TLP:CLEAR

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2025 P11921 – 23 maart 2025

Cryptographic Asset Discovery and Inventory

Een marktverkenning en fit-gap-analyse

Auteurs
Thom Sijpesteijn
Maaike van Leuken
Frederik Kerling

Rubricering verslag
TNO Publiek

Aantal pagina's
64

Aantal bijlagen
2

Gefinancierd door
CIO Rijk
Nationaal Cyber Security Centrum
Ministerie van Economische Zaken

TLP:CLEAR

Managementsamenvatting

Dit document is het resultaat van een onderzoek naar commercieel beschikbare tooling voor Cryptographic Asset Discovery & Inventory (CADI). Het doel van CADI is het creëren van een overzicht van alle cryptografie die binnen een organisatie gebruikt wordt. Zo'n overzicht is belangrijk vanuit veiligheidsoverwegingen en in het bijzonder met het oog op de aanstaande migratie naar post-quantum cryptografie (PQC). Er is input verzameld via een workshop met technische en beleidsmatige stakeholders van de overheid, alsmede middels desk research en gestructureerde interviews met leveranciers van producten. Op basis hiervan zijn er eisen opgesteld voor een *minimum viable product* (MVP) en een *ideale CADI-tool*. Dit onderzoek is gefinancierd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), het Nationaal Cyber Security Centrum (NCSC) en het Ministerie van Economische Zaken (EZK). De resultaten van dit onderzoek zijn zodoende relevant voor overheidspartijen, maar kunnen ook inzichten bieden voor bredere publieke en private organisaties.

Tijdens het onderzoek is gebleken dat er veel verschillen zitten tussen de verschillende CADI-tools, zowel op technisch niveau als in volwassenheid van het product. Het ideaal voor IT-omgevingen wordt nog niet helemaal bereikt, maar enkele tools komen wel in de buurt. We concluderen dat de inzet van CADI-tooling een afweging is waarbij grotere nauwkeurigheid schaalt met grotere inspanning. Ook zijn bestaande *fullstack*-oplossingen voor CADI veelal prijzig en komen ze niet uit Europa. Het beheren van IT-assets in brede zin wordt in veel organisaties reeds als complex gezien, dus is het zaak dat CADI goed aansluit bij bestaande oplossingen. Hiervan zijn de leveranciers van CADI-tooling zich bewust en er wordt gewerkt aan integratie met bestaande, generiekere cybersecurity- en assetmanagementproducten.

Daarnaast zien we dat CADI-tooling op het vlak van *operational technology* (OT) minder ver gevorderd is dan op het vlak van *information technology* (IT) . Zo is er bijvoorbeeld weinig bestaande OT-tooling om op aan te haken en geven sommige leveranciers aan geen interesse te hebben om hun producten uit te breiden met support voor OT. OT speelt echter een steeds belangrijkere rol binnen de overheid, voor bijvoorbeeld vitale infrastructuren, en wordt ook steeds meer gekoppeld aan het internet. Hierdoor achten wij CADI wel als zeer relevant voor OT. We adviseren dan ook om op OT-vlak in CADI meer samen te gaan werken met andere stakeholders en werk te maken van de wet- en regelgeving rondom cryptografische inventarisatie binnen de overheid. Zie ook Strategische Kennisagenda BZK en VRO 2025-2030.

Om de prestaties van verschillende CADI-tools in concrete zin te vergelijken moet men de tools in een gecontroleerde omgeving testen. We zien hier kansen voor de betrokken overheidspartijen: wellicht kunnen deze hun kennis en inzicht in dit onderwerp vergroten door te faciliteren in het bepalen van een *ground truth,* die als baseline kan dienen voor het meten van kwaliteit van verschillende CADI-producten. Daarnaast kunnen ze hun kennis- en leiderspositie rondom CADI versterken met slimme overheidsaanbestedingen rondom CADI-tooling, PQC-migratie, en diensten daaromtrent.

Ten slotte adviseren wij om niet te wachten op de ideale tool of andermans best-practices rondom CADI. Het is zaak om zo snel mogelijk van start te gaan met het bouwen van kennis en kunde rondom de cryptografische assets. Daarvoor kan begonnen worden met het

winnen van informatie uit bestaande, reeds draaiende tools. Daarnaast kunnen de overheidspartijen middels invloed en aanbestedingen (markt)partijen stimuleren om de aanwezige tekortkomingen, *gaps*, aan te vullen.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

Het is belangrijk dat een organisatie een goed beeld heeft van alle cryptografie die ze gebruikt: welke algoritmes (en bijbehorende parameters) worden met welk doel gebruikt, waar, en waarvoor? Deze informatie kan gepresenteerd worden in een zogenaamde *cryptografische inventaris*. Het nauwgezet bijhouden van een cryptografische inventaris kan een organisatie meerdere voordelen bieden, zoals:

- *Voorkomen van datalekken en ongeautoriseerde toegang:* het gebruik van gedateerde, uitgefaseerde of anderszins ongeschikte cryptografie kan leiden tot datalekken en/of ongeautoriseerde toegang. Door goed inzicht te hebben in de gebruikte cryptografie kan een organisatie ervoor zorgen dat het risico hierop wordt geminimaliseerd. Daarnaast kan er met een goede cryptografische inventaris sneller worden gereageerd als er iets misgaat met de cryptografie. De incident response-tijden worden zo verminderd, wat de potentiële impact van een cryptografisch probleem beperkt.
- *Compliance:* organisaties hanteren en/of implementeren beleid rondom het gebruik van cryptografie. Hierbij hoort vaak een crypto-strategie of -beleid, deels op basis van bestaande wet- of regelgeving. Met een cryptografische inventaris kan aangetoond worden of een organisatie voldoet aan beleid en wet- en regelgeving.
- *Planning van de migratie naar PQC:* inmiddels zijn er de eerste standaarden voor post-quantumcryptografie (PQC): cryptografie die bestand is tegen de quantumcomputer. De migratie naar deze nieuwe cryptografie is echter een complexe onderneming. Hiervoor moet een organisatie weten welke systemen en processen binnen een organisatie met welke mate kwetsbaar zijn voor eventuele quantumaanvallen. Hiervoor is een cryptografische inventaris met het juiste inzicht noodzakelijk.

Het opstellen van een cryptografische inventaris is dus een maatregel die het algemene security-niveau van een organisatie naar een hoger niveau kan tillen. We noemen deze onderneming ook wel *Cryptographic Asset Discovery and Inventarisation* (CADI).

CADI is een uitdagende taak. Cryptografie is in moderne IT-infrastructuren namelijk ontzettend wijdverspreid over allerlei systemen, bibliotheken, en applicaties. Veel organisaties hebben geen idee welke cryptografie ze waar gebruiken en ook niet welke cryptografie ingezet wordt door externe diensten of afhankelijkheden. Daarnaast wordt cryptografie op verschillende lagen gebruikt: zowel op hardware- als softwareniveau, maar ook in de netwerklaag. Bovendien zijn er in moderne organisaties vaak legacy-systemen en onderlinge afhankelijkheden tussen de verschillende IT- en OT-assets die CADI nog lastiger maken.

1.2 Doelstelling

In dit rapport doen we verslag van de inzichten en bevindingen uit het onderzoek naar reeds beschikbare CADI-tooling. We leveren daarmee een bijdrage aan de afwegingsprocessen die organisaties hebben rondom het gebruik van dergelijke tooling. De primaire doelgroep voor dit rapport wordt gevormd door (stakeholders binnen) overheidsorganisaties. Reden daartoe is de trekkende rol die de overheid inneemt op het vlak van PQC, alsmede het feit dat

overheidsinstanties een complexe en uitgebreide, zelf beheerde IT-infrastructuur hebben. De opgedane inzichten zullen echter ook relevant zijn voor organisaties buiten de publieke sector, vooral als het grote organisaties met zelf-ontwikkelde applicaties betreft.

De onderzoeksvraag is drieledig:

1. Hoe zien een *minimum viable product* (MVP) en een ideale tool voor CADI eruit en aan welke eisen voldoen ze?
2. Wat is de huidige status van de CADI-tools die al commercieel verkrijgbaar zijn en hoe verhouden deze zich tot het ideaal en de MVP?
3. Hoe is het gat tussen de MVP en een ideale CADI tool te overbruggen?

In de volgende hoofdstukken zullen we deze vragen nader toelichten. Daarnaast definiëren we concrete vervolgstappen en nieuwe onderzoeksvragen die uit het huidige onderzoek voortvloeien.

1.3 Totstandkoming van dit rapport

Dit onderzoek is gefinancierd door CIO Rijk, het Nationaal Cyber Security Centrum (NCSC-NL), en het ministerie van Economische Zaken (EZ). Het onderzoek is uitgevoerd door TNO. Deze partijen werken op verschillende manieren, samen en zelfstandig, aan de voorbereidingen en uitvoering van migraties naar quantumveilige cryptografie. Zij werken ook samen in Quantumveilige Cryptografie (QvC) Rijk.

Ook is er in samenwerking met de partijen een workshop georganiseerd met andere Nederlandse (particuliere) organisaties over het gebruik en de noodzaak van CADI tooling. Deze organisaties hadden elk een grootschalige aanwezigheid van gevarieerde IT- en/of OT-systemen.

1.4 Vertrouwelijkheid en volledigheid van leveranciers

Dit rapport bevat vertrouwelijke informatie (Bijlagen 2, 3, en 4) over leveranciers, die alleen inzichtelijk is voor de eerder genoemde overheidspartijen. Mogelijk is u een versie bekomen zonder deze bijlagen. Voor vragen over welke specifieke partijen zijn geraadpleegd verwijzen we u dan ook naar de betrokken overheidspartijen.

We onderkennen dat niet alle mogelijke leveranciers zijn geïnterviewd. Dit heeft verschillende redenen. Soms kwam het contact niet of lastig tot stand waardoor een interview niet meer mogelijk was. Soms heeft de leverancier aangegeven niet geïnterviewd te willen worden. In een enkel geval hebben we ervoor gekozen een partij niet te interviewen omdat er al meerdere partijen van dezelfde soort waren geïnterviewd.

Als we een partij niet hebben geïnterviewd, zegt dit dus niets over de kwaliteit van hun producten of diensten. Het feit dat een partij niet in dit rapport genoemd wordt, moet niet gebruikt worden als argument om geen diensten of producten van deze partij af te nemen.

1.5 Terminologie

Over het algemeen maken we in dit document gebruik van terminologie die standaard is in de IT. Voor de volledigheid benoemen we hieronder enkele vaktermen.

Cryptografische assets – Een parapluterm voor alle componenten of elementen van een systeem die met cryptografie te maken hebben. Dit omvat zaken zoals algoritmes of sleutels, maar ook protocollen of versleutelde gegevens die van cryptografie gebruikmaken.

Cryptographic Asset Discovery and Inventory (CADI) – Het inventariseren van cryptografische assets binnen een van tevoren vastgelegde scope. Dit omvat zowel het zoeken (scannen) naar cryptografische assets als het overzichtelijk opslaan/presenteren daarvan. Bij gebrek aan standaardterminologie is CADI als term door TNO geïntroduceerd omdat dit de lading ons inziens het beste dekt. Er zijn in de markt tal van verschillende termen die op dit fenomeen duiden of de nadruk net anders leggen, zoals *cryptographic scanning, cryptographic discovery, cryptographic inventory* en *cryptographic asset discovery*.

Endpoint – Een endpoint is een fysiek of virtueel apparaat dat verbinding maakt met een netwerk, waaronder: (virtuele) desktop- en laptopcomputers en andere werkplekken, mobiele apparaten, smartphones, tablets, (virtuele) servers, en IoT-apparaten (*Internet-of-Things*).

Agent – Speciaal toegewijde software die op een endpoint draait in functie van andere software (of users). In de huidige context worden agents ingezet om informatie over cryptografische assets op te halen (en naar een centrale entiteit te versturen).

2 Methodologie

Voor het uitvoeren van dit onderzoek naar CADI-tooling is er op verschillende manieren input verzameld. Allereerst is er met *desk research* een eerste verkenning gedaan naar bestaande literatuur in dit domein. Ook is er op kleinere schaal gebrainstormd met experts over CADI en hoe de tool eruit zou kunnen zien. Daarnaast is er een workshop georganiseerd met experts en stakeholders uit zowel de private als de publieke sector, om inzichten op te doen over een ideale CADI-tool. Ten slotte zijn er interviews afgenomen met commerciële partijen die zich op CADI richten of erin geïnteresseerd zijn. We lichten deze drie methodologieën hieronder nader toe.

2.1 Literatuuronderzoek

Als eerste stap in dit project is er door middel van *desk research* onderzoek gedaan naar bestaande literatuur over CADI. Hierbij viel meteen op dat er geen academische literatuur over het onderwerp lijkt te bestaan, vermoedelijk omdat CADI pas relatief recent aandacht krijgt. Ook is er, vermoedelijk tevens ten gevolge van het feit dat dit een jong vakgebied is, weinig consistentie in het taalgebruik: verschillende partijen hanteren verschillende termen door elkaar. Tijdens onze desk research is er dan ook op een grote verscheidenheid aan termen gezocht, zie Bijlage 5 – Zoektermen.

Er zijn wel verschillende blogs over dit onderwerp te vinden. Deze blogs zijn vaak geschreven door leveranciers van CADI-tooling. Dergelijke blogs geven zeker inzichten, maar er dient rekening mee gehouden te worden dat de insteek en beschrijving door commerciële belangen gekleurd kan zijn. De meeste informatie beschikbaar online over de CADI-producten is niet van technische aard – het gaat (bijna) niet in op de technische werking of eigenschappen van de producten. Dit toont ook de relatief lage volwassenheid in het domein van CADI-oplossingen en de adoptie ervan.

Objectiever van inslag zijn enkele documenten van het Amerikaanse National Institute for Standards and Technology (NIST). NIST is reeds bezig met het opstellen van documenten en adviezen rondom CADI-oplossingen, maar dit project verkeert nog in een relatief vroeg stadium[1].

Op basis van dit literatuuronderzoek hebben we een aantal inzichten, eisen en vragen opgesteld. Bovendien hebben we een shortlist opgesteld van CADI-leveranciers met wie een interview interessant zou zijn. Een soortgelijke shortlist is opgesteld voor leveranciers van bredere IT-producten, voor wie de ontwikkeling van of integratie met CADI-oplossingen interessant zou zijn.

2.2 Brainstorms met experts

Op 18 september 2024 hebben Oscar Koeroo (VWS), Dion Koeze (NCSC) en Maaike van Leuken (TNO) een brainstormsessie gehad over hoe een ideale CADI-tool in elkaar zou steken en met welke vragen we de gewenste informatie van de CADI-leveranciers konden uitvragen.

