijkingen ten opzichte van normaal gedrag |
| – Detecteert vooral bekende aanvallen, mogelijk veel false negatives | + Detecteert naast bekende ook onbekende aanvallen |
| + Weinig false positives (bij goede signatures) | – Mogelijk veel false positives en vereist veel fine-tuning vooraf |
| – Vereist continu aanpassingen in signatures | + Maakt detectie mogelijk zonder vooropgestelde patronen (geen updates vereist) |
| + Resource-efficiënt | – Resource-intensief |
| + Duidelijke context bij alerts | – Context bij alerts ontbreekt veelal |

*Tabel 4 - signature & anomaly*

### 3.1.5 Architectuur

Een IDPS bestaat over het algemeen uit een standaard set aan componenten die gezamenlijk detectie/preventie en het beheer hierover mogelijk maken. De benamingen die leveranciers aan deze componenten geven kunnen verschillen, maar vaak komt het uiteindelijk neer op in ieder geval de volgende componenten:

- Een **sensor** of **agent** die de bron van de detectie vormt en daarmee aan de basis van het IDPS staat. De sensor of agent ontvangt bijvoorbeeld het netwerkverkeer (NIDPS) of heeft bijvoorbeeld toegang tot logbestanden (HIDPS).

- Eén of meerdere **databases** voor het opslaan van in ieder geval detectieinformatie (signatures en dergelijke) en alerts. In gedistribueerde omgevingen beschikken vaak zowel de sensoren als de managementsystemen over een database.

- **Managementservices** die het mogelijk maken om bijvoorbeeld aangesloten sensoren/agents aan te sturen, nieuwe agents of updates uit te rollen en de meldingen vanuit deze systemen te verwerken en/of te correleren.

- Een **console** die beheerders in staat stelt om alle administratieve en monitoringactiviteiten uit te voeren. Denk daarbij aan het bekijken van alerts die sensoren hebben gegenereerd, het invoeren van detectie-signatures, het genereren van rapportages en het configureren van agents. Een console kan zowel een losstaand programma zijn dat beheerders op hun desktop installeren als web gebaseerd zijn.

In sommige gevallen voegen leveranciers ook koppelingen met de cloud toe waarbij bijvoorbeeld patronen gecontroleerd worden tegen een database in een cloud of waarbij verdachte bestanden dynamisch worden geanalyseerd binnen de cloud.

Bij het inrichten van Intrusion detection en Intrusion prevention binnen een organisatie is een belangrijke keuze die de organisatie moet maken een keuze tussen een stand-alone oplossing of een gedistribueerde oplossing. De stand-alone oplossing is de meest eenvoudige oplossing, maar deze is in grotere omgevingen niet goed beheersbaar en niet efficiënt.

Bij een stand-alone oplossing bestaat er één systeem of één pakket dat geheel zelfstandig in staat is om malafide activiteiten binnen een netwerk of op een systeem te herkennen. Bij een dergelijke oplossing bevat één systeem dus alle eerder genoemde componenten en is het niet mogelijk om vanaf een centraal managementsysteem alerts te bekijken of configuratiewijzigingen door te voeren. Bij een klein aantal installaties is dit goed te doen maar wanneer detectie op meerdere plaatsen gewenst is, betekent dit dat alle losse installaties ook apart beheerd moeten worden.

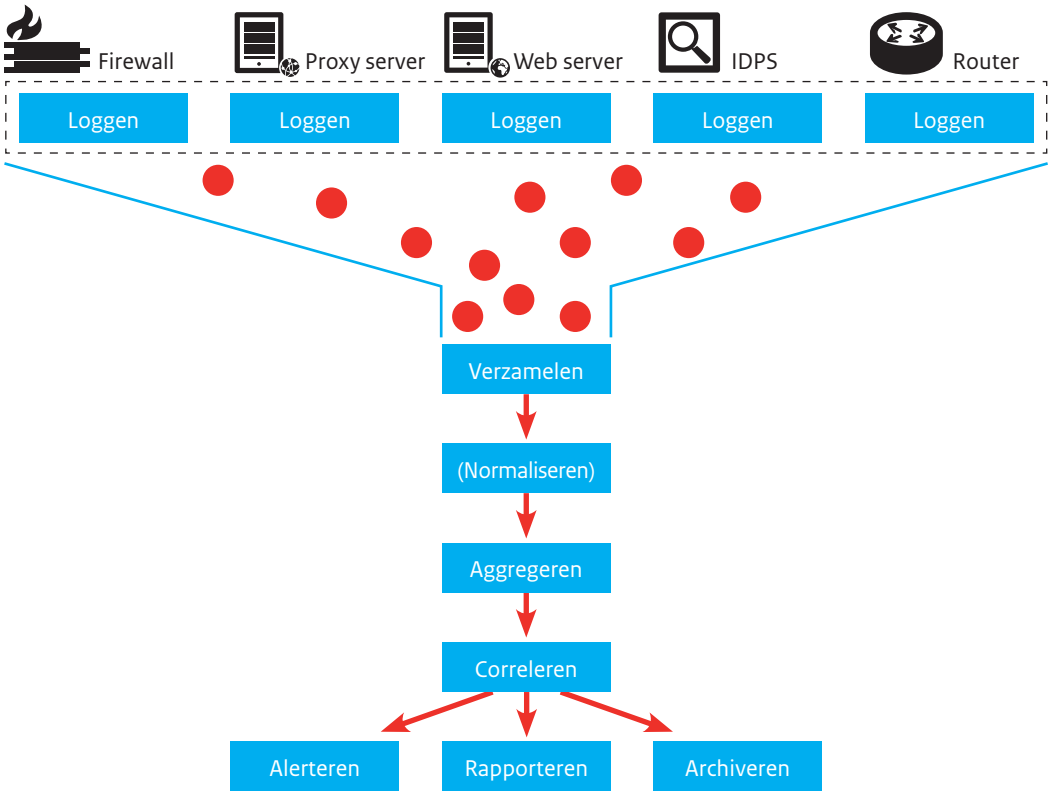
Daarom schakelen veel organisaties al snel over op een oplossing waarbij gedistribueerde agents of sensoren zorgen voor de daadwerkelijke detectie en centrale managementservers verantwoordelijk zijn voor de aansturing van deze agents of sensoren. Het uitrollen van nieuwe signatures of het bekijken van gegenereerde alerts verloopt via deze centrale servers waardoor het beheer, zeker bij een groot aantal "meetpunten", een stuk efficiënter is ingeregeld.

## 3.2 Security Information Event Management (SIEM)

Naast een IDPS, kan een organisatie er ook voor kiezen om een zogenoemde *Security Information Event Management* (SIEM) oplossing in te zetten. Bij een dergelijke oplossing verzamelt één systeem logginginformatie vanuit allerlei componenten in het netwerk om deze informatie vervolgens te normaliseren, te correleren en te aggregeren om op die manier alerts en andere rapportages beschikbaar te kunnen maken. Een SIEM helpt daarmee om het maximale te halen uit de beschikbare logging. Daar waar logging in het verleden vaak alleen gebruikt werd voor forensische toepassingen (wat is er bij dit incident gebeurd?) of alleen achteraf maandelijks of dagelijks werd bekeken, zorgt het SIEM ervoor dat er in sommige gevallen real-time en geautomatiseerd actie kan worden ondernomen op basis van opvallende zaken uit de beschikbare logging. Daarbij kan een SIEM ook helpen om contextuele informatie bij een alert te verzamelen.

### 3.2.1 Stappen van een SIEM

Aan de basis van een SIEM staan de bronnen die informatie uit logging aanleveren. Het SIEM verzamelt al deze logging centraal op één plek. Figuur 5 geeft de werking van een SIEM in grote lijnen weer.




*Figuur 5. SIEM*

De verschillende stappen uit figuur 5 worden hieronder verder uitgewerkt.

### 3.2.2 Loggen

Vrijwel alle systemen binnen een organisatie zullen in staat zijn om logging te genereren m.b.t. de acties die op dit systeem plaatsvinden. Niet alle logging is even interessant of bruikbaar voor in het SIEM. De focus voor het SIEM moet uiteraard liggen op logging informatie die te gebruiken is om security-gerelateerde activiteiten te ontdekken.

Het SANS Institute heeft een aantal categorieën van logging opgesteld die essentieel zijn om op regelmatige basis te monitoren om op die manier beveiligingsincidenten te kunnen ontdekken. Deze categorieën zou een organisatie dan ook kunnen gebruiken om bronnen te verzamelen voor input in het SIEM. SANS onderscheidt in de "*6 categories of critical log information*"[7] de volgende soorten logging:

1. **Authenticatie- en autorisatielogs**. Denk hierbij aan informatie over mislukte inlogpogingen, login-pogingen die buiten reguliere kantoortijden plaatsvinden en pogingen tot het uitvoeren van acties met bijzondere rechten.

