CMDB en Tooling in de PA/OT/IACS

Hoe kan (security) tooling helpen een CMDB op te zetten en te onderhouden

www.securitydelta.nl/ipcs

IPCS
INDUSTRIEEL
PLATFORM
CYBER SECURITY

Revisie

datum	naam	revisie
10-apr-2025	Ron Perrier	Eerste IPCS (HSD) uitgave, Q2-2025
11-apr-2025	Marcel Jutte	QC en contactinformatie geactualiseerd

Wat is een CMDB?

Een ‘asset register’ is een overzicht van alle systemen die met uw netwerk verbonden zijn. Dat klinkt niet al te moeilijk, maar is het vaak wel. Er is namelijk veel méér aan een netwerk gekoppeld dan in eerste instantie gedacht wordt.

Een stap verder is het doorgroeien van een asset register naar een CMDB (Configuration Management Database). In een CMDB kan naast de informatie over de assets ook de relaties tussen assets worden vastgelegd.

Zowel bij het opzetten van een asset register of een CMDB als bij het up-to-date houden daarvan geniet het de voorkeur gebruik te maken van tooling die daarbij helpt.

Waarom willen we een CMDB?

Een *up-to-date* CMDB, is van groot belang om wijzigingen, incidenten en storingen te kunnen beheersen en tijdig en gedetailleerd de diverse (preventieve) onderhoudstaken te kunnen plannen.

Hoe ziet een CMDB eruit?

De componenten die in een CMDB zijn opgenomen noemen we ‘assets’. Deze assets zijn onderverdeeld in assettypen en deze hebben elk (meerdere) attributen. Dit kunnen zowel hardware als software attributen zijn. In tabel 1 is een voorbeeld (referentie) weergegeven hoe een CMDB er idealiter eruit zou kunnen zien, onderverdeeld in assettypen en attributen.

Tabel 1:Referentie CMDB

Assettypen + Attributen	
Computer hardware (servers, werkstations);	**Virtualisatie software;**
○ Fysieke locatie;	○ Producent;
○ Producent;	○ VM naam;
○ Productnaam;	○ VM type;
○ Type;	○ Host type
○ Model;	○ Functie;
○ Datum van aanschaf;	○ Custodian;
○ OS-versie;	○ Verantwoordelijke organisatie.
○ Patchlevel;	**Besturingshardware (PLC, controllers, i/o, RTU, IED, HMI);**
○ Datum laatste backup;	○ Locatie;
○ Backuplocatie;	○ Producent;
○ CPU informatie	○ Productnaam/type;
○ RAM geheugeninformatie;	○ Datum van aanschaf;
○ Opslagmedia informatie;	○ Firmareversie;
○ Firmwareversie;	○ Datum laatste backup;
○ Asset ID;	○ Backuplocatie;
○ Device type;	○ Verantwoordelijke organisatie.
○ Serie nummer;	**Besturingssoftware**
○ Function;	○ Locatie;
○ Netwerk interface(s);	○ Operating System naam/type;
○ Netwerk adress (L2 MAC, L3 IP);	○ Version;
○ Verantwoordelijke organisatie	○ Function;
Programmatuur (applicaties, antimalware);	○ Custodian;
○ Locatie;	○ Verloopdatum licentie;
○ Systeemnaam;	○ Verantwoordelijke organisatie.
○ Producent;	**Database**
○ Productnaam/type;	○ Locatie;
○ Softwareversie;	○ Systeemnaam;
○ Datum van ingebruikname;	○ Producent;
○ Datum laatste update;	○ Productnaam/type;
○ Verloopdatum licentie;	○ Softwareversie;
○ Verantwoordelijke organisatie.	○ Datum van ingebruikname;
Documentatie (ontwerpen, handleidingen);	○ Datum laatste update;
○ Documentlocatie;	○ Verloopdatum licentie;
○ Systeemnaam;	○ Verantwoordelijke organisatie.
○ Type document;	**Applicatie Protocollen**
○ Documentversie;	○ SNMP
○ Aanmaakdatum;	○ PING
○ Datum laatste wijziging;	○ IEC xx

Hoe leg ik een CMDB aan?

De effort die het aanleggen van een CMDB vraagt is natuurlijk sterk afhankelijk van de omvang van de IT/OT infrastructuur. Ook maakt het daarbij veel uit of het gaat om nieuw aan te leggen systemen of reeds bestaande (operationele) systemen.

Tabel 1 geeft een zeer uitgebreide CMDB weer die men in de ideale situatie zou willen hebben. Deze noemen we dan ook de ‘Referentie CMDB’.

