All to keep **you** going

Afstudeerscriptie

Beveiliging operationele technologie

Auteur:

T.L.J. Waanders
466220

Bedrijfsbegeleider:

D. Schutten
Network & Security Specialist

Afstudeerdocent:

E. M. Hageraats

Opdrachtgever:

PCI Nederland B.V.

Onderwijsinstelling:

Saxion Hogeschool, Academie Creatieve Technologie

Opleiding:

HBO-ICT, IT Service Management

Versie:

2.1

Datum:

30-06-2022

Voorwoord

Voor u ligt de afstudeerscriptie “Beveiliging operationele technologie” welke is geschreven in opdracht van PCI Nederland BV ter afsluiting van de opleiding HBO-ICT, studieroute IT Service Management aan het Saxion te Enschede.

Dit onderzoek is uitgevoerd in de periode februari 2022 tot en met juni 2022 bij PCI Nederland, business unit IT-solutions gevestigd in Haaksbergen. In dit onderzoek is gekeken hoe PCI haar klanten kan ondersteunen in het beter beveiligen van operationele technologie.

Het werken met operationele technologie was nieuw voor mij. Ik heb tijdens deze periode veel geleerd over de toepassingsgebieden, werking en beveiligingsaspecten aan operationele technologie. Het onderwerp OT-security is zeer actueel en ik heb gedurende deze periode gemerkt dat het een belangrijk onderwerp voor veel organisaties is. Verder heb ik ervaren hoe het is om individueel een grote onderzoeksopdracht uit te voeren.

Gedurende deze periode heb ik ondersteuning gehad bij het uitvoeren van dit onderzoek van Dennis Schutten, met hem heb ik veel gesproken over de opdracht en heb ik hulp gehad bij inhoudelijke vragen over OT/IT security en werkwijzen van PCI. Ik wil hem bij deze bedanken voor zijn inzet, hulp en feedback tijdens deze periode. Ook wil ik alle andere collega’s van PCI Nederland bedanken voor de hulp en input bij het schrijven van deze scriptie.

Tot slot wil ik mijn afstudeerbegeleider van het Saxion Esther Hageraats bedanken voor de begeleiding bij het opstellen van de scriptie. Gedurende de afstudeergesprekken heeft zij mij geholpen om kritisch naar mijn onderzoek te kijken en zo tot nieuwe inzichten te komen.

Thijs Waanders

Haaksbergen, juni 2022

Samenvatting

PCI Nederland levert een groot aantal IT-diensten aan verschillende klanten. Een deel van deze klanten zijn grote productiebedrijven die gebruikmaken van operationele technologie (OT) voor de aansturing en controle van industriële processen. PCI heeft als doelstelling om haar klanten een zo compleet mogelijk aanbod te bieden in IT-diensten en de IT volledig uit handen te nemen.

Binnen PCI zijn geen oplossingen beschikbaar voor de beveiliging van OT. Om de klanten met OT toch van dienst te kunnen zijn wil PCI graag een aantal standaardoplossingen en best practices kunnen implementeren bij klanten. In dit onderzoek wordt een antwoord gezocht op de hoofdvraag: "**Hoe kan PCI Nederland operationele technologie beter beveiligen bij haar klanten?".** Om het antwoord op deze hoofdvraag goed te onderbouwen worden zeven deelvragen behandeld.

In het literatuuronderzoek is antwoord gegeven op deelvraag één: "Wat is OT en waar bestaat OT uit?". Uit het literatuuronderzoek blijkt dat OT bestaat uit hardware en software welke gebruikt wordt voor het aansturen van fysieke industriële processen en apparatuur. (Gartner, 2022) OT bestaat uit een verzameling van PLCs, DCSs, HMIs en SCADA-oplossingen voor het bedienen van industriële systemen. (AT-Automation, 2022) Deze onderdelen zijn in het literatuuronderzoek verder uitgelegd.

In een behoefteanalyse is gekeken naar deelvraag twee: "Wat voor soort OT zouden klanten van PCI beveiligd willen hebben?". Uit de behoefteanalyse is gebleken dat klanten van PCI voornamelijk gebruik maken van operationele technologie voor industriële toepassingen. Deze operationele technologie bestaat uit HMIs op traditionele computers voor het aansturen van PLCs welke vervolgens industriële processen aansturen. Deze processen worden met SCADA-oplossingen gemonitord zodat verstoringen vroegtijdig opgemerkt worden. De onderzochte technologie maakt vaak verbinding met bedrijfsservers en is extern te beheren door leveranciers.

De derde deelvraag: "Welke eisen stelt PCI aan een security dienst?", is behandeld in een behoefte en contextanalyse. Uit de contextanalyse is gebleken dat PCI zichzelf ziet als een Managed Service Provider (MSP) die diensten levert aan zeer verschillende klanten. Klanten van PCI zijn van verschillende omvang en er wordt met verschillende leveranciers gewerkt. Uit de behoefteanalyse blijkt dan ook dat PCI graag ziet dat een dienst centraal te beheren is, door een IT-specialist te implementeren is, schaalbaar in te zetten is bij verschillende klanten en kan samenwerken met bestaande oplossingen van huidige leveranciers.

Deelvraag vier: "Welke dreigingen zijn er op het gebied van OT?" is beantwoord in het literatuuronderzoek. In veel gevallen vindt vanaf het IT-netwerk een aanval plaats op een traditionele computer in het OT-netwerk waarvandaan machines worden aangevallen, dit omdat deze netwerken vaak onderling verbonden zijn. Risico's voor OT zijn er op het gebied van bedrijfsspionage, het stil leggen van een productielijn of het toebrengen van schade aan mensen of de omgeving.

Deelvraag vijf zoekt naar best practices op het gebied van OT-security. Deze zijn samen te vatten in 16 ontwerpprincipes. Het is verstandig om het ontwerp te baseren op deze ontwerpprincipes.

In het functioneel- en technisch ontwerp is ter beantwoording van deelvraag zes gezocht naar verschillende oplossingen welke door PCI in een OT-security dienst kunnen worden aangeboden. Uit dit ontwerp valt te concluderen dat de dienst moet bestaan uit: Palo Alto IoT security ten behoeve van asset discovery, vulnerability scanning en het detecteren van verdacht netwerkverkeer, netwerksegmentatie op basis van productielijn doormiddel van VLAN en firewall security zones en toegang voor leveranciers via een VPN-verbinding en het jump host principe.

In een adviesrapport is ter beantwoording van deelvraag zeven beschreven hoe de gevonden producten en methodieken kunnen worden ingezet als dienst van PCI. Het wordt aangeraden om deze producten en methodieken op te delen in een managed dienst en eenmalige dienstverlening. De managed dienst bestaat uit het leveren en beheren van Palo Alto IoT security inclusief het opvolgen van alerts volgens de afspraken zoals deze zijn vastgelegd in een SLA. Daarnaast kan in een eenmalige dienst het netwerk van de klant worden gesegmenteerd en een jump host ingericht worden.

Het antwoord op de gestelde hoofdvraag is: Door netwerken van klanten goed te segmenteren, klanten een jump host aan te bieden voor toegang door externe leveranciers, het OT-netwerk in kaart te brengen en te monitoren en dit onder te brengen in een dienst kan PCI operationele technologie beter beveiligen bij haar klanten.

Inhoudsopgave

Lijst van tabellen & figuren

Versiebeheer

Tabel 1, Versiebeheer

Versie nr.	Datum	Wijzigingen
0.1	17-03-2022	Vooronderzoek ingevoegd in afstudeerscriptie
0.2	28-03-2022	Eerste onderdelen ontwerp toegevoegd, document gereed gemaakt voor tussentijdse inlevering.
0.3	31-03-2022	Feedback verwerkt: indeling verslag verbeterd, methodieken uitgebreider onderbouwd, hoofd/deelvragen in probleemstelling en schema.
0.4	22-04-2022	Ontwerp en advies uitgewerkt en toegevoegd aan scriptie. Eerste onderdelen ontwerpevaluatie en eindevaluatie toegevoegd.
0.5	26-04-2022	Feedback verwerkt. Hoofdstuk 6.2 aangepast, use-case diagrammen aangepast, verwijzingen in architectuur toegevoegd.
0.6	02-05-2022	Voorwoord geschreven, ontwerpevaluatie uitgewerkt, eindevaluatie opgesteld en hoofdstuk discussie beschreven.
0.7	13-05-2022	Discussie uitgebreid en aanpassingen indeling document doorgevoerd.
1.0	17-05-2022	Feedback verwerkt, totale document controle voor inlevering aan PCI.
1.1	25-05-2022	Feedback vanuit PCI verwerkt, laatste aanpassingen aan samenvatting en totale document controle.
2.0	09-06-2022	Document gereed gemaakt voor definitieve inlevering.
2.1	30-06-2022	Interviews geanonimiseerd ivm openbare publicatie.

1. Inleiding

Dit document bevat de afstudeerscriptie van Thijs Waanders voor de opleiding HBO-ICT van het Saxion te Enschede. Dit onderzoek is uitgevoerd in opdracht van PCI Nederland (hierna ook genoemd als de opdrachtgever). De opdrachtgever levert IT-diensten aan een groot aantal klanten, een deel van deze klanten zijn productiebedrijven die naast standaard IT-gebruik maken van operationele technologie (OT). In toenemende mate komen klanten met vraagstellingen over het beveiligen van OT. Dit onderzoek richt zich op het verbeteren van de beveiliging van operationele technologie.

Dit afstudeeronderzoek is uitgevoerd conform de onderzoeksmethodiek ontwerponderzoek. (Linden, Hageraats, & Haveman, 2016) In dit verslag worden de verschillende fasen van het ontwerponderzoek doorlopen om tot een goed onderbouwd onderzoeksresultaat te komen.

Dit document start met de probleemanalyse vanuit verschillende perspectieven. Deze perspectieven zijn bepaald in een stakeholderanalyse. Op basis van de probleemanalyse zijn de hoofd- en deelvragen opgesteld. Vanuit het perspectief van de stakeholders is vervolgens gekeken naar de specifieke behoefte, waarbij wordt gekeken waar het product aan moet voldoen en wat de verschillende stakeholders nodig hebben. Om de randvoorwaarden aan het ontwerp te bepalen is de context van de opdracht geanalyseerd in de contextanalyse. In deze contextanalyse is naar zowel de interne als externe omgeving gekeken. Hoofdstuk vijf bevat een literatuuronderzoek waarin wordt gekeken naar literatuur welke kan ondersteunen in het beantwoorden van de deelvragen, het geven van een onderbouwd advies en het opstellen van ontwerpen.

In hoofdstuk zes wordt gestart met het functioneel ontwerp. Dit functionele ontwerp bestaat uit een aantal use-case diagrammen, functionaliteit beschrijving en een architectuurmodel. Op basis van het vooronderzoek en het functioneel ontwerp is vervolgens in een technisch ontwerp een geschikte oplossing van het probleem van PCI gezocht en ontworpen. Dit ontwerp wordt met het vooronderzoek gevalideerd in een ontwerpevaluatie in hoofdstuk zeven. Hoofdstuk acht van het verslag bestaat uit een advies dat aan PCI wordt gegeven op basis van de resultaten van het onderzoek. Dit advies gaat verder in op de manier waarop de gevonden ontwerpen bij klanten in een dienstvorm geïmplementeerd kunnen worden en is te vinden in hoofdstuk acht.

Gedurende het onderzoek worden verschillende dataverzamelingsmethodieken gebruikt. Deze methodieken zijn afkomstig uit de onderzoeksmethodiek ontwerponderzoek (Linden, Hageraats, & Haveman, 2016), aangevuld met dataverzameling en onderzoeksmethodieken uit het DOT model. (HBO-i, 2021)

1.1. Achtergrond

PCI Nederland helpt organisaties met een complete werkomgeving. PCI biedt haar klanten totale oplossingen waarmee de basis voor een werkplek kan worden geboden.
PCI bestaat uit vier business units:

- IT Solutions

Deze business unit richt zich op de totale inrichting van de IT-infrastructuur. PCI helpt ondernemers met het bieden van een veilige IT-omgeving die altijd aan de laatste eisen voldoet.

- Audiovisueel

Deze business unit richt zich in het bieden van de juiste audiovisuele oplossingen aan ondernemers. Dit gaat van het inrichten van vergaderruimtes, tot digitale billboards en presentatiemiddelen.

- Managed Print Services

Deze business unit levert zakelijke printoplossingen. PCI adviseert klanten op het gebied van multifunctionele printers, productieprinters, print management en plotters.

- Supplies

Deze business unit levert kantoorartikelen aan klanten van PCI. Hierbij kan worden gedacht aan papier, toners, kabels en andere kantoorartikelen.

Vanuit deze business units levert PCI diensten aan ondernemers waarmee een totale IT-werkomgeving wordt geboden. Zo kan de IT-infrastructuur aangevuld worden met printers en printer-

benodigdheden, worden vergaderruimtes uitgerust met audiovisuele middelen en worden medewerkers voorzien in thuiswerkplekken. (PCI Nederland, 2021)

Het hoofdkantoor van PCI zit gevestigd in Lijnden, het hoofdkantoor van de business unit IT-Solutions zit gevestigd in Haaksbergen. Deze business unit levert totale IT-oplossingen aan een groot aantal klanten. (PCI Nederland, 2022) De afstudeeropdracht wordt uitgevoerd binnen de IT-solutions business unit en richt zich op de producten, diensten en klanten van deze business unit.

2. Probleemanalyse

Voor het vaststellen van de vraag van PCI is een probleemanalyse uitgevoerd. Voor het uitvoeren van de probleemanalyse is gebruik gemaakt van onderzoeksmethodieken welke in de volgende paragraaf worden beschreven. Het doel van deze probleemanalyse is het vaststellen van de vraag van de opdrachtgever, bekeken vanuit verschillende perspectieven.

2.1. Methodiek

Om tot een zo compleet mogelijke probleemstelling te komen wordt het “probleem” vanuit verschillende perspectieven (views) bekeken. Dit verhoogt de betrouwbaarheid van het onderzoek (triangulatie). Dit gebeurt vanuit de view van enkele stakeholders.

Voor het vaststellen van de perspectieven is begonnen met een longlist van mogelijke belanghebbenden bij het resultaat van dit onderzoek, deze longlist is op basis van het eerste gesprek met de netwerkspecialist binnen PCI tot stand gekomen. Deze lijst van stakeholders is vervolgens gecategoriseerd op basis van het type stakeholder. De prioritering van de stakeholders gebeurt op basis van de Mendelow methodiek, deze methodiek prioriteert de stakeholders op basis van macht en belang bij het project. (Mendelow, 1991) Op basis van deze prioritering is een shortlist van stakeholders opgesteld. Door te bepalen welke stakeholders daadwerkelijk een hoge betrokkenheid hebben wordt de validiteit van het onderzoek verbeterd, zo wordt er niet vanuit slecht geïnformeerde stakeholders gekeken. Deze stakeholderanalyse is te vinden in bijlage B

Om de probleemstelling zo goed mogelijk te bepalen is gekeken vanuit verschillende perspectieven. Deze perspectieven zijn “views” zoals gedefinieerd in de IT-architectuur. (Boer, 2019) De views zijn gebaseerd op de shortlist van stakeholders aangevuld met het perspectief vanuit de literatuur en het perspectief van de onderzoeker.

2.1.1. Interview

Als eerste wordt gekeken vanuit het perspectief van de verschillende stakeholders welke op de shortlist voorkomen. Per stakeholder wordt een interview afgenomen. De interviews vinden op een semigestructureerde wijze plaats. Dit betekent dat er vooraf bedachte open vragen worden gesteld in willekeurige volgorde. Hierbij bestaat er de mogelijkheid om door te vragen op de gegeven antwoorden. Deze manier van interviewen geeft veel gedetailleerde informatie doordat er de mogelijkheid bestaat om door te vragen zoals in een open interview. Maar door deze manier van werken worden wel alle onderwerpen behandeld omdat er vooraf wordt nagedacht over de te stellen vragen. (Genau, 2021)

De probleemstelling wordt vervolgens opgesteld op basis van de interviews met de stakeholders, aangevuld met het perspectief vanuit de literatuur en vanuit de onderzoeker. De interviews zijn te vinden in bijlage A. Voor het opstellen van de probleemstelling is gesproken met:

- Technical field service manager, voor het opdrachtgever perspectief
  Voor het bepalen van het opdrachtgeversperspectief is gesproken met de technical field service manager van PCI. Deze medewerker is verantwoordelijk voor de technische afdeling en heeft een belangrijke rol in de ontwikkeling van nieuwe diensten
- Netwerk & security specialist
- Klant PCI met OT (producent van kunststof producten)
- Service level manager

2.1.2. Desk research

Naast het interview wordt desk research in de vorm van literatuuronderzoek uitgevoerd voor het bepalen van het literatuur- en overheidsperspectief. Hiervoor wordt gebruik gemaakt van bronnen afkomstig van de Nederlandse overheid en IT-onderzoeksinstituten.

2.2. Resultaten

Dit hoofdstuk bevat het resultaat van de probleemanalyse.

2.2.1. Literatuurperspectief

Als eerste is gekeken naar de exacte definitie van operationele technologie (OT). Gartner schrijft: “Operationele technologie (OT) is hardware en software die een verandering detecteert of veroorzaakt door de directe bewaking en/of controle van industriële apparatuur, activa, processen en gebeurtenissen.” (Gartner, 2022) Het Digital Trust Center schrijft: “Operational Technology (OT) is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld zoals het aansturen en monitoren van (industriële) apparatuur. Het kan dan gaan om het uitlezen van sensoren of het inschakelen van een pomp of schakelaar op basis van een bepaalde conditie.” (Digital Trust Center, 2022) Op basis van deze definities wordt verder gewerkt in dit onderzoek.

In vergelijking met de meeste traditionele IT-systemen hebben OT-systemen een nog grotere gevoeligheid voor kleine verstoringen. Een licht vertraagde email zal geen problemen veroorzaken, een chemisch proces dat vertraagd reageert kan grote gevolgen hebben. (Conklin, 2016) OT bestond oorspronkelijk uit individuele machines of kleine fysieke netwerken die enkel fysiek door een medewerker fysiek te bedienen waren. In de loop van de jaren zijn steeds meer OT-systemen aan het internet gekoppeld om gebruik te maken van bestaande IT-oplossingen. (Anton, et al., 2021) Naast gemak brengt dit ook security risico’s met zich mee. OT-systemen zijn daarnaast in veel gevallen ontworpen om vele jaren gebruikt te worden. De aanschaf van productiemachines is een grote kostenpost welke over een langere periode moet worden terugverdiend. In deze periode raken onderdelen van OT zoals software, communicatieprotocollen, encryptiemethodieken en besturingssystemen out of date. (Conklin, 2016)

2.2.2. Opdrachtgeverperspectief (Technical Field Service Manager)

PCI levert een groot aantal IT-diensten aan zeer verschillende klanten. Een deel van deze klanten zijn grote productiebedrijven die gebruikmaken van operationele technologie voor de aansturing en controle van industriële processen. PCI heeft als doelstelling om haar klanten een zo compleet mogelijk aanbod te bieden in IT-diensten en het beheer van IT-middelen volledig uit handen te nemen.

Binnen PCI zijn geen specifieke oplossingen beschikbaar voor de beveiliging van OT. Om de klanten met OT toch volledig van dienst te kunnen zijn wil PCI graag een aantal standaardoplossingen en best practices kunnen implementeren in de netwerken van klanten. PCI is hierbij op zoek naar methodieken of producten die bij klanten kunnen worden ingezet om de vraag van de klant te kunnen beantwoorden. PCI wil de huidige oplossingen op het gebied van security uitbreiden met oplossingen voor de beveiliging van OT. PCI wil dit graag als dienst kunnen leveren aan klanten maar ook als los product kunnen verkopen. De oplossing moet hiervoor ondersteuning bieden.

PCI IT-Solutions is een managed serviceprovider voor IT-diensten. PCI is op zoek naar een dienst die zij universeel kunnen aanbieden aan klanten die gebruik maken van OT in productieomgevingen. Deze dienst moet voldoen aan de eisen die PCI stelt aan een dienst en eenvoudig bij meerdere klanten in te zetten zijn.

2.2.3. Netwerkspecialisten perspectief

De netwerkspecialist van PCI geeft aan van klanten vaak vragen te krijgen over oplossingen die PCI kan bieden voor een verbeterde beveiliging van operationele technologie. Hij ziet dat klanten OT steeds vaker willen aansluiten op traditionele IT-systemen, terwijl hij het vanuit security oogpunt liever niet zou hebben. Dit omdat OT-hardware vaak veel langer meegaat als IT-software, OT-hardware

bevat soms oude besturingssystemen en legacy software. Verder geeft hij aan dat bepaalde klanten niet eens weten welke OT er precies aanwezig is. Hij geeft aan dat hij als netwerkspecialist veel beheer uitvoert op locatie bij klanten, voor extern beheer wordt hiervoor gebruik gemaakt van de bij PCI geldende standaarden. Het oplossen van verstoringen op productiemachines gebeurt echter vaak door de leverancier van de machine. Deze leveranciers gebruiken verschillende werkwijzen, oplossingen en verbindingen voor het beheren van OT. In veel gevallen maakt de leverancier hiervoor direct een verbinding met een machine vanaf het internet. Dit is iets wat vanuit het perspectief van de netwerkspecialist niet wenselijk is.

2.2.4. Klantperspectief

Met het begrip “de klant” wordt in dit onderzoek de klanten van PCI IT-Solutions bedoeld die gebruik maken van operationele technologie. Deze klanten zijn productiebedrijven die operationele technologie nodig hebben voor de continuïteit van de core business. Het uitvallen van operationele technologie is voor deze klanten onaanvaardbaar. Klanten besteden het IT-beheer uit aan PCI als dienst, PCI levert hardware en beheert deze hardware. In andere gevallen levert PCI enkel de hardware en voert een implementatie uit als eenmalig project. De klant is vervolgens zelf verantwoordelijk voor het uitvoeren van onderhoud en het oplossen van storingen. De klanten geven aan interesse te hebben in oplossingen van PCI voor het beter beveiligen van operationele technologie. De klanten willen graag de bevestiging krijgen dat de operationele technologie voldoende beveiligd is. Dit onderzoek gaat over OT-security als een universele dienst voor diverse klanten.

De klanten van PCI hebben onvoldoende inzicht in de beveiliging van de OT-omgeving. Deze klanten hebben het netwerkbeheer uitbesteed aan PCI en willen graag dat PCI ook het productienetwerk goed beveiligd. Een aantal klanten van PCI werkt 24/7 in de productie, het stilvallen van machines kan daarom niet worden ingehaald en heeft direct grote gevolgen. Verder worden er momenteel machines aangeschaft waarvan de IT-inrichting niet bekend is. Klanten willen graag zien welke apparatuur er allemaal aanwezig is in het OT-netwerk, hiervoor willen ze graag ondersteuning van PCI krijgen.

2.2.5. Overheidsperspectief

Voor het bepalen van het overheidsperspectief is gekeken naar de landelijke Nederlandse overheid. Dit omdat cybersecurity een onderdeel is dat voor het grootste deel bij de landelijke overheid ligt, de verantwoordelijkheid ligt bij het Ministerie van Justitie en Veiligheid. (Rijksoverheid, 2022) Voor de invulling van dit perspectief is deskresearch uitgevoerd. De overheid ziet dat OT bij zowel grote als kleinere ondernemingen voorkomt, OT speelt een grote rol in verschillende industrieën en sectoren en is in veel essentiële sectoren van groot belang voor de continuïteit van bedrijfsprocessen. (Digital Trust Center, 2022) Het Nationaal Cyber Security Centrum geeft aan dat OT (ook wel Industrial Control Systems (ICS) genoemd) in toenemende mate het doelwit is van cyberaanvallen. (Vos, Brink, & Schie, 2019)

Het Nationaal Cyber Security Centrum (NCSC) ziet daarnaast dat OT en IT steeds vaker op elkaar worden aangesloten en dat daardoor OT-infrastructuur indirect is aangesloten op het internet. Omdat OT wordt ingezet in vitale sectoren kan een aanval op OT maatschappij ontwrichtende gevolgen hebben. Ook als OT wordt ingezet in productiebedrijven buiten vitale sectoren kan een cyberaanval grote gevolgen hebben. Bijvoorbeeld wanneer OT gebruikt wordt in de aansturing van chemische processen, wanneer deze processen niet goed worden gecontroleerd kan dit grote gevolgen hebben voor de nationale veiligheid. (Nationaal Cyber Security Centrum, 2022)

2.2.6. Service level manager perspectief

Een aantal IT-oplossingen worden door PCI aangeboden aan klanten als managed dienst. Dit betekent dat PCI bijvoorbeeld een omgeving beveiligd door een implementatie uit te voeren, monitoring te verzorgen en het beheer van bijvoorbeeld een firewall uitvoert. Bij een managed dienst wordt een vooraf gedefinieerde dienst voor een vast bedrag per maand geleverd aan een klant. De klant koopt hierbij geen product maar neemt een dienst af. PCI heeft een redelijk aandeel klanten in de productiesector. Op dit moment worden er voornamelijk generieke diensten geleverd die voor alle soorten klanten inzetbaar zijn. Omdat PCI een redelijk aandeel productiebedrijven als klant heeft is het goed mogelijk om hier een specifieke dienst voor te leveren.

Service Level Management ontwerpt diensten na vraag van een klant. Omdat er door meerdere klanten al is aangegeven dat OT-security interessant zou zijn wil SLM graag een advies ontvangen over het inzetten van OT-security oplossingen als diensten en een voorbeeld van een SLA waarmee deze diensten aangeboden kunnen worden.

2.2.7. Perspectief onderzoeker

Na de eerste probleemanalyses zoals deze in dit hoofdstuk is weergegeven en na het maken van een start met het literatuuronderzoek is OT-security vanuit het perspectief van de onderzoeker zeer van belang. Aanwezige data en kantoorautomatisering wordt op dit moment al goed beveiligd maar de operationele technologie is voor bepaalde klanten van PCI belangrijker dan de kantooromgeving. Wanneer de productie van deze bedrijven stilvalt door een OT-security incident heeft dit vrijwel direct grote gevolgen voor het halen van planningen en doelstellingen. Ook het veiligheidsperspectief wordt door de onderzoeker als zeer belangrijk gezien. Medewerkers op productielocaties vertrouwen op de aansturing van machines en passen daar werkwijzen op aan. Als een machine onverwacht gedrag vertoond of metingen niet langer betrouwbaar zijn kan dit grote gevolgen hebben. Daarnaast herkent de onderzoeker de probleemstelling die door PCI en de klant wordt gegeven. Er is vaak weinig kennis van beveiliging van OT en OT wordt aangesloten op het internet zonder dat precies bekend is hoe de machine werkt en onderhouden wordt.

2.3. Conclusie

Op basis van de door PCI gestelde probleemstelling is een hoofdvraag voor dit onderzoek opgesteld. Om tot een goed onderbouwd antwoord op de hoofdvraag te komen zijn meerdere deelvragen opgesteld. Deze deelvragen worden in de loop van dit onderzoeksrapport behandeld.

2.3.1. Hoofdvraag

De hoofdvraag is opgesteld om in één vraag de totale probleemstelling te omvatten. PCI is de opdrachtgever van dit onderzoek en levert IT-diensten aan haar klanten, deze klanten hebben behoefte aan een verbeterde beveiliging van de aanwezige operationele technologie. De hoofdvraag van dit onderzoek is daarom:

Hoe kan PCI Nederland operationele technologie beter beveiligen bij haar klanten?

2.3.2. Deelvragen

Om tot een juiste beantwoording van de hoofdvraag te komen zijn meerdere deelvragen opgesteld. Deze deelvragen geven gezamenlijk antwoord op de hoofdvraag van het onderzoek. In figuur 1 is weergegeven welke deelvragen in welk deel van het onderzoek beantwoord worden.

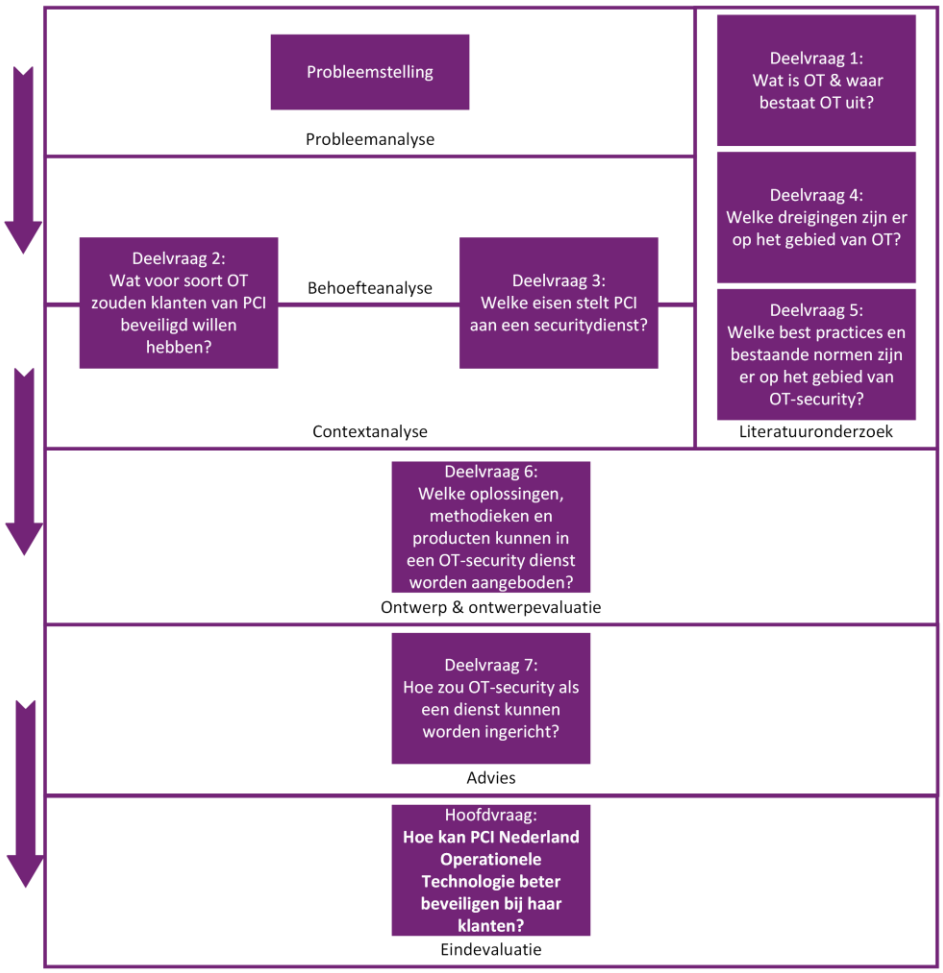
1. Wat is OT & waar bestaat OT uit?
   Voor het goed kunnen uitvoeren van dit onderzoek is het van belang om de definitie van OT duidelijk te hebben. Zonder deze definitie kan er geen goed onderzoek worden gedaan. Uit de eerste analyses blijkt dat OT bestaat uit meerdere onderdelen, hier moet nog meer kennis over worden opgedaan. Deze onderzoeksvraag wordt behandeld in het literatuuronderzoek.
2. Wat voor soort OT zouden klanten van PCI beveiligd willen hebben?
   OT is een erg groot begrip. Om tot een goed antwoord te komen op de volgende deelvragen is het van belang om een onderzoek te doen naar welke OT klanten van PCI gebruiken. Afhankelijk hiervan kunnen de eisen aan te gebruiken oplossingen en methodieken worden bepaald. Deze deelvraag wordt behandeld in de behoefteanalyse en resulteert in requirements.
3. Welke eisen stelt PCI aan een securitydienst?
   In een behoefteanalyse wordt gekeken aan welke eisen een dienst moet voldoen bij PCI. Om de gevonden oplossingen als dienst in te kunnen zetten moet aan deze eisen worden voldaan. Omdat het in dit geval specifiek om een securitydienst gaat wordt hiernaar gekeken. Omdat dit voor een deel ook afhankelijk is van de werking van PCI als IT-dienstverlener wordt naar PCI gekeken in een contextanalyse. Deze deelvraag resulteert in requirements en randvoorwaarden.

4. Welke dreigingen zijn er op het gebied van OT?
   Om te bepalen wat het risico is en waarom OT-security nodig is bij klanten van PCI, is het van belang om te weten welke dreigingen er voorkomen en wat het risico voor klanten is. Daarnaast is het antwoord van deze vraag nodig om te kunnen bepalen tegen welke dreigingen er oplossingen gezocht moeten worden. Het antwoord op deze deelvraag wordt behandeld in het literatuuronderzoek.
5. Welke best practices en bestaande normen zijn er op het gebied van OT-security?
   Uit de probleemanalyse blijkt dat PCI op zoek is naar enkele best practices welke kunnen worden ingericht in OT-netwerken van klanten. In een literatuuronderzoek worden hier oplossingen voor onderzocht. Daarnaast wordt er gekeken of er in de literatuur bestaande normen bekend zijn voor het beveiligen van OT.

Deze eerste deelvragen vormen de basis van het vooronderzoek, de volgende deelvragen worden verder uitgewerkt in het ontwerp en in het adviesrapport.

6. Welke oplossingen, methodieken en producten kunnen in een OT-security dienst worden aangeboden?
   De dienst voor OT-security moet gebaseerd worden op enkele producten, oplossingen of methodieken die PCI kan inzetten bij klanten. In een functioneel- en technisch ontwerp inclusief productselectie wordt beschreven welke oplossingen op welke manier kunnen worden ingezet afhankelijk van de behoefte van de klanten.
7. Hoe zou OT-security als een dienst kunnen worden ingericht?
   Op basis van het technisch ontwerp wordt een adviesrapport opgesteld over het aanbieden van OT-security als een dienst. Dit adviesrapport gaat in op de vereiste SLA, processen en verantwoordelijkheden.

Onderstaand overzicht geeft aan welke vragen in elk onderdeel van deze scriptie behandeld worden.



Figuur 1, Overzicht deelvragen per fase

3. Behoefteanalyse

In dit hoofdstuk is de behoefte van de verschillende stakeholders in kaart gebracht. Per stakeholder is een behoefteanalyse uitgevoerd. Op basis van de behoefteanalyse zijn requirements opgesteld. In dit hoofdstuk wordt voor een deel antwoord worden gegeven op deelvraag drie: Welke eisen stelt PCI aan een security dienst? Tevens geeft dit hoofdstuk antwoord op deelvraag twee: Wat voor soort OT zouden klanten van PCI beveiligd willen hebben?

3.1. Methodiek

In bijlage C is een behoefteanalyse per stakeholder toegevoegd. Vanuit deze behoefteanalyse is verder gewerkt naar een lijst met concrete eisen aan de uitkomsten van dit onderzoek. Deze eisen zijn weergegeven als requirements. De requirements zijn geprioriteerd en gecategoriseerd volgens de methodieken beschreven in bijlage C.

Voor het opstellen van de behoefteanalyse is gebruik gemaakt van de dataverzamelingsmethodieken interview, observatie en document analyse.

3.1.1. Interview

De behoefteanalyse is uitgevoerd vanuit verschillende perspectieven (views) van relevante stakeholders. Deze stakeholders zijn geïnterviewd in een semigestructureerde interview vorm. Een beschrijving van deze methodiek is terug te vinden in hoofdstuk 2.1. De keuze voor de stakeholders is gebaseerd op de stakeholderanalyse welke terug is te vinden in bijlage B.

Voor de behoefteanalyse is een interview uitgevoerd met:

- Technical Field Service Manager PCI
- Netwerkspecialisten PCI
- Klanten PCI met operationele technologie
    - Machinepark beheerder
    - IT-manager
- Servicelevel manager PCI

Interviews zijn te vinden in bijlage A van dit document.

