ONDERZOEKSRAPPORT COMPETENTIES IACS SECURITY TEAMS

Nationaal Cyber Security Centrum

Onderzoeksrapport Competenties IACS Security Teams
Ralph Moonen
Sjoerd Peerlkamp
Bram Blaauwendraad
Version 1.0
18-11-2021

TLP-WIT

Secura B.V.
Vestdijk 59
5611 CA EINDHOVEN
Nederland

Karspeldreef 8
1101 CJ AMSTERDAM
Nederland

T +31 (0)88 888 31 00
E sales@secura.com
W secura.com

© Secura

INHOUDSOPGAVE

1. INTRODUCTIE

Cybersecurity, met name binnen Industriële Automatiserings- en Controle-Systemen (IACS, ook wel Operationele Technology of kortweg OT genaamd), wordt steeds meer het onderwerp van debat. Niet in de laatste plaats vanwege actieve aanvallen op industriële en kritieke systemen over de hele wereld en de potentiële schade die deze aanvallen kunnen veroorzaken.

In tegenstelling tot IT-netwerken die vaak veel volwassener zijn op security-vlak, zijn IACS-netwerken veel minder bestand tegen aanvallen. De gebruikelijke verdediging is daarom geworden om deze netwerken te segregeren van de IT-omgeving om ze zo te beschermen tegen blootstelling (aan het internet bijvoorbeeld), en dus tegen aanvallen. Naarmate IACS-netwerken volwassener worden en cybersecurity steeds belangrijker wordt in industriële netwerken, moeten de defensieve capaciteiten dat ook worden. Onbekend is echter welke verschillen er bestaan in organisatorische zin en welke specifieke aspecten van IACS-security teams hierbij van belang zijn.

Om deze reden heeft het Nationaal Cyber Security Centrum Secura verzocht een onderzoek uit te voeren naar de organisatievormen en competenties van IACS-security teams.

Door het ontbreken van aanbod van IACS cybersecurity experts (en de onbekendheid van de concrete behoefte aan de vraagkant van het personeelsbestand, bestaat het risico dat belangrijke vaardigheden ondervertegenwoordigd zijn in het personeelsbestand in Nederland. Dit heeft als gevolg dat organisaties grotere moeite hebben hun IACS-omgevingen adequaat te beveiligen tegen almaar groeiende dreigingen. Het is daarom belangrijk om helder te krijgen welke competenties en vaardigheden essentieel zijn voor (het functioneren van) een IACS-cybersecurity team. Hiertoe is de volgende hoofdvraag gedefinieerd:

“Wat zijn de belangrijkste competenties en vaardigheden voor personeel dat verantwoordelijk is voor de beveiliging van IACS binnen een organisatie, zowel individueel als in teamverband?”

Het onderzoek is in twee fases uitgevoerd. In fase 1 van dit onderzoek zijn de belangrijkste rollen en verantwoordelijkheden voor een efficiënt IACS-cybersecurity team geïdentificeerd. In fase 2 van dit onderzoek zijn interviews afgenomen met negen organisaties met een omvangrijke IACS-infrastructuur. In hoofdstuk drie wordt deze methode nader uitgelegd, terwijl de resultaten van fase 1 en 2 in respectievelijk hoofdstuk 4 en hoofdstuk 5 worden besproken. In hoofdstuk 6 worden onze conclusies gepresenteerd.

2. MANAGEMENTSAMENVATTING

Als resultaat van het onderzoek heeft Secura bevonden dat IACS-cybersecurity teams over het algemeen anders zijn georganiseerd dan IT-beveiligingsteams. Ook is naar voren gekomen dat de vereiste competenties moeilijk te vinden zijn in de arbeidsmarkt en grotendeels niet overeenkomen met academische curricula en het (commercieel) aanbod voor training en certificering.

OT-cybersecurity teams zijn over het algemeen minder gecentraliseerd binnen een organisatie dan IT-security teams, vanwege het feit dat binnen industriële omgevingen asset-eigenaren en fabrieksmanagers vaak primair verantwoordelijk zijn voor de beveiliging, en dit direct gekoppeld is aan fysieke processen en dus locatie-gebonden is. Cybersecurity wordt veelal gezien als een verlengstuk van veiligheid (een logisch gevolg van het belang van veiligheid in industriële besturingssystemen en fysieke processen).

Er zijn geen significante verschillen tussen sectoren vastgesteld met betrekking tot de organisatie en benodigde basiscompetenties van een IACS-cybersecurity team, hoewel meer volwassen organisaties, bijvoorbeeld in de olie- en gassector, over het algemeen grotere en meer centraal aangestuurde teams hedden.

Op het gebied van competenties rapporteerden alle geïnterviewde organisaties een gebrek aan beschikbaarheid van gekwalificeerd cybersecurity personeel. Omdat beveiligingskennis binnen IACS-omgevingenleverancier-specifiek is, worden de experts ook vaak bij deze leveranciers in dienst genomen, en niet zozeer bij de organisaties zelf. Dit betekent dat er een grote afhankelijkheid van die leveranciers is voor beveiligingskennis, hetgeen een potentieel problematische belangenconflict creëert.

Er wordt nu veelal intern opgeleid en capabel personeel wordt soms van de decentrale organisaties naar het hoofdkantoor gehaald, maar vooral voor de kleinere organisaties bestaat het gevaar dat deze mensen daarna snel de organisatie verlaten met hun nieuwe competenties. Ook kwam naar voren dat kennis van de primaire processen van een sector van belang is (veel meer dan bij IT), en dat competent IACS-securitypersoneel hierdoor binnen de ene sector niet vanzelfsprekend waarde kan toevoegen in de andere sector.

De meeste organisaties geven verder aan dat IACS-security nog in opbouw is. Er is (te) weinig focus en expertise, maar wel bewustwording dat dit nodig is en er worden stappen gezet. Het wordt ook steeds meer een directieonderwerp, wat helpt in het verkrijgen van de juiste mandaten en transparant risicomanagement. Samenwerken voor een kruisbestuiving van kennis binnen sectoren zou veel meerwaarde bieden, maar is lastig omdat bepaalde organisaties en hun problemen “one of a kind” zijn (of wordt althans zo gepercipieerd).

Er is grote behoefte aan kennis vanuit bijvoorbeeld het NCSC over daadwerkelijke dreigingen en Tactics, Techniques and Procedures (TTPs) van aanvallers, ter voorkoming van incidenten. De ene sector is hier al verder mee dan de andere. Vooral grote bedrijven zien ook leveranciers als zwakke schakel, en het afdwingen van standaarden om hun cybersecurity meetbaar op orde te krijgen zoals IEC62443 zou daarom van belang zijn.

3. METHODIEK

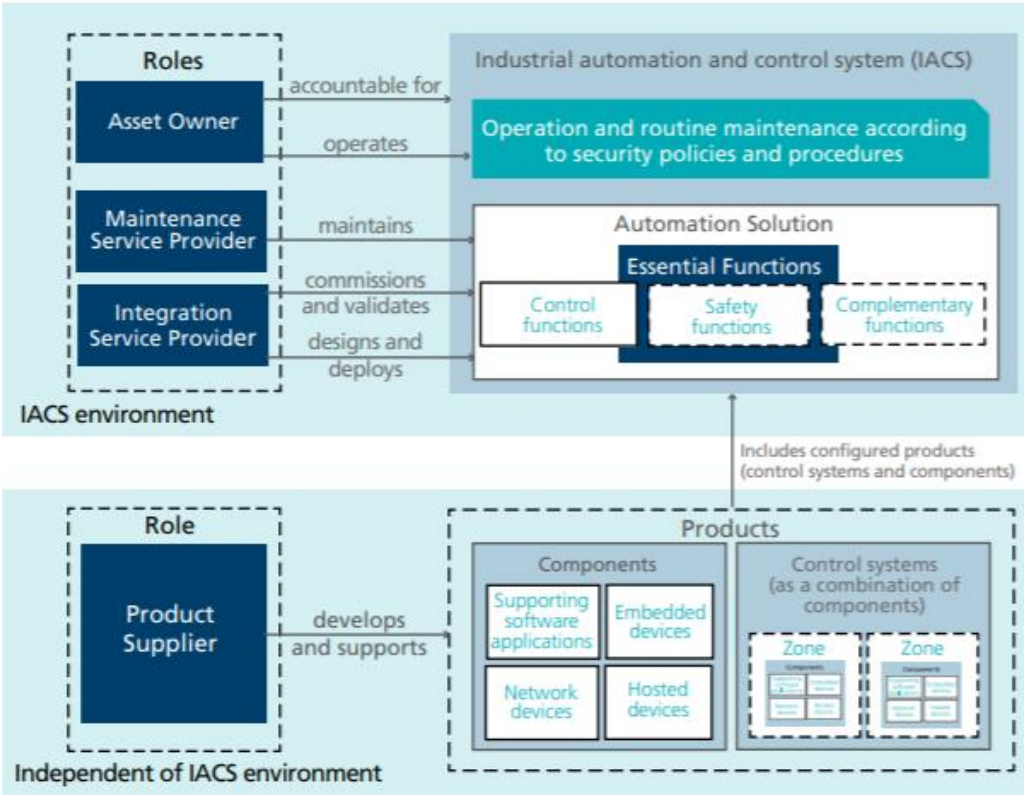
Het onderzoek is in twee fases uitgevoerd. In fase 1 van dit onderzoek zijn de belangrijkste rollen en verantwoordelijkheden voor een efficiënt IACS-cybersecurity team geïdentificeerd. Nederlandse, Europese en internationale standaarden en literatuur zijn geraadpleegd in deze fase.

