
ZERO TRUST
INNOVATORS
ZERO TRUST INNOVATORS

Content

ON2IT
ZERO TRUST INNOVATORS

Weet jij bij een cyberaanval direct wat er aan de hand is?

Datadiefstal en cyberaanvallen zijn helaas een harde realiteit. Hoe hard je ook inzet op preventie, de risico's zijn nooit 100% uit te sluiten. Maar hoe kun je je het beste wapenen, en hoe zorg jij ervoor dat je, in het geval van een inbreuk, binnen 30 minuten volledig op de hoogte bent? Weet jij direct wat er is gebeurd, welke gegevens het betrof en hoe de aanval is gepareerd?


ZERO TRUST
SECURITY
VALIDATION

Geef je security uit handen, maar behoud de controle

Met de steeds groter wordende verscheidenheid aan beveiligingsrisico's missen bedrijven vaak de middelen – waaronder een toereikend budget en goed gekwalificeerd personeel – die nodig zijn om hun systemen 24/7 te beschermen. Wij helpen je graag om je datacenter, netwerk, endpoints en cloud te beveiligen op een manier waarbij je zelf de volledige controle behoudt en voortdurend zicht hebt op alles wat er gebeurt. Ook kunnen wij ervoor zorgen dat je compliant bent en voldoet aan alle geldende richtlijnen op bijvoorbeeld het gebied van privacy.

Alles op basis van Zero Trust

Kort gezegd, nemen wij het hele securityproces uit handen zodat jij je kunt richten op dat wat écht belangrijk is: je bedrijf managen en groei realiseren. Wij bieden onze Managed Security Services aan vanuit een eigen, hypermodern SOC, waar we werken met een combinatie van de beste technologische oplossingen en een team van deskundige securityspecialisten. We laten ons bij onze dienstverlening leiden door de Zero Trust principes. Hiermee onderscheiden we ons ook direct van de concurrentie. Onze aanpak is uniek in de markt en maakt dat we in binnen- en buitenland zijn uitgegroeid tot een toonaangevende partij.

Wie en wat kun je nog vertrouwen?

De IT-wereld is voortdurend in beweging, en ook de manier waarop we naar cybersecurity kijken, is de afgelopen jaren sterk veranderd. Lange tijd werd er simpelweg een grens getrokken tussen ‘de onveilige buitenwereld’ en het ‘vertrouwde’ eigen bedrijfsnetwerk. Firewalls moeten ongewenst verkeer tegenhouden en eenmaal binnen het netwerk beschouwde men al het verkeer als vertrouwd. Het gebruik van mobiele devices, webapplicaties en de toegang van klanten, of bijvoorbeeld leveranciers, tot het netwerk, heeft echter een totaal ander IT-securityconcept noodzakelijk gemaakt.

In 2009 introduceerde Forrester-analist John Kindervag zijn Zero Trust securitystrategie in de Verenigde Staten. Kort daarna droeg ON2IT als eerste diezelfde filosofie uit in Europa.

Wij zijn dan ook dé Europese adopter van de Zero Trust principes, die voorschrijven dat je niets kunt vertrouwen en alles moet verifiëren.

Wat is Zero Trust?

Bij Zero Trust ligt de focus niet langer op het buiten het netwerk houden van bedreigingen, maar op het beschermen van je data en applicaties. We doen dit met behulp van segmentatie. Data, applicaties en gebruikers worden opgedeeld in kleine, overzichtelijke segmenten zodat jij de controle behoudt en precies ziet wat er gebeurt.

Zero Trust is gebaseerd op 5 principes:

- Alle resources worden op een veilige manier benaderd, ongeacht locatie
- Toegangsrechten worden uitsluitend verleend op een ‘need to know’ basis
- Geen enkele datastroom wordt vertrouwd, en alles wordt geverifieerd
- Al het dataverkeer wordt geïnspecteerd en gelogd
- Het netwerk wordt van binnen naar buiten ontworpen

Wat is de meerwaarde?

