

mbo°digitaal

Kwetsbaarheden opsporen en oplossen

.....

11 december 2025
Mick Deben & Ry Boxem

SAMENWERKEN AAN

CYBERVEILIGHEID

IN HET MBO

JAAR
3



PROGRAMMA
Cyberveiligheid



NETWERK
Informatiebeveiliging
en Privacy

MBO Raad

mbo°digitaal

mbodigitaal.nl/cyberveiligheid

Inhoud

Introductie

Levenscyclus kwetsbaarheid

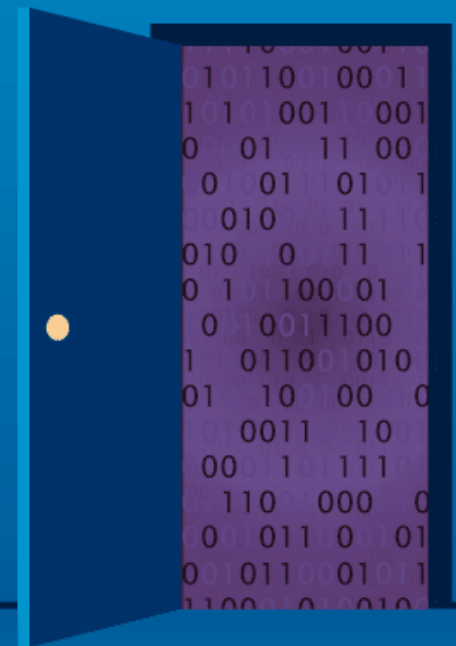
Initiatief weerbaarheidstesten

- Voortgang eduC2

- Voortgang ASM

- Omgaan met bevindingen

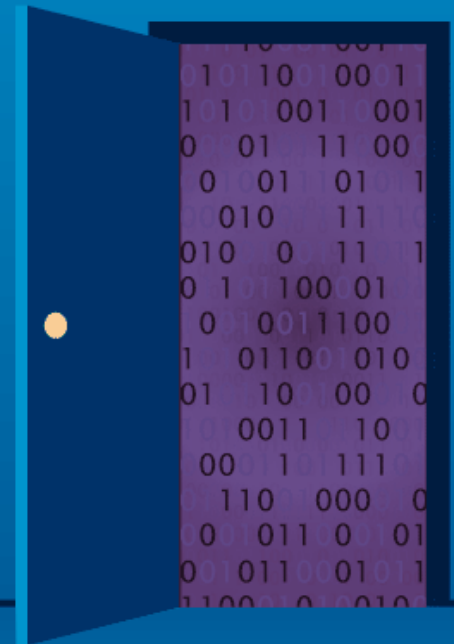
- Toekomst



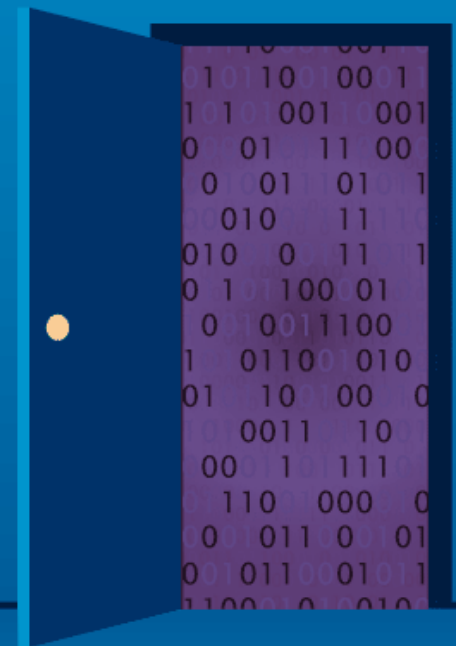
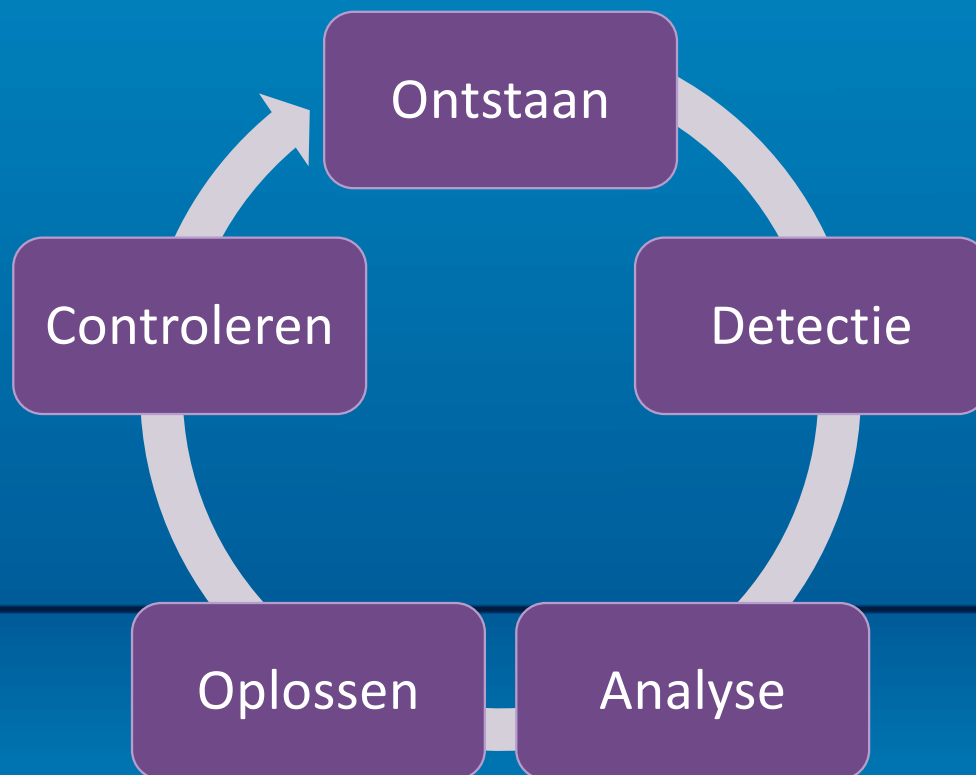
Introductie

