mbo digitaal

Kwetsbaarheden opsporen en oplossen

SAMENWERKEN AAN CYBERVEILIGHEID IN HET MBO

11 december 2025

Mick Deben & Ry Boxem

mbo digitaal

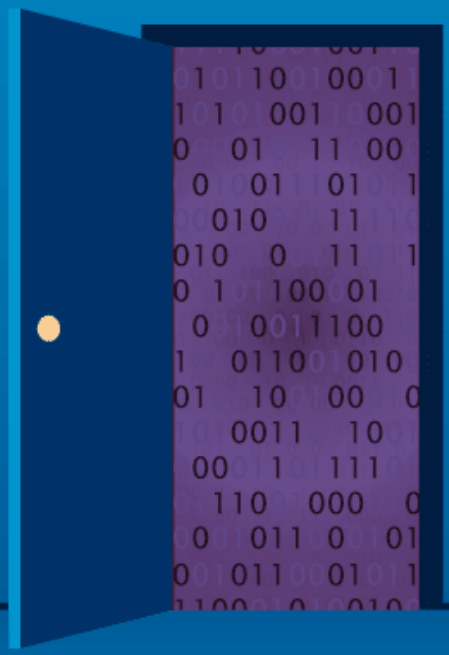
Inhoud

Introductie

Levencyclus kwetsbaarheid

Initiatief weerbaarheidstesten

- Voortgang eduC2
- Voortgang ASM
- Omgaan met bevindingen
- Toekomst



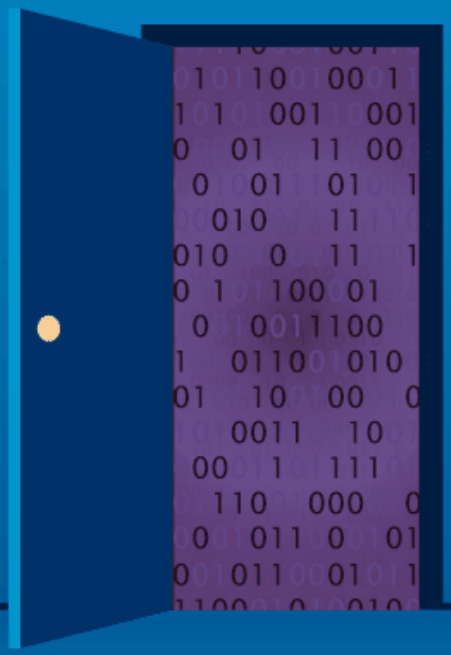
mbo digitaal

Introductie

- **Doel van deze workshop**:
  - Leren over kwetsbaarheden
  - Ophalen van pijnpunten, en dus behoeften

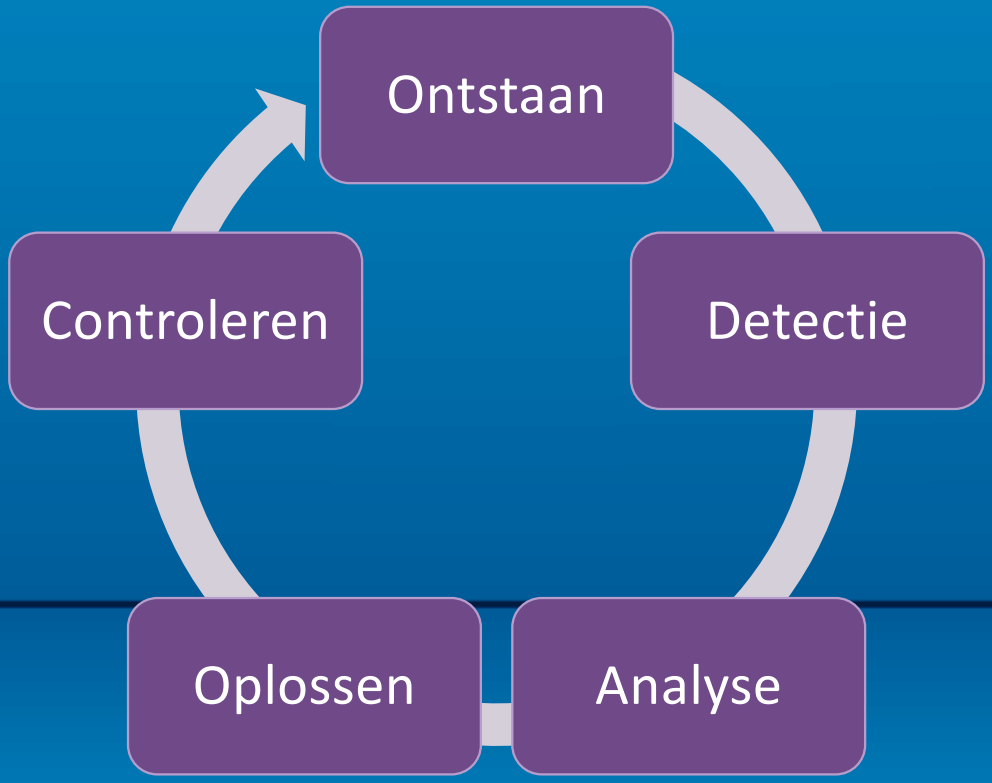
- **Belang van vulnerability management:** vrijwel alle grote cyberincidenten terug te voeren zijn op misbruik van bekende **kwetsbaarheden,** eventueel in combinatie met andere aanvalstechnieken.

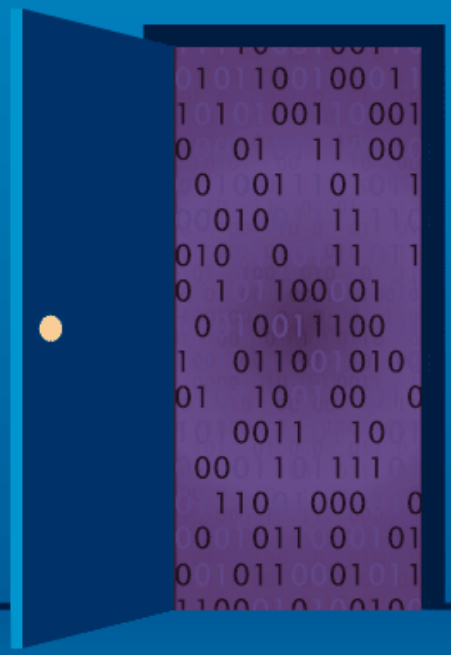
Kwetsbaarheid: *“blootgesteld kunnen worden aan risico en onzekerheid.”*



mbo digitaal

Levencyclus van een kwetsbaarheid

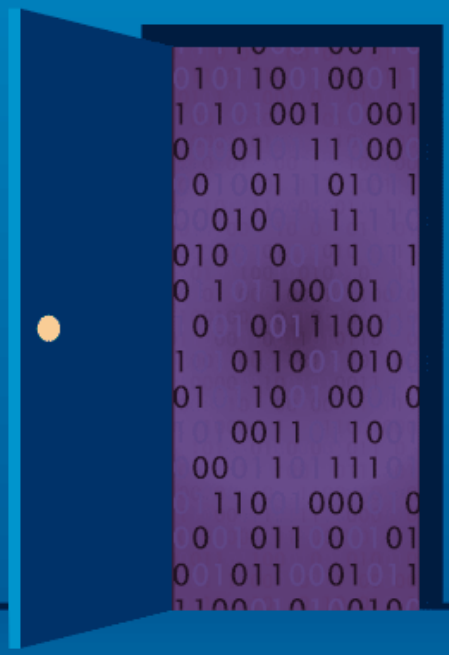




mbo digitaal

Ontstaan

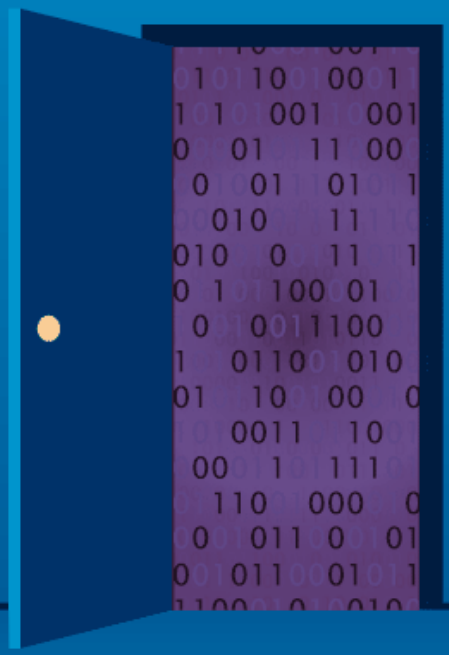
- Fout in ontwerp, code of configuratie
- Verouderde of niet-gepatchte software
- Complexiteit meer kans op menselijke fouten
- Nieuwe features zonder security-review
- Onvoldoende hardening / baseline-beheer