[1] Migration to Post-Quantum Cryptography | NCCoE i.h.b. NIST SP 1800-38B

Om de ideale tool en MVP te kunnen schetsen, was het belangrijk om in kaart te brengen wat onze aanpak zou zijn om een CADI-oplossing te maken. We zijn gekomen tot een algemene gewenste opzet, waarbij eerst de netwerkinfrastructuur in kaart gebracht moet worden, vervolgens met netwerkdetectie inzicht kan worden verkregen in interessante endpoints op het netwerk, waarna deze endpoints met behulp van agents gescand worden op welke (crypto)library's ze aanroepen. Dit zou al een goede basis vormen voor een MVP. Om vervolgens te weten welke cryptografische protocollen en primitieven daadwerkelijk in runtime aangeroepen worden, zal een dynamische tracing met behulp van een agent uitgevoerd moeten worden. Deze gelaagdheid, waarbij kleine stapjes ondernomen kunnen worden om meer nauwkeurigheid te krijgen, ligt ten grondslag aan het model beschreven in sectie 4.3.2. Oscar gaf vanuit zijn operationele kennis aan dat hij heel tevreden zou zijn als 80% van de cryptografische assets gevonden kunnen worden.

Daarnaast is er kort besproken hoe we de CADI-leveranciers het beste scherp kunnen bevragen. Daartoe gaf Oscar een aanzet tot een use case beschrijving, aan de hand van welke wij de interviews hebben gestructureerd. Oscar heeft ook een blik geworpen op onze vragenlijst en daar twee vragen aan toegevoegd.

2.3 Workshop

Dit onderzoek draagt bij aan de kennis rondom CADI binnen Nederland. In het bijzonder is de insteek dat Nederlandse overheidsinstanties (én eventueel private partijen) concrete uitkomsten van dit onderzoek kunnen meenemen in hun overwegingen. Om deze link met overheid en industrie te waarborgen is er in dit project een workshop georganiseerd, die op 23 september 2024 heeft plaatsgevonden.

Het doel van deze workshop was om met de relevante stakeholders na te gaan aan welke eisen een CADI-tool moet voldoen, wil deze succesvol in de verschillende IT-infrastructuren worden ingezet. De workshop, die in totaal zo'n twee uur besloeg, bestond uit twee delen. In het eerste deel werd er een serie vragen over praktische eisen aan CADI-tooling gesteld. Deze vragen/eisen waren opgesteld op basis van het literatuuronderzoek. Per vraag zijn de antwoorden van de deelnemers verzameld en zijn eventuele opvallende overeenkomsten of verschillen bediscussieerd. Voor het tweede deel van de workshop werden de deelnemers in groepen verdeeld en werd er in een losser format gesproken over CADI en de bijbehorende uitdagingen.

Een uitgebreider verslag van de workshop is te vinden in de bijlage. Binnen het project zijn de uitkomsten van deze workshop bovendien gebruikt om gerichter vragen te kunnen stellen tijdens de interviews met leveranciers.

2.4 Interviews

In het kader van dit onderzoek zijn er een aantal interviews afgenomen met bedrijven. Om een breder beeld van het ecosysteem te kunnen schetsen zijn er twee verschillende soorten bedrijven geïnterviewd. Ten eerste is er met een drietal bedrijven gesproken die tooling aanbieden die specifiek op CADI gericht is. Daarnaast is er een vijftal leveranciers van andere, gerelateerde cybersecurity-tooling geïnterviewd, om uit te zoeken of CADI bij hen op de radar staat en hoe ze er tegenaan kijken.

2.4.1 Interviews met CADI-leveranciers

In de markt worden er al verschillende CADI-tools aangeboden die door commerciële entiteiten zijn ontwikkeld. Binnen dit onderzoek zijn een aantal dergelijke leveranciers van CADI-tools benaderd voor een interview, met als doel om de kwaliteit van de tool te achterhalen. Uiteindelijk zijn er drie interviews gehouden. Bij deze interviews was het de insteek om kritische vragen te stellen op basis van de hierboven omschreven desk research, workshop en brainstorms.

In Hoofdstuk 5 beschrijven we de belangrijkste conclusies van deze interviews. De precieze interviewvragen en samenvatting van de interviews zijn te vinden in Bijlage 3 – Samenvatting interviews met CADI-leveranciers.

2.4.2 Interviews met generieke security-leveranciers

Naast leveranciers van losstaande CADI-producten zijn er ook een vijftal interviews geweest met marktpartijen die andere cybersecurity-tooling leveren. Het idee is dat het voor een dergelijke partij misschien ook interessant is om de bestaande productlijn uit te breiden met CADI-tooling. In het bijzonder zou daarbij wellicht gebruik gemaakt kunnen worden van de bestaande tooling en/of infrastructuur. Bovendien gaven veel deelnemers in onze workshop (zie hierboven) aan dat integratie met bestaande tooling voor CADI-tooling zeer wenselijk is, om beheer overzichtelijk te houden.

Het doel van deze interviews was dan ook om te toetsen in hoeverre de betreffende leveranciers interesse hebben in de integratie met CADI-tooling, dan wel ambitie hebben om zelf een tool in dit domein te ontwikkelen. Omdat deze partijen op dit moment nog geen CADI-tool hebben, was de insteek van de interviews meer verkennend, zoekend en constructief.

In hoofdstuk 6 beschrijven we de belangrijkste conclusies van deze interviews. De interviewvragen en samenvatting van de interviews zijn te vinden in Bijlage 4 – Samenvatting Interviews met generieke security-leveranciers.

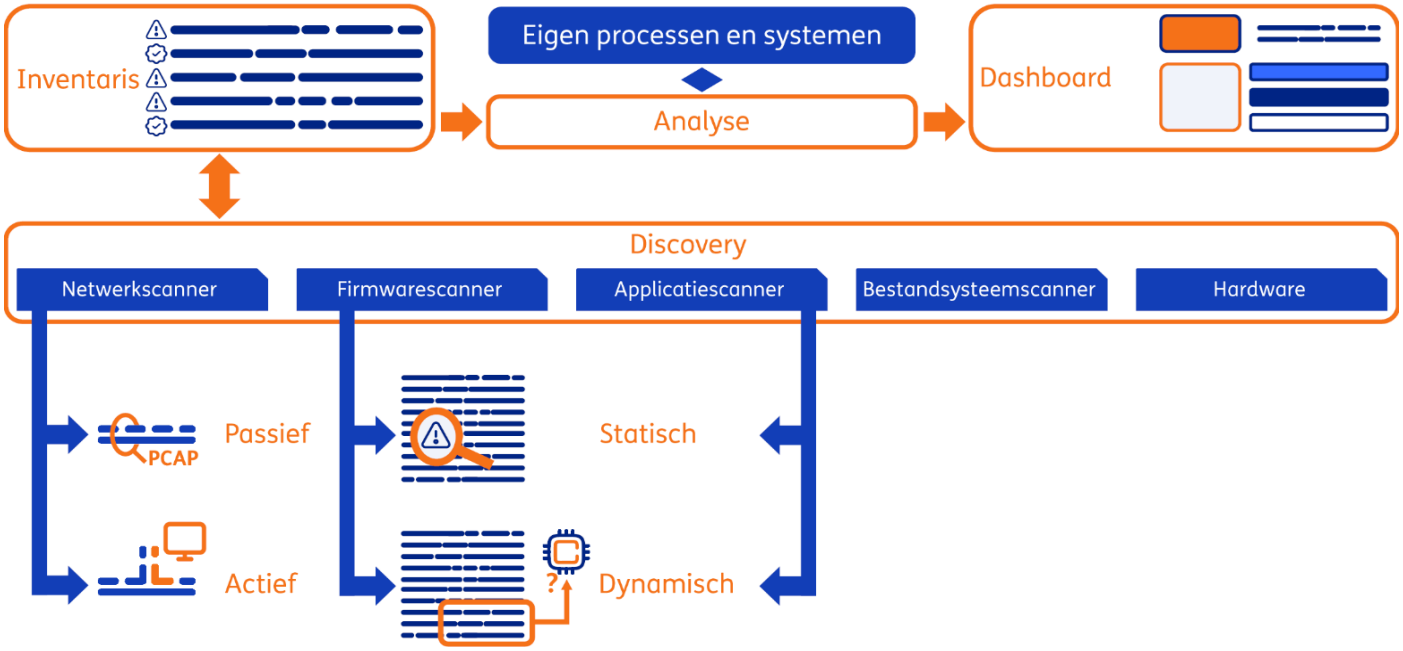
3 Technische achtergrond

3.1 Soorten scanners

Voor het opstellen van een cryptografische inventaris binnen een organisatie moet de IT-infrastructuur gescand worden. Hiervoor bestaan, zoals we in dit rapport beschrijven, verschillende tools. In moderne IT-infrastructuren wordt cryptografie echter op allerlei verschillende plaatsen gebruikt en niet al het gebruik van cryptografie is op dezelfde manier te detecteren.

In de praktijk gebruiken CADI-tools daarom onder de motorkap verschillende 'subtools', die elk een andere laag of een andere manier van scannen hanteren. We noemen deze subtools ook wel *puntoplossingen*. De output van zulke puntoplossingen kan worden geaggregeerd, geanalyseerd en eventueel in een dashboard worden gepresenteerd, zie Figuur 1. In de praktijk komt het voor dat commerciële CADI-tools één of meer opensource oplossingen die ze met eigen oplossingen combineren tot een tool met bredere dekking.

In deze sectie lichten we toe welke verschillende soorten puntoplossingen er zijn. In het bijzonder zijn er verschillende niveaus van diepgang mogelijk: sommige scans zijn nauwkeuriger dan andere, maar over het algemeen vereisen die ook meer inspanning of zijn ze invasiever. Zie hiervoor ook het model in sectie 4.3.



Figuur 1. Schematische weergave van een CADI-tool en haar subtools in de verschillende lagen. De CADI-tooling wint informatie uit andere systemen (e.g. cybersecuritymanagement-tooling), en kan ook informatie leveren naar bestaande systemen, (e.g. een incident naar een SIEM-tool).

3.1.1 Verschillende lagen

Op basis van desk research hebben we een aantal lagen onderscheiden, die vervolgens tijdens de interviews met CADI-leveranciers gevalideerd zijn. Het gaat om:

Netwerk

Netwerkscanners richten zich op *data in transit*: gegevens die over een verbinding tussen verschillende computers of endpoints gedeeld worden. Deze netwerkverbindingen moeten geanalyseerd worden om te achterhalen welke cryptografie er gebruikt en ondersteund wordt. Dit omvat bijvoorbeeld TLS- en SSH-verkeer, zowel binnen een organisatie als naar buiten toe. Aangezien het meeste verkeer versleuteld is, kan de data inhoudelijk niet geanalyseerd worden op aanwezigheid van cryptografische assets.

Applicaties en library's

Applicaties die op een endpoint draaien maken ook vaak gebruik van cryptografie, bijvoorbeeld door bepaalde cryptografische library's aan te roepen. Om na te gaan welke cryptografie dit is, moeten alle applicaties en library's in een systeem dus ook geanalyseerd worden.

Firmware

Niet alleen de applicaties en library's die óp een systeem draaien gebruiken cryptografie, maar ook de firmware van het systeem zelf. Zo wordt cryptografie bijvoorbeeld gebruikt om veilig te kunnen updaten. Ook deze moet dus gescand worden.

Bestandssystemen

Waar netwerkscanners zich richten op *data in transit*, richten scanners voor bestandssystemen zich op *data at rest*. Daarmee doelen we op (gevoelige) gegevens die de organisatie in versleutelde vorm heeft opgeslagen. Een cryptografische inventaris dient te benoemen hoe deze gegevens precies versleuteld zijn. Hiervoor moeten de bestandssystemen van een organisatie gescand worden, inclusief eventuele databases.

Hardware

Voor een volledig overzicht van alle cryptografie moet ook de hardware meegenomen worden. Voor het achterhalen van cryptografie die in hardware wordt gebruikt zijn er verschillende opties, afhankelijk van het soort hardware en de context.

Voor smartcards (bijv. toegangspasjes voor een pand) kunnen relevante gegevens gevonden worden door eerst netwerk endpoint detectie te doen. Vervolgens kan er met netwerkverkeersanalyse naar de gebruikte cryptografie gekeken worden. De scanning valt dan in zekere zin onder de netwerklaag, maar heeft ook te maken met de hardwarelaag.

Daarnaast is er hardware in de vorm van hardware security modules (HSM's) en verwante technologieën die gezien kunnen worden als een cryptografische coprocessor. In dat geval kan er analyse worden gedaan door de firmware te scannen, waarmee het opnieuw onder een andere tak van scanning valt.

Idealiter zouden hardwareleveranciers met hun producten een *cryptographic bill of materials* (CBOM) (zie sectie 4.2.4) meegeven: dat is het meest nauwkeurige het minst ingrijpende proces.

3.1.2 Soorten scans

Scanners verschillen niet alleen van elkaar in de laag waarop ze scannen, maar ook in de manier waarop ze scannen.

Actief of passief

Binnen scanners die zich richten op netwerkverbindingen zijn in brede zin twee stromen te onderscheiden. Passieve scanners 'luisteren mee' naar dataverkeer en analyseren de pakketjes om te achterhalen welke vormen van cryptografie gebruikt worden. Het nadeel hiervan is dat een passieve scan dus ontdekt welke cryptografie er binnen een bepaalde verbinding momenteel gebruikt wordt, maar niet welke (eventuele onveilige) cryptografie er ondersteund wordt. Een actieve scan kan dit wel, omdat deze actief probeert verbinding met endpoints probeert op te zetten om zo te onderzoeken welke cryptografie er allemaal ondersteund wordt. Een actieve scan is dus nauwkeuriger, maar kost ook meer inspanning: de endpoints worden immers bestookt met verzoeken voor verbindingen.

Statisch of dynamisch
Ook in de applicatie- en library laag zien we een onderscheid tussen passieve scans (statisch) en actieve scans (dynamisch). Het onderscheid tussen statisch en dynamisch is vooral te zien in de applicatie- en librarylaag. Een statische scan analyseert de reeds beschikbare source code van een applicatie of library en kijkt welke cryptografie daarin genoemd of aangeroepen wordt. Een statische scan voert de code echter niet uit: alleen de code zelf wordt geanalyseerd. Een dynamische scan verschilt precies daarin: door (delen van) de code aan te roepen, wordt er run-time gecheckt waar eventuele kwetsbaarheden voor kunnen komen. Een dynamische scan geeft dus ook inzicht in welke libraries daadwerkelijk aangeroepen worden en worden ook configuratiebestanden mee genomen. Dit onderscheid is ook relevant als we het over firmware hebben, maar bijvoorbeeld niet als we het over bestandssystemen hebben, aangezien deze niet uitvoerbaar zijn.

Online of offline
Sommige lagen kunnen gescand worden terwijl het apparaat niet operationeel is, waarmee het dus los getest kan worden, zonder invloed op bedrijfsvoering. Denk hierbij aan het statisch analyseren van applicaties, firmware en images (bijvoorbeeld voor *operating systemen*). Het dynamisch analyseren van code kan ook offline, mits er een testomgeving is (*staging*) met de juiste configuratiebestanden en de juiste afhankelijkheden (*dependencies*). Bij de netwerklaag is het níet mogelijk om offline te scannen, omdat het juist om de samenhang gaat.