2. **Wijzigingslogs**. Het gaat hierbij niet om rapportages over bijvoorbeeld geplande wijzigingen in het kader van wijzigingsbeheer maar over wijzigingen die op laag niveau plaatsvinden op systemen en die van invloed kunnen zijn op de beveiliging ervan. Denk daarbij aan het wijzigen van essentiële bestanden op het systeem (bijvoorbeeld kernel-bestanden), installatie van nieuwe programma's en wijzigingen in bestandstoegang.

3. **Logs met betrekking tot netwerkactiviteit**. Informatie over verdachte netwerkactiviteit kan helpen in het ontdekken van malafide activiteiten. Voorbeelden van potentiële verdachte netwerkactiviteiten zijn grote hoeveelheden uitgaand netwerkverkeer naar één specifiek IP-adres, VPN-activiteit buiten kantoortijden en verkeer op basis van niet-standaard protocollen. Verder zou ook logging rondom netwerkactiviteit vanuit derden (leveranciers, outsourcers) scherp in de gaten moeten worden gehouden omdat via dit soort verbindingen vaak toegang mogelijk is tot interne systemen.

> ***Volledige network packet captures***
> Naast het loggen van metadata rondom netwerkactiviteit kan een organisatie er ook voor kiezen om, in bepaalde plaatsen in het netwerk, de volledige netwerkactiviteit vast te leggen in de vorm van een network packet capture. Het hebben van deze volledige captures maakt het bijvoorbeeld mogelijk om nieuwe signatures te toetsen tegen historisch netwerkverkeer. Bovendien kunnen de captures zeer bruikbaar zijn bij forensisch en juridisch onderzoek in het geval van incidenten. Gezien de grote hoeveelheid opslag die volledige captures vereisen, is het belangrijk te realiseren dat niet dezelfde tijdsspanne kan worden bereikt als bij het vastleggen van alleen metadata rondom netwerkactiviteit.

4. **Logs met betrekking tot de toegang tot kritieke resources**. Bij een aanval zal een indringer zich vaak richten op kritieke resources binnen het netwerk. Door bijvoorbeeld logging over toegang tot kritieke databases, logservers en firewalls te monitoren kan dit mogelijk ontdekt worden. Ook logging van een *Data Loss Prevention* (DLP) oplossing, een type systeem dat toeziet op het lekken van gevoelige informatie vormt hiervoor een bruikbare input.

5. **Logs met betrekking tot malwareactiviteit**. Informatie afkomstig van virusscanners (gedetecteerde virussen), over virusscanners (eventuele problemen bij het scannen van bestanden) en informatie over verbindingen naar verdachte (malware-gerelateerde) IP-adressen zijn indicaties van eventuele beveiligingsproblemen.

[7] http://www.sans.edu/research/security-laboratory/article/sixtoplogcategories

6. **Logs met betrekking tot kritieke fouten**. Malafide activiteiten kunnen leiden tot het falen of crashen van applicaties en systemen, bijvoorbeeld bij misbruik van een kwetsbaarheid. Logging over bijvoorbeeld het (ongepland) herstarten van applicaties en systemen en het vollopen van bestandssystemen kunnen daarom bijdragen aan het detecteren van malafide activiteit.

De informatie voor deze logging kan afkomstig zijn van diverse componenten binnen het netwerk. Voor de hand liggende bronnen zijn proxyservers, mailservers, virusscanners, databaseservers en authenticatie-systemen (bijvoorbeeld Microsoft Active Directory). Maar ook de logging van IDPS-installaties binnen het netwerk kunnen van grote waarde zijn om de informatie in het SIEM te voeden. Daarbij kan het SIEM er ook voor zorgen dat een mogelijk onschuldig ogend alert van een IDPS uiteindelijk toch een hoge prioriteit krijgt nadat deze alert is gecorreleerd met informatie uit een ander systeem (bijvoorbeeld informatie van een HIDS gecombineerd met informatie uit een NIDS). Daarmee wordt duidelijk dat een IDPS en een SIEM niet los van elkaar staan maar elkaar juist kunnen versterken.

Naast de genoemde typen logging bestaat er nog een ander type logging dat heel waardevol kan zijn in het detecteren van malafide activiteiten: applicatie-logging. Applicatie-logging is zeer specifiek voor een bepaalde applicatie en geeft de mogelijkheid om transacties op te merken die op zich wel valide kunnen zijn maar ongebruikelijk, onmogelijk of onverwacht zijn gegeven de context van de transactie. Denk bijvoorbeeld aan een betaalsysteem waarbij dezelfde gebruiker twee keer zijn pinpas aanbiedt: één keer voor een pintransactie in Utrecht en één keer voor een pinbetaling in een winkel in Barcelona. Beide acties zijn los van elkaar niet opmerkelijk, maar wanneer beide transacties binnen een half uur na elkaar plaatsvinden, is sprake van een incident omdat het voor één-en-dezelfde persoon fysiek gezien niet mogelijk is om binnen een half uur zowel in Utrecht als in Barcelona aanwezig te zijn. Hoewel deze vorm van logging en detectie verder niet aan bod komt in dit whitepaper, kan het zeker een waardevolle toe-voeging vormen bovenop de andere detectie-mechanismen in een netwerk.

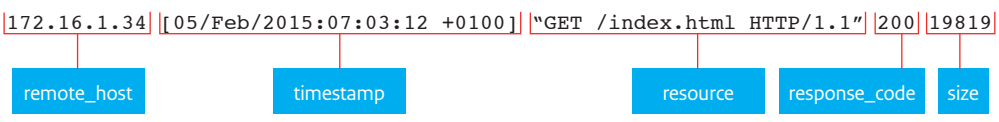
### 3.2.3 Verzamelen

De verschillende systemen in een netwerk zullen de logging vaak decentraal – dus op de devices zelf – opslaan. Om het SIEM toch toegang te kunnen geven tot deze logging moeten koppelingen gelegd worden tussen deze decentrale systemen en het centrale SIEM. De beschikbare protocollen en applicaties om deze koppeling te realiseren zijn legio en het gaat dan ook te ver deze in dit whitepaper te bespreken. Voorbeelden van veel voorkomende oplossingen zijn SYSLOG, bestandskopieën op basis van FTP of SCP en HTTP(S) in combinatie met XML-gebaseerde protocollen (zoals het Security Device Event Exchange (SDEE) protocol).

Het is geheel afhankelijk van de architectuur, systemen en platformen die binnen een organisatie in gebruik zijn, welke koppelmethode het meest effectief en het meest efficiënt is. Dit bepaalt ook of de SIEM zelf logbestanden moet ophalen (pull-methode) of dat systemen juist zelf actief logbestanden aanleveren aan de SIEM (push-methode).

### 3.2.4 Normaliseren

Elk systeem zal logging in een ander formaat aanleveren. Dit betekent dat het SIEM informatie nodig heeft over hoe deze informatie is opgebouwd om er vervolgens individuele velden/eigenschappen uit te kunnen halen. Neem bijvoorbeeld onderstaande logregel van een Apache webserver:




Als het SIEM niet verteld wordt hoe deze Apache-regel is opgebouwd, kan deze er in eerste instantie niet veel mee doen. Is het eerste IP-adres bijvoorbeeld het adres van het bron- of het doelsysteem? Via een invoerdefinitie kan het SIEM bepalen welke informatie op welke plek in de logregel terug te vinden is waardoor de hierboven getoonde Apache-regel uiteindelijk resulteert in 5 afzonderlijke elementen.