mbo digitaal

Detectie

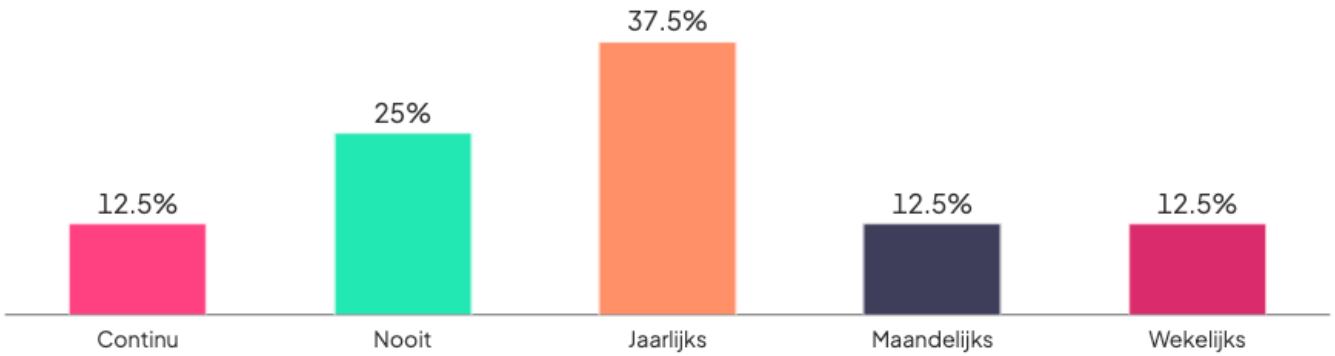
- Vuln scanners
  - Intern
  - Extern
  - Applicaties
- Benchmarks (compliance checks)
- OSINT
- Pentesting/Red Teaming
- Bug bounty/CVD
- Beheerders (leveranciers, medewerkers)



mbo digitaal

Poll

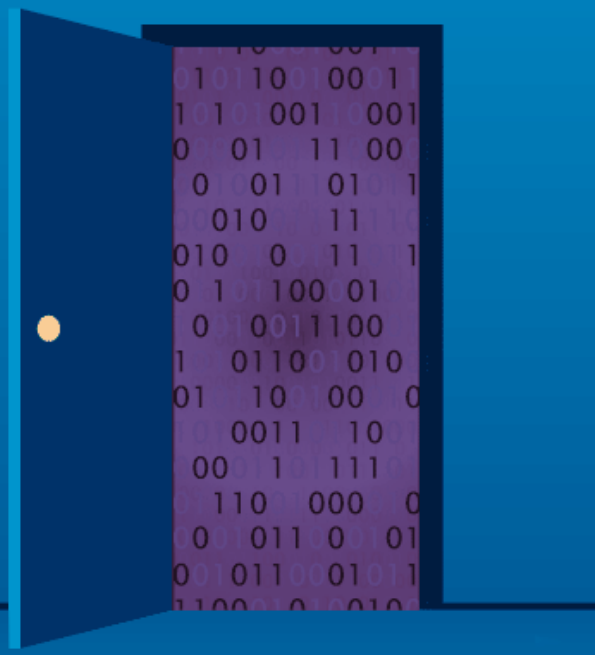
Hoe vaak voeren jullie kwetsbaarheden scans uit?



mbo digitaal

Analyse

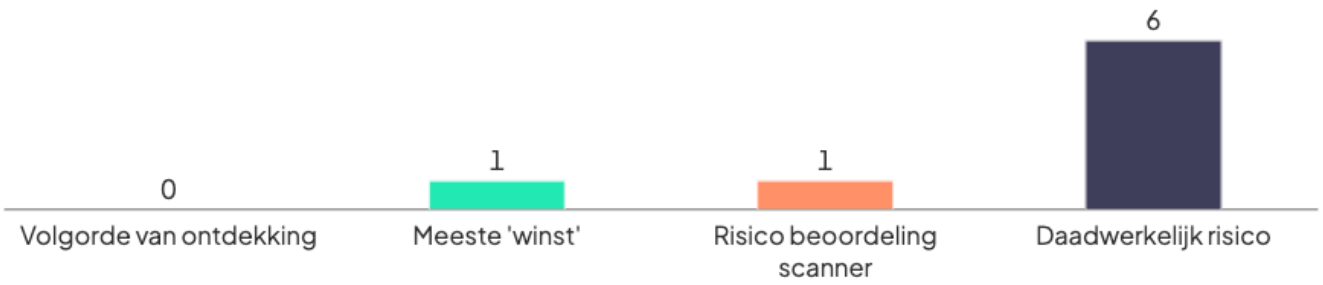
- Bepalen: *kans x impact x epss*
- Koppeling aan businessprocessen
- Zijn er mitigerende maatregelen?
- False positives uitsluiten
- CVSS ≠ Risico



mbo digitaal

Poll

Hoe prioriteer je het adresseren van kwetsbaarheden?



mbo digitaal

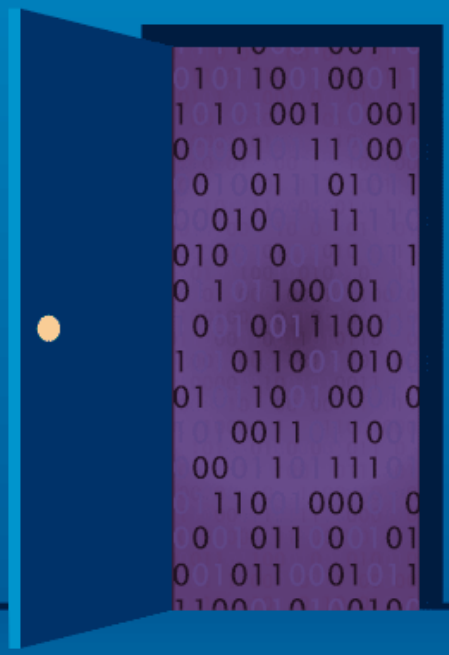
Poll

Binnen welke periode moeten kritische kwetsbaarheden worden geadresseerd?

mbo digitaal

Oplossen

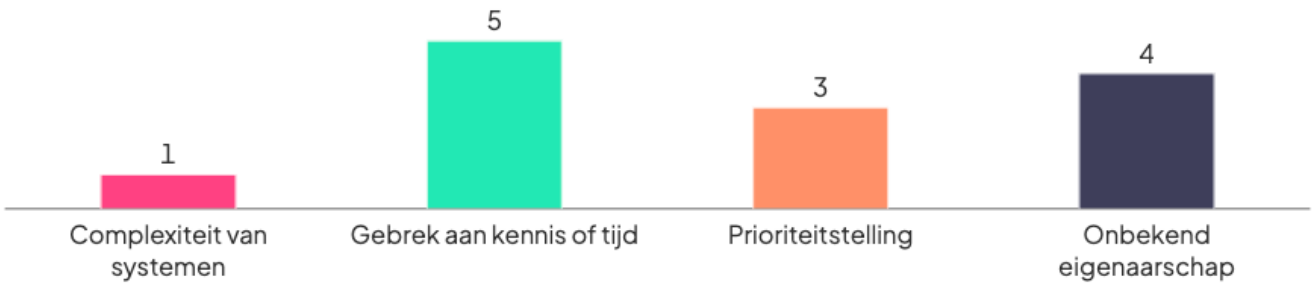
- Patching
- Configuratieaanpassingen (policies, hardening)
- Workarounds of mitigaties



mbo digitaal

Poll

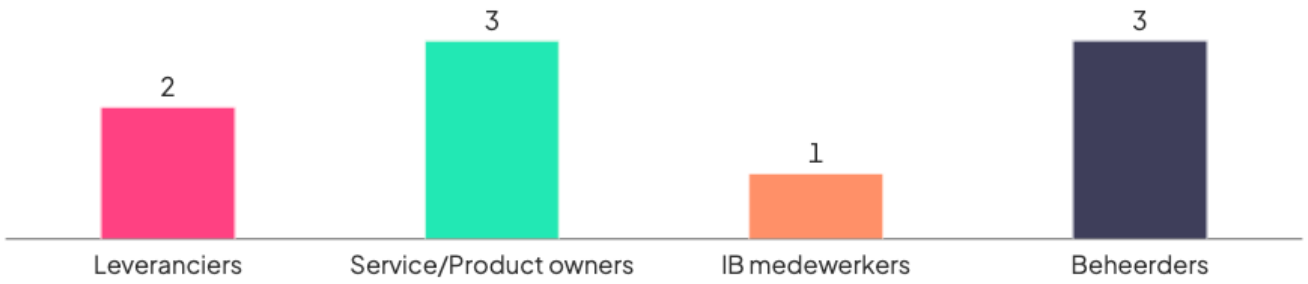
Wat is jullie grootste uitdaging bij het oplossen van kwetsbaarheden?



