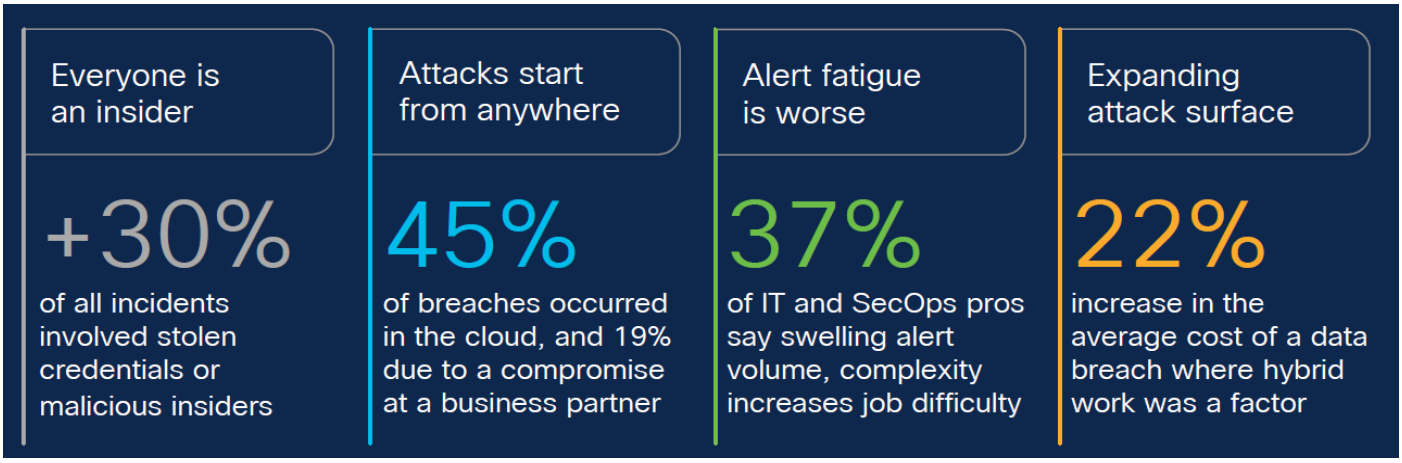
aaZoo B.V.
Duit 1
8305 BB Emmeloord

088 12 62 400
www.aazoo.nl
info@aazoo.nl

Uitdagingen

De wedloop is in volle gang. Cybercrime voert binnen ons bestaan een cruciale rol.
De vraag is niet of maar wanneer je als organisatie slachtoffer gaat worden. Security-risico's worden groter en de benodigde ICT-infrastructuur voor beveiliging wordt hierdoor complexer.
Uitval van kritische processen kunnen we ons niet meer permitteren en de schade is niet meer te overzien als dit gebeurt. In een hybride, multi-vendor, multi-vector omgeving geldt:



Tactieken, Technieken en Procedures (TTP's) die ooit bedoelt en ingezet zijn tegen overheden van vele landen worden nu gebruikt door dagelijkse aanvallers! Om de bedreigingen van morgen aan te kunnen, moeten we vandaag de opsporing en detectie veranderen.

Een gedegen voorbereiding en de juiste preventieve maatregelen vormen de beste strategie voor continuïteit en een veilige omgeving. Voor het vaststellen hoe groot de kans is op een cyberincident in jouw organisatie stelt de Overheid een risicoklasse tool ter beschikking. Deze test is er ook voor industriële controlesystemen (ICS) of operationele techniek (OT).

Om te kijken of de juiste preventieve maatregelen genomen zijn, worden securitytesten ingezet. Als lid van CyberveiligNederland voeren wij regelmatig dit soort testen/scans uit. Om ervoor te zorgen dat de uitkomsten van een test de juiste inzichten geven, is het handig om uw behoeften vooraf helder te formuleren. Een hulp hierbij biedt het volgende overzicht/stroomschema

De kennis om netwerk veiligheid te borgen is inmiddels zeer specialistisch geworden. Je kunt niet meer volstaan met een enkele veiligheidsmaatregel maar zult een bewezen methodiek toe moeten passen om te komen tot een juiste ICT-architectuur. Door het toepassen van de Zero Trust methodiek is de data veilig en kunnen gebruikers veilig en vertrouwt toegang krijgen via het netwerk tot deze data. Hiervoor zijn een 5-tal stappen nodig om alle systemen op een juist beveiligingsniveau te brengen die passend is bij een organisatie, zijnde: (1) Verkrijg inzicht, (2) Segmenteren, (3) Context, (4) Endpoints en (5) Combineer en Automatiseer. Meer uitleg via ons Webinar: In 5 praktische stappen naar een Zero Trust strategie.

aaZoo B.V.
Duit 1
8305 BB Emmeloord

088 12 62 400
www.aazoo.nl
info@aazoo.nl

Deze laatste stap – Combineer en Automatiseer - is een belangrijke stap, want door correlatie ontstaat er een geïntegreerde beveiligingsoplossing. Want wie zorgt er voor het inzicht van de veelheid aan loginformatie uit al die oplossingen? En wellicht is er met de loginformatie uit oplossing A wel een samenhang met de loginformatie uit oplossing B?