3.1.2. Observatie

Daarnaast is een observatie uitgevoerd op enkele locaties van klanten van PCI. Dit om een goed beeld te krijgen van de aanwezige OT. Voor de observatie is bij één klant de aanwezige OT bekeken gezamenlijk met een OT-specialist van het betreffende bedrijf. De klant waarbij de observatie is uitgevoerd is een productiebedrijf voor kunststof producten. Deze klant is gekozen omdat door PCI is aangegeven dat hier zeer veel operationele technologie wordt gebruikt. Daarnaast stond deze klant open voor het meewerken aan dit onderzoek.

3.1.3. Document analyse

Tot slot is er gekeken naar de standaard SLA welke door PCI wordt gehanteerd bij bestaande security producten. (PCI IT-Solutions, 2022) Dit document is bekeken omdat tijdens de probleemstelling duidelijk is geworden dat PCI op zoek is naar een dienst voor OT-security. De SLA geeft een goede indruk van de standaarden en eisen welke PCI stelt aan een IT-security dienst.

3.2. Resultaten

Een verklaring van de velden in onderstaande tabellen is te vinden in bijlage C van dit document.

3.2.1. Business requirements

Tabel 2, Business requirements

Volg Nr.	Func/Non func	Prioriteit	Genereert	Realiseert	Beschrijving
B01	Functioneel	Must	U01, U03, U04, U05, U06, U07, U09		De organisatie zal de oplossing inzetten bij klanten met operationele technologie.
B02	Functioneel	Must	U01, U02, U03, U05, U06, U08, U09		De organisatie zal haar klanten in staat stellen de beveiliging van OT te verbeteren.
B03	Functioneel	Must	U03, U07, U09, U12, U13		De organisatie zal met de oplossing haar security dienstverlening uitbreiden.
B04	Functioneel	Must	U03, U07, U10, U12, U13, U14		De organisatie zal de oplossing bij meerdere klanten inzetten.
B05	Niet-functioneel	Must	U07, U10, U12, U13, U14		De organisatie zal de oplossing als dienst leveren aan haar klanten.
B06	Niet-functioneel	Must	U05, U06		De organisatie zal de oplossing als product implementeren bij klanten.
B07	Functioneel	Must	U07, U13		De organisatie zal een advies krijgen over hoe de oplossing als dienst aan te bieden is.
B08	Functioneel	Should	U04, U05, U09, U11		De organisatie zal inzicht krijgen in dreigingen en kwetsbaarheden op IT-gebied in een OT-netwerk.

3.2.2. User requirements

Tabel 3, User requirements

Volg Nr.	Func/Non func	Prioriteit	Genereert	Realiseert	Beschrijving
U01	Functioneel	Must	S01	B01, B02	De securityspecialist zal een oplossing leveren aangeraden door onafhankelijk onderzoek.
U02	Functioneel	Must	S02, S06	B02	De leverancier van de klant zal extern beheer en onderhoud op de productiemachine uitvoeren.
U03	Functioneel	Must	S09, S10, S12	B01, B02, B03, B04	De netwerkspecialist zal het ontwerp bij verschillende klanten implementeren.
U04	Functioneel	Must	S04, S13	B01, B08	De netwerkspecialist zal inzicht krijgen in de aanwezige OT bij een klant.
U05	Functioneel	Must	S04, S13	B01, B02, B06, B08	De klanten van PCI zullen inzicht krijgen in de aanwezige OT.
U06	Functioneel	Must	S04, S07, S13, S15, S18	B01, B02, B06	De netwerkspecialist zal ondersteunt worden in het segmenteren van OT-netwerken.
U07	Niet-functioneel	Must	S05, S09, S10, S12, S17	B01, B03, B04, B05, B07	De service level manager zal de oplossing als managed dienst in een SLA opnemen.
U08	Functioneel	Must	S07	B02	De klant van PCI zal machines op afstand kunnen bedienen.
U09	Functioneel	Must	S03, S06, S08, S11, S13	B01, B02, B03, B08	De netwerkspecialist zal OT van klanten beter kunnen beveiligen.
U10	Functioneel	Should	S14	B04, B05	De netwerkspecialist zal de oplossing centraal kunnen beheren.
U11	Functioneel	Should	S04	B08	De klant van PCI zal geen OT netwerktekeningen aanleveren.
U12	Niet-functioneel	Should	S09, S14, S16, S17	B03, B04, B05	De servicedesk zal inkomende meldingen vanuit OT analyseren.
U13	Niet-functioneel	Should	S10, S12	B03, B04, B05, B07	De servicelevel managers zullen een dienstbeschrijving opstellen voor OT-security.
U14	Niet-functioneel	Should	S10, S14	B04, B05	De beheerders van PCI zullen afhankelijk van de functie toegang tot de oplossing hebben.

3.2.3. System requirements

Tabel 4, System requirements

Volg Nr.	Func/Non func	Prioriteit	Genereert	Realiseert	Beschrijving
S01	Niet-functioneel	Must		U01	De oplossing zal ingericht worden op basis van best practices.
S02	Functioneel	Must		U02	De oplossing zal leveranciers toestaan op een veilige manier verbinding te maken met productiemachines.
S03	Functioneel	Must		U09	De oplossing zal zoeken naar kwetsbaarheden in OT-systemen.
S04	Functioneel	Must		U04, U05, U06, U11	De oplossing zal het OT-netwerk schematisch in beeld brengen.
S05	Niet-functioneel	Must		U07	De oplossing zal afkomstig zijn van een gevestigde leverancier.
S06	Functioneel	Must		U02, U09	De oplossing zal OT-protocollen monitoren.
S07	Functioneel	Must		U06, U08	De oplossing zal ondersteunen in het veilig koppelen van OT en IT.
S08	Functioneel	Must		U09	De oplossing zal ondersteunen in het beveiligen van PLCs en HMI PCs
S09	Functioneel	Must		U03, U07, U12, U14	De oplossing zal over een centrale management interface beschikken.
S10	Niet-functioneel	Should		U03, U07, U13	De oplossing zal schaalbaar in te zetten zijn afhankelijk van de behoefte van de klant.
S11	Niet-functioneel	Should		U09	De oplossing zal gebruik maken van een CVE-database voor kwetsbaarheden.
S12	Niet-functioneel	Should		U03, U07, U13	De kosten van de oplossing zullen schaalbaar zijn voor klanten van verschillende formaten.
S13	Functioneel	Should		U04, U05, U06, U09	De oplossing zal ondersteunen in het beveiligen van legacy hard/software.
S14	Niet-functioneel	Should		U10, U12, U14	De oplossing zal over rolebased access beschikken.
S15	Niet-functioneel	Could		U06	De oplossing zal te koppelen zijn met de Palo Alto Next Gen Firewall.
S16	Functioneel	Could		U12	De oplossing zal in staat zijn om van meldingen automatisch incidenten aan te maken in Connectwise.
S17	Functioneel	Could		U07, U12	De oplossing zal in staat zijn om de huidige status van de te monitoren omgeving weer te geven in Logic Dashboards
S18	Functioneel	Won't have		U06	De oplossing zal communiceren met Aruba Clearpass voor automatische netwerksegmentatie.

4. Contextanalyse

Om ervoor te zorgen dat de resultaten van dit onderzoek bruikbaar zijn voor PCI, bij de klanten van PCI worden in dit hoofdstuk enkele randvoorwaarden opgesteld.

4.1. Methodiek

Om tot een lijst met randvoorwaarden te komen is een contextanalyse uitgevoerd. In de contextanalyse is gekeken naar de omgeving waar de resultaten van het onderzoek gebruikt gaan worden. De interne contextanalyse is uitgevoerd doormiddel van het 7-S model van McKinsey (Schop, 2022). Vanuit dit model is gekeken naar PCI als interne organisatie en is bijgevoegd in bijlage D. Daarnaast zijn voor de externe organisatie de leveranciers van PCI, concurrenten van PCI en klanten van PCI bekeken. Voor het verzamelen van informatie over de omgeving zijn interviews afgenomen met de stakeholders, is documentatie bekeken en is een observatie op locatie van een productiebedrijf uitgevoerd.

4.1.1. Interviews

De interviews zijn te vinden in bijlage A, de gebruikte interview methodiek in hoofdstuk 2.1. Voor de contextanalyse is gesproken met de volgende stakeholders:

- Field Service Manager PCI (als opdrachtgever)
- Netwerkspecialisten PCI
- Servicelevel managers PCI

Deze stakeholders zijn gekozen omdat deze stakeholders betrokken zijn bij het project en gecategoriseerd zijn als interne stakeholder, deze hebben daarom invloed op de interne organisatie. De stakeholderanalyse waarop deze keuze gebaseerd is, is te vinden in bijlage B.

4.1.2. Observatie

Voor de aanwezige systemen is een observatie uitgevoerd van de aanwezige systemen binnen PCI en bij klanten van PCI. Deze observatie is gedurende de afstudeerperiode tot stand gekomen.

4.1.3. Document analyse

Tot slot zijn interne documenten bekeken waarin de missie, visie en doelen van PCI zijn vastgelegd. (PCI Nederland, 2021) Daarnaast is de generieke SLA voor IT-diensten bekeken om te bepalen waaraan een dienst volgens PCI moet voldoen. (PCI IT-Solutions, 2022) Voor het bepalen van de concurrenten is online onderzoek uitgevoerd. Hierbij is gezocht naar IT-bedrijven die OT-security aanbieden.

4.2. Resultaten

De resultaten van de contextanalyse zijn opgedeeld in de interne organisatie en externe organisatie bestaande uit de klanten, concurrenten en leveranciers van PCI.

4.2.1. Interne organisatie PCI

PCI biedt haar klanten totale oplossingen waarmee de basis voor een werkplek kan worden geboden. PCI bestaat uit de business units IT-Solutions, Audiovisueel, Managed Print Services en Supplies. (PCI Nederland, 2022) De business unit IT-Solutions levert totale IT-oplossingen aan een groot aantal klanten. Dit onderzoek richt zich op productiebedrijven omdat deze bedrijven gebruik maken van OT. PCI wil haar klanten een zo compleet mogelijke werkplek bieden, vanuit de verschillende business units worden hiervoor oplossingen aangeboden. PCI wil altijd het beste voor de klant en wil vanuit verschillende specialismes complexe oplossingen kunnen bieden.

PCI heeft deskundige IT-specialisten in dienst die zelfstandig implementaties uitvoeren en incidenten oplossen. De medewerkers beschikken over een specialisme binnen de IT. Dit zijn de specialismes: Workspace Solutions, Datacenter Solutions, Networking & Security en Cloud Productivity

PCI biedt IT-oplossingen als eenmalige projecten of als managed dienst. De omgevingen bij klanten worden altijd op ongeveer dezelfde manier ingericht. PCI maakt standaard gebruik van de Palo Alto Next generation Firewall in combinatie met een Aruba Networks (HPe) switch omgeving. Routering vindt standaard plaats op de firewall. Daarnaast zijn er klanten die gebruik maken van de Barracuda Firewall. Bij een toenemend aantal klanten wordt gewerkt met Aruba Clearpass voor het automatisch toewijzen van een netwerksegment. (Azure) Active Directory wordt gebruikt voor het beheer van gebruikersaccounts. Voor het bijhouden van storingen maakt PCI intern gebruik van Connectwise. Het monitoren van de managed omgevingen bij klanten gaat via Logic Dashboards.

4.2.2. Externe organisatie PCI

Klanten PCI

De klanten van PCI nemen diensten of producten af bij één of meerdere business units van PCI. PCI heeft een groot aantal klanten die werkzaam zijn in verschillende branches. Een deel van deze klanten maakt gebruik van operationele technologie voor het aansturen van productiemachines.

Klanten hebben in bepaalde gevallen zelf intern ICT-personeel in dienst en maken gebruik van de diensten van PCI als aanvulling op de eigen IT-dienstverlening. Andere klanten hebben de totale IT-dienstverlening aan PCI uitbesteed, gebruikers bellen in deze gevallen direct met de klantenservice van PCI, PCI verzorgt in deze gevallen alle dienstverlening. PCI levert diensten aan kleine tot middelgrote bedrijven.

De productiebedrijven waarvoor dit onderzoek interessant is zijn grotere bedrijven met behoorlijke budgetten op het gebied van IT-security. Het uitvallen van een productielijn kan voor deze bedrijven catastrofale gevolgen hebben en is onaanvaardbaar. De te gebruiken machines zijn vaak waardevol en duur om te vervangen. Voor een oplossing die op security vlak ondersteunt in het langer operationeel houden van deze machines is daarom ruim budget beschikbaar. Hierbij moet uiteraard rekening worden gehouden met de omvang van de klanten. Het gaat om MKB tot MKB+ klanten. Deze productiebedrijven hebben in een aantal gevallen meerdere vestigingen verspreid over een groot gebied. Enkele bedrijven zijn volledig op één locatie gevestigd.

Voor de productiebedrijven is het niet goed bekend hoeveel systemen er in het OT-netwerk aanwezig zijn. OT-systemen zijn in veel gevallen verouderd en het updaten naar een nieuwe versie van bijvoorbeeld een besturingssysteem brengt te veel kosten met zich mee.

Leveranciers PCI

PCI levert IT-dienstverlening en koopt hiervoor producten en diensten in bij een groot aantal leveranciers binnen en buiten Nederland. PCI heeft de voorkeur om standaard gebruik te maken van producten die door haar partner leveranciers worden geleverd. Voor de IT-solutions business unit zijn de belangrijkste leveranciers:

- HP
- HP Enterprise
- Microsoft
- Aruba
- Palo Alto Networks
- Barracuda
- Citrix
- Rapid7
- MijnSam
- Sentinel One
- Acronis

(PCI Nederland, 2022)

PCI staat open voor contacten, overeenkomsten en partnerships met nieuwe leveranciers. Voorwaarde is wel dat de leverancier zich reeds heeft bewezen als leverancier van een stabiel en bewezen product.

Concurrenten PCI

Tot slot is een analyse uitgevoerd van de concurrenten van PCI op het gebied van security van operationele technologie door een IT-dienstverlener. Er is gezocht naar IT-bedrijven die informatie over OT-security op de website vermeld hebben. Er is gekeken naar Nederlandse IT-dienstverleners, dit omdat PCI een Nederlands bedrijf is en opereert en concurreert met bedrijven binnen Nederland. Uit dit onderzoek blijkt dat er slechts enkele grotere IT-dienstverleners en enkele specialistische IT-security bedrijven zijn die zich bezighouden met OT-security. Deze bedrijven staan in tabel 5.

Tabel 5, Concurrenten PCI

Bedrijf	Aangeboden diensten
CGI Nederland (CGI, 2022)	• Risicoanalyse • Firewall inrichten voor OT • Advies & consultancy
Capgemini (Capgemini, 2022)	• Risicoanalyse • Netwerkscans • Strategisch advies
Secura (Secura, 2022)	• Risicoanalyse • Kwetsbaarheden scan • Red teaming (Penetration testing)
Thales (Thales, 2019)	• IT/OT integratie
Access24 (Access24, 2022)	• OT-monitoring • OT discovery • OT vulnerability scanning

Wat opvalt uit de analyse is dat enkel een aantal grotere IT-leveranciers zich momenteel bezighouden met OT-security. Al deze bedrijven gebruiken bestaande IT-security technieken om klanten met OT beter te beveiligen. Dit gaat bij de meeste bedrijven momenteel enkel om risicoanalyses, strategisch advies en het segmenteren van netwerken. Specifieke OT-security oplossingen worden momenteel nog niet aangeboden op de publieke websites. Een aantal beveiligingsbedrijven bieden dat echter wel aan, dit zijn geen IT-dienstverleners en zijn daarom op IT gebied geen concurrenten van PCI. Dat PCI een OT-security dienst zou aanbieden maakt PCI hierom uniek vergeleken met haar concurrenten.

4.3. Conclusie

Vanuit de context analyse is gekeken naar randvoorwaarden, ook wel beperkende requirements, die gelden in de omgeving waar de uitkomst van dit onderzoek geïmplementeerd wordt. Deze randvoorwaarden geven aan waar de oplossing binnen moet passen om ingezet te kunnen worden door PCI bij klanten met operationele technologie. Randvoorwaarden zijn absolute vereisten en worden niet verder geprioriteerd.

Tabel 6, Randvoorwaarden

Nr.	Beschrijving
R01	Het ontwerp moet door een MSP-leverancier aan te bieden zijn.
R02	Het ontwerp moet in de op Aruba Networks gebaseerde netwerkomgeving te plaatsen zijn.
R03	De oplossing moet binnen het vakgebied van PCI passen. (IT)
R04	De oplossing moet achter een door PCI geïmplementeerde firewall te plaatsen zijn.
R05	Het ontwerp moet in een complex IT-netwerk met meerdere VLANs te implementeren zijn.

Na het opstellen van de randvoorwaarden is antwoord gegeven op deelvraag twee en drie van dit onderzoek. De requirements en randvoorwaarden geven antwoord op deze deelvragen.

5. Literatuuronderzoek

In dit literatuuronderzoek is begonnen met het verder definiëren van de definitie van OT, vervolgens is gekeken naar recente dreigingen op het gebied van OT. Hiermee kunnen deelvraag één en vier worden beantwoord. Verder is in dit literatuuronderzoek gezocht naar best practices die kunnen dienen als ontwerpprincipes tijdens de volgende fase van het ontwerponderzoek, deze vallen onder deelvraag vijf.

5.1. Methodiek

In dit hoofdstuk is gezocht naar relevante literatuur welke kan bijdragen aan de beantwoording van onderzoeksvragen. Het is van belang dat literatuur voldoende betrouwbaar en valide is. De betrouwbaarheid wordt gewaarborgd door enkel gebruik te maken van betrouwbare bronnen. In dit onderzoek wordt enkel gewerkt met wetenschappelijke publicaties (te herleiden naar een erkende universiteit, databank of overheidsinstantie) en publicaties en whitepapers van gerenommeerde gevestigde organisaties zoals grote IT-leveranciers.

De validiteit wordt gewaarborgd door bij elke stelling een bron te vermelden en uitspraken te onderbouwen doormiddel van een ontwerpprincipe, op deze manier wordt iedere uitspraak op dezelfde manier beschreven en is elke uitspraak te herleiden naar één of meerdere bronnen.

Voor de volgende fase zijn in dit literatuuronderzoek ontwerpprincipes gezocht. Ontwerpprincipes worden altijd volgens een vaste standaard geformuleerd “**Als** probleem **dan** oplossing **omdat** redernering uit de literatuur” (Linden, Hageraats, & Haveman, 2016)

5.2. Resultaten

In dit hoofdstuk zijn de resultaten van het literatuuronderzoek beschreven.

5.2.1. Definitie OT

Gartner schrijft: “Operationele technologie (OT) is hardware en software die een verandering detecteert of veroorzaakt door de directe bewaking en/of controle van industriële apparatuur, activa, processen en gebeurtenissen.” (Gartner, 2022) Het Digital Trust Center schrijft: “Operational Technology (OT) is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld zoals het aansturen en monitoren van (industriële) apparatuur. Het kan dan gaan om het uitlezen van sensoren of het inschakelen van een pomp of schakelaar op basis van een bepaalde conditie.” (Digital Trust Center, 2022) Naast OT wordt in de literatuur vaak gesproken over Industrial Control Systems (ICS). ICS heeft in de literatuur, in de industriële context dezelfde definitie als OT, echter wordt met ICS vaak één enkel component bedoeld terwijl OT meer als verzameling van een groep ICS-systemen kan worden gezien. (Williamson, 2015) Verder wordt vaak gesproken over Supervisory Control and Data Acquisition (SCADA) waarmee de interface wordt bedoeld waarmee de industriële processen gecontroleerd en visueel inzichtelijk worden gemaakt in een user interface. (Williamson, 2015)

De totale definitie van OT is breder als in de context van productiesystemen. Het aansturen van fysieke processen komt bijvoorbeeld ook voor in de zorg waar medische systemen worden gebruikt voor het toedienen van medicatie, controle van lichaamsfuncties en het geven van een alarm als een bepaalde conditie zich voordoet of ergens van wordt afgeweken. (PWC, 2020) Een security incident op deze OT kan direct het leven van een mens in gevaar brengen. Daarnaast kan OT ook voorkomen in gebouwbeheersystemen, een brand- of inbraakalarm en toegangscontrole systemen. Ook hier wordt een vooraf geprogrammeerd programma gebruikt voor het aansturen of monitoren van een fysiek proces. (NIST, 2022)

Omdat de probleemstelling van deze opdracht zich richt op operationele technologie in productiebedrijven richt dit onderzoek zich hier ook verder op.

OT bestaat net als IT vaak uit een netwerk met switches en routers. IT bestaat echter voor een belangrijker deel uit computers, storage en servers. OT bestaat voornamelijk uit industriële apparatuur en computers waarmee industriële apparatuur wordt aangestuurd en gecontroleerd. (Bigelow &

Lutkevich, 2021) OT bestaat vaak uit een verzameling van HMIs, PLCs, DCSs en SCADA-systemen. (RedHat, 2022)

Een PLC (programmable logic controller) is een industriële computer ontworpen voor het besturen van productieprocessen. PLCs hebben ingangen en uitgangen en voeren op basis van input een programma uit welke weer output levert. Een PLC kan aan een SCADA of HMI (Human Machine Interface, een gebruikersinterface voor het bedienen van machines) gekoppeld worden waarmee de werking van een PLC kan worden aangepast indien nodig. (AT-Automation, 2022) Voor de verbinding met een SCADA of HMI kan een PLC met een ethernet verbinding worden aangesloten op een netwerk. Hierdoor kan de PLC worden benaderd via het OT-netwerk en kan het programma worden beïnvloed of aangepast vanaf een PC.

PLCs worden vaak gebruik voor het aansturen van één enkel proces. Een DCS (distributed control system) wordt gebruikt om meerdere processen aan te sturen en te controleren. (Budimir, 2022)

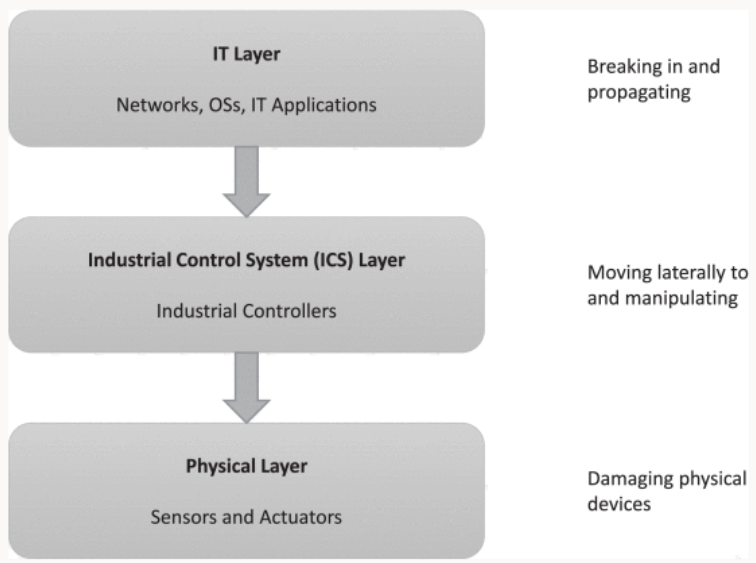
Met dit deel van het literatuuronderzoek is antwoord gegeven op deelvraag één: “Wat is OT en waar bestaat OT uit?”. Uit het literatuuronderzoek valt te concluderen dat OT bestaat uit hardware en software welke gebruikt wordt voor het aansturen van fysieke industriële processen en apparatuur. OT bestaat uit een verzameling van PLCs, DCSs, HMIs en SCADA-oplossingen. Deze systemen werken samen om zo industriële apparatuur te bedienen.

5.2.2. Dreigingen OT

Om een goed beeld te krijgen waar klanten van PCI kwetsbaar voor zijn op OT gebied is literatuuronderzoek gedaan naar dreigingen op het gebied van OT-security. Hiermee kan antwoord worden gegeven op deelvraag vier van dit onderzoek: “Welke dreigingen zijn er op het gebied van OT?”.

In de literatuur valt te lezen dat de laatste jaren de behoefte aan data uitwisseling tussen IT en OT steeds groter wordt. Cyberaanvallen kwamen al langer voor op IT en door de verbondenheid met OT komen cyberaanvallen op OT-omgevingen vaker voor. (PWC, 2019) Dit is ook zichtbaar in de cijfers over aanvallen op OT-systemen. Een steeds groter aandeel van het totaal aantal cyberaanvallen is gericht op operationele technologie. (Kaspersky, 2021) OT-systemen zijn oorspronkelijk niet ontworpen vanuit het oogpunt van IT-security. OT bestond oorspronkelijk uit individuele machines of kleine fysieke netwerken die enkel fysiek door een medewerker te bedienen waren. In de loop van de jaren zijn steeds meer OT-systemen aan het internet gekoppeld om gebruik te maken van bestaande IT-oplossingen. (Anton, et al., 2021) OT-systemen zijn daarnaast in veel gevallen ontworpen om vele jaren gebruikt te worden. De aanschaf van productiemachines is een grote kostenpost welke over een langere periode moet worden terugverdiend. In deze periode raken onderdelen van OT zoals software, communicatieprotocollen, encryptiemethodieken en besturingssystemen out of date. (Conklin, 2016) Er moet hierom worden nagedacht dat als er een productiemachine wordt aangeschaft met een lange levensduur, dan moet er een plan zijn voor het veilig inzetten van legacy software, omdat IT in de regel een kortere levensduur heeft dan een productiemachine.

Het type malware dat door beveiligingsonderzoekers van Kaspersky voornamelijk wordt aangetroffen op aan OT gekoppelde computers zijn backdoors (Trojans) en spyware. (Kaspersky, 2021) Dit kan erop wijzen dat er veel bedrijfsspionage voorkomt op OT-systemen. Daarnaast zijn er ook aanwijzingen dat deze malware wordt gebruikt voor het beïnvloeden van veiligheidssystemen in operationele processen om zo productieprocessen te verstoren. In het verleden is er een bekend voorbeeld geweest van malware speciaal ontworpen om de controle over OT te verkrijgen en hiermee gericht grote schade te veroorzaken, dit ging om de malware genaamd Triton. Waarschijnlijk is deze malware op het OT-netwerk terechtgekomen vanuit het interne IT-netwerk via een slecht gepatchte Windows computer. (Giles, 2019) Uit onderzoek blijkt daarnaast ook dat aanvallen op OT vaak zijn gestart vanaf een IT-omgeving. Er wordt geprobeerd in te breken op het IT-netwerk van een organisatie, de meest voorkomende methode is hierbij Social Engineering. Social engineering is een hacking techniek waarbij toegang tot een organisatie wordt gekregen door middel van psychologische manipulatie van medewerkers. (Digital Trust Center, 2022) Vanuit hier wordt in de meeste gevallen een aanval gedaan op een ICS-component, dit zijn vaak computers die fysieke OT aansturen. Vanaf deze systemen kan dan ook fysieke OT worden aangevallen. (Anton, et al., 2021) Onderstaand figuur geeft dit proces weer.



Figuur 2, Veelgebruikte werkwijze OT aanval (Anton, et al., 2021)

Het ontwerpprincipe dat hieruit kan worden getrokken is: als je OT wil beveiligen tegen externe dreigingen, dan zal je ook rekening moeten houden met dreigingen vanaf het interne IT-netwerk, omdat deze netwerken tegenwoordig nauw verbonden zijn. (Anton, et al., 2021) (Giles, 2019)

Omdat OT voor veel bedrijven kritiek is voor het primaire bedrijfsproces is het voor criminelen zeer aantrekkelijk om een OT-netwerk te infecteren met ransomware. “Ransomware is malware die systemen van gebruikers versleutelt met als doel om deze later te ontsleutelen in ruil voor losgeld.” (Nationaal Cyber Security Centrum, 2022) De laatste jaren neemt het aantal meldingen van ransomware op OT-netwerken sterk toe. Vaak gaat het in deze gevallen om ransomware die ook wordt aangetroffen op IT-netwerken, ransomware speciaal ontworpen voor OT komt weinig voor. (Holmström, 2021) Toch zijn er inmiddels vormen van ransomware gericht op PLCs. Deze ransomware werkt vaak anders als traditionele ransomware en richt zich niet op het versleutelen van systemen doormiddel van het versleutelen van gegevens maar op het onbeschikbaar maken van een PLC door overbelasting, het injecteren van corrupte programmacode of het veroorzaken van foutmeldingen waardoor de PLC zichzelf of een machine uitschakelt. (Zhang, 2020) Dit onderzoek bevestigt ook dat in bijna alle gevallen de aanval verloopt via een reeds geïnfecteerde traditionele computer of een besmet USB-station. De ransomware kan bijna nooit direct vanaf het internet op de PLC worden geplaatst. Hieruit volgt een ontwerpprincipe: Als je een aanval op OT-hardware wil voorkomen, dan zul je deze OT moeten beschermen van interne IT-bronnen, omdat onderzoek uitwijst dat malware voor PLCs vaak op het OT-netwerk terechtkomt via een traditioneel IT-systeem. (Zhang, 2020) (Holmström, 2021)

Binnen de IT-security ligt de focus vaak op het bekende CIA-model (confidentiality, integrity and availability) Dit zijn drie perspectieven die bij de beveiliging van standaard IT van belang zijn. Een IT-omgeving moet beschikbaar, afgeschermd en integer zijn. Hier zit een groot contrast met OT-security. OT moet ervoor zorgen dat processen veilig verlopen en bij een incident kan dit fysieke gevolgen hebben voor mensen, de omgeving en het milieu. (Hollerer, Kastner, & Sauter, 2021) Hieruit kan worden gesteld dat naast het afschermen en integer houden van data het voor OT ook van belang is om systemen af te schermen van ongewenste bediening. Bij het opstellen van een risicoanalyse moet er worden gekeken naar de samenhang van veiligheid en de bekende IT CIA driehoek. Een veiligheidsincident kan ervoor zorgen dat de beschikbaarheid van een productiesysteem wordt aangetast. Uit dit onderzoek volgt het ontwerpprincipe: als de beveiliging van OT verbeterd wordt, dan is het van belang om een risicoanalyse uit te voeren die verder als de CIA-driehoek gaat, omdat bij OT ook fysieke beveiliging en de veiligheid van mensen en milieu een grote rol spelen. (Hollerer, Kastner, & Sauter, 2021)

In dit deel van het literatuuronderzoek is antwoord gegeven op deelvraag vier: “Welke dreigingen zijn er op het gebied van OT?”. Dreigingen op OT komen in veel gevallen vanuit het interne IT-netwerk van organisaties, dit omdat deze netwerken steeds vaker onderling verbonden zijn. (PWC, 2019) Via

een bekende hacking techniek (zoals social engineering, password guessing, man-in-the-middle, spyware of trojan horse installatie) probeert een aanvaller binnen te komen op het interne netwerk, daarmee is de firewall aan de buitenkant van een organisatie overwonnen. Doordat het vaak slecht mogelijk is om direct in te breken op een PLC, DCS of HMI vindt er in de meeste gevallen vanaf het IT-netwerk een aanval plaats op een traditionele computer op het OT-netwerk. (Anton, et al., 2021) Risico's voor OT zijn er op het gebied van bedrijfsspionage, het stil leggen van een productielijn of het toebrengen van schade aan mensen of de omgeving. Het gaat hier in veel gevallen om het beïnvloeden van OT doormiddel van het injecteren van programmacode. (Kaspersky, 2021) (Zhang, 2020) Leveranciers hebben in veel gevallen extern toegang tot het OT-netwerk, deze verbinding vanaf het internet introduceert tevens een kwetsbaarheid in het OT-netwerk.

5.2.3. Best practices

Voor het beantwoorden van deelvraag vijf is gezocht naar een aantal best practices op het gebied van OT-security. Deze best practices zijn afkomstig uit literatuur van IT-onderzoeksbureaus, overheden, universiteiten en gerenommeerde leveranciers. Verder is gezocht naar bestaande standaarden in de OT-security.

Bestaande standaarden

Binnen de IT wordt vaak gewerkt met normen en standaarden van ISO. Een bekende norm is de ISO 27001, deze norm richt zich op informatie security (ISO, 2013) bij OT gaat het echter voornamelijk om de beveiliging van fysieke systemen en processen. Het beveiligen van informatie is hier minder van toepassing, het zou daarom geen goed idee zijn om de OT-omgeving te toetsen aan de ISO 27001 standaard en dan te concluderen dat de beveiliging voldoende is ingericht.

Er bestaat een NEN-norm voor cyber security op het gebied van operationele technologie, dit gaat om de norm IEC 62443. Deze norm richt zich echter voornamelijk op de beveiliging lokaal op de systemen en biedt best practices voor communicatie, user rollen en encryptie en is dus voornamelijk van toepassing voor de leverancier van de productiemachines (machineleveranciers van klanten van PCI). Alleen de leverancier van de productiemachine kan bepalen welke communicatieprotocollen er gebruikt worden, hoe deze versleuteld worden en hoe welke userrollen er lokaal in de productiesystemen geconfigureerd kunnen worden. Slechts voor een (klein) deel van de norm gaat het om netwerkbeveiliging, segmentatie en monitoring. Voor PCI als IT-dienstverlener is het daarom niet mogelijk om klanten te certificeren voor deze norm. De norm richt zich bijvoorbeeld op wachtwoordbeleid voor PLCs, user rollen op SCADA en encryptie van OT-protocollen. (IEC, 2013) Wel schrijft de norm voor dat netwerken op OT gebied gesegmenteerd moeten worden van alle andere netwerken, moet de externe toegang tot machines alleen worden toegestaan op incidentele basis en moeten alle systemen op een least privilege manier worden ingericht. De norm kan daarom worden gebruikt voor het onderschrijven van een aantal best practices in dit literatuuronderzoek.

Verder zijn er meerdere internationale en nationale instanties die best practices aanbieden voor de beveiliging van operationele technologie. Dit zijn echter nog geen standaarden waaraan een organisatie gecertificeerd kan worden. In dit hoofdstuk wordt een breed onderzoek opgezet om tot best practices te komen om daarmee een zo optimaal mogelijke OT-security dienst aan klanten aan te kunnen bieden.