mbo digitaal

Poll

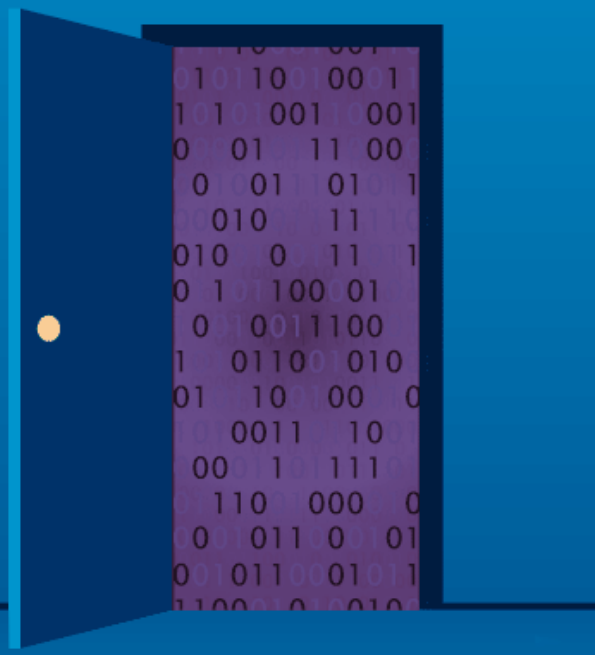
Wie is er verantwoordelijk voor vulnerability management



mbo digitaal

Controleren

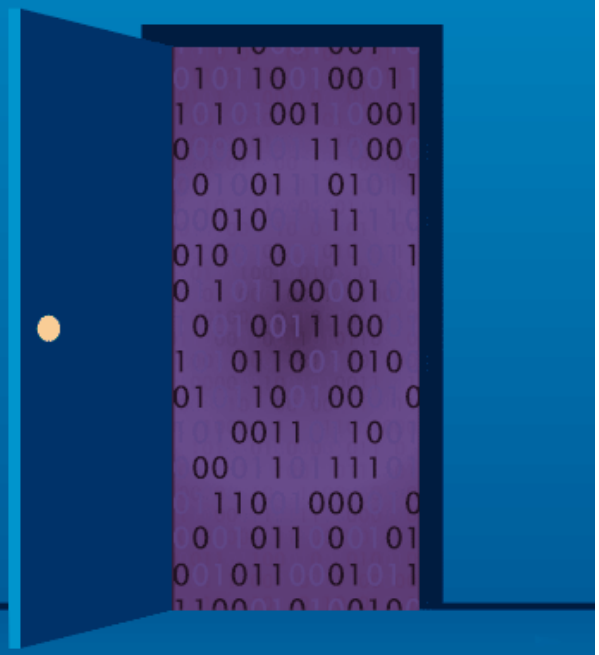
- Herscan of opnieuw testen
- Controleren of mitigerende/compenserende maatregelen gewenst effect hebben



mbo digitaal

Initiatief weerbaarheidstesten - eduC2

Met remote testen identificeren we kwetsbaarheden en misconfiguraties in het interne aanvalsoppervlak (netwerk, AD/Entra ID)



Doelen:

- Het signaleren van bekende kwetsbaarheden in het aanvalsoppervlak
- Het bieden van duiding en handelingsperspectief voor kwetsbaarheden
- Door modulariteit snel kunnen bevestigen of uitsluiten

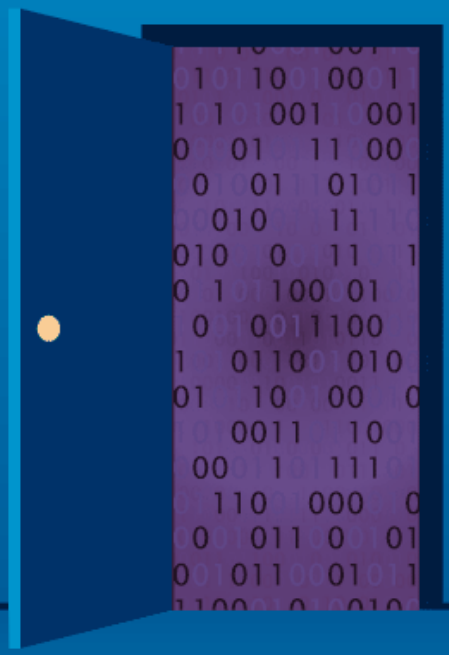
Draagt bij aan:

- Het signaleren van veelvoorkomende kwetsbaarheden en misconfiguraties die door dreigingsactoren misbruikt (kunnen) worden
- Het signaleren van missers in veilige configuraties en security updates
- Het prioriteren van corrigerende maatregelen
- Het voorkomen van misbruik van bekende kwetsbaarheden

mbo digitaal

Testen EduC2

- Soma College
- Zadkine
- Zone College



mbo digitaal

Poll

Suggesties voor testmogelijkheden EduC2

Kerberos,

Segmenteren (het ontbreken ervan) en clientisolation activering

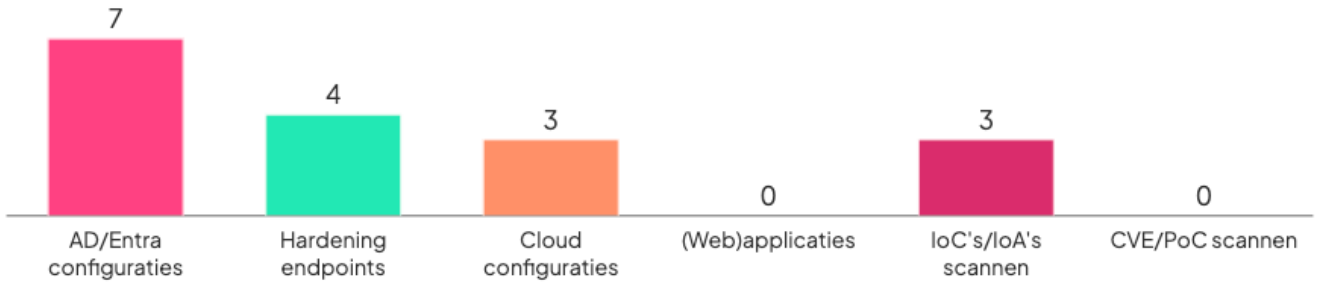
Aan kunnen sluiten op de security diensten van bijvoorbeeld een Microsoft

Authenticatieprotocollen, encryptiestandaarden voor data in transit (en authenticatie). Maar die werden al genoemd volgens mij. MITM simulaties

mbo digitaal

Poll

Welke testen vinden jullie het waardevolst om toe te voegen



mbo digitaal

Initiatief weerbaarheidstesten - Attack Surface Management

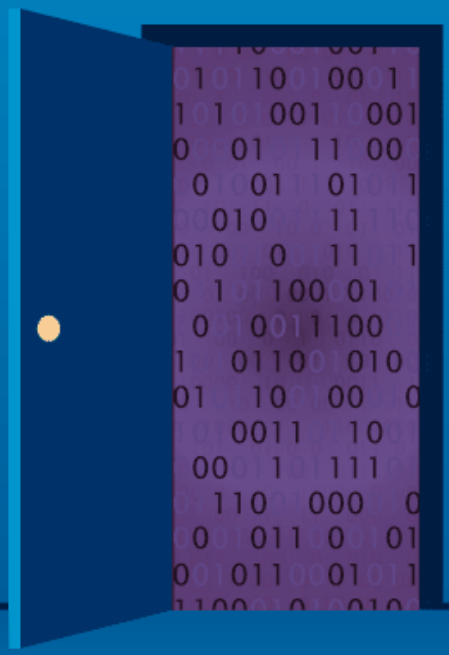
Inzicht krijgen en houden in alle systemen, applicaties, diensten en configuraties die vanaf buiten zichtbaar en bereikbaar zijn. ASM toont welke digitale “ingangen” een organisatie onbedoeld of ongecontroleerd aan de buitenwereld presenteert.