3.1.3 Inzet van agents

Een andere dimensie waarin tools van elkaar verschillen is het wel of niet inzetten van agents. Een agent is een stukje software dat op een endpoint geïnstalleerd en gedraaid wordt en vanaf daar zaken analyseert, in ons geval cryptografische assets. Agents zijn zeer flexibel en kunnen daarmee een grotere diepgang en nauwkeurigheid geven dan mogelijk is voor een scan die geen gebruik maakt van agents. Het nadeel is echter dat agents enigszins invasief zijn: er wordt dan immers software geïnstalleerd op endpoints, wat meer toegang en inspanning vereist dan een passievere aanpak. Daarnaast neemt de agent rekenkracht en geheugen op, waardoor de continuïteit van de bedrijfsprocessen in het gedrang kan komen.

De inzet van agents is in werkelijkheid meer een spectrum dan een binaire kwestie. Zo kunnen agents verschillende niveaus van privilege toegereikt krijgen en bestaan er ook tijdelijke agents. In de context van CADI is het bovendien een optie om voor de inzet van agents mee te liften op de agents die al worden ingezet door andere cybersecurity-producten.

3.2 CADI-tools

Zoals in de voorgaande sectie is toegelicht bestaan er allerlei verschillende puntoplossingen, die onderling verschillen in hun aanpak en domein. CADI-leveranciers bieden vaak een

product dat verschillende puntoplossingen combineert. De output van deze puntoplossingen wordt vervolgens gecombineerd om zo tot een inventaris te komen die verschillende lagen afdekt. Sommige van de puntoplossingen zijn ook los als open-source oplossing beschikbaar, terwijl andere ontwikkeld zijn door de CADI-leveranciers zelf.

Sommige CADI-leveranciers presenteren de gecombineerde bevindingen van de puntoplossingen ook nog in een grafisch overzicht. Als een CADI-leverancier veel puntoplossingen combineert om een overkoepelde inventaris te krijgen én deze grafisch presenteert, spreken we van een *fullstack-oplossing*.

3.3 Generieke security-tools

Generieke security-producten zoals van Generieke security-leverancier D en Generieke security-leverancier B, worden alom gebruikt om de beveiliging van organisaties te waarborgen. Het bedrijfsnetwerk wordt bijvoorbeeld gescand om connecties met malafide IP-adressen te detecteren en te blokkeren. Maar ook alle ingekochte IT-producten, -diensten en andere -assets worden bijgehouden. Dit helpt bijvoorbeeld bij de administratie van benodigde licenties, en daarmee het voorkomen van boetes en onverwachte kosten tijdens audits. Veel van deze producten zijn door de jaren heen gegroeid naar multifunctionele platforms waarbij meerdere taken binnen één product geborgen worden.

Alle grote organisaties maken gebruik maken van één of meer cybersecurity-producten. Het is daarom logisch CADI-tooling met zulke producten te kunnen integreren, zeker als er overlap in technische functionaliteit is met het bestaande product. In sectie 5.1 is ook te lezen dat dit al gebeurt. Hiertoe hebben we naast enkele CADI-leveranciers in dit onderzoek ook verschillende generieke security-leveranciers gesproken.

Hieronder schetsen we een beeld van de verschillende typen gangbare security-tools en hun onderlinge connecties. De overlap met CADI-functionaliteiten wordt beschreven in sectie 6.2.

Endpoint Detection and Response (EDR/XDR) monitort op dreigingen met het gebruik van agents op de endpoints zoals mobiele apparaten en IoT-apparaten. *Extended Detection and Response* (XDR) breidt dit uit met netwerkgedrag van endpoints en gedrag van gebruikers.

IT Asset Management (ITAM) wordt gebruikt om de levenscyclus van IT-assets te beheren. Het omvat informatie rondom welke apparaten in gebruik zijn, de MAC en IP adressen, de versienummers, serienummers, toegeschreven licenties, en toegang.

Certificate Lifecycle Management (CLM) wordt gebruikt om bij te houden welke digitale certificaten er binnen een organisatie gebruikt worden en deze te beheren.

Een **Configuration Management Database (CMDB)** houdt gegevens bij over de verschillende hardware- en softwareonderdelen van een IT-systeem en hoe deze met elkaar verbonden zijn. Dit helpt bij het effectief beheren en onderhouden van deze onderdelen. Een CMDB is typisch gekoppeld aan verschillende securitytools, zoals ITAM-tooling.

Vulnerability scanning tools onderzoeken IT-systemen op beveiligingsproblemen, zoals ontbrekende updates en verkeerde configuraties, om mogelijke dreigingen te identificeren. Deze generen dan een alert, waardoor ze opgelost kunnen worden.

Security Operations Centers (SOCs) monitoren de IT-omgeving op eventuele aanvallen en incidenten en reageren daarop. SOC-analisten krijgen via het platform alerts binnen die zijn gegenereerd met behulp van andere security tooling, zoals **een Intrusion Detection Systems (IDS)**, **vulnerability scanners** en **Security Information & Event Management (SIEM).**

IT Service Management (ITSM) refereert aan een proces en de daarbij behorende tooling die servicemeldingen afhandelt. Dit omvat vaak ook andere disciplines, zoals applicatiebeheer, technisch beheer, en andere beheerstaken met geassocieerde tooling. Er is hier enige overlap met ITAM.

Voor bovenstaande tools bestaat er een zeer gevarieerd en soms open-source aanbod. In de shortlist van sectie 6.1 is daarom uitgegaan van de tools die reeds bij verschillende ministeries in gebruik waren, of die bekend waren bij TNO en daarmee een overlap toonden met het beoogde doel.

3.4 IT en OT

Dit onderzoek heeft een brede scope in de zin dat zowel *operational technology* (OT) als *information technology* (IT) beschouwd worden. In tegenstelling tot IT is OT veelal gericht op fysieke processen in de organisatie en aansturing daarvan.

OT-systemen zijn vaak sterk beperkt in hun rekenkracht en geheugen. Voor het aansturen van fysieke processen is vaak niet zoveel rekenkracht nodig als sommige berekeningen in het IT-domein. Endpoints in een OT-omgeving hebben een specifiek doel, met bijbehorende (lage) rekenkracht, en het behalen van dat doel mag niet beïnvloed worden. In combinatie met de intellectuele eigendomsrechten van de maker op de software en hardware maakt dit het lastig of onmogelijk om agents in te zetten.
Daarnaast bestaan OT-omgevingen uit een mix van moderne en grotendeels *legacy* systemen, elk met eigen communicatieprotocollen, API's en onderliggende cryptografie. Als het dus al mogelijk is om agents in te zetten, zou er voor elk type product nieuwe code geschreven moeten worden om ermee te kunnen communiceren en vervolgens de juiste informatie eruit op te halen. Actieve detectie van cryptografische assets in OT-omgevingen is vanwege deze redenen (haast) onhaalbaar.

Een ander verschil tussen OT- en IT-omgevingen is de beveiliging ervan. OT-beveiliging loopt significant achter op IT-beveiliging, juist ook door de bovengenoemde verschillen, zoals legacy en beperkte aanpasbaarheid van de systemen. Daarnaast is de beschikbaarheid van OT-omgevingen belangrijker dan bij IT-omgevingen, waardoor beschikbaarheid de hoogste prioriteit heeft en integriteit en vertrouwelijkheid daarna pas komen. Dit betekent dat er minder security-tooling, zoals netwerk- en vulnerability-scanners worden gebruikt dan in IT-omgevingen. Ook de netwerkarchitectuur is anders. Deze is bij IT-omgevingen vaak gesegmenteerd (*air-gapped*), terwijl OT netwerken vaak niet gesegmenteerd zijn.
De nieuwe NIS2-richtlijn[2] probeert dit gat te dichten in OT-security, door te vereisen dat netwerk- en informatiesystemen proactief gescand worden op kwetsbaarheden en dat assets geïnventariseerd worden.

[2] Zie de NIS2-richtlijn, L_2022333NL.01008001.xml.

4 Ideale tool en MVP

In dit hoofdstuk beschrijven we functionele en praktische eisen voor een zogenaamd *minimum viable product* (MVP) en voor een ideale CADI-tool. In het bijzonder geven we een lijst met mogelijke eigenschappen van CADI-tooling die zijn geïdentificeerd op basis van desk research, de workshop en de interviews met CADI-leveranciers. Per eigenschap lichten we toe wat de vereiste invulling van die eigenschap is voor een MVP en hoe de eis er voor een ideale oplossing uit zou zien.

In sectie 4.3 worden de eigenschappen en de vereiste invullingen daarvan voor een MVP en een ideale tool overzichtelijk samengevat in een tabel. Ook introduceren we daar een model waarin de verschillende niveaus van CADI-tooling worden weergegeven, met oplopende nauwkeurigheid en inspanning (Figuur 2).

In hoofdstuk 5 kijken we vervolgens naar CADI-tools in de markt en hoe deze zich tot de MVP en de ideale tool verhouden.

4.1 Definitie MVP en ideale tool

In sectie 4.2 omschrijven we welke eigenschappen er voor CADI-tools bestaan en aan welke eisen een MVP en de ideale CADI-tool moeten voldoen. Eerst specificeren we wat we bedoelen met een MVP en een ideale tool.

4.1.1 Minimum viable product (MVP)

Een *minimum viable product* (MVP) hoort bij een specifieke strategie om een nieuw product te lanceren. Het idee van een MVP is dat het product nog niet perfect is, maar wel 'levensvatbaar' als product op zich. Voor gebruikers biedt een MVP al genoeg nut om de aanschaf waard te zijn; voor leveranciers biedt een MVP kans om al iets te releasen zonder dat het definitieve product met alle features en opties klaar is.

In de context van CADI beschouwen we de MVP als een product dat door een organisatie al ingezet kan worden om een eerste (deel-)indruk te krijgen van de cryptografie die binnen de organisatie gebruikt wordt, zonder dat de gewonnen inzichten later opnieuw gedaan moeten worden.

Het idee is dat de organisatie op basis van de uitkomsten van scans van de MVP eerste acties kan ondernemen, en daarmee ook meer ondersteuning vanuit management weet te halen voor een grootschaligere uitrol van CADI-tooling. Een goede MVP is zodoende niet specifiek qua welke 'laag' (zie Figuur 1), maar sluit wél goed aan bij latere stadia van een PQC-migratie en is makkelijk te migreren/in te lijven in een latere *fullstack*-oplossing.

In de workshop (zie 2.3 en Bijlage 1) werd door verschillende stakeholders aangegeven dat het prettig zou zijn om te beginnen met inventarisatie – zelfs als dit nog geen compleet beeld oplevert. Hiervoor is de MVP dus nuttig, het doorbreekt het kip-ei probleem voor de integratie van CADI-tooling.

4.1.2 Ideale tool

Met een ideale CADI-tool bedoelen we een tool die cryptografische inventarisatie *zo goed als realistisch mogelijk* uitvoert. De ideale tool is dus niet een platonisch ideaal dat alleen in een perfecte wereld kan bestaan: we kiezen er juist bewust voor om de ideale tool te interpreteren als de beste tool op het spectrum van wat technisch gezien realistisch is. De reden hiervoor is dat we in Hoofdstuk 5 enkele bestaande CADI-tools met dit ideaal (en de MVP) zullen vergelijken. Een dergelijke vergelijking heeft minder nut als het ideaalbeeld niet realistisch is.

Let op: de specificatie van een MVP en van een ideale oplossing is sterk afhankelijk van de use case. Zo kan een concrete invulling afhangen van de operationele setting, businessprocessen die draaien, eisen rondom beschikbaarheid en het risicoprofiel (dat de gewenste nauwkeurigheid van de resultaten dicteert). Daarom kiezen we ervoor om waar mogelijk een onderscheid te maken tussen IT- en OT-omgevingen, wetende dat het onderscheid verder gemaakt moet worden tijdens het uitwerken van een concrete use case.

4.2 Eigenschappen en eisen

In elk van de volgende secties wordt een andere eigenschap van CADI-tooling beschreven. Ook wordt per eigenschap toegelicht wat de vereiste invulling voor deze eigenschap is voor een MVP en voor een ideale tool.

4.2.1 Scanfrequentie

Met de scanfrequentie van een tool bedoelen we het aantal momenten waarop de scan wordt uitgevoerd. Hoe groter de scanfrequentie, des te nauwkeuriger de cryptografische inventaris zal zijn, en dus hoe eerder eventuele abnormaliteiten of kwetsbaarheden worden geïdentificeerd.

Let op: de onderstaande overwegingen geven slechts een richtlijn, waar in sommige gevallen van afgeweken kan worden. Zo kan de frequentie tijdelijk opgeschroefd worden als er grote veranderingen in het systeem worden doorgevoerd. Daarnaast is een volledige scan van het systeem niet altijd nodig: zoals elders beschreven bestaat CADI-tooling uit verschillende sub-scans, waarvan sommige vaker noodzakelijk zijn dan andere. Voor meer informatie over de verschillende soorten scans verwijzen we naar sectie 3.1 en in het bijzonder naar Figuur 1.

Een ideale oplossing in een IT-omgeving scant continu zowel actief als passief, zodat de cryptografische inventaris altijd up-to-date is. Eventuele kwetsbaarheden worden dan meteen geïdentificeerd en kunnen op korte termijn worden verholpen. Voor OT ligt het anders: actieve scans zijn daar momenteel niet haalbaar (en vaak zelfs niet wenselijk in verband met veiligheid) en worden dus niet geëist. Ook voor passieve scans gaven stakeholders tijdens de workshop aan dat het niet realistisch is om continu te scannen. Een scan gebruikt immers rekenkracht en toegang, die in OT beide vaak beperkt zijn. Een scan zou bijvoorbeeld met het correct functioneren van de omgeving kunnen interfereren. Ook zijn OT-omgevingen vaak lastiger bereikbaar, wat het uitvoeren van een scan bemoeilijkt. Aan de andere kant wordt OT minder vaak geüpdatet dan IT, waardoor een cryptografische inventaris ook minder vaak bijgewerkt hoeft te worden. In het ideale geval stellen we daarom dat een OT-omgeving dagelijks passief gescand dient te worden. Waar dagelijks niet haalbaar is, vanwege fysieke of operationele beperkingen, betekent dagelijks ‘zo vaak als haalbaar’. Dit kan op een moment dat de normale processen van het systeem tot een minimum beperkt zijn, bijvoorbeeld ’s nachts voor een *building management system*.

Voor een MVP eisen we in IT nog steeds continue passieve scanning. Voor actieve scanning vragen we een minimale scanfrequentie van eenmaal per week. Hoewel een hogere frequentie beter is, kosten scans rekenkracht en bandbreedte, wat kan interfereren met andere (business)processen. Bij een lagere frequentie dan eenmaal per week kunnen kwetsbaarheden enkele weken ongedetecteerd blijven, wat een te groot risico vormt. In OT stellen we voor een MVP een minimale passieve scanfrequentie van eens per maand en is actief scannen wederom buiten scope.