Best practices

Uit onderzoek van TNO volgen een aantal succesfactoren waaraan voldaan moet worden om OT-security op een professionele manier vorm te geven in een organisatie. TNO schrijft dat voor het veilig houden van het primaire bedrijfsproces het van belang is om assetmanagement op orde te hebben. Zonder juist assetmanagement is een goede risicoanalyse niet mogelijk. TNO schrijft voor om een CMDB bij te houden met daarin informatie over alle aanwezige OT inclusief informatie over leveranciers en gebruikte software. Bij een aanpassing moet dit direct in de CMDB aangepast worden. Het ontwerpprincipe dat hieruit voortkomt is: als je OT-security op een professionele manier wil opzetten in een organisatie, dan is het van belang om assetmanagement goed te implementeren omdat het anders niet mogelijk is om een compleet beeld te hebben van de risico's in het OT-netwerk. (Vos, Brink, & Schie, 2019) Voor een inventarisatie van aanwezige OT raadt Gartner aan om gebruik te maken van specialistische OT discovery tools. Deze zijn gericht op het vinden van OT-hardware en zullen tot betere resultaten komen als traditionele netwerkscanners. (Contu & Orans, 2020) Dit resulteert in ontwerpprincipe: Als er een goed beeld moet komen van de aanwezige OT, dan is het

van belang om specialistische OT discovery scanners te gebruiken, omdat traditionele netwerkscanners minder geschikt zijn voor het opsporen van OT. (Contu & Orans, 2020) Het goed in kaart brengen van OT is ook een van de aangeraden stappen in NEN 62443 (IEC, 2013)

Het Digital Trust Center van het ministerie van economische zaken geeft aan dat het verstandig is om OT en IT op netwerkgebied van elkaar te scheiden. Verder wordt aangegeven dat als OT-systemen geen software updates meer krijgen het verstandig is om via netwerksegmentatie deze systemen te isoleren. Dit kan voorkomen dat malware zich kan verspreiden binnen een netwerk. Hieruit kan het ontwerpprincipe worden opgesteld: Als er gebruik wordt gemaakt van OT welke geen software updates meer ontvangen, dan is het verstandig om deze systemen op netwerkniveau te isoleren, omdat niet geüpdatete systemen een risico vormen in de verspreiding van malware. (Digital Trust Center, 2022)

Verder is netwerksegmentatie van belang als het gaat over verschillende niveaus van security binnen een OT-netwerk. Hierbij zou gewerkt moeten worden volgens het least access privilege principe en communicatie zou moeten worden ingericht op basis van white listing in plaats van black listing. Dit volgens het principe: als het niet nodig is om een OT-systeem met een ander netwerk te verbinden, dan moeten deze systemen niet verbonden worden omdat dit de kans op het verspreiden van malware via het netwerk of inbraak vanaf het internet kan voorkomen. (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015) Ook het segmenteren van netwerken, zover als mogelijk is wordt aangeraden in de NEN 62443 norm. (IEC, 2013)

Het Digital Trust Center raadt aan dat wanneer er op afstand verbinding moet worden gemaakt met een OT-systeem er moet worden voorkomen dat deze systemen direct met het internet verbonden worden. Het is verstandig om gebruik te maken van een “Jump Host”. Hieruit komt het ontwerpprincipe: Als een OT-systeem extern moet worden beheerd, dan is het verstandig om met een “Jump Host” te werken, omdat dit voorkomt dat kwetsbare OT direct aan het internet wordt aangesloten. (Digital Trust Center, 2022) Gartner en het NIST onderschrijven dit principe en raden aan om een soort DMZ te creëren tussen het IT en OT-netwerk. (Contu & Orans, 2020) (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015) Het NIST stelt daarnaast dat als een leverancier remote een verbinding wil maken met de jump host, dan zal dit met een versleuteld protocol zoals VPN moeten gebeuren, omdat deze verbinding anders onderschept kan worden door ongewenste externen. (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015)

De NEN-norm 62443 geeft daarnaast aan dat deze verbinding tot stand gebracht zou moeten worden met gebruik van multifactor authenticatie wanneer verbinding vanaf een extern netwerk wordt gestart. (IEC, 2013) Als er vanaf een extern, onvertrouwd netwerk een verbinding wordt opgezet met het OT-netwerk, dan moet hiervoor gebruik worden gemaakt van een vorm van multifactor authenticatie, omdat dit ervoor zorgt dat de verbinding minder makkelijk te misbruiken is door het wachtwoord te raden. (IEC, 2013)

Ook Gartner heeft een top-10 securitymaatregelen voor OT-omgevingen opgesteld, deze bestaat uit zowel bedrijfsmatige als technische maatregelen. De technische maatregelen zijn voor het belangrijkste deel maatregelen die eerder beschreven zijn, dit onderschrijft het belang van asset inventory, netwerksegmentatie en patching. Verder beschrijft dit onderzoek het belang van het definiëren van rollen in OT-security, training van gebruikers, incident response en monitoring. Medewerkers die zich bewust zijn van de risico’s die ontstaan bij het gebruik van OT (bijvoorbeeld toegang aan externen bieden, websites bezoeken, USB-stations gebruiken) zullen hier veiliger mee omgaan. Als je OT-security binnen de organisatie wil verbeteren, dan is het van belang om medewerkers bewust te maken van hun rollen en verantwoordelijkheid, omdat dit voorkomt dat ongewenste personen toegang krijgen tot deze systemen. (Moore, 2021)

In de best practices staat ook het belang van monitoring benoemd, onverwacht netwerkverkeer moet worden gerapporteerd. Door het tijdig rapporteren van verdacht netwerkverkeer kan een aanvaller eerder opgemerkt worden en kan een aanval tijdig geblokkeerd worden. Als OT verbinding kan krijgen met andere IT/OT systemen, dan is netwerklogging en monitoring van belang, omdat veel aanvallen op OT via het netwerk verspreid worden tussen systemen. (Moore, 2021) (Zhang, 2020)

Gartner onderschrijft verder dat voor een snel herstel na een aanval op OT het van belang is om scenario’s voor te bereiden. Zo kan er gedacht worden aan het maken van een back-up van productieprogramma’s, het afsluiten van een reparatie overeenkomst met een leverancier en het

gereed hebben van een recovery plan. Als je na een aanval op OT snel weer beschikbaar wil zijn, dan is een plan voor disaster recovery en juiste back-ups van belang, omdat ook in goed beveiligde OT-omgevingen een aanval niet uit te sluiten is. (Moore, 2021)

General Electric geeft aan dat als er een firewall of monitoring tool wordt ingezet in een OT-netwerk, dan moet deze naast bekende IT-protocollen (SMTP, DNS, DHCP, TCP, UDP, etc.) ook specifieke OT-protocollen (Modbus, DNP3, OPC, etc.) kunnen lezen, omdat OT-protocollen inhoudelijk sterk verschillen van traditionele IT-protocollen. (GE, 2022) Daarnaast stelt het NIST dat het wordt afgeraden dat als er gebruik wordt gemaakt van industriële OT-protocollen, dan zouden deze niet zomaar het OT-netwerk mogen verlaten, omdat deze protocollen vaak niet zijn ontworpen vanuit security oogpunt en deze eenvoudig te onderscheppen zijn. (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015)

5.3. Conclusie

Vanuit bovenstaand literatuuronderzoek zijn ontwerpprincipes opgesteld. Deze worden gebruikt voor het beantwoorden van deelvraag vijf en vormen de input voor het ontwerp en adviesrapport.

Deelvraag vijf zoekt naar best practices op het gebied van OT-security. Deze best practices zijn samen te vatten in de ontwerpprincipes welke in dit hele literatuuronderzoek gevonden zijn. Het antwoord op deelvraag vijf: “Welke best practices zijn er op het gebied van OT-security?” is daarom een verzameling van onderstaande ontwerpprincipes:

Per ontwerpprincipe is aangegeven waarom deze wel/niet wordt gebruikt in het ontwerp of advies. Deze selectie is gemaakt omdat enkele ontwerpprincipes in strijd zijn met de context- of requirementsanalyse of buiten de scope van dit project vallen.

P1) Als je OT wil beveiligen tegen externe dreigingen, dan zal je ook rekening moeten houden met dreigingen vanaf het interne IT-netwerk, omdat deze netwerken tegenwoordig nauw verbonden zijn. (Anton, et al., 2021) (Giles, 2019)
   a) Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.
P2) Als er een productiemachine wordt aangeschaft met een lange levensduur, dan moet er een plan zijn voor het veilig inzetten van legacy software, omdat IT in de regel een kortere levensduur heeft als een productiemachine. (Conklin, 2016)
   a) Dit ontwerpprincipe wordt meegenomen in de selectie van methodieken. Het opstellen van een plan is echter de verantwoordelijkheid voor de organisatie die de productiemachine koopt en niet van PCI als IT-dienstverlener.
P3) Als je een aanval op OT-hardware wil voorkomen, dan zul je deze OT moeten beschermen van interne IT-bronnen, omdat onderzoek uitwijst dat malware voor PLCs vaak op het OT-netwerk terechtkomt via een traditioneel IT-systeem. (Zhang, 2020) (Holmström, 2021)
   a) Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.
P4) Als de beveiliging van OT verbeterd wordt, dan is het van belang om een risicoanalyse uit te voeren die verder als de CIA-driehoek gaat, omdat bij OT ook fysieke beveiliging en de veiligheid van mensen en milieu een grote rol spelen. (Hollerer, Kastner, & Sauter, 2021)
   a) *Dit ontwerpprincipe richt zich op fysieke veiligheid, en hoewel dit het belang van OT-security onderschrijft kan dit niet door een IT-dienstverlener zoals PCI geleverd worden binnen een dienst.*
P5) As je OT-security op een professionele manier wil opzetten in een organisatie, dan is het van belang om assetmanagement goed te implementeren omdat het anders niet mogelijk is om een compleet beeld te hebben van de risico’s in het OT-netwerk. (Vos, Brink, & Schie, 2019)
   a) Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.
P6) Als er een goed beeld moet komen van de aanwezige OT, dan is het van belang om specialistische OT discovery scanners te gebruiken, omdat traditionele netwerkscanners minder geschikt zijn voor het opsporen van OT. (Contu & Orans, 2020)
   a) Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.
P7) Als er gebruik wordt gemaakt van OT welke geen software updates meer ontvangen, dan is het verstandig om deze systemen op netwerkniveau te isoleren, omdat niet bijgewerkte systemen een risico vormen in de verspreiding van malware. (Digital Trust Center, 2022)
   a) Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.

P8) Als het niet nodig is om een OT-systeem met een ander netwerk te verbinden, dan moeten deze systemen niet verbonden worden omdat dit de kans op het verspreiden van malware via het netwerk of inbraak vanaf het internet kan voorkomen. (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015)
   a) *Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.*

P9) Als een OT-systeem extern moet worden beheerd, dan is het verstandig om met een “Jump Host” te werken, omdat dit voorkomt dat kwetsbare OT direct aan het internet wordt aangesloten. (Digital Trust Center, 2022)
   a) *Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.*

P10) Als je OT-security binnen de organisatie wil verbeteren, dan is het van belang om medewerkers bewust te maken van hun rollen en verantwoordelijkheid, omdat dit voorkomt dat ongewenste personen toegang krijgen tot deze systemen. (Moore, 2021)
   a) *Dit ontwerpprincipe wordt niet meegenomen, het bewust maken van medewerkers is de verantwoordelijkheid van de klant van PCI.*

P11) Als OT-verbinding kan krijgen met andere IT/OT systemen, dan is netwerklogging en monitoring van belang, omdat veel aanvallen op OT via het netwerk verspreid worden tussen systemen. (Moore, 2021) (Zhang, 2020)
   a) *Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.*

P12) Als een leverancier remote een verbinding wil maken met de jump host, dan zal dit met een encrypt protocol zoals VPN moeten gebeuren, omdat deze verbinding anders onderschept kan worden door ongewenste externen. (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015)
   a) *Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.*

P13) Als er vanaf een extern, onvertrouwd netwerk een verbinding wordt opgezet met het OT-netwerk, dan moet hiervoor gebruik worden gemaakt van een vorm van multifactor authenticatie, omdat dit ervoor zorgt dat de verbinding minder makkelijk te misbruiken is door het wachtwoord te raden. (IEC, 2013)
   a) *Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.*

P14) Als je na een aanval op OT snel weer beschikbaar wil zijn, dan is een plan voor disaster recovery en juiste back-ups van belang, omdat ook in goed beveiligde OT-omgevingen een aanval niet uit te sluiten is. (Moore, 2021)
   a) *Dit kan aan klanten geadviseerd worden maar wordt niet ondergebracht in een OT-security dienst omdat dit buiten de scope van een dienst valt.*

P15) Als er een firewall of monitoring tool wordt ingezet in een OT-netwerk, dan moet deze naast bekende IT-protocollen (SMTP, DNS, DHCP, TCP, UDP, etc.) ook specifieke OT-protocollen (Modbus, DNP3, OPC, etc.) kunnen lezen, omdat OT-protocollen inhoudelijk sterk verschillen van traditionele IT-protocollen. (GE, 2022)
   a) *Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.*

P16) Als er gebruik wordt gemaakt van industriële OT-protocollen, dan zouden deze niet zomaar het OT-netwerk mogen verlaten, omdat deze protocollen vaak niet zijn ontworpen vanuit security oogpunt en eenvoudig te onderscheppen zijn. (Stouffer, Pillitteri, Lightman, Abrams, & Hahn, 2015)
   a) *Dit ontwerpprincipe wordt meegenomen in het technisch ontwerp.*

6. Ontwerp

Dit hoofdstuk bevat het ontwerp van enkele standaarden welke PCI kan aanbieden voor het verbeteren van de OT-netwerk omgevingen bij klanten. In dit hoofdstuk wordt antwoord gegeven op deelvraag zes van het onderzoek: “Welke oplossingen, methodieken en producten kunnen in een OT-security dienst worden aangeboden?”.

6.1. Methodiek

Gedurende het vooronderzoek zijn in de verschillende hoofdstukken requirements, randvoorwaarden en ontwerpprincipes gevonden. In dit hoofdstuk wordt een ontwerp gemaakt van enkele universele diensten welke PCI bij haar klanten in kan zetten voor het verbeteren van de beveiliging van operationele technologie. Het document bestaat uit een functioneel ontwerp met een dienstbeschrijving, use-case diagrammen en een architectuurmodel, een productselectie op basis van het vooronderzoek en een technisch ontwerp. Het ontwerp wordt in het volgende hoofdstuk geverifieerd op basis van de requirements, randvoorwaarden en ontwerpprincipes. Per onderdeel van het ontwerp wordt de gebruikte methodiek toegelicht.

6.2. Vereiste functionaliteiten

Uit het literatuuronderzoek blijkt dat om OT bij klanten van PCI op een goede manier te beveiligen het vereist is om gebruik te maken van één of meerdere oplossingen op basis van best practices. Zo moet er een oplossing worden gevonden voor het in kaart brengen van aanwezige OT bij een bedrijf. Ook moet de oplossing kunnen zoeken naar kwetsbaarheden in een OT-component of het netwerk en verdacht netwerkverkeer op het OT-netwerk. Ook moeten leveranciers op een veilige manier verbinding kunnen maken met het OT-netwerk. Deze onderdelen kunnen nog niet worden geleverd met een bestaand product dat PCI momenteel in haar portfolio heeft.

Verder moet de beveiliging van het netwerk bij klanten met operationele technologie worden verbeterd. PCI voert al netwerkimplementaties uit maar heeft nog geen standaard voor het inrichten van OT-netwerken. Er moet een standaard komen voor het segmenteren van netwerken zodat OT en IT niet onderling verbonden zijn maar wel veilige toegang tot bepaalde IT-bronnen mogelijk is en zodat componenten in het OT-netwerk niet onnodig verbonden zijn met andere componenten in het OT-netwerk. Dit laatste wordt uitgewerkt in een standaard die PCI kan inzetten bij het uitvoeren van netwerkimplementaties of netwerkverbeteringen in OT-omgevingen bij klanten. Dit is geen nieuwe dienst omdat PCI al netwerkimplementaties uitvoert maar is wel nieuw omdat er momenteel geen standaard werkwijze is voor het opbouwen van een OT-netwerk. Het technische ontwerp beschrijft een standaard voor deze segmentaties

De OT-security diensten van PCI moeten de volgende functionaliteit bieden. Per functionaliteit is aangegeven op welke ontwerpprincipes dit gebaseerd is.

Tabel 7, Vereiste functionaliteiten

Functionaliteit	Ontwerpprincipe
Asset discovery	P5, P6
OT vulnerability scanning	P2
OT netwerk monitoring	P11, P15
Leverancier toegang via jump host	P9, P12, P13
Netwerksegmentatie	P1, P3, P7, P8, P16

Op basis hiervan moet er een nieuw product aan het portfolio van PCI worden toegevoegd. Een product dat binnen een nieuwe dienst kan worden aangeboden voor OT asset discovery, kwetsbaarheden inventarisatie, netwerk monitoring en veilige toegang voor leveranciers. PCI heeft aangegeven dat hier een nieuw product voor kan worden ingekocht. Voor het segmenteren van netwerken wil PCI gebruik kunnen maken van de bestaande producten waarvoor een partnerrelatie bestaat.

6.3. Use-Case diagrammen

Om een goed beeld te krijgen van de eisen aan het technisch ontwerp en als input voor het adviesrapport is in kaart gebracht welke actoren bepaalde functies uitvoeren met het ontwerp. Dit is weergegeven in een aantal use-case diagrammen. Use-case diagrammen geven voornamelijk de functionele eisen aan het ontwerp weer.

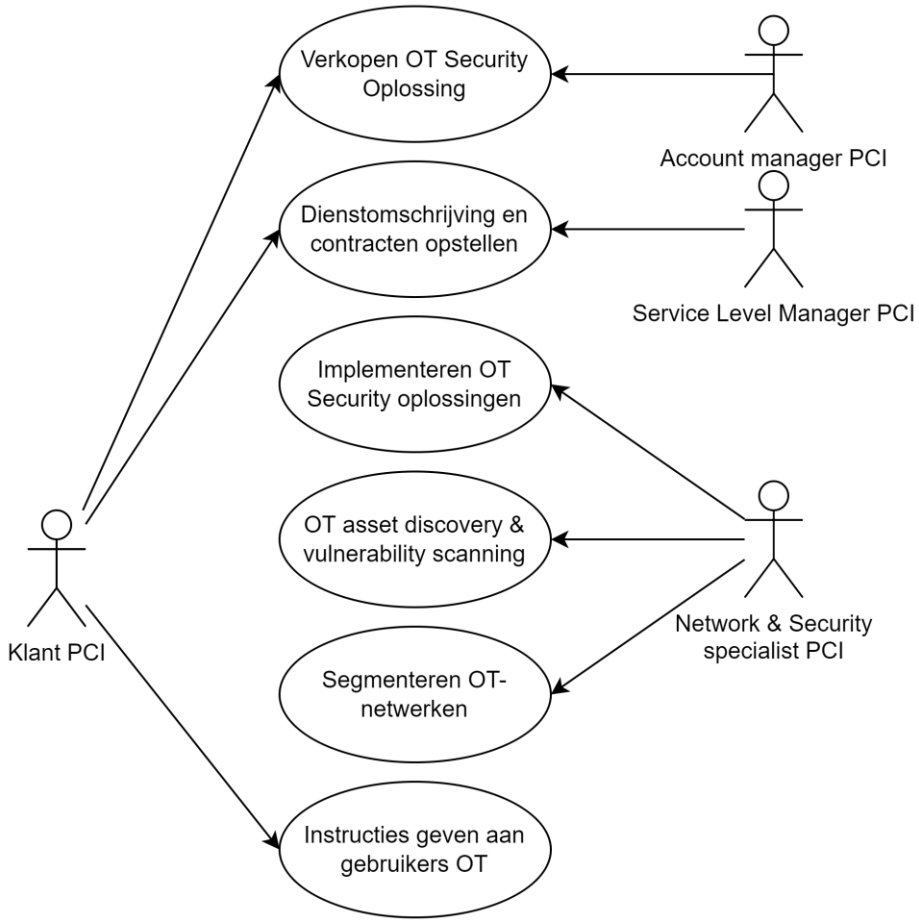
6.3.1. Methodiek

Voor het opstellen van onderstaande use-case diagrammen is gebruik gemaakt van de modelleertaal UML. (Fowler, 2003) Aan de linkerkant van de use-case diagrammen staan de externe stakeholders, aan de rechterkant de interne stakeholders. De stakeholders zijn betrokken bij de activiteiten waaraan ze verbonden zijn. In het architectuurmodel worden deze activiteiten verder uitgewerkt. Voor het invullen van de activiteiten in de use-cases is gebruik gemaakt van de resultaten van de behoefte- en contextanalyse.

6.3.2. Resultaten

Use-case diagram implementatie OT-security

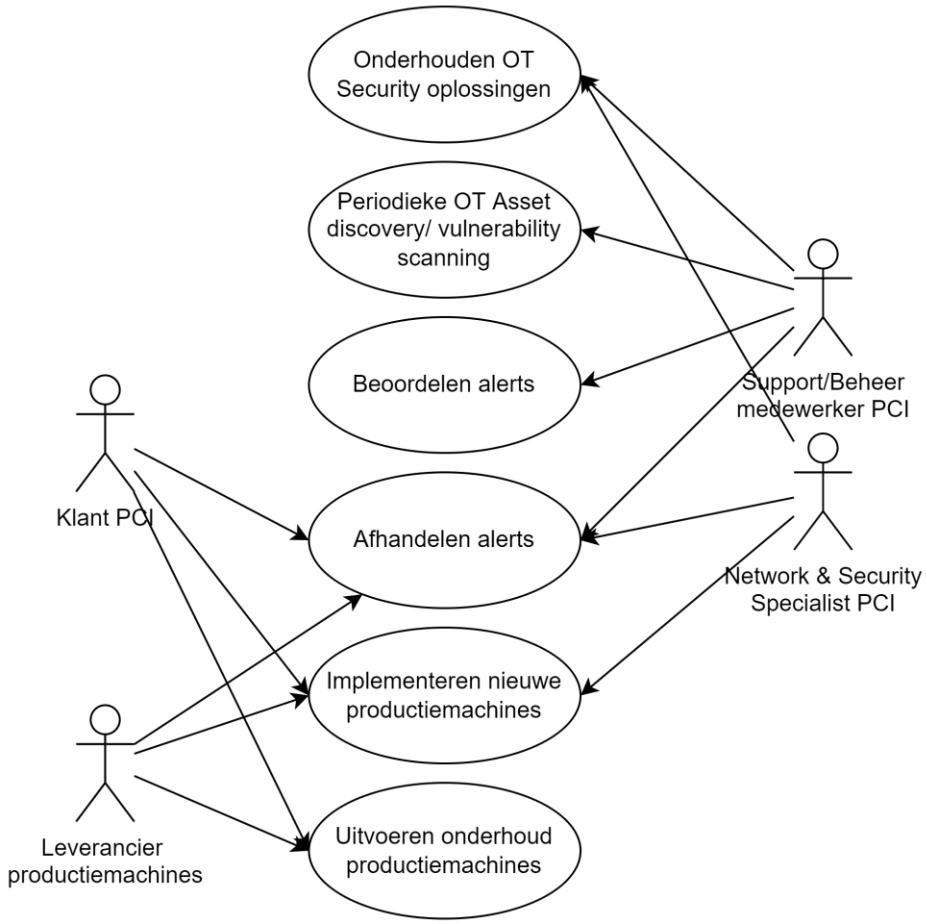
De onderstaande use-case gaat over het implementeren van OT-security bij een generieke klant van PCI. De verschillende activiteiten zijn zeer globaal beschreven omdat deze kunnen wisselen per klant. Bij het implementeren van OT-security zijn de netwerkspecialist van PCI, de SLM-medewerker van PCI en een klant van PCI betrokken. Deze voeren de verschillende activiteiten uit. De onderste activiteit “instructies geven aan gebruikers OT” richt zich op een deel bewustwording bij eindgebruikers. Hoewel PCI hierin kan adviseren is PCI niet actief betrokken bij deze laatste activiteit.



Figuur 3, Use case implementatie OT-security

Use-case diagram OT-security dienst

Dit diagram gaat over het uitvoeren van de dienst die ontstaat na het implementeren van OT-security. Deze use-case gaat er voor de startsituatie vanuit dat de eerste use-case volledig uitgevoerd is. Bij deze use-case zijn naast de netwerkspecialist en de klant ook een support & beheer medewerker van PCI en een externe leverancier van productiemachines betrokken. PCI is niet betrokken bij het uitvoeren van onderhoud aan productiemachines. Hiervoor is in de implementatiefase door PCI een standaard aan de klant aangeboden en het verschaffen van toegang ligt bij de klant van PCI. Dit omdat PCI onvoldoende kennis heeft van het machinepark van de klant en geen direct contact heeft met leveranciers van de klant.



Figuur 4, Use case OT Security dienst

6.4. Architectuur

In dit hoofdstuk is een ontwerp gemaakt van de architectuur van de actoren, processen, applicaties en infrastructuur welke ingezet gaat worden binnen de nieuw te ontwikkelen OT-security dienstverlening van PCI.

6.4.1. Methodiek

Voor het in kaart brengen van de vereiste applicaties en infrastructuur ter ondersteuning van de processen welke bij OT-security betrokken zijn is een architectuurmodel opgesteld. Voor het opstellen van de architectuur is gebruik gemaakt van de Archimate modelleer methodiek, versie 2.1. (The Open Group, 2013)

Er is begonnen met het bepalen welke rollen en actoren betrokken zijn bij de security dienst. Hiervoor is gekeken naar de eerder uitgevoerde stakeholderanalyse (bijlage B). Stakeholders met een rol binnen de processen die betrokken zijn bij de dienst zijn overgenomen in het architectuurmodel.

De processen en een deel van de applicatie- en infrastructuur-laag zijn gebaseerd op de interne contextanalyse, gecombineerd met de behoefteanalyse. Deze analyses zijn de basis voor de nieuwe dienstverlening. De oplossing is verder ontworpen op basis van gevonden en geselecteerde ontwerpprincipes.

Het architectuurmodel heeft geholpen om te komen tot nieuwe inzichten voor vereiste koppelingen tussen applicaties en infrastructuur en heeft bijgedragen aan het verder ontwikkelen van het “Jump Host” principe zoals aangeraden in ontwerpprincipe P9.

6.4.2. Resultaten

Onderstaand model bevat de 3-lagen architectuur van de te ontwerpen security dienst welke PCI zal aanbieden aan klanten die behoefte hebben aan een verbeterde beveiliging van operationele technologie.

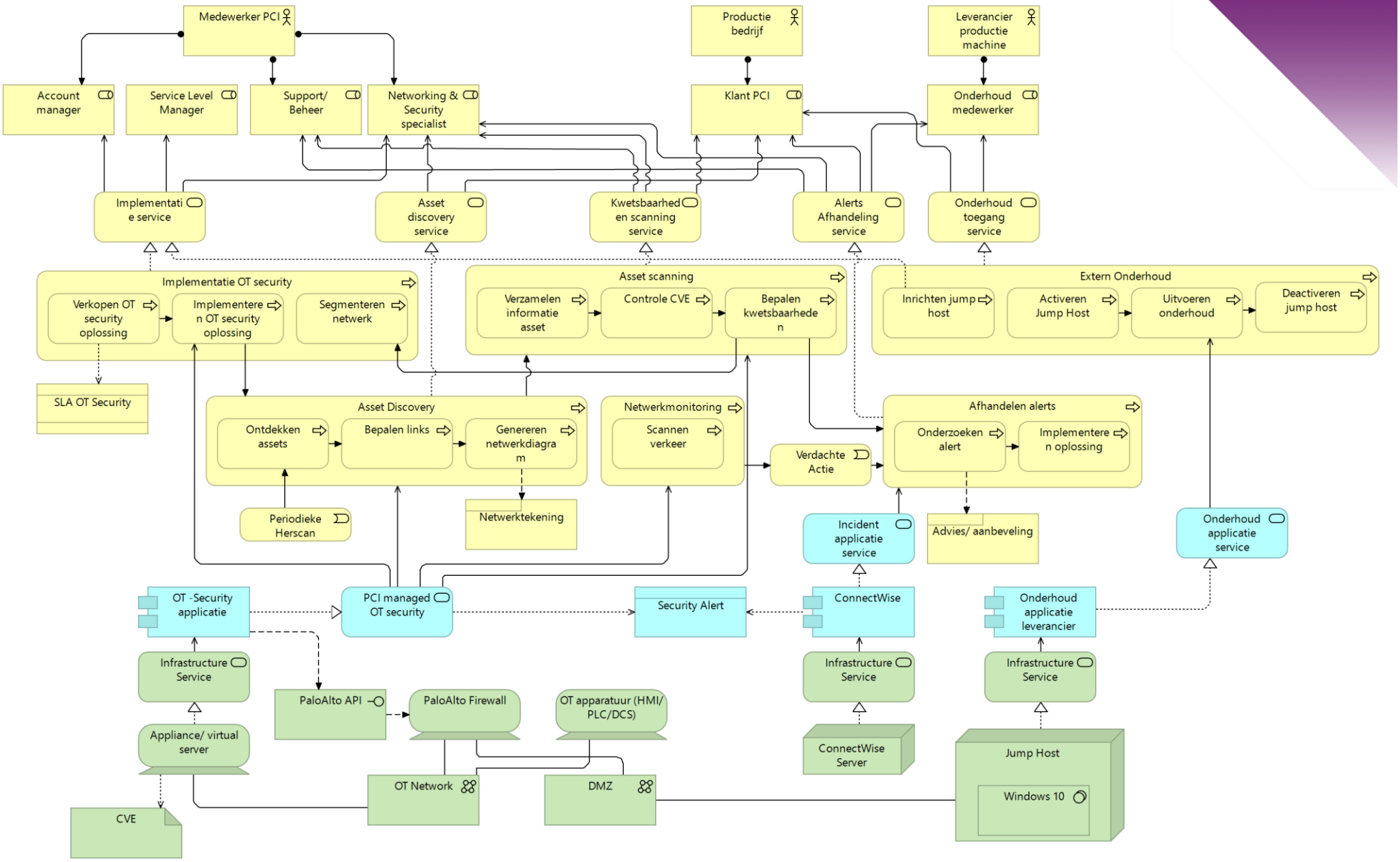
Bij het proces zijn drie actoren betrokken. Dit zijn de medewerkers van PCI, de medewerkers van de klant van PCI, het productiebedrijf, en de leverancier van de productiemachines die betrokken is vanwege de uit te voeren onderhoudswerkzaamheden.

De medewerker van PCI is bij de dienst betrokken in de rollen van: Accountmanager, Service Level manager, Support/Beheer medewerker en de Netwerk & Security specialist. Het productiebedrijf heeft binnen de dienst de rol klant van de dienst van PCI. De leverancier van machines is als onderhoud medewerker betrokken bij enkele van de processen.

In de processen-laag zijn in totaal zes processen ingetekend. Er wordt altijd gestart met de implementatie van OT-security. Het verkopen van de oplossing resulteert in een SLA en start de implementatie. Hierna wordt er gestart met het in kaart brengen van het OT-netwerk, waarna het netwerk gesegmenteerd kan worden op basis van de bevindingen. Indien er een kwetsbaarheid wordt gevonden in het OT-netwerk of wanneer de oplossing een alert genereert vanwege een verdachte actie wordt hiervan de servicedesk engineer van PCI op de hoogte gesteld. Deze medewerker informeert vervolgens de klant van een kwetsbaarheid of onderneemt actie om een aanval te blokkeren. Indien er onderhoud moet plaatsvinden op het OT-netwerk gebeurt dit door een externe leverancier, PCI is niet bij dit proces betrokken.

In de applicatie-laag zijn drie applicaties aanwezig. Een nader te selecteren OT-security oplossing van PCI, de servicedesk applicatie Connectwise van PCI en een eventuele onderhoudsapplicatie van een externe leverancier. De OT Security applicatie kan een security alert genereren welke naar Connectwise wordt doorgestuurd.

De infrastructuur-laag bevat de OT-systemen, een appliance voor de OT Security oplossing, de Jump Host en vereiste PCI infrastructuur. Het belangrijkste in deze laag is de koppeling tussen de OT-security server en de Palo Alto Firewall die door PCI aan de klant wordt geleverd. Hierdoor is het mogelijk om netwerkaanpassingen door te voeren. De OT-apparatuur wordt op een eigen OT-netwerk geplaatst en is voor leveranciers vanaf het DMZ toegankelijk, niet direct vanaf het internet.



Figuur 5, Architectuur OT-security

6.5. Productselectie

Uit het vooronderzoek is gebleken dat PCI op zoek is naar een oplossing die in OT-omgevingen kan worden ingezet voor het verbeteren van de beveiliging van OT-netwerken. Naast een netwerkontwerp wordt een security product gezocht welke kan ondersteunen in het beveiligen van deze omgevingen. Dit moet een nieuw product worden omdat PCI momenteel nog geen bestaande IT-oplossingen aanbiedt die specifiek OT-protocollen en apparaten controleren. Dit wordt echter wel aangeraden vanuit ontwerpprincipe P6 en P15 en is terug te vinden in hoofdstuk 6.2, de vereiste functionaliteit. In dit hoofdstuk wordt een goed onderbouwde keuze gemaakt voor een product dat kan worden ingezet bij klanten van PCI. Er is gekeken naar een oplossing die zoveel mogelijk van de problemen oplost binnen één product. Mocht één van de vereiste onderdelen aan de dienst niet uitgevoerd kunnen worden binnen het product wordt hiervoor een andere oplossing of ontwerp gezocht.

6.5.1. Methodiek

In deze fase is gebruik gemaakt van de onderzoeksmethodiek Available product analysis vanuit het DOT-model. (HBO-i, 2021) Deze methode houdt in dat er wordt gekeken naar in de markt beschikbare oplossingen voor de probleemstelling van het onderzoek.

Om tot een goed onderbouwde keuze te komen voor een OT-security oplossing die past binnen de randvoorwaarden, voldoet aan de requirements van PCI en haar klanten en wordt onderschreven door de literatuurprincipes is er een multicriteria analyse uitgevoerd. Als eerste is er online gezocht naar mogelijke oplossingen voor OT-security. Hiervoor is gebruik gemaakt van gegevens van Gartner. (Gartner, 2022) Deze bron is voor de long-list gekozen omdat Gartner een onafhankelijk IT-onderzoeksbureau is. Deze oplossingen zijn aangevuld met enkele oplossingen aangeraden door leveranciers of medewerkers van PCI.

Het zoeken naar een geschikt product voor OT-security gebeurt volgens een multicriteria analyse. (Janse, 2018) De mogelijke producten die voor OT-security kunnen worden ingezet worden getoetst aan een set criteria. Om tot een goed onderbouwde keuze te komen zijn deze criteria gebaseerd op de requirements, randvoorwaarden en ontwerpprincipes. Een overzicht van deze criteria en hoe deze is onderbouwd is te vinden in bijlage E.

Om tot een productkeuze te komen is aan de criteria in de multicriteria analyse een score gekoppeld. Per criteria kan aan één of meerdere requirements, randvoorwaarden en ontwerpprincipes worden voldaan. Er is voor dit systeem gekozen in plaats van het scoren per requirement omdat veel requirements, randvoorwaarden en ontwerpprincipes elkaar aanvullen of ondersteunen. Alle onderdelen individueel scoren zorgt voor een onoverzichtelijke werkwijze. Per criteria is een variabele score gekoppeld, afhankelijk van het type en aantal requirements, randvoorwaarden of ontwerpprincipes dat onder dit criterium valt. Wanneer aan een must requirement of randvoorwaarde is voldaan worden hiervoor drie punten toegekend, als aan een overig requirement of ontwerpprincipe is voldaan wordt hiervoor één punt gerekend. In de laatste kolom is weergegeven hoeveel punten aan een bepaalde criteria is toegewezen.

6.5.2. Longlist oplossingen

Op basis van de behoefteanalyse, het literatuuronderzoek en het architectuurmodel is PCI op zoek naar een netwerk gebaseerde IDS oplossing (Intrusion detection systems (Juniper, 2022)) gericht op industriële systemen en computers die het netwerk in kaart brengen en verdachte acties monitoren. De volgende producten zijn doormiddel van online onderzoek naar specifieke IDS oplossingen voor operationele technologie gevonden. Deze producten zijn mogelijk geschikt en bieden online een OT-security oplossing aan.

- Palo Alto Networks, IOT Security
- Nozomi, Guardian
- Darktrace, Industrial Immune System
- Kaspersky, Industrial Security
- Tenable, Tenable.OT
- Waterfall Security, Unidirectional Security Gateway
- ScadaFence

6.5.3. Resultaten

Onderstaande tabel dient als vergelijking van enkele OT-security oplossingen. In de bovenste regel zijn de verschillende oplossingen weergegeven. In de eerste kolom is aangegeven op welke criteria is gescoord. Een + betekent dat een functie aanwezig is, een – betekent dat de functie ontbreekt.

