Samen aanjagen van vernieuwing

Handreiking configuratiebeheer

CO.01 & CO.02 SURFaudit toetsingskader

Auteur(s): Ry Boxem & Mick Deben
Versie: 1.0
Datum: 29 januari 2026
Kenmerk: Handreiking configuratiebeheer

Inhoudsopgave

1 Inleiding 3

2 Registreer je assets 4

2.1 Traditionele (on-premise) assets 4
2.2 Cloud assets 4

3 Ontdek en beheer je assets 5

3.1 Actieve vs. passieve detectie 5
3.1.1 Actieve detectie 5
3.1.2 Passieve detectie 5
3.1.3 Detectie met en zonder agent 6
3.2 Automatiseren van detectie 6
3.3 Onbekende assets adresseren 6

4 Ontdek en beheer je software 7

4.1 Software ontdekken 7
4.2 Ongewenste software weren 7

1 Inleiding

De twee statements over configuratiebeheer in het SURFaudit toetsingskader (CO.01 en CO.02) zijn vanuit cybersecurity perspectief enorm belangrijk. Zonder inzicht in alle configuratie-items (CI's) ontstaat een wildgroei van systemen, applicaties of IoT-apparaten die buiten het zicht van IT vallen (schaduw-IT). Dit verhoogt het risico op gebruik van onveilige applicaties, ongeautoriseerde toegang en systemen die niet meegenomen worden in patchrondes. Je kunt namelijk alleen beschermen wat je kent en zonder een actuele CI-lijst en security baseline weet je niet welke systemen kwetsbaar zijn bij nieuwe Common Vulnerability & Exposures (CVE's). Bij incidenten is het essentieel om snel te weten wat waar draait, met welke configuratie en wie de verantwoordelijke is. Zonder juiste en volledige CI-registratie is incident response complexer en tijdrovender, waardoor de impact vrijwel zeker hoger zal uitvallen. Door security baselines te bepalen en toe te passen kun je voorkomen dat ongewenste of onveilige wijzigingen worden doorgevoerd, zie de handreiking security baselines.[1]

De context van educatieve instellingen is uitdagend vanwege de hoeveelheid verschillende gebruikers (studenten, docenten, medewerkers en externen), vrijheid in het gebruik van eigen software voor projecten en onderzoeken, veelvuldig gebruik van BYOD en de altijd beperkte middelen voor IT en cybersecurity.

Wat is vereist voor het derde volwassenheidsniveau?

CO.01 Identificatie en onderhoud van configuratie-items

- Er bestaan geformaliseerde configuratieprocedures en werkmethoden om alle configuratie-items en hun attributen te identificeren en te onderhouden;
- De procedure is in overeenstemming met procedures voor wijzigings-, incident- en probleembeheer;
- De procedure is gedocumenteerd, gestandaardiseerd en gecommuniceerd;
- Er zijn processen geïmplementeerd voor het beheer van aangeschafte, toegewezen, gearchiveerde en verlopen licenties, zodat aan de licentie voorwaarden/afspraken voldaan wordt.

CO.02 Configuratiedatabase en baseline

- Alle middelen en wijzigingen in middelen worden gemonitord en vastgelegd in een centrale repository;
- De relaties tussen configuratie-items worden geïdentificeerd en bijgehouden;
- Een tool voor configuratiebeheer (of gelijksoortige tools) wordt (worden) geïmplementeerd voor alle platforms;
- Er wordt enige automatisering ter ondersteuning gebruikt bij het volgen van wijzigingen in apparatuur en software;
- Configuratie baselines voor componenten worden vastgesteld en gedocumenteerd als benchmark na wijzigingen;
- Wijzigingen in de configuratiedatabase (CMDB) worden geregistreerd.

In deze handreiking bieden we handelingsperspectief om het derde volwassenheidsniveau te bereiken voor beide configuratiebeheer statements.

[1] https://sec.surf.nl/beveiligingsinstellingen-bepalen-en-beheren-met-de-security-baseline/

2 Registreer je assets

Doel: registreren *wat* je hebt, *waar* het staat en *wie* ervoor verantwoordelijk is.

Het registreren van je assets[2] kan op veel manieren en in de *richtlijn informatiebeveiliging binnen operationele ITIL-beheerprocessen* staan best practices rondom configuratiebeheer.[3] Door de adoptie van cloud technologieën is een traditionele CMDB onvoldoende omdat cloud assets daarin (meestal) afwezig zijn. Een geïntegreerd register met zowel on-premise als cloud assets is daarom nodig om het overzicht en de beveiliging te kunnen bewaken. In de praktijk worden vaak tools zoals Topdesk en ServiceNow gebruikt om assets, configuratie-items en metadata te registeren en bij te houden.

