De volgende stap voor EDR
Managed Traps en Cortex XDR-as-a-Service

Managed Traps en Cortex XDR staan garant voor de meest geavanceerde endpointdetectie, inclusief integratie met het netwerk en de cloud. We bieden deze geïntegreerde oplossing aan voor een vast bedrag per maand.

De uitdaging: Het beheer van EDR-oplossingen (Endpoint Detection and Response) is voor veel organisaties te complex en te duur om intern goed te kunnen regelen.

Aanvallers moeten een bepaalde reeks gebeurtenissen – de zogenaamde aanvalscyclus – doorlopen om in hun opzet te slagen, of het nu gaat om het stelen van informatie of het uitvoeren van ransomware. Vrijwel elke aanval begint met een actie die is gericht op een endpoint, en hoewel de meeste organisaties endpointprotectie hebben geïmplementeerd, komen infecties met malware en exploits nog regelmatig voor.

Aanvallers richten zich echter niet alleen op endpoints, maar op de gehele infrastructuur van een organisatie. Ze maken gebruik van geavanceerde technieken om waardevolle gegevens te bemachtigen of bedrijfsactiviteiten in gevaar te brengen.

The solution: 24/7 Managed Next Generation EDR

XDR is de volgende stap voor Endpoint Detection and Response. Dankzij de toevoeging van Cortex XDR aan de managed Traps oplossing die we al langer aanbieden, beschikken onze analisten over veel meer data – en dat maakt dat we direct toegang hebben tot alle data die nodig is om nog beter inzicht te krijgen in wat er is gebeurd, én om snel en efficiënt te kunnen reageren. Zo kunnen we bij een datalek binnen 30 minuten een root cause analyse uitvoeren en alle betrokkenen volledig informeren.

Inzicht in echte dreigingen:
Op endpoints gerichte aanvallen worden steeds vaker geautomatiseerd en worden ook steeds complexer. Voor IT- en security-afdelingen betekent dit dat ze te maken krijgen met een steeds groter aantal events, een tekort aan getrainde security-analisten, tijdgebrek en stijgende personeelskosten.

CISO's en CSO's moeten beter inzicht krijgen in de totale infrastructuur, sneller kunnen reageren en dreigingen kunnen aanpakken voordat deze schade aanrichten. Wat ze nodig hebben, zijn resultaatgerichte oplossingen die de tijd, kosten en complexiteit van het hele proces van het opsporen en onderzoeken van security-events beperken. Ze zijn niet geïnteresseerd in de enorme hoeveelheid 'false-positive' alerts, maar willen beter inzicht in de échte dreigingen.

Powered by Palo Alto Networks en ON2IT:
De managed endpointoplossing die wij aanbieden, bestaat uit één enkel cloud-gebaseerd product dat de bekroonde Traps en Cortex XDR producten van Palo Alto Networks combineert met onze eigen SOC-as-a-Service voor een vast bedrag per maand. Het is de ideale combinatie van detectie, preventieve bescherming, respons en forensisch onderzoek, en het is beschikbaar voor Linux, Mac, Android en Windows endpoints (servers, desktops, on-premise en in de public cloud).

Geavanceerde automatiseringstechnieken:
Cortex XDR voorziet onze SOC-analisten en forensisch specialisten van rijke gecontextualiseerde log- en eventgegevens en threat intelligence. Door gebruik te maken van automatiseringstechnieken zoals deep learning, behavioral baselining en Indicators of Good©, filtert het ON2IT Security Automation and Orchestration Platform de ruis van de relevante alerts, waardoor onze analisten zich volledig kunnen richten op het opsporen en herstellen van kritische security-events. We kunnen toekomstige risico's verminderen en de preventie voortdurend versterken door het toepassen van kennis die is opgedaan door middel van detectie, onderzoek en respons.