Op basis van de literatuurstudie is gekozen om de theoretische analyse naar rollen uit te voeren door gebruik te maken van de levenscyclus van industriële assets uit de IEC62443 standaard, omdat verschillende rollen al worden benoemd in die standaard.

Het onderzoek heeft zich niet beperkt in termen van industriële marktsegmenten, maar is wel beperkt in termen van de rollen die een organisatie heeft. De IEC 62443 standaard definieert de belangrijkste rollen van een industriële organisatie als volgt:

- Asset Owner (de organisatie die eigenaar en operator is van de IACS-omgeving)
- Maintenance Service Provider (de organisatie die de IACS-omgeving onderhoudt)
- Integration Service Provider (de bouwer en integrator van de omgeving)
- Product Supplier (Vendor of verkoper van de componenten)

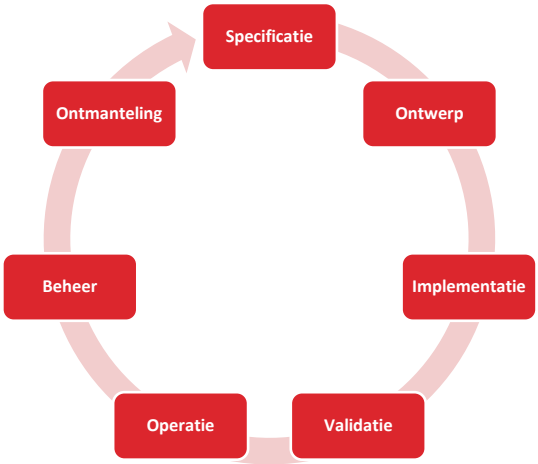
Ons onderzoek heeft zicht daarbij gericht op de rollen “Asset Owner” en “Maintenance Service Provider” omdat deze twee rollen vaak binnen organisaties aanwezig zijn. De verantwoordelijkheden van deze rollen op hoog niveau (niet noodzakelijkerwijs gerelateerd aan cybersecurity) in de levenscyclus van automatiseringsoplossingen worden weergegeven in *figuur 1*.



Figuur 1: IACS Rollen en Verantwoordelijkheden op hoofdlijnen

Hoewel de focus ligt op de teams die de IACS-omgeving exploiteren en onderhouden, zijn er ook verantwoordelijkheden op hoog niveau afgeleid voor andere afdelingen, bijvoorbeeld om de implementatie van een Information Security Management System (ISMS) te faciliteren.

Aan de hand van de levenscyclus van IACS-omgevingen is vervolgens gekeken naar de specifieke verantwoordelijkheden op cybersecurity-gebied.

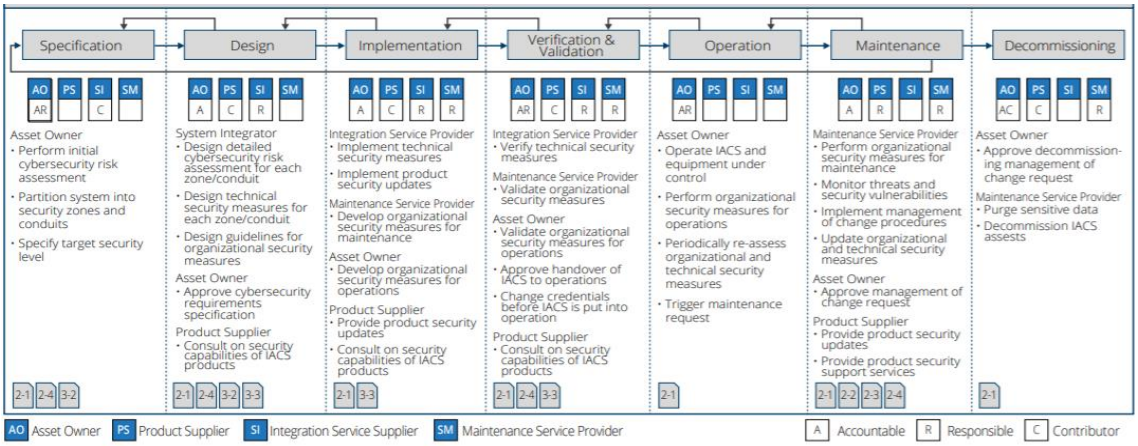


Figuur 2: Levenscyclus OT-systemen

Ook binnen cybersecurity bestaat een verdeling naar activiteiten, hiervoor is gekozen de internationaal geaccepteerde NIST Cybersecurity Framework te gebruiken. Deze onderkent vijf categorieën van activiteiten die allen relevant zijn voor IACS-cybersecurity teams.

Figuur 3: De vijf categorieën activiteiten uit het NIST Cybersecurity Framework

Vervolgens zijn deze activiteiten vergeleken met de security-verantwoordelijkheden zoals genoemd in de IEC62443 standaard:



Figuur 4: Cybersecurity verantwoordelijkheden per fase van de levenscyclus.

Het combineren van deze high-level rollen en verantwoordelijkheden in de diverse fases en activiteiten, resulteerde in een generieke opbouw van IACS-cybersecurity teams.

Vervolgens is deze (theoretische) analyse gevalideerd en verder onderzocht door het uitvoeren van fase 2 van het onderzoek, het veldonderzoek. In fase 2 zijn interviews afgenomen met negen organisaties met een omvangrijke IACS-infrastructuur. Deze bedrijven opereren in verschillende sectoren en hebben uiteenlopende primaire processen. De antwoorden op deze vragen zijn vervolgens vastgelegd in gespreksverslagen en onze conclusies zijn door hen geaccordeerd. Uit deze verslagen heeft Secura trends en afwijkingen gedestilleerd en conclusies getrokken, die geanonimiseerd in dit rapport zullen worden weergegeven.

De organisaties zijn gekozen op basis van de sectoren waarin zij actief zijn, en het nationale belang dat zij hebben. Dit onderzoek was gericht op organisaties met middelgrote tot grote IACS-omgevingen, die zeer afhankelijk zijn van de beschikbaarheid hiervan. Dit betekent dat niet alleen WBNI ‘Operators of Essential Services’ (OES) maar ook providers van niet-essentiële diensten die sterk afhankelijk zijn van IACS in het onderzoek zijn meegenomen. De sectoren die zijn geïnterviewd zijn:

- Olie en Gas
- Netbeheerders
- Transport
- Nucleair
- Infrastructuur
- Chemie

In alle gevallen zijn de eindverantwoordelijken voor security geïnterviewd, meestal was dit de CISO (Chief Information Security Officer). De besproken onderwerpen volgden daarbij de onderzoeksvragen zoals door het NCSC gedefinieerd. De individuele verslagen zijn uitgeschreven en aan de geïnterviewden ter goedkeuring en becommentariëring voorgelegd.

In verband met de vertrouwelijkheid van de gesprekken zijn de volgende afspraken gemaakt met de geïnterviewden:

- Het NCSC of een andere partij krijgt geen toegang tot de directe gesprekverslagen van de interviews. Alleen onherleidbare conclusies worden met het NCSC gedeeld.
- De gespreksverslagen zullen na afronding van het onderzoek worden vernietigd.
- Persoonsgegevens worden door Secura verwerkt in overeenstemming met de AVG.
- Deelnemers ontvangen het onderzoeksrapport van Secura.