Bij aanleg van een nieuw systeem is het natuurlijk veel eenvoudiger om alle benodigde informatie te verzamelen. Al bij het ontwerp-, inkoop- en implementatieproces kunnen in dit geval de benodigde gegevens al worden opgeslagen.

Bij bestaande infrastructuren moeten deze gegevens achteraf worden opgehaald, vaak uit lopende operationele systemen. Het is zo goed als onmogelijk om alle genoemde deze informatie uit een (bestaand) systeem op te halen, en zeker niet in 1 keer.

Daarom wordt geadviseerd om de CMDB gefaseerd aan te leggen. Dit kunnen we doen door de op te halen informatie volgens het “MoSCoW” principe te prioriteren in:

- Prio 1: Must Have ;
- Prio 2: Should Have; en
- Prio 3: Could Have.

In tabel 2 t/m 4 is een voorbeeld opgenomen hoe de prioritering van de in tabel 1 aangegeven CMDB er uit zou kunnen zien. Let wel: de prioriteit van de benodigde informatie wordt aangegeven door de systeemeigenaar/-beheerder. De getoonde tabellen dienen daarom ook zuiver als voorbeeld. De kolommen H, P en A geven aan hoe de informatie wordt verzameld; dit wordt hieronder in detail uitgelegd.

Tabel 2: Prio 1 - Must-Haves

Assettypen + Attributen	Ophalen		
Computer hardware (servers, werkstations)	**H**	**P**	**A**
o Fysieke locatie	×		
o Producent	×	×	×
o Productnaam	×		
o Type	×		×
o Model	×		
o OS-versie	×		×
o Firmwareversie	×		×
o Serienummer	×		
o Netwerkadres (L2 MAC, L3 IP)		×	×
Programmatuur (applicaties, antimalware)	**H**	**P**	**A**
o Locatie	×		
o Systeemnaam	×		
o Producent	×		
o Softwareversie	×		
o Datum laatste update	×		
Virtualisatie software	**H**	**P**	**A**
o VM naam	×		
o VM type	×		
o Functie	×		
Besturingshardware (PLC, controllers, i/o, RTU, IED, HMI)	**H**	**P**	**A**
o Locatie	×		
o Producent	×	×	×
o Firmareversie	×	×	×
Besturingssoftware	**H**	**P**	**A**
o Locatie	×		
o Operating System naam/type	×	×	×
o Versie	×		×
o Functie	×		
Database	**H**	**P**	**A**
o Locatie	×		
o Systeemnaam	×		

Assettypen + Attributen	Ophalen		
Computer hardware (servers, werkstations)	**H**	**P**	**A**
o Softwareversie	×		
Applicatieprotocollen	**H**	**P**	**A**
o SNMP		×	
o PING		×	
o IEC xx		×	

Tabel 3: Prio 2 - Should-Haves

Assettypen + Attributen	Ophalen		
Computer hardware (servers, werkstations)	**H**	**P**	**A**
o Patchlevel	×		×
o Asset ID	×		
o Device type	×	×	×
o Functie	×		
o Verantwoordelijke organisatie	×		
Programmatuur (applicaties, antimalware)	**H**	**P**	**A**
o Productnaam/type	×		
o Verloopdatum licentie	×		
o Verantwoordelijke organisatie	×		
Documentatie (ontwerpen, handleidingen)	**H**	**P**	**A**
o Documentlocatie	×		
o Systeemnaam	×		
o Type document	×		
o Documentversie	×		
Virtualisatie software	**H**	**P**	**A**
o Producent	×		
o Host type	×		
o Verantwoordelijke organisatie	×		
Besturingshardware (PLC, controllers, i/o, RTU, IED, HMI)	**H**	**P**	**A**
o Productnaam/type	×	×	×
o Datum laatste back-up	×		
o Back-uplocatie	×		
o Verantwoordelijke organisatie	×		
Besturingssoftware	**H**	**P**	**A**
o Verloopdatum licentie	×		
o Verantwoordelijke organisatie	×		
Database	**H**	**P**	**A**
o Producent	×		
o Productnaam/type	×		
o Verloopdatum licentie	×		
o Verantwoordelijke organisatie	×		

