mbo digitaal

Kwetsbaarheden opsporen en oplossen

TLP: AMBER+STRICT

SAMENWERKEN AAN CYBERVEILIGHEID IN HET MBO

11 december 2025

Mick Deben & Ry Boxem

PROGRAMMA Cyberveiligheid

NETWERK Informatiebeveiliging en Privacy

MBO Raad

mbo digitaal

mbodigitaal.nl/cyberveiligheid

mbo digitaal

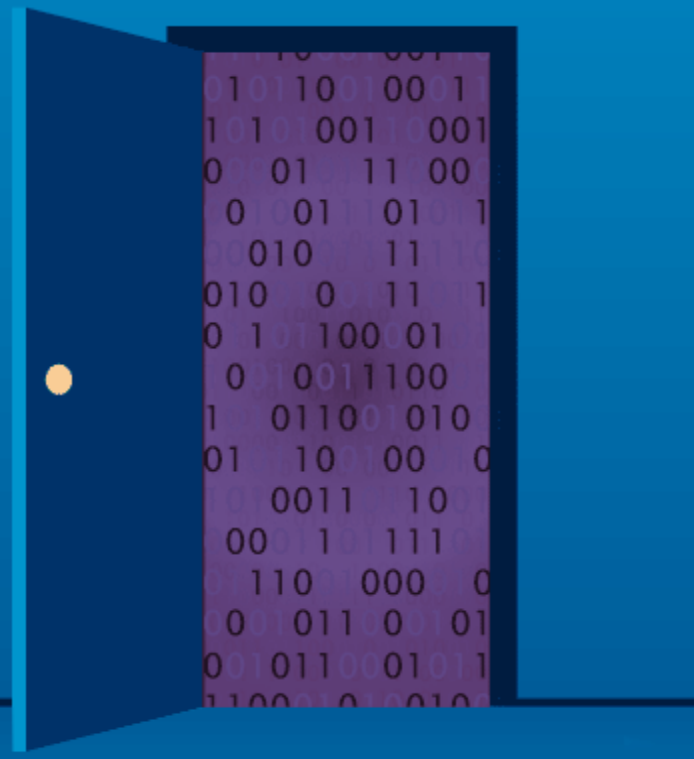
Inhoud

Introductie

Levencyclus kwetsbaarheid

Initiatief weerbaarheidstesten

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



