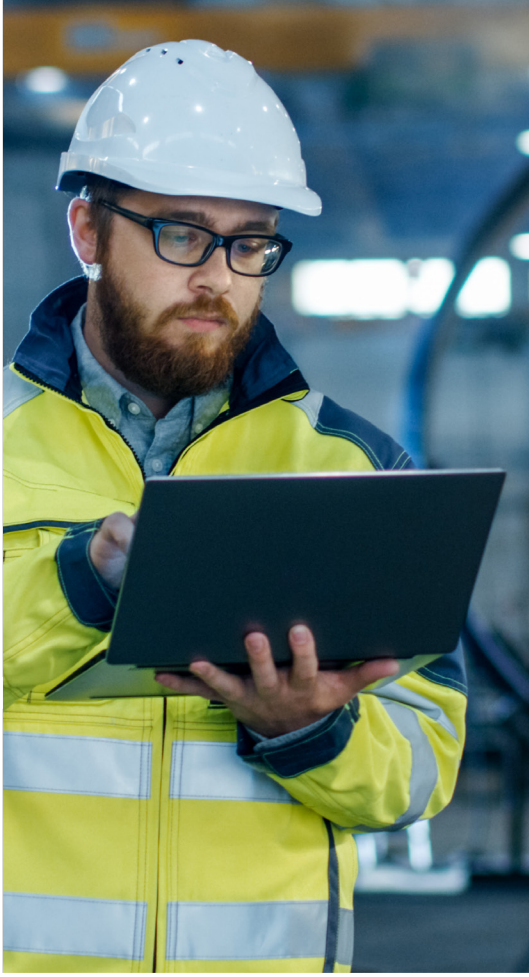
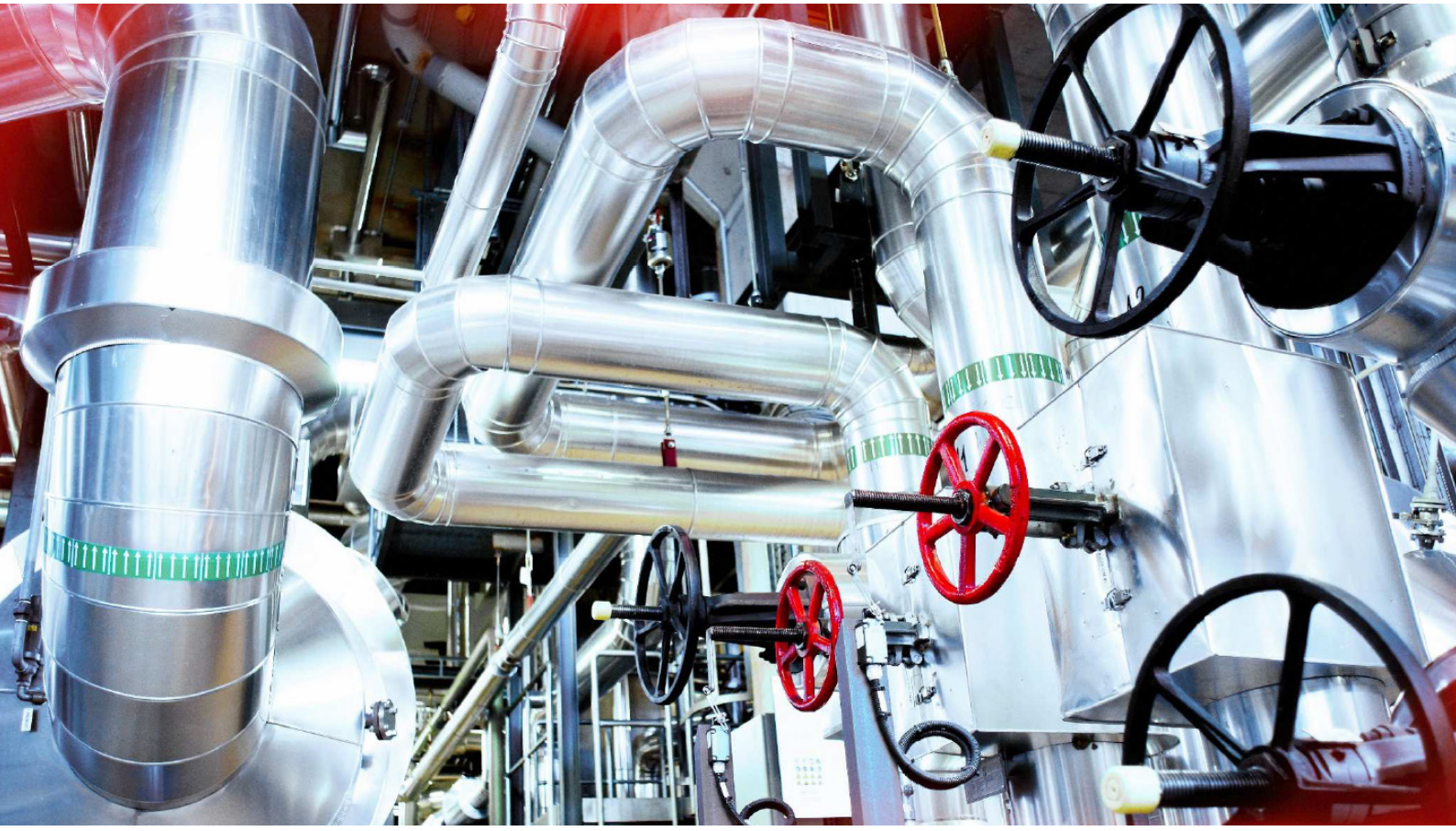
Cybersecurity van operationele technologie