Tabel 8, Multicriteria analyse

	Palo Alto IOT Security	Nozomi Guardian	Darktrace Industrial Immune system	Kaspersky Industrial security	Tenable.OT	Waterfall Security	Scadafence	Toegewezen punten
Must requirements & randvoorwaarden								
Gevestigde leverancier	+	+	+	+	+	+	-	3
Biedt OT asset discovery	+	+	+	+	+	-	+	6
Genereert netwerkdiagrammen	+	+	+	+	+	-	+	6
Monitort OT-protocollen	+	+	+	+	+	+	+	12
Bevat vulnerability scanner	+	+	+	+	+	-	+	6
Biedt ondersteuning voor een MSP-model	+	+	+	+	+	+	+	3
Vervangt niet de bestaande firewall	+	+	+	+	+	-	+	3
Werkt met meerdere VLANs	+	+	+	+	+	+	+	9
Beschikt over centrale management interface	+	+	+	+	+	-	+	3
Ondersteund remote access via jump host	-	-	-	-	-	-	-	6
Should & Could requirements								
Schaalbaar licentiemodel	+	+	+	+	+	+	+	2
Maakt gebruik van CVE-database	+	+	+	+	+	-	+	1
Beveiligd legacy hard/software	+	+	+	+	+	+	+	2
Bevat rolebased access control	+	+	+	+	+	-	-	1
Te koppelen met Palo Alto Firewall voor automatisch blokkeren van aanvallen	+	+	-	-	-	-	+	1
Is in staat om OT-protocollen te isoleren van het internet.	+	+	-	-	-	+	-	2
Te koppelen met Connectwise voor het automatisch aanmaken van meldingen	+	+	+	+	+	-	+	1
Te koppelen met Logic dashboard voor netwerkmonitoring	+	+	+	+	+	+	-	1
Kan meerdere (fysiek gescheiden) locaties monitoren vanuit een omgeving	+	+	-	+	-	-	+	1
Bron	(Palo Alto, 2022)	(Nozomi, 2022)	(Darktrace, 2022)	(Kaspersky, 2022)	(Tenable, 2022)	(Waterfall, 2022)	(ScadaFence, 2022)	
Totaal	63	63	59	60	59	34	56	69

6.5.4. Conclusie

Uit de productselectie is gebleken dat de Palo Alto IoT Security, Nozomi Guardian en Kaspersky Industrial Security als beste scoren op basis van de gestelde criteria. In overleg met de netwerkspecialisten van PCI is besloten om de oplossing van Kaspersky niet mee te nemen in de verdere productkeuze. Dit omdat Europese overheden afraden om gebruik te maken van Kaspersky producten vanwege de verbondenheid met de Rusland. (Hofmans, 2022) (Franx, 2022) De oplossingen van Tenable en Darktrace vallen af omdat deze te veel should en could requirements missen. Voornamelijk het niet kunnen verbinden met de bestaande firewall is een belangrijk minpunt van deze oplossingen. De oplossing van Waterfall security is een ander soort product als waar PCI naar op zoek is, dit blijkt uit de context- en requirementsanalyse. Tot slot mist de oplossing van Scadafence een belangrijk must requirement, dit gaat om een relatief nieuw product van een jonge leverancier. PCI heeft als belangrijke eis aangegeven dat er enkel zaken wordt gedaan met reeds bewezen leveranciers.

De oplossingen van Palo Alto en Nozomi liggen dicht bij elkaar en hebben dezelfde score in de multicriteria analyse. De oplossing van Palo Alto heeft als grote voordeel dat een groot deel van de klanten van PCI al een Palo Alto Next Generation firewall in gebruik heeft. De IoT Security oplossing maakt gebruik van de bestaande firewall als netwerk sensor waarvandaan data gemonitord kan worden. De implementatie hiervan is hierdoor vele malen simpeler als Nozomi waar in het netwerk van de klanten een nieuwe appliance moet worden geplaatst en het netwerk geconfigureerd moet worden om vanaf deze appliance het netwerk te kunnen beheren. (Nozomi, 2022) Het gebruik van de bestaande hardware in plaats van nieuwe hardware zorgt tevens voor lagere kosten.

De oplossing van Nozomi lijkt echter op detailniveau geavanceerder, uit de multicriteria analyse blijkt dat de functionaliteit hetzelfde is maar de oplossing van Nozomi lijkt in de eerste analyse verder doorontwikkeld. Als er ongelimiteerde resources in geld en tijd beschikbaar zouden zijn is dit een zeer goede oplossing om in te zetten bij klanten waar OT-security van groot belang is. Omdat de oplossingen van Palo Alto en Nozomi in functionaliteit gelijk zijn, er al een partnerrelatie tussen PCI en Palo Alto bestaat en de vereiste hardware bij veel klanten al geplaatst is, is de keuze gevallen op de oplossing van Palo Alto, IoT security als beste keuze in de OT-omgevingen bij klanten van PCI. Deze oplossing wordt dan ook verder uitgewerkt in dit onderzoek.

Door geen van de oplossingen wordt het must requirement gerealiseerd over het beveiligen van een jump host verbinding voor externe leveranciers. Dit requirement wordt op een andere wijze uitgewerkt in het technisch ontwerp.

6.6. Technisch ontwerp

Dit hoofdstuk bevat het technisch ontwerp dat antwoord geeft op de zesde deelvraag van dit onderzoek.

6.6.1. Methodiek

Het technisch ontwerp is opgesteld op basis van de geselecteerde OT-security oplossing en ontwerpprincipes die dienen als best practices voor een universeel OT-netwerkontwerp. Dit hoofdstuk bevat geen huidige en toekomstige situatie maar schetst een universeel, globaal netwerkontwerp dat met minimale aanpassingen bij elke klant met OT is in te zetten.

Zoals aangegeven bestaat het ontwerp uit een aantal diensten geleverd doormiddel van een OT-security product en een universeel verbeterd netwerkontwerp inclusief een “jump host” oplossing.

Voor het opstellen van het ontwerp van de OT-security dienst is uitgegaan van de oplossing IoT Security van Palo Alto Networks (Palo Alto, 2022). Bij het opstellen van het ontwerp hiervan is gebruik gemaakt van de technische documentatie van het betreffende product. (Palo Alto Networks, 2022) Daarnaast is er een interview gehouden met een technisch engineer van Palo Alto. Deze engineer heeft uitleg gegeven over de opbouw van het product, de functies hiervan en de vereisten aan het technisch ontwerp. (Buijs, 2022) Dit interview is toegevoegd in bijlage A.

Bij het opstellen van de netwerkontwerpen is uitgegaan van de standaard producten en diensten welke PCI momenteel aanbiedt bij klanten met operationele technologie. Het gaat hierbij om systemen welke tijdens de contextanalyse gevonden zijn.

Verder is tijdens de ontwerpfase regelmatig overleg geweest met de Network & Security Specialist van PCI. Tijdens deze gesprekken is de dataverzamelingsmethodiek brainstorm gebruikt. Mogelijke oplossingen zijn besproken en voor- en nadelen aan bepaalde methodieken en best practices zijn bekeken.

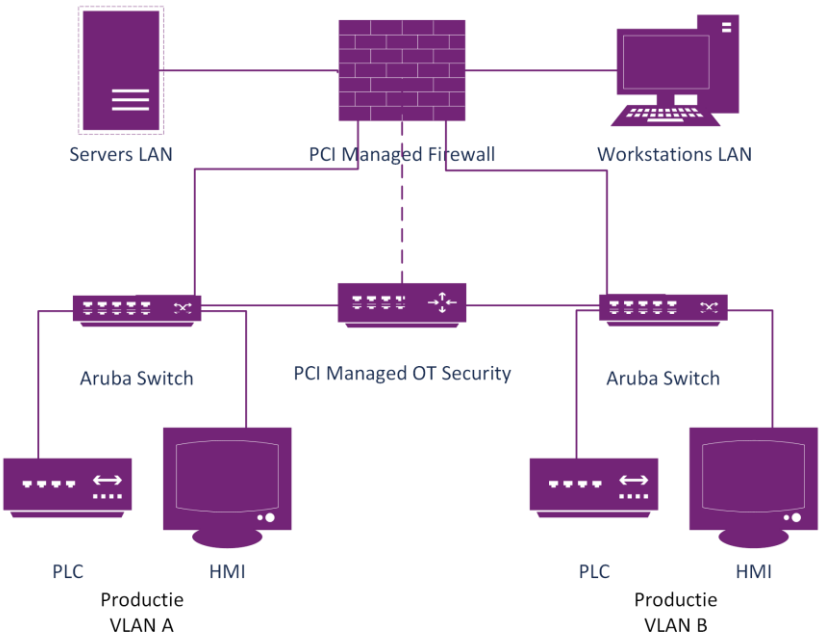
6.6.2. Technische uitwerking Palo Alto IoT Security

De oplossing die in dit hoofdstuk uitgewerkt wordt is Palo Alto IoT-security. Dit product richt zich op het uitbreiden van de bestaande Palo Alto producten om meer inzicht te krijgen in IoT en OT-omgevingen. De oplossing omvat een SaaS-dienst welke gebruik maakt van bestaande Palo Alto firewalls als data collectors (sensoren). De oplossing vereist daarom dat de klanten van PCI reeds gebruik maken van de PCI firewall, dit kan een hardware of virtuele firewall zijn. (Palo Alto Networks, 2022)

Om een zo compleet mogelijk beeld te krijgen van al het verkeer op het lokale netwerk wordt er een extra netwerkpoort geconfigureerd op de firewall welke in TAP-modus geplaatst wordt. In de netwerkconfiguratie (switching) wordt deze poort als SPAN/Mirror poort geconfigureerd. Hierdoor krijgt de OT-security oplossing inzicht in al het verkeer op het lokale netwerk.

Logisch ontwerp

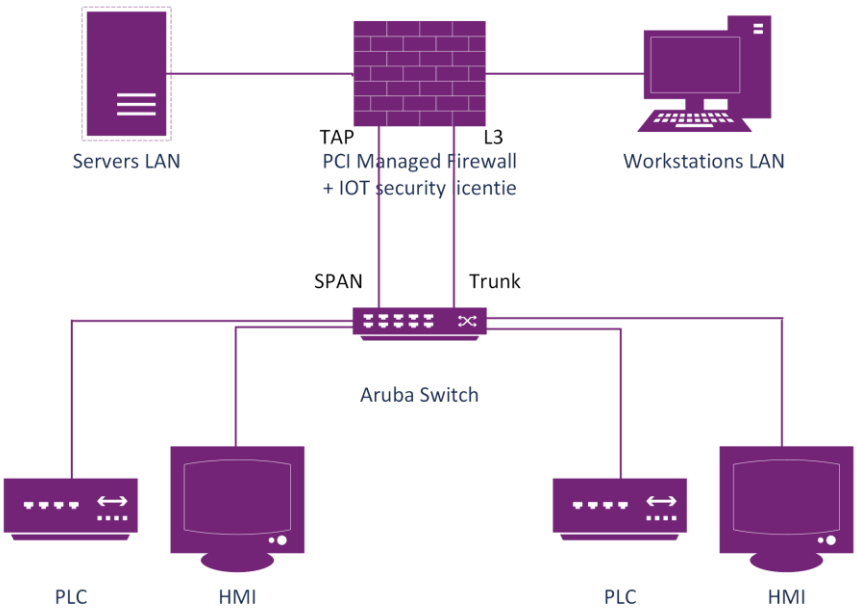
Het onderstaande figuur geeft het logische ontwerp van de OT-security oplossing weer. Hier is weergegeven dat de OT security oplossing als een sensor in het netwerk geplaatst wordt en een verbinding heeft met elk VLAN. Via deze verbinding worden de verschillende VLANs gescand en gemonitord. De OT-security oplossing heeft daarnaast een verbinding met de firewall voor het uitwisselen van policy’s en netwerkinformatie.



Figuur 6, Logisch ontwerp managed OT-security

Fysiek ontwerp

Het volgende figuur geeft het fysieke netwerkontwerp weer van de IoT-security oplossing van Palo Alto. Hier is weergegeven dat de OT-security dienst als extra optie op de bestaande firewall ingeschakeld is. Via een tweede (TAP naar SPAN) verbinding wordt een verbinding opengesteld waarover al het netwerkverkeer in het productienetwerk gemonitord wordt. Er is voor gekozen om hier een tweede lijn in gebruik te nemen omdat dit voorkomt dat de bestaande netwerkverbinding hinder ondervindt van het mirror verkeer. (Palo Alto Networks, 2022) Dit kan netwerkverkeer afkomstig uit meerdere VLANs zijn. De meeste productienetwerken bestaan uit een verzameling van access en core switches. De Aruba Switches met een uitgebreide firmware versie ondersteunen een remote mirror/SPAN poort. (Hewlett Packard Enterprise, 2019) Dit betekent dat verkeer vanuit een volledig VLAN, verspreid over meerdere switches vanaf één core switch gemonitord kan worden. Het gebruik van een mirror/SPAN poort zorgt voor de meest accurate en complete netwerkanalyses, het product van Palo Alto kan echter ook functioneren zonder SPAN interface, in dit geval wordt enkel het netwerkverkeer dat via de firewall loopt gecontroleerd.



Figuur 7, Fysiek netwerkontwerp managed OT-security

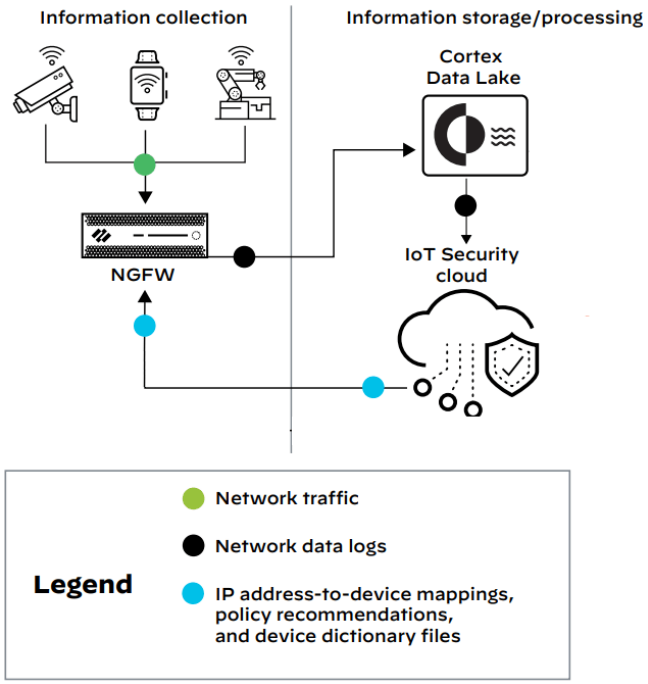
Onderdelen Palo Alto IoT Security

Palo Alto IoT security bestaat uit een cloud dienst, data lake en een sensor in het productienetwerk volgens de configuratie zoals is weergegeven in figuur 8. IoT-security is een SaaS-dienst welke wordt aangeboden vanuit de Cloud van Palo Alto Networks. Hiervoor is het vereist dat een sensor verbinding kan maken met het internet voor het doorsturen van logs. De logs worden eerst verzonden naar een Cortex Data Lake. Een basis licentie hiervoor zit inbegrepen in IoT-security. Vanuit dit data lake vindt analyse plaats op de logs en worden security maatregelen verzonden naar de firewall. Palo Alto maakt gebruik van een eigen logging format dat op de firewall geconfigureerd kan worden. Beveiligingsaanbevelingen vanuit IoT-security kunnen geautomatiseerd worden omgezet in firewall regels. De volgende configuratie zal moeten worden aangemaakt op de firewall:

- Interface in TAP modus
- Security zone: TAP Zone
- Object: Log forwarding IoT Security op basis van enhanced application logging
- Policy op tap zone: Allow all traffic
- Configureer policy tap zone voor log forwarding: IoT Security

Daarnaast stuurt de IoT Security dienst een device-to-ip map naar de Firewall. Deze combinatie maakt het mogelijk om firewall regels op basis van apparaat type te definiëren. Zowel de SaaS-dienst als het datalake zijn altijd binnen Nederland geplaatst. (Buijs, 2022) Voor het kunnen blokkeren van verdacht netwerkverkeer wordt er een deny any-any regel op de firewall aangemaakt, gekoppeld aan het device-id restricted IoT-devices. Op het moment dat er een alert voorkomt in IoT security en de netwerkspecialist het verkeer wil blokkeren kan dit direct vanuit de alert en wordt dit afgehandeld via de aangegeven regel.

De oplossing kan automatisch alerts naar een mailbox versturen. Door hier gebruik te maken van de mailbox van Connectwise kunnen automatisch meldingen aangemaakt worden. Daarnaast kan voor prioriteit hoog meldingen SMS notificatie worden ingeschakeld.



Figuur 8, Opbouw Palo Alto IoT Security (Palo Alto, 2022)

De firewall zal zich automatisch aanmelden bij het IoT Security dashboard nadat de licentie is toegevoegd. Indien de klant over meerdere fysiek gescheiden locaties beschikt dienen de firewalls opgedeeld te worden in sites. Per fysieke locatie moet één site aangemaakt worden.

6.6.3. Netwerkontwerp

PCI richt voor klanten netwerken in, hiervoor wordt gebruik gemaakt van de PCI managed Firewall en HPe Aruba switching apparatuur. Uit de context analyse blijkt dat voor de managed firewall de Barracuda of Palo Alto firewall wordt gebruikt, bij de meeste OT- en nieuwe klanten wordt de Palo Alto firewall gebruikt, hier wordt in het ontwerp dan ook mee gewerkt.

Momenteel heeft PCI geen standaard voor de inrichting van OT-netwerken, tijdens een observatie bij een klant is gebleken dat alle productiesystemen in één VLAN geplaatst zijn. Dit is vanuit security oogpunt niet wenselijk. Uit de ontwerpprincipes blijkt dat het segmenteren van OT-netwerken zeer belangrijk is. Dit kan de kans op verspreiding van malware, ransomware of bedrijfsspionage voorkomen. Operationele technologie maakt voor onderlinge communicatie gebruik van specifieke industriële protocollen. (Knapp & Langill, 2015)

Met de netwerkspecialisten van PCI zijn twee verschillende vormen van netwerksegmentatie besproken. Uit de observatie van een productienetwerk is gebleken dat het netwerk op twee verschillende manieren gesegmenteerd zou kunnen worden. Een productienetwerk bestaat in veel gevallen uit meerdere productielijnen, dit zijn enkele machines van één of meerdere leveranciers die gezamenlijke input en output hebben. Het is mogelijk om het netwerk te segmenteren op basis van productielijn of op basis van leverancier van de productiemachines.

In onderstaande tabel is weergegeven wat de voor- en nadelen zijn van de verschillende vormen van netwerksegmentatie.

Tabel 9, Voor- en nadelen netwerksegmentatie

Segmentatie per lijn	Segmentatie per leverancier
Voordelen: • Malware kan lokaal slechts één lijn besmetten. • (Legacy) Layer 2 protocollen kunnen binnen de lijn communiceren. • Toegang tot IT-resources kan per lijn bepaald worden. (Least access) • (Nieuwe) lijnen met moderne apparatuur zijn beter afgeschermd van (oude) lijnen met legacy apparatuur. • Toegang voor interne medewerkers kan tot een (aantal) lijnen beperkt worden.	Voordelen: • Leveranciers hebben voor onderhoudswerkzaamheden alleen toegang tot eigen machines.
Nadelen: • Minder zicht op communicatie binnen een lijn. • Leveranciers met machines in meerdere lijnen krijgen tot een groot deel van het netwerk toegang.	Nadelen: • Layer 2 protocollen worden gehinderd door een router/firewall. • Wanneer een type machine in elke lijn voorkomt en er ontstaat een security incident, heeft dit invloed op alle lijnen.

Op basis van deze analyse is besloten om netwerksegmentatie op basis van productielijn toe te passen. Deze manier van segmenteren kent meer voordelen en deze voordelen worden beter onderschreven vanuit het literatuuronderzoek, dit blijkt ook uit ontwerpprincipes P08, P11 en P14. Daarnaast is het waarschijnlijk voor een deel van de productiebedrijven onbekend bij welke leverancier welke hardware hoort en hoeveel leveranciers er precies aanwezig zijn in het netwerk. Tot slot wordt er in de OT in bepaalde gevallen gewerkt met specifieke protocollen. Deze protocollen communiceren met andere machines binnen dezelfde lijn en zijn soms niet geschikt om te routeren en zouden volgens ontwerpprincipe P16 het lokale netwerksegment niet mogen verlaten.

Wanneer PCI een nieuw IT-netwerk inricht voor een productiebedrijf, of een bestaand netwerk beter wil beveiligen moet dit op basis van netwerksegmentatie per productielijn gebeuren. PLCs, HMIs en SCADA-oplossingen kunnen binnen het netwerk vrij communiceren maar kunnen geen verbindingen maken met machines en IT-bronnen buiten de eigen productielijn als hier geen expliciete toestemming

voor is gegeven. Wanneer er geen duidelijke lijnen aanwezig zijn kan ervoor worden gekozen om per machinegroep waarbinnen communicatie nodig is te segmenteren.

Uit de contextanalyse is gebleken dat PCI als richtlijn heeft om routering tussen netwerken plaats te laten vinden op de firewall. De verschillende netwerksegmenten dienen als security zone op de firewall aangemaakt te worden. Deze segmenten kunnen als VLAN op de netwerkapparatuur worden aangemaakt. Hierdoor ontstaat er een virtuele scheiding tussen de netwerken. Deze vorm van netwerksegmentatie wordt ondersteund op de binnen PCI gebruikte netwerkapparatuur van Aruba Networks. (HPe, 2022) De bestaande IP-subnetten maken gebruik van private IP-adressen. Deze subnetten kunnen worden verkleind om zo meer netwerken mogelijk te maken. Het uitwerken van een IP-plan is geen onderdeel van deze scriptie omdat dit een universeel netwerkontwerp betreft.

6.6.4. Jump Host inrichting

Uit het literatuuronderzoek is gebleken dat het verstandig is om externe leveranciers die toegang tot het OT-netwerk nodig hebben dit te verschaffen via een vorm van een jump host. Dit betekent dat de leverancier eerst verbinding maakt met een desktop of server in een geïsoleerd netwerk. Deze desktop of server is specifiek aangemaakt voor het uitvoeren van beheerwerkzaamheden. (Microsoft, 2021) Onderstaand figuur geeft aan hoe een jump host principe werkt. Omdat de jump host in het beheer en interne netwerk van de klant van PCI valt is er meer controle over wat er wel en niet kan gebeuren op het productienetwerk. Zo worden er geen ongecontroleerde systemen direct met OT verbonden.

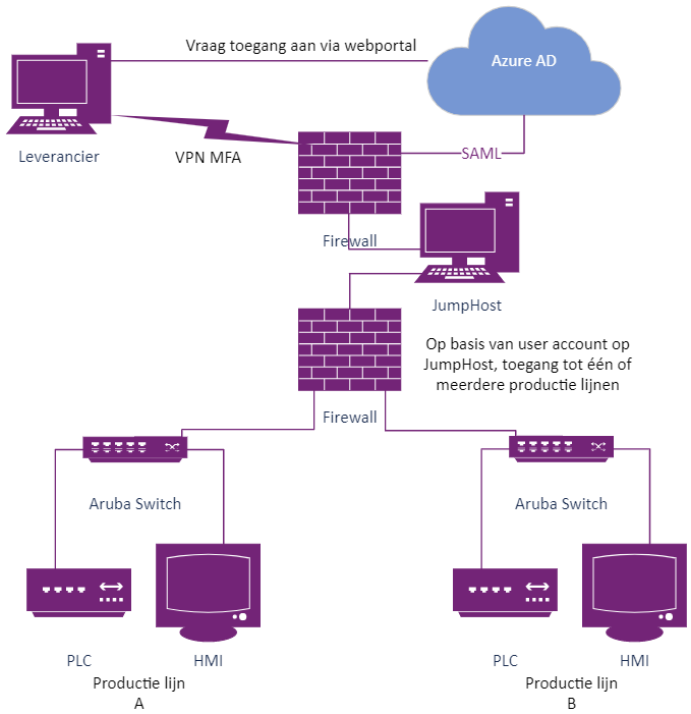
Figuur 9, Werking jump host

De jump host is een standaard werkstation die enkel op netwerkniveau op een bijzondere locatie geplaatst is. De jump host kan als virtuele machine aangemaakt worden. Als besturingssysteem is gekozen voor Windows 10, dit omdat uit de contextanalyse is gebleken dat PCI gebruik maakt van Microsoft producten op werkplekken. Het is van belang dat de jump host voldoende beveiligd is doormiddel van antivirus en een host firewall die geen verbindingen anders dan vanaf de leverancier VPN toestaat.

Verder is uit het literatuuronderzoek naar voren gekomen dat het van belang is om de externe verbinding tussen de leverancier en de jump host te beveiligen doormiddel van een versleutelde VPN-verbinding. De verbinding tussen de jump host en het OT-netwerk wordt ingericht volgens het least access principe. Klanten van PCI maken gebruik van de Next Generation Firewall van Palo Alto Networks. Deze firewall beschikt over een VPN-gateway waarmee een externe verbinding kan worden opgezet en beschikt over de mogelijkheid om op basis van een user account toegang tot een subnet te geven. Voor toegang tot de VPN-verbinding wordt standaard gebruik gemaakt van Azure Active Directory accounts via een SAML verbinding. Deze dienst beschikt over de mogelijkheid om een access review in te richten via de service Azure Identity Governance (Microsoft, 2022). PCI richt hierbij voor de klant een VPN-gateway in, toegang tot deze gateway is enkel mogelijk indien het user account lid is van een specifieke Azure AD groep. Een externe gebruiker kan via een website toegang tot deze groep aanvragen. Standaard wordt deze toegang 8 uur toegewezen. Voor deze periode is gekozen omdat uit gesprekken met de machinepark beheerder van een van de klanten is gebleken dat het meeste onderhoud één werkdag duurt. Als onderhoud langer duurt moet dit worden aangevraagd en kan een langere termijn worden toegewezen. De technische dienst van de klant van PCI ontvangt een email met de vraag of de leverancier toegang mag krijgen. Indien dit volgens de technische dienst klopt kan toegang worden gegeven voor maximaal 8 uur. Indien langer nodig is kan dit direct in Azure worden ingericht. Er kan vervolgens via 2-factor authenticatie op de VPN-verbinding ingelogd worden. Deze VPN-verbinding biedt enkel toegang tot het DMZ netwerk en maakt gebruik van de Palo Alto Global Protect VPN applicatie. (Microsoft, 2021) (PaloAlto Networks, 2022)

De leverancier beschikt over een gebruikersnaam en wachtwoord voor de jump host welke in het DMZ geplaatst is. Nadat op deze jump host ingelogd is kan op basis van username toegang worden

gekregen tot één of meerdere segmenten van het OT-netwerk. (Palo Alto Networks, 2022) Deze user accounts worden vanuit de Active Directory van de klant beheerd zodat er voldoende controle is over eisen aan gebruikersaccounts en wachtwoorden. Verder is het niet mogelijk om vanaf de jump host verbinding met het internet te maken. In onderstaande logische netwerktekening is de werking van de jump host schematisch weergegeven.



Figuur 10, Logisch ontwerp jump host

6.6.5. Firewall configuratie

Voor het inrichten van de in dit hoofdstuk beschreven oplossingen worden er aanpassingen gedaan op de door PCI beheerde firewall oplossingen. Dit ontwerp is gebaseerd op de Next Generation Firewall van Palo Alto Networks.

Zoals aangegeven wordt het netwerk gesegmenteerd op basis van productielijn, er ontstaat één productienetwerk bestaande uit meerdere security zones. Deze zones zijn op netwerklaag 2 uit het OSI-model gescheiden doormiddel van VLANs. Voor de inrichting van de security zones wordt gebruik gemaakt van het least access principe. Standaard wordt er daarom een regel aangemaakt die al het netwerkverkeer van en naar de security zones verbiedt (Deny any-any). Vervolgens kunnen er regels toegevoegd worden die verbindingen met specifieke servers toestaan. Hierbij moet packet inspectie op protocol niveau worden ingeschakeld. Alleen goedgekeurde protocollen mogen verbinding maken met servers vanaf het productienetwerk. De Palo Alto IoT-security oplossing kan gebruikt worden voor het opstellen van de vereiste firewall regels.

Uit de behoefteanalyse is gebleken dat in bepaalde gevallen medewerkers vanaf het clientnetwerk machines moeten kunnen aanpassen. Omdat dit bij de onderzochte bedrijven om slechts een select aantal medewerkers gaat wordt hiervoor toegang per gebruiker (user ID) en protocol ingericht. Een vooraf geselecteerde groep gebruikers mag via een vooraf bepaald protocol verbinding met het machinenetwerk maken. Indien gewenst kan dit per productielijn worden ingesteld. Hiervoor wordt gebruik gemaakt van Active Directory groepen.

In het productienetwerk is geen toegang tot het internet mogelijk. Hiervoor dient altijd gebruik te worden gemaakt van het clientnetwerk. Hier is voor gekozen omdat het productienetwerk in veel gevallen te veel legacy software bevat. Om deze software veilig in te kunnen zetten moet een verbinding met het internet geblokkeerd worden. Hiermee worden ontwerpprincipes P07 en P08 gerealiseerd.

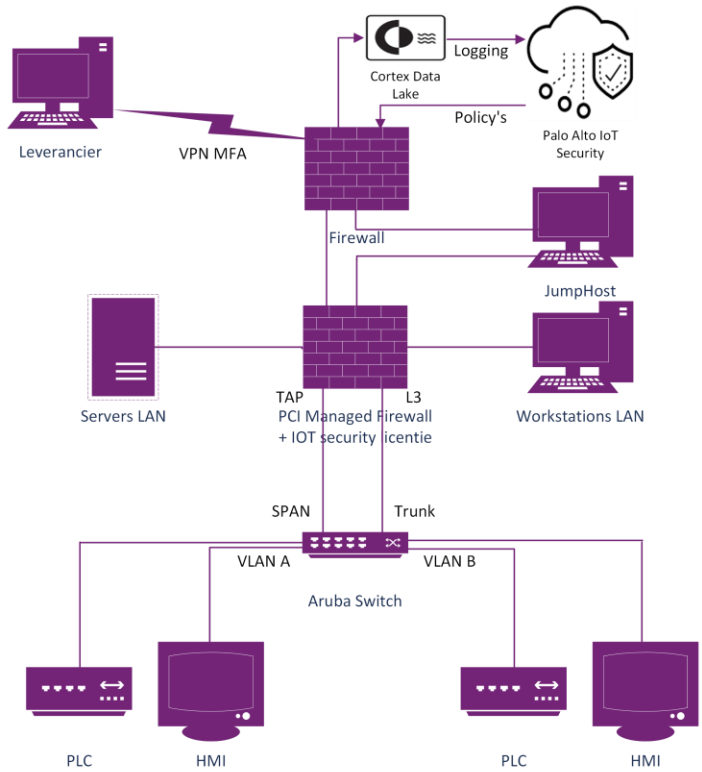
Voor de realisatie van de jump host wordt een DMZ aangemaakt op de firewall. Vanaf het DMZ moet op basis van gebruikersaccount (User ID) op de jump host verbindingen worden toegestaan naar specifieke productielijnen. Om extern een verbinding te maken met de jump host wordt gebruik gemaakt van een VPN-verbinding. De configuratie hiervan is te vinden in het hoofdstuk dat de jump host beschrijft.

6.6.6. Conclusie

In dit hoofdstuk zijn verschillende ontwerpen opgesteld die gezamenlijk de beveiliging van OT verbeteren. Uit het ontwerp is gebleken dat voor het verbeteren van OT-security bij klanten van PCI er meerdere producten en methodieken ingezet moeten worden.

Om de beveiliging optimaal te verbeteren wordt het aangeraden om eerst het netwerk te verbeteren doormiddel van de eenmalige netwerksegmentatie, een jump host voor veilige verbindingen tussen leveranciers en het OT-netwerk en Palo Alto IoT security voor asset discovery, vulnerability (kwetsbaarheden) scanner en monitoring.

Het totale OT-netwerk ziet er na het uitvoeren van de diensten door PCI uit zoals is weergegeven in figuur 11. Dit is een logisch ontwerp, in praktijk wordt er slechts één firewall geplaatst.



Figuur 11, Totaalontwerp OT security

6.7. Aanbevelingen

Uit het vooronderzoek is gebleken dat PCI bij haar klanten in toenemende mate gebruik maakt van Aruba Clearpass. Dit is een Network Access Control systeem waarmee automatisch apparaten toegang kan worden gegeven tot een netwerk. Zo kan op basis van het type apparaat een VLAN worden toegewezen en kan toegang tot resources worden gegeven. (HP Enterprise, 2022) Het koppelen met Aruba Clearpass is als “Won’t have” requirement gesteld, dit betekent dat het niet binnen de scope van dit project valt maar wel een eis voor in de toekomst is. De oplossing Palo Alto IoT Security kan gekoppeld worden met Aruba Clearpass. In het geval van een security alert kan dit naar Clearpass worden doorgestuurd en kan het betreffende apparaat automatisch in quarantaine worden geplaatst. Het apparaat heeft op dat moment geen toegang tot het netwerk meer. Dit kan een goede toevoeging zijn voor prioriteit hoog incidenten. Dit voorkomt dat een aanval zich verspreid over het interne netwerk binnen één security zone. (Palo Alto Networks, 2022)

7. Ontwerpevaluatie

In dit hoofdstuk wordt onderzocht of het opgestelde ontwerp overeenkomt met de requirements en randvoorwaarden vanuit het eerste deel van het afstudeerverslag. Uit deze evaluatie moet blijken of het ontwerp een juist antwoord geeft op de deelvraag: “Welke oplossingen, methodieken en producten kunnen in een OT-security dienst worden aangeboden?”.

7.1. Methodiek

Voor het verifiëren van het technisch ontwerp wordt gebruik gemaakt van de methode prototyping vanuit het DOT-model (HBO-i, 2021). Volgens deze methodiek wordt er een prototype opgesteld waarmee vervolgens testen kunnen worden uitgevoerd. Er wordt een prototype van een versimpelde omgeving van de ontworpen oplossing gerealiseerd. Voor het testen met OT-systemen is een master en slave PLC gesimuleerd binnen Windows, gebruikmakend van het industriële protocol Modbus en een hardware OT component. Dit is een vorm van een System Test, het ontwerp wordt gedemonstreerd en gecontroleerd aan de requirements. (HBO-i, 2021)

De gebruikte testmethodiek is een afgeleide, versimpelde versie van SmarTEST. Deze methodiek gaat uit van testen aan acceptatiecriteria op basis van requirements. Volgens SmarTEST zijn acceptatiecriteria “een meetbaar gemaakte subset van de requirements waarvoor de acceptanten een beoordeling wensen alvorens zij tot acceptatie overgaan”. (Bouman, 2008) Omdat in dit onderzoek is gewerkt met vooraf opgestelde requirements is SmarTEST een logische testmethodiek in dit onderzoek. Alle requirements met uitzondering van de “won’t have” requirements moeten worden getest. De volledige SmarTEST methodiek is niet geschikt voor deze ontwerpevaluatie, dit omdat er tijdens dit onderzoek niet is gewerkt met een grote organisatie. Het opzetten en implementeren van een grote testorganisatie is niet nodig in deze ontwerpevaluatie.

Per uitgevoerde test is in een acceptatiecriterium aangegeven waaraan moet worden voldaan om de test te laten slagen. De testen zijn opgesteld op basis van de requirements en randvoorwaarden.

Aan elke test zit een belang gekoppeld, dit is gebaseerd op het aantal en de prioriteit van de requirements die aan de betreffende test gekoppeld zitten. Dit is gedaan volgens de volgende verdeling:

- Must requirement: 5 punten
- Should requirement: 3 punten
- Could requirement: 1 punt
- Randvoorwaarde: 5 punten

De onderbouwing van het belang van een test op basis van de bovenstaande verdeling is te vinden in bijlage F van dit document. Tijdens het uitvoeren van de testen zijn alle aangetroffen resultaten als onderbouwing toegevoegd in bijlage G.

7.2. Resultaten

In dit hoofdstuk wordt als eerste beschreven hoe het prototype is opgebouwd, vervolgens worden de uitgevoerde testen en testresultaten beschreven.