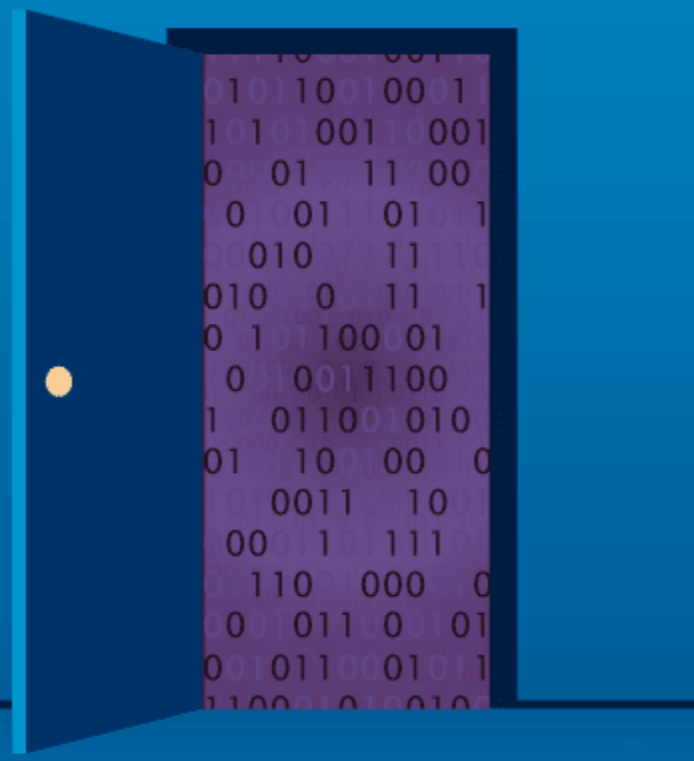
mbo digitaal

Introductie

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

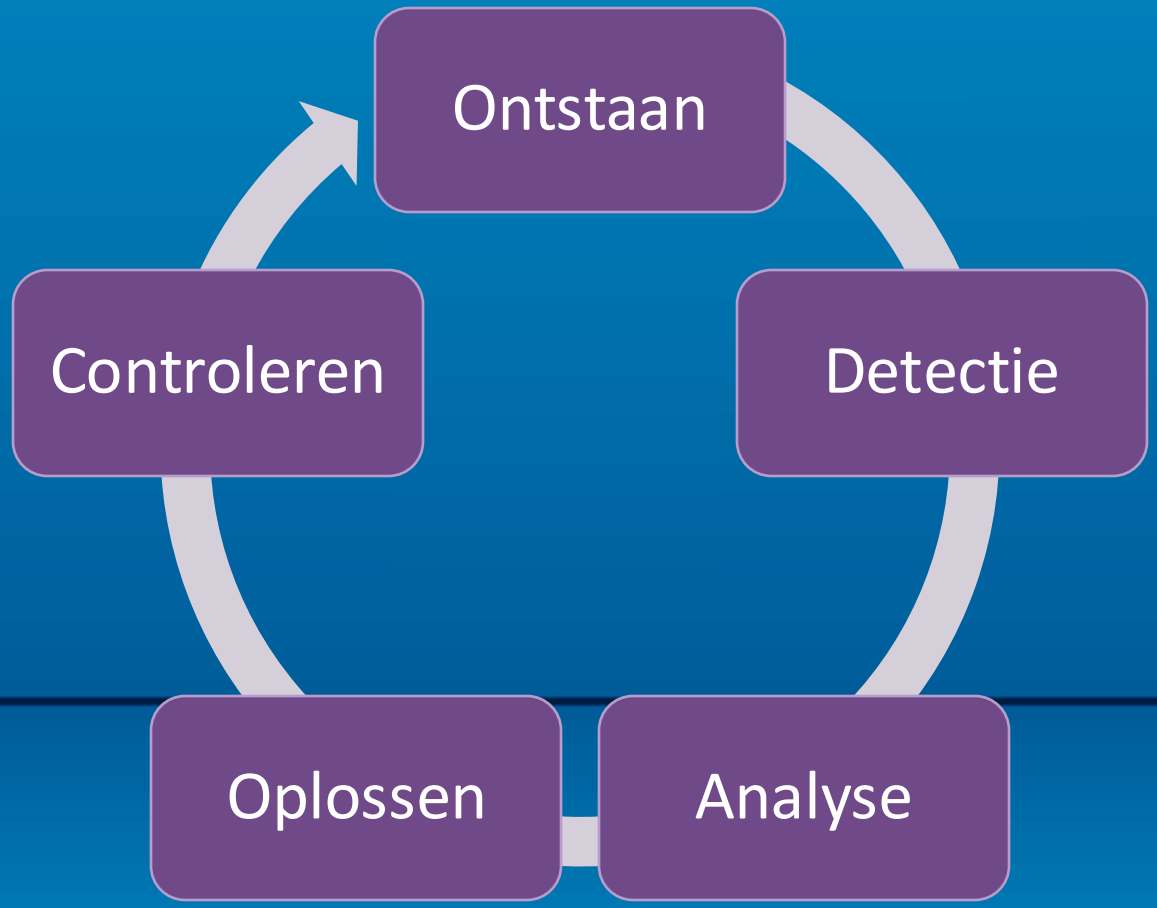
- **Belang van vulnerability management:** vrijwel alle grote cyberincidenten terug te voeren zijn op misbruik van bekende **kwetsbaarheden,** eventueel in combinatie met andere aanvalstechnieken.

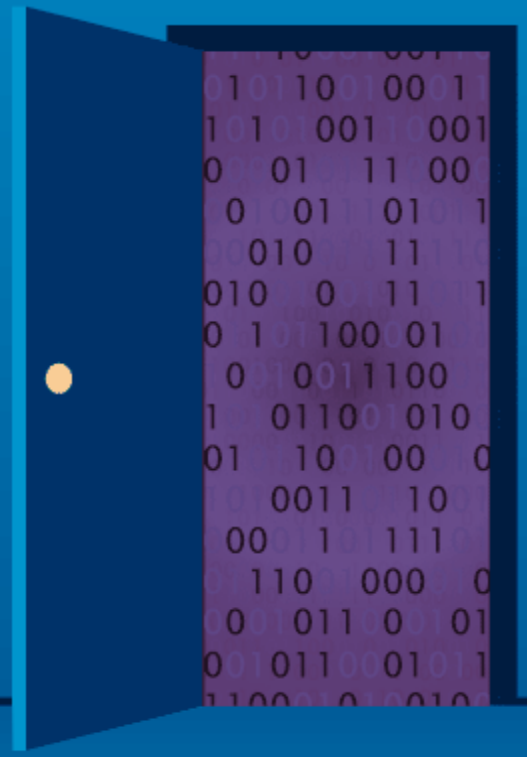
Kwetsbaarheid: *“blootgesteld kunnen worden aan risico en onzekerheid.”*