4.2.2 Locatie (on-premise/remote)

Hier doelen we op de locatie waar de tool wordt ingezet of draait. Er zijn in brede zin twee smaken. Zo kan tooling direct op de systemen van een organisatie worden geïnstalleerd en draaien. We noemen dit ook wel *on-premise*. De andere optie is het draaien van de tool op afstand (*remote*), bijvoorbeeld via een SaaS-achtige *(Software as a Service)* constructie.

Voor zowel de MVP als een ideale oplossing eisen we de **optie** tot on-premise inzet van de tool. Remote draaien vereist namelijk een netwerkverbinding met de leverancier van de tool, wat beveiligingsrisico's met zich meebrengt. Hoewel sommige CADI-leveranciers wel cloudversies van hun tool (willen gaan) leveren, is dit voor de doelgroep van dit onderzoek niet relevant. Het is de mening van de schrijvers van dit rapport dat CADI te gevoelig en ingrijpend is voor cloud deployment. Bovendien gaven de stakeholders tijdens de workshop aan zelf een grote mate van controle over de inzet van tooling te willen behouden; geen van de aanwezigen gaf aan het te accepteren als gegevens met een leverancier worden gedeeld.

Er moet dus de optie zijn om de CADI-leverancier **geen inzicht** in de resultaten van de scans te geven. Anders komt de leverancier te weten waar eventuele kwetsbare cryptografie in een organisatie gebruikt wordt. Er moet in dat geval dus ook worden gewaarborgd dat er geen communicatie plaatsvindt van on-premise naar buiten het netwerk.

4.2.3 Gebruik van agents

De inzet van agents zorgt voor veel flexibiliteit en nauwkeurigheid, omdat de agents autonoom in het systeem draaien en actief informatie kunnen verzamelen. Zonder agents is bepaalde informatie simpelweg niet te achterhalen, zoals welke cryptografische modules er in een stuk software worden aangeroepen. Een nadeel is dat de inzet van agents een grote mate van toegang en enige rekenkracht vereist. Het gebruiken van agents is gebruikelijk voor algemene, bredere cybersecurity-tooling.

Om zo groot mogelijke nauwkeurigheid en flexibiliteit te bereiken, zal bij een ideale tool de inzet van agents nodig zijn. De noodzaak van agents voor voldoende diepgang werd erkend door experts (buiten het directe projectteam) van TNO, tijdens de brainstorm met experts (zie 2.2) en door verschillende CADI-leveranciers die agents aanbieden. In het ideale geval worden de agents wel dermate slim en efficiënt geplaatst en gedraaid, dat de impact op andere processen geminimaliseerd wordt. Dit kan bijvoorbeeld door de agents te laten meeliften op bestaande agents in reeds gebruikte cybersecurity-tooling.

Om dezelfde reden zal een MVP over het algemeen ook agents inzetten. In het geval van een MVP voor OT is dit echter niet het geval: de inzet van agents in OT is niet haalbaar vanuit

rekenkracht en zelfs niet wenselijk vanuit veiligheidsoverwegingen, omdat ze mogelijk de beschikbaarheid van vitale processen kunnen verstoren.

We merken ten slotte op dat we hier spreken over de *optie tot* inzet van agents. Er kan bij daadwerkelijke implementatie van de tool eventueel voor gekozen worden om agents alleen in te zetten in een bepaald deelsysteem of met een bepaalde scope.

4.2.4 Inlezen van CBOMs

Naast zelf scannen naar cryptografische assets zou een CADI-tool ook inzichten kunnen opdoen uit reeds bestaande kennis over een systeem. Zo zijn er bijvoorbeeld CADI-tools die bestaande overzichten omtrent cryptografie, bijvoorbeeld in de vorm van een Cryptographic Bill of Materials (CBOM), kunnen inlezen.

Voor zowel een ideale oplossing als een MVP stellen wij dat het importeren van CBOMs van een derde partij ondersteund moet worden. Deze inschatting is hoofdzakelijk gemaakt op basis van de huidige onderzoekers. Door externe CBOMs te kunnen inlezen, kan de nauwkeurigheid van een cryptografische inventaris namelijk met relatief minimale inspanning worden verhoogd. Sommige producten, zoals bijvoorbeeld liboqs van Open Quantum Safe[3] leveren bij de code al een CBOM mee. Het kunnen inlezen van zo'n CBOM is een laagdrempelige doch zeer nuttige eigenschap, die we daarom voor zowel een MVP als de ideale tool vereisen.

4.2.5 Logs

De belangrijkste uitkomsten van een scan zullen door de meeste tools duidelijk en overzichtelijk gepresenteerd worden. Naast deze belangrijkste uitkomsten zullen de meeste scans echter nog veel meer informatie verzamelen, zoals tussenresultaten, errors en andere ogenschijnlijk minder prominente informatie. Met *loggen* doelen we op het wegschrijven (en dus niet weggooien) van deze informatie naar een apart bestand (een log).

Voor zowel de ideale oplossing als een MVP is het opslaan of wegschijven van *alle* verzamelde informatie in logs een harde vereiste. Tijdens de workshop gaven alle stakeholders namelijk aan logging zeer belangrijk te vinden. Daarnaast is het wegschrijven van logs op een zorgvuldige manier al de standaard voor vrijwel alle bestaande cybersecurity-tooling en is het dus logisch om voor CADI-tooling hetzelfde te eisen.

4.2.6 Assets binnen scope

Er zijn verschillende soorten cryptografische assets die in een systeem kunnen voorkomen. Zo zijn er cryptografische sleutels, die symmetrisch of asymmetrisch kunnen zijn. Daarnaast kan er gezocht worden naar verschillende soorten cryptografische primitieven, zoals algoritmes voor sleuteluitwisseling, digitale handtekeningen, symmetrische primitieven en hashfuncties. Voor elk van deze primitieven zijn er verschillende algoritmes beschikbaar. Ten slotte is het ook interessant binnen welke protocollen (TLS, SSH, etc) er welke cryptografie gebruikt wordt.

Voor zowel een ideale tool als een MVP vereisen we dat deze alle bovenstaande cryptografische assets kan detecteren voor hedendaagse of al verouderde cryptografie . Dit is immers

[3] liboqs/docs/cbom.json at main · open-quantum-safe/liboqs

noodzakelijk voor een kloppende en bruikbare cryptografische inventaris. Voor een ideale tool vereisen we bovendien dat deze assets ook geïdentificeerd kunnen worden voor nieuwere, quantumveilige cryptografie. Voor organisaties die al verder zijn bij het opstellen van een inventaris (en voor wie een MVP dus niet meer relevant is), is het namelijk ook interessant om te weten waar er al PQC wordt gebruikt.

Daarnaast plaatst de ideale CADI-tool de ontdekte cryptografische assets in context: waar mogelijk wordt per asset aangegeven wie of welke afdeling de eigenaar is en met welk businessproces het verband houdt. We merken wel op dat dit een stuk integratie vergt in breder verband dan enkel CADI-tooling, zoals in breder asset-management, organisatieinrichting en/of architectuur.

Tijdens de workshop was deze wens nog niet voor alle stakeholders even prominent. Toch denken wij dat dit een zeer belangrijk aspect is van een gezonde inventaris. Daarnaast gaven CADI-leverancier B & CADI-leverancier C aan dat juist deze contextinformatie volgens hen en hun klandizie vaak belangrijk is.

4.2.7 Nauwkeurigheid

Met nauwkeurigheid doelen we op de mate van volledigheid van het overzicht dat uit een scan resulteert. Met andere woorden: hoeveel van de in een organisatie/systeem aanwezige cryptografie kan er door de tool worden gevonden? We merken op dat de nauwkeurigheid van een tool in een praktijksituatie niet te verifiëren is: het daadwerkelijk berekenen hiervan vereist immers kennis over de totale aanwezige cryptografie. Nauwkeurigheid wordt daarom veelal ingeschat op basis van schattingen en resultaten in testomgevingen.

Voor een ideale tool eisen we in IT een nauwkeurigheid van 85%. In het interview met CADI-leverancier B refereerde onze contactpersoon aan een grote Wall Street-bank die bij hun klant is. Deze bank gaf aan te streven naar een nauwkeurigheid van 85%. Ook in onze workshop gaven de deelnemers aan dat een nauwkeurigheid van 80-90% van een tool al voldoende is. Voor nog hogere nauwkeurigheid kan handmatig werk verricht worden. Voor OT is scannen complexer, dus verlagen we de drempel naar een minimum van 60%: een goede indruk van wat er speelt, maar nog geen uitputtend overzicht.

Een MVP hoeft qua nauwkeurigheid minder goed te presteren. De redenering is dat een MVP minder nauwkeurig is, maar ook minder inspanning vereist. Met een MVP kan er een eerste inschatting gemaakt worden van de omvang van cryptografiegebruik binnen een organisatie, wat an sich al zeer nuttig is. We eisen daarom een nauwkeurigheid van 60% binnen IT en 30% binnen OT.

Net als bij de scanfrequentie moeten de getallen hierboven worden geïnterpreteerd als richtlijnen. Per toepassing kunnen de wenselijkheid en haalbaarheid van een bepaalde nauwkeurigheid namelijk verschillen. Bovendien bestaan CADI-tools veelal uit een aantal sub-tools en kan de (verwachte) nauwkeurigheid per sub-tool verschillen.

4.2.8 Integratie

Veel organisaties gebruiken al allerlei vormen van tooling om hun IT-omgeving te beheren en veilig te houden. Voor het gebruik van CADI-tooling is het zeer waardevol als deze met dergelijke reeds aanwezige tooling integreert. Zo zou CADI-tooling bijvoorbeeld informatie kunnen importeren over het systeem of zelfs al over cryptografische assets. Bovendien kunnen CADI-agents mogelijk meeliften op bestaande infrastructuur, wat de inzet ervan

aanzienlijk vergemakkelijkt. Andersom kan het ook zo zijn dat bestaande tooling juist voortbouwt op uitkomsten van de CADI-tool. Zo zouden uitkomsten van een CADI-tool bijvoorbeeld geëxporteerd kunnen worden naar aan andere tool.

Voor een ideale CADI-tool verwachten we dat deze integreert met de grote of bekende andere security-tooling: er zijn kant-en-klare modules (API calls) die gemakkelijke koppeling mogelijk maken. Bovendien levert de ideale leverancier van CADI-tooling maatwerk om de integratie met andere, minder bekende tooling te bewerkstelligen. We baseren deze eis op twee inzichten. Ten eerste gaven veel van de deelnemers aan de workshop aan dat de inzet van nieuwe tooling geen probleem vormt, mits deze exporteert naar bestaande tooling die ze al in gebruik hebben. Ten tweede hebben wij op basis van onze gesprekken met de CADI-leveranciers geconcludeerd dat integratie ook van hun kant belangrijk is: niet alleen voor het exporteren van de resultaten, maar ook voor het meeliften op bestaande infrastructuur, bijvoorbeeld voor het deploy van agents op een minder ingrijpende manier.

Een MVP hoeft geen kant-en-klare integraties te bieden. Wel is integratie met bestaande tooling dermate belangrijk dat de tool hier op zekere hoogte rekening mee houdt. De leverancier adviseert over hoe de integratie met bestaande tooling geïmplementeerd kan worden. Daarnaast kan er wel de koppeling worden gelegd tussen verschillende systemen, doordat de resultaten van de CADI-tool makkelijk exporteerbaar **moeten** zijn.

4.3 Overzicht & inspanning-nauwkeurigheid

In het voorgaande zijn de verschillende eigenschappen en eisen rondom CADI-tooling beschreven. In deze sectie vatten we deze bevindingen samen in een tabel. Bovendien introduceren we een model waarin we de mogelijke (deel)functionaliteiten van een CADI-tool plotten op een as met toenemende mate van nauwkeurigheid en inspanning.

4.3.1 Overzicht van eigenschappen en eisen

In de tabel hieronder wordt het bovenstaande overzichtelijk samengevat: welke eisen hebben we geïdentificeerd en hoe worden deze voor een MVP dan wel een ideale oplossing ingevuld.

Eis	Korte beschrijving	MVP	Ideale oplossing
Scanfrequentie	Hoe vaak vindt de scan plaats?	Maandelijks passief (OT); continu passief en wekelijks actief (IT)	Dagelijks passief (OT); continu passie en actief (IT)
Locatie	Waar draait de scan (on-prem/remote)?	Optie tot on-premise	Optie tot on-premise
Agents	Kunnen er agents worden ingezet en gebruikt?	Nee (OT), ja (IT)	Ja*
Inlezen van CBOMs	Kunnen CBOMs van leveranciers ingelezen worden?	Ja	Ja
Logs	Welke informatie wordt er gelogd?	Alle informatie rondom het uitvoeren van de scan, errors en resultaten	Alle informatie rondom het uitvoeren van de scan, errors en resultaten
Scope	Welke cryptografische assets kunnen worden gevonden?	Sleutel(materiaal), crypto primitieve en protocol	Idem als voor MVP, maar ook voor PQC. Plaatst de assets ook in context (eigenaar, proces)
Nauwkeurigheid	Hoeveel cryptografische assets kunnen gevonden worden?	30% (OT), 60% (IT)	60% (OT), 85% (IT)
Integratie	In hoeverre integreert de tool met reeds bestaande/aanwezige tooling?	Niet kant-en-klaar. Wel advies.	Kant-en-klaar met met grote, bekende producten. Maatwerk voor andere producten

Tabel 1. Overzicht van eisen aan MVP en ideaal

** Agents op OT-endpoints is een relatief nieuw begrip. Over het algemeen worden er geen agents op OT-systemen geplaatst uit angst voor negatieve impact op systeem-uptime en operationele prestaties. Doordat er echter steeds meer cybersecurity-risico's zijn voor OT-endpoints (geïnfecteerde onderhouds-hardware, controllerfouten, kwaadaardige medewerkers, gestolen authenticatiegegevens, etc.), en dit vooral een aantrekkelijk doelwit is voor Advanced Persistant Threats (APTs) is er steeds meer noodzaak voor endpoint-oplossingen zoals bij de IT.*
Hoewel deze verandering dus deels in nieuwe OT aanwezig is, en daarmee agents ook een mogelijkheid worden, is dit in het overgrote gedeelte van bestaande OT niet een mogelijkheid.

4.3.2 Het inspanning-nauwkeurigheidsmodel

Voor de ingebruikname van CADI-tooling geldt een algemene tendens: hoe nauwkeuriger de resultaten dienen te zijn, hoe groter de benodigde inspanning is. Nauwkeurigheid interpreteren we hier zoals in sectie 4.2.7: het percentage gevonden cryptografische assets. Inspanning verwijst naar een combinatie van de benodigde tijd, financiële middelen en personeel, maar ook de impact van de scan op het onderzochte systeem.