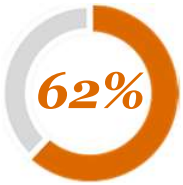
De Cybersecurity van Operationele Technologie is belangrijker dan ooit.

Onze cybersecurity experts helpen u uw vitale infrastructuur te beschermen.



pwc

Wat is onze ervaring
en hoe kunnen wij u helpen?



van de bedrijven ervoer verstoringen en downtime van productie.

69% van de organisaties gelooft dat OT een mogelijke aanvalsvector zal zijn.

38% verwacht dat aanvallen zich het komende jaar zullen uitbreiden van IT naar OT.

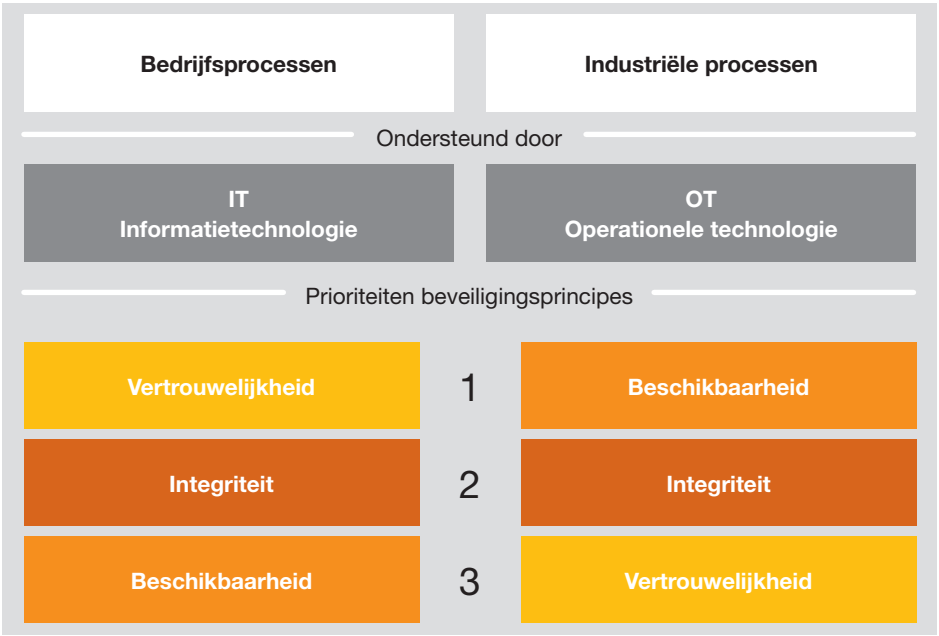
van de ondervraagde bedrijven beschouwt de kans dat zij doelwit worden van een OT-cyberaanval in de komende 12 maanden als zeer waarschijnlijk (7% meer t.o.v. vorig jaar).

Bron:
- PwC Digital Trust Insights Survey, 2018
- Cisco, 2018 Annual Cybersecurity Report
- Kaspersky Labs' ICS Whitepaper, 2018

Operationele Technologieën (OT)[1], inclusief Industrial Control Systems (ICS), vormen het hart van de nationale vitale infrastructuur, die onder andere bestaat uit de elektriciteitsvoorziening, de olie- en gasvoorziening, (drink)waterbeheer, luchtvaart, spoorwegen en (water)wegen. OT-systemen zijn oorspronkelijk ontworpen met weinig aandacht voor cybersecurity. De reden hiervoor was simpel: ze waren volledig gescheiden van andere IT-systemen en het Internet, uitgerold in een geïsoleerde omgeving met beperkte fysieke en logische toegang en beperkte data-uitwisseling met de IT-omgeving. Hierdoor werden ze van nature als veilig beschouwd.