mbo digitaal

Levencyclus van een kwetsbaarheid

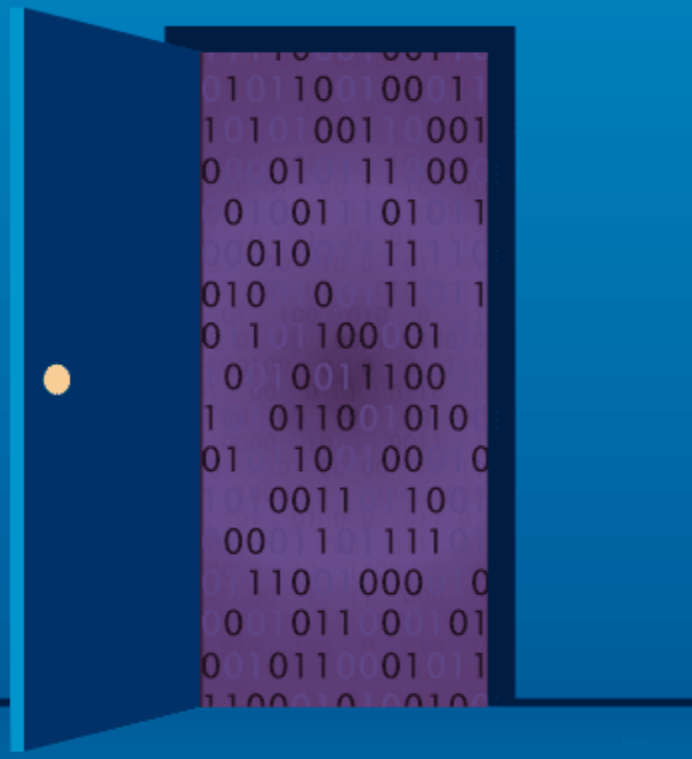




mbo digitaal

Ontstaan

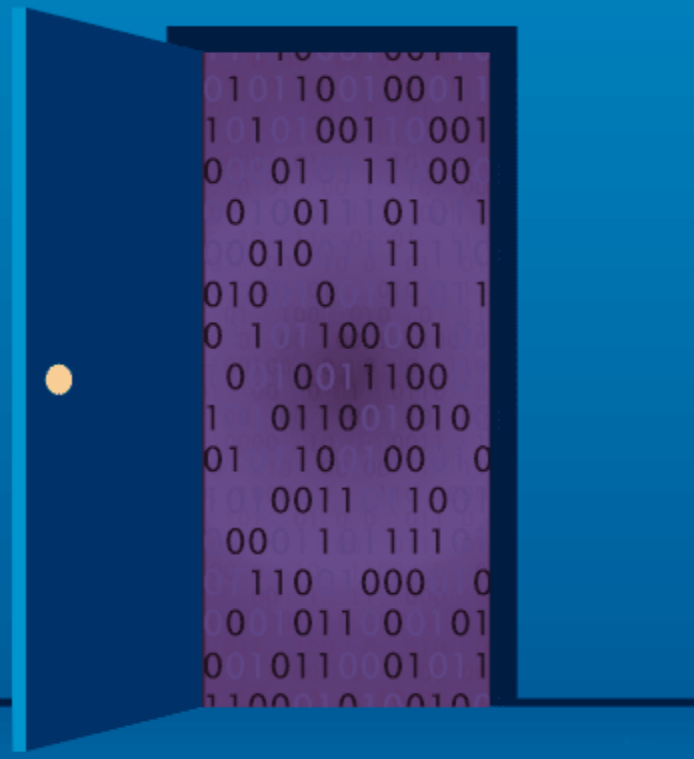
- Fout in ontwerp, code of configuratie
- Verouderde of niet-gepatchte software
- Complexiteit meer kans op menselijke fouten
- Nieuwe features zonder security-review
- Onvoldoende hardening / baseline-beheer



mbo digitaal

Detectie

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



Poll

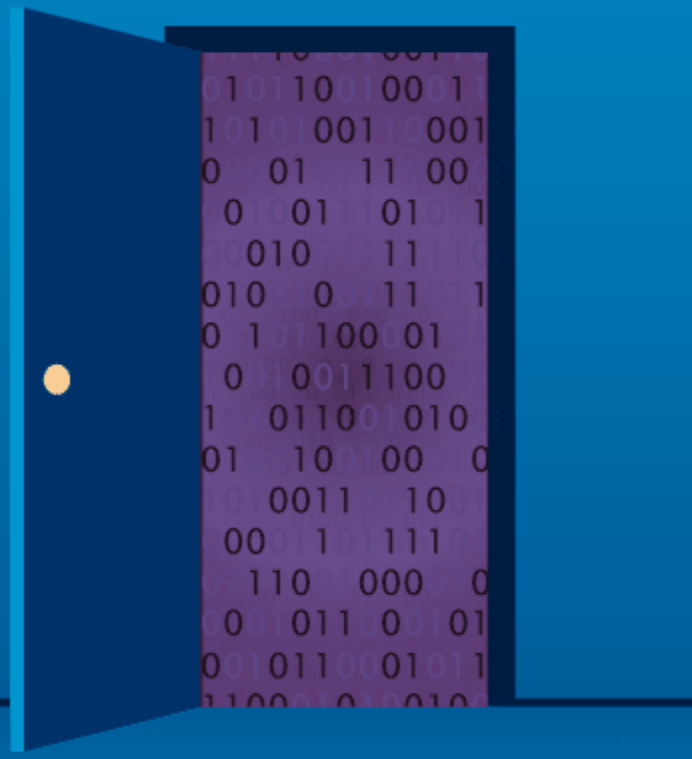
ahaslides.com/AZ3N8

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



Poll (2x)

ahaslides.com/AZ3N8

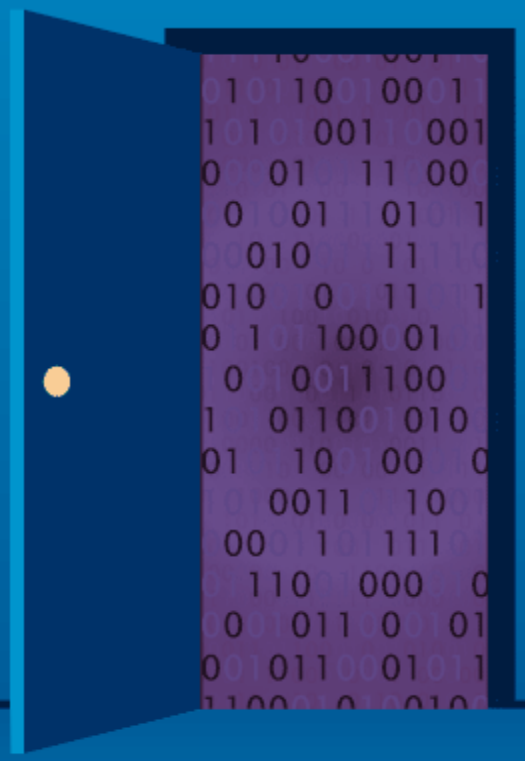
Hoe prioriteer je het adresseren van kwetsbaarheden?