Tabel 4: Prio 3 - Could-Haves

Assettypen + Attributen	Ophalen		
Computer hardware (servers, werkstations)	**H**	**P**	**A**
o Datum van aanschaf	×		
o Datum laatste back-up	×		
o Back-uplocatie	×		
o CPU informatie	×		
o RAM geheugeninformatie	×		
o Opslagmedia informatie	×		
o Netwerk interface(s)		×	×
Programmatuur (applicaties, antimalware)	**H**	**P**	**A**
o Datum van ingebruikname	×		
Documentatie (ontwerpen, handleidingen)	**H**	**P**	**A**
o Aanmaakdatum	×		
o Datum laatste wijziging	×		
Virtualisatie software	**H**	**P**	**A**
o Verantwoordelijke organisatie	×		
Besturingshardware (PLC, controllers, i/o, RTU, IED, HMI)	**H**	**P**	**A**
o Datum van aanschaf	×		
Besturingssoftware	**H**	**P**	**A**
o Verantwoordelijke organisatie	×		
Database	**H**	**P**	**A**
o Datum van ingebruikname	×		
o Datum laatste update	×		

Ophalen van CMDB-informatie

Er bestaat helaas geen methode of tool om alle informatie over assets in één keer op te halen. Er is een combinatie nodig van diverse methodieken. We onderscheiden hierin:

- Handmatig verzamelen (H);
- Passief scannen (P);
- Actief scannen (A).

Handmatig verzamelen

Bij het handmatig verzamelen van de informatie gaan we alle assets langs en noteren we de benodigde informatie. Dit heeft natuurlijk niet de voorkeur omdat dit erg tijdrovend is en foutgevoelig. Maar sommige informatie is niet of nauwelijks automatisch op te halen, denk daarbij bijvoorbeeld aan de fysieke locatie (objectadres, kastnummer, enz.).

Voordelen handmatig ophalen:

1) Er vindt meteen een visuele check plaats van de assets;
2) Afwijkingen zullen eerder worden waargenomen.
3) Vaak de enige mogelijkheid om bepaalde informatie op te halen die niet met scantools kan worden verzameld.

Nadelen handmatig ophalen:

1) Tijdrovend;
2) Saai, herhalend werk dat snel kan leiden tot fouten.

Passief netwerk scannen

Bij passief scannen wordt netwerkverkeer op strategische plaatsen in het netwerk afgetapt middels “SPAN” (of “mirror”) poorten, en de informatie uit het netwerkverkeer als input gebruikt voor geschikte tooling. Deze techniek wordt ook wel aangeduid als “Network Security Monitoring’ (NSM).

Als voorbeeld is een NSM tool in staat uit sommige protocollen een aantal parameters op te halen, zoals firmwareversie en systeeminstellingen. Daarnaast wordt automatisch een zogenaamde “connectivity matrix” opgebouwd: wie communiceert met wie, en met welk protocol.

Voordelen passief scannen:

1) Technische implementatie relatief eenvoudig. Alleen SPAN ports zijn nodig plus connectie mogelijkheden voor de DPI tool
2) Gebruiksgemak
3) Geen **OEM** toestemming noodzakelijk (want er is geen invloed op de operatie)
4) Snel inzicht in bestaand netwerk conform het Purdue model
5) In-depth protocolanalyse op procesparameters
6) Gedetailleerde detectieregels mogelijk op basis-procesparameters en systeemgedrag
7) Analyse vrijwel 100% protocol onafhankelijk
8) Protocol manipulatie zoals “Man In The middle” attack makkelijk te detecteren

Nadelen passief scannen:

1) 100% inzicht is lastig in oudere netwerken door beperking van technische mogelijkheden
2) Inzicht in details van patch levels niet mogelijk
3) Inzicht in het OS van endpoints is beperkt
4) Asset manipulatie is moeilijk detecteerbaar
5) Inzicht in het analoge deel (I/O) van een OT netwerk lastig

Actief netwerk scannen

Bij actief scannen wordt gebruik gemaakt van de query mogelijkheden zoals die vaak geboden worden door systeem-specifieke protocollen. De volgende ‘commands’ worden bijvoorbeeld veel gebruikt voor het ophalen van asset gegevens:

1) Directory info
2) System Info
3) Blocks move
4) PLC Control
5) Date and Time

6) Security
7) Programming

Daarnaast kunnen actieve tools systeemgegevens vanuit engineering-tools opvragen en combineren in het asset register. Een toevoeging op actief netwerk scannen is het toevoegen van “Detectie Agents” op de endpoints.

Voordelen actief scannen:

1) Asset register bevat veel details
2) Gebruiksgemak
3) Alle owners bereikbaar middels het protocol worden geregistreerd. Het is niet afhankelijk van netwerkbeperkingen
4) Inzicht in patch levels geeft meer details
5) Inzicht in het OS van endpoints geeft meer details. Bij gebruik van “Detectie Agents” is het detail niveau nog beter
6) Asset manipulatie is goed detecteerbaar

Nadelen actief scannen:

1) Analyse is protocolspecifiek.
2) In een multivendor omgeving is meer toolconfiguratie nodig
3) OEM toestemming noodzakelijk
4) OEM toestemming bij het gebruik van “detectie agents” vaak moeizaam
5) Installatie moet door specialisten gebeuren
6) Protocol manipulatie zoals “Man In The Middle” attack moeilijker te detecteren

Conclusie

Alle methodes hebben verschillende mogelijkheden, elk met eigen voor en nadelen. De informatie uit deze methodes van scannen is in praktijk licht overlappend en zeker aanvullend op elkaar.