- **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.”*

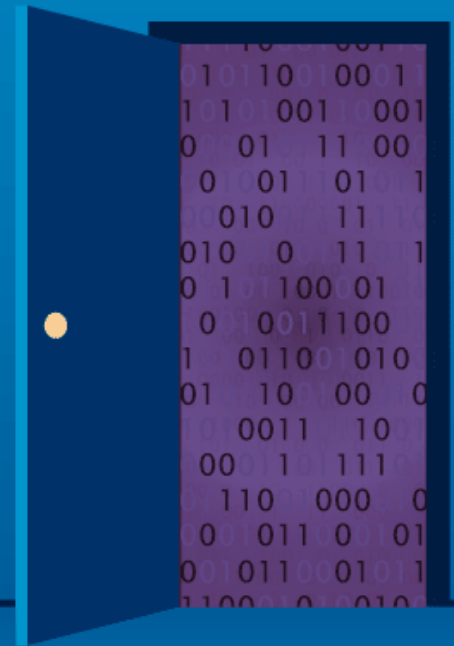


Levenscyclus van een kwetsbaarheid



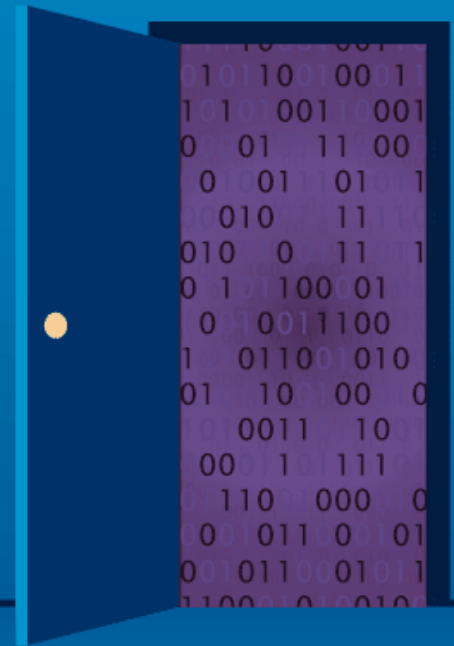
Ontstaan

- 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



Detectie

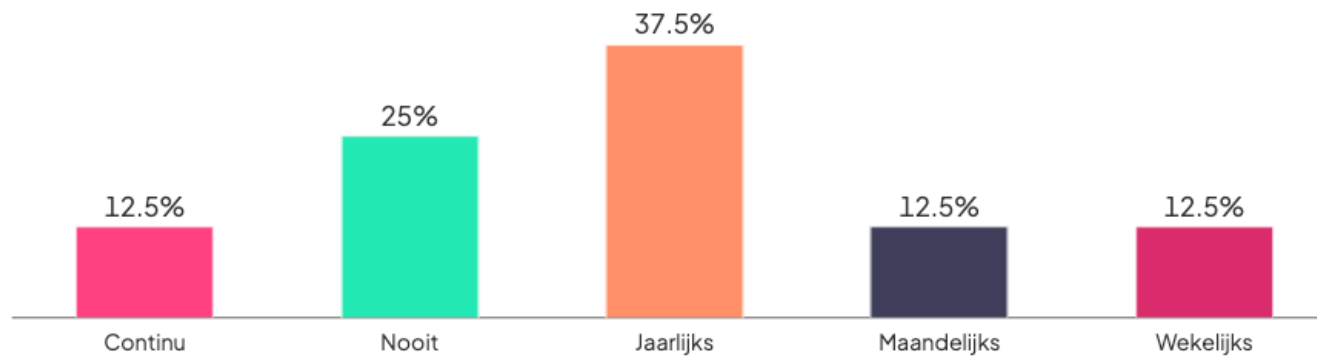
- Vuln scanners
 - Intern
 - Extern
 - Applicaties
- Benchmarks (compliance checks)
- OSINT
- Pentesting/Red Teaming
- Bug bounty/CVD
- Beheerders (leveranciers, medewerkers)



Poll

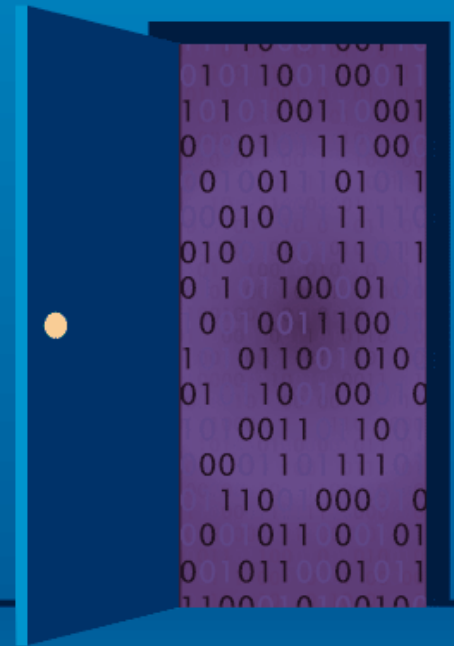


Hoe vaak voeren jullie kwetsbaarheden scans uit?