ON2IT heeft de belangrijkste aspecten van de Zero Trust principes geautomatiseerd. Denk hierbij aan micro- en nanosegmentatie, controle van het dataverkeer en strikte regels over wie toegang heeft tot wat. Deze aanpak minimaliseert de blootstelling aan bekende en onbekende threats, zorgt voor lagere operationele kosten en een betere compliance. Bijkomend voordeel is dat wanneer één server onverhoopt besmet raakt, dit geen gevolgen heeft voor andere servers.

De belangrijkste voordelen van Zero Trust:

- Minimale blootstelling aan cyberthreats
- Lagere operationele kosten
- Grotere continuïteit voor cruciale bedrijfsprocessen
- Betere en kosteneffectieve compliance
- Toekomstbestendige architectuur

De beste service met de beste mensen

ON2IT, dat voor veel van haar klanten de complete IT-security regelt, werkt vanuit een eigen hypermodern Security Operations Center (SOC) met een uitgebreid team hooggekwalificeerde securityspecialisten. Wij houden ons continu bezig met het opsporen en analyseren van security-events, en zorgen voor passende reacties. Hiervoor maken we gebruik van een in-house ontwikkeld Security Automation & Orchestration Platform (SAOP). We beperken ons niet tot het datacenter en netwerk, maar bieden dezelfde bescherming voor de endpoints en cloudomgeving.


ZERO TRUST
MAXIMUM
VISIBILITY

Wat doet het SOC?

Het ON2IT SOC kan je complete IT-security verzorgen op een manier die vandaag de dag voor veel organisaties intern moeilijk is te realiseren. Het blijkt vaak lastig om de juiste mensen te vinden en te behouden – de war for talent woedt immers nog steeds – en budgetten zijn vaak niet toereikend. De werkzaamheden van ons SOC kunnen globaal worden opgedeeld in twee categorieën: monitoring en alerting, en preventie en countermeasures.

Monitoring en alerting (SOC)

- ON2IT Security Automation & Orchestration Platform
- Threat Event Enrichment, Analysis & Correlation
- Incident Monitoring, Alerting & RCA
- Remote Breach Support
- Security Dashboard
- Compliance Reporting
- AI-based Threat Hunting*
- Post-Mortem Investigation*

Preventie en countermeasures (Managed)

- Availability Monitoring & Backup
- Operational & Capacity Management
- Updates & Upgrades
- Policy Compliance & Best Practice Validation
- Device & Policy Configuration Change Management
- Automated Rules of Engagement
- Policy Topology Reporting
- Behavior Baselining*

* Optioneel (vereist XDR)

De voordelen van uitbesteden

Zelfs als je organisatie beschikt over een grote, eigen IT-afdeling, biedt het uitbesteden van het SOC uitgebreide beveiligingsvoordelen die je zelf vaak moeilijk in huis kunt halen. Wanneer je je security overlaat aan het ON2IT SOC, profiteer je van de professionele expertise van meerdere specialisten met verschillende achtergronden op het gebied van informatiebeveiliging. Doordat we daarnaast werken met maandelijkse abonnementskosten is het een voordelig alternatief dat nieuwe investeringen – in mensen, tools en software – overbodig maakt.

Als je je security uitbesteedt bij ON2IT, profiteer je van:

- Visibility en control
- Compliance op basis van Zero Trust
- Deskundige securityspecialisten
- Je betaalt voor het resultaat
- Flexibele abonnementen

SOC-app voor Cortex van Palo Alto Networks

Afgelopen jaar heeft ON2IT een SOC-app gelanceerd voor Cortex van Palo Alto Networks. Deze app versnelt de onboarding en beveiligingsconfiguratie van je IT-infrastructuur (on-premises, hybride of cloud-based), waardoor je direct toegang hebt tot de 24/7 detectie- en responsmogelijkheden van het ON2IT Zero Trust SOC-team. De koppeling kan met één klik tot stand worden gebracht en is binnen een uur operationeel.