Doelen:

- Continu inzicht krijgen in alle extern zichtbare systemen, diensten en configuraties.
- Onbedoelde blootstelling (shadow IT, vergeten assets, misconfiguraties) snel identificeren.
- Het aanvalsoppervlak verkleinen.

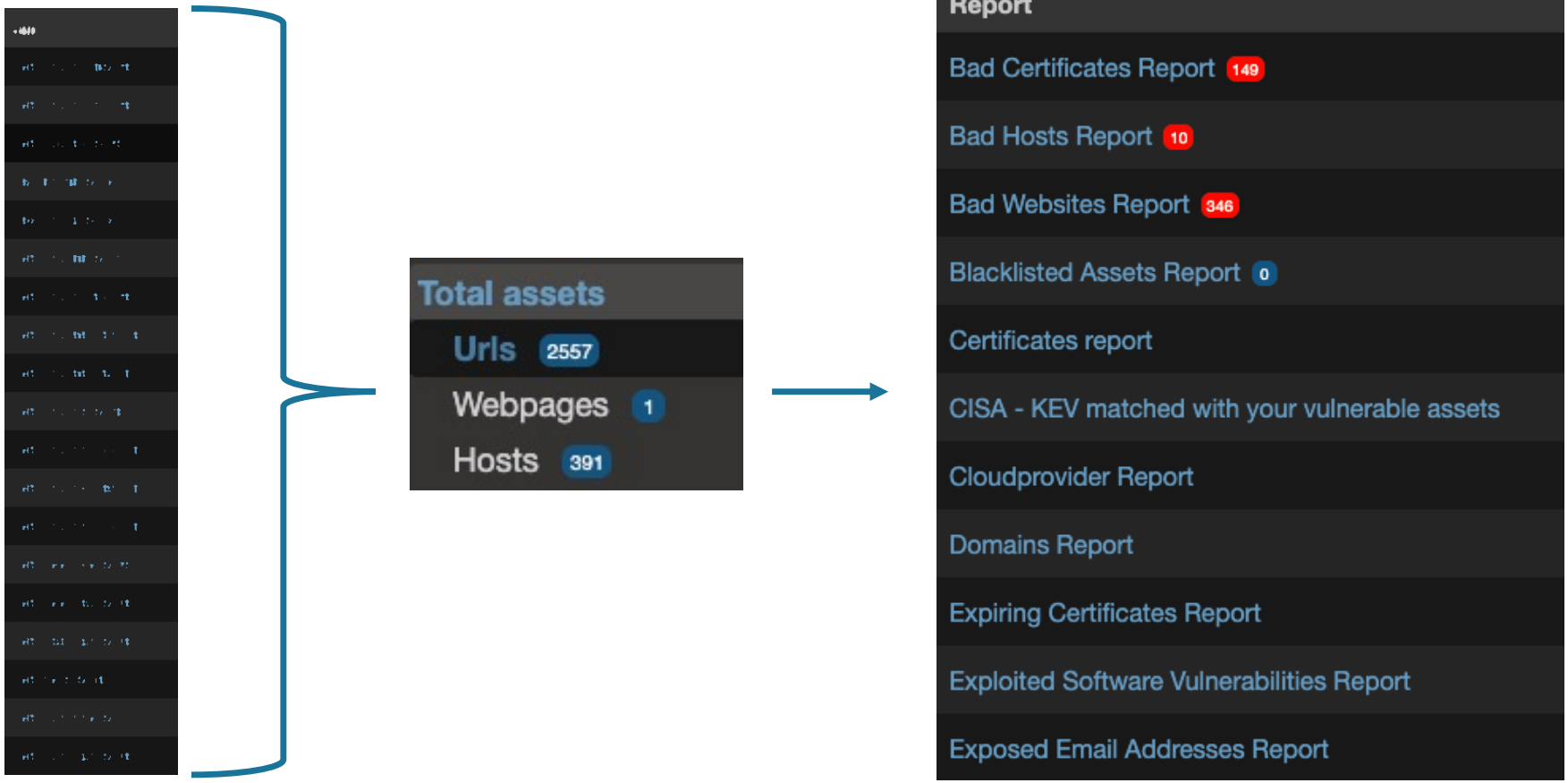
Waar draagt het aan bij:

- Proactieve beveiliging: risico’s aanpakken voordat aanvallers ze aanpakken.
- Ondersteuning van vulnerability management.



mbo digitaal

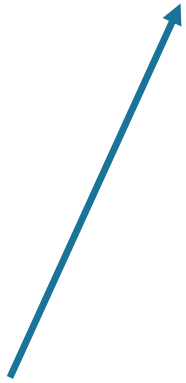
Attack Surface Management



mbo digitaal

Attack Surface Management

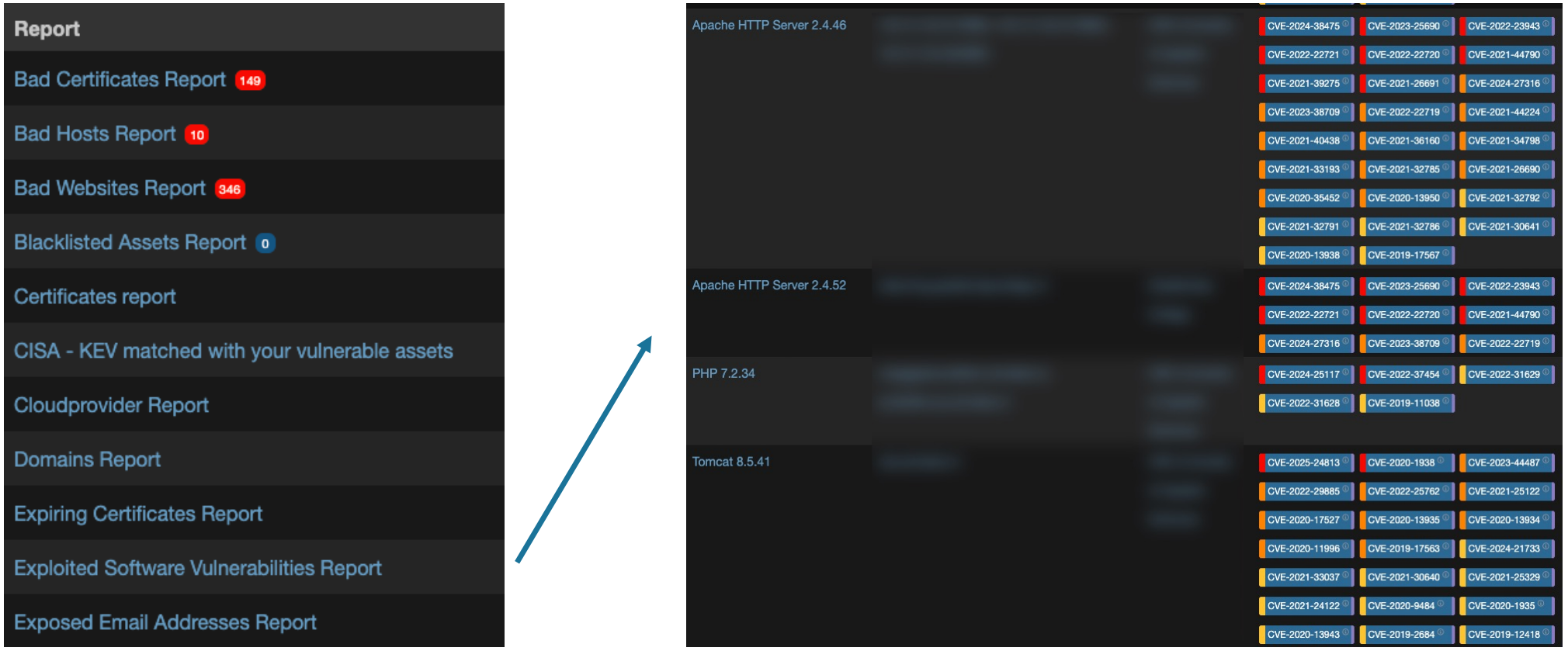
Report
Bad Certificates Report 149
Bad Hosts Report 10
Bad Websites Report 346
Blacklisted Assets Report 0
Certificates report
CISA - KEV matched with your vulnerable assets
Cloudprovider Report
Domains Report
Expiring Certificates Report
Exploited Software Vulnerabilities Report
Exposed Email Addresses Report



