OT Perimeter Assessment

De grenzen tussen informatietechnologie (IT) en operationele technologie (OT) vervagen. Het beschermen van de link tussen IT- en OT-netwerken is cruciaal om het OT-aanvalsvlak te beveiligen. Dit OT Perimeter Assessment helpt om uw OT-systemen veilig te houden.

Het OT Perimeter Assessment geeft u:

Inzicht in bedreigingen

U krijgt inzicht in potentiële entry points voor cyberaanvallen en in kwetsbaarheden.

Concrete actiepunten

U ontvangt concrete aanbevelingen, zodat u uw systemen kunt beschermen.

Advies van OT-specialisten

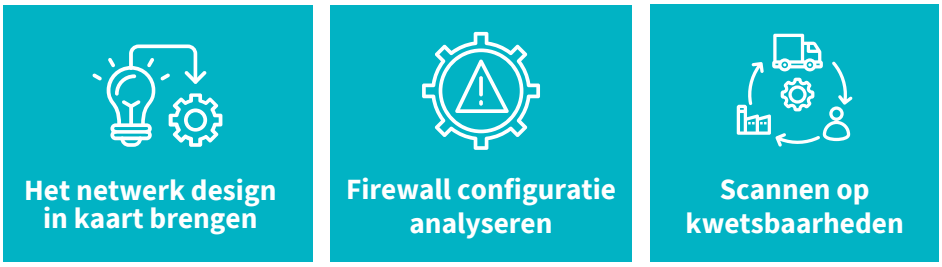
OT-security vereist expertise: onze OT-specialisten delen graag hun kennis met u.

Waarom het OT Perimeter Assessment?

IT- en OT-netwerken zijn steeds meer met elkaar verbonden - voor automatisering, efficiëntie en directe data-analyse. Deze IT/OT-convergentie is een gevolg van Industrie 4.0, de vierde revolutie in industriële productie. Het maakt uw systemen kwetsbaarder voor cyberaanvallen - vooral als ze ook verbonden zijn met het internet en de cloud. Het **OT Perimeter Assessment** controleert deze drie dingen: het ontwerp van uw OT-netwerk, de stroom van het dataverkeer en kwetsbaarheden in het netwerk. We richten ons op systemen in IT- en OT-netwerken die met elkaar moeten communiceren. Dit omvat IT-systemen die samenwerken met dual-homed IT/OT-systemen of die de Demilitarized Zone (DMZ) doorkruisen. Het OT Perimeter Assessment is een uitstekende plek om te beginnen met OT-beveiliging. De resultaten van dit assessment kunnen u een idee geven over welke volgende stappen verstandig zijn.

Hoe het OT Perimeter Assessment werkt

Elk OT Perimeter Assessment bevat de volgende drie elementen.



1. Het netwerk design in kaart brengen

Na bestudering van tekeningen, asset registers en technische informatie stellen we eerst een netwerkdiagram op. Uw experts en de onze bekijken dit diagram vervolgens om alle mogelijke entry points aan te wijzen, waaronder UPS-beheer op afstand, fysieke toegangscontroles of HVAC en BMS ("building management system"). Uw IT- en OT-experts worden ook betrokken bij een high-level Threat Modeling-sessie om potentiële bedreigingen in kaart te brengen.

2. De firewall configuratie analyseren

Het verkeer tussen uw IT en OT wordt waarschijnlijk gefilterd door een of meer firewalls of andere grensbeschermingsapparaten. We analyseren de firewallinstellingen grondig. Het doel is om te:

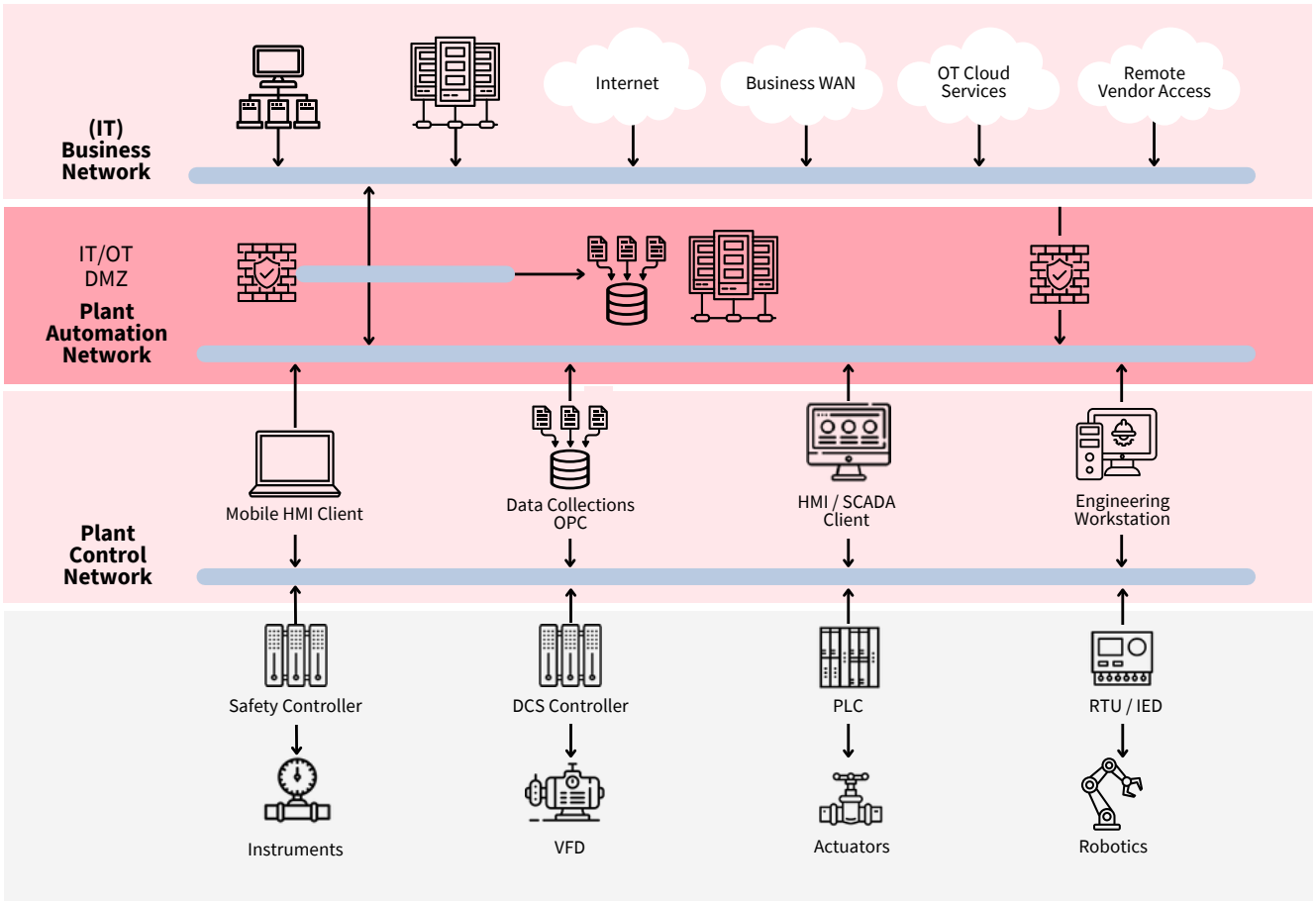
- Verifiëren dat alleen de minimale hoeveelheid vereist verkeer wordt doorgelaten en al het andere verkeer wordt geweigerd.
- Controleren dat verkeer alleen tussen bevoegde eindpunten stroomt.
- Het toegestane verkeer correleren met de beveiligingsconfiguraties van de eindpunten.

3. Scannen op kwetsbaarheden

Op basis van de geanalyseerde netwerkdiagrammen en firewallconfiguratie kunt u aanvullende OT-netwerkscans verwachten om een dieper inzicht te krijgen in het daadwerkelijke netwerkverkeer. We gebruiken twee verschillende technieken:

Passief scannen. Dit is een "alleen-lezen" techniek die gebruik maakt van een kopie van bestaand netwerkverkeer. Deze methode kan kwetsbaarheden blootleggen, zoals zwakke protocollen, slechte configuratie of verouderde firmware.

Actief scannen. Deze queries worden afgestemd op een enkele host of een deel van het netwerk. Zo kunnen we zwakke of niet-versleutelde protocollen, zwakke of onveilige softwaretoepassingen of services, onbekende IT/OT-communicatiestromen, onbekende systemen of slecht geconfigureerde systemen en bekende beveiligingsproblemen (CVE's) ontdekken.



Deze grafiek toont de focus van het assessment. De belangrijkste focus, in rood, is de scheidslijn tussen IT en OT. We controleren echter ook relevante delen van de OT- of IT-systemen, weergegeven in roze.