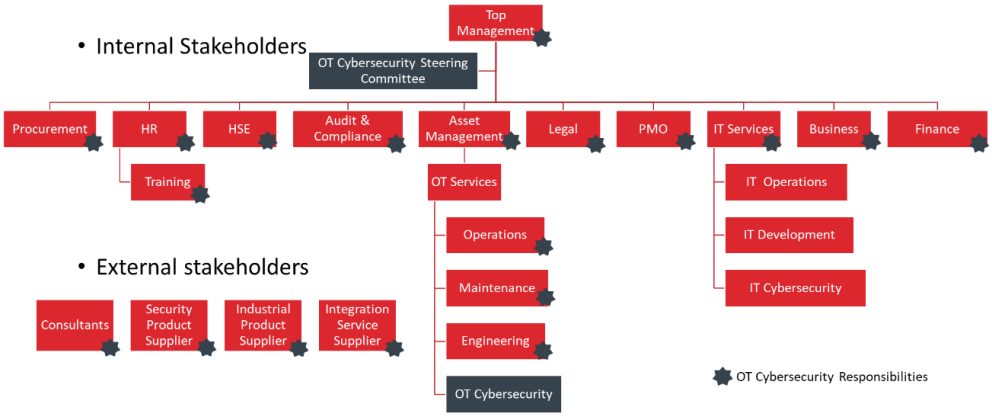
De interviews leverden een veelzijdig beeld op van de organisatiegraad en volwassenheid van de IACS-cybersecurity teams. In de volgende hoofdstukken zullen de resultaten van de twee fases van het onderzoek worden gepresenteerd, gevolgd door de conclusies.

4. FASE I: IDENTIFICATIE VAN IACS ROLLEN EN VERANTWOORDELIJKHEDEN

De focus van deze fase lag op het uitwerken van een IACS-specifieke taxonomie die het mogelijk maakt om op een systematische manier rollen en verantwoordelijkheden van een IACS-cybersecurity team af te leiden. Daarnaast worden ook de IACS-cyberbeveiligingsverantwoordelijkheden van de belangrijkste afdelingen waaruit een organisatie bestaat afgeleid, mede gegeven het belang van een holistische benadering van IACS-cyberbeveiliging.

4.1. Verantwoordelijkheden op afdelingsniveau

Een "Asset Owner" die IACS-cyberbeveiliging integreert in zijn technische teams, het middenmanagement en in de besluitvormingsprocessen op het hoogste niveau, heeft duidelijk gedefinieerde verantwoordelijkheden voor elke interne en externe belanghebbenden, zie figuur 2.



*Figuur 5: Belanghebbenden binnen een organisatie met profiel "*Asset Owner"

Onderstaand zijn de belangrijkste belanghebbenden en hun rol in de IACS-security uitgewerkt:

Het **Top Management** houdt zich bezig met strategie en planning, betrekt risicobeheersing hierbij en is eindverantwoordelijk voor het beleid.

Top Management:

- Stelt strategie en jaarplannen op voor IACS-cyberbeveiliging in de hele organisatie.
- Zorgt ervoor dat cyber risico's onderdeel van het beslisproces zijn.
- Is eindverantwoordelijk voor risicobeheersing.
- Voorziet in bedrijfsmiddelen (financieel, personeel, etc.) die nodig zijn om de cyber risico's binnen acceptabele grenzen te houden.
- Geeft formele goedkeuring aan het cybersecurity beleid.

OT Cybersecurity stuurgroep:

- Bevat een representant van iedere relevante afdeling.
- Adviseert Top Management (OT CISO).
- Overlegt over IACS-cybersecurity onderwerpen met algemene relevantie.
- Draagt bij aan het IACS-security beleid.
- Keurt risico-acceptatiecriteria goed.

Asset Management (beheerder van bedrijfsmiddelen):

- Is eigenaar van de bedrijfsmiddelen.
- Verantwoordelijk voor de levenscyclus van middelen van inkoop tot afvoer.
- Verantwoordelijk voor het definiëren van de minimale beveiligingseisen voor bedrijfsmiddelen.
- Classificeert/rubriceert informatie en middelen volgens het classificatieschema.

OT Services:

- **Operations** dient zich bewust te zijn van cyberdreigingen, en borgt best-practices in hun dagelijkse takenpakket. Zij zijn vaak het eerste aanspreekpunt voor incident respons en herstel van diensten.
- **Beheerteam** zorgt ervoor dat beveiligingsmaatregelen efficiënt blijven werken. Dit impliceert regelmatige hardware, software en besturingssysteem updates volgens de adviezen van industriële en security vendoren.
- **Engineering** is verantwoordelijk voor de security configuratie van de diverse componenten en bedrijfsmiddelen.
- **IACS-Cybersecurity Team** draagt de verantwoordelijkheid voor een robuust en gelaagd defensieplan door het bedenken, implementeren, monitoren en optimaliseren van een degelijk netwerk- en systeemarchitectuur in alle fases van de levenscyclus van IACS-omgevingen. Dit team ondersteunt ook de technische verantwoordelijkheden en kennis van de andere afdelingen (met uitzondering van de IT-diensten).

4.2. Verantwoordelijkheden van het IACS-cybersecurity team

De verantwoordelijkheden van het IACS-cybersecurity team kunnen worden weergegeven aan de hand van de fases van de levenscyclus van IACS-omgevingen (zie figuur 2):

Specificatiefase:

- Uitvoeren van de initiële risicoanalyse.
- Specificatie van de technische beveiligingsfunctionaliteiten van de OT-oplossing.
- Selectie van technische beveiligingsmaatregelen.
- Bepalen van beoogde volwassenheidsniveau van iedere beveiligingsmaatregel.

Ontwerpfase

- Goedkeuren van cybersecurity oplossingen.
- Goedkeuren cybersecurity high-level en low-level ontwerpen.
- Goedkeuren cybersecurity richtlijnen en organisatie.

Implementatiefase

- Ontwikkelen van organisatorische beveiligingsmaatregelen voor Operations.
- Ontwikkelen van organisatorische beveiligingsmaatregelen voor Beheer.

Validatiefase

- Valideren en goedkeuren van technische cybersecurity maatregelen ten behoeve van inproductiename door Operations.
- Valideren en goedkeuren van organisatorische cybersecurity maatregelen ten behoeve van inproductiename door Operations.
- Valideren en goedkeuren van organisatorische cybersecurity maatregelen ten behoeve van het Beheerproces.
- Wijzigen van attributen voor logische toegangsbeveiliging (accounts, wachtwoorden, certificaten etc.).

Operationele fase

- Uitvoeren van technische beveiligingsmaatregelen.
- Uitvoeren van organisatorische cybersecurity maatregelen voor Operations.
- Toetsing van technische en organisatorische beveiligingsmaatregelen.

Beheerfase

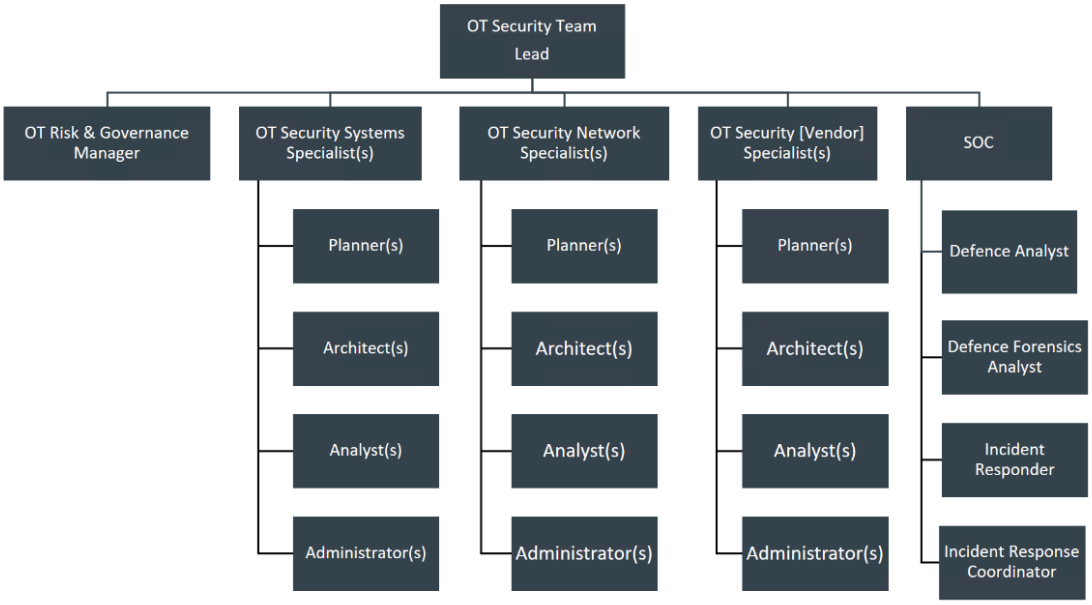
- Goedkeuren beheeractiviteiten.
- Uitvoeren organisatorische cybersecurity matregelen voor beheer.
- Monitoren van bedreigingen en kwetsbaarheden.
- Implementeren van beheerprocedures.
- Periodiek review en onderhoud van de organisatorische en technische maatregelen.