De integratie van Security-oplossingen is cruciaal en vereist continue monitoring om het maximale effect te bereiken. Dit monitoren is een complexe en specialistisch werk welke vaak niet past of tijd beschikbaar voor is binnen de al drukke werkzaamheden van een ICT-team.

Security Monitoring is het meest effectief wanneer speciaal ingerichte systemen samen met de aaZoo-professionals de gegenereerde gegevens analyseren en de eerste beoordeling uitvoeren. Dit levert input die de risico's op incidenten aanzienlijk vermindert en snelle detectie, respons en grondige preventie mogelijk maakt. Zowel Cisco en Meraki oplossingen zijn geïntegreerd in deze dienstverlening. Maar ook andere security oplossingen zoals Microsoft Defender en vele (Cloud)applicaties zijn te integreren in deze dienstverlening.

Wat zegt Gartner

Bron -> (Emerging Tech:Security – Adoption Growth Insight for Extended Detection and Response (14 April 2023)

De toename van het volume van cyberdreigingen stimuleert de vraag naar snellere, effectievere detectie- en responsoplossingen. De wereldwijde belangstelling voor XDR groeit snel, maar de mate van acceptatie is verdeeld en voornamelijk afhankelijk van de huidige bestaande implementatieniveaus van detectie- en responstechnologieën.

Er bestaat een opkomende markt binnen XDR nu de acceptatie meer verschuift naar kleinere organisaties die vanwege een tekort aan interne middelen (mensen, kennis e.d.) op zoek zijn naar MDR-providers en MSSP's om de operationele vaardigheden te leveren die ze nodig hebben.

Niet-technische kopers worden actievere deelnemers aan cyberbeveiliging beslissingen, waardoor het belangrijker dan ooit is om te benadrukken met voorbeelden die laten zien hoe de implementatie van XDR-oplossingen kan leiden tot succesvollere algemene bedrijfsresultaten.

Interesse in XDR is wijdverspreid in de meeste branches, maar de acceptatie is meer geconcentreerd onder bedrijven die in het verleden geen andere tooling hiervoor ingezet hebben.

Beschrijving van de basistechnologie
Uitgebreide detectie en respons (XDR) levert uniforme detectie van beveiligingsincidenten en respons mogelijkheden. XDR integreert log, bedreigingsinformatie en telemetriegegevens van meerdere bronnen met beveiligingsanalyses om contextualisering en correlatie te bieden voor security waarschuwingen. XDR moet native sensoren bevatten waarvan er één zich op het eindpunt bevindt. Ook vereist zijn automatisering, triage en uniforme responsmogelijkheden voor het waarschuwen van incidenten. XDR kan on-premises of als een cloudaanbod worden geleverd.

aaZoo B.V.
Duit 1
8305 BB Emmeloord

088 12 62 400
www.aazoo.nl
info@aazoo.nl

Primaire functies van XDR zijn onder meer:

- Centralisatie en normalisatie van telemetriegegevens van security gebeurtenissen in een cloud opslagplaats voor analyse
- Integratie van security waarschuwingen, security telemetrie en bedreigings-informatie in geprioriteerde incidenten voor onderzoek
- Verbeterde bescherming en detectie- en reactie-efficiëntie als gevolg van een geconvergeerde oplossing met vereenvoudigde configuratie en security product coördinatie
- De mogelijkheid om de status van individuele security producten aan te passen voor reactie en hersteldoeleinden

XDR is een snel evoluerende markt en zal naar verwachting op de korte termijn een aanzienlijke impact hebben op de security operaties met name bij organisaties met een lagere volwassenheid. Geïntegreerde dreigingsdetectie- en responsmogelijkheden waren voorheen alleen mogelijk met aanzienlijk meer resources (tools, budget e.d.) voor met name geavanceerde organisaties.