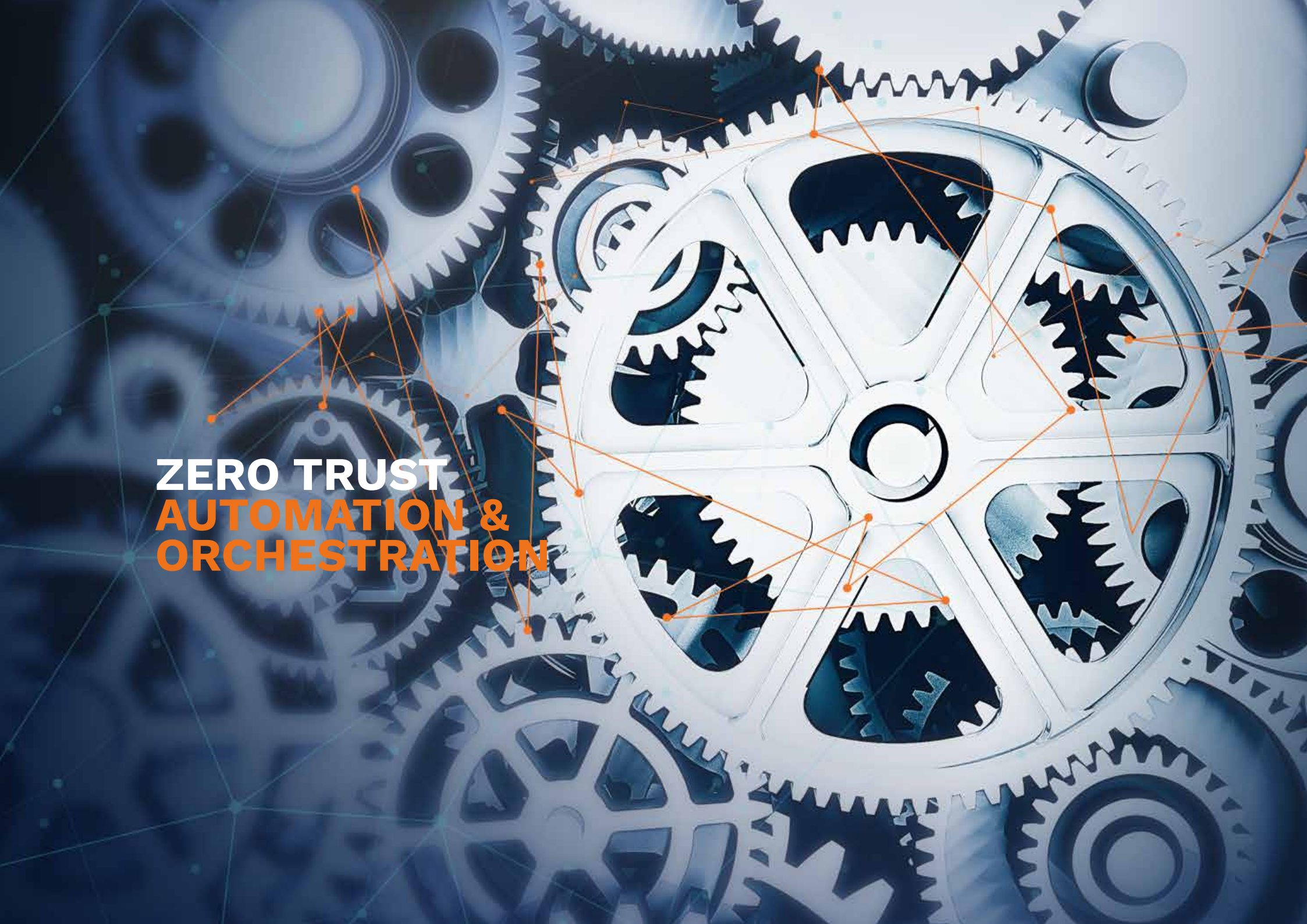
Het centrum van onze dienstverlening

Aan de basis van ons SOC ligt het in-house ontwikkelde Security Automation & Orchestration Platform (SAOP). Dit is het centrale en geautomatiseerde centrum van onze Managed Security Services.

