“Hoe u uw Operationele Technologie weerbaarder kan maken tegen cybercrime.”

Industrial Control Cybersecurity van CGI

CGI

Experience the commitment®

Industrial Control Cybersecurity van CGI

ICCS: een geïntegreerde cybersecurity-aanpak voor Operationele Technologie.

Digitalisering is bij de meeste organisaties inmiddels de normaalste zaak van de wereld. Efficiëntie, kostenbesparing, ‘client centric’ processen, een kortere time-to-market: iedereen ziet de voordelen. Waarbij de klant altijd vooropstaat.
Helaas zitten er ook nadelen aan digitalisatie. Cybercriminelen liggen op de loer en breken in bij centrale (goedbeveiligde) servers om bedrijfsinformatie te stelen. Niet voor niets groeit het aantal cybersecurity-diensten snel, met als doel organisaties te ondersteunen en weerbaarder te maken bij hun digitale ontwikkeling.

OT met IT

Haast ieder kantoor is tegenwoordig gedigitaliseerd. Nu zit de productiekant in deze transformatie. Want ook daar hebben de mensen baat bij een efficiënt operationeel proces en optimale effectiviteit. Bijvoorbeeld door off-site monitoring, remote maintenance en predictive maintenance. Of agile-productontwikkeling op basis van actuele inzichten uit de markt. Ontwikkelingen op het gebied van het Internet of Things (IoT) en Big Data Analytics staan dan ook sterk in de belangstelling bij bedrijven. In toenemende mate voorzien organisaties – bijvoorbeeld de maakindustrie, transport- en nutssector, olie- en gasmarkt en gezondheidszorg – hun Operationele Technologie (OT) van IT-technologie. Daardoor komen zij in verbinding te staan met wijdverbreide IT-netwerken. OT-omgevingen worden overigens ook wel Production Control Department-omgevingen (PCD) of Industrial Control Systems-omgevingen (ICS) genoemd.

Secure by design

Met een modern bedrijf ontkom je in deze tijd niet aan zo’n digitale integratie van OT en IT. En ook die zorgt weer voor uitdagingen. De OT-assets die op dit moment in gebruik zijn, dateren vaak uit de jaren ’80 en ’90, zijn niet ontworpen voor interconnectieve operaties en daarmee inSecure by design. Ieder IT-element dat wordt toegevoegd aan de operationele bedrijfsomgeving en gekoppeld aan OT, leidt tot exposure en vergroot de kans op een aantal security breaches. Een bijkomend probleem is dat veel organisaties weinig zicht hebben op de omvang en status van alle assets in de operationele omgeving. Daarbij zijn ze vaak aangewezen op reactief beheer in plaats van proactieve monitoring. En juist tijdige detectie is een eerste vereiste voor adequaat ingrijpen.

Kwetsbaar voor cybercriminelen

Organisaties in verschilende sectoren zijn door deze digitaliseringsslag zeer kwetsbaar. Cyberincidenten ontstaan door hackers die actief een weg naar binnen forceren. Het kan gaan om eigen medewerkers die kwaadwillenden bewust (sabotage) of onbewust (phishing) ongeautoriseerde toegang geven tot systemen en data. Maar er zijn ook groepen criminelen die erop uit zijn om zoveel mogelijk schade aan te richten. Inmiddels weten we hoe enorm de gevolgen kunnen zijn van aanvallen op Enterprise-IT. En de impact is nog groter als het gaat om incidenten bij industrieën en nutsbedrijven. Dan gaat het niet alleen om verlies van data en/of waardevolle bedrijfskennis, stokkende processen en financiële of reputatieschade. Maar ook om reëel gevaar voor de plant safety, kans op lichamelijke schade en zelfs een concrete bedreiging van mensenlevens en het milieu.

Aangescherpte wet- en regelgeving

Op dit moment hebben veel organisaties nog niet in de gaten dat hun OT-systemen kwetsbaar zijn of aangevallen worden. Dit komt door gebrek aan monitoring. Toch groeit het bewustzijn wel rondom cybersecurity in het PCD. Dat heeft te maken met publiciteit rondom grote aanvallen. Ook de overheid speelt hierbij een rol. De wet- en

CGI's portfolio, robuuste oplossingen voor Industrial Control Systems

Operate with Confidence

Operate with Confidence is een businessgerichte aanpak waardoor u uw complexe informatiebeveiliging en bedrijfsomgeving kunt beheren. Van compliance en audits tot beleid en architectuur. Met cybersecurity services van CGI bent u daarvan verzekerd.

Assess the Risk

Met Assess the Risk helpen we u cyberbedreigingen en kwetsbaarheden te begrijpen en risico's in te schatten. Samen schatten we de ROI op beveiligingsinvesteringen in, bouwen we businesscases voor beveiliging en bepalen we de beste cyberstrategie voor uw organisatie.