Ontmantelingsfase

- Goedkeuren van ontmanteling.
- Verwijderen gevoelige data.
- Verwerking van middelen (destructief, afvloeiing).

4.3. Rollen binnen het IACS-cybersecurity team

De analyse van de bovenstaande afdelingen en rollen is naast de functies gelegd (zie appendices). Dit levert een generiek beeld van de structuur van een volwassen IACS-cybersecurity organisatie, waaruit de volgende rollen naar voren komen:



Figuur 6: Afgeleide rollen binnen volwassen IACS-cybersecurity teams

Voor het doel van dit onderzoek is de volwassenheid van een IACS-cybersecurity organisatie gedefinieerd als de mate waarin de bovenstaande structuur en rollen zijn doorgevoerd of worden onderkend, tezamen met de mogelijkheden voor opleiding en training.

5. FASE II: INTERVIEWS

In deze fase van dit onderzoek zijn interviews afgenomen met negen organisaties met een omvangrijke OT-infrastructuur. Deze bedrijven opereren in verschillende sectoren en hebben uiteenlopende primaire processen. De antwoorden op deze vragen zijn vervolgens vastgelegd in gespreksverslagen en onze conclusies zijn door hen geaccordeerd. Uit deze verslagen heeft Secura trends en afwijkingen gedestilleerd en conclusies getrokken, die in dit hoofdstuk zijn uitgewerkt.

In de aanvraag van het NCSC was een hoofdvraag geformuleerd:

"Wat zijn de belangrijkste competenties en vaardigheden voor personeel dat verantwoordelijk is voor de beveiliging van IACS binnen een organisatie, zowel individueel als in teamverband?"

Ook is een aantal deelvragen geformuleerd:

1. **Hoe ziet de rolverdeling binnen een IACS-securityteam eruit? Welke taken kunnen van elkaar worden onderscheiden?**
2. **Welke competenties worden door het individu en het team aangeduid als meest waardevol?**
3. **Welke mogelijkheden bestaan er om competenties binnen het team onder te verdelen?**
4. **Op welke competenties en vaardigheden is de grootste schaarste?**
5. **Hoe zien organisaties het huidige aanbod om teamleden de juiste competenties te leren in Nederland?**

Secura heeft hiernaast ook beperkt naar de volgende aspecten gekeken:

1. **Bestaat er verschil in invulling van een IACS-securityteam tussen marktgroepen (bijv. tussen critical infra, Oil&Gas, Chemical of andere markten)?**
2. **Welke competenties kunnen worden uitbesteedt of ingekocht?**
3. **Welke informatiebronnen heeft het IACS-securityteam nodig om efficiënt te kunnen opereren?**
4. **Welke governance structuur en mandaten heeft een dergelijk team nodig om effectief te kunnen zijn?**

In de interviews zijn deze onderwerpen besproken, en later aan de hand van de verslagen, met elkaar vergeleken. In de navolgende hoofdstukken zijn de resultaten van deze gesprekken geanonimiseerd weergegeven.

5.1. Organisatievormen IACS-cybersecurity teams

Bij de organisatievormen zijn met name twee aspecten bekeken: de governance, en de uitvoerende verantwoordelijkheid.

De governance van IACS-cybersecurity wordt binnen de verschillende organisaties op twee manieren belegd: centraal of decentraal. In beide situaties is een centrale rol aanwezig die bedrijfsbreed governance en risicomanagement doet, de CSO/CTO/CISO. Er lijkt geen verband te zijn tussen de sector en het centraal of decentraal beleggen van IACS-cybersecurity verantwoordelijkheid.

Bij een centraal belegde verantwoordelijkheid is er een centraal expertise-team dat binnen het bedrijf ingezet kan worden. Deze geven advies, stellen algemeen beleid op en ontwerpen de opzet van IACS-cybersecurity. Vaak worden plannen op locatie bij de assets nog op maat gemaakt, binnen de regels en eisen gesteld door het centrale team. Dit stelt de organisatie in staat om mankracht flexibeler in te zetten en vaktechnische ontwikkelingen makkelijker te organiseren, maar zicht op de werkvloer is minder en de kwaliteit van de implementatie bij de assets is erg afhankelijk van de relaties.

Het tweede scenario komt aanzienlijk minder voor in de praktijk. Hierbij wordt de governance van de IACS-cybersecurity decentraal belegd en liggen de beleids- en kaderstellende functies centraal. Dit blijkt in de praktijk lastig omdat veel asset managers niet de kennis en capaciteit in huis hebben om IACS-cybersecurity adequaat in te richten. Een aantal organisaties gaf ook aan dat de decentrale organisatieonderdelen (bijvoorbeeld een fabriek of chemische plant) op zichzelf vaak niet genoeg te bieden hebben (in termen van functie, beloning, carrière en trainingsmogelijkheden) voor experts op zowel IACS- als security-gebied. Dit maakt opleidingen (zowel intern als extern) aanbieden ook minder aantrekkelijk, gezien er een grote kans is dat de werknemers daarna vertrekken (bijvoorbeeld naar functies bij vendoren). Dit is een nadeel van het decentrale model. Een voordeel van decentrale inrichting is echter dat de primaire processen beter bekend zijn en vaak ook specifiek voor die locatie or fabriek/plant.

De uitvoerende verantwoordelijkheid voor cybersecurity is aan de andere kant vaak wel decentraal belegd. De plant-manager die veelal uit de operationele organisatie komt, is vaak het meest bekend met de technologie, en sowieso al verantwoordelijk voor de veiligheid en fysieke beveiliging van de fabriek of plant. Alleen bij organisaties met een hoger volwassenheidsniveau of een zeer klein aantal fysieke locaties, is ook de uitvoerende verantwoordelijkheid centraal belegd. De rollen van de benodigde technisch experts kunnen centraal of decentraal belegd zijn, maar in beide gevallen worden ze geplaatst binnen een organisatieonderdeel (bijvoorbeeld finance, HR of anders).

Enkele geïnterviewden gaven aan dat de IACS-omgeving zodanig gescheiden was van de IT-omgeving, dat geen gebruik gemaakt kon worden van de IT-competenties binnen de organisatie. Anderen gaven aan dat er wel gebruik gemaakt werd van de IT-beveiligingscompetenties, althans tot op het koppelvlak van IT en OT (bijvoorbeeld voor het beheer van de firewalls).

In vrijwel alle gevallen werden delen van de IACS-cybersecurity organisatie extern belegd (door inkoop van bepaalde diensten zoals monitoring), of ontbraken deze (deels). Lang niet alle geïnterviewde partijen hadden bijvoorbeeld een OT-Security Operations Center (SOC). Als delen extern belegd werden, was dat voornamelijk bij de vendor van de IACS-systemen, of ten behoeve van monitoring door het interne SOC. Uit de interviews bleek dat dit voornamelijk veroorzaakt werd door de onvolwassenheid van het nieuwe domein IACS-cybersecurity.

Ten slotte werd door verschillende geïnterviewden gemeld dat de bewustwording van de cybersecurity risico's snel groeit en het steeds meer een onderwerp voor de directie wordt. Dit blijkt uit vragen die aan de teams worden gesteld vanuit het hoger management, maar ook uit de toenemende mogelijkheden voor cybersecurity activiteiten zoals interne penetratietests en red-team exercities. Toch hebben de meesten het gevoel dat IACS-cybersecurity nog in de kinderschoenen staat en achterloopt bij de daadwerkelijke bedreigingen. Geïnterviewden geven bijvoorbeeld aan dat het onderwerp pas in de laatste twee jaar überhaupt aandacht heeft gekregen en dat rollen nog in ontwikkeling zijn (inclusief de bijbehorende functieomschrijvingen). En aan de technische kant is bijvoorbeeld de detectie- en respons veelal niet uitgekristalliseerd. Van een echt SOC is soms al geen sprake, laat staan een OT-gericht SOC.