7.2.1. Prototype ontwerp

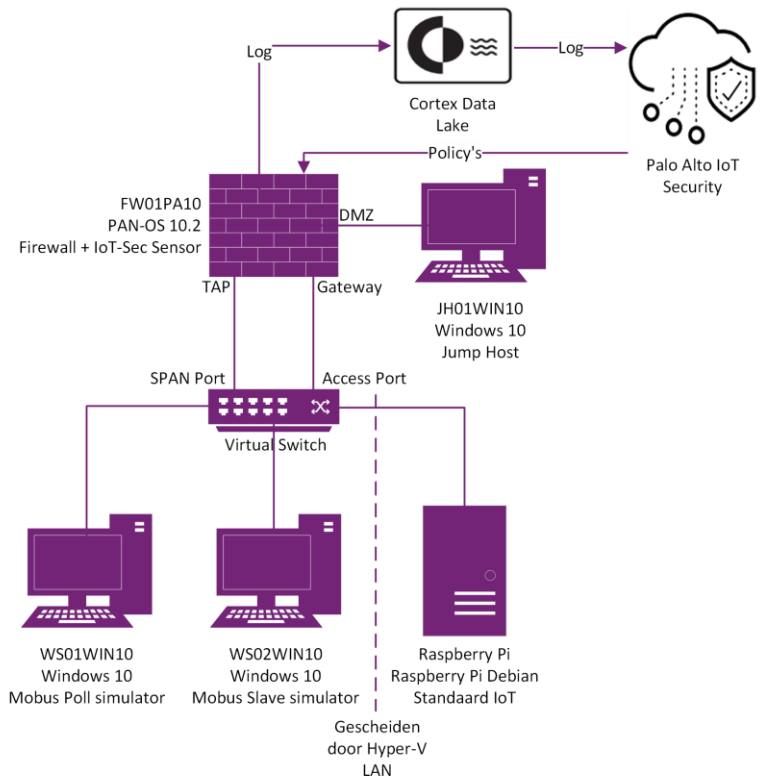
Het prototype is in een gesimuleerde omgeving ingericht. Er is een virtuele Palo Alto Next Generation firewall geïmplementeerd waarop de IoT-security licentie is toegevoegd. Het ontwerp maakt gebruik van de Hypervisor Hyper-V op een Windows 10 installatie.

De Palo Alto Firewall is geconfigureerd met zowel een gateway als TAP poort zoals ook is aangeraden in het technisch ontwerp. Het netwerk waaraan deze systemen verbonden zijn bestaat uit een Hyper-V virtual switch waarop port mirroring is ingeschakeld. Aan deze virtuele switch zitten de volgende systemen verbonden:

- Windows 10 virtual machine, met Modbus Poll simulator
- Windows 10 virtual machine, met Modbus Slave simulator
- Windows 10 virtual machine, als jump host in DMZ
- Raspberry Pi hardware (lichtgewicht computer met Linux Debian)

De Windows 10 systemen bevatten simulatiesoftware waarmee het netwerkverkeer tussen een HMI en PLC kan worden gesimuleerd, dit voor het controleren of de IoT security oplossing het industriële protocol Modbus herkent. De hardware Raspberry Pi is aangesloten om te controleren of deze wordt herkend als OT en of kwetsbaarheden en verdachte acties kunnen worden herkend. De derde Windows 10 machine is in het DMZ geplaatst en wordt gebruikt als simulatie van de jump host.

Onderstaand figuur bevat het netwerkontwerp van het prototype. Er is gebruik gemaakt van volledig functionele evaluatie licenties. De Raspberry Pi is in een ander subnet geplaatst als de Windows 10 virtuele machines.



Figuur 12, Netwerkontwerp prototype

Met behulp van dit prototype kan worden geverifieerd of het technisch ontwerp voldoet aan de door PCI gestelde eisen.

7.2.2. Testresultaten

Onderstaande tabel geeft het beknopte resultaat van de uitgevoerde testen. In bijlage G is een detail overzicht bijgevoegd van de resultaten die tijdens de testen zijn aangetroffen.

Tabel 10, Testresultaten

Volg nr.	Belang	Acceptatiecriterium	Resultaat	Opmerking
T01	36	Er wordt een compleet beeld gegeven van aanwezige OT en andere assets in het OT-netwerk.	Geslaagd	Er is op alle aangesloten apparatuur in het prototype gescand.
T02	31	Kwetsbaarheden in OT kunnen worden gescand.	Geslaagd	
T03	28	Leverancier A heeft vanaf de Jump Host wel toegang tot het interne netwerk, leverancier B heeft vanaf de Jump Host geen toegang tot het interne netwerk	Geslaagd	
T04	23	Er worden industriële protocollen herkend.	Geslaagd	Er is een verbinding tussen twee Windows 10 systemen met het industriële protocol Modbus opgezet.
T05	20	Verbindingen tussen assets worden herkend.	Geslaagd	
T06	20	De oplossing herkent verdacht netwerkverkeer op industriële systemen.	Geslaagd	Hiervoor is een regel aangemaakt welke een alert zou moeten reageren bij een ping naar een ander systeem.
T07	18	Er kan een sessie op laag 2 van het netwerk gevolgd worden.	Geslaagd	
T08	18	Kwetsbaarheden worden verwezen naar een CVE-database.	Geslaagd	
T09	18	De oplossing bevat een centraal management dashboard.	Geslaagd	
T10	15	De oplossing kan door een MSP-partner besteld worden.	Geslaagd	Dit is getest op basis van de documentatie op de website van de leverancier.
T11	13	De oplossing scant meerdere VLANs vanuit één appliance.	Geslaagd	
T12	11	Er kan een gebruiker met afwijkende rechten worden aangemaakt.	Geslaagd	
T13	11	De status van de oplossing wordt weergegeven in Logic Dashboards.	Geslaagd	Enkel de sensoren kunnen in Logic gemonitord worden, de SaaS-applicatie niet.
T14	11	Het is mogelijk om later sensoren toe te voegen.	Geslaagd	Sensoren zijn bij de onderzochte oplossing fysieke of virtuele firewalls.
T15	10	De oplossing werkt in combinatie met de Palo Alto Next Generation Firewall.	Geslaagd	

T16	8	Klanten kunnen zelfstandig de inventory bekijken zonder een aanpassing te doen.	Geslaagd	
T17	7	Er kan automatisch een melding in Connectwise worden gemaakt.	Geslaagd	Connectwise beschikt over de optie om automatisch een ticket van een email bericht te maken, de onderzochte oplossing beschikt over de functionaliteit om een mail te sturen.
T18	6	De oplossing is gekoppeld aan de firewall.	Geslaagd	In deze test is gecontroleerd of policy's vanuit IoT-Security automatisch worden overgenomen in de firewall regels.

7.3. Conclusie

Uit het testrapport is gebleken dat alle testen zijn geslaagd. Omdat de testmethodiek uit gaat van testen op basis van requirements en randvoorwaarden als acceptatiecriteria kan hieruit worden geconcludeerd dat het ontwerp aan alle gestelde requirements en randvoorwaarden voldoet.

Het testrapport is uitgevoerd om te verifiëren of het ontwerp een juist antwoord geeft op deelvraag zes van het onderzoek: “Welke oplossingen, methodieken en producten kunnen in een OT-security dienst worden aangeboden?”.

Het ontwerp geeft als antwoord op deze vraag dat de volgende oplossingen, methodieken en producten voldoen aan de eisen van PCI om binnen een OT-security dienst aangeboden te worden:

- Palo Alto IoT security ten behoeve van asset discovery, vulnerability scanning en het detecteren van verdacht netwerkverkeer.
- Netwerksegmentatie op basis van productielijn doormiddel van VLAN en firewall security zones
- Een jump host in een DMZ, met toegang tot één of meerdere lijnen op basis van user ID

In het prototype is van al deze systemen een simulatie gecreëerd en gecontroleerd of met deze drie producten aan alle requirements is voldaan. Omdat alle testen geslaagd zijn valt te concluderen dat aan alle requirements is voldaan en dat het ontwerp daarmee een juist antwoord heeft gegeven op deelvraag zes van het onderzoek.

8. Advies

Het adviesrapport richt zich op het beantwoorden van deelvraag zeven van het onderzoek: “Hoe zou OT-security als een dienst kunnen worden ingericht?”.

8.1. Methodiek

Op basis van de resultaten van het functioneel- en technisch ontwerp wordt in dit hoofdstuk bekeken hoe de ontworpen producten, methodieken en oplossingen als diensten aan klanten van PCI kunnen worden verkocht. Als eerste wordt beschreven hoe de OT-security diensten opgebouwd zouden moeten worden. Vervolgens wordt beschreven hoe de SLA is opgebouwd, dit volgens de standaarden van PCI. (PCI IT-Solutions, 2022). Tot slot is in dit hoofdstuk een advies gegeven over het inrichten van de interne processen welke binnen PCI vereist zijn voor het uitvoeren van de diensten rondom OT-security.

8.2. Dienstinrichting

Het wordt aangeraden om het ontwerp op te delen in een eenmalige dienst waarin de beveiliging verbeterd wordt doormiddel van een ontwerp en een managed dienst waarin OT voortdurend beveiligd wordt. Deze manier van het aanbieden van diensten past het beste binnen het huidige dienstenportfolio van PCI en bij de werkwijzen van PCI.

8.2.1. Verbeterd netwerkontwerp OT

In het technisch ontwerp is een standaard omschreven voor het inrichten en segmenteren van een OT-netwerk. Dit ontwerp is universeel in te zetten bij klanten van PCI en maakt gebruik van de reeds aanwezige apparatuur.

Het wordt aangeraden om klanten van PCI die gebruik willen maken van de managed OT-security dienst eerst een verbeterd netwerkontwerp aan te bieden. Omdat dit geen doorlopende dienst is kan dit éénmalig als projecting dienst aangeboden worden aan klanten. Het netwerk wordt hierbij door een PCI specialist geanalyseerd, er wordt een plan voor netwerksegmentatie opgesteld en na goedkeuring van de klant wordt de segmentatie uitgevoerd. De klant moet betalen voor het aantal uren dat de specialist van PCI met de segmentatie bezig is geweest.

Tevens wordt aangeraden om nieuwe netwerken met operationele technologie waar PCI implementaties gaat uitvoeren volgens deze standaard in te richten.

Binnen een eenmalig project kan ook een jump host worden ingericht volgens de standaarden beschreven in het technisch ontwerp.

PCI levert aan klanten een managed firewall oplossing. Als deze klanten ook de managed OT-security oplossing afnemen kan nuttige informatie over bijvoorbeeld verbindingen tussen het IT en OT-netwerk of het OT-netwerk en het internet in kaart kan worden gebracht. Daarnaast is de managed OT-security dienst een IDS systeem, om adequaat op meldingen te reageren is het van belang dat PCI de firewall kan configureren op basis van de bevindingen van de oplossing. De managed OT-security oplossing maakt gebruik van een Palo Alto Firewall als data sensor in het productienetwerk. Om een firewall als sensor voor OT-security in te kunnen richten moet PCI hier licenties aan kunnen toevoegen.

Om een managed firewall optimaal in te richten op een OT-netwerk wordt aangeraden om klanten met operationele technologie altijd de managed firewall in combinatie met de managed OT-security dienst te verkopen.

8.2.2. Managed OT Security

In het ontwerp wordt gesproken over een OT-security oplossing. De gevonden oplossing (Palo Alto IoT Security) beschikt over centrale beheer functionaliteit, staat MSP verkoop toe en voldoet aan de eisen die PCI stelt aan IT-security diensten. PCI kan hierom Palo Alto IoT-security als managed dienst verkopen voor OT asset discovery, OT vulnerability detectie en OT netwerk monitoring.

PCI beschrijft haar managed diensten in een service level agreement. Dit document bevat een omschrijving en alle kenmerken van services die PCI als managed dienst aanbiedt. In het onderdeel “service level agreement” van dit hoofdstuk wordt de SLA van de managed OT-security dienst weergegeven volgens het geldende template van PCI.

De dienst zal bestaan uit:

- Het inkopen en licenseren van het product Palo Alto IoT security
- Het in het netwerk plaatsen van het product
- Het configureren en aan Connectwise koppelen van het product
- Het koppelen van het product aan een door PCI geleverde managed firewall
- Het in kaart brengen van het OT-netwerk
- Het monitoren van alerts
- Het automatisch blokkeren van verdacht verkeer
- Het informeren van de klant bij gevonden kwetsbaarheden

Deze dienst zal kwetsbaarheden ontdekken en alerts genereren veroorzaakt door verdacht netwerkverkeer. Aangeraden wordt om het afhandelen van alerts te laten plaatsvinden op basis van nacalculatie. Dit omdat het afhandelen van kwetsbaarheden en alerts voor zeer veel werk kan zorgen, het is aan de klant om te beslissen welke oplossing ze wensen en wat de maximale kosten hiervoor zijn. In de regel bestaat OT voor een belangrijk deel uit legacy hard- en software. Een nadeel aan legacy software is dat deze in veel gevallen bekende kwetsbaarheden bevat welke niet meer opgelost kunnen worden doormiddel van een update. PCI moet nooit de verantwoordelijkheid dragen voor legacy hard- en software, het is de keuze van de klant om deze te gebruiken. PCI kan volgens het best-effort model de klant adviseren en de beveiliging van legacy zo goed mogelijk verbeteren.

Voor het oplossen van een deel van de kwetsbaarheden moet contact plaatsvinden tussen PCI en de leverancier van de operationele technologie. PCI kan hierin ondersteunen op verzoek van de klant, werkzaamheden moeten volledig plaatsvinden op basis van nacalculatie.

8.3. Service level agreement

De managed OT-security dienst kan als managed service door PCI aan klanten worden aangeboden. Afspraken rondom een managed dienst worden bij PCI vastgelegd in een service level agreement. In dit hoofdstuk is een service level agreement opgesteld voor de dienst Managed OT Security. Deze dienst is opgesteld op basis van het template SLA van PCI. (PCI IT-Solutions, 2022)

PCI Managed OT Security

Managed OT Security bestaat uit een netwerkmonitoringstool specifiek gericht op operationele technologie in industriële omgevingen. Deze dienst voert een 24/7 scan uit van het netwerkverkeer en kwetsbaarheden op een OT-omgeving. Optioneel kan deze dienst gekoppeld worden aan de firewall van PCI voor het blokkeren van verdachte verbindingen.

PCI is verantwoordelijk voor:

- Inventariseren van het OT-netwerk
- Installatie en onderhoud van de OT-security appliance
- Leveren van support: reageren op alerts en informeren klanten
- Het direct isoleren van een verdacht systeem
- Leveren van rapportages van bedreigingen

Tabel 11, Service level agreement (PCI IT-Solutions, 2022)

Kenmerken services	
Incident support	Maandag tot en met vrijdag van 08:00 tot 17:00 Maandag tot en met zondag 24 uur per dag bij prio hoog meldingen. (met 24 uursservice)
Maximale responstijd per prio	Prio hoog: 1 uur (alleen verdacht netwerkverkeer) Prio middel: 3 uur Prio laag: 8 uur
Monitoring	24*7
Onderhoud:	Door PCI
Asset overzicht:	Tijdens implementatie & op verzoek via servicerequest (nacalculatie)
Rapportages:	Door PCI, op verzoek of na automatische melding.
Bescherming tegen:	Bekende (CVE) kwetsbaarheden in PLCs en DCSs Bekende (CVE) kwetsbaarheden in Windows en Linux HMI Verdachte verbindingen met OT Ongeautoriseerde toegang tot OT netwerken
Ondersteunende systemen:	Industriële apparatuur met TCP/IP verbinding.
Niet inbegrepen in ondersteuning:	Onsite support Ondersteuning bij kwetsbaarheden in OT PCI is niet verantwoordelijk voor het dichten van kwetsbaarheden.

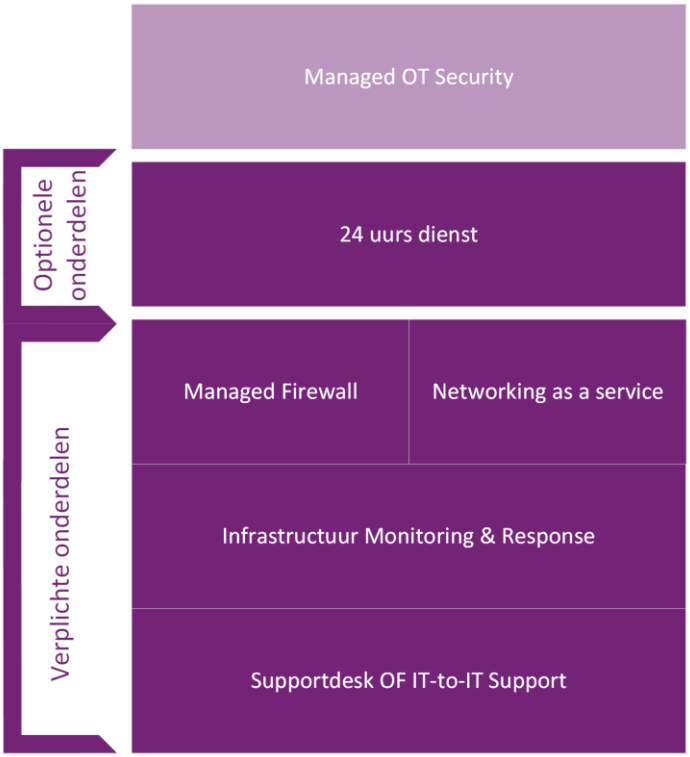
Om Managed OT security op een beheerbare manier aan te bieden aan klanten wordt PCI aangeraden om het afnemen van een aantal andere diensten verplicht te stellen. Dit gebeurt momenteel al met andere diensten die in de SLA van PCI voorkomen. Dit gaat voor managed OT-security om de volgende diensten:

- Supportdesk OF IT-to-IT Support
  Elke klant van PCI die managed diensten afneemt heeft standaard een abonnement voor de supportdesk of IT-to-IT support nodig. Dit abonnement is van belang voor de eerste hulp en afhandeling van problemen.

- Infrastructuur Monitoring & Response
  Deze dienst is vereist omdat het bij Managed OT Security gaat om het continu monitoren van het netwerk en het ondernemen van actie bij een alert. Dit is binnen PCI vastgelegd in de dienst infrastructuur monitoring & response. Deze dienst is vereist voor alle managed diensten van PCI.
- Managed Firewall
  Omdat de gevonden oplossing voor een belangrijk deel afhankelijk is van de communicatie met de firewall en de firewall gebruikt als data-collector is het vereist voor klanten om een managed firewall af te nemen. Op deze manier gebruiken klanten de juiste firewall, is deze gekoppeld aan de monitoringsdienst van PCI en kan PCI deze volledig beheren.
- Networking as a service
  Voor de implementatie van de managed OT-security dienst, is het vereist dat er aanpassingen gedaan worden op laag 2 (switching) van het netwerk van klanten. Om dit juist te kunnen beheren is het van belang dat de juiste netwerkapparatuur aanwezig is en dat PCI deze kan beheren. De networking as a service oplossing is hierom vereist.

Optioneel kan de dienstverlening uitgebreid worden met de 24 uurs dienst van PCI. Dit betekent dat prioriteit 1 incidenten ook buiten kantooruren worden opgelost. Deze dienst is niet verplicht en wordt verder uitgewerkt in het advies over de interne inrichting binnen PCI van de Managed OT Security dienst.

Onderstaand figuur geeft deze onderlinge vereisten weer in de vorm waarop dit standaard is in de SLA van PCI.



Figuur 13, Verplichte en optionele onderdelen dienstverlening

8.4. Organisatie inrichting

Zoals aangegeven bestaat de uitkomst van het technisch ontwerp uit een project/implementatie dienst en een managed dienst. Van de managed dienst is in de vorige paragraaf een SLA uitgewerkt. Om deze dienst op de juiste manier te kunnen beheren wordt in dit deel van het adviesrapport een advies gegeven over de interne inrichting binnen PCI voor het correct kunnen beheren van de managed OT-security dienst.

De organisatie van PCI bestaat uit meerdere business units. Omdat het bij OT-security om IT-dienstverlening gaat valt deze dienst volledig binnen de business unit IT-solutions. Deze business unit bestaat uit meerdere afdelingen. De technische afdelingen beheer & controle, projecting & consultancy en de supportdesk zijn betrokken bij de diensten voor OT-security.

Wanneer een klant bij een accountmanager een aanvraag doet voor netwerkbeveiliging op OT gebied zal er door de afdeling projecting & consultancy een éénmalige dienst worden uitgevoerd waarin de inrichting van het netwerk wordt verbeterd op basis van de best practices uit het technisch ontwerp van dit onderzoek. Daarnaast is deze afdeling verantwoordelijk voor het configureren, plaatsen en testen van de managed OT-security dienst.

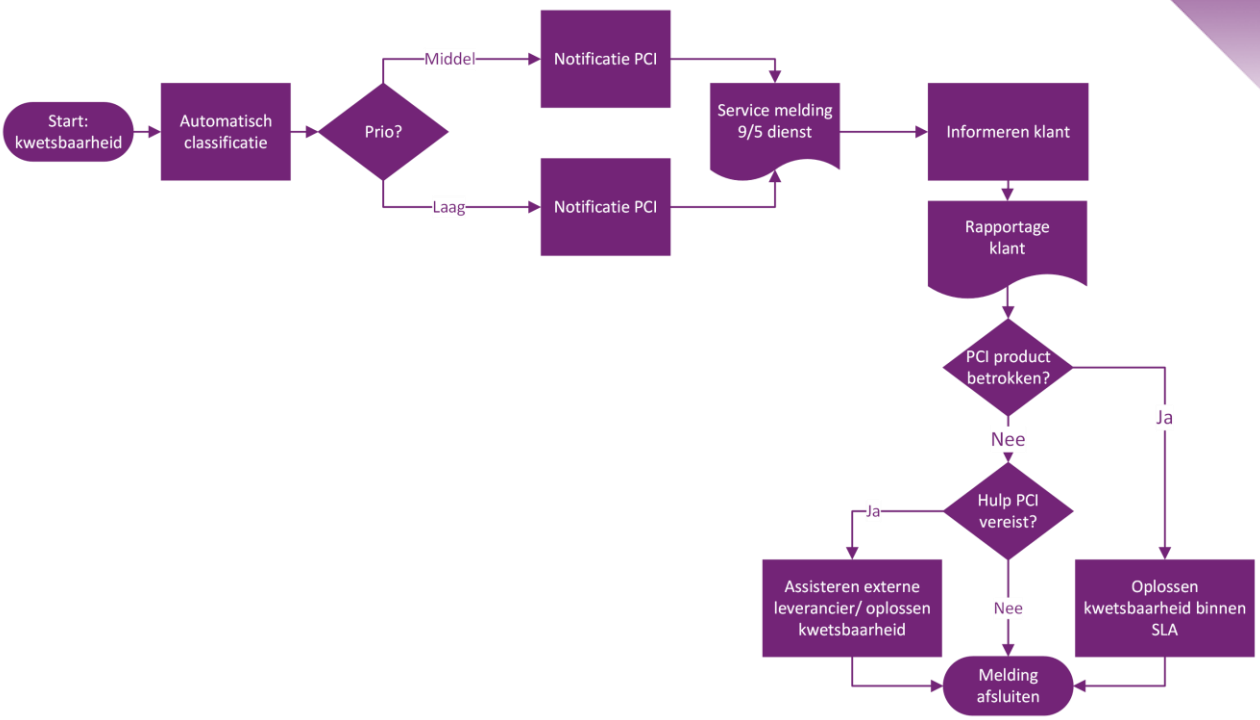
Nadat de managed OT-security dienst is opgeleverd wordt deze conform de SLA beheerd door de afdeling beheer & controle. Updates worden uitgevoerd door deze afdeling op basis van de updatecyclus van de leverancier.

Onderdeel van de managed OT-security dienst is het scannen op kwetsbaarheden en het monitoren van verkeer op verdachte acties. Indien er een kwetsbaarheid optreedt of verdacht verkeer is gedetecteerd wordt dit gemeld bij de supportdesk van PCI. Prioriteit hoog meldingen worden gemeld bij de 24 uurs dienst indien de klant een 24/7 serviceovereenkomst afneemt. De supportdesk bepaald of de prioriteit hoog genoeg is om direct een medewerker in te schakelen, indien de melding terecht is kan in de IoT-security oplossing direct het netwerkverkeer van het betreffende apparaat geblokkeerd worden.

Prioriteit hoog meldingen kunnen alleen voorkomen bij verdacht netwerkverkeer, niet bij het vinden van een kwetsbaarheid. Kwetsbaarheden worden altijd als een prioriteit 2 of 3 melding afgehandeld.

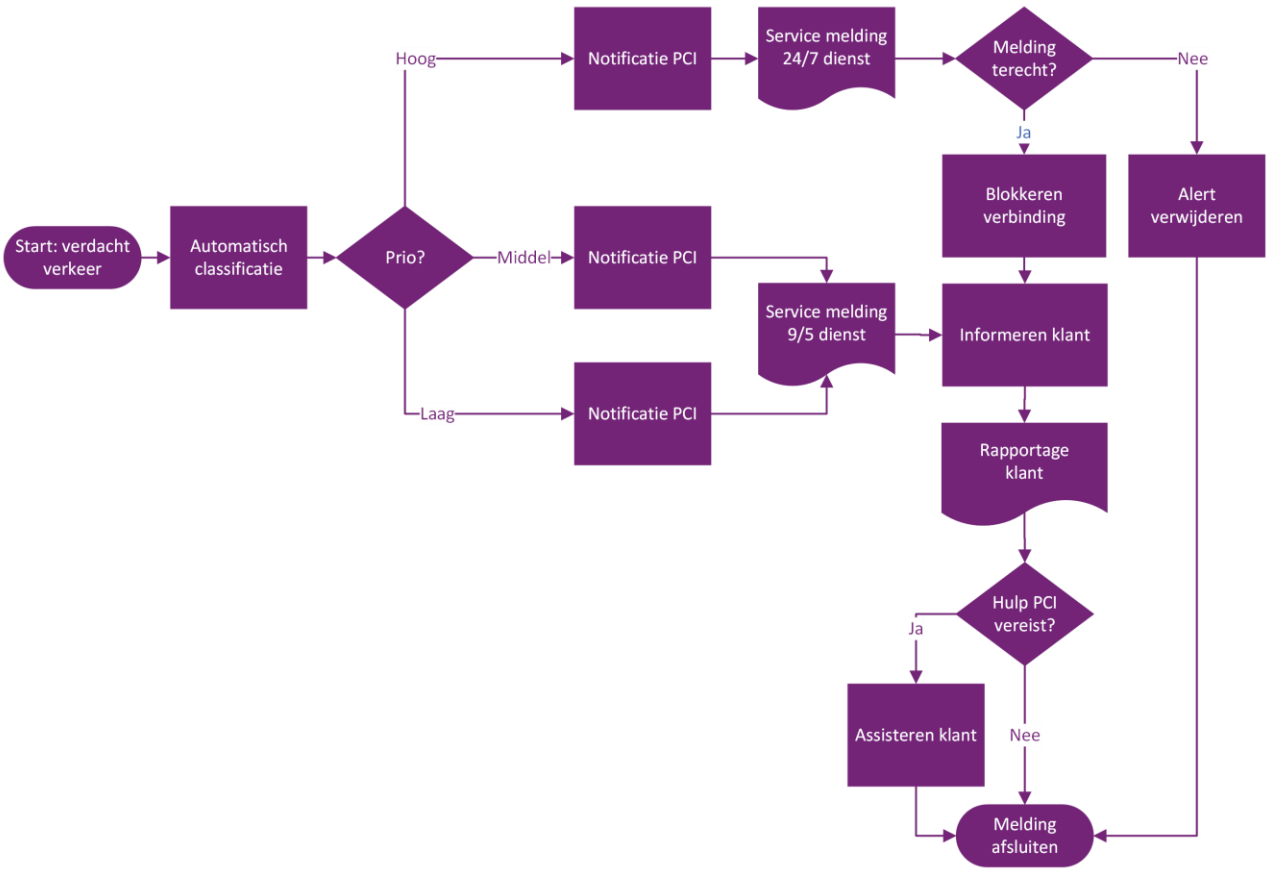
Indien het gaat om een melding van een kwetsbaarheid in een product van PCI, waarbij de klant een SLA van PCI voor het betreffende product heeft, wordt de kwetsbaarheid door PCI verholpen. In alle overige gevallen wordt de kwetsbaarheid aan de klant gemeld, indien PCI kan assisteren in het verhelpen van de kwetsbaarheid kan de kwetsbaarheid of het verdachte netwerkverkeer kan de afdeling beheer & controle of Projecting & consultancy hierbij assisteren. Dit zit niet bij de managed dienst inbegrepen maar vindt enkel plaats op verzoek van de klant.

Onderstaande flowchart geeft aan hoe een melding van een vulnerability zal lopen:



Figuur 14, Flowchart kwetsbaarheid

De volgende flowchart geeft het proces van een melding van verdachte netwerkactiviteit weer:



Figuur 15, Flowchart verdacht netwerkverkeer

8.5. Conclusie

In deze laatste fase van het onderzoek is een advies gegeven over hoe de opgestelde ontwerpen kunnen worden ingezet als dienst welke wordt geleverd aan klanten van PCI. Het advies geeft antwoord op deelvraag zeven “Hoe zou OT-security als een dienst kunnen worden ingericht?”.

De gevonden producten en opgestelde ontwerpen kunnen als twee verschillende diensten worden ingericht.

- Eenmalige projecting dienst
  - Netwerksegmentatie
  - Jump host inrichting
- Managed OT Security dient
  - Palo Alto IoT Security
    - OT asset discovery
    - OT vulnerability scanning
    - OT monitoring

De managed dienst wordt binnen een SLA geleverd aan klanten van PCI. De SLA is zo opgesteld dat indien dit in de toekomst nodig is, het gevonden product kan worden verwisseld met een ander product. Om klanten optimaal van dienst te zijn worden er een aantal andere diensten voorwaardelijk gesteld om OT-security als managed dienst af te nemen bij PCI. Tot slot is er een procesbeschrijving opgesteld voor het uitvoeren van de OT-security dienst.

PCI kan haar managed klanten verder de aanbeveling geven om medewerkers bewust te maken van de risico’s van het werken met operationele technologie. Zo zou de klant beleid op moeten stellen over het gebruik van IT-middelen in productiebedrijven en het gebruik van USB-stations. Dit conform het literatuuronderzoek. Omdat dit niet binnen de OT-security dienst valt is dit beleid niet tijdens de afstudeeropdracht ontworpen.

Verder kan PCI klanten de aanbeveling geven dat het van belang is om een recovery plan op te stellen. Ondanks het inzetten van de OT-security dienst kan een incident voorkomen, het is van belang dat de klant een plan heeft hoe hierop gereageerd moet worden.

9. Eindconclusie

Aan het begin van dit onderzoek is een hoofdvraag opgesteld. Als er een antwoord kan worden gegeven op de hoofdvraag, is het “probleem” van PCI zoals gesteld in de probleemstelling opgelost. Om tot een beantwoording van de hoofdvraag over te gaan moeten eerst de zeven deelvragen beantwoord worden. In dit hoofdstuk wordt daarom gestart met het beantwoorden van de deelvragen, op basis hiervan kan de hoofdvraag beantwoord worden.

9.1. Beantwoording deelvragen

In dit hoofdstuk wordt antwoord gegeven op de deelvragen zoals deze zijn opgesteld in de probleemanalyse.

Deelvraag 1: Wat is OT en waar bestaat OT uit?

In het literatuuronderzoek is antwoord gegeven op deelvraag één: “Wat is OT en waar bestaat OT uit?”. Uit het literatuuronderzoek valt te concluderen dat OT bestaat uit hardware en software welke gebruikt wordt voor het aansturen en controleren van fysieke industriële processen en apparatuur. (Gartner, 2022) (Digital Trust Center, 2022) OT komt voor in verschillende sectoren, in dit onderzoek is gewerkt met de definitie in de industriële context zoals beschreven in de probleemstelling. OT bestaat uit een verzameling van PLCs (Programmable logic controller), DCSs (Distributed control system), HMIs (Human machine interface) en SCADA-oplossingen (Supervisory control and data acquisition). Deze systemen werken samen om zo industriële apparatuur aan te sturen. (AT-Automation, 2022)

Deelvraag 2: Wat voor soort OT zouden klanten van PCI beveiligd willen hebben?

In een behoefte- en contextanalyse is gekeken naar deelvraag twee: “Wat voor soort OT zouden klanten van PCI beveiligd willen hebben?”. Uit de behoefteanalyse is gebleken dat klanten van PCI voornamelijk gebruik maken van operationele technologie voor industriële toepassingen. Deze operationele technologie bestaat uit HMI op traditionele computers voor het aansturen van PLCs welke vervolgens industriële processen aansturen. Daarnaast worden er bij meerdere bedrijven SCADA-oplossingen gebruikt voor het monitoren van industriële machines zodat verstoringen vroegtijdig opgemerkt worden. De onderzochte technologie zit in de meeste gevallen gekoppeld aan een IP gebaseerd netwerk voor verbindingen naar centrale bedrijfsservers en het internet voor toegang door leveranciers voor onderhoudswerkzaamheden.

Deelvraag 3: Welke eisen stelt PCI aan een securitydienst?

De derde deelvraag: “Welke eisen stelt PCI aan een securitydienst?” is behandeld in een behoefte- en contextanalyse. Uit de contextanalyse is gebleken dat PCI zichzelf ziet als een Managed Service Provider (MSP) die diensten levert aan verschillende klanten. Klanten van PCI zijn van verschillende omvang en er wordt met meerdere leveranciers gewerkt. Uit de behoefteanalyse blijkt dan ook dat PCI graag ziet dat een dienst centraal te beheren is, door een IT-specialist te implementeren is, schaalbaar in te zetten is bij verschillende klanten en kan samenwerken met bestaande oplossingen van huidige leveranciers. Dit blijkt ook uit de randvoorwaarden en uit de requirements. Deze requirements zijn terug te vinden in de requirementsanalyse en geven aan welke eisen PCI heeft gesteld aan een securitydienst.

Deelvraag 4: Welke bedreigingen zijn er op het gebied van OT?

In het literatuuronderzoek is antwoord gegeven op deelvraag vier: “Welke dreigingen zijn er op het gebied van OT?”. Dreigingen op OT komen in veel gevallen vanuit het interne IT-netwerk van organisaties, dit omdat deze netwerken steeds vaker onderling verbonden zijn. (PWC, 2019) Via een bekende hacking techniek (zoals social engineering, password guessing, man-in-the-middle, spyware of trojan horse installatie) probeert een aanvaller binnen te komen op het interne netwerk, daarmee is de firewall aan de buitenkant van een organisatie overwonnen. Doordat het vaak slecht mogelijk is om direct in te breken op een PLC, DCS of HMI vindt er in de meeste gevallen vanaf het IT-netwerk een aanval plaats op een traditionele computer op het OT-netwerk. (Anton, et al., 2021) Risico’s voor OT zijn er op het gebied van bedrijfsspionage, het stil leggen van een productielijn of het toebrengen van schade aan mensen of de omgeving. Het gaat hier in veel gevallen om het beïnvloeden van OT doormiddel van het injecteren van programmacode. (Kaspersky, 2021) (Zhang, 2020)

Deelvraag 5: Welke best practices en bestaande normen zijn er op het gebied van OT-security?
Uit het literatuuronderzoek is gebleken dat er voor de beveiliging van operationele technologie gebruik kan worden gemaakt van de NEN-norm IEC 62443. (IEC, 2013) Deze norm is voor een deel toepasbaar voor het beveiligen van OT doormiddel van IT-oplossingen. Het volledig implementeren van deze norm door PCI is niet mogelijk, dit omdat een belangrijk deel van de maatregelen geïmplementeerd zou moeten worden door de leveranciers/producenten van OT.

Verder zoekt deelvraag vijf naar best practices op het gebied van OT-security. Deze zijn samen te vatten in 16 ontwerpprincipes. Het is verstandig om het ontwerp te baseren op deze ontwerpprincipes. Deze ontwerpprincipes worden gebruikt voor het verder bepalen van de vereiste functionaliteiten aan methodieken, oplossingen en producten die tijdens de beantwoording van deelvraag zes gezocht worden.