email_address	found_on	data_breaches
[redacted]	[redacted]	Gravatar (2020-10-03)
[redacted]	[redacted]	SynthientCredentialStuffingThreatData (2025-04-11)
[redacted]	[redacted]	PDL (2019-10-16), VerificationsIO (2019-02-25), YouveBeenScraped (2018-10-05), ShareThis (2018-07-09), OnlinerSpambot (2017-08-28), ExploitIn (2016-10-13), MDPI (2016-08-30), LinkedIn (2012-05-05)
[redacted]	[redacted]	LinkedInScrape (2021-04-08), PDL (2019-10-16), YouveBeenScraped (2018-10-05), LinkedIn (2012-05-05)
[redacted]	[redacted]	Dropbox (2012-07-01)
[redacted]	[redacted]	PDL (2019-10-16), Apollo (2018-07-23)
[redacted]	[redacted]	SynthientCredentialStuffingThreatData (2025-04-11), LinkedInScrape (2021-04-08), PDL (2019-10-16), VerificationsIO (2019-02-25), YouveBeenScraped (2018-10-05), LinkedIn (2012-05-05)
[redacted]	[redacted]	PDL (2019-10-16), VerificationsIO (2019-02-25)
[redacted]	[redacted]	VerificationsIO (2019-02-25)
[redacted]	[redacted]	VerificationsIO (2019-02-25)
[redacted]	[redacted]	SynthientCredentialStuffingThreatData (2025-04-11), Twitter200M (2021-01-01), OnlinerSpambot (2017-08-28), MDPI (2016-08-30), Dropbox (2012-07-01)
[redacted]	[redacted]	SynthientCredentialStuffingThreatData (2025-04-11), OpenSubtitles (2021-08-01), Gravatar (2020-10-03), 123RF (2020-03-22), MyHeritage (2017-10-26), Adobe (2013-10-04), Dropbox (2012-07-01)

mbo digitaal

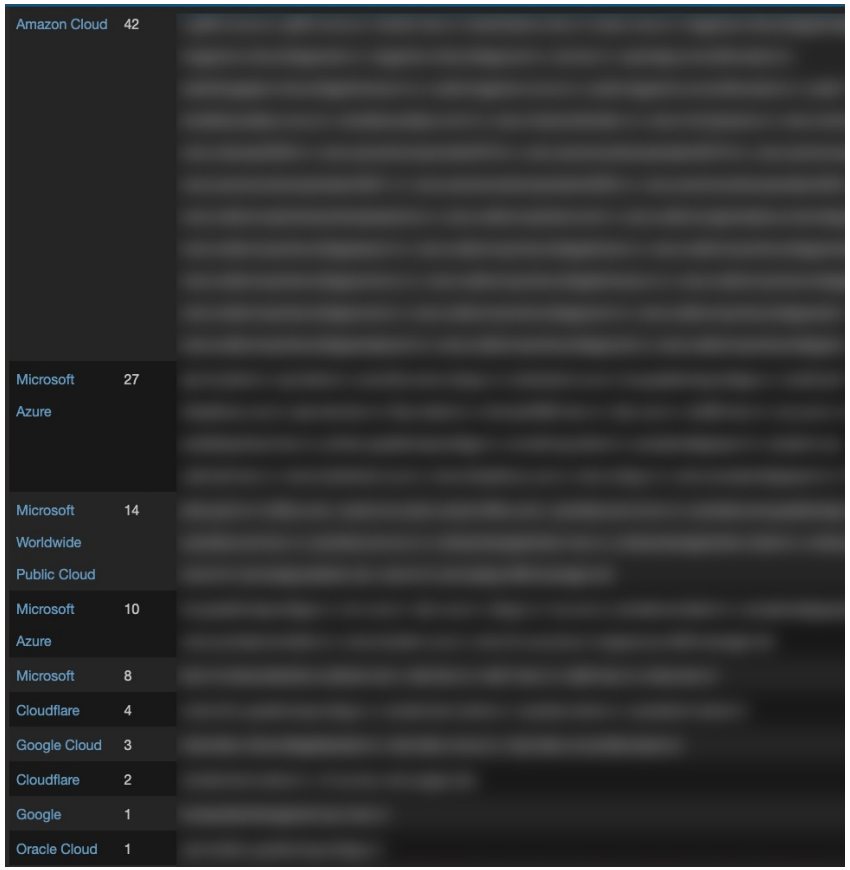
Attack Surface Management



mbo digitaal

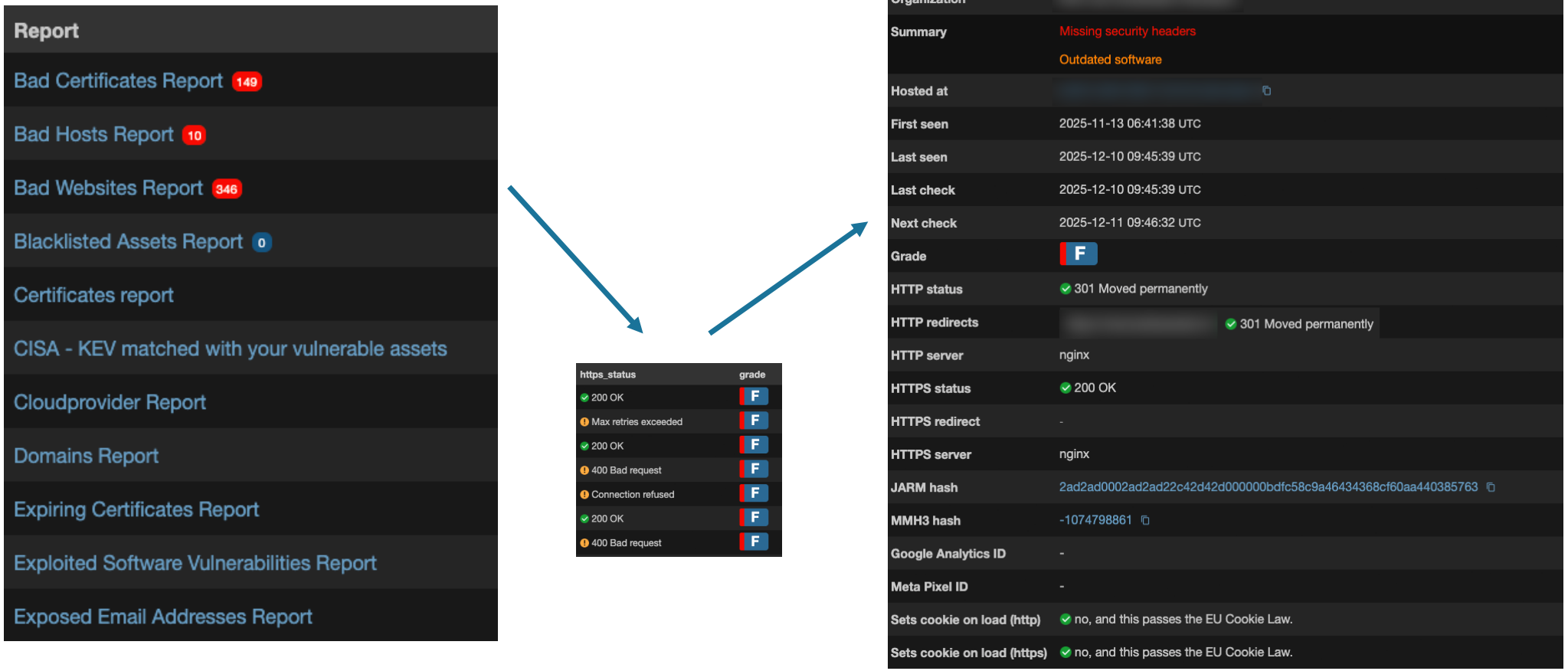
Attack Surface Management

Report
Bad Certificates Report 149
Bad Hosts Report 10
Bad Websites Report 346
Blacklisted Assets Report 0
Certificates report
CISA - KEV matched with your vulnerable assets
Cloudprovider Report
Domains Report
Expiring Certificates Report
Exploited Software Vulnerabilities Report
Exposed Email Addresses Report