Nu, door de groeiende behoefte aan data-uitwisseling worden de IT en OT-werelden steeds meer met elkaar verbonden. Dit zorgt voor een nieuwe uitdaging: OT cybersecurity. Cyberaanvallen op IT-netwerken komen regelmatig voor en de integratie van IT en OT geeft aanvallers nieuwe aanvalsmogelijkheden. Kwetsbaarheden in IT-netwerken kunnen worden gebruikt om gerichte aanvallen op te zetten op OT-netwerken.

Cybersecurity is geen nieuw begrip in het IT-domein en in theorie zou de toepassing van beveiligingstechnologieën uit het IT-domein binnen OT voldoende moeten zijn. Echter, de praktijk bewijst dat een andere benadering voor het beveiligen van IT en OT-systemen nodig is vanwege de verschillen in beveiligingsprioriteiten:



De stijgende behoefte aan 'real time' data voor bedrijfsactiviteiten vereist een continue stroom van data-uitwisseling tussen de OT- en IT-netwerken, bijvoorbeeld voor data-analyses in de cloud om productieprocessen te optimaliseren (onder meer door middel van Artificial Intelligence), voor de monitoring van de staat van vitale infrastructuren en voor de aansturing van industriële IoT (IIoT).

Een laag beveiligingsniveau van OT lokt aanvallen door hackers uit, specifiek door internationale cybercriminelen en 'nation states'-type aanvallers. De gevolgen kunnen, juist in het geval van vitale infrastructuren, potentieel zeer ontwrichtend zijn voor onze maatschappij.

De sleutelrol van OT in het functioneren van economie en maatschappij zorgt ervoor dat regelgeving voor de beveiliging van de nationale vitale infrastructuur steeds meer onder formeel toezicht wordt gesteld. De Wet beveiliging netwerk- en informatiesystemen (Wbni), als uitvloeisel van de Europese NIS-Directive, is hier een concreet voorbeeld van.

Dreigingen in het IT-domein verspreiden zich steeds meer naar het OT-domein. Een simpele toepassing van beveiligingstechnologieën uit het IT-domein binnen het OT-domein is niet genoeg om een afdoende niveau van beveiliging te bereiken.

1 Ook wel naar gerefereerd als: Industriële automatisering (waaronder IIoT), proces automatisering, Industrial Control Systems (ICS).

Hoe kunnen wij u helpen?

OT Quick Scan – Op maat gemaakte Dreigings- en Volwassenheidsanalyse

IT & OT Security Strategie, Operating Model & Risicoanalyse

OT Security Organisatie, Beleid en Bewustzijn

OT Security Monitoring, Detectie, Incident Response & crisismanagement

Ontwerp, ontwikkeling en uitvoering van een Hybrid SOC

ICS Cyber Kinetic Lab

Penetratietesten op centrale systemen

Threat intelligence voor OT Netwerken

Component Testing

Productie Security Assessment

Op de laatste pagina lichten wij deze diensten in meer detail toe.

De hoeveelheid en intensiteit van OT cyber aanvallen en incidenten is aanzienlijk toegenomen	Uitgebreide en wereldwijde praktijkervaring in industrie	Certificaten en professionaliteit
2010 **Uitschakeling uraniumcentrifuges Iran (Stuxnet)**	PwC beschikt wereldwijd over ruim 3500 professionals die gekwalificeerd zijn op IT en OT security. Specifiek voor OT bieden wij u een team van meer dan 100 OT security professionals – voormalig CISO's, engineers, OT security consultants, business en securityspecialisten – met jarenlange ervaring in de energie-, olie en gas, transport-, telecom-, productie-, publieke en IT-sector. Doordat we beschikken over uitgebreide praktijkervaring met complexe vitale infrastructuren in verschillende sectoren, zijn we in staat om gedegen analyses uit te voeren en dreigingen op waarde te schatten. We kunnen u vervolgens adviseren over de beste oplossing en de wijze waarop we deze oplossing duurzaam in uw organisatie kunnen implementeren.	Onze professionals beschikken over verschillende relevante certificeringen op het gebied van cybersecurity in het algemeen en OT security specifiek: • Global Industrial Cyber Security Professional (GICSP) • Certified SCADA Security Architect (CSSA). • Wij werken volgens de standaarden die gebruikelijk zijn in de industrie: – NIST CSF & 800-82 (guidance to protect critical infrastructure) – NERC CIP v5 (critical infrastructure protection) – ISO 22301 (business continuity) – ANSI/ISA 62443 (ISA 99) (ICS security)
2015 + 2016 **Uitval electriciteitsnetwerk Oekraïne**		
2017 **Ransomware Containeroverslagbedrijf Nederland**		
2017 **Triton aanval op de raffinaderij van Aramco**		
2018 **Aanval electriciteitsnetwerk VS**		