Hoe ziet een XDR oplossing eruit

eXtended Detection and Response (XDR) is een nieuwe beveiligingsoplossing die de nadelen van SIEM-oplossingen oplost. XDR biedt een praktische aanpak waarmee organisaties snel solide beveiliging kunnen implementeren door informatie uit meerdere bronnen te combineren. Een aantal voordelen van XDR-oplossingen:

- Voegen context toe aan de gegevens door een gedetailleerd beeld te geven van de aanvalsvector, de identiteit van de aanvaller en de impact van de aanval. Dit geeft beveiligingsteams de informatie die ze nodig hebben om snel en effectief op bedreigingen te reageren.
- Zijn beter in staat om bedreigingen te detecteren door middel van uitgebreide correlatie-mogelijkheden. Dit stelt beveiligingsteams in staat om snel afwijkingen te identificeren, zelfs als deze zich over meerdere bronnen verspreiden.
- Eenvoudiger te implementeren en gemakkelijker te gebruiken, wat ze ook voor kleine en middelgrote ondernemingen toegankelijk maakt. Dit leidt tot een betere ROI en snellere time-to-value voor organisaties.

Bovendien is een belangrijk aspect van XDR de mogelijkheid van automatische remediatie, zoals bijvoorbeeld het automatisch isoleren van endpoints. XDR stelt beveiligingsteams in staat om snel en automatisch te reageren op bedreigingen, waardoor de aanval wordt gestopt en de schade tot een minimum wordt beperkt.

De XDR-oplossingen verschillen per technologie leverancier/provider zeer sterk. Een effectieve XDR-oplossing verzamelt een collectie van security logging van bv. Endpoints, Netwerk, Email, Cloud, Identity, Firewall enz. Dit wordt verwerkt in drie stappen:

1. Analyse & Correlatie – Threat intel

2. Gestroomlijnd onderzoek – Devices & gebruikers context
3. Automate & Response - MITRE

Het implementeren en onderhouden van een SIEM-oplossing is voor veel organisaties een uitdaging vanwege de hoge kosten en de complexiteit van de ontwikkeling en het onderhoud van aangepaste regels en scripts. XDR biedt een praktische oplossing die de nadelen van SIEM-oplossingen oplost door informatie uit meerdere bronnen te combineren en tegelijkertijd robuuste beveiliging te bieden. Door EDR, NDR en MFA-logs te combineren, biedt XDR een diepgaand inzicht in de beveiligingsgebeurtenissen binnen uw organisatie.

XDR is niet bedoeld als een drop-in vervanging voor SIEM, omdat SIEM meer flexibiliteit en configureerbaarheid biedt, maar XDR stelt organisaties in staat om snellere resultaten te behalen. XDR heeft zichzelf bewezen als een praktische oplossing voor organisaties die snel en effectief willen reageren op beveiligingsdreigingen en strenge compliance vereisen. Bovendien biedt XDR de mogelijkheid van automatische remediatie, waardoor de aanval snel wordt gestopt en de schade wordt beperkt.

Dienstverlening met XDR

aaZoo maakt gebruik van een XDR platform om de Secure Operations dienstverlening aan onze klanten aan te bieden. Het doel hiervan is om de Digitale Weerbaarheid van de klant te versterken.

Deze dienstverlening zorgt voor meer detectie, sneller handelen, het verhogen van de productiviteit en een snel aanpassingsvermogen.

In het XDR platform wordt gebruik gemaakt van Talos - het Cisco Security Expertisecenter - Threat Intelligence en 3th party Threat Intelligence. Daarnaast verzamelt aaZoo zelf ook Threat Intelligence door het hosten van Honeypots, via detecties bij bestaande klanten en van derde partijen zoals Unit 42 en zijn wij lid van Cyberveilig Nederland.

Binnen dit verband is er een samenwerking opgezet met het NCSC om kennisdeling toe te passen en gebruik te maken van de OKTT status om via het MISP platform van het NCSC 24x7 operationele informatie uit te wisselen zoals Indicators of Compromise (IoC's) van actuele aanvallen. Er worden rules gebruikt om detectie te doen op basis van IoC's. Het is voor aaZoo belangrijk om actief mee te werken aan het verzamelen, ontdubbelen en aanbieden van Threat Intelligence door middel van IoC's. Hiermee onderscheiden wij ons van vele andere partijen ten gunste van onze klanten!

Alle IoC's worden verwerkt en ontdubbeld op een geautomatiseerde manier (door het inzetten van de producten MISP en Minemeld) en vervolgens als feeds aangeboden. Deze feeds gebruiken we voor detecties binnen het XDR platform en worden daarnaast als blocklist aangeboden in de managed firewalls van onze klanten.

Tijdens de Log4j uitbraak in December 2021 waren wij hierdoor snel in staat om scan en exploitatie pogingen bij onze klanten tegen te gaan. Uiteindelijk wordt al deze Threat Intelligence verwerkt in het Cisco XDR platform.

aaZoo B.V.
Duit 1
8305 BB Emmeloord

088 12 62 400
www.aazoo.nl
info@aazoo.nl

Het SOC (Security Operating Center) binnen aaZoo is de plek waar de meldingen binnenkomen en er, waar nodig, verder onderzoek of benodigde actie worden genomen.