5.2. Meest waardevolle competenties

Alle partijen gaven aan dat kennis van de primaire bedrijfsprocessen in IACS-omgevingen veel belangrijker is dan in de IT-omgeving. Zo is ook veelvuldig genoemd dat iemand die bij de ene organisatie de IACS-security heeft beheerd niet direct aan de slag kan bij de andere. Denk hierbij aan een expert in IACS-security bij een spoorwegmaatschappij, die altijd aan treinsignalering heeft gewerkt. Deze persoon kan een groot deel van deze kennis niet direct toepassen in de energiesector. In sectoren waar sprake is van een monopolie of genationaliseerde organisatie (denk aan delen van de kritieke infrastructuur) speelt dit aspect nog veel sterker. Ervaring opdoen kan dan immers alleen in die

organisatie plaatsvinden, of eventueel in het buitenland. Specifieke cybersecurity opleidingen en trainingen voor deze sectoren ontbreken dan ook.

De meest waardevolle competentie die door alle partijen wordt genoemd is overal ongeveer hetzelfde: iemand die security risico's in de IACS-omgeving op waarde kan schatten en genoeg expertise heeft om deze naar een bedrijfsrisico te vertalen en in een handelingsperspectief kan voorzien.

Ook hier wordt het als zeer belangrijk gezien dat deze persoon kennis heeft van de primaire bedrijfsprocessen (bijvoorbeeld gaswinning, energiedistributie, chemie of transport) en begrijpt dat de risico's en belangen anders zijn in een IACS-omgeving versus een IT-omgeving. Opvallend is dus dat hier niet zozeer technische competenties (bijvoorbeeld specifiek netwerkkennis, OS of protocollen) worden genoemd zoals je bij IT-omgevingen wel verwacht. Ook interessant is dat deze vaardigheid niet expliciet uit de analyse in fase 1 is gebleken. In het overzicht van rollen uit fase 1 is het te verwachten dat deze vaardigheid het dichts ligt tegen de functie van de OT-security Team Lead.

Architecten werden tijdens de interviews ook genoemd als zeer waardevol, omdat deze bij uitstek in staat zijn om cybersecurity mee te nemen in de ontwerpfase. Daardoor kan het nemen van achteraf lastig te implementeren maatregelen worden voorkomen. Typisch zullen dit senioren technici zijn, die zich hebben verdiept in cybersecurity.

Omdat beveiligingskennis binnen IACS-omgevingen vaak leverancier-specifiek is, worden de experts ook vaak bij deze leveranciers (bijvoorbeeld Siemens, Yokogawa of Rockwell) in dienst genomen, en niet zozeer bij de organisaties zelf. Dit is onder meer omdat sommige communicatieprotocollen geen open standaarden zijn, en de programmeeromgevingen van o.a. PLC's veelal ook product-specifiek zijn. Dit betekent dat er een grote afhankelijkheid van die leveranciers is voor technische beveiligingskennis van de componenten binnen een IACS-omgeving, hetgeen een potentieel problematische belangenconflict creëert. Immers, de leverancier is vaak ook (deels) verantwoordelijk voor de implementatie. Daarnaast heeft de leverancier vaak alleen kennis van de eigen systemen terwijl omgevingen ook apparatuur van andere leveranciers omvat.

Andere competenties op technisch vlak zoals testers, red-team leden of threat hunters, worden als minder belangrijk beschouwd omdat deze efficiënter kunnen worden ingehuurd bij externe service providers.

5.3. Mogelijkheden om taken te verdelen

De omvang van het IACS-cybersecurity team bleek in veel gevallen zeer beperkt te zijn, soms maar een of twee personen. Sommige (vooral grotere) organisaties zagen het beschreven takenpakket als te groot voor een enkel persoon, andere organisatie hadden nog niet overwogen hierin een verdere splitsing aan te brengen. Enkele geïnterviewden geven daarbij ook aan dat men nog helemaal niet denkt in termen van rollen, omdat er sowieso slechts enkele mensen met het onderwerp bekend zijn. Aan de andere kant zijn bij bijvoorbeeld de grotere organisaties in onder andere de Olie en Gas industrie, deze rollen wel veel meer afzonderlijk ingevuld.

Over het algemeen werden twee type werknemers geïdentificeerd die geschikt zijn voor deze rollen: iemand die het risico bepaalt en handelingsperspectief biedt is vaak iemand met een technische achtergrond (bijvoorbeeld een elektrotechnisch ingenieur) die zich ook interesseert voor security. Deze persoon zou dan samenwerken met een werknemer met zowel technisch inhoudelijk kennis omtrent cybersecurity als affiniteit voor bedrijfsvoering. Samen zouden deze twee een concrete vertaalslag kunnen maken van een technisch risico naar een concrete impact op de bedrijfsvoering. De security expert zou eventueel deze rol alleen in kunnen vullen zodra er genoeg kennis is opgedaan van het primaire proces.

5.4. Schaarste competenties

De geïnterviewde organisaties geven aan dat personen met bovengenoemde competenties lastig te vinden zijn, vooral voor de kleinere organisaties. De kleinere organisatie hebben minder te bieden (in termen van functie, beloning, carrière en trainingsmogelijkheden) voor experts op zowel IACS- als security-gebied. Hiernaast is het aantal mensen met de juiste competenties beperkt, gezien het in OT-omgevingen draait om competenties met betrekking tot de primaire processen. Deze kennis is zeer specialistisch en wordt voornamelijk opgedaan door hoge opleidingsgraad of werkervaring.

Wanneer gevraagd welk type persoon het moeilijkst te vinden is antwoorden de organisaties unaniem dat het dan ging om iemand met een zeer technische achtergrond die zich later is gaan verdiepen in security (bijvoorbeeld in de rol van architect). Security specialisten zijn ook schaars, maar vooral voor de grote bedrijven wel vindbaar.

5.5. Aanbod om competenties te leren

Het is voor veel organisaties eenvoudiger om iemand die al kennis heeft van de primaire processen van een bedrijf bij te scholen in security dan andersom. Sommige organisaties gaven aan in de interviews dat daarom veelbelovende kandidaten van de decentrale locaties naar het centrale team gehaald worden en een opleiding in cybersecurity aangeboden krijgen om zo kennis op te doen van zowel de primaire processen als security.

Er is een klein aantal succesvolle trainingen genoemd in de interviews, zoals SANS ICS410. De Red Team Blue Team trainingen zoals ENCS die geeft worden gewaardeerd omdat het veel meer hands-on is dan bijvoorbeeld een CISSP-certificering en ook voor beheerders een goede inkijk in cybersecurity geeft. De IEC 62443 trainingen worden vaak als te droog gezien en te weinig praktisch, hoewel de standaard zelf wel als waardevol wordt bestempeld.

Op hogescholen en universiteiten bestaat nog zeer weinig aandacht voor IACS-cybersecurity, zelfs binnen vakgroepen met een cybersecurity specialisatie. Het is daarom ook lastig voor bedrijven om afstudeerders of pas afgestudeerden te vinden die zich verder willen ontwikkelen op IACS-cybersecurity gebied.

Kennis op het gebied van IACS-cybersecurity is vaak niet effectief extern te ontwikkelen. Dit is ook niet gewenst in sommige situaties, gezien de gevoeligheid van de informatie (denk aan de nucleaire sector). In de praktijk is het nog veelal “learning by doing/training on the job”. Hier moet wel vermeld worden dat er grote verschillen zijn in de mate van volwassenheid op dit gebied. Vooral bedrijven die zijn aangemerkt als het leveren van maatschappelijk kritieke diensten zijn hier al veel verder in.

Dit uit zich voornamelijk met hoe ver men is met certificering van werknemers, maar ook met kennisdeling onderling. Kruisbestuiving van kennis tussen aanverwante sectoren kan erg veel bijdragen maar gebeurt nog niet in elke sector. Het valt immers te verwachten dat de diverse energiebedrijven tegen soortgelijke problemen aanlopen op OT-gebied. Kruisbestuiving is vooral onderontwikkeld in sectoren met weinig spelers zoals publiek transport. Zo zijn in Nederland maar weinig grote spoorwegmaatschappijen. Dit weerhoudt ze nog niet van informatie uitwisselen met soortgelijke organisaties of kennis internationaal te zoeken, maar dit gebeurt nog weinig in de praktijk.