ON2IT
ZERO TRUST INNOVATORS

Het maandelijkse Traps en Cortex XDR abonnement omvat:

- Licentiekosten Traps en/of Cortex XDR
- ON2IT Security Automation & Orchestration Platform
- Threat Event Enrichment, Analysis & Correlation
- Incident Monitoring, Alerting & RCA
- Remote Breach Support
- Security Dashboard
- Compliance Reporting
- Automated Rules of Engagement
- AI-based Threat Hunting*
- Behavior Baselining*
- Post-Mortem Investigation*

*In combinatie met Cortex XDR

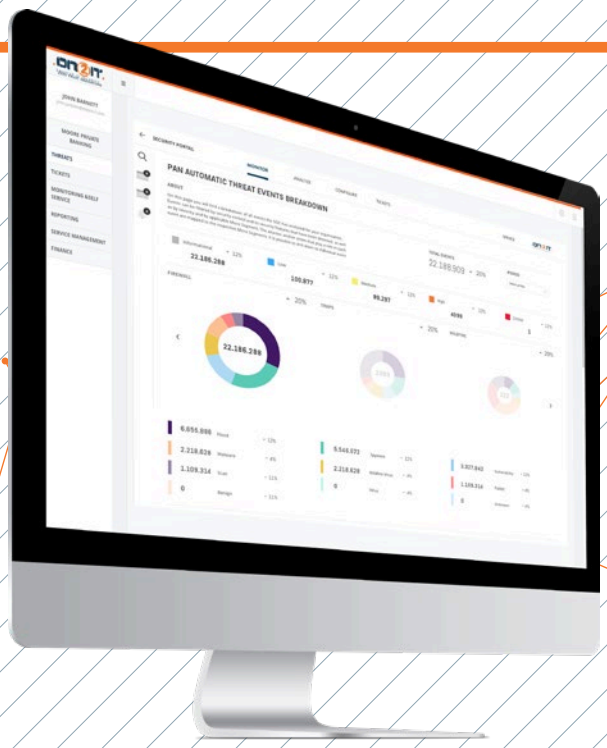
Managed XDR biedt de volgende voordelen

- Geen zorgen over het werven en behouden van personeel
- Uitbreiding van de EDR-voordelen naar de gehele infrastructuur
- De juiste expertise en ondersteuning 24x7
- Kostenbesparingen
- Cloud-oplossing maakt een snelle implementatie en schaalbaarheid mogelijk

Als beste getest

De onafhankelijke onderzoeksorganisatie The MITRE Corporation heeft onlangs de resultaten gepubliceerd van haar MITRE ATT&CK™ cybersecurity-onderzoek. Bij dit onderzoek, waarbij gebruik is gemaakt van het MITRE ATT&CK-framework, is gekeken naar de EDR-oplossingen van 10 vooraanstaande leveranciers. De resultaten laten zien dat de combinatie van Cortex XDR met Traps de meest omvangrijke dekking biedt met de minste gemiste aanvalstechnieken. Van de 136 geteste aanvalstechnieken werden 121 technieken gedetecteerd door Cortex XDR en Traps, en dat is ruim meer dan de andere producten in de test.

ON2IT en Palo Alto Networks: Innovatief op het gebied van cybersecurity



ON2IT biedt sinds 2009 volledige ondersteuning voor de technologie van Palo Alto Networks en sinds 2015 ook voor Traps. Hiermee laten we duidelijk zien dat cybersecurity-innovatie een essentieel onderdeel is van ons DNA.

ON2IT beschikt over de volgende partnerstatussen van Palo Alto Networks: ASC Elite, ATP, CPSP, MSSP en CSSP. Daarnaast zijn we Diamond Partner en hebben we in 2019 de award ontvangen voor 'Global MSSP Partner of the Year'.

We are on to it, and you?

ZERO TRUST INNOVATORS

Regterweistraat 7 / 4181 CE / Waardenburg
E-mail: sales@on2it.net / Tel.: (+31) 22 66 200

ZERO TRUST INNOVATORS

www.on2it.net