Protect the Business

Met Protect the Business bieden we oplossingen en diensten die ontwikkeld zijn:
- voor de bescherming van de integriteit van uw bedrijfsinformatie;
- om uw software aan steeds hogere veiligheidseisen te laten voldoen;
- voor de beschikbaarheid van de belangrijkste assets binnen uw organisatie.

regelgeving rondom cybersecurity wordt steeds beter en sneller aangescherpt. Zo is het in sommige landen al verplicht om integriteitsschendingen te melden. Monitoring van OT-omgevingen wordt essentieel en het hele PCD-domein moet Secure by design worden. Wie in de toekomst niet kan aantonen er alles gedaan te hebben om zijn systemen te beveiligen, verliest zijn license to produce.

Investeren in kennis, vaardigheden en middelen

Dat het bewustzijn rondom cybercrime en -beveiliging groeit, blijkt onder meer uit de CGI Global 1000 Outlook. In de persoonlijke interviews die CGI jaarlijks houdt met ruim 1.000 leiders uit de business en IT-wereld, zegt een groot deel van de ondervraagden uit de industriële en nutssector min of meer voorbereid te zijn op de cybersecurity-bedreigingen van deze tijd. Slechts een enkeling geeft aan in hoge mate voorbereid te zijn. Het ontbreekt simpelweg aan kennis, vaardigheden en middelen om de bedreigingen het hoofd te bieden, met name die in het PCD-domein. Hier ligt duidelijk een taak voor een betrouwbare partner die kan helpen de productiesector zo veilig en weerbaar mogelijk te maken.

Holistische aanpak

Hoe creëer je een veilige en weerbare ICS-omgeving? In de meeste gevallen is dat een lang en complex traject. De uitdaging gaat verder dan het beveiligen van de OT. Dit vereist diepgaande domeinkennis. Daarbij moet je je bewust zijn van de risico's die de samenvloeiing van OT en Enterprise-IT met zich meebrengt. Ook moeten beheer en monitoring van de totale operatie structureel verbeterd worden. Dat vraagt om een belangrijke cultuuromslag: alle betrokkenen binnen de organisatie moeten hun gedrag veranderen. Alleen een holistische aanpak, met aandacht voor mensen, processen en technologie, leidt tot betere weerbaarheid.

Geïntegreerd cybersecurity-portfolio

Zo'n holistische aanpak is precies wat CGI zijn klanten biedt. Wereldwijd beschikken wij over een zeer uitgebreid portfolio cybersecurity-diensten. In combinatie met de kennis van de sectoren waarin we al decennia actief zijn, bieden wij een totaalaanbod van cybersecurity-oplossingen voor specifieke industrieën. We analyseren de informatiebeveiliging in de operationele omgeving, ontwerpen en ontwikkelen beveiligings- en beschermingsmaatregelen en implementeren defensieve oplossingen. Daarnaast trainen we de betrokken medewerkers van de organisatie, testen we alle getroffen maatregelen voor de beveiliging van de systemen en informatie en zorgen we voor het beheer en onderhoud ervan. Al deze diensten zijn gegroepeerd in de werkgebieden: Assess the Risk, Protect the Business en Operate with Confidence (zie hierboven).

CGI's Industrial Control Cybersecurity

Deze op maat gemaakte holistische dienstverlening voor het OT-domein noemen wij Industrial Control Cybersecurity (ICCS). ICCS houdt rekening met de verschillende eisen die gesteld zijn aan IT en OT, zoals Confidentiality, Integrity en Availability (de CIA-driehoek). In de wereld van Industrial Control Systems liggen die anders: Availability en Integrity zijn het belangrijkst en Confidentiality komt op de laatste plaats.
De gewone securitymiddelen voor Enterprise-IT voorzien hier niet in. Voor het PCD-domein zijn dus andere cybersecurity-oplossingen nodig die ook nog eens geïntegreerd kunnen worden in de security van de kantooromgeving. Juist hierin is CGI uniek. Bovendien beschikken we als enige partij voor de Europese markt over een Security Operation Center dat de cybersecurity van Enterprise-IT en OT geïntegreerd benadert.