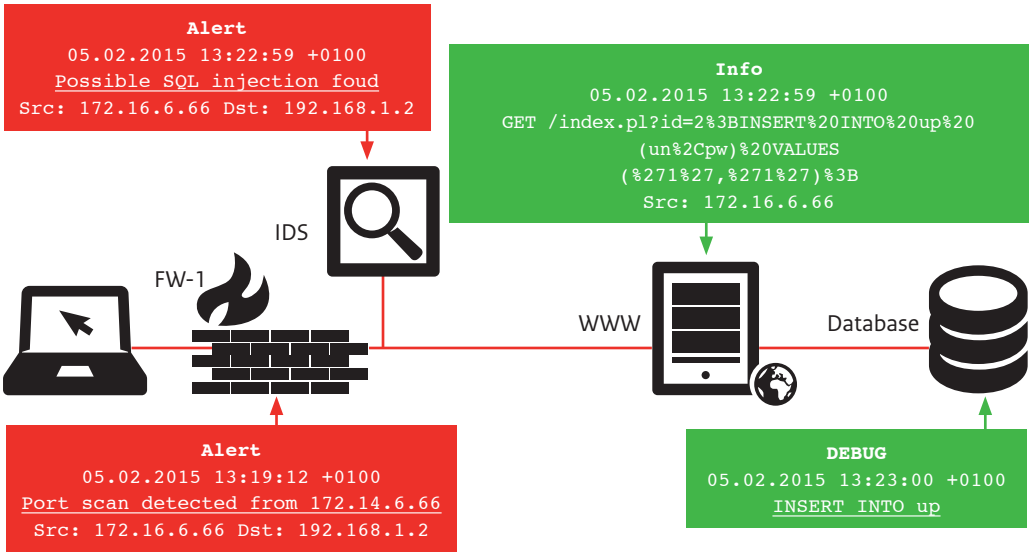
Wanneer het SIEM de informatie opslaat in een eigen (relationele) database dan kan het zijn dat informatie verloren gaat wanneer er in de database geen ruimte is om een bepaald kenmerk op te slaan. Zo kan het zijn dat na het verwerken van de Apache-regel alleen het IP-adres (remote_host), het tijdstip (timestamp) en de geraadpleegde resource worden opgenomen en de overige informatie verloren gaat. Sommige SIEM-toepassingen slaan de informatie in het originele formaat op waardoor deze informatie altijd behouden blijft en er dus geen mapping hoeft te worden gemaakt met een door het SIEM gebruikt dataformaat.

### 3.2.5 Aggregeren

Om te voorkomen dat identieke meldingen leiden tot vele (dubbele) alerteringen, zal het SIEM meldingen zoveel als mogelijk aggregeren. Dit houdt bijvoorbeeld in dat het SIEM niet 1.000 keer melding gaat maken van hetzelfde incident, maar dat het al deze meldingen aggregeert en daarbij specificeert dat deze melding 1.000 keer plaatsvond.

### 3.2.6 Correleren

Nadat normalisatie en aggregatie heeft plaatsgevonden, kan het SIEM starten met correleren. Tijdens het correleren, zal het SIEM de losse stukken informatie in relatie brengen met andere losse stukken informatie die door systemen is aangeleverd en deze informatie, daar waar mogelijk, aanvullen met contextinformatie. Hierdoor kunnen inzichten ontstaan die er niet zijn wanneer alle brokken informatie los worden beoordeeld.




*Figuur 6. Voorbeeld*

In figuur 6 hebben vier systemen afzonderlijk één of meerdere meldingen gemaakt (of gelogd) met betrekking tot een aanval op de website van de organisatie. De firewall heeft hierbij een port scan gedetecteerd en het IDS een poging tot SQL-injectie. De webserver en de databaseserver hebben alleen informatie gelogd, zonder daarbij een alert te genereren. Door de verschillende berichten te correleren, kan het SIEM een compleet beeld schetsen van de aanval:

*Op 5 februari 2015, heeft een aanvaller vanaf het IP-adres 172.16.6.66 een port scan uitgevoerd op de internet-omgeving waarna de aanvaller vervolgens een SQL-injectieaanval uitvoerde op de webserver via de URL "/index.pl?id=2%3BINSERT%20INTO%20up%20(un%2Cpw)%20VALUES (%271%27,%271%27)%3B". Deze aanval heeft er uiteindelijk toe geleid dat een nieuw record aan de tabel "up" (usernames en passwords) is toegevoegd.*

Door de correlatie uit te voeren, ontstaat ook meer inzicht in de impact en het succes van een aanval. Zo vinden SQL-injectieaanvallen op een website veelal dagelijks plaats maar zullen deze in veel gevallen niet succesvol zijn. Een alert van het IDS hierover is daarom ook niet altijd even belangrijk. Wanneer echter blijkt dat een SQL-injectieaanval ook daadwerkelijk gevolgen heeft op databaseniveau – zoals in het voorgaande voorbeeld – dan is een directe reactie vereist.

### 3.2.7 Alerteren

Wanneer het SIEM een activiteit detecteert kan het daarover ook een alert uitsturen. Het SIEM onderscheidt zich daarmee niet van bijvoorbeeld een IDS dat eenzelfde soort melding kan versturen. Het verschil is echter dat een SIEM gecorreleerde informatie en verrijkte informatie (contextinformatie) kan aanleveren. Daarmee is het voor de medewerker die het alert behandelt, een stuk eenvoudiger om op het incident te reageren.

Stel bijvoorbeeld dat het SIEM een malware-infectie in het netwerk detecteert. Wanneer een IDS een dergelijk incident opmerkt, zal het daarover bijvoorbeeld een melding kunnen generen waarbij het IP-adres van het bronsysteem zichtbaar wordt. Wat voor het behandelen van een dergelijk incident vaak belangrijk is, is om niet alleen het IP-adres te weten maar ook de naam van de gebruiker die het incident initieert. Denk bijvoorbeeld aan een malware-incident dat afkomstig is vanaf een systeem waarop vele gebruikers gelijktijdig zijn ingelogd. Het SIEM kan dit soort contextinformatie vaak geautomatiseerd aanleveren bij het alert, waardoor de medewerker deze informatie niet handmatig hoeft op te zoeken.

### 3.2.8 Rapporteren

Een SIEM kan uiteraard rapporteren over de informatie die in het SIEM aanwezig is. Soms zal het SIEM deze rapportages automatisch en met een bepaalde frequentie opleveren (bijvoorbeeld maandrapportages) en in andere gevallen betreft het real-time overzichten. Daarnaast bestaat de mogelijkheid om de informatie in het SIEM te bevragen op specifieke eigenschappen, zoals:

- Welke acties heeft IP-adres A.B.C.D de afgelopen 24 uur geïnitieerd?
- Welke acties heeft gebruiker XYZ het afgelopen uur uitgevoerd?
- Hebben wij verkeer waargenomen richting website http://x.y.nl?
- Naar welk IP-adres is uitzonderlijk veel netwerkverkeer gestuurd?

Een SIEM heeft op het gebied van rapporteren een groot voordeel boven alleen een IDS: een IDS bewaart over het algemeen geen historische ruwe data waardoor het moeilijk is om terug te kijken. Hierdoor is het bijvoorbeeld niet mogelijk om te controleren of er in het verleden hits zijn geweest op een indicator die pas nu bekend wordt.

### 3.2.9 Archiveren

Tot slot zal het SIEM de verzamelde informatie moeten archiveren zodat deze beschikbaar is voor latere bevraging. Bij het archiveren bestaat een aantal aandachtspunten:

- Bepaal hoe lang informatie überhaupt beschikbaar moet blijven voor bevraging en wanneer informatie verwijderd moet worden (retentiebeleid).
- Bepaal of informatie in de live-omgeving beschikbaar moet zijn of dat gearchiveerde informatie ook offline of in een andere omgeving opgeslagen kan worden.
- Bepaal welke informatie wel langere tijd beschikbaar moet blijven en welke informatie niet.

# 4 Best practices


In feite is een detectie-oplossing een nieuw informatiesysteem, zoals elk ander informatiesysteem. De introductie van een detectie-oplossing binnen een organisatie is dan ook op veel punten vergelijkbaar met de introductie van standaard informatiesysteem.

Het proces om te komen tot een werkende detectie-oplossing verloopt in grote lijnen via het model dat werd geïntroduceerd in hoofdstuk 2 (kennis – monitoring – incident respons – incident analyse). Bij elk van deze stappen bestaat er een aantal best practices die specifiek zijn voor detectie-oplossingen. Dit hoofdstuk beschrijft de belangrijkste best practices, onderverdeeld naar de fase waarop ze betrekking hebben. Het gaat hier dus om de belangrijkste best practices die specifiek zijn voor de introductie van een detectie-oplossing, waarbij het hoofdstuk zeker niet pretendeert een volledig overzicht te schetsen van alle mogelijke best practices die er op dit gebied bestaan.

## 4.1 Kennis

Bij de implementatie van een detectie-oplossing is het van belang eerst draagvlak te creëren voor een dergelijke oplossing en andere voorbereidingen te treffen om daarna pas verder te gaan met het analyseren en ontwerpen van de oplossing.

### 4.1.1 Voorbereiding

Voordat een organisatie überhaupt kan starten met een detectie-oplossing, is het dus van belang om eerst draagvlak hiervoor te ontwikkelen binnen de organisatie. Dit draagvlak bestaat het liefst op alle lagen van de organisatie, vanaf de werkvloer tot aan het hogere management. In dit proces wordt ook duidelijk welke hoofddoelen de organisatie met de introductie van een detectie-oplossing hoopt te bereiken.

Onderstaande zaken zijn relevant bij het voorbereiden van detectie binnen een organisatie:

- **Creëer awareness.** Voordat een detectie-oplossing succesvol kan zijn, moet binnen de organisatie eerst het besef leven dat het herkennen en vroegtijdig blokkeren van digitale aanvallen van groot belang is. Helaas bestaan er voldoende voorbeelden van organisaties die door het niet tijdig detecteren van een aanval ernstige schade hebben opgelopen. Deze voorbeelden kunnen zeker helpen om de noodzaak tot goede detectie op de kaart te krijgen.