Binnen welke periode moeten kritische kwetsbaarheden worden geadresseerd?

mbo digitaal

Oplossen

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



Poll (2x)

ahaslides.com/AZ3N8

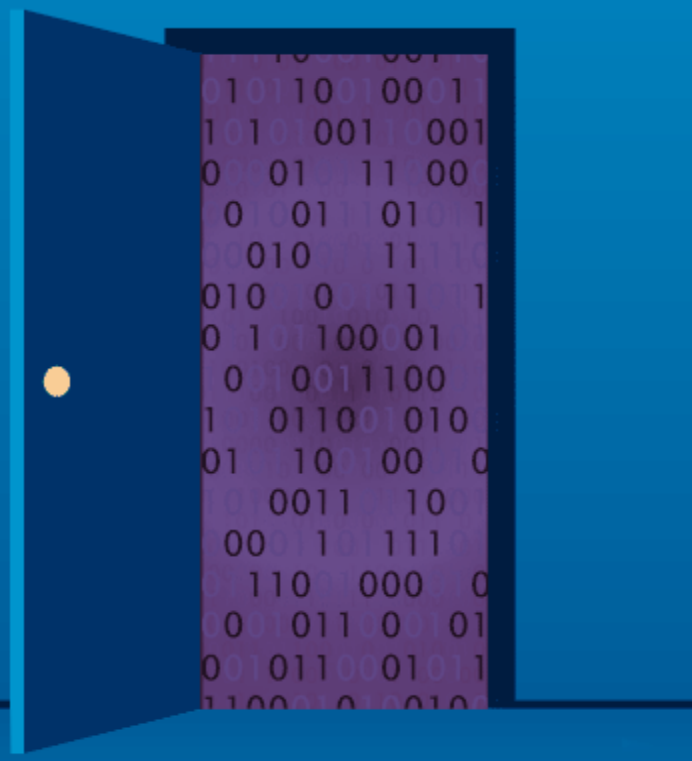
Wat is jullie grootste uitdaging bij het oplossen van kwetsbaarheden?

Wie is er verantwoordelijk voor vulnerability management

mbo digitaal

Controleren

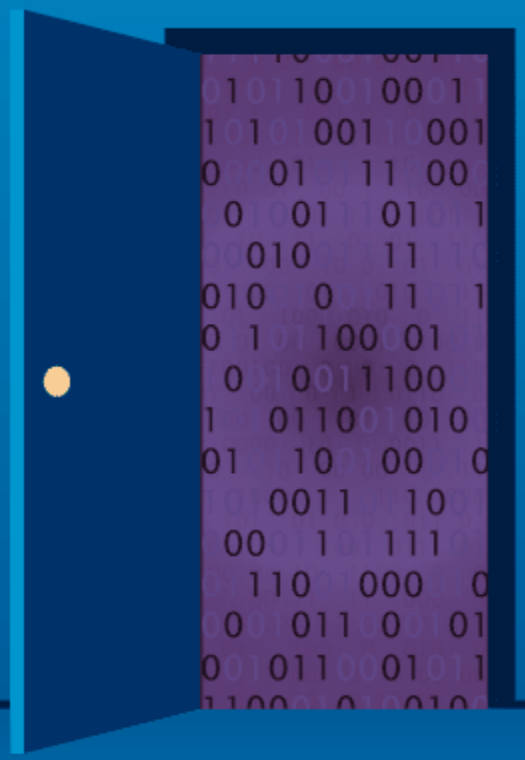
- Herscan of opnieuw testen
- Controleren of mitigerende/compenserende maatregelen gewenst effect hebben



mbo digitaal

Initiatief weerbaarheidstesten - eduC2

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



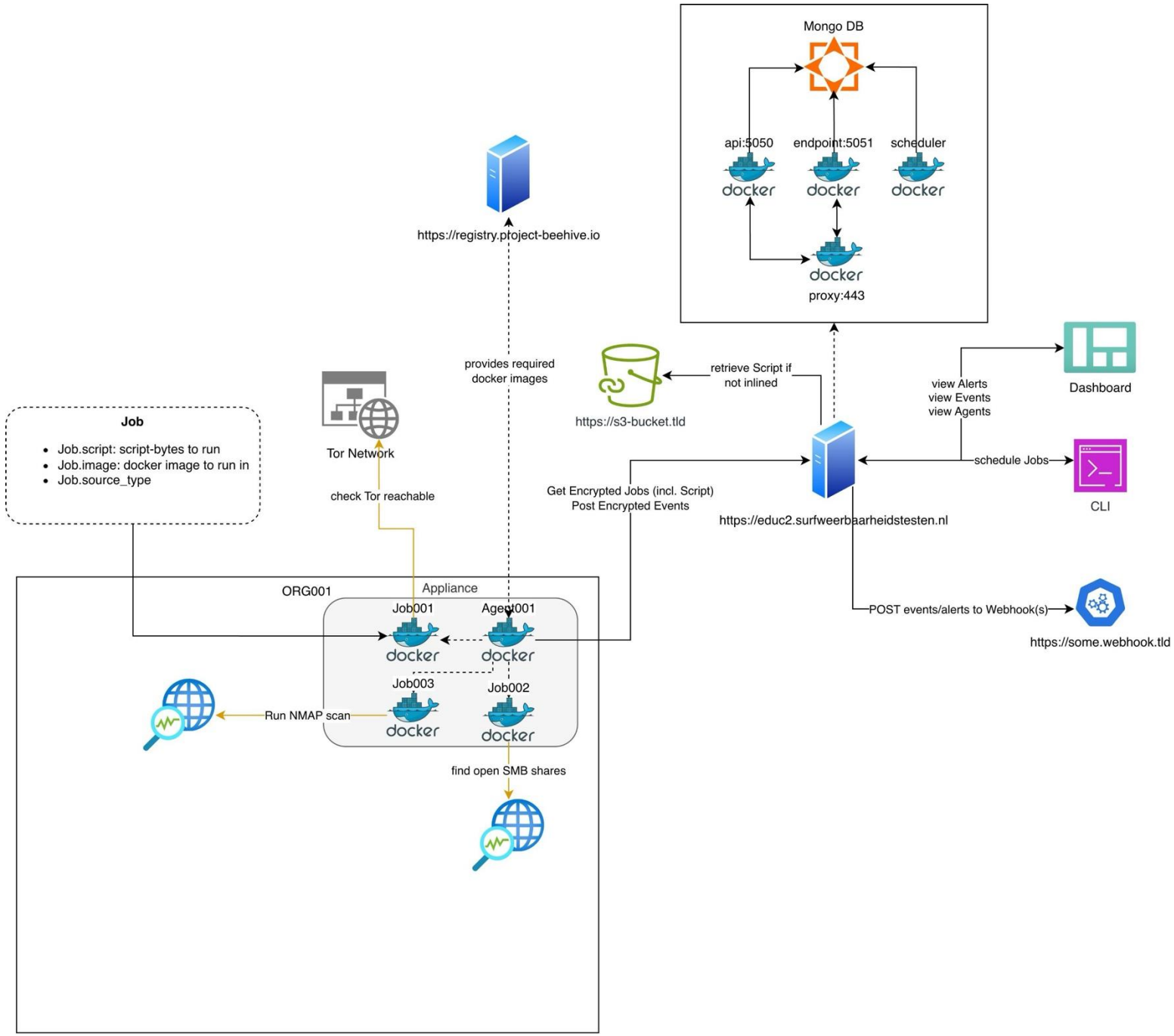
Doelen:

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

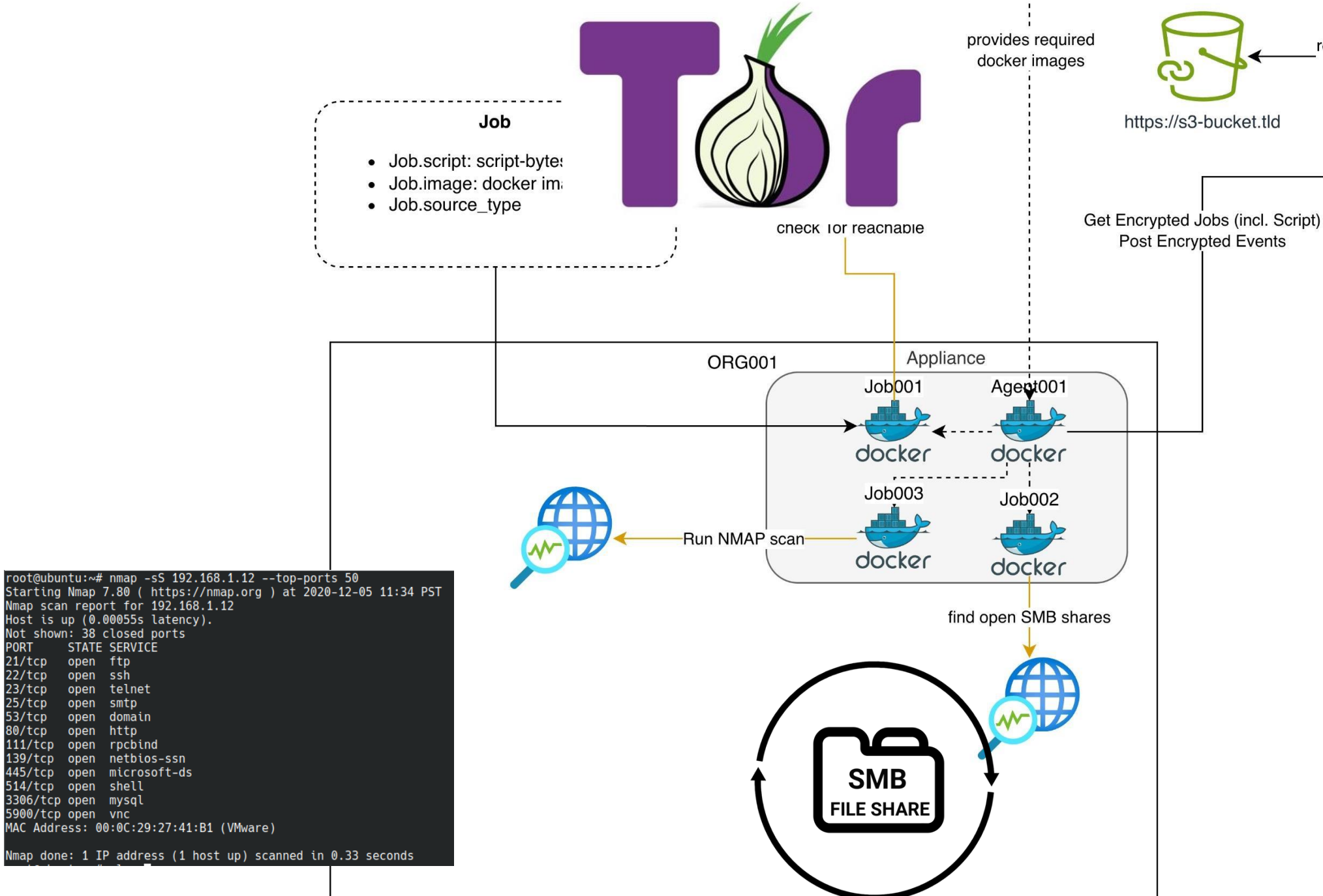
Draagt bij aan:

- 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

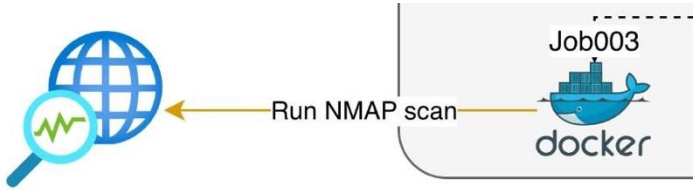


mbo digitaal

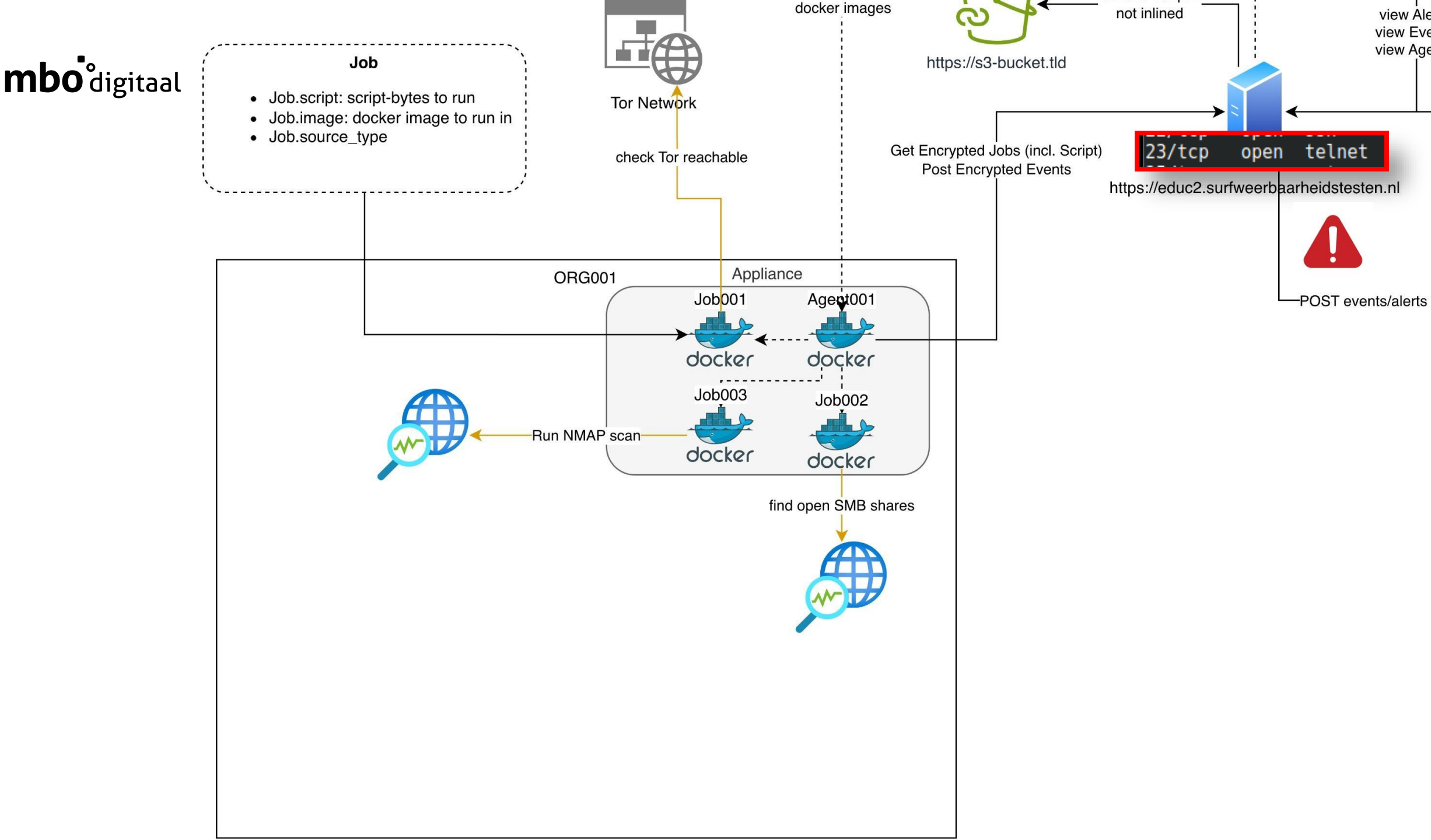


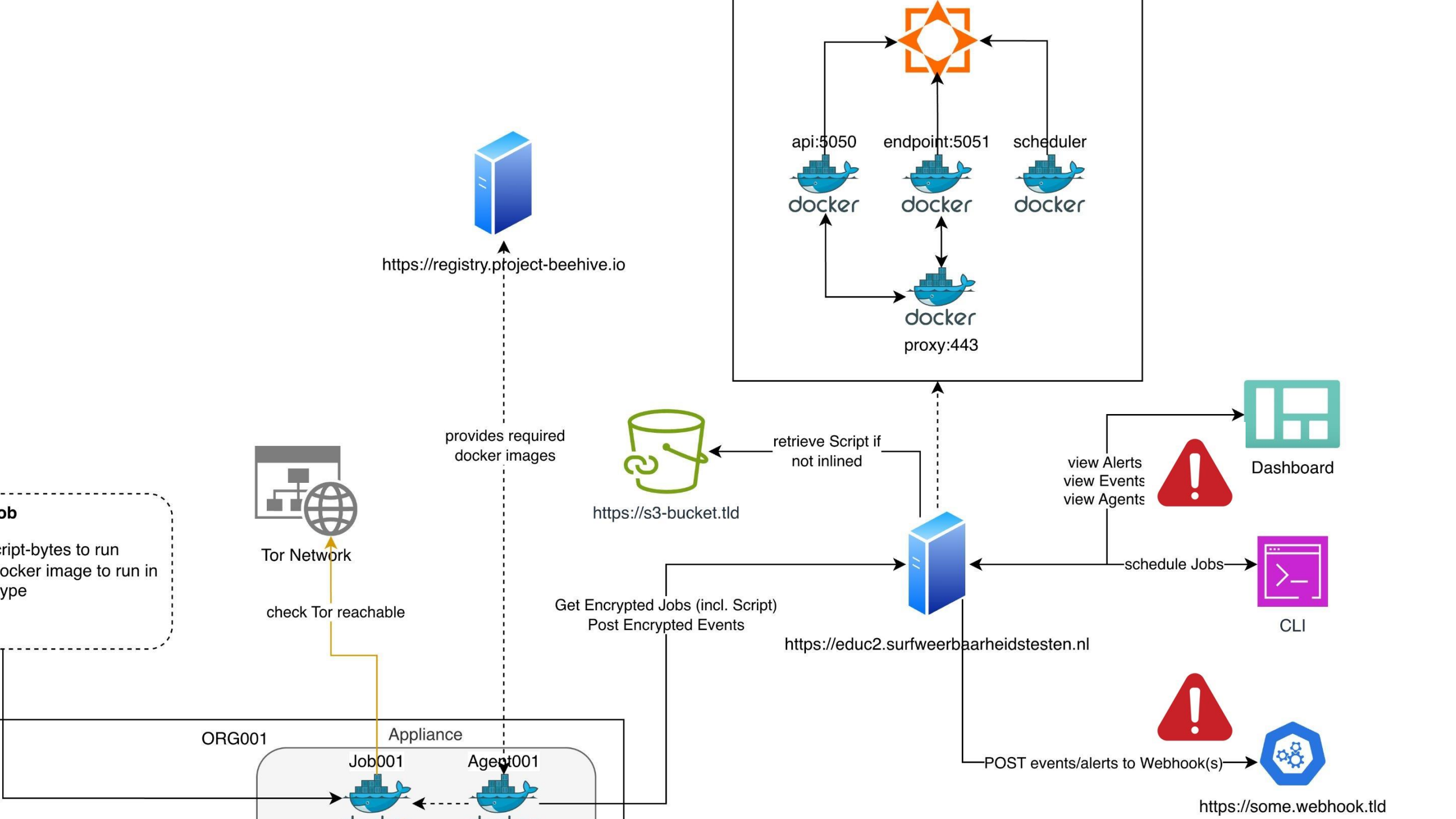

```
root@ubuntu:~# nmap -sS 192.168.1.12 --top-ports 50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-05 11:34 PST