Voordelen

- ✓ Verhoogt de digitale weerbaarheid
- ✓ Vermindert de gemiddelde tijd tot identificatie van het probleem
- ✓ Threat Intelligence op basis van Indicators of Compromise
- ✓ Monitoren, kwalificeren en analyseren 24/7 van externe en interne dreigingen.
- ✓ Detectie en communicatie van incidenten 8/5 of 24/7
- ✓ Eenvoudig te combineren met andere Cisco Security oplossingen
- ✓ Te integreren met vele 3th party Security oplossingen
- ✓ Zeer uitvoerige rapportage
- ✓ Gecertificeerde specialisten
- ✓ Ondersteuning bij incidenten op basis van consultancy (strippenkaart)
- ✓ Snelle implementatie mogelijk

Het XDR platform koppelt alle informatie aan elkaar en verstrekt met de onderliggende bedreigingsinformatie van Cisco Talos en aaZoo voor verrijking van de incidenten met extra context en actieve inzichten. Het vermindert 'false positives' en vergroot de dreiging detectie en respons door duidelijke prioritiseren van waarschuwingen en het bieden van de kortste weg van detectie naar respons.

Met een focus op het verhelpen van de meest kritieke incidenten met behulp van op bewijzen gebaseerde automatisering, presenteert het XDR platform in combinatie met aaZoo een nieuwe aanpak die de traditionele benadering overstijgt en gericht is op eindpuntdetectie en reactie (EDR).

Het verlegt de focus van ons SOC-team om sneller te komen tot resultaten zoals het eerder aanpakken van bedreigingen, prioriteit te geven aan bedreigingen op basis van impact, onderzoek te bespoedigen en de respons te versnellen. Dit stelt ons SOC-team in staat om efficiënter te handelen, met vertrouwen en snelheid, zonder vast te lopen in eindeloos onderzoek.

Binnen de Secure Operations dienstverlening van aaZoo zijn meerdere mogelijkheden aan opties te kiezen om een juiste aansluiting bij onze klanten te voorzien. Zelfs met Third Party Integrations

Verder natuurlijk de gebruikelijke vorm van dienstverlening zoals onze Ondersteuning (helpdesk), Monitoring, Beheer en Incident Response (samenwerking met Invictus) .

aaZoo B.V.
Duit 1
8305 BB Emmeloord

088 12 62 400
www.aazoo.nl
info@aazoo.nl

aaZoo

aaZoo is sinds 2010 actief als een onafhankelijke ICT kennisorganisatie. Ons bedrijf heeft zich door de jaren heen ontwikkeld om de complexe materie op het gebied van Netwerk- en Securitydienstverlening te begrijpen en als gevolg hiervan is de specifieke kennis over ontwerp, implementatie en het operationeel en veilig houden van Netwerk- en Security omgevingen in ruime mate bij onze - veelal gecertificeerde – professionals aanwezig.

Door ons continue te verdiepen in het samenwerken met onze klanten, de dagelijkse en toekomstige uitdagingen, nieuwe beschikbare technieken en het verder uitbouwen van onze kennis, groeien we als organisatie.

Niet voor niets is gekozen voor een nauwe samenwerking met technologiepartners als Cisco en Meraki welke een leidende marktpositie hebben, de juiste oplossingen voor onze klanten en het overbrengen van kennis net zo belangrijk vinden als wij.

aaZoo heeft een aantal certificeringen, te weten:

ISO 9001 kwaliteitsmanagementsysteem uitgegeven door Kiwa (geldig tot 15 nov 2024)

ISO/IEC 27001:2022 managementsysteem voor informatiebeveiliging en de toepassing daarvan uitgegeven door Kiwa (geldig tot 1 jan 2027) inclusief de verklaring van toepasselijkheid.

aaZoo is sinds februari 2020 Cisco Advanced Security Partner! Hiermee zijn wij een van de 14 Nederlandse dienstverleners met deze status.

Verder zijn wij actief lid van Cyberveilig Nederland en maken gebruik van de OKTT status om informatie over IoC's te delen met het NCSC via het MISP platform van het NCSC om geautomatiseerd IoC's uit te kunnen wisselen.

Daarnaast verzamelt aaZoo Threat Intelligence door het hosten van Honeypots en door detecties bij klanten te verwerken in een centraal systeem.

aaZoo voert al jaren Netwerk- en Security dienstverlening uit bij verschillende klanten in uiteenlopende branches in geheel Nederland en zelfs daarbuiten. Verder ondersteunen wij ICT-werkplek partners welke deze specifieke kennis en ervaring niet of nauwelijks in huis hebben.