***Opmerking:*** bij het introduceren van een detectie-oplossing krijgt men te maken met een groot aantal verschillende stakeholders. Denk hierbij aan management (bekostiging project), beheerders (gebruik van het systeem), eindgebruikers (wiens activiteiten bekeken zullen worden) en mede-zeggenschaps-raden (die zich inzetten voor de rechten van eindgebruikers). Daarom is het essentieel om deze partijen al in een vroeg stadium te betrekken bij de plannen en sponsoren voor het project te werven. Stem met de verschillende stakeholders of hun technische rechterhand ook een baseline af waar alle disciplines het mee eens zijn.

- **Bepaal het hoofddoel van detectie**. Bepaal bijvoorbeeld van welk type dreigingen voor de organisatie het meeste gevaar uitgaat en waartegen bescherming gewenst is. Ligt de nadruk bijvoorbeeld op continuïteit (bijvoorbeeld detectie en preventie van DDoS-aanvallen, ransomware of non-targeted attacks) of op het beschermen van informatie tegen aanvallen door "huis, tuin en keuken" hackers of zelfs geavanceerde actoren (bijvoorbeeld detectie en preventie van APT-aanvallen).

- **Bepaal de belangrijkste assets van de organisatie.** Het ligt voor de hand dat aanvallers hun pijlen voornamelijk zullen richten op de spreekwoordelijke kroonjuwelen van een organisatie en dat een succesvolle aanval hierop ook de meeste schade zal berokkenen aan de organisatie. Het is daarom belangrijk om in een vroeg stadium te bepalen wat de belangrijkste assets zijn waarop de detectie-oplossing zich zal moeten richten. Dit betekent niet dat je geen rekening hoeft te houden met scenario's waar aanvallers zich richten op andere informatie en systemen die niet gelabeld zijn als kroonjuweel. Zoals systemen die "per ongeluk" geraakt worden door ransomware en de beschikbaarheid van de systemen wegneemt.

***Opmerking:*** Geef vooraf bij (hoger) management aan dat in de eerste periode (1 a 2 jaar van de implementatie van een detectie-oplossing) het aantal incidenten zal toenemen. Er wordt immers inzage gecreëerd en dit leidt tot meer zichtbare bonafide en malafide incidenten. Hiermee voorkom je dat het management de implementatie zal zien als mislukking. Finetuning is een langdurig proces wat uiteindelijk de implementatie van detectie-oplossingen tot een succes maakt.

### 4.1.2 Analyse en ontwerp

In de analyse- en ontwerpfase analyseert men in eerste instantie welke behoeften er bestaan met betrekking tot de te introduceren oplossing. Deze behoeften (requirements) resulteren uiteindelijk in een ontwerp op basis waarvan de detectie-oplossing kan worden geïmplementeerd. Daarnaast moet in de ontwerpfase ook al worden nagedacht over de processen die rondom detectie moeten worden ingericht.

Bij het opstellen van de requirements zijn de volgende zaken van belang:

- **Bepaal tegen welke dreigingen maatregelen getroffen moeten worden**. In de voorbereiding is al een start gemaakt met de specificatie van de belangrijkste dreigingen waartegen het systeem bescherming moet bieden. In deze fase zullen deze dreigingen in meer detail moeten worden uitgewerkt. Stel bijvoorbeeld dat watering hole-aanvallen als belangrijke dreiging zijn gespecificeerd, dan moet in de fase duidelijk worden om welke type watering hole-aanvallen het dan gaat. Gaat het om het hele spectrum aan drive-by aanvallen voor een generieke doelgroep of juist watering hole-aanvallen met een specifieke doelgroep, zoals rijksambtenaren? Daarnaast is het van belang te bepalen voor welke processen deze typen aanvallen relevant zijn.

- **Bepaal welke onderdelen van de infrastructuur beschermd moeten worden**. Afhankelijk van de te beschermen assets, en de weg die de aanvallers moeten bewandelen om hier te komen, is het van belang te bepalen welke onderdelen van de infrastructuur in ieder geval onderdeel moeten gaan uitmaken van de detectie-oplossing. Een vraag die daarbij centraal moet staan is waar in de infrastructuur detectie vereist is om inzage te krijgen in de eerder vastgestelde dreigingen. Hieruit volgen ook vereisten die gesteld worden op het gebied van te ondersteunen platformen (bijvoorbeeld Windows, Linux of Mac OS X), te ondersteunen netwerken (bijvoorbeeld draadloos of bedraad) en te ondersteunen protocollen.

- **Bepaal welke informatie voor het goed functioneren van het systeem vereist is**. Om goed te kunnen functioneren heeft elke detectie-oplossing voldoende inputs nodig. Bij een netwerk-gebaseerd IDPS betekent dit dat bijvoorbeeld het systeem het juiste netwerkverkeer ontvangt, bij een SIEM dat het systeem de vereiste logging kan verzamelen.

- **Bepaal hoe het detectiesysteem inzage in dreigingen moet gaan bieden.** Zoals hoofdstuk 3 over hulpmiddelen al beschreef, kan een detectie-oplossing op verschillende manieren inzage bieden in de relevante dreigingen die men heeft gedefinieerd.

Tijdens het opstellen van de requirements is het van belang hier een aantal keuzes in te maken. Denk hierbij ook aan uitgaand verkeer waarmee een dreigingsactor informatie exfiltreert. Stel het detectiesysteem hier ook op in.

- **Bepaal de vereiste en/of beschikbare resources**. Het uitvoeren van detectie kan veel van systemen en mensen vragen (uitzonderingen daar gelaten). Systemen kunnen door de grote hoeveelheden data hard moeten werken om daarin malafide zaken te ontdekken en mensen zullen tijd moeten besteden aan het uitvoeren van respons op alerts en het onderhouden van de extra systemen. De hoeveelheid resources die de organisatie vrij wil maken voor detectie bepaalt dan ook voor een groot deel welke oplossingen – en in welke configuratie – geschikt zijn.

  Simpele meldingen, zoals een standaard infectie met bekende malware, kunnen afgehandeld worden door een service desk of externe partij. Hierdoor kunnen de specialisten zich richten op op de geavanceerde aanvallen.

Tabel 5 schetst een overzicht van mogelijke kosten waar een organisatie bij de introductie van een detectie-oplossing rekening moet houden.

| Voortraject | Implementatie | Exploitatie |
|---|---|---|
| Manuren voor:<br>• het opstellen van een business case en het overtuigen van management<br>• overleg met juristen, medezeggenschapsraden en andere stakeholders<br>• het oriënteren op mogelijke oplossingen<br>• het opstellen en toetsen van selectiecriteria<br>• het opstellen van een functioneel ontwerp<br>• het opstellen van een technisch ontwerp<br>• het opstellen van contracten | Manuren voor:<br>• het configureren van systemen waarop het IDPS moet aansluiten (bijvoorbeeld SIEM)<br>• plaatsing van de IDPS-systemen<br>• het uitvoeren van testen (performance, security)<br>• het aanpassen en uitbreiden van logging<br><br>Kosten voor:<br>• aanschaf van IDPS hard- en software (o.a. servers en sensoren)<br>• aanschaf van aanvullende componenten of het upgraden van bestaande componenten voor het kunnen realiseren van de oplossing (taps, switches, etc)<br>• mogelijke aanschaf van aanvullende licenties voor bijvoorbeeld een SIEM<br>• opleiding van medewerkers | Manuren voor:<br>• het verwerken van, onderzoeken van en reageren op alerts<br>• het vergaren en effectueren van intelligence<br>• het optimaliseren en tweaken van het IDPS of SIEM<br>• het onderhouden van contacten met de serviceprovider<br>• het beheer van de detectiesystemen<br>• het opstellen en beoordelen van rapportages<br><br>Kosten voor:<br>• afname van rules van externe providers<br>• onderhoudscontracten<br>• soft- en hardwareonderhoud |

*Tabel 5 - overzicht mogelijke kosten*

- **Bepaal de vereiste fout-tolerantie**. Een detectie-oplossing moet fout-tolerant zijn zodat de organisatie erop kan vertrouwen dat het systeem goed blijft functioneren, ook wanneer het systeem zelf onder aanval ligt. Belangrijke eigenschappen op het gebied van fout-tolerantie zijn:
  - Performance: welke reguliere load moet het systeem kunnen verwerken en welke eventuele excessieve loads (zoals bij een DDoS-aanval) moet het systeem aankunnen?
  - Veiligheid: is het systeem weerbaar tegen aanvallen op het systeem zelf en heeft het bijvoorbeeld ingebouwde mechanismen om dit soort aanvallen te detecteren?
  - Fail-secure: loopt de omgeving geen gevaar op op het moment dat het systeem onverhoopt faalt?
  - Redundantie: zijn detectie-oplossingen dubbel uitgerold? Hebben ze een back-up op een externe locatie? Wordt het overschakelen regelmatig getest? Voorkom hiermee dat de detectie-oplossing een “Single Point of Failure” wordt.