Deelvraag 6: Welke oplossingen, methodieken en producten kunnen in een OT-security dienst worden aangeboden?
In het functioneel- en technisch ontwerp is gezocht naar verschillende oplossingen welke door PCI in een OT-security dienst kunnen worden aangeboden. Uit dit ontwerp valt te concluderen dat de dienst moet bestaan uit:

- Palo Alto IoT security ten behoeve van asset discovery, vulnerability scanning en het detecteren van verdacht netwerkverkeer.
- Netwerksegmentatie op basis van productielijn doormiddel van VLAN en firewall security zones
- Een jump host in een DMZ, met toegang tot één of meerdere lijnen op basis van user ID, extern benaderbaar via een VPN-verbinding.

Deze oplossingen zijn onderbouwd doormiddel van de antwoorden op de eerste vijf deelvragen van dit onderzoek. Voor het detecteren van verdacht verkeer, asset discovery en vulnerability scanning is ook het product Guardian van Nozomi geschikt. Er is gekozen voor Palo Alto IoT security in het technisch ontwerp omdat de benodigde hardware aanwezig is bij veel klanten en PCI al een partnerrelatie met Palo Alto heeft.

Het totaalontwerp is een globaal, universeel ontwerp dat met minimale aanpassingen bij meerdere klanten van PCI ingezet kan worden.

Deelvraag 7: Hoe zou OT-security als een dienst kunnen worden ingericht?
In een adviesrapport is ter beantwoording van deelvraag zeven beschreven hoe de gevonden producten en methodieken uit het ontwerp kunnen worden ingezet als dienst bij klanten van PCI. Het wordt aangeraden om deze producten en methodieken op te delen in een managed dienst en eenmalige dienstverlening.

De managed dienst bestaat uit het leveren en beheren van de Palo Alto IoT security oplossing inclusief het opvolgen van alerts volgens de afspraken zoals deze zijn vastgelegd in een SLA.

Daarnaast kan in een eenmalige dienst, binnen PCI bekend als een project, het netwerk van de klant worden gesegmenteerd en kan een jump host worden ingericht.

Om deze diensten goed uit te kunnen voeren wordt aangeraden om klanten minimaal een aantal andere diensten van PCI te leveren. Voordat de managed OT-security oplossing geleverd kan worden zouden klanten ook de diensten supportdesk of it-to-it support, infrastructuur monitoring & response, managed firewall en networking as a service moeten afnemen. Dit zorgt voor een optimale dienstverlening.

9.2. Beantwoording hoofdvraag

Nadat alle deelvragen zijn beantwoord kan een goed onderbouwd antwoord op de hoofdvraag van het onderzoek gegeven worden. De hoofdvraag van dit onderzoek is:

“**Hoe kan PCI Nederland operationele technologie beter beveiligen bij haar klanten?**”

Uit de antwoorden op de deelvragen is gebleken dat PCI als managed service provider (MSP) de operationele technologie bij klanten kan verbeteren in de vorm van een dienst welke centraal te beheren is. Deze dienst richt zich op het verbeteren van de beveiliging van productiemachines, deze machines bestaan uit PLCs, DCSs, HMI en SCADA-systemen.

Operationele technologie is kwetsbaar voor aanvallen die vanaf het internet, vaak via het interne IT-netwerk, op een computer in het machinenetwerk terecht komen. Vanaf deze computers kunnen vervolgens machines en controlesystemen worden beïnvloed. (Anton, et al., 2021)

Voor het verbeteren van de beveiliging zou PCI gebruik kunnen maken van enkele standaarden uit de IEC 62443 norm (IEC, 2013) in combinatie met best-practices uit de literatuur. Deze norm kan echter niet volledig door PCI als IT-dienstverlener worden geïmplementeerd omdat een groot deel van de norm gaat over het inrichten van de productiemachines door de machineleverancier.

Op basis van de door PCI gestelde eisen, wensen van klanten en informatie uit literatuur kan worden geconcludeerd dat de OT-security kan worden opgedeeld in twee diensten waarbinnen methodieken en producten geleverd kunnen worden.

Als eerste bestaat dit uit een éénmalige projecting dienst waarbinnen PCI de netwerkbeveiliging van OT doormiddel van segmentatie en het inrichten van een jump host verbetert volgens de ontwerpen uit het technisch ontwerp van dit onderzoek.

Voor het continu beveiligen van de OT omgeving wordt een managed dienst aan het portfolio van PCI toegevoegd. Binnen deze dienst kan het product Palo Alto IoT-security worden geleverd voor asset discovery, vulnerability scanning en netwerk monitoring. Deze dienst wordt binnen een SLA als managed dienst aan klanten aangeboden.

Door netwerken van klanten goed te segmenteren, klanten een jump host aan te bieden voor toegang door externe leveranciers en het OT-netwerk in kaart te brengen en te monitoren kan PCI operationele technologie beter beveiligen bij haar klanten.

9.3. Discussie

In dit hoofdstuk wordt gereflecteerd op het uitgevoerde onderzoek en de resultaten hiervan. Als eerste wordt gekeken of het uitgevoerde onderzoek beperkingen kent en of er opmerkingen gemaakt moeten worden over de uitkomst van het onderzoek. Vervolgens worden aanbevelingen gedaan voor een vervolgonderzoek.

9.3.1. Beperkingen onderzoek

Het uitgevoerde onderzoek kent een aantal beperkingen. Dit betekent niet dat het onderzoek onjuist of onbruikbaar is maar het is van belang om hier rekening mee te houden bij de interpretatie van de resultaten.

Gedurende dit onderzoek is met slechts één klant van PCI gesproken. Het kan daardoor voorkomen dat er een onvolledig beeld van de probleemstelling is ontstaan. Het meekijken met andere klanten was niet altijd mogelijk en daarom is ervoor gekozen om bij één klant een interview en observatie uit te voeren. Om ervoor te zorgen dat het onderzoek toch in te zetten is bij alle klanten van PCI zijn veel gesprekken gevoerd met de technisch specialisten van PCI over de verschillende omgevingen en is het ontwerp gebaseerd op de universele standaarden van PCI en niet op de situatie van één klant.

In de productselectie liggen de gevonden producten zeer dicht bij elkaar. Zoals ook in de conclusie van de productselectie is aangegeven beschikt het product van Nozomi over dezelfde functionaliteit als de oplossing van Palo Alto. De oplossing van Nozomi lijkt op detailniveau zelfs nog iets geavanceerder en beter doorontwikkeld maar dit vertaalt zich niet in extra functionaliteit. De oplossing van Palo Alto voldoet voor de klanten van PCI aan alle requirements en is een goede oplossing voor een dienst van PCI. Omdat de oplossingen van Palo Alto en Nozomi in functionaliteit gelijk zijn, er al een partnerrelatie tussen PCI en Palo Alto bestaat en de vereiste hardware bij veel klanten al geplaatst is, is de keuze gevallen op de oplossing van Palo Alto IoT security als beste keuze in de OT-omgevingen bij klanten van PCI.

Uit het literatuuronderzoek is gebleken dat operationele technologie een ander werkgebied is als IT. Hoewel OT op zeer veel punten met IT verbonden is en van IT-middelen gebruik maakt zitten er grote verschillen in de werking van een OT-omgeving in vergelijking met een IT-omgeving. PCI is een IT-dienstverlener en levert IT-oplossingen, geïmplementeerd door IT-specialisten. De resultaten van dit onderzoek beschrijven daarom mogelijk niet alle standaarden op het gebied van de beveiliging van OT. Zo is er geen rekening gehouden met fysieke veiligheid en bescherming van mensen en milieu doormiddel van fysieke beveiliging. Het onderzoek beschrijft hoe operationele technologie het beste kan worden beveiligd vanuit een IT-security oogpunt.

9.3.2. Vervolgstappen

De uitkomst van dit onderzoek kan PCI helpen om haar klanten beter van dienst te zijn bij de beveiliging van omgevingen met veel operationele technologie. Om de uitkomsten van dit onderzoek optimaal in te kunnen zetten worden een aantal vervolgstappen aangeraden.

De gevonden producten en methodieken zijn gedurende deze onderzoeksperiode gecontroleerd in een proof of concept met een kleine, gesimuleerde omgeving. Een goede vervolgstap is om een tweede proof of concept uit te voeren in een productienetwerk van een klant. Met een PoC in een klantnetwerk kan beter worden bekeken of het product daadwerkelijk geschikt is om te gebruiken voor de netwerken en de apparatuur van klanten. Daarnaast kan worden geverifieerd of de standaard voor netwerksegmentatie haalbaar is binnen een daadwerkelijke implementatie. Dit zal moeten gebeuren bij een klant die open staat voor het uitvoeren van een proof of concept. Pas nadat dit proof of concept geslaagd is kunnen de definitieve dienstbeschrijvingen worden opgesteld en kunnen de diensten aan meer klanten worden aangeboden.

Verder heeft PCI een aantal zorginstellingen als klanten. De leverancier van Palo Alto IoT-security heeft aangegeven dat de oplossing ook geschikt is voor het gebruik met medische OT. PCI zou een vervolgonderzoek kunnen instellen naar het bieden van managed OT-security voor medische apparatuur.

10. Bibliografie

Access24. (2022, maart 07). *OT Security*. Opgehaald van https://www.access42.nl/diensten/ot-security/

Anton, S., Fraunholz, D., Krohmer, D., Reti, D., Schneider, D., & Schotten, H. (2021). The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities Around the World,. *IEEE Internet of Things Journal, vol. 8, no. 24*, 17525-17540.

Arendsen, M., Cannegieter, J., Grund, A., Heck, P., de Klerk, S., & Zandhuis, J. (2008). *Succes met de requirements!* den Haag: SDU Uitgevers.

AT-Automation. (2022, februari 22). *PLC (Programmable Logic Controller)*. Opgehaald van https://www.at-automation.nl/kennisbank/begrippen/plc/

Bigelow, S. J., & Lutkevich, B. (2021, augustus). *What is IT/OT convergence? Everything you need to know*. Opgehaald van https://searchitoperations.techtarget.com/definition/IT-OT-convergence#:~:text=IT%20systems%20are%20used%20for,in%20enterprise%20and%20industrial%20operations.

Boer, D. d. (2019). Hoorcolleges IT-Architectuur. Enschede: Saxion.

Bouman, E. (2008). Requirements en acceptatiecriteria. In *SmarTEST, Slim testen van informatiesystemen* (pp. 149-156). Den Haag: SDU Uitgevers.

Brevink, B. (2022, februari 25). Interview behoefte & contextanalyse, opdrachtgeverperspectief (Bijlage A). (T. Waanders, Interviewer)

Budimir, M. (2022, februari 16). *What's the difference between PLCs and distributed control systems (DCS)?* Opgehaald van https://www.motioncontroltips.com/faq-whats-difference-plcs-distributed-control-systems-dcs/#:~:text=PLCs%20still%20are%20used%20to,within%20a%20factory%20or%20plant.&text=On%20the%20other%20hand%2C%20a,entire%20systems%20within%20a%20factory.

Buijs, F. (2022, april 07). Interview PaloAlto IoT Security (Bijlage A). (T. Waanders, Interviewer)

Capgemini. (2022, maart 04). *Beveiligingsanalyse van operationele technologie*. Opgehaald van https://www.capgemini.com/nl-nl/diensten/beveiligingsanalyse-van-operationele-technologie/

CGI. (2022, maart 04). *OT security, het ondergeschoven kindje*. Opgehaald van https://www.cgi.com/nl/nl/blog/ot-security-het-ondergeschoven-kindje

Conklin, W. (2016). IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilienc,. *49th Hawaii International Conference on System Sciences (HICSS)*, 2642-2647.

Contu, R., & Orans, L. (2020, maart 05). *OT Security Best Practices (G00352264).* Gartner.

Darktrace. (2022, maart 10). *Darktrace industrial immune system - product overview.* Opgehaald van https://www.darktrace.com/en/resources/ds-iis.pdf

Digital Trust Center. (2022, februari 14). *Operational Technology*. Opgehaald van Digital Trust Center: https://www.digitaltrustcenter.nl/informatie-advies/operational-technology#:~:text=Operational%20Technology%20(OT)%20is%20een,monitoren%20van%20(industri%C3%ABle)%20apparatuur.&text=OT%20speelt%20een%20grote%20rol%20in%20verschillende%20industrie%C3%ABn%2

Digital Trust Center. (2022, februari 18). *Social Engineering*. Opgehaald van Digital Trust Center: https://www.digitaltrustcenter.nl/informatie-advies/social-engineering

Fowler, M. (2003). *UML Distilled.* US: Pearson Education.

Franx, L. (2022, maart 15). *Duitse inlichtingendienst adviseert om antivirussoftware Kaspersky te vervangen*. Opgehaald van https://tweakers.net/nieuws/194400/duitse-inlichtingendienst-adviseert-om-antivirussoftware-kaspersky-te-vervangen.html

Gartner. (2022, 14 februari). *Operational Technology (OT)*. Opgehaald van Gartner Glossary: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

Gartner. (2022, maart 14). *Products In Operational Technology (OT) Security Market*. Opgehaald van https://www.gartner.com/reviews/market/operational-technology-security

GE. (2022, februari 25). *Network Segmentation for Industrial Control Environments* . Opgehaald van https://www.ge.com/digital/sites/default/files/download_assets/network-segmentation-for-industrial-control-environments-whitepaper.pdf

Genau, L. (2021, september 08). *Semi-gestructureerd of half-gestructureerd interview*. Opgehaald van Scribbr onderzoeksmethoden: https://www.scribbr.nl/onderzoeksmethoden/semigestructureerd-interview/

Giles, M. (2019, maart 05). *Triton is the world's most murderous malware, and it's spreading*. Opgehaald van MIT Technology Review: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

HBO-i. (2021, juli 05). *ICT research methods*. Opgehaald van https://ictresearchmethods.nl/Methods

Hewlett Packard Enterprise. (2019, oktober). *ArubaOS-Switch Software Feature Support Matrix 16.1.* Opgehaald van HPe Support Center: https://support.hpe.com/hpesc/public/docDisplay?docId=a00076278en_us

Hofmans, T. (2022, maart 03). *Minister houdt Kaspersky-verbod bij Rijksoverheid in stand*. Opgehaald van https://tweakers.net/nieuws/193912/minister-houdt-kaspersky-verbod-bij-rijksoverheid-in-stand.html

Hollerer, S., Kastner, W., & Sauter, T. (2021). Towards a Threat Modeling Approach Addressing Security and Safety in OT Environments. *17th IEEE International Conference on Factory Communication Systems (WFCS)*, 37-40.

Holmström, A. (2021). *Applying information security to the operational technology environment and the challenges it brings* . Luleå Zweden: Luleå University of Technology.

HP Enterprise. (2022, april 20). *Secure Network Access Control for Modern IT*. Opgehaald van https://www.arubanetworks.com/products/security/network-access-control/

HPe. (2022, maart 28). *Manual Aruba POE Switch*. Opgehaald van https://support.hpe.com/connect/s/product?language=en_US&tab=manualsAndGuides&kmpmoid=1009060831

IEC. (2013). *IEC 62443-3-3:2013.* Switzerland: NEN.

ISO. (2013). *Information technology security techniques - information security management systems - requirements.* Switzerland: ISO/IEC.

Janse, B. (2018). *Multicriteria analyse (MCA)*. Opgehaald van ToolsHero: https://www.toolshero.nl/besluitvorming/multicriteria-analyse-mca/

Juniper. (2022, maart 14). *What is IDS and IPS?* Opgehaald van https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

Kaspersky. (2021, maart 25). *Threats against industrial control systems on the rise in H2 2020, growing by nearly 8 percentage points in the engineering sector.* Opgehaald van https://www.kaspersky.com/about/press-releases/2021_threats-against-industrial-control-systems-on-the-rise-in-h2-2020

Kaspersky. (2022, maart 14). *Industrial CyberSecurity.* Opgehaald van https://www.kaspersky.com/enterprise-security/industrial-solution

Knapp, E., & Langill, J. (2015). Industrial Network Protocols. In *Industrial Netwok Security (Seccond Edition).* USA: Elsevier Inc.

Linden, S. v., Hageraats, E., & Haveman, K. (2016). *Reader ontwerponderzoek.* Enschede: Saxion Hogeschool.

Mendelow, A. (1991). Environmental Scanning: The Impact of the Stakeholder Concept. In *Proceedings From the Second International Conference on Information Systems* (pp. 407-418). Cambridge, MA.

Microsoft. (2021, juli 29). *Implementing Secure Administrative Hosts*. Opgehaald van https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts

Microsoft. (2021, december 31). *Request access to an access package in Azure AD entitlement management*. Opgehaald van https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-request-access

Microsoft. (2022, april 04). *Wat is Azure AD Identity Governance?* Opgehaald van Microsoft Docs: https://docs.microsoft.com/nl-nl/azure/active-directory/governance/identity-governance-overview

Moore, S. (2021, juli 21). *Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans*. Opgehaald van Gartner: https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

Mulder, P. (2017, juni 06). *MoSCoW methode*. Opgehaald van ToolsHero: https://www.toolshero.nl/project-management/moscow-methode/

Nationaal Cyber Security Centrum. (2022, februari 15). *ICS/SCADA.* Opgehaald van Nationaal Cyber Security Centrum: https://www.ncsc.nl/onderwerpen/ics

Nationaal Cyber Security Centrum. (2022, februari 22). *Wat is Ransomware?* Opgehaald van NCSC: https://www.ncsc.nl/onderwerpen/ransomware/wat-is-ransomware

NIST. (2022, maart 03). *Operational technology*. Opgehaald van COMPUTER SECURITY RESOURCE CENTER: https://csrc.nist.gov/glossary/term/operational_technology

Nozomi. (2022, maart 14). *Nozomi networks product overview.* Opgehaald van https://www.nozominetworks.com/products/overview/

Palo Alto. (2022, maart 14). *IOT Security.* Opgehaald van PaloAlto Networks: https://www.paloaltonetworks.com/network-security/iot-security

Palo Alto. (2022, april 20). *Managed Security Service Providers*. Opgehaald van https://www.paloaltonetworks.com/partners/managed-security-service-providers

Palo Alto Networks. (2022, april 20). *Integrate IoT Security with Aruba ClearPass*. Opgehaald van https://docs.paloaltonetworks.com/iot/iot-security-integration/network-access-control/integrate-iot-security-with-aruba-clearpass

Palo Alto Networks. (2022, maart 23). *IoT Security Administrator's Guide*. Opgehaald van Palo Alto Tech Docs: https://docs.paloaltonetworks.com/iot/iot-security-admin.html

Palo Alto Networks. (2022, maart 10). *PAN-OS Administrator's Guide*. Opgehaald van https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/getting-started.html

PaloAlto Networks. (2022, maart 14). *Set Up SAML Authentication*. Opgehaald van https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/authentication/set-up-external-authentication/set-up-saml-authentication.html

PCI IT-Solutions. (2022, januari 03). Service Level Agreement IT Services. Haaksbergen, Overijssel, Nederland.

PCI Nederland. (2021). *Over onze strategie Simpel & Samen 2021*. Lijnden: PCI Nederland.

PCI Nederland. (2022, februari 14). *Over PCI*. Opgehaald van Publieke website PCI: https://www.pcinederland.nl/oplossing/over-ons/

Projectmanagementsite. (2022, februari 11). *Stakeholderanalyse*. Opgehaald van https://projectmanagementsite.nl/stakeholdersanalyse/#.YgPH-urMKUk

PWC. (2019). *Cybersecurity van operationele technologie.* Opgehaald van https://www.pwc.nl/nl/marktsectoren/publieke-sector/documents/pwc-emea-ot-security-capabilities.pdf

PWC. (2020, oktober 19). *The unseen danger: cyber security threats to hospitals' operational systems.* Opgehaald van https://www.pwc.de/de/cyber-security/the-unseen-danger-cyber-security-threats-to-hospitals-operational-systems.pdf

RedHat. (2022, februari 07). *What is operational technology (OT)?* Opgehaald van https://www.redhat.com/en/topics/edge/what-is-ot

Rijksoverheid. (2022, februari 15). *Cybercrime en cybersecurity*. Opgehaald van https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity

ScadaFence. (2022, maart 14). *The SCADAfence Platform.* Opgehaald van https://www.scadafence.com/platform/

Schop, G. (2022, februari 18). *7S-model*. Opgehaald van Managementmodellensite: https://managementmodellensite.nl/7s-model-2/

Schutten, D. (2022, februari). Interview technische omgeving klanten (bijlage A). (T. Waanders, Interviewer)

Secura. (2022, maart 04). *OT*. Opgehaald van https://www.secura.com/nl/services/operationele-technologie

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security.* United States: National Institute of Standards and Technology (NIST). Opgehaald van https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Tenable. (2022, maart 14). *Tenable.OT.* Opgehaald van https://www.tenable.com/products/tenable-ot

Thales. (2019, februari 08). *De noodzaak voor een geïntegreerde IT/OT/IOT cybersecurity aanpak*. Opgehaald van https://www.thalesgroup.com/en/netherlands/references/noodzaak-voor-een-geintegreerde-itotiot-cybersecurity-aanpak

The Open Group. (2013). *ArchiMate 2.1 Specification.* United Kingdom: The Open Group.

Verheij, D. (2022, maart 08). Interview SLM perspectief (Bijlage A). (T. Waanders, Interviewer)

Vos, J., Brink, P. v., & Schie, T. v. (2019, november 26). *Onderzoek ICS TNO: Succesfactoren voor digitaal veilige Operationele Technologie.* Opgehaald van Nationaal Cyber Security Centrum: https://www.ncsc.nl/documenten/publicaties/2019/november/26/onderzoek-ics-tno

Waterfall. (2022, maart 14). *Unidirectional security gateways.* Opgehaald van https://waterfall-security.com/unidirectional-security-gateways/

Williamson, G. (2015, juli 07). *OT, ICS, SCADA – What's the difference?* Opgehaald van https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

Zhang, Y. (2020). All Your PLCs Belong to Me: ICS Ransomware Is Realistic. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 502-509.

Bijlagen

11. Bijlage A: Interviews & gespreksverslagen

Datum: 17-12-2021
Geïnterviewde: Networking & Security specialist
Onderwerp: Formulering afstudeeropdracht

Tijdens het eerste gesprek over de formulering van een afstudeeropdracht is gesproken over de eerste ideeën over een onderzoek naar beveiliging van OT-security. Deze informatie zal gebruikt worden als input voor het afstudeervoorstel

De specialist geeft aan dat hij zich als netwerkspecialist bezighoudt met het beheer en het beveiligen van netwerken van klanten van PCI. Een aantal van deze klanten zijn productiebedrijven die gebruik maken van operationele technologie voor het aansturen van productiemachines. De specialist krijgt in toenemende mate vragen vanuit klanten om oplossingen die PCI biedt voor het beveiligen van OT. De specialist geeft aan dat PCI hier op dit moment geen beleid voor heeft en vaak gebruik maakt van standaard IT-security oplossingen. Verder geeft hij aan dat de configuraties bij klanten sterk verschillen maar dat dit vaak gaat om een IT-middel dat communiceert met een PLC-module. Deze systemen hebben vaak toegang nodig tot het internet of interne servers om informatie op te halen. De internetverbinding wordt daarnaast door leveranciers gebruikt voor extern onderhoud aan een machine. Hier heeft PCI geen standaard methodiek voor en er wordt vaak een door de leverancier aangedragen oplossing voor gebruikt zoals Teamviewer, een VPN-verbinding of een andere remote verbinding.

De specialist ziet de beveiliging van OT als een belangrijk punt, zeker met de recente ontwikkelingen rondom ransomware aanvallen en malware specifiek gericht op OT (Stuxnet).

Datum: 10-02-2022
Geïnterviewde: Networking & Security specialist
Onderwerp: Bespreking PVA & start onderzoek

Tijdens dit gesprek is de eerste versie van het plan van aanpak besproken en is kort gesproken over de probleemstelling. Omdat het PVA geen onderdeel is van dit verslag is hiervan geen gespreksverslag opgemaakt.

Tijdens dit gesprek zijn eerste vragen gesteld omtrent de probleemstelling, context en eisen aan het onderzoek. De specialist geeft aan dat vanuit zijn rol als netwerkspecialist hij het belangrijk vindt dat PCI altijd de beste oplossing biedt aan de klanten. Hij kijkt hierbij zelf graag naar onderzoeken van Gartner, een bekende IT-vergelijkingssite. Belangrijke stakeholders aan het onderzoek zijn bijvoorbeeld de technical field service manager, als het om een dienst gaat iemand van SLM en natuurlijk de klanten die dit gaan gebruiken.

Datum: 24-02-2022
Geïnterviewde: Networking & Security specialist
Onderwerp: Interview netwerkspecialist perspectief

1. Wat is de leverancier van PCI voor netwerkapparatuur?
   Wij maken gebruik van switches en netwerkapparatuur van HPe/ Aruba.
   a. Zijn er klanten met meer specifieke OT-netwerkapparatuur?
      Een specifieke klant maakt gebruik van Siemens switches in het OT-netwerk. Meeste klanten gebruiken Aruba switches voor OT-netwerken.
2. Welke firewall oplossingen worden gebruikt?
   Op locaties van klanten wordt gebruik gemaakt van de firewall oplossingen van Palo Alto en Barracuda. Het gaat hierbij om een Next Generation Firewall.

3. Welke leveranciers heeft PCI op het gebied van IT-oplossingen?
   HP, Microsoft, Citrix, HPe, Barracuda, Palo Alto, MijnSam, Sentinel One, Rapid7, Acronis
4. Is er een voorkeur voor fysieke of virtuele appliances?
   Op netwerkgebied hebben wij een lichte voorkeur voor fysieke appliances. Virtuele appliances zijn echter ook goed mogelijk. Dit is voor een deel ook afhankelijk van de klant.
5. Waaruit bestaat OT vanuit het perspectief van de netwerkengineer?
   Het bestaat vanuit mijn perspectief uit twee delen, aansturing en controle van processen. Vanuit een HMI, dat is bijvoorbeeld een PC, wordt een machine bediend, hoe dat proces precies loopt heb ik geen zicht op. Deze HMI stuurt een PLC aan.
6. Wat is er nu ingericht op het gebied van netwerksegmentatie/VLAN?
   In het verleden was het OT-netwerk vaak een compleet gescheiden netwerk. De laatste tijd worden er steeds vaker netwerken aan elkaar gekoppeld en doormiddel van VLAN gescheiden. Tussen het IT-netwerk en OT-netwerk worden verbindingen gelegd zodat deze systemen onderling kunnen communiceren. Het hele productienetwerk is vaak één VLAN.
   a. Wordt er gebruik gemaakt van een private VLAN?
      Op dit moment niet, ik verwacht ook niet dat de access switches hiervoor de mogelijkheden hebben.
   b. En zijn er andere oplossingen op layer 2 security die veel worden toegepast?
      De Aruba switches hebben de functie NAC, hierdoor worden de aansluitmogelijkheden van een switch beperkt.
7. Wat zie jij als belangrijke punten ten aanzien van een oplossing op het gebied van OT-security?
   De oplossing moet Multi tenant in te zetten en te beheren zijn. Naast discovery van het netwerk gaat het in mijn opzicht voor een belangrijk deel om het scannen op kwetsbaarheden. De leverancier van een PLC sluit deze vaak zonder overleg aan op een vrije netwerkpoort. Wat voor apparaat het is en welke kwetsbaarheden erin zitten is vaak niet bekend.

Datum: 25-02-2022
Geïnterviewde: Technical Field Service Manager
Onderwerp: Interview opdrachtgever perspectief

De geïnterviewde is als Technical Field Service Manager verantwoordelijk voor de afdeling Projecting & Consultancy, vanuit deze rol is hij geïnterviewd als opdrachtgever voor dit onderzoek.

Er wordt gestart met enkele technische/inhoudelijke vragen over de vraagstelling van PCI:

1. Hoe biedt PCI op dit moment IT-security aan?
   Security is in mijn opzicht meer als alleen cyber security. Het gaat hierbij ook om het fysiek afschermen van locaties, het in kaart brengen van assets en uiteindelijk het bieden van een cyberoplossing.
   PCI biedt voornamelijk “Point” diensten en producten aan klanten. Wij hebben één bepaald product en vullen daarmee een bepaald security vraagstuk in. Het mooiste voor de klant is als het gaat om de overkoepeling, het overnemen van de totale IT-security, dit biedt PCI momenteel niet.
2. Levert PCI IT security als dienst of als product?
   Dit is afhankelijk van de klant. Een aantal klanten van ons zijn zelf druk met de eigen core business en hebben geen eigen IT-specialisten in dienst. Deze klanten nemen de producten van ons af als managed dienst. Grotere klanten met eigen IT-personeel nemen vaak het product af met implementatie. Dit noemen wij een P&C aanvraag, dit staat voor Projecting en Consultancy. Bij de managed dienst leveren wij een dienstomschrijving voor bijvoorbeeld een endpoint scanner. Wij kiezen vervolgens een product dat goed in de markt staat en daar certificeren wij ons voor. Mocht er later een ander product beter zijn, kunnen wij de klanten een ander product aanbieden zonder dat hiervoor het contract met de klant wijzigt. Het is immers een managed dienst. Bij een P&C opdracht leveren wij een product inclusief implementatie en staat in het contract beschreven welk product het is. Voorwaarde is wel dat wij alleen producten leveren waar we op dat moment voor gecertificeerd zijn/kennis van hebben. De klant voert vervolgens zelf het beheer uit.
   a. Kun je een voorbeeld geven van een product waarvoor jullie gecertificeerd zijn?

Wij zijn Microsoft Gold partner, zijn gecertificeerd voor Sentinel One en Palo Alto en leveren dan ook deze producten.

3. Wie draagt de verantwoordelijkheid over securityoplossingen?
   Als het een MSSP-dienst is ligt dit vast in de dienstomschrijving, SLA en DAP. Deze zul je op moeten vragen. Voor P&C ligt de verantwoordelijkheid bij de klant.
4. Hoe zou je de uitkomst van mijn onderzoek willen inzetten?
   Kan zowel als dienst en als P&C opdracht. Ik verwacht niet dat je tijdens je scriptie ook de kosten bepaald en bedenkt hoe de prijs moet worden opgebouwd maar houdt hier wel rekening mee. Het product moet multi tenant te beheren zijn. Ik verwacht een product/idee wat wij aan klanten kunnen aanbieden en zelf verder kunnen uitwerken tot (ideaal gezien) een SECAAS (Security as a service) dienst.
   a. Als een oplossing een managed dienst is, hoe moeten meldingen e.d. die vanuit het systeem komen aankomen bij PCI?
      De afdeling beheer/supportdesk is hiervoor verantwoordelijk. Bij voorkeur werken zij met een dashboard genaamd Logic. Dit dashboard kan direct gekoppeld zijn met SNMP.
      Op de afdeling hangen schermen waarop meldingen zichtbaar zijn.
5. Is er een bepaald beleid voor appliances?
   Nee dit is er niet, wij werken met verschillende soorten appliances zolang ze maar van grotere leveranciers afkomstig zijn.
6. Hoe gaan jullie om met de ondersteuning van legacy software/hardware/OS?
   Wij ondersteunen alleen software waarmee een onderhoudscontract is met de leverancier. Mochten wij zelf leverancier zijn (bijvoorbeeld van VMWare/Microsoft Windows) bieden wij ondersteuning voor legacy in een best effort model. Wij zullen bijvoorbeeld duidelijk aangeven dat er geen officiële ondersteuning vanuit Microsoft is voor Windows XP en wij doen wel ons best om dit systeem zo goed mogelijk te beheren. Risico's zijn voor de klant.
7. Stel je bepaalde eisen aan een nieuwe leverancier?
   Veel leveranciers van IT-producten zijn bij grote bedrijven begonnen. Sentinel One is groot geworden omdat een van de eerste klanten Netflix was, deze bedrijven zijn groot genoeg om ontwikkelkosten te dragen en zo bestaat er de mogelijkheid om marktleider te worden. Wij zoeken vooral naar dit soort bedrijven die na verloop van tijd op zoek gaan naar de meer MKB-organisaties. Een nieuwe marktleider die nog volop in ontwikkeling is vraagt vaak een hoge minimale afname aan licenties/endpoints met de bijbehorende hoge kosten. Dit is voor ons niet geschikt. Veel van deze bedrijven zullen echter in de loop van de tijd de oplossing afslanken zodat deze geschikt wordt voor het MKB. Dit zijn immers de meeste bedrijven en ook onze klanten.

Vervolgens zijn enkele vragen gesteld over de organisatie PCI, deze vragen zullen input zijn voor het invullen van de contextanalyse. Er is begonnen met enkele vragen tbv de externe organisatie.

8. Hoe groot zijn de klanten van PCI.
   Zeer verschillend, wij beginnen bij de kleine bedrijven (enkele tientallen endpoints), MKB, MKB+, Small Enterprise maar daar houdt het op. Wij zullen een KLM, Rabobank of bedrijven van die grootte niet kunnen aannemen. Te kleine klanten worden ook niet aangenomen. Op dit moment zit PCI vol aan klanten/capaciteit.
   a. Hanteren jullie hier een bepaald getal voor (endpoints, FTE, omvang)
      Nee, dit is een kwestie van het gesprek aangaan en aanvoelen wat er gevraagd wordt en dan bekijken of je dit kunt en wil leveren.
   b. Wat is het formaat van de productiebedrijven?
      Dit zijn veelal MKB/MKB+-organisaties.
   c. Wat zijn deze klanten bereid om uit te geven aan OT-security?
      Deze klanten zullen vaak best bereid zijn om geld uit te geven aan IT, bij een securityoplossing is het vaak wel een probleem dat je geen directe functionaliteit levert. De klant moet wel te overtuigen zijn van het nut van de oplossing. De kosten moeten goed in balans zijn met de functionaliteit, we kunnen dit niet verkopen "omdat het er mooi uit ziet".
9. Bij hoeveel en wat voor soort klanten zou mijn onderzoek inzetbaar zijn?

Wij hebben verschillende klanten in de productiesector. Van plastic leveranciers tot scheepsbouw. Ik schat dat dit ongeveer 15 klanten zijn.

Vragen over de interne organisatie:

10. PCI bestaat uit business units, in hoeverre zijn dit zelfstandige bedrijven of moet ik het meer zien als afdelingen?
    De business units zijn bijna helemaal zelfstandig, hebben een eigen budget en eigen omzet. Wel wordt er verwacht dat je als medewerker van PCI ook kijkt naar producten/diensten van andere business units. Bijvoorbeeld je levert een klant IT vanuit deze business unit maar ontdekt dat de klant ook op zoek is naar AV-oplossingen. Deze kun je dan als PCI leveren. Elke business unit heeft zijn eigen accountmanagers maar deze accountmanagers worden extra beloond voor "cross-selling" dit betekent dat oplossingen uit verschillende business units worden gecombineerd.
11. Ik voer mijn opdracht uit voor het team Networking en Security, binnen welke afdeling valt dit?
    De technische teams vallen binnen de afdeling Projecting & Consultancy. Deze afdeling wordt intern ook wel de 3e lijn genoemd maar dat wekt de verkeerde indruk. Het gaat juist ook om het uitvoeren van projecten, niet alleen tickets oplossen.
    a. Wat zijn de overige teams?
       Datacenter, Workspace solutions, Cloud productivity en Networking & Security.
12. Hoe zie je jouw rol als leidinggevende binnen PCI?
    Ik ben als leidinggevende bezig met beslissingen, meedenken en beleid uitzetten. Ik zoek in samenspraak met teamleiders en servicelevel managers naar nieuwe diensten, zoek nieuwe leveranciers en bepaal criteria waaraan nieuwe producten moeten voldoen.
    a. Direct leidinggeven in taken komt dus weinig voor bij PCI?
       Het verdelen van het werk noem ik planning en geen leidinggeven. De dagplanning houdt zich bezig met wat de engineers doen op een dag. Deze planners overleggen wel met mij welke engineer voor een bepaalde klus geschikt is.