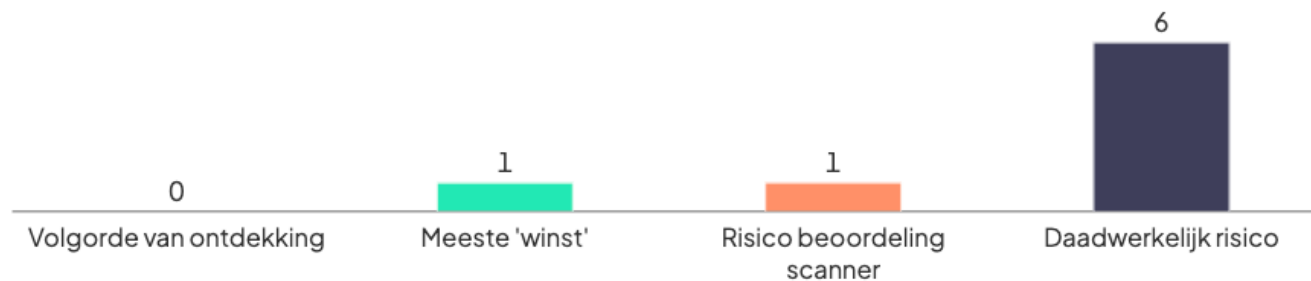
Analyse

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



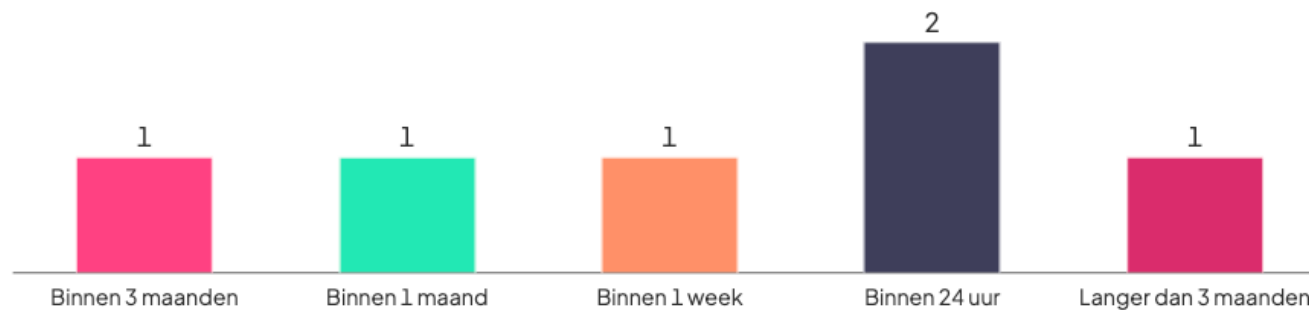
Poll

Hoe prioriteer je het adresseren van kwetsbaarheden?



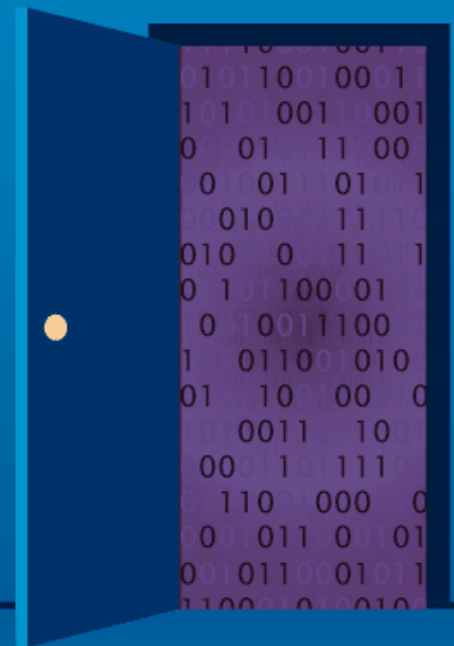
Poll

Binnen welke periode moeten kritische kwetsbaarheden worden geadresseerd?