- **Bepaal de vereiste mate van omgevingsbewustzijn (context awareness).** Bij het alerteren over en blokkeren van een mogelijk beveiligingsprobleem, is de context van een dergelijk probleem van groot belang. Detecteert een IDS bijvoorbeeld een Windows-exploit richting een Linux-machine, dan is het probleem veel minder urgent dan wanneer dezelfde exploit wordt afgevuurd op een (mogelijk kwetsbare) Windows-machine. Een IDS dat zich bewust is van dit feit, kan de urgentie van alerts hierop afstemmen. Dit bewustzijn rondom de context valt uiteen in diverse gebieden. Tabel 6 beschrijft enkele veel voorkomende gebieden waarop een IDPS bewustzijn kan opbouwen.

| Awareness | Omschrijving |
|---|---|
| Applicatie | Bewustzijn rondom de applicatie (de software) die het verkeer heeft geïnitieerd of die het verkeer zal ontvangen. Zo kan bewustzijn van het gebruik van Adobe Coldfusion op een webserver bijvoorbeeld helpen bij het duiden van aanvallen op poort 80 (http). |
| Identiteit/ gebruiker | Identiteit kan een belangrijke rol spelen bij detectie en preventie. Een aanval op een medewerker die toegang heeft tot veel gevoelige informatie (bijvoorbeeld de CEO) kan bijvoorbeeld een stuk ernstiger zijn dan een aanval op een medewerker die dit soort autorisaties niet heeft. Daarnaast kan het vaststellen van een gebruiker helpen bij anomalie-detectie (wat is bijvoorbeeld afwijkend netwerkgedrag bij een specifieke gebruiker?). |
| Locatie | De locatie van een gebruiker is bijvoorbeeld van groot belang bij een wireless IDPS. |
| Inhoud | Door niet alleen puur naar metadata te kijken, kan gerichter worden gedetecteerd. Zo is er bij TCP-verkeer over poort 80 (metadata) meestal sprake van HTTP-verkeer, maar het kan bijvoorbeeld ook gaan om IRC-verkeer vermomd als HTTP-verkeer. |

*Tabel 6 - IDPS & awareness*

- **Bepaal de sourcing-strategie**. Dit whitepaper gaat er voor een groot gedeelte vanuit dat de organisatie zelf een detectie-oplossing inricht en onderhoudt. Het is echter ook mogelijk dat de organisatie ervoor kiest om de gehele detectie of onderdelen daarvan niet zelf te exploiteren maar dit uit te besteden aan een derde partij. In een vroeg stadium moet de organisatie daarom bepalen welke activiteiten zij zelf zal uitvoeren en welke zaken bij een derde partij worden belegd. Een aantal aandachtspunten is van groot belang bij de keuze voor outsourcing van detectie en het opstellen van requirements hieromtrent:
  - bepaal welke informatie wel en welke informatie niet bij de outsourcer terecht mag komen;
  - bepaal welke activiteiten, op basis van intern beleid, bij een derde partij belegd mogen worden;
  - bepaal welke risico's de organisatie introduceert bij het uitbesteden van detectieactiviteiten;
  - zorg voor een goede relatie met de outsourcer (is er een klik?);
  - besteed aandacht aan referenties en reputatie van een outsourcer;
  - kijk of een outsourcer aan informatiebeveiligingsnormen voldoet en daarvoor gecertificeerd is (PCI-DSS compliancy wanneer het gaat om PAN nummer verwerking, NEN7510 compliancy in de zorgsector, etc.);
  - besteed aandacht aan een goed, volledig en gestructureerd contract;
  - zorg ervoor dat interne kennis m.b.t. detectie en monitoring behouden blijft; en
  - zorg dat er geen belangenverstrengeling kan optreden.

Bij het opstellen van het ontwerp zijn de volgende zaken van belang:

- **Bepaal het gewenste type detectie-oplossing**. Wanneer men detectie-oplossingen gaat aanschaffen of open source varianten wil implementeren, dan wordt aangeraden dat de organisatie een scope bepaalt:
  - Op welke devices moeten de tools kunnen werken?
  - Welke devices, zoals servers en netwerk componenten, moeten de tools kunnen monitoren?
  - Wat voor soort data wordt er gemonitord? Gerubriceerde informatie etc.?

Daarnaast wordt aangeraden dat de organisatie requirements opstelt waar de tools op van toepassing zijn en wat zij moeten kunnen. Bijvoorbeeld:

- Hoeveel logopslag heb ik nodig?
- Hoeveel retentietijd heb ik nodig?
- Is real-time analysis mogelijk?
- Is trend analyse mogelijk?
- Is threat correlatie mogelijk?
- Is incident reporting mogelijk?
- Kan er een koppeling gemaakt worden met andere systemen zoals bijvoorbeeld ticketingsystemen? Hiermee wordt voorkomen dat incidenten niet worden afgehandeld.
- Etcetera.

- **Bepaal hoe de verschillende onderdelen van de detectie-oplossing ingepast moeten worden**. De detectie-oplossing zal ongetwijfeld aanpassingen aan de bestaande infrastructuur vereisen. Het is dus van belang te bepalen hoe de verschillende onderdelen van deze detectie-oplossing ingepast kunnen worden in de bestaande infrastructuur waarbij aandacht wordt besteed aan zaken als:
  - de manier van aansluiten van sensoren (bijvoorbeeld via een SPAN-aansluiting of een tap);
  - de vereiste communicatie tussen systemen;
  - de integratie met bestaande detectie-oplossingen (bijvoorbeeld het aansluiten van een IDPS op een reeds aanwezige SIEM-oplossing); en
  - de plaats binnen de infrastructuur.

Met betrekking tot de plaats binnen de infrastructuur is een aantal eigenschappen van belang. Een netwerk bestaat veelal uit diverse compartimenten zoals het client-LAN, het server-LAN en de Demilitarized Zones (DMZ), firewall clusters, etc. De organisatie zal moeten bepalen op welke plekken en op welke systemen een IDPS vereist is. Een aanpak die men hierbij kan hanteren is het bepalen van een aantal typische routes die aanvallers zouden kunnen nemen om tot de meest waardevolle informatie van de organisatie door te dringen[8]. Nadat deze routes in kaart zijn gebracht (de "*attack graph*"), ontstaat een beeld van de plekken binnen de infrastructuur waar deze routes samenkomen en waar logischerwijs een sensor geplaatst zou moeten worden. Het doel is daarbij om het aantal sensoren te minimaliseren en de ingezette sensoren zo effectief mogelijk te benutten.

Naast het zo efficiënt mogelijk inzetten van sensoren moet een organisatie ook stilstaan bij de bruikbaarheid van alerts die deze sensoren genereren. Stel bijvoorbeeld dat een IDPS het netwerkverkeer tussen een proxy server en het internet monitort. In dit geval zal een alert, bij het detecteren van een mogelijk beveiligingsprobleem, alleen het IP-adres van de proxyserver tonen. Om erachter te komen welk systeem het betreffende verzoek heeft gedaan, is dan informatie van de proxyserver zelf vereist. In dit geval is het dus van belang om een koppeling met de proxy-logging tot stand te brengen of de netwerkdetectie te verplaatsen naar de andere kant van de proxy.

Grofweg gezien bestaat een netwerk van een organisatie uit een buitenkant (de koppeling van het netwerk aan het internet of een ander extern netwerk) en een binnenkant. De keuze om een IDPS aan de binnen- en/of buitenkant van een netwerk te plaatsen brengt een aantal consequenties en adviezen met zich mee. Zo is het advies bij een nieuwe IDPS-oplossing altijd te starten op een plek aan de binnenkant van het netwerk omdat daar de hoeveelheid dreigingen beperkt is. Daarnaast bepaalt de locatie de breedte van dreigingen waarop gemonitord kan worden, hoe eenvoudig het duiden van alerts is, hoe zichtbaar beveiligingsproblemen daar zijn en hoe efficiënt en effectief het inzetten van een IDPS is. Tabel 7 beschrijft deze eigenschappen in meer detail.