Voor Industrial Control zijn dus andere cybersecurity-oplossingen nodig, die eveneens geïntegreerd kunnen worden in de security van de kantooromgeving

Opdrachtgevers en uitdagingen

- Voor een omvangrijke internationale voedsel-producent beoordeelde CGI de hele OT-organisatie en -techniek op professionalitiet. Hieruit is een advies voortgekomen voor de strategie voor de komende jaren.
- Voor een internationale bierbrouwer bepaalde CGI de corporate strategie voor ICCS en definieerde hiervoor ook het beleid.
- In de olie- en gasindustrie is CGI actief bij een van de grootste spelers op het gebied van ICCS. Momenteel werken professionals op de raffinaderijen en de offshore-installaties aan het ICCS-beleid. Daarnaast werken zij aan de implementatie van technische aspecten.
- Voor een toonaangevend staalconcern toetste CGI de professionaliteit van het ICCS-beleid. Daarnaast verzorgde CGI een op maat gemaakte workshop voor het ICCS-bewustzijn.

Toegevoegde waarde van ICCS en CGI

Met CGI's ICCS Global Center of Excellence stellen we raamwerken, templates voor richtlijnen en kennis beschikbaar voor alle medewerkers die zich specialiseren in ICCS. Zo komt er ook een schat aan wereldwijd opgebouwde kennis beschikbaar voor onze klanten.

Zetten we wereldwijd honderden experts in op het gebied van ICCS. CGI heeft het grootste aantal ICCS-experts ter wereld in dienst. Samen staan zij voor *deep local support, global wide reach*.

Bieden we een unieke combinatie van ICCS-expertise, inzicht in en kennis van de ICT-systemen in specifieke markten. En garanderen we de betrokkenheid van een groot aantal domeinexperts (bijvoorbeeld op het gebied van Manufacturing, Utilities, Olie en Gas, Health en Rail).

Werken we altijd met gecertificeerde professionals.

Hebben we geïntegreerde Security Operation Centers ICCS voor zowel Enterprise-IT als OT. We ondersteunen wereldwijd en lokaal. In Europa zijn we enige die zo'n expertisecenter heeft.

Helpen we organisaties inzicht te krijgen. Hoe professioneel is hun ICCS-beleid? Ook assiseren we bij de implementatie en letten daarbij op mensen, processen en technologie.

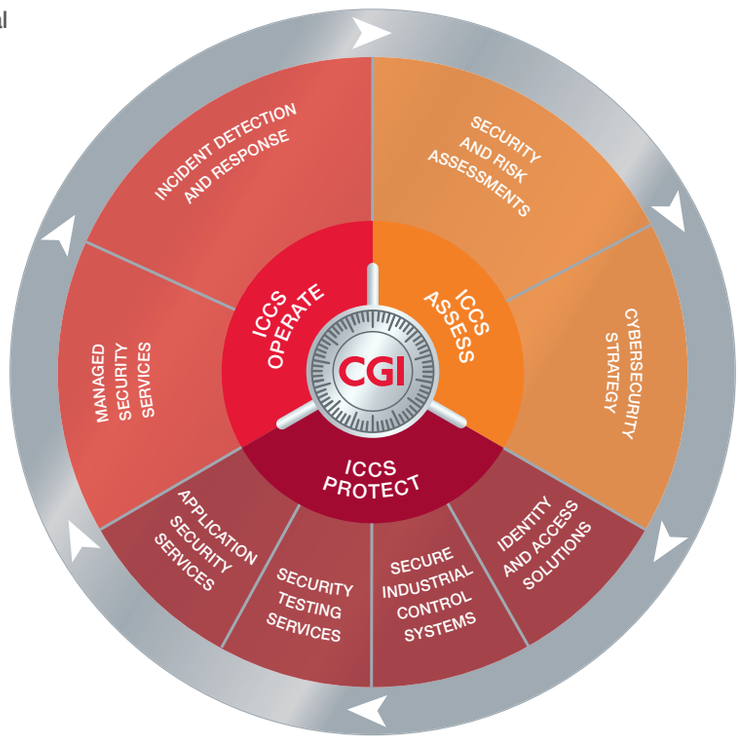
Hebben we te allen tijde geautomatiseerd inzicht in de ICT-topologie* en de gekoppelde productiecomponenten.

Beloven we 24/7/365-detectie, snelle terugkoppeling en daarmee minder kans op (gevolg)schade en sneller herstel.

* De topologie is de manier waarop bijvoorbeeld computers onderling met elkaar verbonden zijn.

Industrial Control Cybersecurity-oplossingen voor uw organisatie

Met ICCS biedt CGI een aantal hoogwaardige, concrete oplossingen voor de maakindustrie, transport- en nutssector, olie & gas en gezondheidszorg.