De meeste bedrijven nemen wel deel aan ISAC’s (Information Sharing and Analysis Center) en vinden dat waardevol. Echter, de onderwerpen van gesprek zijn meer IT- dan OT gerelateerd..

5.6. Advies aan NCSC

Vooral de grotere organisaties zien leveranciers als zwakke schakel. Hoewel leveranciers de technische kennis hebben van de producten die ze verkopen ontbreekt het hen aan informatie over echte dreigingen. Ze weten weinig van het dreigingslandschap en het zou de digitale weerbaarheid ten goede komen als het NCSC meer diepgaande analyses, dreigingsbeelden en de TTPs van actoren binnen het OT-gebied zou verschaffen.

Ook het stimuleren van standaarden binnen de OT-omgeving zoals de IEC62443 zou kunnen bijdragen aan de weerbaarheid van deze organisaties en de meetbaarheid daarvan. Kleinere partijen kunnen voordeel ondervinden van hapklare methoden om deze standaarden toe te passen, gezien ze zelf niet veel OT-security kennis in huis hebben. Ook op het gebied van kruisbestuiving zien de organisaties voor het NCSC een actieve rol. Zij kunnen partijen binnen verwante sectoren stimuleren om samen te werken binnen een vertrouwde omgeving zoals de ISAC's.

6. CONCLUSIES

De voornaamste conclusies van het onderzoek kunnen als volgt worden samengevat:

De organisatie en inbedding van IACS-cybersecurity teams staat veelal in de kinderschoenen. Het volwassenheidsniveau (in termen van organisatiestructuur, invulling van rollen, opleidingen, etc.) en weerbaarheid (preventie, detectie, respons) is in IT-omgevingen veel hoger. Daar waar IT-security teams vaak centraal zijn georganiseerd, is dit binnen IACS-cybersecurity vaak decentraal, afhankelijk van de fysieke locatie en de primaire processen ter plekke.

Het theoretische model van rollen en taken dat in fase 1 is uitgewerkt, blijkt in de praktijk niet erg expliciet te worden ingevuld, meestal omdat de teams te klein zijn om deze rollen te onderkennen en ze daarom vaak gecombineerd worden in een persoon. Daarnaast is de belangrijkste genoemde competentie, namelijk het kunnen communiceren van IACS-cybersecurityrisico's naar hoger management, niet direct terug te voeren op het theoretische model.

De benodigde competenties zijn verder zeer schaars en de opleidingen (zowel academisch als commercieel) sluiten niet aan bij de vraag. De meest waardevolle competenties hebben te maken met domeinkennis van het primaire proces en het kunnen inschatten van het business-risico en vertaling daarvan naar handelingsperspectief, en niet zozeer met technische kennis op het gebied van cybersecurity.

Hoewel er tussen bedrijven wel degelijk verschillen bestaan in de organisatorische invulling van IACS-cybersecurity, zijn de organisatorische verschillen niet zozeer sector-afhankelijk. Wel is de specifieke domeinkennis sector-afhankelijk: IACS-specialisten in de transportsector zullen niet noodzakelijkerwijs hun kennis en ervaring direct in kunnen zetten in de chemische sector. Er wordt veel gesteund op externe kennis en ervaring. Enerzijds van vendoren van IACS-apparatuur (Siemens, Bosch, Yokogawa etc.) en anderzijds van leveranciers van beveiligingsdiensten (bijv. red-teaming, pentesting, certificering en SOC/monitoring).

Het NCSC kan meerwaarde toevoegen in dit veld door standaarden te stimuleren en zo de digitale veiligheid en de meetbaarheid daarvan te verhogen. Er is ook duidelijk een behoefte naar diepgaande analyses, dreigingsbeelden en de TTPs van actoren binnen het OT gebied. Ook kan het NCSC partijen met grote OT omgevingen binnen verwante sectoren stimuleren om samen te werken binnen een vertrouwde omgeving zoals de ISAC's.

APPENDIX A: GERAADPLEEGDE LITERATUUR

De volgende bronnen zijn in dit onderzoek gebruikt:

6.1. Nederlandse Bronnen

- TNO - Improving Human Capital for SOCs And CSIRTs
- Beroepsprofielen Informatie beveiliging 2.0 - Een basis voor uniforme kwalificatie van informatiebeveiligers
- NTA 8120 - Assetmanagement - Eisen aan een veiligheids-, kwaliteits- en capaciteitsmanagementsysteem voor het elektriciteits- en gasnetbeheer

6.2. Europese bronnen

- Cybersecurity Skills Development in the EU
- EU Cybersecurity Education Database
- Certification of Cyber Security skills of ICS/SCADA professionals
- European e-Competence Framework 3.0 (CEN)
- ENISA service list
- Step-by-Step Approach on how to set up a CSIRT

6.3. Internationale bronnen

- ISO 27021: Competences for ISMS professionals
- Security Lifecycles in the ISA/IEC 62443 Series
- NIST SP 800-181: NIST National Initiative For Cybersecurity Education (NICE)

APPENDIX B: PHASE 1 DETAILS

The focus of this phase is the elaboration of an IACS-specific taxonomy that allows deriving roles and responsibilities of an OT Cybersecurity team in a systematic way.

In addition, OT cybersecurity responsibilities of the main departments that an asset owner is comprised of are also provided to highlight the importance of treating OT cybersecurity holistically in an organization.

6.4. Department-level Responsibilities

An asset owner that incorporates OT cybersecurity in its technical teams, mid-management, as well as in top-level decision processes, has clearly defined responsibilities for each internal and external stakeholder, Figure *2*.

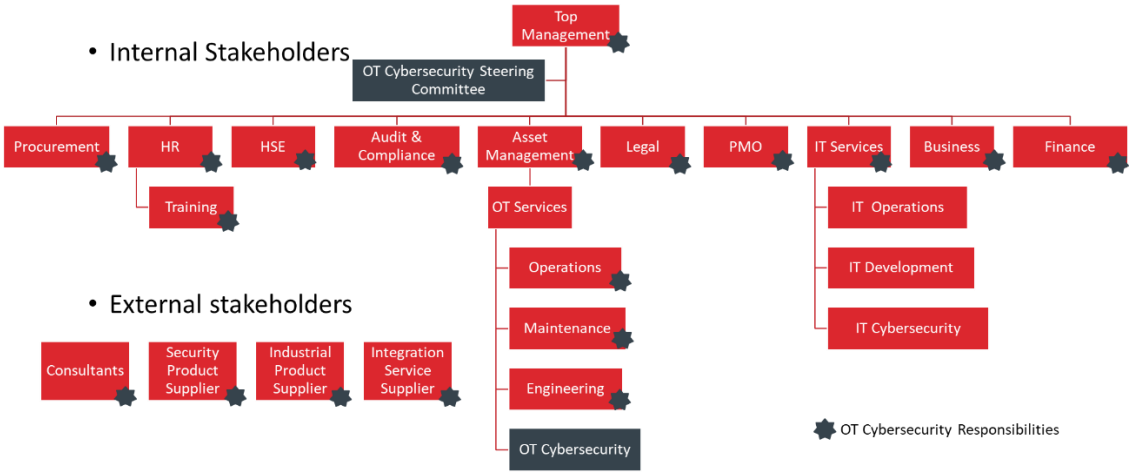


Figure 2: Stakeholders of an Asset Owner

Top Management:

- Sets strategy, and year plans for OT cybersecurity across the organization
- Ensures OT cyber risks are part of business decision processes
- Overall accountability for risk management
- Ensures resources (human, financial, etc.) to maintain cyber risks at acceptable level
- Signs-off OT cybersecurity policies

OT Cybersecurity Steering Committee:

- Includes a representative from each department
- Advisory body to Top Management (OT CISO)
- Discusses OT cybersecurity topics relevant to all departments
- Reviews and contributes to OT security policies
- Approves risk acceptance criteria

Procurement:

- Ensures minimum OT cybersecurity capabilities are included in tender documentation
- Assess OT suppliers and OT supply chain(s) from the cybersecurity perspective

HR:

- Ensures cybersecurity in the employee lifecycle
  - Hiring (e.g., background checking)

- During Employment (e.g., training and awareness programs)
- Contract termination (e.g., removal of privileges)

- Specific responsibilities for training and awareness programs:
  - Curriculum Development
  - Knowledge Management
  - Content delivery

HSE ensures proper use of funds allocated to OT cybersecurity activities.