mbo digitaal

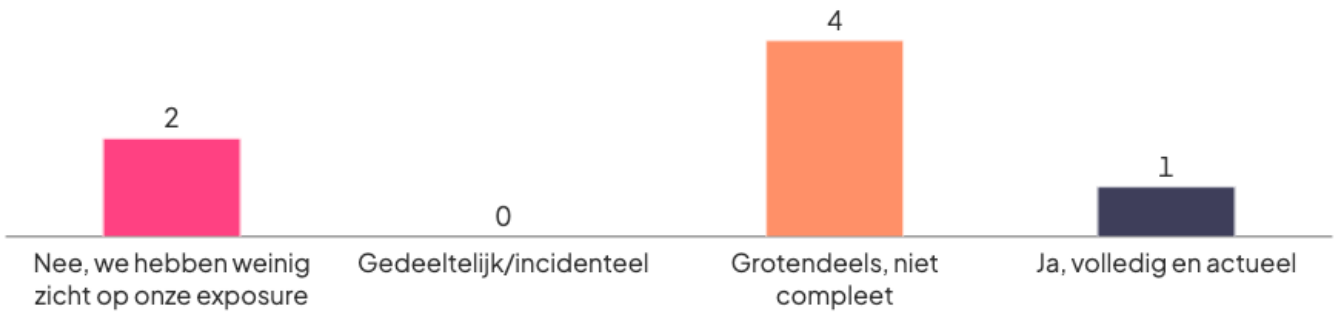
Attack Surface Management



mbo digitaal

Poll

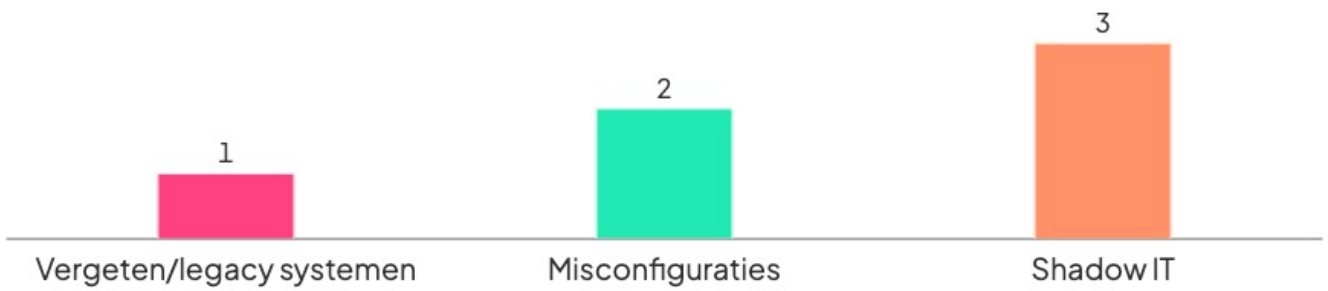
Heeft jouw organisatie een volledig en actueel overzicht van alle extern zichtbare assets?



mbo digitaal

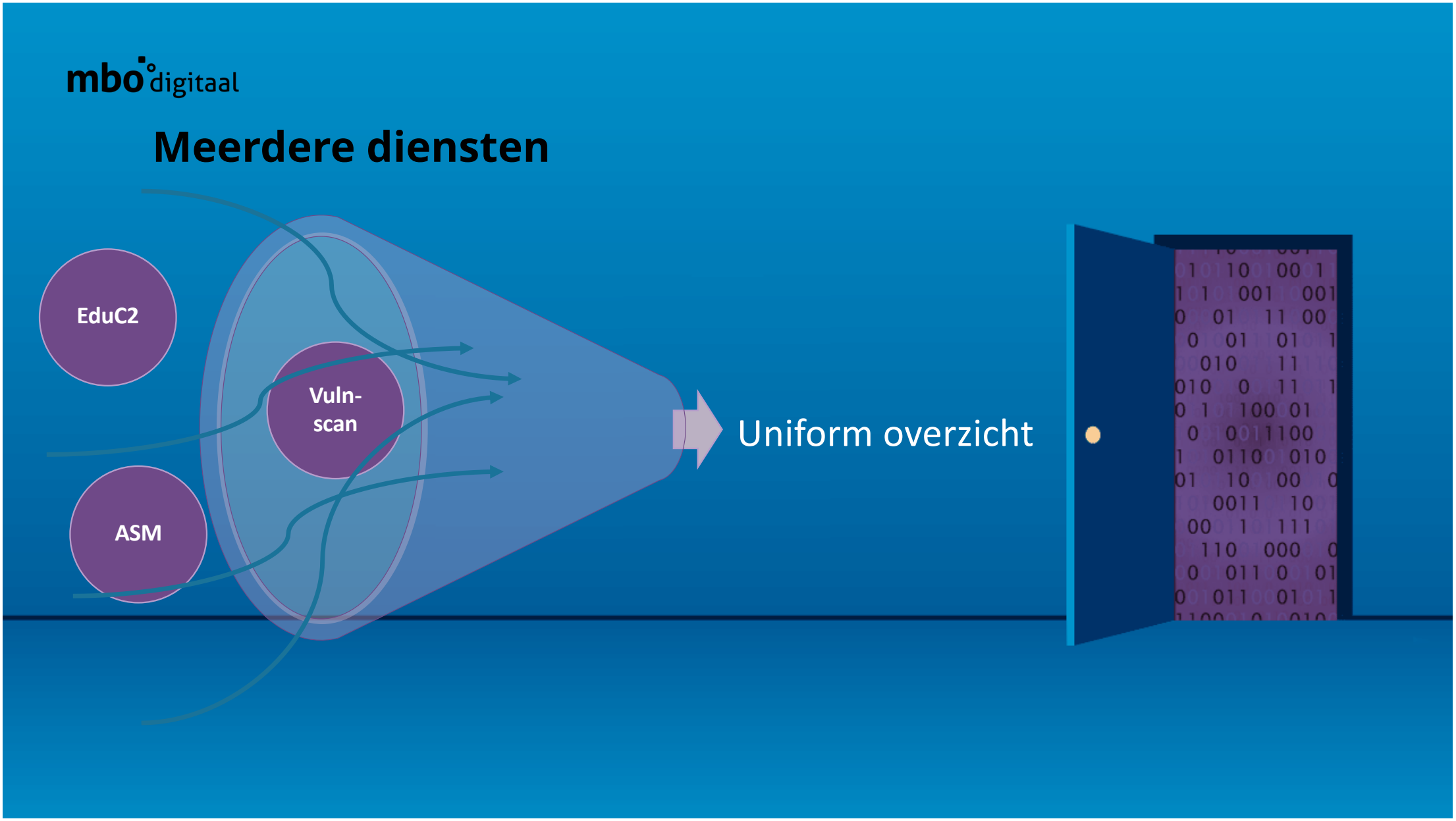
Poll

Wat is op dit moment de grootste uitdaging in jullie attack surface?



mbo digitaal

Meerdere diensten

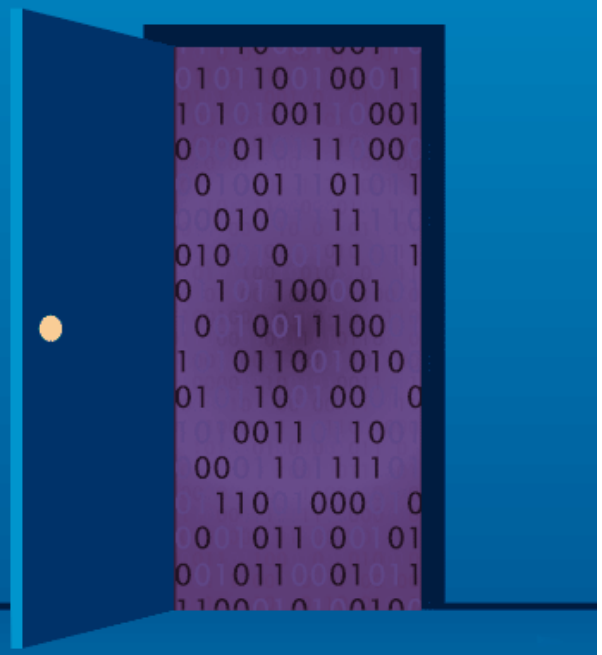


mbo digitaal

Initiatief weerbaarheidstesten – ’projectmanagement’