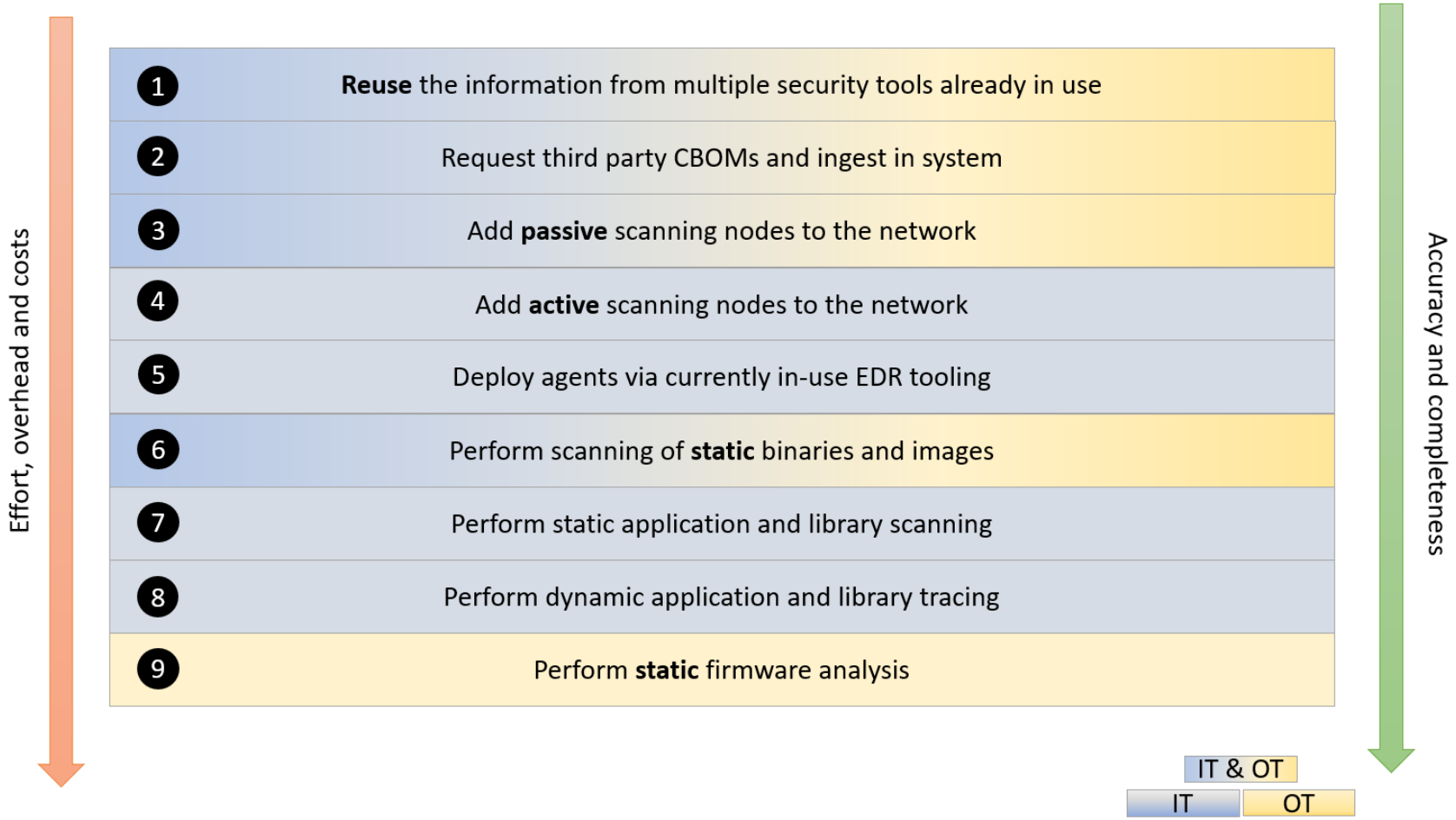
We hebben het spectrum van kleine inspanning/lage nauwkeurigheid tot grote inspanning/hoge nauwkeurigheid concreet gemaakt in Figuur 2. De bovenste stappen refereren aan maatregelen of sub-tools van een CADI-tool die makkelijk haalbaar of inzetbaar zijn, maar beperkte nauwkeurigheid bieden. Voor een grotere nauwkeurigheid kunnen stappen lager op de ladder worden ingezet; die vereisen dan wel een hogere inspanning.

De MVP voor OT bestaat uit (1), (2) en (3). De eerste twee stappen zijn erg makkelijk uitvoerbaar en vereisen geen nieuwe tooling, noch extra rekenkracht op endpoints. De kans is echter wel aanwezig dat dit heel weinig informatie oplevert. Vandaar dat we ook het passief scannen (3) van het netwerkverkeer zien als onderdeel van de MVP. Dit vereist het inzetten van een nieuwe tool, maar heeft weinig tot geen invloed op de continuïteit van bedrijfsprocessen. Het passieve scannen zou informatie op moeten kunnen leveren over welke endpoints berichten uitsturen en welke protocollen er gebruikt worden.

De ideale tool voor OT omvat naast (1), (2) en (3) ook (6) en (9). Actief scannen van online systemen in OT-omgevingen met behulp van agents lijkt ons, zoals eerder beschreven, niet haalbaar. Het offline scannen van binary's en firmware heeft geen invloed op de bedrijfsprocessen, maar vereist wel gespecialiseerde tools, waarbij legacy-producten voor problemen kunnen zorgen. Meerdere producten van hetzelfde type hoeven maar eenmalig geanalyseerd te worden (mits ze dezelfde configuratie hebben). Het statisch analyseren van binary's levert op welke cryptosystemen aangeroepen kunnen worden, terwijl het dynamisch scannen van firmware inzicht geeft in welke cryptosystemen daadwerkelijk aangeroepen worden.

De MVP voor IT bestaat uit (1), (2), (3), (4), (5) en (7). Net zoals voor OT zijn (1) en (2) zijn gemakkelijk te implementeren en geven ze al veel inzicht. (3) zal ook weinig inspanning behoeven, aangezien (grote) IT-bedrijven al gebruik maken van netwerkscanners. Het is echter een vak apart om de sensoren goed te plaatsen, vanwege de netwerksegmentatie die grote IT-bedrijven hebben vanwege beveiligingsoverwegingen. In tegenstelling tot OT vereisen we voor een MVP bij IT de optie tot inzet van agents. Dat kan door nieuwe agents in te voeren (4) (eventueel door bestaande probes of agents in aangepaste vorm te hergebruiken), maar liever door agents te hergebruiken en te integreren met bestaande EDR-tooling (5) (zie ook sectie 3.3). Op het vlak van applicatie- en libraryscanning vereisen we van een MVP in IT geen actieve scans, maar wel passieve (7) omdat die makkelijker haalbaar zijn.

De ideale tool voor IT heeft daarbij ook nog (6) en (8). Zoals voor OT al opgemerkt werd, heeft het offline scannen van binary's en firmware geen invloed op de bedrijfsprocessen, maar vereist het wel gespecialiseerde tools (6). Voor het dynamische tracen van applicaties en library's zijn ook speciale tools nodig, die zeer veel werkgeheugen vereisen. Dit kan effect hebben op de bedrijfsprocessen en het is vermoedelijk niet haalbaar om dit continu te doen. Het statisch scannen van firmware (9) vereist een zeer grote inspanning. Hoe groot het informatiegat is dat deze vorm van scannen überhaupt kan dichten zal moeten blijken na het uitvoeren van de eerste 8 stappen van het model. Vandaar dat het momenteel niet als onderdeel van de ideale tool voor IT is beschreven.



Figuur 2. De verschillende niveaus van CADI-Functionaliteiten. Des te hoger het nummer van de functionaliteit, des te hoger de resulterende nauwkeurigheid alsmede de benodigde inspanning het te vergaren.

5 Commerciële CADI-tools

Hoewel cryptografie al langer en zeer wijdverspreid wordt gebruikt, is het domein van commerciële CADI-tooling relatief jong: pas in 2013 en 2014 werden de eerste bedrijven opgericht die zich hierin specialiseren. In dit hoofdstuk beschouwen we een aantal commerciële CADI-tools en hun eigenschappen.

Het hoofdstuk is als volgt gestructureerd. In sectie 5.1 wordt een kort overzicht gegeven van het huidige landschap van aanbieders van CADI-tooling en dienstenleveranciers. Dit wordt gevolgd door welke CADI-tools onderzocht zijn in de shortlist in sectie 5.2. Vervolgens bespreken we de mapping van de oplossingen op de MVP- en ideale CADI-tool in sectie 5.3. We eindigen met de belangrijkste conclusies die volgen uit ons onderzoek en de interviews in sectie 5.4. Aan het einde van dit hoofdstuk wordt de link gelegd in een tabel tussen de MVP, het ideaal, de CADI-leveranciers en de andere geïnterviewde leveranciers.

5.1 Marktlandschap

De beschrijving van het marktlandschap wordt opgebouwd op basis van bestaande kennis van TNO tenzij anders aangegeven.

Het marktlandschap bestaat uit de bekende CADI-leveranciers en generieke security-leveranciers zoals hier genoemd. Het bestaat echter ook uit de organisaties die deze oplossingen adopteren, integreren en onderhouden.

5.1.1 Adoptie door dienstenleveranciers

Uit de belangstelling voor het PQC-migratiehandboek[4] en de presentaties rondom dit onderwerp weten we dat de adoptie voor diensten rondom CADI-tooling toeneemt. De geïnteresseerden omvatten zowel eindgebruikers, als consultancy-firma's en andere dienstenleveranciers die reeds bekend zijn met integraties van IT-assetmanagement-tooling bij eindklanten.

De meeste de geïnterviewde CADI-leveranciers geven aan dat een deel van hun verdienmodel de consultancy is rondom het opzetten en draaiende houden van hun CADI-tool bij de eindgebruiker. Alleen CADI-leverancier A geeft aan uitsluitend een *software-as-a-service*-bedrijf te willen zijn. Voor leveranciers die geen consultancy aanbieden zal het opzetten en draaiende houden óf zó simpel en goed gedocumenteerd moeten zijn dat een eindgebruiker dit zelf kan, óf een dienstenleverancier kan in dit gat springen. Dienstleveranciers beschikken over de kennis en ervaring die nodig zijn voor grootschalige implementaties in IT-landschappen, en de implementatie in de bij de klant bestaande risicomanagementmethodologieën. Dit komt omdat dit voor software- en hardware-assetmanagement een reeds bestaande markt is voor deze dienstenleveranciers. In het algemeen geldt voor PQC-migraties dat sommige organisaties dit zelf kunnen en willen opzetten, terwijl anderen dit graag uitbesteden naar een dienstenleverancier. Consultancybedrijven en de gesproken generieke security leveranciers lijken zich hier al op voor te (willen) bereiden. Dit blijkt uit de interviews (zie Bijlage

[4] Vernieuwd handboek voor quantumveilige cryptografie

4 – Samenvatting Interviews met generieke security-leveranciers) en hun aanhoudende interesse om hier met TNO over te sparren.

5.1.2 Fusies, overnames, of nieuwe ontwikkelingen

We verwachten dat veel van de startups die CADI-tooling maken, zullen worden overgekocht door grotere bedrijven. CADI-leverancier B gaf aan dat dit reeds bij hun is gebeurd. Wij verwachten dat er in brede zin twee soorten organisaties zijn die CADI-tools zullen inkopen om hun aanbod te versterken. Ten eerste zijn er generieke security leveranciers in het IT-domein, voor wie CADI een natuurlijke uitbreiding van het aanbod is zodra de markt zich verder ontwikkelt. Ten tweede zijn er organisaties met een bestaande klantbasis voor wie (een specifieke vorm van) CADI in het bijzonder relevant is, zoals in het OT-domein.

Het is ook aannemelijk dat bestaande leveranciers van generieke security-tooling zelf CADI-functionaliteiten gaan ontwikkelen, zodra de markt voor CADI-tooling groeit. Twee van de generieke security leveranciers (A en D) bewegen zich al enigszins die kant op.
Omdat de grotere generieke security leveranciers al een grote, bestaande klantenbasis hebben, kunnen ze relatief snel en gemakkelijker hun marktaandeel via *upselling* laten groeien. Ze hebben als nadeel dat ze niet over de kennis en ervaring op dit onderwerp beschikken die bijvoorbeeld de CADI-leverancier B en CADI-leverancier C reeds hebben.

5.1.3 Verwachte ontwikkelingen

Het is onze verwachting dat het onderscheid tussen bestaande CADI-oplossingen en de uitbreiding van bestaande oplossingen vooral zal gemaakt worden door de dienstenleveranciers.

Waar de dienstenleveranciers niet op een nauwkeurigheid worden beoordeeld, óf waar ze niet als dienstenleverancier verantwoordelijk worden gehouden voor de daadwerkelijke migratie van een asset naar een PQC-variant, zullen zij voor een makkelijk te integreren en goedkope oplossing gaan. Dat kan bijvoorbeeld een reeds bestaande oplossing zijn die is uitgebreid CADI-capaciteiten. Dit is voor hun namelijk het meest winstgevend.
Als een dienstenleverancier echter wél wordt beoordeeld op nauwkeurigheid, óf als ze zelf de migratie gaan doen, zullen ze eerder geneigd zijn meer te investeren in hun CADI-tool om een hogere volwassenheid en nauwkeurigheid te behalen. Dit zorgt ervoor dat ze makkelijker kunnen door ontwikkelen in de toekomst en zo hun winstgevendheid toeneemt.
Hiermee heeft de eindklant met een eindvraag dus een directe invloed op de selectie van de CADI-tooling door de dienstenleveranciers.

We verwachten dat dit de komende vijf jaar de ontwikkeling van CADI-tooling, bestaande dan wel nieuwe, zal gaan beïnvloeden.

5.2 Opstellen shortlist

Als eerste stap hebben we op het internet en in ons netwerk gezocht naar bedrijven die in dit gebied actief zijn. Hierbij is rekening gehouden met het feit dat CADI-tooling onder verschillende benamingen bekend staat. Een greep hieruit is: *crypto(graphy) scanning, cryptographic inventory, cryptographic discovery*, *cryptographic asset discovery*, alsmede variaties hieropen combinaties ervan (zie Bijlage 5 – Zoektermen). Er werd op deze manier een lijst van bedrijven verzameld, veelal start-ups. Voor een aanzienlijk deel van deze bedrijven was de informatievoorziening echter zeer minimaal: soms was er geen website (en werd er

alleen naar de tool verwezen in een ander document), soms was de website nogal amateuristisch opgezet en vaak was het niet duidelijk wat de leverancier precies aanbood: bestaat er al een werkend product of is het meer reclame voor een tool die nog gemaakt wordt?

Daarom is ervoor gekozen om een 'shortlist' te compileren: commerciële CADI-tools die we als voldoende volwassen beschouwen om nader te onderzoeken door middel van een interview. Daarnaast hebben we ook CADI-leverancier A meegenomen, <>.

Deze partijen zijn op verschillende manieren benaderd. Bij CADI-leverancier B is er via een TNO-collega iemand benaderd, die ons intern doorverwees naar de juiste contactpersoon voor het CADI-product. CADI-leverancier C is via LinkedIn benaderd, aangezien er op het contactformulier geen (tijdige) respons kwam. CADI-leverancier A is benaderd via email, waarbij de emailadressen op de site stonden. CADI-leverancier F is ook via mail benaderd, maar na een eerste (positieve) kennismaking via de mail begin juni is het contact gestrand.