2.1 Traditionele (on-premise) assets

Voordat je begint is het natuurlijk van belang om te bepalen welke assets je gaat registreren en met welk doel. Vanuit cybersecurity oogpunt willen we servers, werkstations, mobiele apparatuur netwerkapparatuur, randapparatuur, IoT-apparatuur, OT-apparatuur, software en softwarelicenties registreren (inclusief Hardware- en Software Bill of Materials (HBOM/SBOM). Het registreren van merknamen, serienummers, MAC- en IP-adressen, fysieke locatie, gebruikte services, poorten, protocollen, (onderlinge) afhankelijkheden en zonering zorgen voor een goed omgevingsbewustzijn. Dit helpt de context te begrijpen en snel(ler) te schakelen bij CVE's en incidenten.

2.2 Cloud assets

Voor cloud assets kun je tools zoals AWS Config[4] of Azure Resource Manager[5] gebruiken om je cloud infrastructuur automatisch in kaart te brengen. Je kunt daarmee alle resources binnen een subscriptie inzichtelijk maken en bijvoorbeeld geautomatiseerd monitoren en alarmeren op basis van wijzigingen aan resources. Ongewenste wijzigingen en uitgaven kunnen hierdoor snel gemitigeerd worden.

Leveranciers van SaaS-diensten kun je verzoeken om een Software-Bill-of-Materials (SBOM) aan te leveren, zodat alle 'ingrediënten' van hun producten en diensten bekend zijn. Dit helpt om snel te kunnen schakelen bij nieuwe CVE's en incidenten.

---

[2] Informatie of digitale systemen die van waarde zijn voor een organisatie. Voorbeelden zijn: intellectueel eigendom, een klantendatabase, personeelsinformatie etc.

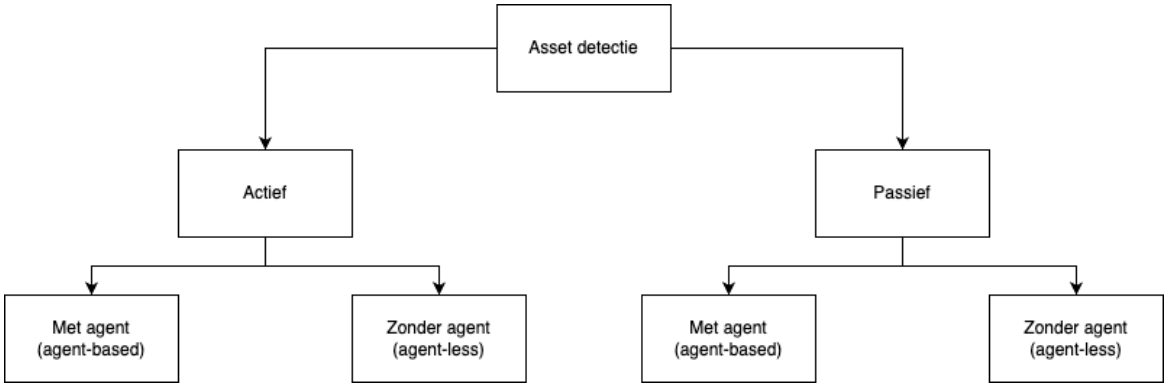
[3] https://sec.surf.nl/asset/template-richtlijn-informatiebeveiliging-binnen-operationele-itil-beheerprocessen/?category=identificatie-en-onderhoud-van-configuratie-items

[4] https://aws.amazon.com/config/

[5] https://azure.microsoft.com/nl-nl/get-started/azure-portal/resource-manager/

3 Ontdek en beheer je assets

3.1 Actieve vs. passieve detectie



3.1.1 Actieve detectie

Het netwerk wordt gescand met tools die zelf verbinding maken met apparaten. Een tool[6] stuurt netwerkverkeer (bijvoorbeeld ICMP, SNMP, TCP) om apparaten op te sporen en informatie te verzamelen. Deze vorm van detectie is nauwkeuriger dan passieve detectie, toont direct online apparaten en geeft meer technische details zoals open poorten, besturingssysteem en services. Het nadeel van deze methode is extra netwerkbelasting en het kan alarmeringen veroorzaken, bijvoorbeeld door firewalls of IDS/IPS.

```
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          nginx 1.18.0
MAC Address: 00:11:22:33:44:55 (Cisco Systems)
Device type: router
Running: Cisco IOS 12.X
OS CPE: cpe:/o:cisco:ios:12
OS details: Cisco IOS 12.4
```

Figuur 1 Voorbeeld actief assets ontdekken met Nmap

3.1.2 Passieve detectie

Het netwerk wordt afgeluisterd zonder zelf verkeer te genereren. Passieve detectie luistert mee naar bestaand netwerkverkeer of analyseert logbestanden, bijvoorbeeld via een SPAN/mirror-poort op een switch of door het inzien van DHCP-, DNS-, ARP- en NetFlow-logs. Passieve detectie veroorzaakt geen extra netwerkbelasting.