[8] Zie bijvoorbeeld http://csis.gmu.edu/noel/pubs/2008_JNSM.pdf (Steven Noel, Sushil Jajodia, "Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs," Journal of Network and Systems Management)

| Eigenschap | Buitenkant | Binnenkant |
|---|---|---|
| Fase binnen IDPS-traject | Inrichten nadat kennis en ervaring met het IDPS is opgedaan aan de binnenkant van het netwerk. Voornamelijk door de grote stroom aan ongefilterde inputs die het systeem te verwerken zal krijgen. | Aan de start van een IDPS-traject vanwege afbakening en filtering van inputs. |
| Breedte | Gericht op een breed scala aan dreigingen. | Gericht op dreigingen die relevant zijn voor de binnenkant van het netwerk. |
| Filtering | Veel van de inkomende verbindingen worden mogelijk nog geblokkeerd door firewalls en andere beveiligingsoplossingen. Inkomende verbindingen zijn ongefilterd. | De inkomende verbindingen zijn reeds gefilterd en zullen uiteindelijk succesvol zijn. |
| | Uitgaande verbindingen zijn reeds gefilterd en zullen uiteindelijk succesvol zijn. | Veel van de uitgaande verbindingen worden mogelijk nog geblokkeerd door firewalls en andere beveiligingsoplossingen. Uitgaande verbindingen zijn (deels) ongefilterd. |
| Duiding | Duiding is vaak lastig: het succes van de aanval is niet altijd bekend en correlatie van alertinformatie met interne logging e.d. is vaak vereist voor duiding. | Duiding is eenvoudiger: doordat filtering voor een deel al heeft plaatsgevonden |
| Zichtbaarheid | Door filtering van uitgaande verbindingen blijven infecties binnen het netwerk mogelijk onopgemerkt. | Infecties van systemen kunnen worden opgemerkt, ook als de uiteindelijke communicatie met bijvoorbeeld een C2 mislukt door filtering. |
| | Hackpogingen van interne medewerkers op interne systemen blijven mogelijk onopgemerkt | Hackpogingen van interne medewerkers op interne systemen kunnen worden opgemerkt. |
| Efficiëntie | Diverse interne onderdelen van het netwerk komen vaak samen aan de buitenkant van het netwerk. Hierdoor kan één IDPS detectie uitvoeren op acties vanuit meerdere interne netwerken. | Interne onderdelen van het netwerk zijn mogelijk gecompartimenteerd waardoor voor elk intern netwerk apart een IDPS-oplossing moet worden ingericht. |
| Effectiviteit | De wijze van detectie bepaalt of een bepaalde plek in de infrastructuur waardevol voor een IDPS kan zijn. Stel bijvoorbeeld dat een oplossing op basis van DNS-verzoeken bepaalt of een netwerkpakket mogelijke malafide is. De resultaten hiervan kunnen zeer verschillen, afhankelijk van de plek in de infrastructuur waar men deze detectie-oplossing plaatst: | |
| | DNS-verzoeken richting externe resolvers worden zichtbaar. Verzoeken zijn niet direct te relateren aan het bronsysteem: de interne DNS-server is immers altijd de bron van het verzoek. Daarnaast ziet het IDPS op deze plek niet alle DNS-verzoeken die konden worden beantwoord op basis van de cache van de interne DNS-server. | Alle DNS-verzoeken worden zichtbaar, ook DNS-verzoeken aan interne resolvers en DNS-verzoeken die beantwoord werden op basis van een cache. Verzoeken zijn veelal direct te relateren aan een bron. |

*Tabel 7 - buiten- en binnenkant*

- **Bepaal de vereiste aanpassingen of uitbreidingen aan bestaande systemen**. Zodra in kaart is gebracht welke afhankelijkheden er zijn vanuit de detectie-oplossingen, moet er ook vanuit de bestaande systemen gedacht worden. Zijn er aanpassingen nodig vanuit bestaande applicaties om bijvoorbeeld logs door te sturen?

- **Bepaal de impact die implementatie van de detectie-oplossing heeft**. De introductie van de oplossing zal consequenties hebben voor de bestaande infrastructuur waarmee rekening zal moeten worden gehouden. Zo zal het aanmaken van een SPAN-poort op een switch betekenen dat dit systeem zwaarder wordt belast en mogelijk een performance bottleneck ontstaat. Kiest men voor een inline oplossing, dan kan dat betekenen dat een Single Point of Failure (SPOF) ontstaat. Het is belangrijk deze risico's te onderkennen en hier óf mitigerende tegenmaatregelen voor te treffen óf deze expliciet te accepteren.

- **Bepaal welke informatie vereist is om opvolging te kunnen geven aan een alert**. Bij het reageren op een incidentmelding wil de incident handler beschikken over zoveel mogelijk informatie om het incident goed te kunnen analyseren. Uiteraard is het vrijwel ondoenlijk (en onwenselijk) om elke activiteit binnen de infrastructuur tot in detail vast te leggen. Daarom moet vastgesteld worden welke informatie in ieder geval beschikbaar moet zijn om goed te kunnen reageren op een incident.

> ***Voorbeeld***
> Bij een IDS is het mogelijk om ruwe informatie rondom een alert vast te leggen. Daarbij kan ervoor gekozen worden om alleen het netwerkpakket dat een alert genereert op te slaan of ook meerdere pakketten daarom heen en om alleen metadata op te slaan of meer dan dat. Voor incident respons is het belangrijk dat het IDS in ieder geval de packet header van een "alertpakket" vastlegt, maar liefst ook de payload ervan.

## 4.2 Monitoring / implementatie

### 4.2.1 Algemeen

- **Weet hoe de infrastructuur eruit ziet en hoe het zich gedraagt**. Het beter kijken naar de infrastructuur door monitoring, betekent ook dat men meer gaat zien. Wanneer de beheerders binnen de organisatie al niet op voorhand een beter beeld hebben ontwikkeld van de infrastructuur, kan dit betekenen dat deze beheerders geconfronteerd worden met allerlei meldingen die zij moeilijk kunnen duiden. Daarom is het van belang dat betrokkenen al tijdens de implementatiefase zorgen voor een verbeterd inzicht in de infrastructuur waarbij zij antwoorden proberen te zoeken op vragen als welke informatiestromen bestaan er, welke applicaties gebruiken we en welke protocollen passen deze applicaties toe?

Kiest een organisatie ervoor om monitoring in te richten op basis van anomalieën, is deze stap extra belangrijk. Om een afwijking (anomalie) te kunnen ontdekken is het immers van belang om eerst vastgesteld te hebben wat dan normaal gedrag is.

### 4.2.2 Logging

Een essentieel middel om monitoring in te kunnen richten en opvolging te kunnen geven aan alerts die voortkomen uit monitoring, is goede logging. Zeker bij de implementatie van een SIEM, is logging essentieel, maar ook bij de implementatie van een IDS of IPS is logging belangrijk om alerts op te kunnen volgen. Onderdeel van het implementatietraject moet dan ook het inrichten of aanpassen van logging op bestaande systemen zijn. Hierbij zijn de onderstaande zaken van belang:

- **Valideer de instellingen op elk systeem**. Bekijk hierbij de instellingen van elk systeem en de software daarop om te garanderen dat de logs compleet zijn. Systemen maken daarbij liefst gebruik van een gestandaardiseerd formaat zoals SYSLOG. Ondersteunt het systeem geen standaard formaat, dan is normalisatie hiervan door bijvoorbeeld een SIEM een vereiste.

- **Richt beveiliging van de logging goed in.** Logging is waardevolle informatie voor een aanvaller. Niet alleen de informate in de logging zelf is interessant voor een aanvaller, ook manieren om logging te doen verdwijnen zijn voor een aanvaller van groot nut omdat de aanvaller zijn sporen hiermee kan uitwissen. Daarom is aandacht voor beveiliging van logging van groot belang. Dit betekent in ieder geval dat de volgende zaken tijdens de implementatiefase de aandacht krijgen:
  - Hoewel logging op een systeem zelf vaak niet eenvoudig is in te zien door een kwaadwillende, bestaat wel de kans dat een kwaadwillende deze logging ziet doordat deze logging onversleuteld wordt verstuurd naar een ander systeem, bijvoorbeeld het SIEM. Daarom is het van belang te zorgen voor **versleutelde kanalen** waarover logginginformatie wordt uitgewisseld.
  - Zorg dat de logging geen **geclassificeerde gegevens** bevat. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden.

- Beperk de toegang tot de logbestanden zodat **alleen specifieke rollen** deze kunnen inzien (bijvoorbeeld de auditor, SIEM-beheerders en security-analisten) en zorg dat deze toegang beperkt is tot **alleen lezen**.
- **Dwing af dat logbestanden niet kunnen worden aangepast of gemanipuleerd**, door bijvoorbeeld het gebruik van een write-only device of een losstaande loggingservice die draait op een aparte, toepassingsgerichte server.
- **Classificeer** de logging minimaal op het niveau van de informatie waarop deze betrekking heeft.
- Vergeet niet dat een aanvaller ook zijn strategie kan bepalen aan de hand van de wetenschap van wat er **niet** gelogd wordt.