Audit & Compliance is responsible for internal OT cybersecurity audits and meeting compliance regulations.

Legal is responsible for establishing legal conditions in services and product contracts (e.g., penalties for unavailability of outsourced OT SOC).

Asset Management:

- Owns the assets, which are among the most critical (and expensive) elements of an OT company.
- Accountable for the Asset Lifecycle management, from acquisition to disposal
- Accountable for defining minimum OT cybersecurity requirements for each asset.
- Classifies assets and the information processed by them according to the organization classification scheme.

Project Management Office (PMO) ensures that projects take OT cybersecurity into account at various levels (technical, legal, safety, etc.). PMO interacts and relies on other departments for the implementation of security requirements at different levels.

IT Services ensures cybersecurity of the corporate environment is properly planned, implemented, monitored and optimized.

Business is responsible for business continuity planning. It should include OT security threats in its BCP and DRP.

Finance ensures proper use of funds allocated to OT security activities.

OT Services:

- **Operations** shall be highly aware of cyber threats, and embed security best practices in their routine functions. They are often the first link for incident response plans, as well as for restoring services.
- **Maintenance** ensures that security controls are efficient throughout time. This implies regular OS, SW and HW updates in alignment with industrial and security vendors.
- **Engineering** ensures that the various systems and assets that comprise the automation solution are properly configured for the security point of view.
- **OT Cybersecurity Team** ensures that a robust defence-in-depth is in place by planning, implementing, monitoring and optimizing a proper network and system architecture in all phases of the automation solution lifecycle.
  This team also supports the technical responsibilities of the other departments (except IT Services).

6.5. OT Cybersecurity Team Responsibilities

OT Cybersecurity Team ensures that a robust defense-in-depth is in place by planning, implementing, monitoring and optimizing a proper network and system architecture in all phases of the automation solution lifecycle.

To ensure that no IACS responsibility was overlooked, the following process, solely based on IACS concepts, was used to account for all phases of an automation solution lifecycle, all types of security activities, and all layers of an OT environment,

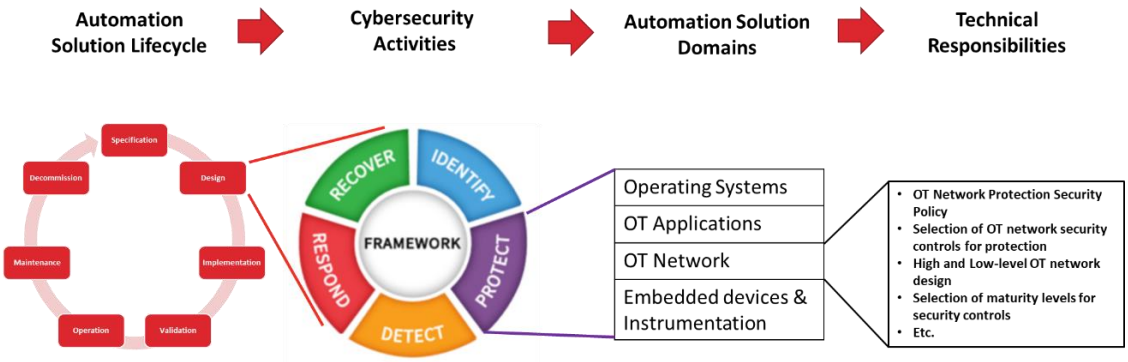


Figure 3: Process to Derive OT Cybersecurity Team Responsibilities

6.5.1. Automation Solution Lifecycle

As defined by the IEC 62443 standard, the Automation Solution Lifecycle and high-level security responsibilities for each phase are represented in Figure 4.

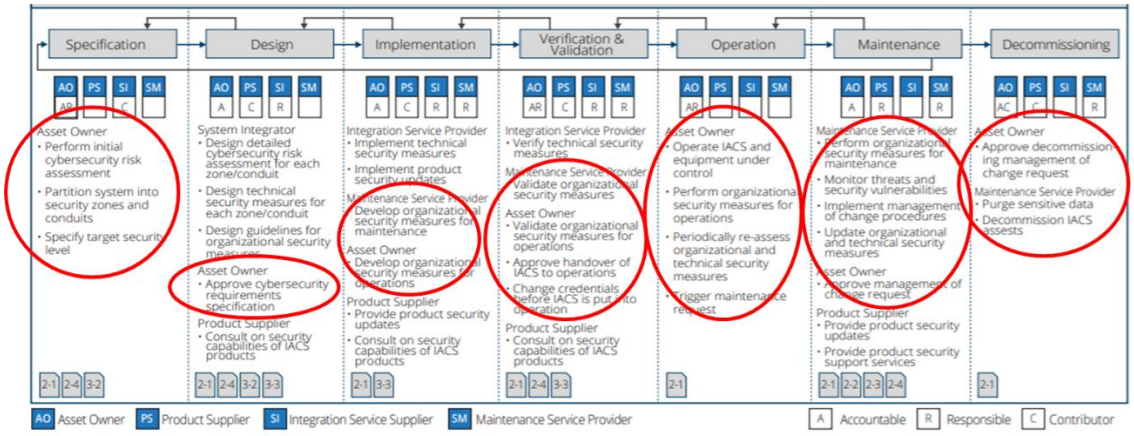


Figure 4: Automation Solution Lifecycle and High-level Responsibilities

The red circles highlight the responsibilities of the Asset Owner and Maintenance Service Provider, as the two organizational roles this project focuses on.

Specification Phase:

- Asset Owner Role
  - **Initial risk assessment** (eventually "paper-based") to identify risks, threats and known vulnerabilities of the solution and the environment it will be implemented in.

- **Specification of technical security capabilities** of the automation solution (based on the risk assessment) to mitigate unacceptable risks. These risks can also be avoided or transferred if mitigation is not feasible.
- **Selection of technical security controls** (based on the capabilities)
  - In some cases, end-to-end security solutions may be needed, while in other cases it only integration with security solutions existing in the environment are needed.
- **Selecting a maturity level for each control** to find the right balance between achieving the target and resources needed (financial, human, time, etc.)

Design Phase

- Asset Owner Role
  - **Approve cybersecurity solution capabilities** specified by the Product Supplier
  - **Approve cybersecurity high-level and low-level designs** specified by the Integration Service Provider
  - **Approve cybersecurity guidelines for organizational** specified by the Integration Service Provider

Implementation Phase

- Asset Owner Role
  - **Develop organizational cybersecurity measures** for operations

- Maintenance Service Provider Role
  - **Develop organizational cybersecurity measures** for maintenance

Validation Phase

- Asset Owner Role
  - **Validate and approve cybersecurity measures for handover** of automation solution to operations
  - **Change access management attributes** for operations (accounts, passwords, certificates, etc.)
  - **Validate and approve organizational cybersecurity measures** for operations

- Maintenance Service Provider Role
  - **Validate and approve organizational cybersecurity measures** for maintenance

Operation Phase

- Asset Owner Role
  - **Operate cybersecurity technical measures** of the automation solution
  - **Execute cybersecurity organizational measures** for operations
  - **Periodic assessment** of security and organizational measures

Maintenance Phase

- Asset Owner Role
  - **Approve MoC** requests

- Maintenance Service Provider Role
  - **Execute cybersecurity organizational measures** for maintenance
  - Monitor cyber **threats and vulnerabilities**

- **Implement MoC** procedures
- **Update organizational and technical security measures**

Decommissioning Phase

- Asset Owner Role
  - **Approve decommissioning** MoC
- Maintenance Service Provider Role
  - **Purge** sensitive data
  - **Decommission** assets

6.5.2. Cybersecurity Activities

To list and characterize cybersecurity activities, NIST Cyber Security Framework (CSF) was selected as it purpose-built for critical infrastructures, Table *1*.