5.3 Mapping van bestaande oplossingen op MVP en ideaal

In hoofdstuk 4 is beschreven aan welke eisen een CADI-tool dient te voldoen om te gelden als minimum viable product (MVP) en welke eisen we stellen aan een ideale CADI-tool. In de tabel verderop worden de CADI-producten van CADI-leverancier A, CADI-leverancier B en CADI-leverancier C aan deze eisen getoetst.

Per eis wordt weergegeven in hoeverre elk van de producten aan de eisen van MVP dan wel het ideaalbeeld voldoet:

- Een groene markering betekent dat het product voor deze eis voldoet aan het ideaal;
- Een gele markering betekent dat het product voor deze eis voldoet aan de MVP, maar niet aan het ideaal;
- Een rode markering betekent dat het product voor deze eis niet voldoet aan de MVP (en dus ook niet aan het ideaal);
- Een blauwe markering betekent dat het onduidelijk of onbekend is in hoeverre het product aan de eis voldoet.

Merk op: omdat alle drie de partijen tijdens de interviews aangaven geen ervaring te hebben in de OT, hebben we er in onderstaande tabel voor gekozen om de CADI-tools te vergelijken met MVP en ideaal in een IT-setting.

5.4 Belangrijkste conclusies

Hieronder vatten we de belangrijkste conclusies rondom CADI-tooling samen. Deze conclusies bevatten inzichten uit de mapping van de verschillende tools op het ideaalbeeld en de MVP, maar ook uit de interviews met deze CADI-leveranciers.

De conclusies in de rest van dit hoofdstuk zijn gebaseerd op een aantal verschillende bronnen:

- Interviews met leveranciers, soms meerdere gesprekken met dezelfde partij, op basis van een eerder overeengekomen lijst van vragen.

- Verdiepingsvragen (bij vervolg interviews en via email) die op functionele tooling capaciteiten van andere leveranciers waren gebaseerd. (zonder vermelding van de leverancier).
- Overleg met eigen TNO-experts over gelijkende tooling en uitdagingen daarvan, ook om sommige claims uit interviews te duiden over hun haalbaarheid.
- (Online) bronnenonderzoek.

Eis	MVP (IT)	Ideale oplossing (IT)	CADI-leverancier A	CADI-leverancier B	CADI-leverancier C
Scanfrequentie	Wekelijks	Continu	Niet besproken	Kan over het hele spectrum. Wekelijkse updates komen nu vaak voor bij klanten.	Ze suggereren zelf elk kwartaal. Kan ook maandelijks of zelfs dagelijks.
Locatie	On-premise	On-premise	On-premise	On-premise (of via cloud)	On-premise
Agents	Ja	Ja	Nee	Meerdere opties mogelijk	Meerdere opties mogelijk
Inlezen van CBOMs	Ja	Ja	Nee	Ja	Niet besproken
Logs	Alle informatie rondom het uitvoeren van de scan, errors en resultaten	Alle informatie rondom het uitvoeren van de scan, errors en resultaten	Alle informatie rondom het uitvoeren van de scan, errors en resultaten	Alle informatie rondom het uitvoeren van de scan, errors en resultaten	Alle informatie rondom het uitvoeren van de scan, errors en resultaten
Scope	Sleutel(materiaal), cryptoprimitieven en protocollen	Idem als voor MVP, maar ook voor PQC. Plaatst de assets ook in context (eigenaar, proces)	Sleutel(materiaal), cryptoprimitieven en protocollen.	Sleutel(materiaal), cryptoprimitieven en protocollen. Ook aandacht voor het plaatsen van assets in context (bijv. kruisreferenties). Over het vinden van PQC is niet gesproken.	Sleutel(materiaal), cryptoprimitieven en protocollen. Ook PQC.
Nauwkeurigheid	60%	85%	CADI-leverancier A analyseert alleen netwerkverkeer, maar claimt daarop zeer nauwkeurig te zijn.	Geen duidelijke data over, want er is geen ground truth.	Geen duidelijke data over, want er is geen ground truth.
Integratie	Niet kant-en-klaar. Wel advies.	Kant-en-klaar met met grote, bekende producten. Maatwerk voor andere producten	Nog geen integraties, maar plan voor een API naar een CMDB.	Veel integratie met bestaande tools.	Veel integratie met bestaande tools. Dat is (naar eigen zeggen) een van de sterkste punten.

Tabel 2. Relatie tussen tools van geïnterviewde partijen, MVP en ideaal. Zie 5.3.

5.4.1 OT-omgevingen

Voor OT-omgevingen is er een grote discrepantie tussen de ideale en de bestaande oplossingen, vanwege de uitdagingen beschreven in sectie 3.4. Zoals hierboven al werd benoemd, gaven alle drie de CADI-leveranciers aan dat ze geen ervaring hebben in het inzetten van de tool in het OT-domein. CADI-leverancier B gaf aan dat OT ook niet tot hun doelen behoort: dergelijke toepassingen zijn volgens de contactpersoon te niche om de investering waard te zijn. CADI-leverancier C en CADI-leverancier A stonden eventueel wel open om toepassingen in het OT-domein te verkennen, maar hadden op het moment van spreken hiervoor geen concrete plannen.
Dit vereist een specifiek toegewijde partij die dit probleem gaat aanpakken. Vanuit deze gesprekken zijn we tot de conclusie gekomen dat analyse van de firmware het meest geschikt lijkt. We zien momenteel maar één tool die de firmware van OT-systemen zou kunnen analyseren, namelijk Generieke security-leverancier E. Dit vereist wel dat de endpoints goed in kaart zijn gebracht.

5.4.2 Beschikbaarheid van CBOMs van derde partijen

Het scannen van library's of software van derde partijen is zeer complex en vereist inzicht in de code (*white-box*). Het zou veel schelen als softwareleveranciers bij elk van hun producten een CBOM zouden leveren waarin wordt aangegeven welke cryptografie er allemaal in het product wordt gebruikt. Op deze manier kunnen organisaties de CBOM in hun cryptografische inventaris opnemen en hoeven ze niet elk product te scannen (voor zover dat überhaupt mogelijk is).
We adviseren bij te dragen aan wetgeving en adviezen, om de markt deze kant op te bewegen, eventueel op Europees niveau. Veel producten uit de VS gaan dit wellicht sneller doen door het voorlopen van de VS op wetgeving omtrent PQC.

5.4.3 Ontbreken van een *Ground Truth* voor nauwkeurigheid

Meerdere partijen, in het bijzonder CADI-leverancier B en CADI-leverancier C, gaven aan dat het lastig is om in te schatten hoe nauwkeurig hun oplossing is. Dit komt omdat er geen *ground truth* is: je weet van een gegeven systeem niet a priori welke cryptografie er allemaal gebruikt wordt, dus kun je ook niet vergelijken hoeveel procent hiervan je met de tool gevonden hebt.
Beide partijen gaven aan geïnteresseerd te zijn in een test. Zo zou men een testomgeving kunnen opzetten waarin handmatig alle cryptografie bij het opzetten wordt bijgehouden en gelabeld. Dan bestaat er wel een ground truth en vervolgens zouden de tools hierop losgelaten kunnen worden, en kan per niveau en vorm van scannen worden nagegaan wat er gevonden wordt en daarmee wat de nauwkeurigheid is van de CADI-tool. Dit zou een objectieve meetstaaf kunnen vormen voor de evaluatie van CADI-tooling.

5.4.4 Kosten

De commerciële CADI-tools zijn over het algemeen erg duur. Verschillende bedrijven hanteren verschillende prijsmodellen, waarbij de prijs af kan hangen van factoren als het aantal endpoints, aantal applicaties, aantal en soort scanners, aantal integraties met andere tools, et cetera. Voor grotere organisaties lopen de bedragen al snel in de honderdduizenden of zelfs miljoenen euro's per jaar. Voor veel organisaties is een dergelijke investering lastig of wellicht zelfs onhaalbaar.

5.4.5 Herkennen van PQC

Voor zover bekend is momenteel alleen de tool van CADI-leverancier C in staat om de (nieuwe) PQC-algoritmes te ontdekken. Dit is misschien nu ook niet de hoogste prioriteit, maar wordt in de komende jaren wel belangrijk, om te kunnen inschatten in hoeverre de organisatie al quantumveilig is en welke PQC-algoritmes gebruikt worden en waarvoor. Ook als algoritmen, zoals bijvoorbeeld SIKE, al zijn geïmplementeerd, maar toch kwetsbaar blijken te zijn, kan dit worden gedetecteerd en gemigreerd worden.

5.4.6 Wel/niet gebruik agents

Niet alle oplossingen maken gebruik van agents. Het gebruik van agents wordt namelijk vaak als ongewenst gezien. Dit kwam ook uit de workshop, en CADI-leverancier B & CADI-leverancier C kregen dit in het verleden ook herhaaldelijk terug van hun klanten. Zij hebben er daarom voor gekozen om 3 smaken aan te bieden:

1. **Geen agents**, maar hiermee komt ook een verminderde kwaliteit van de opgehaalde inhoudelijke informatie, omdat sommige informatie niet opgehaald kan worden zonder agents.
2. ***Dissolving* of *piggy-backing* agents**, die een klant zelf in bestaande agents van bijvoorbeeld een reeds gebruikt security product kan plaatsen. Op deze manier hoeft er geen nieuwe strategie of implementatie gemaakt te worden om extra agents in te zetten. Dat vermindert het risico op problemen tussen agents en rekenkracht en daarnaast kan geheugengebruik geminimaliseerd worden.
3. **Eigen, nieuwe agents,** die een klant dan naar eigen inzicht kan installeren.

Optie 2 lijkt TNO het meest gewenst, omdat het niet realistisch is een volledige cryptografische inventaris te krijgen zonder gebruik van agents. Aan de andere kant zijn agents met volledige privileges weer zeer invasief, wat voor organisaties vaak onwenselijk is. De kosten en baten zullen per use case en organisatie ingeschat moeten worden.

		MVP - IT	Ideaal - IT	MVP - OT	Ideaal - OT	CADI-leve-rancier A	CADI-lever-ancier B	CADI-leve-rancier C	Generieke se-curity-leve-rancier B	Generieke se-curity-leve-rancier C	Generieke se-curity-leve-rancier D	Generieke se-curity-leve-rancier E
Netwerk	Passief	X	X	X		X	X	X	X			
	Actief	X	X			X	X	X	X		X	
Applicaties & library's	Statisch	X	X				X	X	X	X	X	
	Dynamisch		X				X					
Firmware	Statisch		?		X			X			X	X
	Dynamisch		?									
Bestands-syteem	Statisch	X	X		X		X	X				

Tabel 3 Overzicht van lagen en soorten scans voor MVP's, ideale tools, CADI-oplossingen en de mogelijkheden voor cybersecurity-oplossingen om op dit niveau te scannen.

6 Cybersecurity-oplossingen

Zoals beschreven in sectie 3.2.2 kunnen generieke cybersecurity-oplossingen uitgebreid worden met CADI-functionaliteiten. In sectie 6.1 beschrijven we de totstandkoming van de interview shortlist, in sectie 6.2 hoe de cybersecurity-oplossingen zouden kunnen voldoen aan de eisen (beschreven in sectie 4.1) en tot slot de belangrijkste conclusies van deze interviews in sectie 6.3.

6.1 Opstellen shortlist

Naast de eerder geselecteerde CADI-leveranciers, hebben we de uitvraag vanuit QvC Rijk om ook gevestigde leveranciers van asset management oplossingen, ook meegenomen. Hieruit bleek dat Generieke security-leverancier D, Generieke security-leverancier G en Generieke security-leverancier B het meest gebruikt werden onder de uitgevraagde overheidsinstanties. We waren op zoek naar een verscheidenheid aan cybersecurity-oplossingen, zoals beschreven in sectie 3.2.2.

- Generieke security-leverancier B (SOC, SIEM, EDR, ITAM)
- Generieke security-leverancier D (SOC, SIEM, EDR, CMDB, ITSM, ITAM)
- Generieke security-leverancier G (ITAM, CMDB)
- Generieke security-leverancier F (SOC, SIEM, EDR, CMDB, ITSM)
- Generieke security-leverancier H (CMDB, ITSM, ITIM)

Bij Generieke security-leverancier G en Generieke security-leverancier F is het niet gelukt om tijdig contact te krijgen met de juiste personen.
Generieke security-leverancier C is via contacten van het team en eerder getoonde interesse in CADI benaderd.
Generieke security-leverancier A is als verkenning gesproken, door contacten bij het team.

Het was mooi geweest als we Generieke security-leverancier D, wiens producten bij de meeste ministeries gebruikt wordt, hadden kunnen interviewen. Dit is helaas niet gelukt.

6.2 Uitbreiding met CADI-functionaliteiten

Een aantal generieke security-producten beschreven in sectie 3.3 hebben een technologische basis die lijkt op die van CADI-tooling. Zo maken ze bijvoorbeeld gebruik van eenzelfde backend als nodig is voor netwerkscanning, applicatie- en library-scanning, firmware(code)scanning, en bestandsysteemscanning.

- **EDR/XDR:** oplossingen komen voort uit de bescherming van endpoints tegen virussen en malware. Naarmate er meer geautomatiseerd wordt, en de dreigingen gespecialiseerder worden, zijn EDR-oplossingen zich gaan baseren op agents met diepgaande rechten om zaken die zich op een endpoint afspelen in te zien, te scannen, en waar nodig in te grijpen.
  Deze agents zijn óók nodig voor CADI-tooling. Maar door hun hoge mate van toegang, en hoge doorontwikkeling en uitdaging zoals te lezen in sectie 5.4.6, is het

uitbreiden van de agents niet altijd gewenst. EDR/XDR-tools kunnen relatief makkelijk uitgebreid worden naar actieve scanning van gebruik van cryptografie. Veel van de agents of agent-opties van de CADI-leveranciers werken hierop ook. Er heerst dan wél de vraag hoe efficiënt dit kan gebeuren. Er is altijd een vraag tussen hoe compleet de agents (voor EDR/XDR óf CADI) kunnen zijn ten opzichte van de gebruikerservaring.

- **ITAM:** deze tools scannen doorgaans de gehele IT-omgeving. Dit is een voorwaarde voor CADI-tooling: een volledige CBOM kan alleen komen uit een volledige scope van IT-assets. Daarnaast kan ITAM-tooling er óók voor zorgen dat systemen aan businessprocessen worden gekoppeld. ITAM tools gebruiken zelf vaak ook agents.

- **CLM:** deze tools beheren certificaten inhoudelijk. Hoewel een CLM-oplossing voor een organisatie niet noodzakelijk is, baten organisaties er zeker bij voor grootschalige wijzigingen zoals een cryptografische migratie. CADI-tooling lijkt over het algemeen uitstekend in staat certificaten te vinden, maar is niet in staat ze te beheren. Ook wordt CLM niet vaak op zichzelf staand gedaan, en is het vaak onderverdeeld bij verschillende services en onderdelen van het IT-landschap. Dit werkt goed in hoe men er nu geautomatiseerd mee omgaat, want het wordt vaak opgezet, en alleen bij incidenten hoeft er actief beheer uitgevoerd te worden. Dit is niet het geval bij een systematische migratie, noch bij het beheer van bijvoorbeeld hybride certificaten[5].