Ook in andere al bestaande logbestanden zitten vaak aanwijzingen dat er een nieuw systeem is gecreëerd of opgestart, voorbeelden zijn de audit logging van Azure of lokale Domain Controllers wanneer het nieuwe systeem domain joined is en/of gebruik maakt van bestaande authenticatie mechanismen.

[6] Zoals: Nmap, Advanced IP Scanner, OpenAudIT, Lansweeper

3.1.3 Detectie met en zonder agent

Naast onderscheid tussen actief en passief detecteren, is er nog een onderscheid in **agent-based** en **agent-less** tools:

- **Met agent (agent-based)**
  - Software op het apparaat verzamelt hardware-, software- en statusinformatie.
  - Voordelen: diepgaande informatie, altijd up-to-date, werkt ook buiten het bedrijfsnetwerk.
  - Nadelen: installatie- en beheerlast voor agents.
- **Zonder agent (agent-less)**
  - De tool scant via protocollen als SNMP, WMI of SSH zonder software op endpoints.
  - Voordelen: snelle uitrol, geen installatie op apparaten, minder beheerlast.
  - Nadelen: minder detail, afhankelijk van netwerktoegang en protocoltoestemming.

Veel instellingen maken gebruik van Microsoft Defender for Endpoint/Server. Op ieder systeem waar dit draait is communicatie met de Azure tenant van de instelling. Daardoor kan Defender ook een rapportage[7] opleveren van systemen die wel op dezelfde netwerken zitten maar niet onderdeel zijn van de beheer omgeving en/of securitymaatregelen.

3.2 Automatiseren van detectie

Met name voor (cloud)omgevingen die erg dynamisch van aard zijn en waarin veel assets het netwerk betreden is automatisering van het ontdekken van assets, of wijzigingen daaraan, essentieel. Het automatiseren van detectie kan simpelweg via scripts die door middel van cronjobs of geplande taken periodiek uitgevoerd worden. De output daarvan dient geïntegreerd te worden met de tool die gebruikt wordt voor het bijhouden van de assets. Afhankelijk van de tool kan dit bijvoorbeeld via een API-koppeling, JSON, CSV of bijvoorbeeld database import.

3.3 Onbekende assets adresseren

De output van actieve en passieve asset detectie dient gecorreleerd te worden met de asset database (CMDB). Hierdoor is het mogelijk om onbekende assets (automatisch) te identificeren, te isoleren, te blokkeren of nader te onderzoeken.

[7] https://learn.microsoft.com/en-us/defender-endpoint/device-discovery

4 Ontdek en beheer je software

Doel: ontdekken welke software gebruikt wordt, voldoen aan licentievoorwaarden, tijdig inspelen op capaciteitstekorten, voorkomen van ongeautoriseerde toegang, malafide en kwetsbare applicaties.

4.1 Software ontdekken

Het ontdekken van software gebeurt idealiter geautomatiseerd, zodat de informatie actueel en volledig blijft. Gebruik automatische (agent-based) tools om software op endpoints, servers en cloud infrastructuur te detecteren, zoals bijvoorbeeld Intune discovered apps. Denk hierbij aan ook webbrowser en geïnstalleerde extensies. Het gebruik van SaaS-applicaties (schaduw-IT) kun je in kaart brengen via een Cloud Access Security Broker (CASB), DNS- en firewall logging.

4.2 Ongewenste software weren

Ongewenste software dient bij voorkeur automatisch geweerd te worden. Dit kan bijvoorbeeld door Application Allowlisting op Windows systemen met AppLocker of Intune.[8][9] Endpoint protection kan ook helpen om het installeren en/of uitvoeren van ongewenste software te voorkomen door deze in quarantaine te plaatsen, direct te verwijderen of door het endpoint te isoleren. Met browser policies kun je voorkomen dat ongewenste extensies gedownload en geïnstalleerd worden.

[8] https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/applocker-overview

[9] https://learn.microsoft.com/nl-nl/intune/configmgr/core/understand/introduction