

Connect & Protect OT: van uitdaging naar concurrentievoordeel

Van industriële connectiviteit tot 24/7 security monitoring – spotit is uw partner voor betrouwbare en veilige OT-omgevingen.

Industriële bedrijven staan vandaag voor een dubbele uitdaging: **productieprocessen moeten steeds efficiënter en digitaal worden, terwijl de risico's op cyberaanvallen, downtime en compliance-overtredingen groter dan ooit zijn.** Operationele technologie (OT) vormt het hart van uw fabriek, uw logistieke keten of uw nutsvoorziening. Zonder robuuste connectiviteit en beveiliging komt business continuity onmiddellijk in gevaar.

Spotit is gespecialiseerd in het verbinden en beschermen van IT- en OT-omgevingen. **Onze kracht ligt in het combineren van diepgaande IT- én OT-expertise, zodat u niet moet kiezen tussen stabiliteit of innovatie.** Wij begeleiden organisaties van de eerste netwerkscan tot continue monitoring in ons Network Operations Center (NOC) en Security Operations Center (SOC), steeds met oplossingen die afgestemd zijn op industriële realiteit.

Onze kernbeloftes

- » **Connectiviteit waarop je kan rekenen** – wij zorgen voor bekabelde en draadloze netwerken die bestand zijn tegen zware industriële omstandigheden en voorbereid zijn op de toekomst.
- » **Volledige zichtbaarheid & segmentatie** – wij brengen uw OT-assets in kaart, zorgen voor OT-netwerksegmentatie en beperken zo de risico's op cybersecurity incidenten en downtime.
- » **Veilige & compliant IT/OT-integratie** – onze oplossingen helpen om compliant te zijn met regelgeving (NIS2, Cyber Resilience Act) en industriële standaarden (IEC62443) en zijn ontworpen om samenwerking tussen IT en OT te versterken.



**DISCOVER
MORE ABOUT
SPOTIT OT**

Onze
partners



De 6 stappen van spotit OT



1 OT Visibility Assessment

We starten altijd met zichtbaarheid. Welke assets hebt u? Welke kwetsbaarheden bestaan er? Welke protocollen zijn in gebruik? Onze assessments, vaak ondersteund door gespecialiseerde tooling, brengen dit in kaart en leveren u een helder rapport met prioriteiten en quick wins. Dit vormt de basis voor elke volgende stap.



2 OT Network Segmentation

Veel productieomgevingen draaien nog op platte netwerken. Eén besmetting kan zo een volledige fabriek platleggen. Met onze segmentatie-aanpak structureren we uw netwerk in logische zones, beperken we laterale bewegingen van aanvallers en verhogen we de betrouwbaarheid van uw OT-architectuur.



3 OT Secure Remote Access

Onderhoud door leveranciers of interne experts gebeurt steeds vaker vanop afstand. Zonder controle is dit een groot risico. Onze oplossingen laten toe om per gebruiker, per sessie en per toestel te bepalen wie toegang krijgt, wanneer en tot welke componenten. Zo combineert u veiligheid met operationele efficiëntie.



4 Industrial Connectivity

Een betrouwbare OT-omgeving begint bij de basis: connectiviteit. Wij implementeren industriële switches, routers en draadloze oplossingen die bestand zijn tegen extreme omstandigheden, compatibel zijn met industriële protocollen en future proof ontworpen zijn. Van bekabelde netwerken tot industriële 5G.



5 OT Threat Monitoring & Response

Cyberaanvallen stoppen niet buiten kantooruren. Met OT-specifieke threat monitoring detecteren we afwijkend gedrag in real time. Onze SOC-teams grijpen in waar nodig en werken samen met uw OT-operators om incidenten veilig te verhelpen en om de impact op de productie zoveel mogelijk te beperken.



6 Managed Services (Network Operations Center & Security Operations Center)

Beveiliging is geen eenmalige oefening, maar een continu proces. Via ons Network Operations Center en Security Operations Center monitoren we uw OT-omgeving 24/7. We bieden OT cybersecurity awareness consultancy, incident response en proactief beheer van netwerk en security. Zo hebt u gemoedsrust, terwijl u focust op uw core business.

Kansen en uitdagingen

Met de komst van digitalisering, Internet of Things en cloud zijn OT-systemen niet langer geïsoleerde eilanden. Machines, sensoren, PLC's en productielijnen communiceren steeds vaker met IT-systemen, externe leveranciers en met de cloud. Dit biedt enorme voordelen op vlak van efficiëntie, onderhoud en innovatie, maar maakt OT ook kwetsbaar:

Stijgend aantal OT-specifieke cyberaanvallen
aanvallen op industriële netwerken kunnen productie stilleggen en zelfs de veiligheid van mensen of milieu in gevaar brengen.

Strengere regelgeving
wetgeving of standaarden zoals NIS2 en IEC 62443 verplichten bedrijven om hun OT-omgeving aantoonbaar veilig en compliant te maken.

Meer connectiviteit betekent meer risico
draadloze toepassingen, remote access en nieuwe digitale technologieën vergroten de attack surface.

IT en OT werken vaak langs elkaar heen
veel organisaties hebben geen volledig overzicht van assets en kwetsbaarheden, of geen gedeeld beleid tussen IT- en OT-teams.

Wij werken voor

- » **Roger & Roger**
- » **Ajinomoto Omnicheem**
- » **Aurubis Beerse**
- » **Galloo**
- » **Crops**
- » **MPET**
- » **FEBELCO**
- » en vele anderen

Wij helpen u

Spotit helpt bedrijven deze uitdagingen om te zetten in concurrentievoordeel. Wij geloven dat een veilige en goed verbonden OT-omgeving de sleutel is tot succesvolle digitalisering. Onze aanpak is opgebouwd rond zes duidelijke stappen, die u elk afzonderlijk kan afnemen, maar die samen een volledig beveiligde en toekomstbestendige OT-omgeving vormen.

Waarom kiezen voor spotit?

Unieke expertise in IT én OT

wij begrijpen de noden van fabrieksvloer en IT-afdeling en slaan de brug tussen beide werelden.

Van A tot Z, maar ook modulair

u kiest zelf of u één stap wil uitbesteden of het volledige traject aan ons toevertrouwt.

Meer dan 100 experts

gespecialiseerd in netwerk, security en compliance voor kritieke infrastructuren.

Bewezen track record

ervaring in diverse sectoren, zoals voeding, chemie, farma, energie, havens, logistiek en recycling.

Altijd in lijn met internationale standaarden

NIS2, IEC 62443 en de Cyber Resilience Act zijn geïntegreerd in onze aanpak.

Threat monitoring & incident response

proactieve bewaking en snelle incidentrespons om risico's te beperken.

Managed network & security services

volledig beheerde netwerk - en securitydiensten die continuïteit en veiligheid garanderen.

Uw oplossing



DISCOVER
MORE ABOUT
SPOTIT OT

Got hacked? Contact us 24/7
+32 (0)9 322 04 35

www.spotit.be info@spotit.be