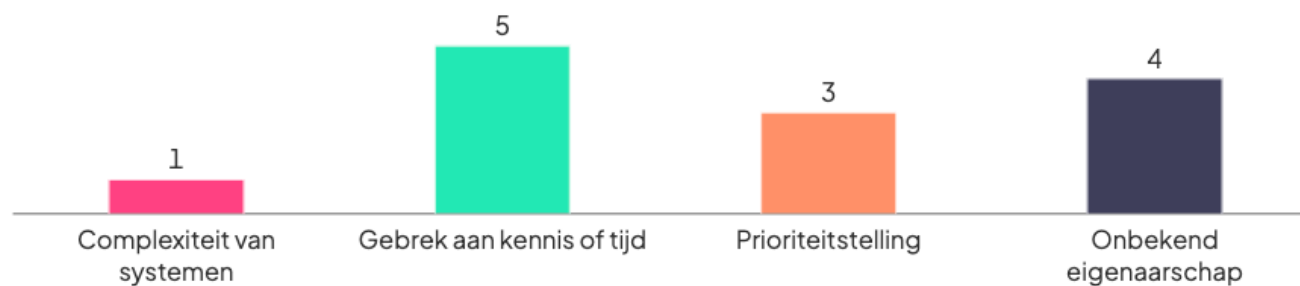
Oplossen

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



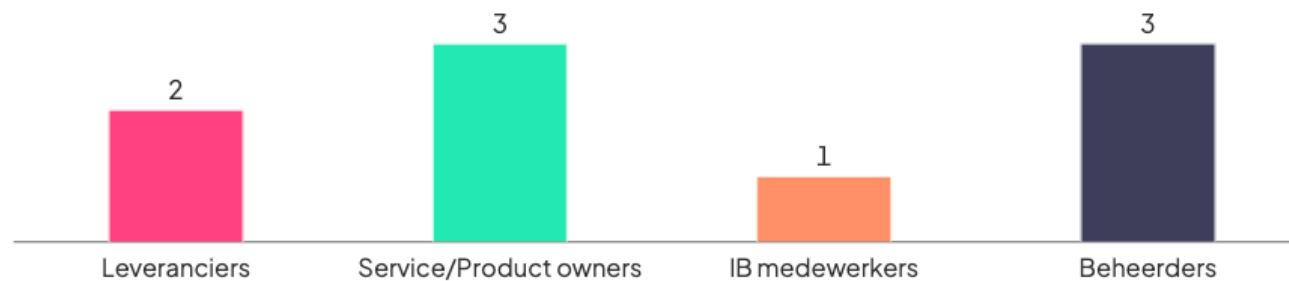
Poll

Wat is jullie grootste uitdaging bij het oplossen van kwetsbaarheden?



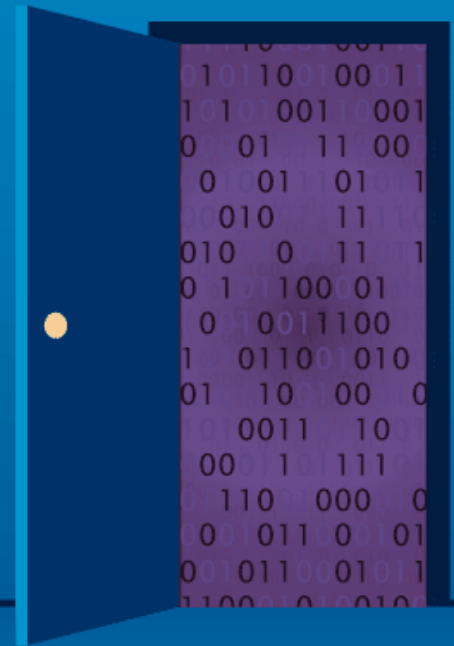
Poll

Wie is er verantwoordelijk voor vulnerability management



Controleren

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



Initiatief weerbaarheidstesten - eduC2

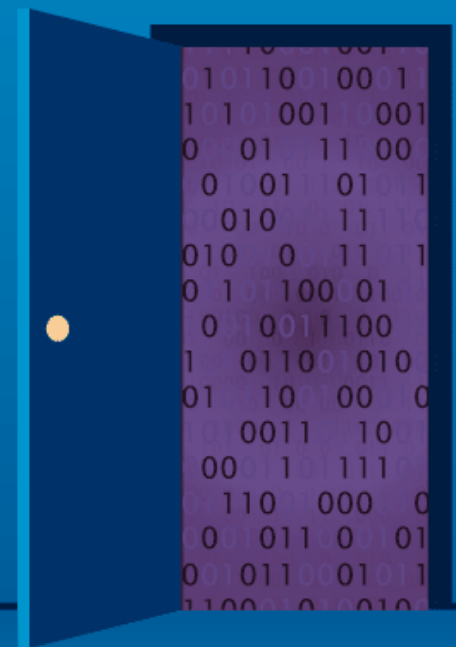
Met remote testen identificeren we kwetsbaarheden en misconfiguraties in het interne aanvalsoppervlak (netwerk, AD/Entra ID)

Doelen:

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

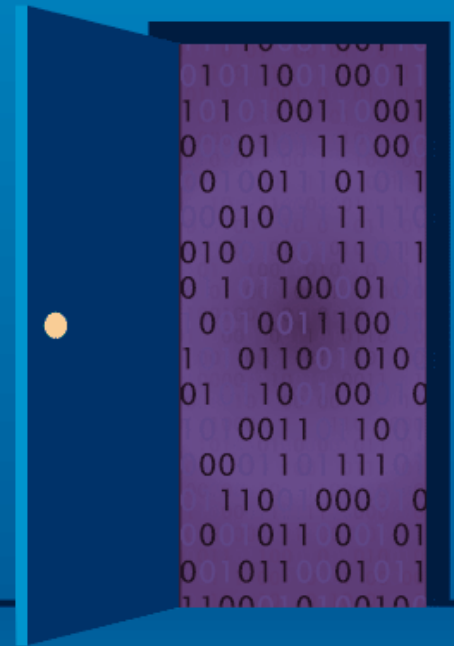
Draagt bij aan:

- 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



Testen EduC2

- Soma College
- Zadkine
- Zone College



Poll



Suggesties voor testmogelijkheden EduC2

Kerberos,

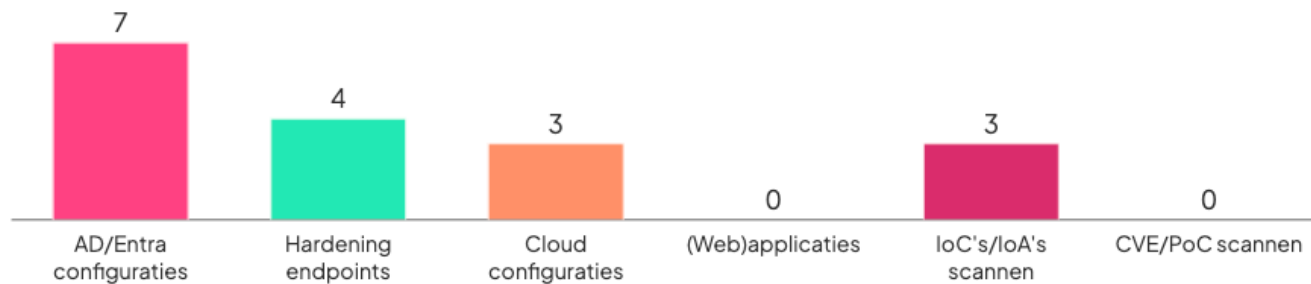
Segmenteren (het ontbreken ervan) en
clientisolation activering