Contactgegevens:

Remco van Mosel
Director

Cybersecurity & Privacy
Publieke sector
Mobiel: +31 6 10 925 731
E-mail:
remco.van.mosel@pwc.com

Angeli Hoekstra
Partner

Cybersecurity & Privacy
Commerciële sector
Mobiel: +31 6 30 861 522
E-mail:
hoekstra.angeli@pwc.com

Wouter Otterspeer
Director

Cybersecurity & Privacy
Offensive security
Mobiel: +31 6 10 801 462
E-mail:
wouter.otterspeer@pwc.com

Gedetailleerde catalogus van onze OT security diensten

OT Quick Scan – Op maat gemaakte Dreigings- en Volwassenheidsanalyse

Beoordelen van het volwassenheidsniveau van het vermogen van uw organisatie om OT-cyberbedreigingen en -incidenten het hoofd te bieden; uw OT-middelen en -maatregelen in kaart brengen en ontwikkelen van een gezamenlijk plan om uw belangen te beschermen.

IT & OT Security Strategie, Operating Model & Risicoanalyse

Ontwerpen van de toekomstige staat, de governance en de roadmap voor de implementatie van maatregelen in de IT- en OT infrastructuur, in overeenstemming met uw bedrijfs- doelstellingen, compliance vereisten en het dreigingslandschap.

OT Security Organisatie, Beleid en Bewustzijn

Implementeren van een volwassen organisatie, definiëren van normen en het bevorderen van het beveiligingsbewustzijn bij medewerkers.

Productie Security Assessment

Betrekken van IT- en productie-stakeholders die een sleutelrol vervullen bij het identificeren en evalueren van de belangrijkste risico's van de productiefaciliteiten. Hierbij wordt gebruik gemaakt van een gemeenschappelijke norm en methode voor de beoordeling van productiefaciliteiten en voor het identificeren en beperken van de risico's voor operationele activiteiten. Beoordelen van de risico's en het prioriteren van herstelwerkzaamheden met als doel het inzicht in sterke en zwakke punten vergroten en uw strategie zo in te richten dat de belangrijkste security uitdagingen worden meegenomen.

Threat intelligence voor OT Netwerken

Organisaties die afhankelijk zijn van Industrial Control Systems (ICS) worden geconfronteerd met steeds geavanceerder wordende aanvallers, die een veelheid aan aanvalsvectoren benutten. Traditionele IT-gecentreerde threat intel (T.I.) voldoet onder deze omstandigheden voor OT niet meer. PwC helpt organisaties bij het beheersen van cyberrisico's door T.I. in te zetten. We bieden een uitgebreide dekking van het dreigingslandschap voor IT- en OT-netwerken, stellen organisaties in staat geïnformeerde en effectieve beslissingen te nemen om hun belangen te beschermen.

OT Security Monitoring, Detectie, Incident Response en Crisismanagement

Verkorten van de reactietijd op incidenten, door snelle detectie van potentiële kwetsbaarheden als een belangrijke stap naar het maximaliseren van de beschikbaarheid en een adequate reactie op incidenten wanneer ze zich voordoen.

Ontwerp, ontwikkeling en uitvoering van een Hybrid SOC

Ontwerpen van agile detectiemiddelen / sensoren en implementeer data-analyse van hybride OT-bronnen, threat intel en informatie-uitwisseling binnen de sector, met als doel een IT / OT SOC te creëren dat in staat is om complexe cyberaanvallen af te slaan.

ICS Cyber Kinetic Lab

Ontwerpen, bouwen en exploiteren van een platform dat het mogelijk maakt nieuwe technologieën diepgaand te evalueren, geavanceerde aanvallen te simuleren en cyberdeskundigen op te leiden, op echte operationele kinetische modules die volledig zijn uitgerust en representatief zijn voor productieomgevingen.

Penetratietesten op centrale systemen

Centrale systemen verzamelen gegevens over bijvoorbeeld meters, en delen deze met andere bedrijfssystemen (bijvoorbeeld ERP). We voeren black-, white- en greybox penetratietesten uit op deze systemen met als doel technische kwetsbaarheden te vinden.

Component Testing

Door gebruik te maken van het Purdue model kunnen we op verschillende niveaus en op verschillende componenten uw omgeving testen op kwetsbaarheden. Denk hierbij bijvoorbeeld aan het testen van netwerk segmentatie, het testen van componenten zoals DCS, PLC, RTU, MMI, HMI, maar ook Historian, Operator Workstations, Engineering Stations, Drives, Scada applicaties etc. In bijvoorbeeld de utility sector hebben we ook uitgebreide ervaring met het testen van de Advanced Metering Infrastructure en Smart Meters.

pwc