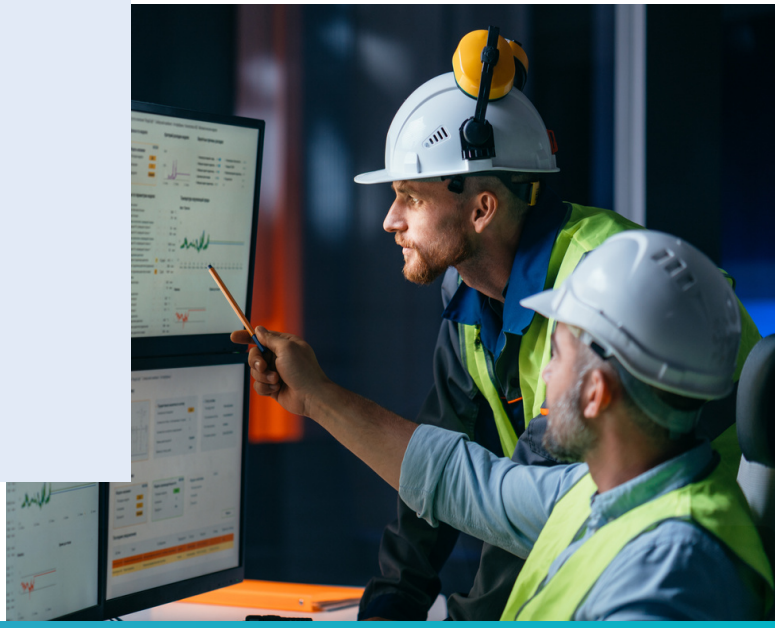
Actie ondernemen

Alle bevindingen uit deze drie stappen worden vervolgens gecombineerd en geanalyseerd. Het resultaat is een rapport met actiepunten voor verbetering, zodat u direct actie kunt ondernemen.

Wat onze klanten zeggen

“Dit was echt een eye-opener”

“We zijn nog maar net begonnen met onze beveiliging. De OT Perimeter Assessment liet ons zien hoeveel misconfiguraties er eigenlijk aanwezig waren in ons netwerk. Dit was een echte eye-opener voor ons.”



Gerelateerde diensten

NIS2 Diensten

De kans is groot dat uw bedrijf onder de Europese NIS2-richtlijn valt. Wij bieden Gap Assessments en implementatieondersteuning om u te helpen volledig aan de NIS2-richtlijn te voldoen.

OT Site Assessment

Het OT Site Assessment omvat bezoeken aan de locatie, reviews van de systeemarchitectuur en overleg met experts om zwakke punten in uw beveiliging te identificeren en aan te pakken. Met dit assessment kunt u uw OT-beveiliging optimaliseren.

Industriële pentesting

Vulnerability assessments en penetratietesten kunnen helpen om zwakke plekken in de beveiliging van uw OT-systemen te ontdekken. Onze gespecialiseerde OT-penetratietesters helpen u hier graag bij.

Secura
A BUREAU VERITAS COMPANY

Over Secura / Bureau Veritas

Secura is een toonaangevend cybersecuritybedrijf. Ons doel is om uw cyberweerbaarheid te vergroten. Onze klanten variëren van overheid en zorg tot financiën en industrie. Secura biedt technische diensten aan, zoals vulnerability assessments, penetratietesten en red teaming. We bieden ook audits, forensische diensten en awarenesstrainingen aan.

Secura is onderdeel van Bureau Veritas (BV), een beurs-genoteerde onderneming die gespecialiseerd is in testen, inspecteren en certificeren. BV is opgericht in 1828, heeft ruim 80.000 medewerkers en is actief in 140 landen.

Voorbeeld | OT Perimeter Assessment

Welk probleem had de klant?

Een grote fabrikant met meerdere wereldwijde vestigingen wilde voor elk van de vestigingen weten hoe veilig de scheiding was tussen IT en OT. Ze hadden geen bedrijfsbreed beleid voor hun OT-security.

Resultaat

Tijdens het OT Perimeter Assessment ontdekten we bijvoorbeeld dat een aanvaller die toegang had gekregen tot één faciliteit ook andere faciliteiten kon bereiken. Omdat we alle faciliteiten hadden getest, konden we deze klant helpen bij het prioriteren van de risico's en adviseren over verbeteringen.

BUREAU VERITAS 1828

Meer weten?

Neem contact met ons op om uw cyberweerbaarheid te verhogen.

info@secura.com

+31 (0) 88 888 3100

secura.com