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

Poll

Welke testen vinden jullie het waardevolst om toe te voegen



Initiatief weerbaarheidstesten - Attack Surface Management

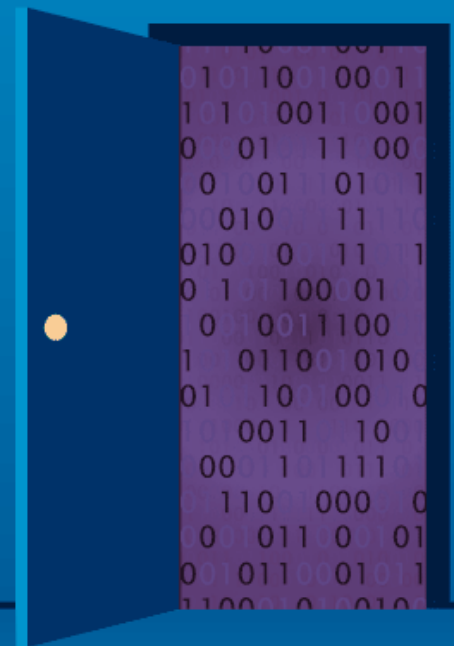
Inzicht krijgen en houden in alle systemen, applicaties, diensten en configuraties die vanaf buiten zichtbaar en bereikbaar zijn. ASM toont welke digitale "ingangen" een organisatie onbedoeld of ongecontroleerd aan de buitenwereld presenteert.

Doelen:

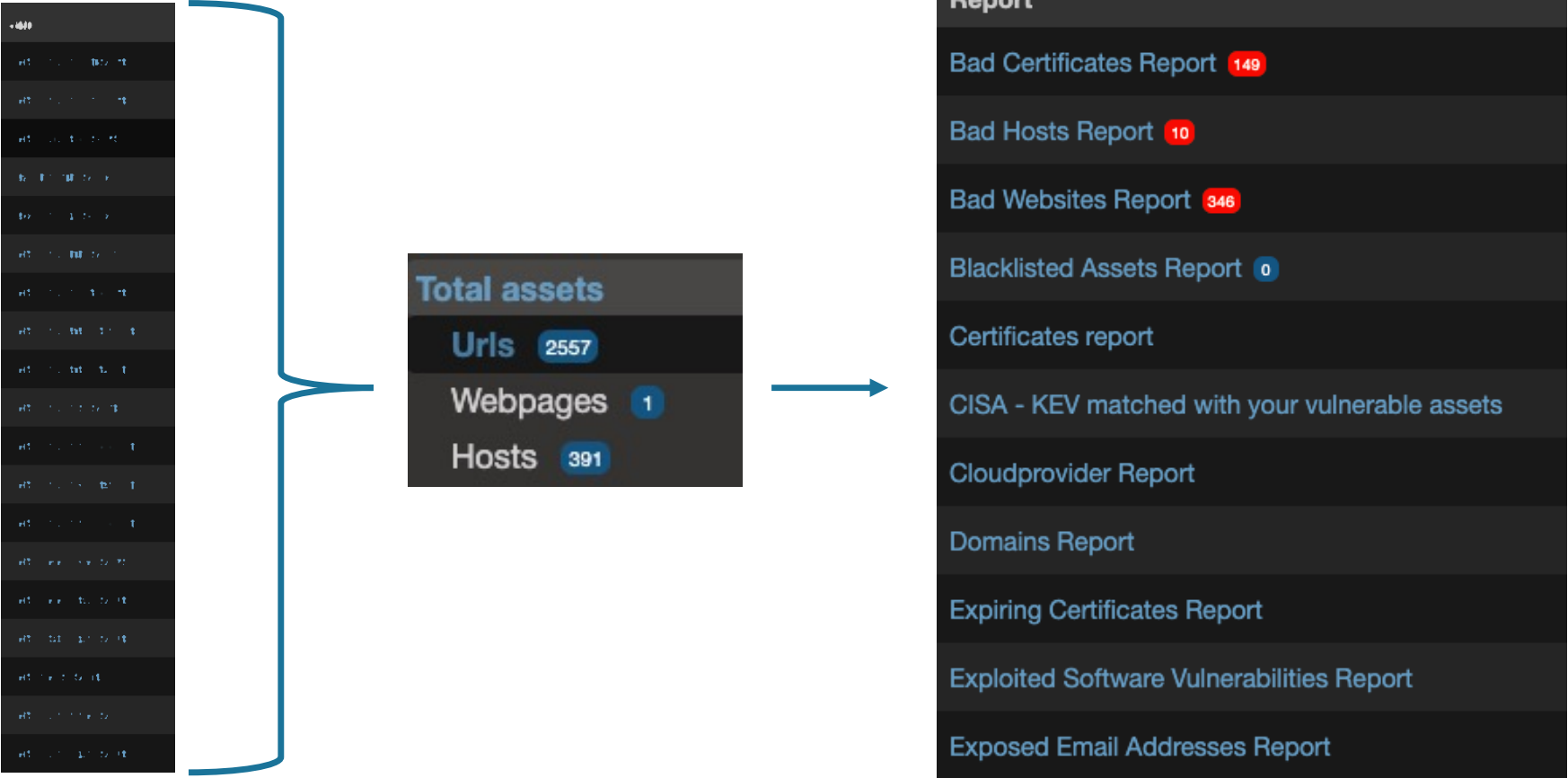
- Continu inzicht krijgen in alle extern zichtbare systemen, diensten en configuraties.
- Onbedoelde blootstelling (shadow IT, vergeten assets, misconfiguraties) snel identificeren.
- Het aanvalsoppervlak verkleinen.