- **Zorg dat minimale informatie aanwezig is in het log**. Om logging in een latere fase bruikbaar te laten zijn, moet deze in ieder geval de volgende informatie bevatten:
  - een tot een natuurlijk persoon herleidbare gebruikersnaam of ID (indien beschikbaar);
  - een systeemnaam of locatie van het systeem (indien beschikbaar);
  - de handeling die heeft plaatsgevonden;
  - het object waarop de handeling heeft plaatsgevonden;
  - het resultaat van de handeling;
  - de datum en het tijdstip van de gebeurtenis; en
  - bron- en doeladres.

***Voorbeelden***
Onderstaande gebeurtenissen zijn typische gebeurtenissen die moeten worden vastgelegd in een log:
- wijzigen van belangrijke instellingen;
- uitvoeren van systeemcommando's;
- starten en stoppen van services,
- uitvoeren van een back-up of restore;
- release van nieuwe functionaliteit;
- ingrepen in gegevenssets (waaronder databases);
- op- en afvoeren van gebruikers;
- toekennen en intrekken van rechten;
- uitgifte en intrekken van cryptosleutels;
- aanwezigheid van malware;
- geweigerde pogingen tot toegang;
- pogingen van smartcardtoegang bij ruimtes die slechts voor enkelen toegankelijk zijn;
- vollopen van queues;
- systeemfouten;
- wijzigingen van tijden van meer dan enkele seconden;
- gebruik van online transacties; en
- toegang tot bestanden door systeembeheerders.

- **Zorg dat systemen een minimale set aan gebeurtenissen loggen**. Niet alleen de hoeveelheid informatie die systemen vastleggen is belangrijk (zie voorgaand punt), maar ook de gebeurtenissen waarvoor dit geldt. Zo moeten logregels bestaan voor technische en functionele beheeracties, beveiligingsbeheer, beveiligingsincidenten, fysieke toegang, handmatige meldingen bij een security officer, verstoringen in een productieproces en handelingen van gebruikers.

- **Privacy.** Stem met de interne stakeholders, de Ondernemingsraad, de Medezeggenschapsraad en betrokkenen af wat er wel en niet gelogd mag worden om de privacy van gebruikers te borgen zonder dat de veiligheid van informatie in het geding komt.

## 4.3 Incident respons/exploitatie

In de exploitatiefase gaat de organisatie daadwerkelijk gebruik maken van de detectie-oplossing. Hoewel de ingerichte oplossing heel veel zaken geautomatiseerd zal uitvoeren, zal het dagelijks beheer ook een inspanning vergen van medewerkers. Dit dagelijks beheer bestaat bijvoorbeeld uit het geven van opvolging aan alerts die het systeem genereert en het troubleshooten van eventuele problemen die zich voordoen. Een reëel gevaar is echter dat het systeem dusdanig veel werk (alerts) genereert dat de beheerders het overzicht verliezen, de belangrijke alerts niet meer kunnen onderscheiden van de minder belangrijke alerts en hierdoor uiteindelijk alsnog een incident plaatsvindt dat aan de aandacht ontsnapt.

Onderstaande best practices kunnen helpen om het succes van het systeem zo groot mogelijk te laten zijn:

- **Begin klein**. Het gevaar bestaat dat men bij de introductie van een detectie-oplossing direct alle mogelijke alerts inschakelt. Hierdoor ontstaat een stortvloed aan alerts die voor de beheerders niet meer te behappen zijn. Het advies is daarom om altijd klein te beginnen; begin met alerts op rules die geprioriteerd zijn op gewenst beleid. Zodra dit resultaten heeft opgeleverd en behapbaar blijkt voor de beheerders, kan men ervoor kiezen om langzaamaan alerts op andere rules in te schakelen.

- **Beperk actief het aantal alerts**. Beheerders zouden niet alleen naar de afzonderlijke alerts moeten kijken, maar ook moeten bekijken welke rules de meeste alerts opleveren. Stel bijvoorbeeld dat een systeem per dag 1.000 alerts genereert, terwijl 750 van deze alerts veroorzaakt blijken te zijn door dezelfde rule. Op zo'n moment is het goed om te bekijken of er sprake is van terechte alerts (true positives) en of de alerts relevant zijn. Wanneer blijkt dat er veel false positives tussen de alerts zitten of de alerts niet relevant zijn, dan kan het uitschakelen van de alert op de rule of aanpassen van de bijbehorende rule een enorme verlichting opleveren voor de beheerders.

- **Heb aandacht voor de beveiliging van de oplossing zelf**. Een IDS of een SIEM bevat zelf veel gevoelige informatie over activiteit die plaatsvindt binnen het netwerk van de organisatie of heeft zelfs toegang tot alle ruwe informatie op het netwerk. Daarmee kan het IDS of de SIEM zelf veranderen in een kroonjuweel voor hackers en het is dan ook van groot belang om deze oplossing zelf goed te beschermen. Dit betekent bijvoorbeeld dat beheerders continu nieuwe updates en patches installeren om te voorkomen dat kwaadwillenden een kwetsbaarheid in het IDS of SIEM misbruiken om hiertoe ongeautoriseerde toegang te verkrijgen.

- Niet alleen de informatie die de monitoringoplossing verzamelt, is vertrouwelijk. In sommige gevallen kan dit ook gelden voor de signatures waarvan de oplossing gebruik maakt omdat ze bijvoorbeeld inzicht geven in modus operandi. Organisaties moeten eventuele processen van informatiedeling daarom zodanig inrichten dat er geen hoog gerubriceerde signatures – of meta-data hiervan – gedeeld kunnen worden tenzij deze compleet geanonimiseerd zijn en geen modus operandi weggeven.

- **Onderhoud de kwaliteit van detectierules**. De kwaliteit van alerts is afhankelijk van de kwaliteit van de rules om deze te genereren. Het is dan ook uitermate belangrijk dat deze rules continu up-to-date worden gehouden en informatie over nieuwe (en relevante) dreigingen en kwetsbaarheden (*threat intelligence*) verwerkt worden in een rule. Indien de organisatie deze rules afneemt van een externe organisatie dan volstaat het om ervoor te zorgen dat het updateproces goed verloopt. Wanneer de organisatie echter (ook) zelf intelligence verzamelt en verwerkt in rules dan moet de organisatie continu investeren in het onderhouden van dit proces. Zo is het actief delen van informatie met derde partijen vaak een voorwaarde om ook zelf weer waardevolle informatie te kunnen ontvangen. Ook het op regelmatige basis deelnemen aan bijeenkomsten is hierbij een inspanning die misschien niet direct tot resultaten leidt, maar op de langere termijn wel randvoorwaardelijk is voor het verkrijgen van goede intelligence.

***Aandachtspunten bij threat intelligence***

- Maak gebruik van threat intelligence deelplatformen zoals diverse ISAC's, CERT-samenwerkingen en MITRE.
- Maak voor het delen van informatie gebruik van bekende standaarden als OpenIOC, STIX, Snort-signatures, etc ...
- Denk goed na welke informatie de organisatie deelt met threat intelligence platformen. Zorg dat gevoelige informatie alleen geanonimiseerd wordt gedeeld met een "trusted circle" of dat het helemaal niet gedeeld wordt.
- Voer altijd een historische zoekactie uit zodra de organisatie nieuwe correlaties maakt of nieuwe intelligence ontvangt. Hierdoor bestaat de kans een eerder onopgemerkte "breach" of aanval alsnog te detecteren.

- **Zorg voor gesynchroniseerde systeemklokken en timestamps**. Systeemklokken van alle (relevante) informatiesystemen moeten zodanig worden gesynchroniseerd tegen eenzelfde tijdsbron zodat altijd een betrouwbare analyse en correlatie van logbestanden mogelijk is. Gebruik hiervoor bijvoorbeeld het Network Time Protocol (NTP) met de nauwkeurigste tijdsbron (stratum 0 of 1). Daarnaast moeten systemen elke alert die plaatsvindt "timestampen" (bijvoorbeeld UTC) met een referentie aan het originele auditlog om forensisch onderzoek te vergemakkelijken.

## 4.4 Incident analyse/evaluatie

Wanneer is een SIEM-implementatie of andere monitoringoplossing geslaagd? Hoe weet een organisatie dat de investering in mens en middelen rendeert in een veiligere netwerkomgeving? Het zijn lastige vragen om te beantwoorden. Waar de ene organisatie erg enthousiast is over hun monitoringoplossing is de ander juist ontevreden en gaat de monitoringactiviteiten juist weer afbouwen. Het gebruik van indicatoren kan helpen bij het meetbaar maken van de effectiviteit van een monitoringimplementatie.