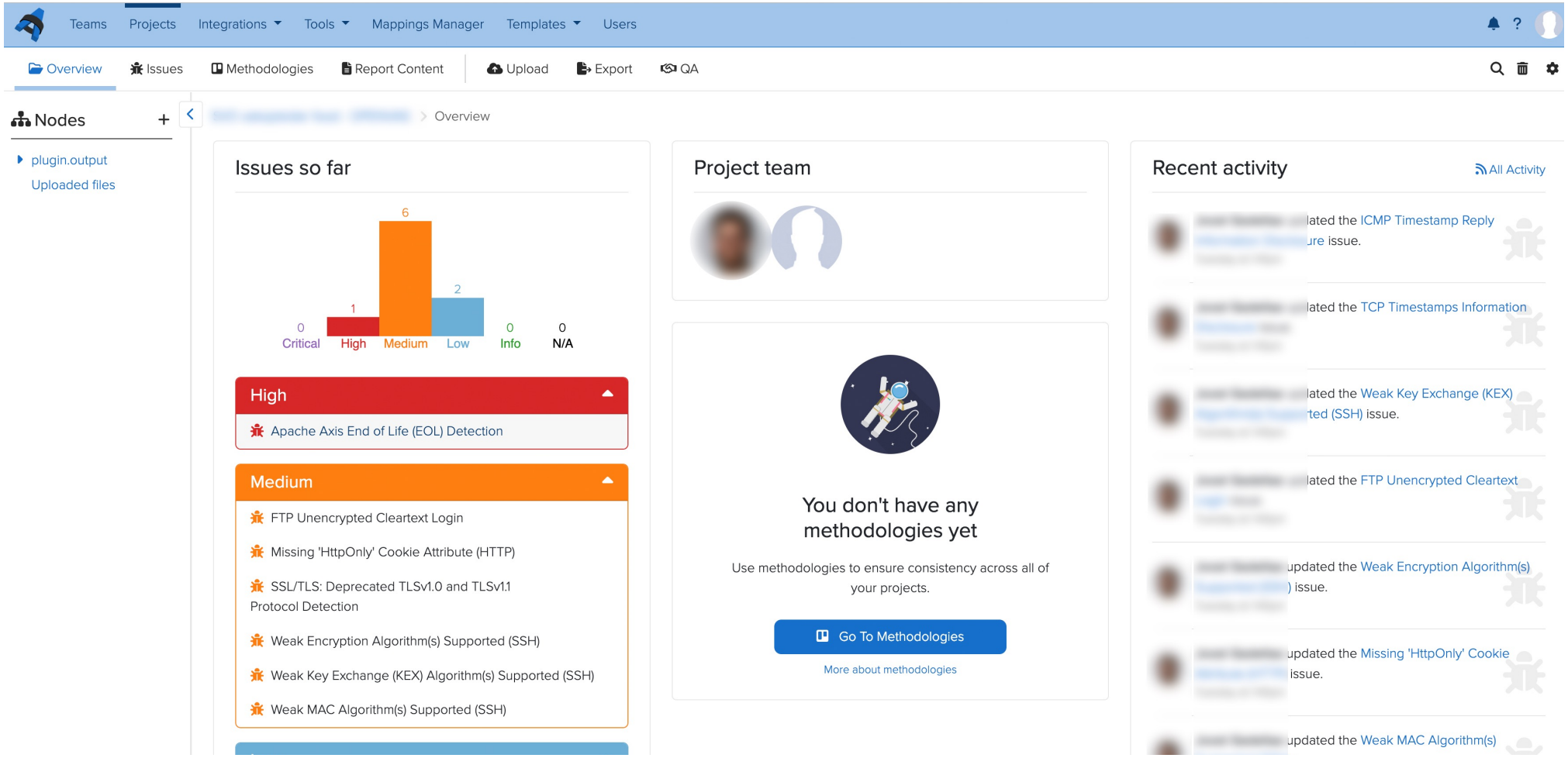
Geleerd bij het ‘van check tot hack’ traject.

10 instellingen x 5/6 checks = 🤯



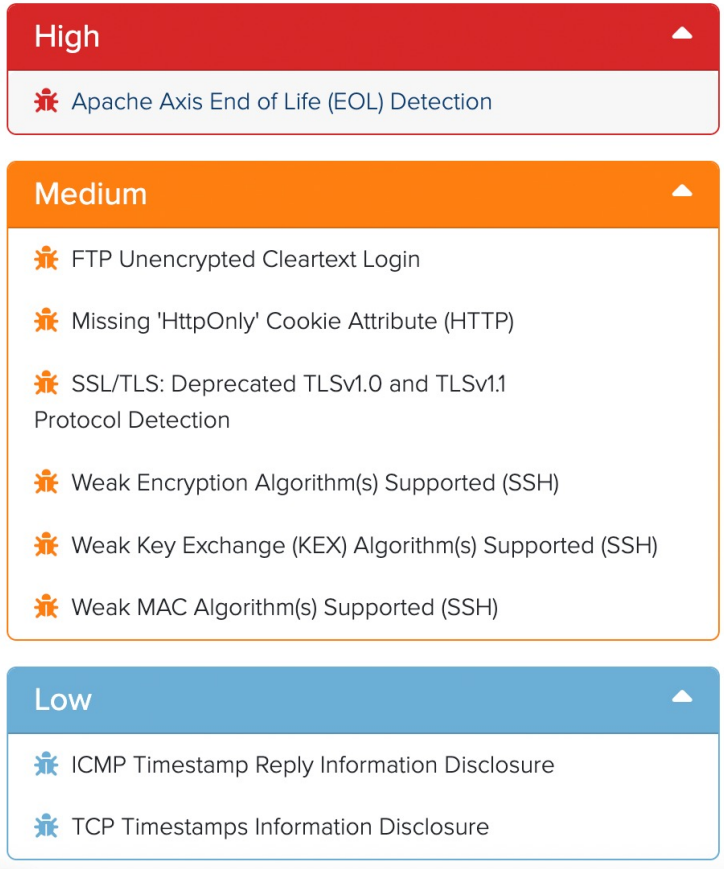
mbo digitaal

Bevindingen



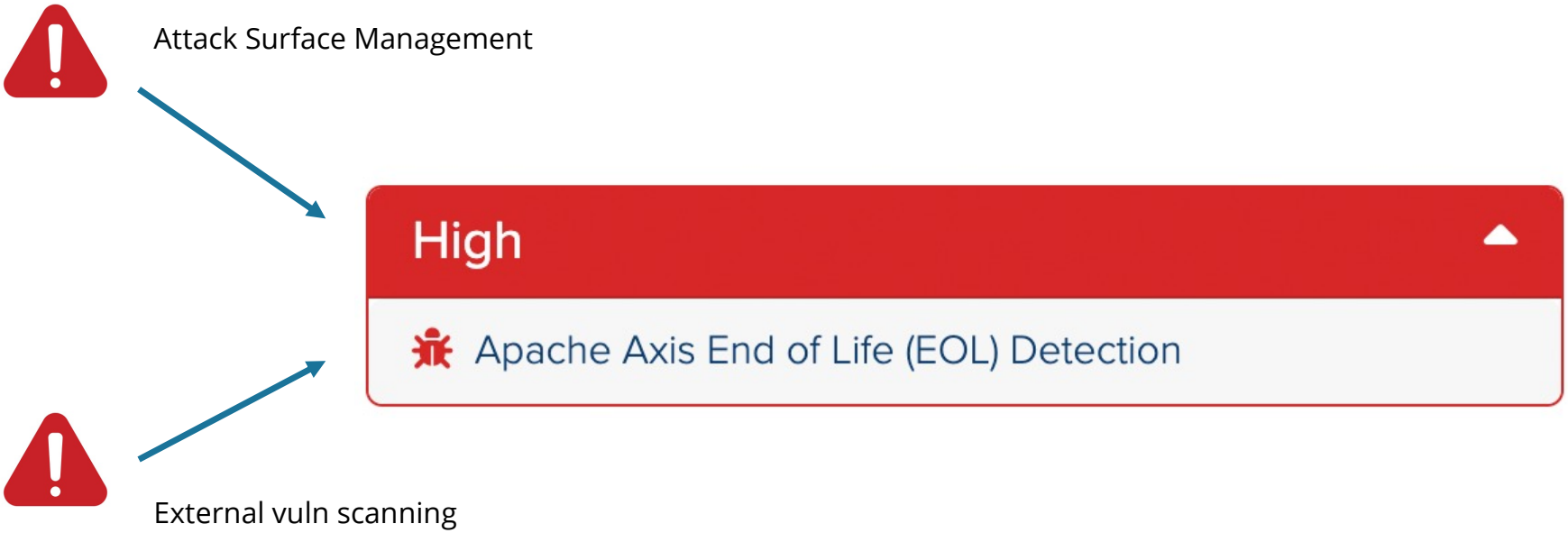
mbo digitaal

Bevindingen



mbo digitaal

Normalisatie



mbo digitaal

Normalisatie - voordelen

- Hogere integriteit
- Minder (duplicate) meldingen
- Betere performance

mbo digitaal

Details

Apache Axis End of Life (EOL) Detection

Edit •••

Title

Apache Axis End of Life (EOL) Detection

CVSSv2

10.0

AffectedSoftware

Description

The Apache Axis installation on the remote host has reached the
End of Life (EOL) / is discontinued and should not be used anymore.