Waar draagt het aan bij:

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

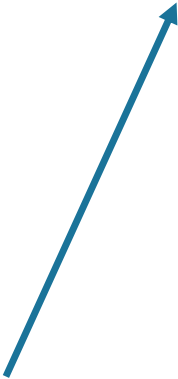


Attack Surface Management



Attack Surface Management

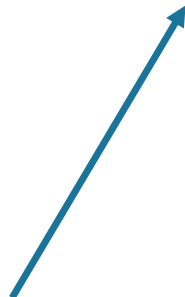
Report
Bad Certificates Report 149
Bad Hosts Report 10
Bad Websites Report 346
Blacklisted Assets Report 0
Certificates report
CISA - KEV matched with your vulnerable assets
Cloudprovider Report
Domains Report
Expiring Certificates Report
Exploited Software Vulnerabilities Report
Exposed Email Addresses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



email_address	found_on	data_breaches
		Gravatar (2020-10-03)
		SynthientCredentialStuffingThreatData (2025-04-11)
		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)
		LinkedInScape (2021-04-08), PDL (2019-10-16), YouveBeenScraped (2018-10-05), LinkedIn (2012-05-05)
		Dropbox (2012-07-01)
		PDL (2019-10-16), Apollo (2018-07-23)
		SynthientCredentialStuffingThreatData (2025-04-11), LinkedInScape (2021-04-08), PDL (2019-10-16), VerificationsIO (2019-02-25), YouveBeenScraped (2018-10-05), LinkedIn (2012-05-05)
		PDL (2019-10-16), VerificationsIO (2019-02-25)
		VerificationsIO (2019-02-25)
		VerificationsIO (2019-02-25)
		SynthientCredentialStuffingThreatData (2025-04-11), Twitter200M (2021-01-01), OnlinerSpambot (2017-08-28), MDPI (2016-08-30), Dropbox (2012-07-01)
		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)

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	



Apache HTTP Server 2.4.46	CVE-2024-38475	CVE-2023-25690	CVE-2022-23943
	CVE-2022-22721	CVE-2022-22720	CVE-2021-44790
	CVE-2021-38275	CVE-2021-26691	CVE-2024-27316
	CVE-2023-38709	CVE-2022-22719	CVE-2021-44224
	CVE-2021-40438	CVE-2021-36160	CVE-2021-34798
	CVE-2021-33193	CVE-2021-32785	CVE-2021-26690
	CVE-2020-35452	CVE-2020-13950	CVE-2021-32792
	CVE-2021-32791	CVE-2021-32786	CVE-2021-30641
	CVE-2020-13938	CVE-2019-17567	
Apache HTTP Server 2.4.52	CVE-2024-38475	CVE-2023-25690	CVE-2022-23943
	CVE-2022-22721	CVE-2022-22720	CVE-2021-44790
	CVE-2024-27316	CVE-2023-38709	CVE-2022-22719
PHP 7.2.34	CVE-2024-25117	CVE-2022-37454	CVE-2022-31629
	CVE-2022-31628	CVE-2019-11038	
Tomcat 8.5.41	CVE-2025-24813	CVE-2020-1938	CVE-2023-44487
	CVE-2022-29885	CVE-2022-25762	CVE-2021-25122
	CVE-2020-17527	CVE-2020-13935	CVE-2020-13934
	CVE-2020-11996	CVE-2019-17563	CVE-2024-21733
	CVE-2021-33037	CVE-2021-30640	CVE-2021-25329
	CVE-2021-24122	CVE-2020-9484	CVE-2020-1935
	CVE-2020-13943	CVE-2019-2684	CVE-2019-12418

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



Amazon Cloud	42
Microsoft	27
Azure	
Microsoft	14
Worldwide	
Public Cloud	
Microsoft	10
Azure	
Microsoft	8
Cloudflare	4
Google Cloud	3
Cloudflare	2
Google	1
Oracle Cloud	1

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	

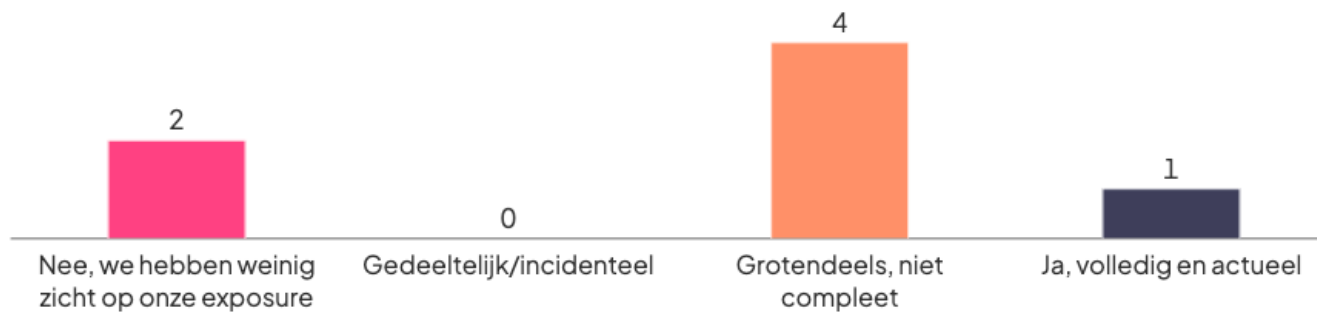
https_status	grade
200 OK	F
Max retries exceeded	F
200 OK	F
400 Bad request	F
Connection refused	F
200 OK	F
400 Bad request	F