- **CMDB:** deze tooling is vaak afhankelijk van goede ITAM- én EDR/XDR-oplossingen om het te voeden. Op zijn beurt is CMDB weer een bron voor systemen die specifieke IT-assets beheren zoals Software Asset Management (SAM) systemen. De oplossingen lopen soms wat door elkaar: ITAM-, SAM-, en CMDB-oplossingen vormen vaak gezamenlijk het voltallige assetmanagement. Vaak is óf de CMDB- óf de ITAM-oplossing de *single source of truth*, waarop beheer wordt uitgevoerd. Sommige CADI-tooling maakt dus gebruik van een dergelijke bestaande single source of truth, of is er zelfs afhankelijk van. Deze single source of truth is ook een mogelijke plek waar we een resulterende CBOM verwachten terug te vinden, en waar crypto assets gekoppeld zijn aan hardware- en softwareonderdelen voor beheer. Maar dit kan ook apart, zolang de koppeling maar goed is.

- **Vulnerability scanning:** deze tools scannen op mogelijke kwetsbaarheden. Sommige vulnerability scanners geven nu al incidenten als er verouderde cryptografie wordt gebruikt, zoals Generieke security-leverancier E. We vermoeden dat veel CADI-tools verder hebben gebouwd op bestaande vulnerability-scanners voor de applicatie- en firmwarescanning van cryptografie. Dergelijke tools hebben wél toegang nodig tot de source-code en zijn vaak niet of slecht geschikt voor software gemaakt of geleverd van/door derden.

De ontwikkeling van bovenstaande tooling wordt al decennia gedreven door gebruikers. Ze volgt volledig de vraag vanuit de markt. Het is daarom aannemelijk dat dergelijke bestaande oplossingen hun repertoire uitbreiden met CADI-functionaliteiten, als of zodra daar vraag naar is.

[5] https://hapkido.tno.nl/news/proof-concept-live/

6.3 Belangrijkste conclusies

De generieke security-leveranciers stonden over het algemeen geïnteresseerd tegenover CADI als mogelijke uitbreiding op hun huidige aanbod. Het volwassenheidsniveau verschilde hierin per leverancier: sommige bedrijven waren al enige tijd met dit onderwerp bezig, terwijl het voor andere nieuw doch interessant was.

De belangrijkste conclusie was echter de volgende: verschillende organisaties gaven aan geïnteresseerd te zijn in CADI als onderwerp, maar er momenteel nog geen concrete stappen in te ondernemen vanwege een gebrek aan directe drijfveren. Sommige leveranciers hadden een enkele keer van een klant vragen over PQC of CADI gehad, maar over het algemeen was dit tot een minimum beperkt. Daardoor was het voor deze leveranciers vanuit commercieel oogpunt momenteel nog niet aantrekkelijk om meer in CADI te onderzoeken, ontwikkelen en aan te bieden.

7 Samenvatting en conclusie

In dit hoofdstuk vatten we de inzichten uit het onderzoek samen in enkele conclusies. Voor een aantal concrete aanbevelingen (die aan deze conclusies verwant zijn) verwijzen we naar Hoofdstuk 8.

Voor de volledigheid herhalen we hieronder de drieledige onderzoeksvraag uit de inleiding.

1. Hoe zien *minimum viable product* (MVP) en een ideale tool voor CADI eruit en aan welke eisen voldoen ze?
2. Wat is de huidige status van de CADI-tools die al commercieel verkrijgbaar zijn en hoe verhouden deze zich tot het ideaal en de MVP?
3. Hoe is het gat tussen de MVP en een ideale CADI tool te overbruggen?

Voor onderzoeksvraag 1 verwijzen we naar Tabel 1, en voor onderzoeksvraag 2 verwijzen we naar Tabel 2. Voor het antwoord op de derde onderzoeksvraag doen we een aantal aanbevelingen in Hoofdstuk 8.

Cryptografische inventarisatie zit op een spectrum van nauwkeurigheid en inspanning. Een CADI-tool bestaat onder de motorkap uit verschillende puntoplossingen. Hoe meer van deze puntoplossingen worden ingezet en hoe dieper (i.e. hogere nummering) de puntoplossingen gaan (zie Figuur 2), hoe nauwkeuriger, volledig er en duurder de cryptografische inventaris wordt.

Bestaande fullstack-oplossingen voor CADI zijn duur. Van CADI-leverancier B en CADI-leverancier C krijgen we tijdens de interviews een grove schatting voor de kosten van het afnemen van hun tool, die in de orde van grootte van honderdduizenden of miljoenen euro's per jaar liep. Er is daardoor sprake van een soort kip-ei-probleem: tijdens de workshop noemden verschillende stakeholders dat het lastig is om budget te krijgen voor PQC-gerelateerde activiteiten, en dat ze een cryptografische inventaris willen gebruiken om de ernst van het probleem aan hoger management te laten zien. Voor de inventarisatie zelf is in die gevallen dus maar zeer beperkt budget beschikbaar, waardoor dure tooling problematisch is.

Bestaande fullstack-oplossingen voor CADI zijn niet-Europees. CADI-leverancier B en CADI-leverancier C zijn beide niet in Europa gevestigd. Hoewel er on-premise gewerkt kan worden en er constructies met *non-disclosure agreements* (NDA's) mogelijk zijn, is dit voor high assurance-omgevingen wellicht een probleem.
Opvallend is dat veel van de technologische experts van deze bedrijven wél Europees zijn. Dit laat zien dat er geen gebrek is aan kennis in Europa, maar een gebrek aan kansen om een bedrijf in Europa op dit gebied op te zetten of te laten groeien. Dit kan dus veranderen als de vraag in Europa voor CADI-oplossingen hoger wordt dan in de VS.

De markt voor CADI-leveranciers is *compliance-driven*. Zowel CADI-leverancier B als CADI-leverancier C gaven aan dat voldoen aan wet- en regelgeving voor hun klandizie momenteel de belangrijkste drijfveer is. Hoewel de aanstaande migratie naar PQC en algemene cryptografische hygiëne ook wel eens worden genoemd, werd compliance als eerste

argument gebruikt. De wetgeving op PQC-migratie en specifiek cryptographic asset discovery loopt in de VS voor[6] op de Europese Unie.

Integratie met generieke cybersecurity-tooling staat hoog in het vaandel. Dit is het geval voor de stakeholders die we bij de workshop spraken, maar óók voor de CADI-leveranciers. Dit tweede feit is een goede ontwikkeling omdat het de adoptie en integratie van dergelijke systemen vereenvoudigd. Andersom gaven ook alle generieke security leveranciers aan geïnteresseerd te zijn in CADI. Sommige partijen gaven aan zelf eventueel CADI-tooling te willen ontwikkelen, maar ook het overnemen van een bestaande CADI-leverancier werd als optie genoemd.

Operational technology (OT) loopt op security- en CADI-gebied achter. Hoewel enkele leveranciers aangaven hierin wel geïnteresseerd te zijn, had geen van de geïnterviewde CADI-leveranciers ook maar enige ervaring met klanten in het OT-domein. Omdat OT een kleinere markt vormt dat IT, met extra uitdagingen, is er voor de CADI-leveranciers geen business incentive. Ook vanuit expertise van TNO-collega's en uit de workshop kwam er naar voren dat er op OT nog veel uitdagingen liggen.
Dit zorgt voor grote uitdagingen op het OT-vlak, waarover ook binnen TNO nog beperkte kennis opgebouwd is. Dit betekent dat er weinig kennis is over hoe groot de PQC-migratie uitdaging voor het OT-domein is, welke specifieke operationele uitdagingen daarbij komen kijken, en wat voor specifieke karakteristieken CADI-tooling zou moeten hebben om voldoende cryptografische assets te vinden. Bijvoorbeeld; uit gesprekken en kennis die deze onderzoekers én TNO collega's hebben gehad, blijkt dat veel OT-technologie eigendomsrechtelijk beschermd is. Omdat er geen inzicht is in de source-code of hoe de protocollen in OT precies worden uitgevoerd, wordt het inzetten van een CADI-tool onmogelijk. Er moet dus wil zijn vanuit de OT-leveranciersmarkt om met dit probleem om te gaan. Dit staat in de weg van de ontwikkeling van soortgelijke onafhankelijke CADI-tooling.

Er zijn in bredere zin uitdagingen rondom asset management. Voor de inzet van een MVP in een organisatie is het nuttig om te weten waar de kroonjuwelen zich bevinden. Op die manier is er een prioritering om de CADI-tool in te zetten. Tijdens de workshop bleek echter dat verschillende organisaties niet weten waar de eigen kroonjuwelen zijn. Organisaties zijn afhankelijk van goed assetmanagement, om inzichtelijk te maken waar de kroonjuwelen zich bevinden, en daarmee een prioritering te krijgen voor de inzet van een CADI-tooling. Zelfs voor de start met een MVP, waarvoor ten minste een deel van de assets van de kroonjuwelen goed inzichtelijk moet zijn, kan dit een knelpunt vormen. Zonder dit minimale beeld kan er dus niet begonnen worden, hetgeen de algehele adoptie van dergelijke tooling in de weg kan zitten. Dergelijke afhankelijkheid van goed asset management heeft dus een nadelig effect op adoptie van CADI-tooling, en daarmee marktstimulatie.

[6] Text - H.R.7535 - 117th Congress (2021-2022): Quantum Computing Cybersecurity Preparedness Act | Congress.gov | Library of Congress

8 Advies

Werk intensief samen met het bestaande OT-stakeholderlandschap. Uit de workshop en interviews in dit rapport werd duidelijk dat de OT écht een heikel punt is. Een groot gedeelte van de Nederlandse vitale infrastructuur is afhankelijk van veilige OT. OT-omgevingen worden steeds meer verbonden wordt met het internet[7]. Kwetsbaarheden in OT zijn erg aantrekkelijk voor *advanced persistent threats* (APTs) en zullen in toenemende mate worden uitgebuit.
Uit dit onderzoek is gebleken dat voor veel CADI-tooling OT een blinde vlek is. Er is geen marktprikkel voor CADI-leveranciers om hun tool uit te breiden naar OT. De uitdagingen die de CADI-leveranciers hier ondervinden is echter niet cryptografie-specifiek en worden breder gevoeld bij generieke security-leveranciers. Er is nog veel te winnen op het gebied van OT-beveiliging. Cryptografie biedt voor veel van deze OT-toepassingen een sterk verdedigingsmiddel. Er wordt door verschillende partijen onderzoek gedaan op het gebied van OT beveiliging. Dit moet verder gestimuleerd worden en het CADI-onderzoek moet hierop aangehaakt worden.
Middels samenwerking met het bestaande stakeholderlandschap van QvC Rijk kunnen hier concrete stappen voorwaarts worden gedefinieerd. Dat biedt een kans om het gat van CADI-tooling voor OT te dichten.
Relevant voor

- *NCSC: in samenwerking met hun relaties met beheerders kritieke infrastructuur,*
- *CIO-Rijk: in het aanjagen van bijvoorbeeld Rijkswaterstaat om hierin een leidende rol te nemen*

Faciliteer in het bepalen van een ground truth rondom nauwkeurigheid. QvC Rijk heeft een unieke positie en stakeholderlandschap, om in samenwerking tot een CADI-competitie te komen. Deze CADI-competitie zal een ground truth nodig hebben, namelijk alle cryptografie die in de testomgeving is geïmplementeerd, waaraan partijen zich kunnen meten.

Hoewel dit niet zonder kosten komt, is dit dé manier voor het rijk om invloed en sturing te geven aan commerciële oplossingen en hun nauwkeurigheid. Door hiermee de markt te stimuleren zullen uiteindelijke grootschalige migraties goedkoper zijn. Dit weegt ruimschoots op tegen de kosten van een dergelijke competitie. Omdat QvC Rijk internationaal goed aangeschreven staat, kan zij in samenwerking met andere verbanden of organisaties met een dergelijke status een goed onderschreven competitie neerzetten. CADI-leveranciers hebben tijdens de interviews al aangegeven hier aan mee te willen doen, omdat ze zelf niet over een dergelijke objectieve omgeving beschikken en er nu dus niets is om hun resultaten aan te refereren. Het dient voor hun dus ook als een verkooppunt als ze hier goed uit de test komen.
Relevant voor QvC Rijk, NCSC, BZK, en EZ: in het gebruik maken van hun huidige internationale positie als voorlopend overheidsinitiatief op dit gebied.

Verbeteren van inzicht in kroonjuwelen. Inzicht in de kroonjuwelen bevordert de inzet van CADI-tools binnen organisaties, maar ook beveiliging in het algemeen. Dit is niet een randvoorwaarde, maar wel een pré.

[7] Het Cybersecuritybeeld Nederland 2023, zie Cybersecuritybeeld Nederland 2023 | Rapport | Rijksoverheid.nl.

Start met een (MVP) oplossing. Niet elke CADI-oplossing is even geschikt voor een grootschalige implementatie, maar wel is elke CADI-oplossing in staat om een eerste risico-inzicht te verschaffen. Grootschalige implementaties van CADI-tooling zullen niet goedkoop zijn en hier is ondersteuning vanuit management voor nodig. Deze ondersteuning komt er alleen als er een duidelijk risico voor de organisatie is. Dit risico is alleen te kwantificeren middels een eerste inventaris, het liefst op een selecte high-impact scope van de organisatie. Dit is te doen met elke oplossing die we hebben geïnterviewd, en wordt soms al als dienst aangeboden. Wacht niet op de ideale oplossing, en loop zodoende op de organisatorische uitdagingen vooruit. Zelfs als er geen totaalbeeld is van de 'kroonjuwelen', is het goed om met het bekende deel ervan tijdig te beginnen.
Relevant voor alle organisaties, zowel publieke als private organisaties.
*Afhankelijk van "Verbeteren **van inzicht in** kroonjuwelen".*

Belang van scope van aanbesteding. Zoals beschreven onder sectie 5.1.3 heeft de wens vanuit de eindgebruiker invloed op de kwaliteit en scope van de CADI-tool. Omdat er momenteel geen betrouwbare indicator is van de nauwkeurigheid van de CADI-tools, is deze wens moeilijk te definiëren en achteraf te valideren dat deze is volbracht. We adviseren dat een tender voor grootschalige implementatie van CADI-tooling óók een servicecomponent voor interpretatie of definitie van migratie-actie bevat, zodat de verantwoordelijkheid van een lage nauwkeurigheid bij de serviceleverancier ligt. We benadrukken hier nogmaals het advies rondom de ground truth, welke hierboven is beschreven.
Relevant voor alle grote eindgebruikers, in het bijzonder overheidsorganisaties, omdat er binnen initiatieven zoals QvC Rijk een grote focus is op PQC.

Stimuleer aanbestedingen. (CADI-)leveranciers hebben marktprikkels nodig om verder te ontwikkelen en verbeteren. Het is niet de vraag óf deze markt groot wordt, maar wanneer. Waar deze markt geografisch groeit, is wel bepalend voor hoe de toekomstige ontwikkelingen zich zullen ontvouwen. Hier is een kans voor QvC Rijk, aangezien dit verband reeks een hoge volwassenheid en sterke focus heeft op PQC. Zie ook bovenstaand advies.
Relevant voor QvC Rijk.
Afhankelijk van "Belang van scope van aanbesteding".