Wat ons uniek maakt, en waarmee we ons duidelijk onderscheiden van andere partijen, is dat we ervoor hebben gekozen om zelf een platform te ontwikkelen waarbij we fors hebben ingezet op automatisering. We hebben dit gedaan vanuit de overtuiging dat we alleen op deze manier flexibel, onafhankelijk en innovatief kunnen zijn. Dit platform stelt ons SOC in staat om optimaal te performen. Bovendien wordt het systeem met elke SOC-actie verder verbeterd.

Automatisering is volgens ons niet alleen wenselijk, maar absoluut noodzakelijk om handmatige controles – en bijgevolg de kans op menselijke fouten – tot een minimum te beperken. Het is ook de enige manier om de steeds groter wordende datastromen snel en goed te kunnen controleren. Automatisering levert uiteraard tijdwinst op en vertaalt zich in een ongekende betrouwbaarheid.

Met ons platform monitoren we jouw IT-security, detecteren en onderzoeken we threats en geven we je aanbevelingen om individuele incidenten op te lossen en je infrastructuur sterker te maken. Ook kunnen we automatisch policy's aanpassen en verbeteringen aanbrengen zodat je continu profiteert van de best mogelijke preventie.


ZERO TRUST
AUTOMATION &
ORCHESTRATION

De best mogelijke preventie met een optimale visibility

Het SAOP biedt een groot aantal voordelen. Zo bieden we dankzij een verregaande automatisering de best mogelijke preventie, en zorgt orchestratie voor een optimale visibility en control. Hieronder lichten we een paar elementen nader toe:

Securityoverzicht per microsegment
Door een verregaande segmentatie in functionele domeinen bieden we inzicht in de securitystatus per segment, applicatie of datatype. Zo vallen abnormaliteiten direct op en weten we bij een infectie meteen waar het probleem zit – en kunnen we dus sneller reageren.

Rules of Engagement
In onze Rules of Engagement staat beschreven welke geautomatiseerde acties het platform onderneemt zonder tussenkomst van menselijk handelen. Dit gebeurt op basis van best practices en ingestelde parameters. De best practices zijn beschreven in zogenaamde playbooks. Hierdoor kunnen we een antwoord bieden op een mogelijke aanval. De playbooks worden continu geüpdatet met nieuwe bevindingen en ervaringen. Dit betekent dat het systeem steeds beter wordt, en dat elk incident onze preventie verder versterkt.

Inidicators of Good
Vaak zoeken securityspecialisten uitsluitend naar zogenaamde Indicators of Compromise (IoC's): aanwijzingen waarmee de aanwezigheid van een specifieke dreiging, zoals een bepaald malware-exemplaar, binnen het netwerk kan worden vastgesteld. Omdat je bij dreigingen die je niet kent ook niet weet je zoekt, hebben wij voor een omgekeerde aanpak gekozen, en gaan we eerst op zoek naar de Indicators of Good. Wij kijken bij het filteren van verkeer naar wat wel is toegestaan. Welke applicaties zijn akkoord, welke gebruikers enz. Dit maakt dat we uiteindelijk veel minder data hoeven te inspecteren, en daarmee besparen we tijd en vinden we ook sneller abnormaliteiten.


ZERO TRUST
LOGICAL
SEGMENTATION

Meer weten?
Wil je meer weten over onze Managed Security Services, neem dan contact met ons op via 088-2266200.

ZERO TRUST INNOVATORS

Regterweistraat 7 / 4181 CE Waardenburg / Algemeen 088-2266200

ZERO TRUST INNOVATORS

www.on2it.net