De makkelijkste methode om een asset register op te bouwen is met een passieve tool. Gemiddeld genomen is na een week scannen op de strategische plekken in een netwerk een 90% inzicht mogelijk op de meer moderne netwerken. Zeer oude netwerken, welke vaak met seriële communicatie-protocollen werken, zijn echter lastig of slecht inzichtelijk te maken met passief scannen.

Actief scannen effectief inrichten geeft meer details maar is bewerkelijker en zal altijd in overleg moeten gebeuren met de verantwoordelijke voor het correct functioneren van een site en de OEM.

Belangrijke aandachtspunten bij aanleg en beheer van een CMDB

Het aanleggen van een CMDB is een hele klus, maar eenmaal ingericht is het zeer waardevol. Het beheer van de informatie in de database is van minimaal even groot belang als het aanleggen ervan. Zo moeten er om de CMDB heen een aantal processen zijn ingericht om de CMDB up-to-date te

houden en eenmaal per jaar te controleren. Ook bij de controle van de inhoud van een CMDB kunnen scantools van grote waarde zijn.

- Bij de start van een CMDB: begin klein
- Breid later op behoefte (nut en noodzaak) de hoeveelheid data uit
- Houd bij welke data de scantools kunnen controleren/welke niet
- Bepaal frequentie van controle, bijvoorbeeld elk half jaar automatisch, en elk jaar de rest handmatig.
- Beoordeel met regelmaat of de handmatige items wel noodzakelijk zijn
- Scanning mag geen impact hebben op de operatie. Wanneer dit niet te garanderen is, is het wellicht ook mogelijk de operatie stil te leggen en dan de scans uit te voeren, of gebruik een onderhoudsvenster of geplande productiestop voor een scan.
- Na scannen dient de opgehaalde data gecontroleerd te worden op volledigheid en kwaliteit en vergeleken te worden met eventueel al aanwezige gegevens. Hierdoor komen ook de eventuele 'nieuwe' detecties naar voren.
- Een niet-actuele CMDB heeft weinig tot geen waarde, dus is het aanleggen van een CMDB slechts stap 1. Het beheer van de CMDB is een continu proces, dat geborgd zal moeten zijn om de CMDB actueel te houden.

Afkortingen en begrippen

ALARP	As Low As Reasonable Practical
CMDB	Configuration Management Database
Conduit	Dataverbinding tussen twee zones
DCS	Distributed Control System
DMZ	De-Militarized Zone, datasluis.
DPI	Deep Packet Inspection
ERP	Enterprise Resource Planning system
IACS	Industrial Automation and Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IACS	Industrial Automation Control System
IPCS	Industriëel Platform Cyber Security
IT	Information Technology
HAZOP	HAZard and OPerability study
HMI	Human Machine Interface
MES	Manufacturing Execution System
MoSCoW	Must-have, Should have, Could have, Won't/Would have
OEM	Original Equipment Manufacturer
OT	Operational Technology
PA	Process Automation
PLC	Programmable Logic Controller
SCADA	Supervisory Control And Data Acquisition
SIS	Safety Instrumented System
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Centre
SUC	System under Consideration, het te onderzoeken systeem / bedrijfsdeel.
SL-A	Security Level Achieved, het bereikte niveau van beveiliging

SL-T	Security Level Target, het tot doelgestelde beveiligingsniveau
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VDE	Verband der Elektrotechnik Elektronik und Informationstechnik
ZCR	Zone and Conduit Requirements, beschermingseisen gesteld aan gebieden en dataverbindingen

---

Deze publicatie kunt u opvragen via ipcs@securitydelta.nl

Meer info over IPCS via https://securitydelta.nl/ipcs

Dit document is opgesteld door de volgende leden van het Industrieel Platform Cyber Security:

Ron Perrier, Eric ten Bos, Philip Roodzant, Markwin Romijn.

Met dank aan Rob Hulsebos voor het redigeren van de teksten en de overige leden van de 'IPCS werkgroep IEC 62443' voor het reviewen van dit document.

Security Delta (HSD)
Wilhelmina van Pruisenweg 104
2595 AN The Hague
070 204 41 80

info@securitydelta.nl
www.securitydelta.nl