Werk aan compliance. De reden dat de VS voorop loopt met CADI-tooling is dat er een wet is die van federale instanties een start met CADI vorderde. Het is bekend dat dit een uitdaging is in Europa. Het helpt om hier tijdig mee te beginnen, omdat de markt compliancy-driven is.
Relevant voor QvC Rijk.

Haak vervolgonderzoek aan bij ander BOM-onderzoek. De uitdagingen van Cryptographic Bill of Materials (CBOM) zijn niet uniek voor alleen CBOMs. Soortgelijke technieken worden onderzocht om andere typen assets te vinden. Het lijkt TNO zonde om geen gebruik van deze technologische basis te maken door de scope in (bestaand) BOM-onderzoek te verbreden, omdat we dan het wiel opnieuw zouden uitvinden. Dit is zeker het geval voor de OT.
Relevant voor alle betrokken partijen.

Wees spaarzaam met aandacht voor het dichten van de gap met de ideale CADI-tool voor de IT en focus op OT. Sommige van de CADI-oplossingen zijn al dicht bij het ideaal. Waar ze dit nog niet zijn, zijn ze al goed op weg en komen ze hierop via een stimulans vanuit de markt. Deze stimulans, namelijk de compliancy, alsmede de ground truth is al een eerder genoemd advies, waarna de bestaande gaps zich naar verwachting vanzelf oplossen. Dit is, volgens TNO en zoals besproken tijdens de workshop, niet het geval voor de OT, waar

de gaps overbruggen een grote uitdaging wordt, en waar juist meer aandacht voor moet zijn, omdat de markt deze prikkel momenteel nog niet veroorzaakt. Door aan te haken bij onderzoek naar breder OT beveiliging en BOM, zullen de OT uitdagingen (eigendomsrechten, legacy en rekenkracht-limitaties, zie sectie 3.4) die CADI-leveranciers momenteel ondervinden opgelost worden. Dit verlaagt de drempel voor CADI-leveranciers om deze markt te betreden en daarmee goede CADI-tooling te ontwikkelen.
Relevant voor QvC Rijk, NCSC, BZK, en EZ.
Afhankelijk "Faciliteer in het bepalen van een ground truth rondom nauwkeurigheid" en "Werk aan compliance".

Doe onderzoek naar evaluatiecriteria. CADI-tooling zou idealiter worden geëvalueerd op basis van een gestandaardiseerde set van eisen. Wellicht kan er een standaardframework of reeks aan eisen worden opgesteld waaraan CADI-tools getest kunnen worden. Dit vereist echter wél een bestaande ground truth, zoals eerder geadviseerd. Dit advies ligt daarmee iets verder in de toekomst. Het kan ook hand-in-hand gaan met compliancy, bijvoorbeeld doordat organisaties alleen gecertificeerde CADI-tools mogen gebruiken.
Relevant voor EZ en BZK.
Afhankelijk "Faciliteer in het bepalen van een ground truth rondom nauwkeurigheid".

Bijlage 1 – Samenvatting workshop

Opzet workshop

De workshop vond plaats op 24 september in het conferentiecentrum ZZIIN in Den Haag. De aanwezige groep was zeer gemengd. Zo waren er stakeholders van Rijksoverheid, maar ook uit het bedrijfsleven. Bovendien waren een aantal aanwezigen technische experts, terwijl anderen meer op beleid gericht waren.

In het eerste deel werd er een serie vragen over praktische eisen aan CADI-tooling gesteld. Deze vragen/eisen waren opgesteld op basis van het literatuuronderzoek. Per vraag zijn de antwoorden van de deelnemers verzameld en zijn eventuele opvallende overeenkomsten of verschillen bediscussieerd. In het tweede deel van de workshop werden de deelnemers in groepen verdeeld en werd er in een losser format gesproken over CADI en de bijbehorende uitdagingen.

Hieronder volgt eerst een overzicht van de gestelde vragen en de ontvangen antwoorden. Daarna volgen een aantal observaties die gebaseerd zijn op discussie tijdens de vragen en de notities van de groepen in het tweede deel van de sessie.

Vragenlijst functionele eisen

Hieronder volgen de vragen zoals deze tijdens de workshop gesteld zijn. Er werd steeds een vraag op het scherm geprojecteerd, waarbij de deelnemers uit een aantal opties konden kiezen (meerdere opties aanvinken was ook mogelijk). De antwoorden werden verzameld via Mentimeter[8].

Per vraag is steeds in **blauw gemarkeerd** welk antwoord het meeste voorkwam (of welke antwoorden, als het dicht bij elkaar lag). Eventuele andere discussiepunten staan waar relevant onder de vraag toegelicht.

Integreerbaarheid. Moet een tool met CADI-functionaliteit makkelijk geïntegreerd kunnen worden met andere generieke cybersecurity tooling?

A. De CADI-functionaliteit moet aangeboden worden binnen de bestaande tooling die we al hanteren en ik vind het niet erg daar een aantal jaren op te wachten.
B. Ik zie de CADI-functionaliteit het liefst in mijn bestaande tooling, maar daarvoor moet ik het risico eerst afschatten. Ik kan daarvoor ook een (tijdelijke) tool accepteren, zolang deze maar exporteert naar mijn bestaande tooling.
C. **Ik kan prima overweg met nieuwe tooling, zolang die maar exporteert naar mijn belangrijkste managementtools.**
D. Ik kan prima overweg met nieuwe tooling, ook als deze niet exporteert.

[8] https://www.mentimeter.com/: Interactive presentation software

E. Ik zou een eenmalige scan met een tool nodig hebben voordat ik weet wat mijn risico is en daarmee hoe ik deze vraag kan beantwoorden.
F. Ik wil CADI en generieke cybersecurity-oplossingen compleet los zien van elkaar.
G. Anders, dat licht ik graag mondeling toe.

Volledigheid informatie. Hoe belangrijk is het om *alle* cryptografische assets in beeld te hebben? Binnen welke belangrijke plekken moeten crypto assets gevonden worden? Welke plekken zijn minder belangrijk om te bekijken?

A. Alle crypto assets moeten gevonden kunnen worden. Ik wil heel mijn systeem in kaart gebracht hebben, inclusief de crypto assets van mijn externe producten.
B. Alleen operationele devices, applicaties en netwerken hoeven gescand te worden. Testsystemen of niet-gebruikte systemen vallen buiten scope.
C. Alleen de crypto assets voor communicatie met de buitenwereld moeten gevonden kunnen worden.
D. Anders, dat licht ik graag mondeling toe.

Informatief vermogen. Welke diepgang moet een tool hebben? E.g. Hoe inzichtelijk zijn het resultaat, visualisaties en het inzichtelijk hebben van kruisverwijzingen?

A. Er moet een makkelijke zoekfunctie zijn binnen de tool.
B. Als ik het makkelijk aan systemen kan koppelen via een export, dan kan ik met mijn bestaande tooling al zien hoe systemen van elkaar afhangen.
C. Ik zou het fijn vinden om grafisch te zien welke crypto er is, en hoe deze van elkaar afhangt.
D. Ik wil voldoende inzicht in een (crypto) asset, zodat ik gemakkelijk handmatig de correctheid van het resultaat kan bevestigen.
E. Als het nodig is, zoek ik met alle plezier zelf door een Excel-export, zolang ik maar weet in welk systeem/applicatie wat zit.
F. Ik wil makkelijk kunnen zien welke crypto assets anders zijn ten opzichte van de vorige scan.
G. Anders, dat licht ik graag mondeling toe.

Support. Hoeveel support heb je nodig bij een nieuwe tool, of functionaliteit in de bestaande tooling?

A. Mijn huidige servicelevel bevalt uitstekend!
B. We willen het helemaal zelf kunnen beheren, met eventueel een technisch consult als we er niet uit komen. We verwachten wel (security-)updates, maar geen feature-updates.
C. We beheren het meeste zelf, maar willen wel (security-)updates, feature-updates, en worden graag ontzorgd vanuit de leverancier als het niet goed gaat.
D. Anders, dat licht ik graag mondeling toe.

Toegang. Wat voor toegang wil je dat een tool heeft op jullie omgeving?

A. De tool mag overal systeem access toe hebben in de productieomgeving, maar ik bepaal zelf waar en wanneer de tool functioneert. Ik wil de tool niet 'los' laten op mijn omgeving.
B. De tool mag kernel-level toegang krijgen tot mijn systemen.
C. De tool mag overal systeem access toe hebben, maar niet in de productieomgeving.
D. Ik wil zelf bepalen welke netwerkdomeinen worden gemonitord én wanneer. Daarnaast wil ik zélf de deployment van eventuele scanning-agents op (virtuele) systemen kunnen bepalen.
E. De tool mag overal bijkomen volgens de keuzes gemaakt door de tooling leverancier.

F. De tool mag ook naar een cloud opslag, of in een SaaS-model, resultaten wegschrijven naar de leverancier.
G. De tool mag alleen lokaal resultaten wegschrijven. Ik wil geen gegevens buiten mijn eigen omgeving hebben.
H. De tool moet offline kunnen werken.
I. Anders, dat licht ik graag mondeling toe.

Toevoeging: dit verschilt ook per (sub)tool. Offline is met name belangrijk voor OT.

Logging. Wat moet er allemaal gelogd worden?

A. De resultaten van een scan.
B. Waar, wanneer, en welke scan er is uitgevoerd.
C. Foutmeldingen als een scan niet uitgevoerd heeft kunnen worden en waarom.
D. Onverwachte wijzigingen als een systeem opnieuw gescand is.
E. Anders, dat licht ik graag mondeling toe.

Betrouwbaarheid leverancier. Kunnen we vertrouwen op de leverancier?

A. Er moet een duidelijke overeenkomst opgesteld worden met de leverancier, met mogelijkheid tot specificaties van mijn situatie, ik wil niet een standaard overeenkomst.
B. Als de standaard overeenkomst van de leverancier voldoet aan mijn security eisen en wettelijke verplichtingen, dan is dat prima.
C. De leverancier moet een Nederlandse partij zijn.
D. De leverancier moet op zijn minst binnen de EU zijn.
E. De leverancier moet een van onze huidige generieke security tool leveranciers zijn.
F. Anders, dat licht ik graag mondeling toe.

Toevoeging: dit kan wel complex zijn voor multinationals, als er verschillende eisen zijn.

Continuïteit & back-up. Welke eisen stellen we aan de continuïteit van de tool?

A. Geen, ik beheer hem zelf, en sla de resultaten en instellingen zelf op. Het is dus mijn eigen verantwoordelijkheid.
B. Ik verwacht de tool niet vaak te gebruiken, als hij een weekje niet beschikbaar is, is dat geen probleem, een maand wordt lastig.
C. Ik verwacht de tool intensief te gaan gebruiken, dus hij moet er niet meer dan een dag tot een week uitliggen.
D. Ik verwacht deze tool maar 1 of 2 keer per jaar te gebruiken, dan moet hij beschikbaar zijn.
E. Ik wil geen resultaten kwijt raken en er moet een dagelijkse of betere back-up optie zijn.
F. Ik wil maximaal 1 week werk over moeten doen, en de back-ups moeten dat reflecteren.
G. Ik exporteer gegevens eigenlijk direct en laat het niet in het platform staan, dus een back-up functionaliteit lijkt me overbodig.
H. Anders, dat licht ik graag mondeling toe.

Systeem capaciteitsbehoefte. Welke impact heeft het runnen van de tool op andere systemen en applicaties?

A. Ik wil niet al te zware systeem requirements hebben, maar ik ben voornemens hem niet op productie te draaien, dus mijn medewerkers merken weinig impact.
B. Ik wil een duidelijk beeld, dus draai ik de tool op productie, ik wil nergens meer dan 10% extra capaciteit nodig hebben.

C. Ik wil een duidelijk beeld, dus draai ik de tool op productie, ik wil nergens meer dan 30% extra capaciteit nodig hebben.
D. **Zolang mijn kern bedrijfsprocessen maar niet verstoord worden. Ik ga dit zelf uitzoeken als ik de tool heb en daar een eigen weg in vinden.**
E. Anders, dat licht ik graag mondeling toe.

Toevoeging: capaciteit is vaak niet zo'n probleem, maar vooral problematisch voor OT.

Exports. Moet je de ruwe data kunnen exporteren? Zo ja, in welk bestandstype?
A. Het bestandstype moet JSON zijn.
B. **Het bestandstype maakt niet, zolang het maar een breed gebruikt en erkend type is. (e.g. JSON, CSV, TSV, XML, HTML, etc).**
C. Anders, dat licht ik graag mondeling toe.

Observaties en conclusies

Hieronder volgen de belangrijkste observaties en conclusies die naar voren kwamen tijdens de workshop, zowel tijdens de plenaire vragensessie als in de discussie in groepen.

- Het ontbreekt in veel organisaties nog aan awareness: waarom is CADI nodig? Dit speelt zowel bij developers als bij management.
- Er lijkt een kip-ei probleem te zijn rondom crypto-inventarisatie (en crypto-migraties). Tooling kost geld, daar is een risicoanalyse voor nodig, maar daar is weer de tooling voor nodig.
    - De risicoanalyse hoeft niet meteen compleet/perfect te zijn om management-buy-in te creëren; een onvolledig resultaat is óók een goed begin.
- Er is een groter probleem rondom *asset management*. Sommige organisaties hebben een grote volwassenheid wat betreft overzicht op welke assets ze allemaal draaien, maar dat geldt niet voor iedereen. Ook is er geconcludeerd dat er geen goed dataformat bestaat dat crypto-, hardware-, en software-asset management omvat. Hierdoor ontbreekt er overzicht.
- Er bestaan al deeloplossingen die praktisch inzetbaar zijn, bijvoorbeeld rondom CI/CD pipelines. Maar de uitkomsten daarvan worden nergens geaggregeerd en er is daardoor geen overzicht.
- Tools kunnen in eigen beheer, en een tool moet on-premise/lokaal kunnen draaien, met goede (automatische) export mogelijkheden.

Bijlage 5 – Zoektermen

Tijdens de eerste fase van het onderzoek is er middels desk research gezocht naar beschikbaar materiaal. Hierin zijn in de eerste instantie de volgende termen gebruikt. Vervolgens is er op basis van de zo verkregen bronnen verder gezocht/geklikt.

“cryptographic assets discovery”
“cryptographic assets in organisations”
“crypto(graphy) identification method (scanner)”
“crypto(graphy) scanner”
“cryptography tracer”
“cryptographic discovery”
“cryptographic risk management”
“quantum risk management”
“cryptographic asset management”
“(automated) identify cryptographic vulnerabilities”
“automated cryptographic discovery and inventory” / “ACDI tooling”
“cryptography management (platform)”
“network analyzer cryptography”
“application analyzer cryptography”
“filesystem analyzer cryptography”
“cryptography discovery scanner”
“public key application discovery tools”
“cryptography scanning”