Organization	
Summary	Missing security headers
	Outdated software
Hosted at	
First seen	2025-11-13 06:41:38 UTC
Last seen	2025-12-10 09:45:39 UTC
Last check	2025-12-10 09:45:39 UTC
Next check	2025-12-11 09:46:32 UTC
Grade	F
HTTP status	301 Moved permanently
HTTP redirects	301 Moved permanently
HTTP server	nginx
HTTPS status	200 OK
HTTPS redirect	-
HTTPS server	nginx
JARM hash	2ad2ad0002ad2ad22c42d42d000000bdfc58c9a46434368cf60aa440385763
MMH3 hash	-1074798861
Google Analytics ID	
Meta Pixel ID	
Sets cookie on load (http)	no, and this passes the EU Cookie Law.
Sets cookie on load (https)	no, and this passes the EU Cookie Law.

Poll

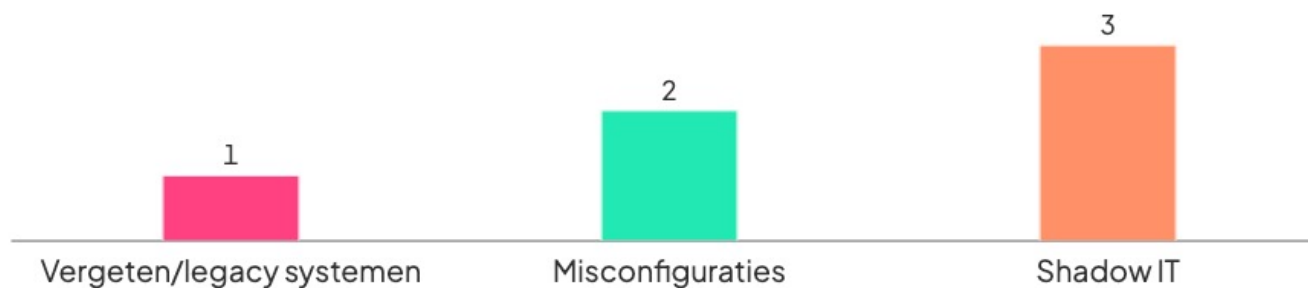


Heeft jouw organisatie een volledig en actueel overzicht van alle extern zichtbare assets?