Nmap scan report for 192.168.1.12
Host is up (0.00055s latency).
Not shown: 38 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
514/tcp  open  shell
3306/tcp open  mysql
5900/tcp open  vnc
MAC Address: 00:0C:29:27:41:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

mbo digitaal

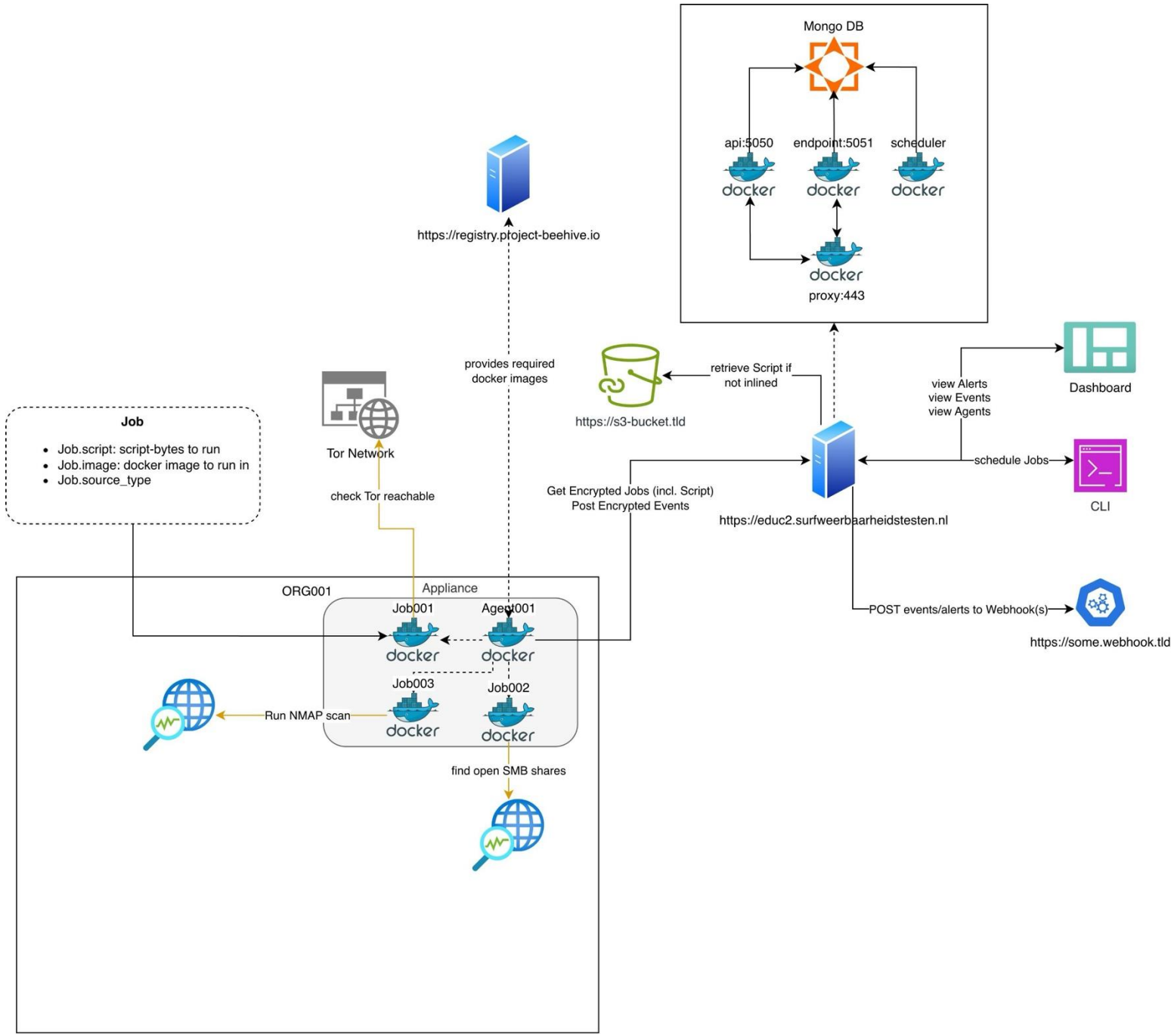