Table 1: NIST CSF Activities

FUNCTIONS	ACTIVITIES
Identify	• Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. • Cybersecurity domains include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy
Protect	• Selection of Protection measures (technical and procedural) to prevent and limit the impact of cyber intrusions • Cybersecurity domains include Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology
Detect	• Selection of Detection measures (technical and procedural) to ensure timely discovery of cybersecurity events • Cybersecurity domains include Anomalies and Events, Security Continuous Monitoring, and Detection Processes
Respond	• Selection of Response measures (technical and procedural) to contain the impact of a potential cybersecurity incident • Cybersecurity domains include Response Planning, Communications, Analysis, Mitigation, and Improvements.
Recover	• Selection of Recovery measures (technical and procedural) to ensure timely recovery to normal operations • Cybersecurity domains include Recovery Planning, Improvements, and Communications.

6.5.3. Automation Solution Domains

To split an automation solution in domains that are relevant for IACS competences, the Purdue Enterprise Reference Architecture (PERA) was used, Figure *5*.

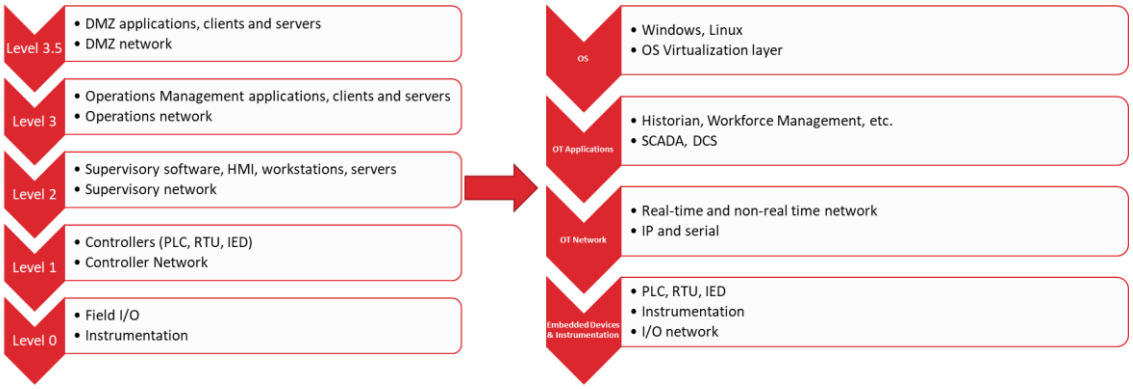


Figure 5: Purdue Model and Competence Domains

From the levels that compose an OT environment, four competences domains were derived: Operating Systems, OT Applications, OT Network, Embedded Devices & Instrumentation.
Since the industrial applications and embedded devices are often from the same vendor and their security is often defined by the capabilities provided by the vendor, these two domains were further collapsed in the definition of roles.

6.6. OT Cybersecurity Team Roles

The definition of roles of the OT Cybersecurity Team follows a similar process of the responsibilities: roles are defined taking into account the automation solution lifecycle and competences domains.

The types of activities by NIST CSF were not used to define roles, as it is expected that the same role will include the identification, protection, detection, response and recovery responsibilities for each competence domain, and for each automation solution lifecycle.

Note that, while the goal of this chapter is to derive roles and responsibilities, the "accountability" of certain responsibilities may belong to a different role in a different department altogether. For example, the responsibility of the definition of security requirements for embedded devices may be associated to a role in the OT Cybersecurity Team, but the accountability falls on the Asset Owner in the Asset Management department.

Considering the Automation Solution Lifecycle responsibilities of an Asset Owner/Maintenance Service Provider, the following roles can be derived:

- **Specification** – Planner
- **Design** – Architect
- **Implementation** – OT Risk & Governance Manager
- **Validation** – Analyst
- **Operation** – Administrator and SOC team
- **Maintenance** – Administrator
- **Decommission** – Administrator

It may seem peculiar that a role named "OT Risk & Governance Manager" is responsible Implementation, but, as it can be seen in section 6.5.1, the responsibilities of the Asset Owner and Maintenance Service Provider in this lifecycle phase are confined to "develop organizational cybersecurity measures". The actual implementation is the Integration Service Provider responsibility.

Considering the Automation Solution competence domains, the following can be derived:

- **Operating Systems** – System Security
- **OT Application** – [Vendor] Security
- **OT Network** – Network Security
- **Embedded Devices & Instrumentation** – [Vendor] Security

Therefore, the OT Cybersecurity team is comprised of the following roles.

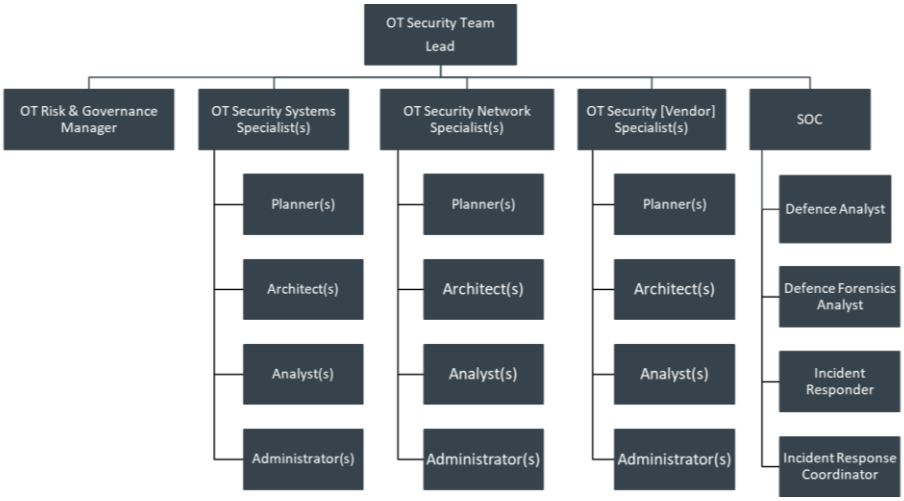


Figure 6: OT Cybersecurity Team Roles

6.7. *Mapping OT Cybersecurity Team Roles to Responsibilities*

The exercise of mapping responsibilities to roles was done in a separate Excel file (filename: 20110952 - NCSC_OT Roles Responsibilities.xlsx). A sample is shown below.

OT CYBERSECURITY TEAM RESPONSIBILITIES (As per IEC 62443)					OT CYBERSECURITY TEAM ROLES		
ASSET OWNER ROLE	SPECIFY	* Risk assessment * Specification of capabilities * Selection of controls * Maturity level	ALL FUNCTIONS	OS APPLICATION NETWORK EMBEDDED	OT Security System Planner OT Security Industrial Planner OT Security Network Planner OT Security Industrial Planner	OT Risk & Governance Manager (Risk Assessment)	OT Security Lead
	DESIGN	* Approve capabilities * Approve HLD AND LLD * Approve guidelines for organizational measures	ALL FUNCTIONS	OS APPLICATION NETWORK EMBEDDED	OT Security System Architect OT Security Industrial Architect OT Security Network Architect OT Security Industrial Architect	OT Risk & Governance Manager (Org. measures)	OT Security Lead
	IMPLEMENT	* Develop organizational cybersecurity measures for operations	ALL FUNCTIONS	OS APPLICATION NETWORK EMBEDDED		OT Risk & Governance Manager (Org. measures)	OT Security Lead
	VALIDATE	* Validate and approve cybersecurity measures for handover * Change access management attributes for operations * Validate and approve organizational cybersecurity measures for operations	ALL FUNCTIONS	OS APPLICATION NETWORK EMBEDDED	OT Security System Analyst OT Security Industrial Analyst OT Security Network Analyst OT Security Industrial Analyst	OT Risk & Governance Manager (Org. measures)	OT Security Lead
	OPERATE	* Operate technical measures * Execute organizational measures * Periodic assessment	IDENTIFY	OS APPLICATION NETWORK EMBEDDED	OT Security System Administrator OT Security Industrial Administrator OT Security Network Administrator OT Security Industrial Administrator	OT Risk & Governance Manager (Periodic Assessment)	OT Security Lead
			PROTECT	OS APPLICATION NETWORK EMBEDDED	OT Security System Administrator OT Security Industrial Administrator OT Security Network Administrator OT Security Industrial Administrator		OT Security Lead
			DETECT	OS APPLICATION NETWORK EMBEDDED	SOC team - Defence Analyst and Defence Forensics Analyst		
			RESPOND	OS APPLICATION NETWORK EMBEDDED	SOC team - Incident Responder and Incident Response Coordinator		
			RECOVER	OS APPLICATION NETWORK EMBEDDED			

Figure 7: OT Cybersecurity Team Roles and Responsibilities