ICCS Assess

Onze assessmentaanpak geeft inzicht in de professionaliteit van het ICCS-beleid van de klant en de manier waarop dit geïmplementeerd is. Hier zetten we mensen, processen en technologie voor in. Het assessment bestaat onder meer uit interviews met een vaste structuur en een beoordelingssysteem. Daarnaast wordt een IT-gerichte topology-scan uitgevoerd, waarbij het dataverkeer van de lagen plant supervisory, direct control en fields level worden doorgelicht op cybercrime-gevoelige plekken. Wij sluiten daar speciale apparatuur voor aan in het live netwerk. Met de resultaten vande metingen maken wij een analyse en rapportage, aangevuld met een geautomatiseerde topology-tekening. Die laat zien welke assets in de OT-omgeving opgenomen zijn en waarmee zij verbonden zijn.

ICCS Protect

Framework voor Security Referentie Architectuur voor Secure by design

CGI beschikt over een uitgebreid framework om klanten te assisteren bij de Cybersecurity Referentie Architectuur. Dit biedt standaarden op gebied van onder meer System hardening, zonering, het inrichten van conduits et cetera. Het fundament van CGI's ICCS-aanpak is gebaseerd op publieke standaarden zoals ISA-99 en IEC 62443 enterprise control system integration, ISO 27002/17799 en NIST, aangevuld door de best practices opgedaan in de laatste 10 jaar. Aan de hand van het framework maakt CGI de IT- en OT-technologie van klanten Secure by design.

Training Global Industrial Cybersecurity Professional

CGI biedt klanten een training aan voor Global Industrial Cybersecurity Professional (GICSP). Na het succesvol afronden van het examen ontvangen deelnemers een in de markt erkend certificaat. De training bestaat uit tien avonden (eventueel via WebEx), een referentiebezoek en wordt afgesloten met een examen. Op dit moment heeft CGI het op één na hoogste aantal GICSP-gecertificeerde medewerkers ter wereld.

ICCS Operate

Geïntegreerde Security Operation Centers ICCS

In CGI's Security Operation Centers ICCS zijn de cybersecurity-diensten voor Enterprise-IT en het OT-domein geïntegreerd. Dit geeft een uitstekend totaalbeeld van eventuele bedreigingen en mogelijke verbindingen tussen verschillende bedreigingen. Zo kunnen we cyberbedreigingen ook van elkaar isoleren, zodat de kans op verspreiding van virussen nihil is. Ook niet-geautoriseerde opdrachten vanuit de kantooromgeving naar de OT-omgeving kunnen worden gedetecteerd en geblokkeerd. Een geïntegreerd Security Operation Center ICCS is ingericht op basis van de technologie van onze partners LogRythm en CyberBIT. LogRythm staat garant voor het IT- en OT-deel en de integratie. CyberBIT levert de ScadaSHIELD-technologie voor de beveiliging van de OT-omgeving.

24/7, 365 dagen

CGI maximaliseert de weerbaarheid (resilience) door een complete cybersecurity-dienstverlening, geleverd vanuit Security Operations Centers in diverse landen. Onze experts en systemen zijn 24 uur per dag actief, 7 dagen per week en 365 dagen in het jaar. We leveren onze services onder meer volgens SANS- en ITIL®-standaarden. Klanten kunnen vertrouwen op de expertise en daadkracht van specialisten met een volledige focus op cybersecurity en de bijbehorende kernactiviteiten. CGI werkt volgens een businessgerichte benadering en opereert onafhankelijk van leveranciers.

Experience the commitment

Waarom CGI?

- Effectieve ICCS-oplossingen, efficiënt geleverd via CGI's Defense in Depth-strategie.
- Inzicht in de kwetsbaarheden van systemen en diensten.
- Onafhankelijke detectie van bedreigingen waaraan de organisatie blootgesteld wordt.
- Beter in staat het hoofd te bieden aan cyberaanvallen.
- Sneller back in business na een eventueel geslaagde aanval.
- Goede governance van en compliance met bestaande wet- en regelgeving.
- Bescherming tegen financiële en reputatieschade, reëel gevaar voor de plant safety, de kans op fysieke schade en bedreiging van mensenlevens en het milieu.
- Lagere kosten en mindere complexiteit door outsourcen van informatiebeveiligingsactiviteiten.
- Werelwijde, geïntegreerde Security Operation Centers ICCS voor zowel IT als OT. We ondersteunen wereldwijd en lokaal.

Bewezen expertise:

- Everest Group (2016) positioneert CGI in het Major Contender-kwadrant – Service Provider Landscape with PEAK Matrix™ Assessment 2015 voor IT Security Services.
- Uitgeroepen tot marktleider in het Ovum-rapport: 'Ovum Decision Matrix: Het selecteren van een IT-OT integratiepartner, 2014-15' voor cybersecuritydiensten op het gebied van OT en IT.

Wilt u meer weten over cybersecurity van CGI, neem dan contact op met uw accountmanager of met CGI via:

T: +31 (0)88 564 0000
E: cybersecurity.nl@cgi.com

www.cginederland.nl/cybersecurity