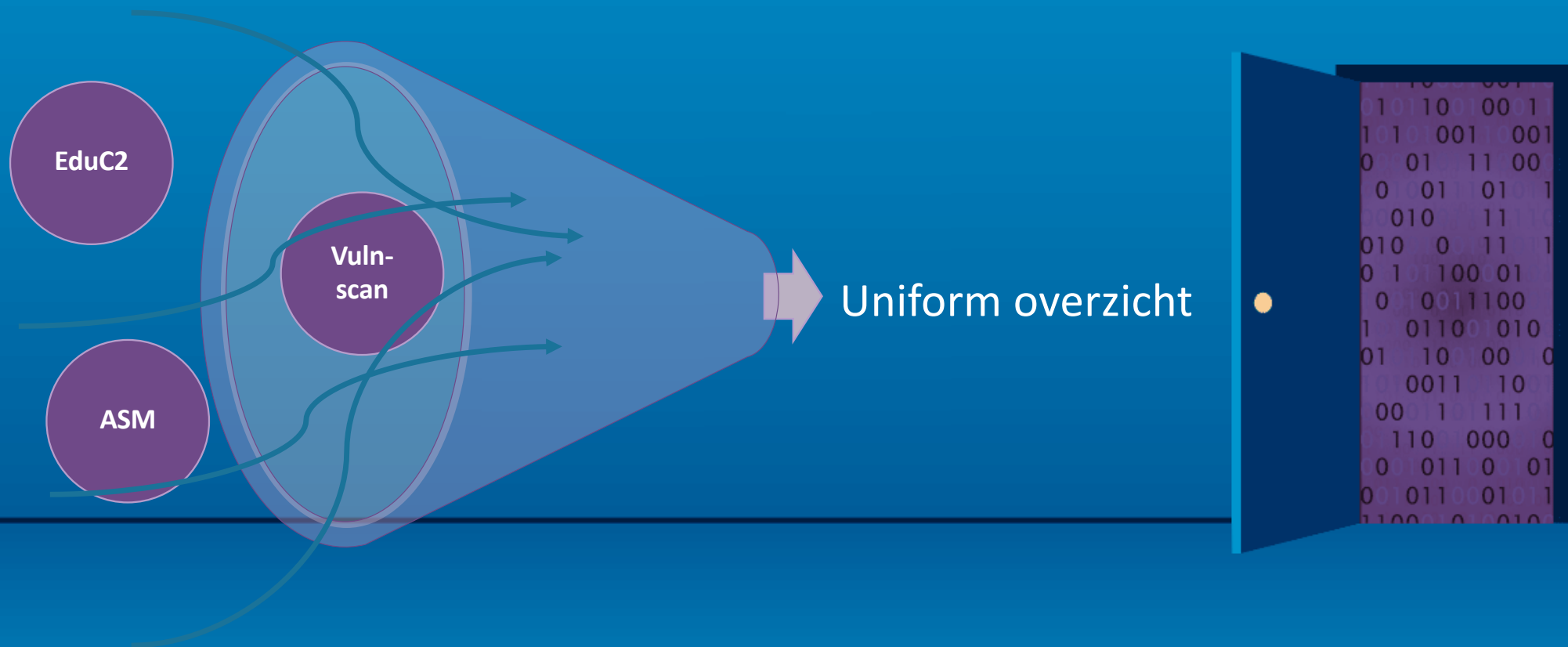


Poll

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



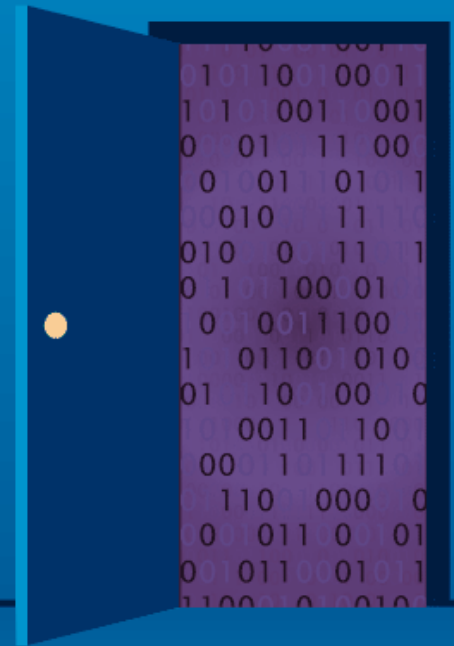
Meerdere diensten



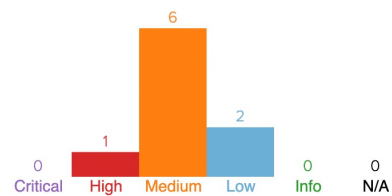
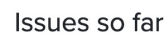
Initiatief weerbaarheidstesten – 'projectmanagement'

Geleerd bij het 'van check tot hack' traject.

10 instellingen x 5/6 checks = 🤯



Bevindingen



High

- ## Apache Axis End of Life (EOL) Detection

Medium

- 🚩 FTP Unencrypted Cleartext Login
- 🚩 Missing 'HttpOnly' Cookie Attribute (HTTP)
- 🚩 SSL/TLS: Deprecate TLSv1.0 and TLSv1.1 Protocol Detection
- 🚩 Weak Encryption Algorithm(s) Supported (SSH)
- 🚩 Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
- 🚩 Weak MAC Algorithm(s) Supported (SSH)

Project team



You don't have any methodologies yet

Use methodologies to ensure consistency across all of your projects.

 [Go To Methodologies](#)

[More about methodologies](#)

Recent activity

All Activity

- Updated the [ICMP Timestamp Reply](#) issue.
 - Updated the [TCP Timestamp Information](#) issue.
 - Updated the [Weak Key Exchange \(KEX\) in SSH](#) issue.
 - Updated the [FTP Unencrypted Cleartext](#) issue.
 - Updated the [Weak Encryption Algorithm\(s\)](#) issue.
 - Updated the [Missing 'HttpOnly' Cookie](#) issue.
 - Updated the [Weak MAC Algorithm\(s\)](#) issue.

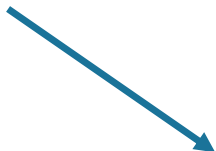
Bevindingen

High
 Apache Axis End of Life (EOL) Detection
Medium
 FTP Unencrypted Cleartext Login
 Missing 'HttpOnly' Cookie Attribute (HTTP)
 SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
 Weak Encryption Algorithm(s) Supported (SSH)
 Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
 Weak MAC Algorithm(s) Supported (SSH)
Low
 ICMP Timestamp Reply Information Disclosure
 TCP Timestamps Information Disclosure

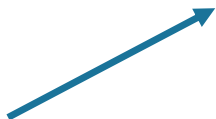
Normalisatie



Attack Surface Management



External vuln scanning

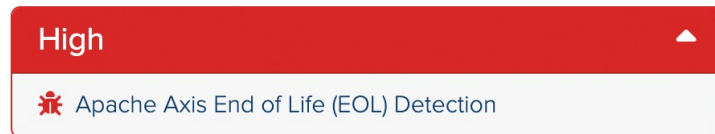


High



Apache Axis End of Life (EOL) Detection

Normalisatie - voordelen



Hogere integriteit



Minder (duplicate) meldingen



Betere performance

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

Prioritering (adressering!)

Apache Axis End of Life (EOL) Detection

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.

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.

Handelingsperspectief

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 expect to create an Axis 1.x release fixing these flaws - If the remote installation has an override for this result

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 remediëringsschappen 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.

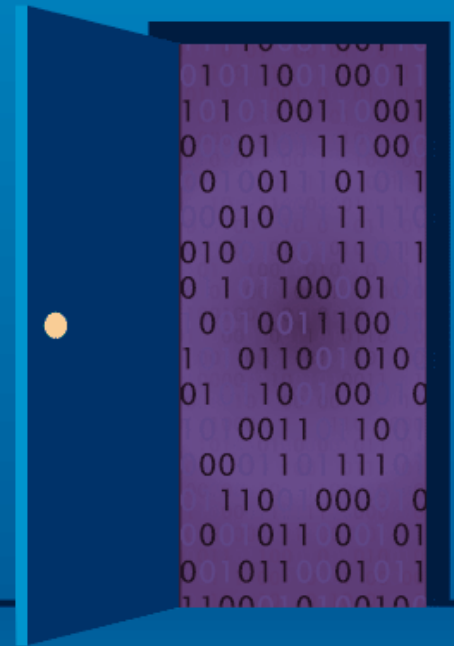
Toekomst

Ontwikkelen detecties EduC2.

Ontwikkelen normalisatie.

Ontwikkelen handelingsperspectief.

En het inrichten van alle bijbehorende processen.



Kwetsbaarheden opsporen en oplossen

Voor vragen:

m.deben@mbodigitaal.nl

r.boxem@mbodigitaal.nl