Bij de evaluatie van de werking van de monitoringoplossing zijn de volgende onderwerpen van belang:

- **Controleer of het systeem naar behoren werkt**. Hierbij bekijkt men of de tooling in de basis doet wat het moet doen. Vragen die men zich hierbij zou moeten stellen zijn:
  - Komen er bij de SIEM logs binnen van al de te monitoren systemen en met nadruk de kritieke systemen?
  - Krijgen IDS-sensoren het netwerkverkeer binnen waarop zij moeten monitoren?
  - Kunnen beschikbare logs correct geparsed worden?
  - Kunnen de logs correct gecategoriseerd worden?
  - Krijgen de logs en alerts de juiste timestamps?
  - Is er vanuit de tooling ondersteuning voor verschillende platformen / typen devices?

- **Controleer of het systeem naar behoren presteert**. Hierbij wordt gekeken naar:
  - de algehele verzameltijd qua "uptime";
  - het percentage van de gecachede events;
  - het percentage van de goed geparseerde events;
  - het percentage van de gecategoriseerde events;
  - het percentage van verzamelde events versus verwerkte events;
  - het percentage van events met "tijds" problemen is.

- **Gebruik metrieken om de werking van het systeem te meten**. Door eerst een nulmeting uit te voeren is het mogelijk om daarna te bekijken of de prestaties van het systeem verbeteren naar mate het systeem nauwkeuriger wordt ingeregeld. We kunnen kijken naar de technische prestaties van de tooling zoals:
  - het aantal rules of signatures die het systeem bevat en gebruikt per dag;
  - het aantal alerts per dag
  - het aantal alerts per werktijd en na werktijd;
  - het aantal gelogde events per dag versus het aantal alerts;
  - het aantal gecorreleerde events versus het aantal alerts;
  - het aantal alerts versus false positives; en
  - het aantal gemonitorde systemen versus de hoeveelheid systemen binnen de organisatie.

  Een organisatie kan ook kijken vanuit business perspectief:
  - Wat is de gemiddelde tijd om handelingen te verrichten met betrekking tot een incident na de implementatie van een detectie-oplossing en verschilt dit met de tijd die voor de implementatie van de detectie-oplossing nodig was (of vergeleken bij latere evaluatie momenten)?
  - Het aantal afgehandelde incidenten en vergelijk dit met het aantal afgehandelde incidenten voor de implementatie van een detectie-oplossing (of vergeleken bij latere evaluatiemomenten).
  - Het aantal changes in netwerk of applicatie beveiliging naar aanleiding van events.
  - Discovery window van aanvallen.
  - Mean Time To Repair (MTTR) na een aanval.
  - Het aantal onderzoeken of potentiële incidenten die zijn gestart/geïdentificeerd aan de hand van een detectie-oplossing en verschilt dit met de tijd voor de implementatie van de detectie-oplossing (of vergeleken bij latere evaluatie momenten).
  - De doorlooptijd van het afhandelen van incidenten.

- **Gebruik de eerder gestelde doelen om de effectiviteit van het systeem te meten**.
  - De doelen zoals deze zijn opgesteld in 4.1.1 Voorbereiding kunnen gebruikt worden om te toetsen of de detectie-oplossing zijn werk gedaan heeft en in welke mate de applicatie effectief is. Bijvoorbeeld: als het doel van het systeem is om de impact van Cryptolocker infecties (een ransomware trojan) te verkleinen, kunnen de resultaten waarin zichtbaar is dat er Cryptolocker infecties gedetecteerd en daardoor gestopt zijn of juist niet zijn gedetecteerd en wel systemen hebben geïnfecteerd, worden vergeleken met de infecties voordat de detectie-oplossing geïmplementeerd was.

# Samenvatting

In dit document heeft u een set met handvatten meegekregen om te starten met detectie of om uw huidige detectie-oplossingen te corrigeren of te verbeteren. U heeft inzicht gekregen in het nut en de noodzaak van detectie naast preventie.

Aan de hand van het model is er een onderverdeling gemaakt in:

1. Kennis: visie, inzicht en informatie omtrent kroonjuwelen, risico- en impact analyses, te beschermen belangen.
2. Monitoring: alle benodigde monitoring om incidenten vast te kunnen stellen en te kunnen analyseren.
3. Incident Respons: wat te doen bij een incident om schade te voorkomen of te beperken.
4. Incident Analyse: wat is er gebeurd en hoe kan dit voortaan voorkomen worden.

In hoofdstuk 3 is er een technisch beeld geschetst over detectie-oplossingen zoals Intrusion Detection, Intrusion Prevention en Security Information and Event Management systemen en is er in detail uitgelegd wat de diverse detectie-oplossingen inhouden en hoe deze ingezet kunnen worden.

Het document eindigt met een set best practises om de werking van een geïmplementeerde detectie-oplossingen te testen.

Het is van belang om te allen tijde de samenhang te zien met al geïmplementeerde maatregelen, maar ook de “business” mee te nemen. IT-middelen en de beveiliging van deze IT-middelen zijn immers een middel ter ondersteuning van de operationele werkzaamheden van een organisatie.

Met deze whitepaper ondersteunen het NCSC, als onderdeel van de NCTV, en het NBV, als onderdeel van de AIVD, diverse bedrijven en instanties om aan de slag te gaan met detectie.

# Definities

### APT – Advanced Persistent Threat
Bij een dreiging van een APT wordt er vanuit gegaan dat deze dreigingsactor beschikt over een specifiek doel, bovengemiddelde hoeveelheid geld, uitgebreide en/of unieke kennis en technische middelen. Bij de bovenstaande punten kan gedacht worden aan de in de BIR uitgesloten groepen zoals Inlichtingendiensten, georganiseerde criminaliteit en terreurgroepen.

### Detectie en Monitoring
Fase na preventie waarin tools zoals SIEM en IDS'en binnengedrongen aanvallers kunnen detecteren en een alert afgeven. Deze alerts kunnen real-time worden afgehandeld of een indicator zijn voor verder forensisch onderzoek.

### SIEM – Security Information and Event Management
Een applicatie die logs verzameld waarna een analyse uitgevoerd kan worden op basis van vooraf ingestelde en ad-hoc "regels". De tool wordt vervolgens ingezet om logs uit diverse systemen met elkaar te correleren zodat aan de hand daarvan aanvallen herkend kunnen worden. De tool geeft de resultaten hiervan weer in rapportages en dashboards welke voor compliancy doeleinden gebruikt kunnen worden.

### NB-IDS / NIDS – Network Based Intrusion Detection System
Software die gebruikt wordt om via datastromen van netwerkverkeer ongewenst bezoek aan computer-netwerken te detecteren op basis van Signatures .

### HB-IDS / HIDS – Host Based Intrusion Detection System
Software agents die gebruikt worden om ongewenst bezoek aan end-points zoals computers, tablets, servers, etc. te detecteren op basis van Signatures.

### IPS – Intrusion Prevention System
Software gebruikt in combinatie met een IDS, om op basis van de gedetecteerde inbraak een bepaalde actie te ondernemen zoals het blokkeren van het verkeer, sturen van een alert, resetten van de verbinding etc

### Signatures
Patronen en indicatoren van een aanval zoals gebruikte poorten, protocollen, IP adressen en gebruikte boodschappen. Deze zijn statisch van aard.

### Anomaly Detection
Aanvallen herkennen op basis van afwijkend gedrag. Hiervoor moet allereerst normaal gedrag in kaart worden gebracht en vervolgens bekend slecht gedrag toegevoegd worden. Deze werkwijze is dynamisch van aard.

### Threat Prevention / Malware detection tools
Software om malware (virussen, trojans, worms, exploitkits etc.) te detecteren en te stoppen.

### Pentesting / Penetratietesten / Ethical hacking / Vulnerability assessments
Penetratie testen waarbij systemen "gehacked" worden door interne of ingehuurde professionals om te kijken of er nog zwakheden in de systemen zitten.

### Redteaming (vs. Blueteaming)
Interne pentest oefeningen waarbij een groep pentesters tegen een groep beheerders "hacken" om te kijken of zij doorbreken of dat de beheerders de aanvallers opmerken. De gebruikte technieken kunnen als anomaly patroon worden verwerkt in een SIEM om een dergelijke aanval in de toekomst te herkennen.

### Honeypot
Gesimuleerde digitale omgeving om hackers van buitenaf te lokken waardoor een organisatie hun gedrag kan analyseren en dit kan verwerken als gedragspatroon in een SIEM of voor andere research doeleinden.

**Colofon**

**Ministerie van Binnenlandse Zaken en Koninkrijksrelaties**
Algemene Inlichtingen- en Veiligheidsdienst
www.aivd.nl

Postbus 20010, 2500 EA Den Haag

**Ministerie van Veiligheid en Justitie**
Nationaal Cyber Security Centrum
www.ncsc.nl

Postbus 117, 2501 CC Den Haag

Oktober 2015