Datum: 08-03-2022
Geïnterviewde: Service Level Manager
Onderwerp: Interview SLM perspectief

1. Wat is jouw functie binnen PCI?
   Ik ben werkzaam binnen de afdeling SLM, servicelevel management, wij houden ons bezig met diensten die PCI levert aan haar klanten. SLM gaat voornamelijk over managed dienstverlening, zogenoemde As A Service oplossingen. Wij werken als SLM aan de SLA en OLA documenten, hierin staat wat verschillende partijen van elkaar verwachten. De SLM-medewerker bevindt zich tussen de afdeling sales, de leverancier en de technische afdelingen.
2. Hoe biedt PCI momenteel securitydiensten aan?
   Wij bieden klanten security aan als managed dienstverlening, as a service, de klant betaald dan een periodiek bedrag (betalen naar gebruik) en krijgt daarvoor de dienst inclusief het beheer zoals beschreven in de dienstomschrijving en SLA. Daarnaast kan een "dienst" ook eenmalig worden geleverd, dit noemen we IT-projecten. Hierbij stelt een opdrachtgever, vaak met eigen IT-personeel, een vraag aan PCI welke wij éénmalig implementeren, het beheer doet de klant vervolgens zelf. Ondersteuning is hierbij los in te kopen.
3. Hoe komen jullie tot nieuwe diensten?
   Dit kan op verschillende manieren gestart worden: vanuit de vraag van een klant, maar ook een push van een leverancier. Als Microsoft bijvoorbeeld een nieuwe dienst aan het Office pakket toevoegt wordt van ons verwacht dat we gaan kijken welke klanten we hiermee kunnen faciliteren. Met een BMC (business model canvas) kijken wij altijd wat de toegevoegde waarde is van een dienst, wat de kosten zijn en hoe we hier wat mee kunnen verdienen.
   Bij het ontwikkelen van een dienst is het van belang om te bedenken voor welk klantsegment je dit wil aanbieden. PCI heeft al een zeer groot klantenbestand dat wij als SLM-afdeling kunnen inzien en kunnen uitsplitsen op marktsegment en omzet percentages. Hiermee

kunnen wij goed inschatten of een dienst slim is om in te zetten. Nieuwe klanten vinden is lastig, je bestaande klanten meer oplossingen aanbieden kost veel minder moeite.

4. Zou OT-security als nieuwe dienst passen binnen PCI?
   We doen hier momenteel nog niks mee, ik zou me er eerst verder in moeten verdiepen maar ik kan zo een hele lijst klanten opnoemen waarvoor dit geschikt kan zijn. Hier zit dus zeker potentie in. Het is een zeer actueel en opkomend onderwerp.
5. Wie draagt de verantwoordelijkheid voor een dienst?
   De beheerafdeling van PCI is verantwoordelijk voor het operationeel houden van diensten die wij aanbieden.
   a. En als het gaat om security bijvoorbeeld bij managed endpoint protection?
      Wij dragen geen (financiële) verantwoording voor security incidenten als er wat misgaat binnen een dienst die wij hebben verkocht, daarvoor blijft de klant verantwoordelijk.
6. Hebben jullie specifieke eisen aan producten die je binnen een dienst wil aanbieden?
   Dat verschilt per dienst en prioriteren wij via MoSCoW.
   a. Zijn er ook bepaalde generieke eisen die voor elke dienst gelden?
      De oplossing moet centraal en multi tenant te beheren zijn. En moet ook op het gebied van beveiliging geschikt zijn voor MSP anders zijn wij een te gemakkelijk doelwit. Een oplossing moet bijvoorbeeld role based access hebben.
7. Hoe verloopt een ondersteuningsvraag van een klant?
   Een klant kan of direct bellen met de supportdesk, dit zijn klanten waarbij de eindgebruikers zelf bellen. De supportdienst is een dienst die we aan klanten aanbieden. Of als er intern IT-kennis bij een klant is bieden wij de dienst IT2IT waarbij de IT-beheerder van de klant direct met onze 2e lijn mag bellen. Dit alles tijdens kantooruren. De klant heeft als toevoeging op beide pakketten de mogelijkheid om 24 uurs dienst af te nemen waarmee ook buiten kantooruren major incidenten kunnen worden gemeld.
   Ik zal je een SLA toesturen, dan kun je lezen hoe we dit aanbieden.
   a. En als het gaat om geautomatiseerde monitoring, zoals alerts?
      Deze komen via email of SMS automatisch binnen op een bepaald adres en worden als meldingen aangemaakt in ons ticket systeem.
   b. Dus hier wordt alleen tijdens werkuren naar gekeken?
      Klopt, het zou een goed idee zijn om bij een major incident (herkende hack/verdacht verkeer) automatisch het verkeer te kunnen blocken of de aanval te kunnen stoppen.

Datum: 18-03-2022
Geïnterviewde: Machinepark beheerder & IT Manager
Onderwerp: Interview klantperspectief

1. Wat is uw functie binnen dit bedrijf?
   De machineparkbeheerder houdt zich bezig met het beheer van de operationele technologie in het machinepark, de IT manager met de inrichting van de IT-voorziening.
2. Wat voor soort productiebedrijf is dit?
   Wij produceren kunststof producten en halffabricaten.
3. Wat voor soort machines worden hiervoor gebruikt?
   Het bestaat uit verschillende grote productiemachines voor het maken van de verschillende halffabricaten. Dit zijn vaak verouderde machines die zeer lang meegaan.
4. Zitten deze machines aan het netwerk gekoppeld?
   Ja, via een ethernet verbinding zitten PCs en PLCs aan het netwerk gekoppeld.
   a. Zitten ze direct op het internet of in een intern netwerk?
      Deze zitten op ons interne, afgeschermde productienetwerk.
   b. Waarvoor maken deze machines verbinding?
      Een deel van de machines is afhankelijk van het netwerk voor het opvragen van recepturen, de status van orders en het ophalen van gewichten.

Een ander deel van de machines zit enkel aan het netwerk gekoppeld voor statistieken waardoor het onderhoudsproces efficiënter wordt. Sensoren worden op afstand uitgelezen en in het geval van een storing krijgt de technische dienst hier melding van. Daarnaast helpt deze software voor het voorspellen van onderhoud. Als het netwerk uitvalt kan de productie in deze gevallen door blijven werken.

5. Waarmee maken OT-systemen verbinding?

   Onze machines maken verbinding met ons interne ERP systeem, dit gaat doormiddel van een bestandsuitwisseling op een ftp-site. Het ERP systeem wordt ook gebruikt in het kantoornetwerk. Daarnaast maakt OT verbinding met het systeem voor verpakkingen en voor het doseren van hoeveelheden aan materiaal.

   a. Waarvoor wordt met het kantoornetwerk verbinding gemaakt?

      Voornamelijk voor het doorgeven van de status van een order, de inhoud van een order en de verpakkingsgegevens, zoals het bruto en nettogewicht na productie.

6. Zitten de systemen in een eigen VLAN

   Alle productiemachines en OT zitten in één VLAN, het productie VLAN.

7. Waar bestaat een stuk OT uit?

   In de meeste gevallen uit PLCs, Linux en Windows systemen.

   a. Gaat dit ook om verouderde systemen?

      Ja, een deel van de systemen draait op een oude Windows versie.

   b. Bestaat er nog de mogelijkheid om deze te updaten?

      Nee, de oude PLC software kan geen verbinding maken met Windows 10. Het vervangen van alle PLC software zou 160.000 euro kosten, dit is te hoog voor een update.

8. Hebben deze machines ook een internetverbinding nodig?

   Leveranciers maken verbinding met het OT-netwerk voor remote onderhoud. Dit kan handig zijn omdat sommige leveranciers in het buitenland gevestigd zitten. Nadeel hieraan is dat het slecht te controleren is en dat de leverancier direct toegang tot het hele OT-netwerk heeft.

   a. Om hoeveel leveranciers gaat dit?

      Dit gaat om 8 leveranciers.

9. Hoe maken leveranciers verbinding met een machine?

   Dit verschilt van leverancier, kan via een VPN-verbinding of een eigen router van de leverancier. Bij een eigen router wordt om onze procedures heen gewerkt. MFA zou een goede toevoeging zijn op dit gebied.

10. Wordt er ook intern verbinding op afstand gemaakt met machines?

    Een aantal machines kunnen we op afstand bedienen vanaf het kantoornetwerk via een VNC-verbinding. Dit kunnen een beperkt aantal medewerkers na invoering van persoonlijke inloggegevens.

    a. Welke risico's zie je hier zelf in?

       Ik zit vooral een risico in dat de teamleiders te makkelijk worden met het bijsturen van een machine op afstand. Als je direct bij een machine staat kun je zien wat er gebeurt, dit kan op afstand niet.

11. Wat zie je als dreiging op OT gebied? Denk hierbij aan spionage, data diefstal, of het stopleggen van de productie.

    Ik zie vooral een risico in de kans dat ons productienetwerk wordt aangevallen en dat daarom de productie stil komt te liggen. Onze productie werkt 24 uur per dag, 7 dagen per week. Een onderbreking in de productie is dus moeilijk in te halen.

12. Hebben jullie ook eigen IT-beheer of is alles uitbesteed?

    Veel IT-beheer is uitbesteed maar we hebben ook nog steeds eigen beheerders in dienst, voornamelijk functioneel beheerders.

    a. Wie gaat er over het toegang geven van leveranciers tot machines?

       Op dit moment bepalen de leveranciers dat zelf, ik zou graag zien dat een teamleider hier over kan beslissen, of iemand van de 24 uurs storingsdienst.

Datum: 07-04-2022
Geïnterviewde: Technisch specialist Palo Alto
Onderwerp: Expert interview

Tijdens het opstellen van het technisch ontwerp is gekeken naar het product Palo Alto, IoT Security. Dit product is geselecteerd als meeste geschikte oplossing voor implementatie in het uiteindelijke ontwerp. Om deze reden is gesproken met een engineer van de leverancier van dit product. Met deze leverancier is gesproken over de mogelijkheden van het product en de installatie vereisten.

1. Wat voor soort product is Palo Alto IoT Security?
   IoT Security is een uitbreiding op onze bestaande IT-security producten en richt zich op de beveiliging van IoT. De term IoT moet je breder zien als de definitie die algemeen wordt gebruikt, slimme apparaten. Het gaat bij ons om bijna alle "niet-standaard" apparaten die met een netwerk verbonden zijn. Hiermee bedoel ik apparaten die een IP verbinding hebben maar geen mogelijkheden tot het installeren van een host-based firewall, monitoringstool of virusscanner. Palo Alto spreekt bij IoT over slimme apparaten (bekende IoT), medische apparatuur en operationele technologie zoals in een productiebedrijf.
2. Hoe is het product ontstaan?
   Palo Alto is een leider als het gaat om geavanceerde firewalls en beveiligingstoepassingen. Een aantal jaren geleden heeft Palo Alto een bestaand bedrijf opgekocht dat een IDS netwerkscanner voor IoT ontwikkelde. Dit was oorspronkelijk een hardware appliance welke in het netwerk geplaatst wordt en vanuit daar op een passieve manier het netwerk monitort.
   Dit product hebben wij doorontwikkeld en de hardware vervangen door onze next generation firewall.
3. Waar richt het product zich op?
   Het product werkt in principe in vijf fases:
   1: Asset discovery
   2: Risicoanalyse, ons systeem is zelf lerend en herkent op basis van eerder geanalyseerde data welk apparaat is aangesloten, welke bekende kwetsbaarheden er zijn en wat de risico's aan het apparaat zijn.
   3: Geautomatiseerd policy's aanraden, op basis van de risico's en aanbevelingen in CVE-databases worden aanbevolen acties weergegeven, met de juiste firewall koppeling kunnen deze policy's automatisch worden overgenomen in de configuratie van de firewall.
   4: Verkeer blokkeren: de oplossing monitort netwerkverkeer en herkent verdacht verkeer, in combinatie met de juiste firewall kan dit verkeer geblokkeerd worden.
   5: Controleer unknown threats: de oplossing is in staat om zelfstandig te leren van netwerkverkeer en kan zo vroegtijdig bedreigingen herkennen.
   Anders als veel andere netwerkoplossingen kan Palo Alto netwerkverkeer segmenteren op laag 2 van het netwerk, dit maakt geavanceerde netwerksegmentatie mogelijk.
4. Waar bestaat het product uit?
   Het product bestaat uit een sensor in het te monitoren netwerk. Dit kan een fysieke Palo Alto Next Generaton Firewall zijn maar ook een VM. Deze sensor krijgt bij voorkeur een SPAN poort in het netwerk.
   De sensor stuurt onze geavanceerde applicatie logging door naar een data lake.
   Onze SAAS-applicatie IoT Security voert de analyses op deze data uit en stuurt policy aanbevelingen terug naar de firewall.
5. Wat zijn de vereisten voor het gebruik van het product?
   Er is tenminste een fysieke of virtuele firewall met netwerkverbinding nodig, een IoT security licentie en een Cortex Data lake. Als de klant geen Cortex Data Lake heeft wordt een uitgeklede variant standaard meegeleverd.
6. Waar staat data opgeslagen?
   Er kan worden gekozen voor de Verenigde Staten, Verenigd Koninkrijk, Duitsland of Nederland.

12. Bijlage B: Stakeholderanalyse

Op basis van de eerste gesprekken met de opdrachtgever en online onderzoek naar het onderwerp van het onderzoek is een longlist van mogelijke stakeholders opgesteld. Een samenvatting van deze gesprekken is te vinden in bijlage A.

- PCI Nederland BV
- Netwerkspecialisten PCI
- Accountmanagers PCI
- Klanten PCI met operationele technologie
- Leveranciers PCI
- Leveranciers productiemachines
- Overheden
- Servicelevel managers PCI

12.1.1. Categorisering stakeholders

Om goed te kunnen bepalen welke macht en invloed een stakeholder heeft op dit project zijn de stakeholders opgedeeld in drie groepen: De interne stakeholders (zijn direct bij het onderwerp betrokken vanuit de eigen interne organisatie), de externe stakeholders (zijn direct bij het onderwerp betrokken vanuit een externe partij), interface stakeholders (zijn niet bij het project betrokken maar hebben er wel een vorm van macht over). (Projectmanagementsite, 2022)

Tabel 12, Stakeholder categorisatie

Categorie	Stakeholders
Interne stakeholders	• PCI Nederland BV • Netwerkspecialisten PCI • Accountmanagers PCI • Servicelevel managers PCI
Externe stakeholders	• Klanten PCI met operationele technologie • Leveranciers PCI
Interface stakeholders	• Leveranciers productiemachines • Overheden

Vervolgens is van dezelfde stakeholders bekeken of ze direct of indirect invloed hebben binnen het project, dit is van belang bij het later prioriteren van de stakeholders.

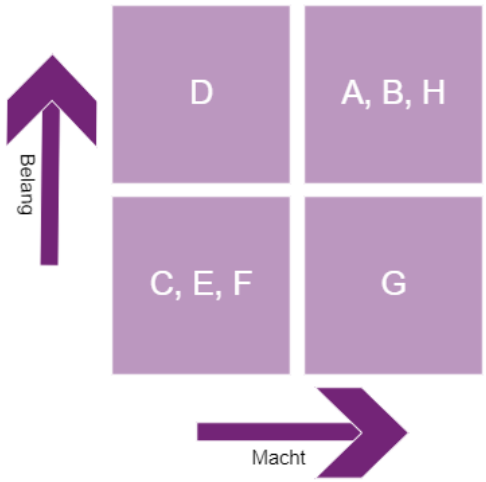
Tabel 13, Invloed van stakeholders

Categorie	Stakeholders
Direct invloed	• PCI Nederland BV • Netwerkspecialisten PCI • Leveranciers PCI • Service level managers
Indirecte invloed	• Accountmanagers PCI • Klanten PCI met operationele technologie • Leveranciers productiemachines • Overheden

12.1.2. Prioritering stakeholders

Om tot een shortlist van stakeholders te komen zijn de stakeholders geprioriteerd op basis van macht en belang volgens de Mendelow methodiek (Mendelow, 1991). Macht geeft aan welke invloed de stakeholder op het project kan leveren. Belang geeft aan in hoeverre de betrokkene een direct belang heeft bij het resultaat van het project.

Stakeholders met een hoge macht of een groot belang bij het resultaat worden automatisch toegevoegd aan de shortlist van stakeholders.



Figuur 16, Stakeholderanalyse

Onderstaande tabel geeft een toelichting op de stakeholderanalyse.

Tabel 14, Stakeholderanalyse

Nr.	Stakeholder	Opmerking
A	PCI Nederland BV (Opdrachtgever)	PCI heeft als opdrachtgever een grote invloed en belang bij de uitkomsten van dit onderzoek. Voor dit perspectief is de Technical Field Service Manager als uitgangspunt gebruikt.
B	Netwerkspecialisten PCI	De netwerkspecialisten van PCI hebben vanwege de functie binnen PCI direct invloed op het project. Omdat zij verantwoordelijk zijn voor de beveiliging hebben ze belang bij het resultaat.
C	Accountmanagers PCI	De accountmanagers van PCI zijn betrokken omdat ze het product uiteindelijk moeten verkopen, ze hebben echter geen direct belang bij de uitkomst. Door de functie hebben ze ook een lage invloed.
D	Klanten PCI met operationele technologie	Klanten van PCI die gebruik maken van operationele technologie hebben een direct belang bij de uitkomst, De klanten hebben belang bij een goed beveiligde omgeving. Doordat het externe stakeholders zijn hebben ze geen directe invloed.
E	Leveranciers PCI	PCI is afhankelijk van haar leveranciers voor het aanbod van securitymiddelen. Hierdoor hebben deze leveranciers een indirecte macht op het resultaat, deze macht is echter laag omdat er

		voor een andere leverancier kan worden gekozen. De leveranciers hebben geen belang bij de uitkomst.
F	Leveranciers productiemachines	Productiemachines worden verkocht om de functie die ze uitvoeren, de leveranciers zijn vaak niet betrokken bij de interne IT-beveiliging.
G	Overheden	Een overheid bepaald regelgeving rondom IT-security. Via regelgeving heeft de overheid invloed op het project, de overheid heeft geen direct belang bij de uitvoering.
H	Servicelevel managers PCI	De servicelevel managers hebben een belang bij de uitkomst van het onderzoek omdat zij verantwoordelijk zijn voor de diensten die PCI aanbiedt. Zij bepalen echter ook waar een dienst aan moet voldoen en hebben daardoor ook een grote macht op het onderzoek.

12.1.3. Stakeholderselectie probleemanalyse

De stakeholders met een hoge macht of invloed op het project worden overgenomen in de shortlist van stakeholders voor de probleemstelling. De stakeholders met een lage macht of invloed worden niet meegenomen in de shortlist omdat deze onvoldoende invloed op- of belang hebben bij- het resultaat.

- PCI Nederland BV (Opdrachtgever, Technical Field Service Manager)
- Netwerkspecialisten PCI
- Klanten PCI met operationele technologie
- Overheden
- Servicelevel managers PCI

12.1.4. Stakeholderselectie Behoefteanalyse

Om tot een zo compleet mogelijke lijst met requirements te komen wordt de behoefte vanuit verschillende perspectieven bekeken. Hiervoor is gekeken naar de stakeholderanalyse zoals deze is uitgevoerd in deze bijlage. In figuur 16 is aangegeven welke stakeholders een groot of klein belang hebben bij de uitkomst en welke stakeholders macht hebben over het onderzoek. De behoefte komt vanuit de stakeholders met een groot belang, om deze reden wordt vanuit het perspectief van de stakeholders met een hoog belang de behoefteanalyse uitgevoerd. De volgende stakeholders hebben op basis van de stakeholderanalyse een groot belang bij de uitkomst van het onderzoek:

- Opdrachtgever (Technical Field Service Manager PCI)
- Netwerkspecialisten PCI
- Klanten PCI met operationele technologie
- Servicelevel managers PCI

12.1.5. Stakeholderselectie contextanalyse

Voor het bepalen van de interne contextanalyse moet met de interne stakeholders gesproken worden. Dit omdat deze stakeholders het beste een beeld kunnen geven van de interne organisatie.

- Opdrachtgever (Technical Field Service Manager PCI)
- Netwerkspecialisten PCI
- Servicelevel managers PCI

13. Bijlage C: Behoefteanalyse

Als eerste wordt er gestart met het bepalen van de behoefte per stakeholder. Deze resultaten zijn in dit hoofdstuk weergegeven.

13.1.1. Perspectief Technical Field Service Manager (opdrachtgever perspectief)

PCI wil haar klanten de totale IT-voorziening uit handen nemen. PCI wil de operationele technologie op locaties van klanten beter beveiligen. PCI levert oplossingen gericht op bepaalde vraagstukken van klanten, dit gaat momenteel veelal om standaard IT-security vraagstukken. PCI wil graag klanten van dienst zijn die komen met vragen over het beveiligen van OT. PCI wil als eerste bij klanten de inventarisatie van OT aan kunnen bieden, hiermee begint elk security vraagstuk. Vervolgens wil PCI OT volgens best practices kunnen beveiligen en monitoren.

PCI levert producten of diensten voor een bepaald vraagstuk, in dit geval OT-security. PCI biedt geen diensten aan die de “totale” IT-security van een klant overneemt. Oplossingen moeten zowel als dienst en als product inclusief implementatie aangeboden kunnen worden. PCI heeft (voornamelijk kleinere) klanten die securityoplossingen als managed service afnemen. De gevonden oplossing moet als dienst kunnen worden beschreven en deze dienst moet door PCI bij klanten uitgevoerd worden. Daarnaast moet de oplossing ook als product/project aangeboden kunnen worden aan klanten. Klanten die de oplossing op deze manier afnemen van PCI moeten het zelf kunnen beheren. Omdat het als managed dienst kan worden verkocht moet het centraal en multi tenant beheerd kunnen worden. Een centraal dashboard voor het beheren van meerdere klanten is hierbij een goede toevoeging. PCI zou graag een oplossing zien waarmee monitoring op OT-netwerken kan worden uitgevoerd. (Brevink, 2022)

PCI wil klanten op een best effort manier ondersteunen op het gebied van legacy software/hardware en operating systems. PCI gaat geen verantwoordelijkheid dragen voor de risico’s hieraan maar wil klanten wel ondersteunen in het verkleinen van de risico’s.

Als er een product van een nieuwe leverancier wordt afgenomen heeft PCI graag dat de leverancier marktleider of goed aangeschreven is op het gebied waar het product gebruikt wordt. PCI maakt enkel gebruik van gevestigde/bewezen producten. (Brevink, 2022)

Op het gebied van kosten moet OT-security realistisch zijn voor MKB/ MKB+ organisaties. Het product moet schaalbaar zijn afhankelijk van de grootte van de organisatie. PCI heeft enkele kleinere klanten en grotere klanten, het heeft geen zin om een product of dienst te leveren dat niet voor kleine en grote organisaties bruikbaar is. De kosten moeten hierop af te stemmen zijn. (Brevink, 2022)

13.1.2. Netwerkspecialisten PCI

De netwerkspecialist geeft aan dat hij graag vanuit zijn rol klanten wil ondersteunen bij vragen over operationele technologie. PCI heeft hier momenteel geen standaard diensten voor beschikbaar terwijl klanten hier wel om vragen. De netwerkspecialist kijkt zelf vaak naar onderzoeken van Gartner om te bepalen welke producten het beste zijn, hij wil altijd het beste product aan een klant aanbieden.

De netwerkspecialist zou graag willen weten hoe kan worden geïnventariseerd welke OT klanten gebruiken voordat hij hier een oplossing aan wil koppelen. Verder zou hij graag willen dat de gevonden oplossingen gebaseerd worden op reeds bekende best practices, dit biedt zekerheid voor PCI en haar klanten.

De netwerkspecialist vindt het verder niet wenselijk dat externe leveranciers vanaf het internet direct een verbinding maken met een productiemachine zonder dat hier een goed onderbouwde standaard voor is. Hij zou graag een oplossing of werkwijze willen hebben voor extern beheer die voldoet aan best practices op security gebied.

De netwerkspecialist geeft aan graag zijn oplossingen te baseren op onderzoek van bekende IT-instituten zoals Gartner. De oplossing moet snel en schaalbaar in te zetten zijn bij klanten van PCI en bij voorkeur multi tenant te beheren zijn, bijvoorbeeld vanuit een centraal dashboard.

De netwerkspecialist erkent dat het inventariseren van OT erg belangrijk is. Dit zal automatisch moeten gebeuren. Door de snelle veranderingen in OT-netwerken is het niet goed mogelijk om een CMDB met OT handmatig bij te houden. Dit gebeurt in de IT vaak ook onvoldoende.

De oplossing moet naast het opsporen van verdacht netwerkverkeer (wat in de praktijk waarschijnlijk erg lastig is) ook moeten zoeken naar kwetsbaarheden in OT-systemen zoals PLCs. Hiervoor kan gebruik worden gemaakt van CVE lijsten, dit is een goede bron voor bekende kwetsbaarheden.

De netwerkspecialist zou daarnaast graag zien dat verdacht verkeer automatisch wordt geblokkeerd op de firewall indien dit mogelijk is. Hiervoor moet de oplossing te koppelen zijn met de gebruikte firewall oplossingen bij PCI. Bij klanten van PCI wordt voornamelijk gebruik gemaakt van de Palo Alto Next Generation Firewall zoals in de context analyse beschreven is.

13.1.3. Klanten PCI met operationele technologie

De klanten van PCI met operationele technologie zijn op zoek naar een oplossing om de OT-omgeving beter te beveiligen om daarmee de doorgang van het primaire proces te kunnen waarborgen.

Een van de klanten van PCI is producent van kunststof producten en halffabricaten. Bij deze klant is gekeken naar de productieomgeving en zijn gesprekken met beheerders van de OT-omgeving gevoerd. Deze klant maakt gebruik van PLCs en Windows en Linux werkstations voor het beheren van het productieproces via een HMI. Deze PLCs zitten direct aan het productienetwerk gekoppeld doormiddel van ethernet verbindingen. Op dit moment is er één groot productienetwerk aanwezig waarin alle machines zitten geplaatst. Deze klant zou graag een oplossing zien voor het beter segmenteren van netwerken zodat bij een incident niet direct de totale productieomgeving wordt getroffen.

Voor het opvragen van recepturen, het centraal aansturen van machines, het opvragen van de status van productieorders, het bijwerken van gegevens van orders en het uitlezen van de status van een machine moeten de productiesystemen toegang krijgen tot een beperkt aantal IT-bronnen uit het kantoornetwerk. Dit gaat in de meeste gevallen via het ftp-protocol. Voor het centraal besturen wordt VNC gebruikt.

Leveranciers van deze klant maken via een VPN-verbinding of een eigen router in het productienetwerk verbinding met de machines voor extern onderhoud. De klant zou graag zien dat dit via de door PCI geleverde infrastructuur op een eenduidige gecontroleerde manier mogelijk wordt, bijvoorbeeld na goedkeuring door een medewerker.

13.1.4. Servicelevel manager PCI

De servicelevel management afdeling zou graag zien hoe OT-security als dienst aangeboden kan worden. De gevonden oplossing moet passen binnen de bestaande SLA omschrijvingen. Een dienst moet zowel als managed service en als eenmalige dienst (IT-project) aan klanten geleverd kunnen worden. Dit betekent dat de oplossing door de klant en door PCI beheerd moet kunnen worden.

Als PCI een oplossing gaat beheren als managed dienst moet de oplossing multi tenant beheerd kunnen worden. Dit betekent dat vanuit één centraal dashboard meerdere omgevingen beheerd kunnen worden. Het heeft de voorkeur als hierin meerdere rollen mogelijk zijn zodat niet elke servicedesk medewerker volledige admin toegang nodig heeft.

Als de dienst bestaat uit één of meerdere nieuwe producten zou het de voorkeur hebben dat incidenten automatisch per email naar het ticket systeem worden verzonden. Daarnaast kan er eventueel een koppeling worden gemaakt met Logic dashboards waarmee de netwerkinfrastructuur van managed klanten wordt gemonitord. Omdat PCI geen 24/7 monitoring beschikbaar heeft, zou het een goede toevoeging zijn als de oplossing gekoppeld wordt aan de bestaande managed Firewall zodat bij een incident de omgeving zonder tussenkomst van een engineer geïsoleerd kan worden. (Verheij, 2022)

13.1.5. Methodiek requirementsanalyse

In gesprekken met de verschillende partijen is de behoefte van deze partijen inzichtelijk gemaakt. In de requirementsanalyse zijn deze behoeftes concreet gemaakt door middel van requirements. De requirements zijn opgesteld en vervolgens geverifieerd bij de stakeholders door middel van een gesloten interview. Dit omdat er hierdoor een duidelijk antwoord ontstaat op de vraag of de gevonden requirements voldoen aan de verwachtingen van de stakeholders. (Arendsen, et al., 2008)

Categoriseren

Om de requirements onderling verifieerbaar te maken zijn deze opgedeeld in drie categorieën: “Business”, “User” en “System” requirements. Een business requirement geeft op hoog niveau aan waarom de oplossing wenselijk is en waarom deze er moet komen. De user requirements geven aan welke functies de oplossing moet bieden. De laatste categorie system requirements geven aan hoe de oplossing zal moeten werken. (Arendsen, et al., 2008)

Functionaliteit

Per requirement is aangegeven of deze wel/niet functioneel is. Functionele requirements zijn functies van de oplossing welke door gebruikers van de oplossing gebruikt worden. Niet functionele requirements zijn eisen aan het systeem die niet direct door gebruikers gebruikt worden. Niet functionele requirements zeggen iets over de werking van de oplossing zonder dat hier functionaliteit aan gekoppeld is.

Prioritering

Om aan te geven welke requirements absolute eisen zijn en welke minder belangrijk zijn worden requirements geprioriteerd volgens de MoSCoW methodiek. Dit is een bekende standaard in de IT om de prioriteit van een requirement aan te geven. “Must” requirements zijn absolute eisen aan de oplossing, zonder deze requirements bestaat de oplossing niet en is deze niet werkbaar. “Should” requirements zijn zeer wenselijk voor een goede functionaliteit maar niet absoluut vereist. “Could” requirements zijn wenselijk, echter kan de oplossing volledig functioneren zonder deze requirements. De laatste categorie “Won’t” have requirements zijn gewenst in een later project. (Mulder, 2017)

Verbanden

Om requirements goed te kunnen verifiëren is het van belang dat tussen de requirements verbanden worden aangegeven. Dit is aangegeven met de termen “genereert” en “realiseert”. Genereert geeft aan welke requirements voorkomen uit het betreffende requirement, realiseert geeft aan welke requirements worden gerealiseerd door het implementeren van dit requirement.

14. Bijlage D: 7-S Model

14.1. Methodiek

Ten behoeve van de interne analyse van PCI is gebruik gemaakt van het 7-S model van McKinsey (Schop, 2022).

14.2. Resultaten

14.2.1. Shared Values (missie & visie)

In deze dimensie wordt gekeken naar welke gedeelde waarden er binnen PCI gelden. Waar staat PCI voor en wat willen ze uitdragen aan de klanten. PCI schrijft in haar missie en visie: “Sinds de oprichting van PCI is er één ding dat vast staat: we zijn er om klanten aan de ideale werkomgeving te helpen. Maar verder verandert binnen PCI voortdurend alles, want we willen door. We willen beter worden en groeien.” (PCI Nederland, 2021) PCI draagt daarnaast de slogan uit “Meer dan IT” en “All to keep you going”. Hiermee wil PCI uitdragen dat ze haar klanten een complete werkomgeving willen bieden en dat PCI altijd gaat voor het beste voor de klant. Dit blijkt ook uit gesprekken die met medewerkers zijn gevoerd. Een veelgehoorde uitspraak is: “Wij willen gewoon de beste oplossing voor onze klanten.”

14.2.2. Strategie

PCI Nederland helpt organisaties met IT en een complete werkomgeving. PCI heeft als doelstelling om de organisatie te laten groeien via de IT-Solutions divisie. PCI helpt klanten met IT-middelen en biedt daarnaast audiovisuele middelen, printers en kantoorartikelen om klanten te kunnen ondersteunen op alle gebieden. (PCI Nederland, 2021) Dit is tevens te herkennen in de slogan van PCI: “All to keep you going”. (PCI Nederland, 2022) PCI ziet IT als de basis voor een ideale werkomgeving. PCI levert maatwerk omdat de ideale werkomgeving voor alle klanten verschillend is.

14.2.3. Structuur

PCI biedt haar klanten totale oplossingen waarmee de basis voor een werkplek kan worden geboden. PCI bestaat uit de business units IT-Solutions, Audiovisueel, Managed Print Services en Supplies. (PCI Nederland, 2022) De business unit IT-Solutions levert totale IT-oplossingen aan een groot aantal klanten. Dit project richt zich op productiebedrijven omdat deze bedrijven gebruik maken van OT. De business unit IT-solutions heeft de hoofdvestiging in Haaksbergen waar ook de servicedesk, beheerafdelingen en de meeste IT-specialisten werken. Bij de business unit IT-solutions zijn c.a. 150 medewerkers werkzaam. Deze business unit is opgedeeld in meerdere afdelingen waarbij de afstudeeropdracht wordt uitgevoerd in opdracht van de afdeling Projecting & Consultancy. Deze afdeling voert implementaties bij klanten uit en lost complexere problemen op. De afdeling is opgedeeld in vier specialismes: Datacenter solutions, Workspace solutions, Cloud productivity en Networking & Security. Deze opdracht valt onder het specialisme Networking & Security.

14.2.4. Systemen

Het resultaat van dit onderzoek wordt ingezet bij klanten van PCI met productiemachines. Deze klanten beschikken over een IT-infrastructuur welke door PCI wordt beheerd. Er is gekeken naar het netwerkontwerp van een aantal productiebedrijven. PCI geeft aan dat deze netwerken altijd op ongeveer dezelfde manier worden ingericht. (Schutten, 2022)

PCI maakt bij klanten gebruik van de Next Generation Firewall oplossingen van Palo Alto Networks of Barracuda. Deze firewall systemen kunnen worden beheerd door PCI als managed service. Bij de meeste klanten met operationele technologie wordt gebruik gemaakt van de Palo Alto Networks firewall, ook in de toekomst zal meer worden overgegaan op de Palo Alto Firewall oplossingen. Routering gebeurt standaard op de firewall. PCI heeft een partnership met Palo Alto.

Bij de meeste klanten maakt PCI gebruik van switches van Aruba Networks (HPe). Bij één enkele klant wordt in het OT-netwerk gebruik gemaakt van Siemens Industriële switches. In de meeste

gevallen is OT aangesloten op de standaard access switches van Aruba Networks. Bij steeds meer klanten wordt de netwerkomgeving uitgebreid met het product Aruba Clearpass. Dit is een network access control systeem waarmee op basis van bepaalde criteria automatisch een systeem toegang kan krijgen tot het netwerk, een VLAN worden toegewezen of in een quarantaine subnet worden geplaatst. Ook met HPe/Aruba heeft PCI een partnership.

Voor de segmentatie van netwerken wordt gebruik gemaakt van VLANs en firewall oplossingen.

Op werkplekken en voor servers wordt gebruik gemaakt van de besturingssystemen van Microsoft. PCI beschikt over een partnership met Microsoft. Voor het beheer van gebruikersaccounts wordt (Azure) Active Directory gebruikt.

Klanten van PCI hebben in de meeste gevallen een eigen IT-omgeving of maken gebruik van de IAAS-omgeving van PCI. Deze omgeving is verspreid over drie datacenters in Oost Nederland.

Voor het bijhouden van de status van systemen bij klanten wordt gebruik gemaakt van dashboards in Logic. Dit systeem kan meldingen direct van een IT-asset via SNMP verwerken en op een scherm/online dashboard weergeven. Indien nodig maakt de supportdesk meldingen aan van verstoringen in een intern ticket systeem Connectwise. Het koppelen aan dit systeem is echter geen harde randvoorwaarde.