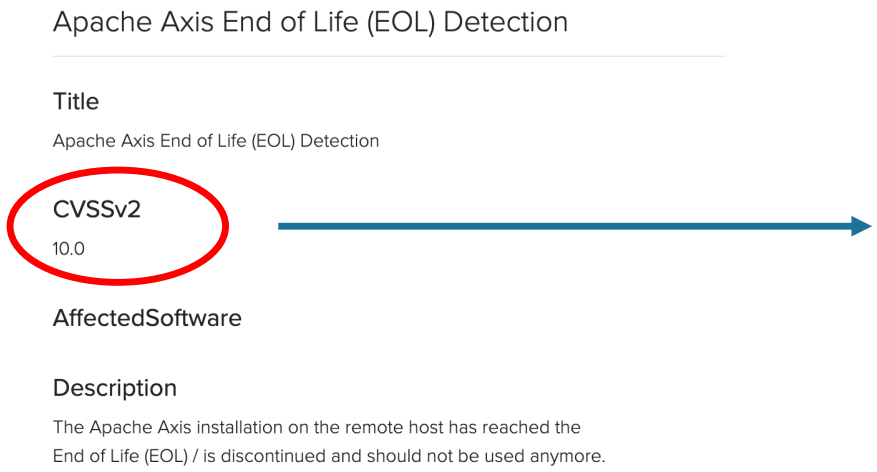
Recommendation

Axis 1 has been EOL and the vendor recommend to migrate to a
different SOAP engine, such as Apache Axis2/Java.

Notes: - The latest available version 1.4 was released on April 22, 2006. Some more recent flaws have been fixed only in the SVN repository - The Apache Axis project does not expect to create an Axis 1.x release fixing these flaws - If the remote installation has been build from the SVN sources or is covered via ‘backports’ of a Linux distribution please create an override for this result

mbo digitaal

Prioritering (adressering!)



Wanneer er voor een kwetsbaarheid een CVSS-score beschikbaar is, gebruiken we deze score als startpunt voor de prioritering. Het biedt duidelijke parameters zoals exploitability, impact op vertrouwelijkheid/integriteit/beschikbaarheid en de complexiteit van de aanval. Daarom is CVSS *leidend* wanneer het beschikbaar is.

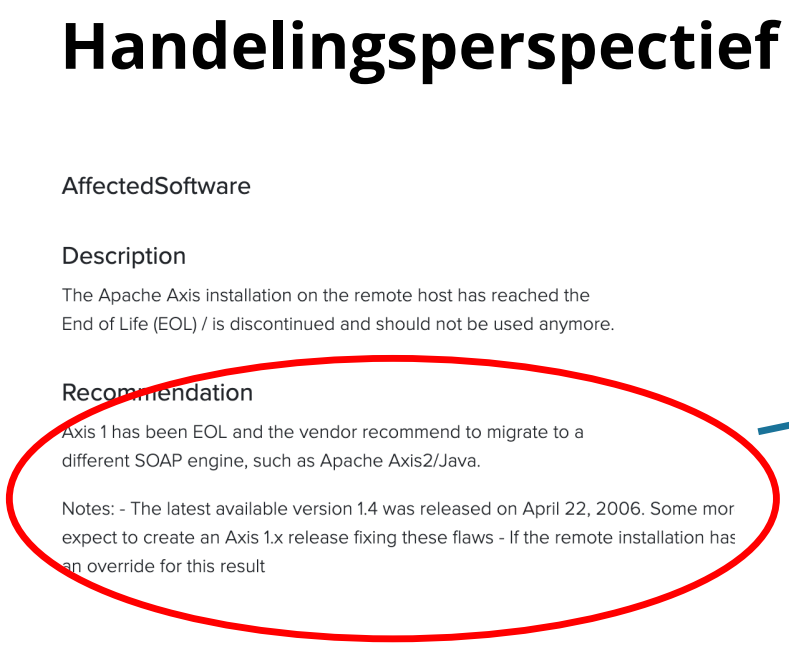
Er zijn ook kwetsbaarheden waar geen CVSS-score voor bestaat. Dit komt vooral voor bij misconfiguraties en ontbrekende (of niet nageleefde) policies. In dergelijke gevallen passen we een prioriteringsmodel toe, hierbij hanteren we de volgende categorieën:

- Critical - Direct risico op misbruik of ernstige schade.
- High - Significant risico.
- Medium – Beperkt risico
- Low – Laag risico

Maar onthoudt CVSS ≠ Risico. We wensen dat de bevindingen worden geadresseerd, dit is niet hetzelfde als oplossen.

mbo digitaal

Handelingsperspectief



Vulnerability scanners leveren bij een gevonden kwetsbaarheid vaak automatisch een aanbevelingen aan. Deze adviezen geven ook direct richting aan de te nemen maatregelen, zoals het installeren van een specifieke patch, het aanpassen van configuraties of het toepassen van security best practices. Dit helpt om snel en consistent te bepalen wat de passende remedie is.

Bij de ASM tooling en bij eduC2 ligt dit anders. Deze tools leveren waardevolle detecties op, maar geven geen automatisch gegenereerde oplossingsadviezen. Dat betekent dat we zelf moeten bepalen welke remediëringsstappen nodig zijn, en dit vraagt om een meer structurele aanpak.

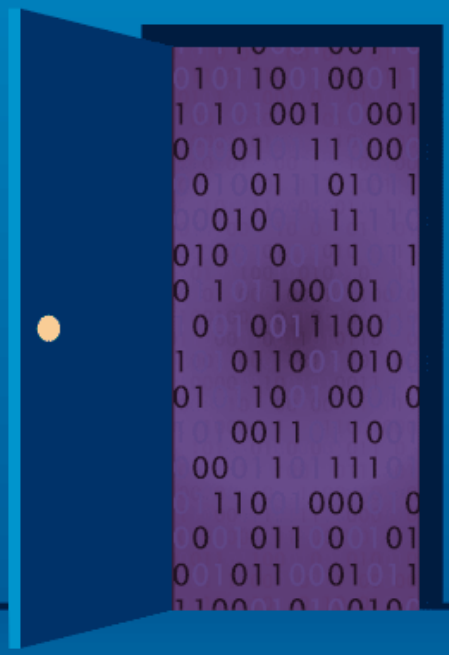
- Richtlijnen per type misconfiguratie (bijv. policies, cloud resources).
- Best practices gebaseerd op CIS-benchmarks of interne baseline-standaarden.
- Heldere instructies voor beheerteams over hoe het probleem te verhelpen is.
- Eventuele workarounds of tijdelijke mitigerende maatregelen wanneer patches niet beschikbaar zijn.

mbo digitaal

Toekomst

Ontwikkelen detecties EduC2.
Ontwikkelen normalisatie.
Ontwikkelen handelingsperspectief.

En het inrichten van alle bijbehorende processen.



mbo digitaal

Kwetsbaarheden opsporen en oplossen

Voor vragen:

m.deben@mbodigitaal.nl

r.boxem@mbodigitaal.nl

MBO Digitaal is een platform van de MBO Raad voor samenwerking aan digitalisering in het mbo. MBO Digitaal werkt samen met alle mbo-instellingen en heeft sterke banden met MBO Voorzieningen, Kennisnet en SURF.