14.2.5. Staf (Personeel)

Binnen de business unit IT-solutions wordt gewerkt in afdelingen welke zijn opgedeeld in teams. Het team dat de opdracht heeft gegeven tot dit onderzoek is het team Networking & Security dat onderdeel is van de afdeling consultancy. De medewerkers van dit team implementeren en beheren/onderhouden de netwerkinfrastructuur op locaties van klanten van PCI. De klanten verschillen van grote tot kleine locaties. De afdeling consultancy is verder verantwoordelijk voor het oplossen van (complexe) storingen indien een medewerker van de afdeling support of beheer geen oplossing kan vinden.

De afdeling waar het onderzoek is uitgevoerd bestaat verder uit de teams Workspace solutions, Datacenter en Cloud productivity. Elk team bestaat uit specialisten met zeer veel kennis over het specialisme van het team. De teams werken samen om zo alle soorten implementaties uit te kunnen voeren en storingen op te kunnen lossen.

14.2.6. Stijl

Medewerkers binnen PCI werken zeer zelfstandig en er is weinig directe sturing. De planning wijst incidenten en implementaties aan medewerkers toe en plant deze in. De medewerkers gaan vervolgens zelfstandig met deze incidenten bezig, op locatie bij klanten, vanuit huis of vanuit een locatie van PCI. De leidinggevende van PCI zijn voornamelijk bezig met het maken van keuzes voor nieuwe leveranciers, diensten en beleid.

14.2.7. Skills

PCI richt zich op het bieden van een complete IT-omgeving met ondersteunende diensten zoals printen, AV en supplies. Wat PCI sterk maakt is de betrokkenheid van medewerkers met klanten en de uitgebreide specialismes. PCI is daarnaast partner van Microsoft, Citrix en HPe, dit betekent dat de medewerkers van PCI beschikken over certificeringen voor deze producten. Er is veel kennis aanwezig over producten van deze leveranciers. PCI bestaat uit vier business units wat (bijna) zelfsturende bedrijven zijn met eigen budgetten, producten en omzet. Echter stimuleert PCI “cross-selling” wat betekent dat er wordt geprobeerd om klanten van bijvoorbeeld Print Services ook IT-diensten te leveren. Dit maakt PCI een totaalleverancier op het gebied van (digitale)werkplekken.

15. Bijlage E: Selectiecriteria multicriteria analyse

Tabel 15, Selectiecriteria

Criteria	Requirements	Randvoorwaarden	Ontwerpprincipes
Gevestigde leverancier (geen startups)	S05		
Biedt OT-asset discovery	S04		P5, P6, P7
Genereert netwerkdiagrammen	S04		P5, P6, P8
Monitort OT-protocollen	S06, S07, S08		P11, P15, P16
Bevat vulnerability scanner	S03		P1, P2, P3
Biedt ondersteuning voor een MSP-model		R01	
Vervangt niet de bestaande firewall		R04	
Werkt met meerdere VLANs		R02, R05	P3, P7, P8
Beschikt over centrale management interface	S09		
Ondersteund remote access via jump host	S02		P09, P12, P13
Schaalbaar licentiemodel	S10, S12		
Maakt gebruik van CVE-database	S11		
Beveiligd legacy hard/software	S13		P2
Bevat rolebased access control	S14		
Te koppelen met Palo Alto Firewall voor automatisch blokkeren van aanvallen	S15		
Is in staat om OT-protocollen te isoleren van het internet.	S15		P16
Te koppelen met Connectwise voor het automatisch aanmaken van meldingen	S16		
Te koppelen met Logic dashboard voor netwerkmonitoring	S17		
Kan meerdere (fysiek gescheiden) locaties monitoren vanuit één omgeving	S09		

16. Bijlage F: Onderbouwing testen & requirements

Tabel 16, Onderbouwing testen & requirements

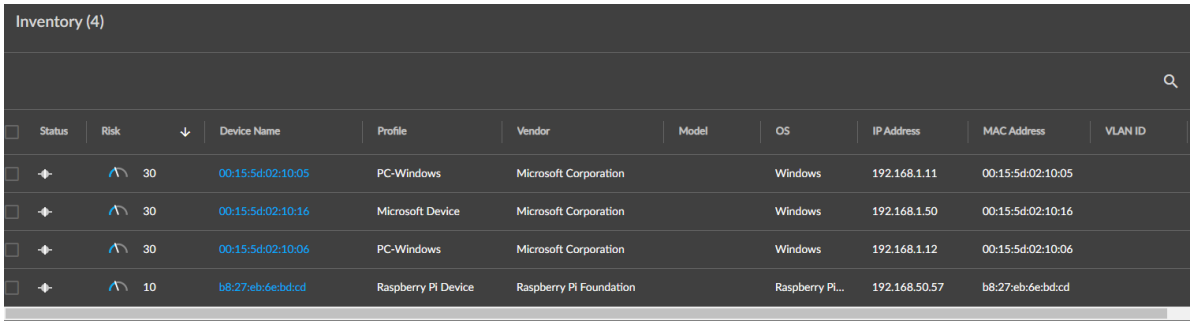
Volg nr.	Belang	Acceptatiecriterium	Must requirements	Should requirements	Could requirements	Rand-voorwaarde
T01	36	Er wordt een compleet beeld gegeven van aanwezige OT en andere assets in het OT-netwerk.	B01, B02, B03, U04, S04	B08, U11		R03
T02	31	Kwetsbaarheden in OT kunnen worden gescand.	B01, B02, B03, U09, S03	B08, S13		
T03	28	Leverancier A heeft vanaf de Jump Host wel toegang tot het interne netwerk, leverancier B heeft vanaf de Jump Host geen toegang tot het interne netwerk.	B02, U02, U07, U08, S02	S14		
T04	23	Er worden industriële protocollen herkend.	B01, B03, U09, S06	B08		
T05	20	Verbindingen tussen assets worden herkend.	B02, U06, S07, S08			
T06	20	De oplossing herkent verdacht netwerkverkeer op industriële apparatuur.	B01, B02, S06, S08			
T07	18	Er kan een sessie op laag 2 van het netwerk gevolgd worden.	U06, S08	S13		R02
T08	18	Kwetsbaarheden worden verwezen naar een CVE-database.	B02, U09, S11	B08		
T09	18	De oplossing bevat een centraal management dashboard.	B04, S09	U10		R01
T10	15	De oplossing kan door een MSP-partner besteld worden.	B05, B06			R01
T11	13	De oplossing scant meerdere VLANs vanuit één appliance.		S12		R02, R05
T12	11	Er kan een gebruiker met afwijkende	B04	U14, S14		

		rechten worden aangemaakt.				
T13	11	De status van de oplossing wordt weergegeven in Logic Dashboards.	B04, B07		S17	
T14	11	Het is mogelijk om later sensoren toe te voegen.		S10, S12		R05
T15	10	De oplossing werkt in combinatie met de Palo Alto Next Generation Firewall.	U03			R04
T16	8	Klanten kunnen zelfstandig de inventory bekijken zonder een aanpassing te doen.	U05	S14		
T17	7	Er kan automatisch een melding in Connectwise worden gemaakt.		U10, U12	S16	
T18	6	De oplossing is gekoppeld aan de firewall.	B03		S15	

17. Bijlage G: Detailresultaten testrapport

T01: Er wordt een compleet beeld gegeven van aanwezige OT en andere assets in het OT-netwerk.

De oplossing heeft gedurende 2 uur een inventory uitgevoerd. Na deze periode is gekeken welke apparaten in het netwerk herkend zijn. Dit zijn alle apparaten welke waren aangesloten op het prototype.



Status	Risk	Device Name	Profile	Vendor	Model	OS	IP Address	MAC Address	VLAN ID
	30	00:15:5d:02:10:05	PC-Windows	Microsoft Corporation		Windows	192.168.1.11	00:15:5d:02:10:05	
	30	00:15:5d:02:10:16	Microsoft Device	Microsoft Corporation		Windows	192.168.1.50	00:15:5d:02:10:16	
	30	00:15:5d:02:10:06	PC-Windows	Microsoft Corporation		Windows	192.168.1.12	00:15:5d:02:10:06	
	10	b8:27:eb:6e:bd:cd	Raspberry Pi Device	Raspberry Pi Foundation		Raspberry Pi...	192.168.50.57	b8:27:eb:6e:bd:cd	

Figuur 17, Testrapport - Inventory OT netwerk

T02: Kwetsbaarheden in OT kunnen worden gescand.

In een passieve scan van een netwerk worden de volgende kwetsbaarheden in OT-systemen zichtbaar.

Figuur 18, Testrapport - Vulnerability scan

T03: Leverancier A heeft vanaf de Jump Host wel toegang tot het interne netwerk, leverancier B heeft vanaf de Jump Host geen toegang tot het interne netwerk

Onderstaande regel is aangemaakt in de firewall. Deze regel beschrijft dat gebruikers in het DMZ (waar de jump host geplaatst is) enkel toegang krijgen tot de zone Internal (waar de productiemachines geplaatst zijn) indien er is ingelogd als Leverancier A.

5	Allow supplier access	none	universal	DMZ	any	Leverancier_A	any	Internal

Figuur 19, Testrapport - Firewall regel jump host

Deze regel toont dat de firewall inderdaad een RDP-verbinding tussen de jump host en een OT simulatie desktop toestaat als leverancier A is ingelogd op dit systeem.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
04/11 15:36:47	end	DMZ	Internal	192.168.100.51	leverancier_a	192.168.1.11	3389	ms-rdp	allow	Allow supplier access

Figuur 20, Testrapport - Leverancier met toegang

De volgende regel toont aan dat dezelfde RDP-verbinding wordt geweigerd als leverancier B is ingelogd op dezelfde jump host.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
04/11 16:37:07	drop	DMZ	Internal	192.168.100.51	leverancier_b	192.168.1.11	3389	not-applicable	deny	interzone-default

Figuur 21, Testrapport - Leverancier zonder toegang

T04: Er worden industriële protocollen herkent.

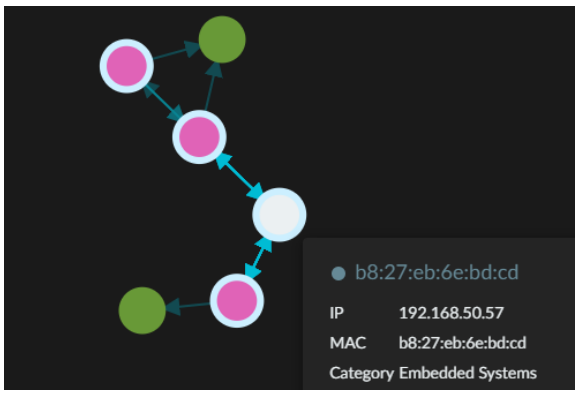
Er is tussen de beide Windows 10 computers met PLC-simulator een Modbus verbinding opgezet, vervolgens is gekeken of dit protocol gevonden is.

Name	Risk Level	Used by Devices	Profiles
ms-store	1	2	PC-Windows
modbus-base	2	2	PC-Windows
netbios-dg	2	2	PC-Windows
netbios-ns	2	2	PC-Windows
ms-update	4	2	PC-Windows
soap	2	2	PC-Windows
modbus-read-holding-registers	2	2	PC-Windows
ms-teams	3	2	PC-Windows

Figuur 22, Testrapport - Industriële protocollen

T05: Verbindingen tussen assets worden herkend.

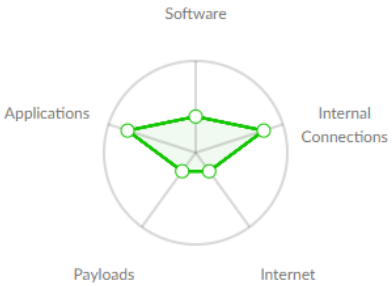
Er is een SSH-verbinding tussen een Windows 10 systeem en de Raspberry Pi en een Modbus verbinding tussen de beide Windows 10 systemen. Onderstaand netwerkmodel wordt herkend door Palo Alto IoT Security.

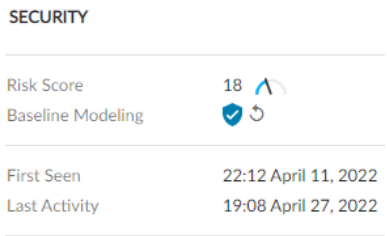


Figuur 23, Testrapport - Verbindingen tussen assets

T06: De oplossing herkent verdacht netwerkverkeer op industriële apparatuur

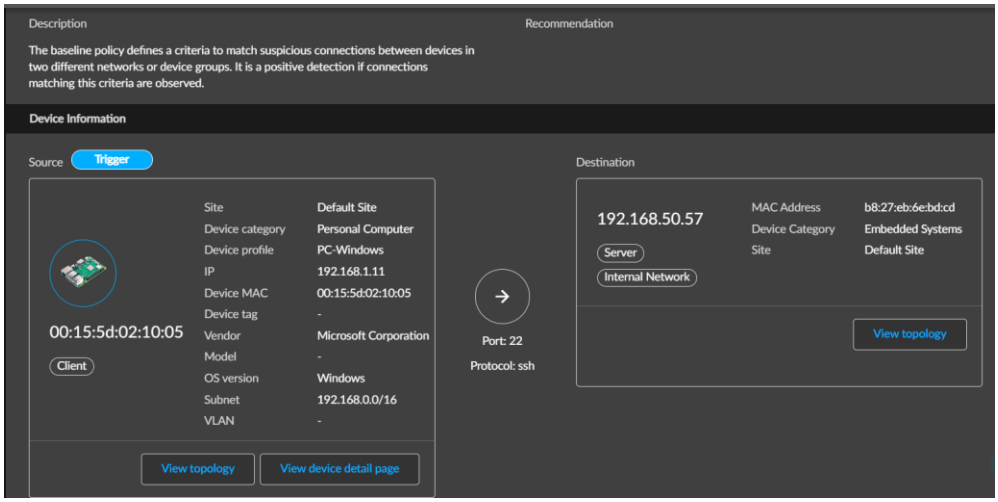
De oplossing heeft ruime tijd gekregen om een baseline op te bouwen van het netwerkverkeer van een Raspberry Pi. De volgende baseline is ontstaan, op basis van dit model moet verdacht verkeer herkent kunnen worden.





Figuur 24, Testrapport - Baseline

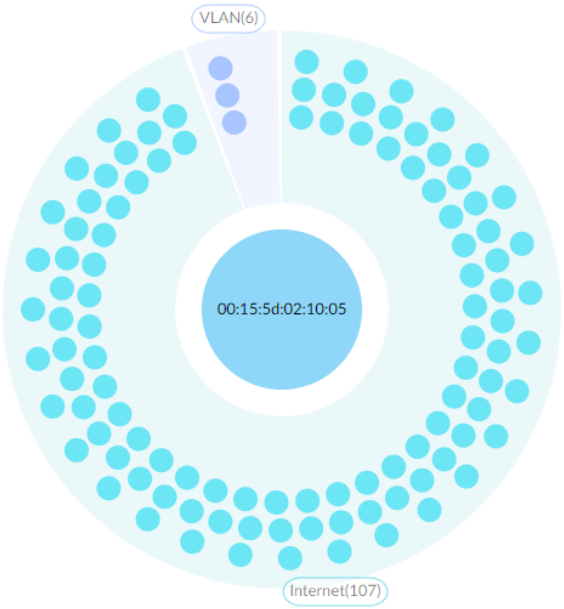
Vervolgens is vanaf het kantoornetwerk een verbinding met SSH opgezet, deze verbinding past niet binnen de baseline en geeft daarom een alert.



Figuur 25, Testrapport - Alerts

T07: Er kan een sessie op laag 2 van het netwerk gevolgd worden.

Doordat er een Span/Mirror interface aan de virtual switch gekoppeld is kan er verkeer op het lokale VLAN (tussen 2 virtuele machines) worden gevolgd, dit verkeer gaat niet via de Firewall.



Figuur 26, Testrapport - Verbindingen op lokaal netwerk

T08: Kwetsbaarheden worden verwezen naar een CVE-database.

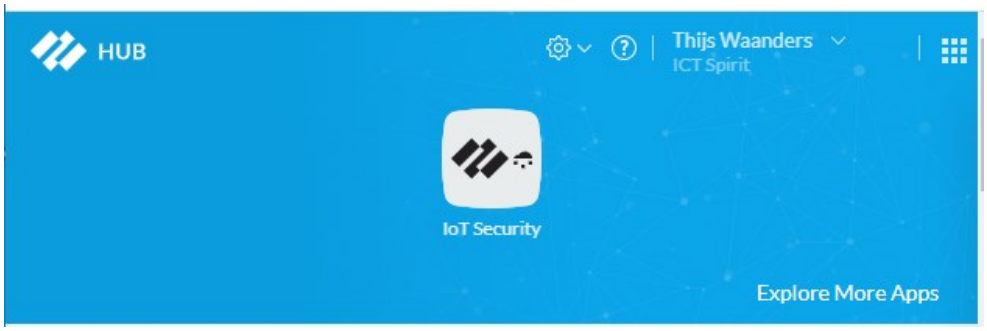
Een deel van de kwetsbaarheden waarop gescand wordt verwijst direct naar een CVE nummer.

Severity	Vulnerabilities
	TLS 1.0/1.1 Usage
	End-of-life Windows OS
	CVE-2018-1283
	CVE-2017-9788
	CVE-2017-3167

Figuur 27, Testrapport - CVE database

T09: De oplossing bevat een centraal management dashboard.

Wanneer wordt ingelogd op de PaloAlto hub kan worden gekozen naar welke omgeving er moet worden ingelogd, dit is mogelijk vanaf het internet gebruikmakend van een SSO gebruikersnaam en wachtwoord.



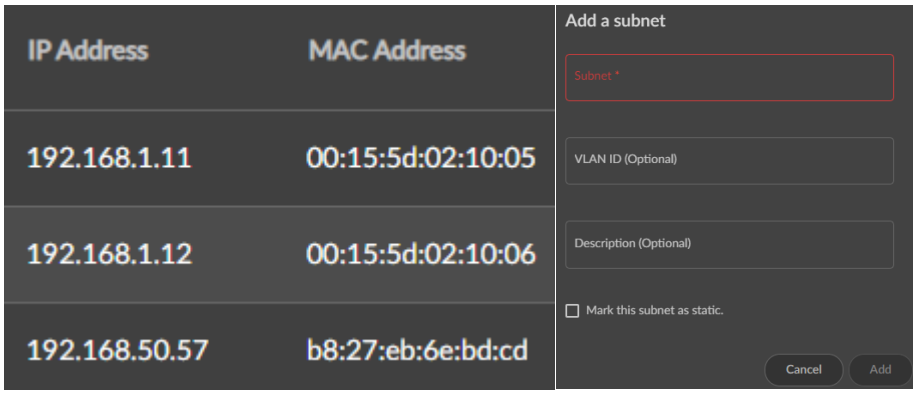
Figuur 28, Testrapport - Multi-tenant scherm

T10: De oplossing kan door een MSP-partner besteld worden

Het volgende is op de publieke website vermeld: “By partnering with Palo Alto Networks, MSSPs can deliver differentiated security services to market segments of all sizes and in every industry, broadening their footprint into new markets.” (Palo Alto, 2022)

T11: De oplossing scant meerdere VLANs vanuit één appliance.

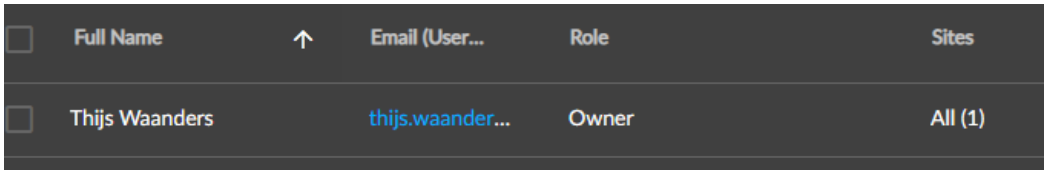
Zoals in de inventory weergegeven zijn niet alle apparaten in hetzelfde subnet geplaatst. In de configuratie is te kiezen welke subnetten in de monitoring zichtbaar moeten zijn.



Figuur 29, Testrapport - VLAN overzicht

T12: Er kan een gebruiker met afwijkende rechten worden aangemaakt.

Het is mogelijk om gebruikers met verschillende rollen aan te maken. Bij grotere omgevingen kan tevens worden aangegeven tot welke fysieke locaties toegang wordt verkregen.



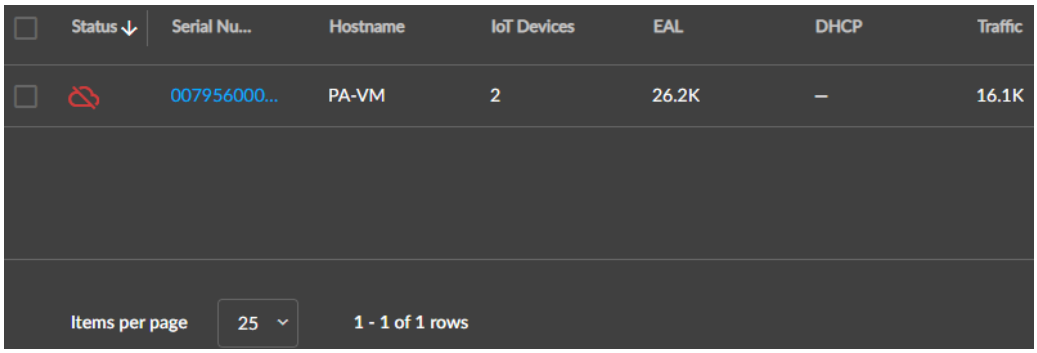
Figuur 30, Testrapport - Gebruikers

T13: De status van de oplossing wordt weergegeven in Logic Dashboards.

Het is niet mogelijk om de status van de SaaS-dienst weer te geven in Logic Monitoring. Dit valt onder de verantwoordelijkheid van de leverancier. De door PCI beheerde scanners zijn bestaande Palo Alto firewalls. Hiervan kan de status wel worden gecontroleerd in Logic Dashboards. Omdat deze momenteel al aan Logic gekoppeld zijn.

T14: Het is mogelijk om later sensoren toe te voegen

Het is mogelijk om firewalls aan dezelfde omgeving te koppelen indien deze firewalls over de IoT-security licentie beschikken.



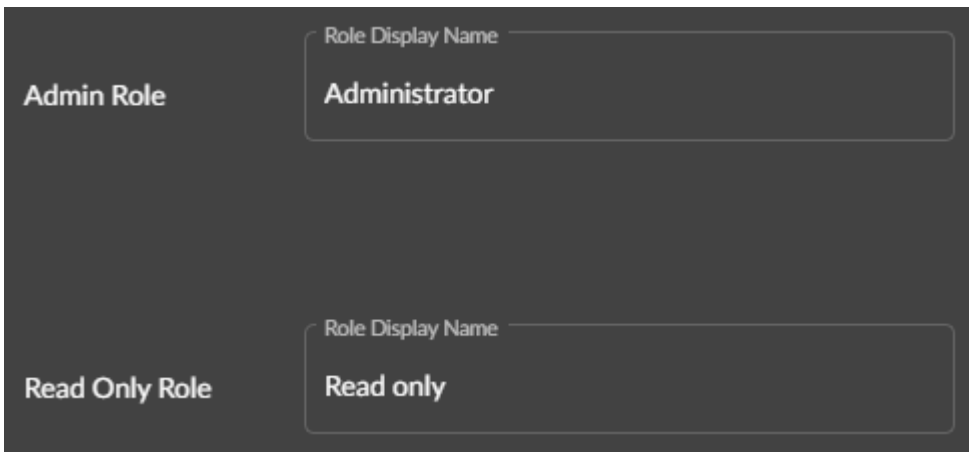
Figuur 31, Testrapport - Sensoren

T15: De oplossing werkt in combinatie met de Palo Alto Next Generation Firewall

Zoals in het prototype ontwerp is aangegeven is de oplossing geplaatst in een netwerk welke door Palo Alto Next Generation Firewall wordt beveiligd. De oplossing is tevens afkomstig van deze leverancier.

T16: Klanten kunnen zelfstandig de inventory bekijken zonder een aanpassing te doen.

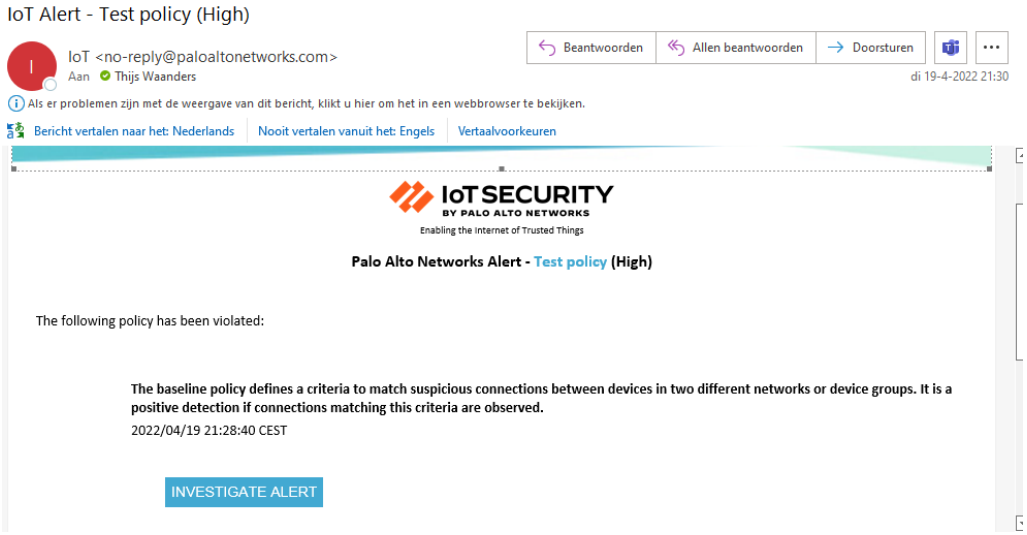
Er kan een gebruiker worden aangemaakt met een read-only rol. Deze gebruikers kunnen geen aanpassingen doen.



Figuur 32, Testrapport - Gebruikersrollen

T17: Er kan automatisch een melding in Connectwise worden gemaakt.

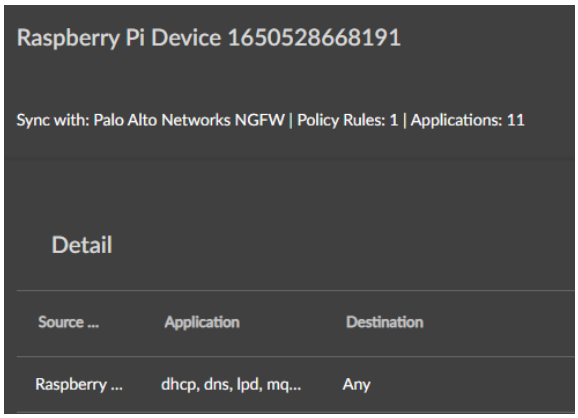
Van een alert wordt automatisch een email gestuurd op het moment dat de alert is geclassificeerd als prioriteit hoog.



Figuur 33, Testrapport - Email melding

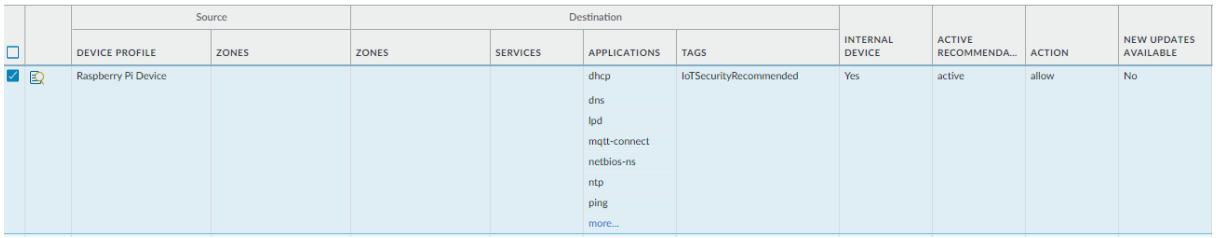
T18: De oplossing is gekoppeld aan de firewall.

In de IoT security oplossing worden de volgende policy aanbevelingen gegeven op basis van de aangeleerde baseline voor het betreffende hardware profiel:



Figuur 34, Testrapport - Aanbevelingen firewall regels

Deze aanbeveling wordt vervolgens ook in de firewall getoond:



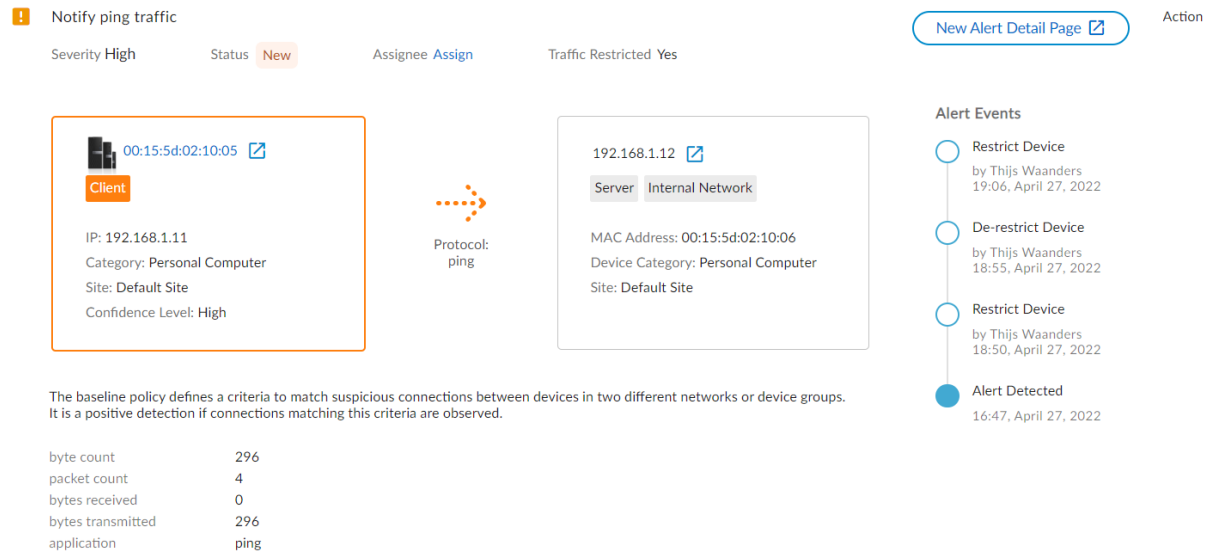
Figuur 35, Testrapport - Koppeling firewall

Nadat deze is gecontroleerd en akkoord bevonden kan de aanbeveling in één klik in een firewall regel worden omgezet:

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
1	Taprule	none	universal	tapzone	any	any	any	tapzone	any	any	any	any	Allow
2	Raspberry Pi Device	Raspberry Pi De... IoTSecurityReco...	universal	any	any	any	Raspberry-P...	any	any	any	dhcp dns lpd mqtt-connect netbios-ns ntp ping more...	application-...	Allow

Figuur 36, Testrapport - Regels in firewall

Daarnaast beschikt de oplossing ook over een koppeling voor het kunnen isoleren van apparaten indien een alert hier aanleiding toe geeft.

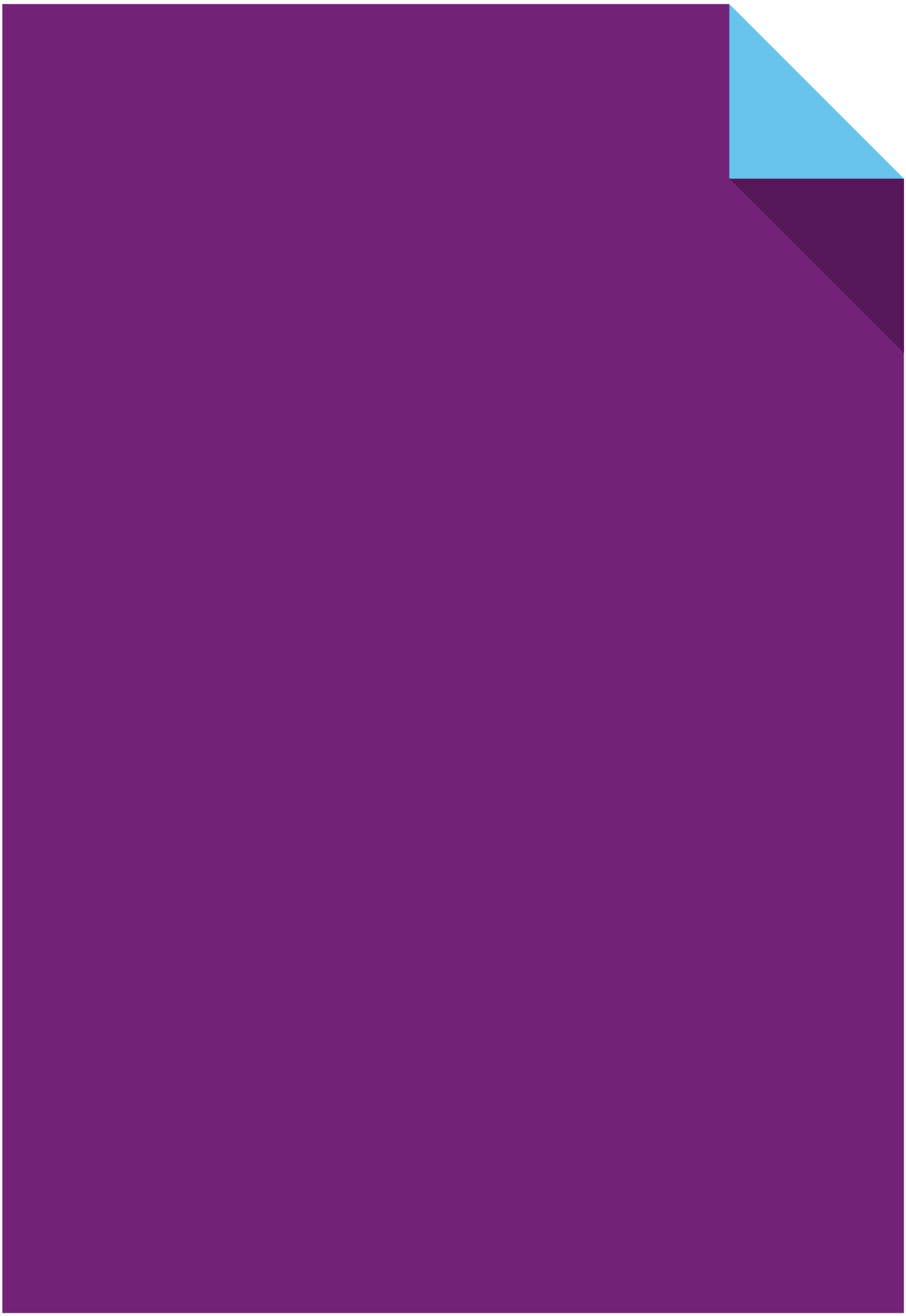


Figuur 37, Testrapport - Alert details

Als een alert is gegenereerd en is gecontroleerd door de medewerker van PCI kan indien gewenst vanuit de IoT security applicatie al het verkeer van en naar het betreffende apparaat geblokkeerd worden.

RECEIVE TIME	SOURCE DEVICE CATEGORY	SOURCE DEVICE HOST	NAT SOURCE PORT	SOURCE DEVICE PROFILE	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
04/27 19:14:38	Restricted	00:15:5d:02:10:...	0	PC-Windows	drop	Internal	External	192.168.1.11	8.8.8.8	53	not-applicable	deny	Restrict IoT network access
04/27 19:14:33	Restricted	00:15:5d:02:10:...	0	PC-Windows	drop	Internal	External	192.168.1.11	8.8.8.8	53	not-applicable	deny	Restrict IoT network access
04/27 19:14:33	Restricted	00:15:5d:02:10:...	0	PC-Windows	drop	Internal	External	192.168.1.11	8.8.8.8	53	not-applicable	deny	Restrict IoT network access

Figuur 38, Testrapport - Resultaat restrict traffic



www.pci nederland.nl