```
root@ubuntu:~# nmap -sS 192.168.1.12 --top-ports 50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-05 11:34 PST
Nmap scan report for 192.168.1.12
Host is up (0.00055s latency).
Not shown: 38 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
514/tcp  open  shell
3306/tcp open  mysql
5900/tcp open  vnc
MAC Address: 00:0C:29:27:41:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```


Job
Job.script: script-bytes to run
Job.image: docker image to run in
Job.source_type
Tor Network
check Tor reachable
docker images
not inlined
https://s3-bucket.tld
Get Encrypted Jobs (incl. Script)
Post Encrypted Events
23/tcp open telnet
https://educ2.surfweerbaarheidstesten.nl
POST events/alerts
ORG001
Appliance
Job001
Agent001
Job003
Job002
Run NMAP scan
find open SMB shares


api:5050
endpoint:5051
scheduler
docker
docker
docker
docker
proxy:443
https://registry.project-beehive.io
provides required
docker images
https://s3-bucket.tld
retrieve Script if
not inlined
view Alerts
view Events
view Agents
Dashboard
Tor Network
check Tor reachable
schedule Jobs
CLI
Get Encrypted Jobs (incl. Script)
Post Encrypted Events
https://educ2.surfweerbaarheidstesten.nl
POST events/alerts to Webhook(s)
https://some.webhook.tld
ORG001
Appliance
Job001
Agent001

mbo digitaal



mbo digitaal

EduC2
Dashboard

Dashboard Jobs Scheduler Events Agents Organizations Download Report Config Logout

Status	UUID	Created	Organization	Job	Agent	Source	Data
⚠	6924f2e2e5988ea2f991550a	2025-11-25T00:05:54.009000Z	Organization 001	NMAP Vunerability Scan	Agent 001	nmap_vulnerability_scan	{ "status": true, "hosts": [{ "IP": "192.168.2.115", "cves": [{ "id": "CVE-2020-1472", "cvss": 10 }] }] }
⚠	6924f2e0e5988ea2f9915500	2025-11-25T00:05:52.006000Z	Organization 002	NMAP Vunerability Scan	Agent 002	nmap_vulnerability_scan	{ "status": true, "hosts": [{ "IP": "192.168.2.115", "cves": [{ "id": "CVE-2020-1472", "cvss": 10 }] }] }
⚠	6924f289e5988ea2f9915469	2025-11-25T00:04:25.006000Z	Organization 002	Tor Check	Agent 002	tor_access	{ "status": true, "ip": "185.220.101.37" }
⚠	6924f283e5988ea2f9915458	2025-11-25T00:04:19.005000Z	Organization 001	Tor Check	Agent 001	tor_access	{ "status": true, "ip": "185.220.101.99" }
⚠	6924f20ae5988ea2f991532e	2025-11-25T00:02:18.008000Z	Organization 001	Detect NBNS	Agent 001	nbns	{ "status": true, "hosts": [{ "IP": "192.168.2.115" }] }
⚠	6924f208e5988ea2f9915324	2025-11-25T00:02:16.005000Z	Organization 002	Detect NBNS	Agent 002	nbns	{ "status": true, "hosts": [{ "IP": "192.168.2.115" }] }
✓	6924f1cee5988ea2f9915295	2025-11-25T00:01:18.009000Z	Organization 002	SSH Banner Grab	Agent 002	ssh_banner	{ "host": "192.168.2.115", "banner": { "host": "192.168.2.115", "port": 22, "key_type": "ssh-ed25519", "fingerprint_md5": "b2:d9:58:14:dd:4c:69:c4:10:16:94:0c:93:6c:da:b9", "fingerprint_sha256": "4a09c526c21befac6651625f3153e34500a9bc286d356a0867f934d2dd40a8a5", "fingerprint_sha256_base64": "SHA256:SgnFJsIb76xmUWJfMVPjRQCpvChtNWoIZ/k00t1AqKU" } }
✓	6924f1c8e5988ea2f9915284	2025-11-25T00:01:12.009000Z	Organization 001	SSH Banner Grab	Agent 001	ssh_banner	{ "host": "192.168.2.115", "banner": { "host": "192.168.2.115", "port": 22, "key_type": "ssh-ed25519", "fingerprint_md5": "b2:d9:58:14:dd:4c:69:c4:10:16:94:0c:93:6c:da:b9", "fingerprint_sha256": "4a09c526c21befac6651625f3153e34500a9bc286d356a0867f934d2dd40a8a5", "fingerprint_sha256_base64": "SHA256:SgnFJsIb76xmUWJfMVPjRQCpvChtNWoIZ/k00t1AqKU" } }
✓	6924f19ee5988ea2f991521e	2025-11-25T00:00:30Z	Organization 001	Find SMB Shares with Guest Access enabled	Agent 001	open_samba_share	{ "status": false, "host": "192.168.2.115", "port": 445 }
✓	6924f199e5988ea2f991520d	2025-11-25T00:00:25.005000Z	Organization 001	Find SMB Shares with Guest Access enabled	Agent 001	open_samba_share	{ "status": false, "host": "192.168.2.115", "port": 139 }

« ‹ 1 2 3 4 5 › » 10

mbo digitaal

n	Job	Agent	Source	D
n	NMAP Vunerability Scan	Agent 001	nmap_vulnerability_scan	{
n	NMAP Vunerability Scan	Agent 002	nmap_vulnerability_scan	{
n	Tor Check	Agent 002	tor_access	{
n	Tor Check	Agent 001	tor_access	{
n	Detect NBNS	Agent 001	nbns	{
n	Detect NBNS	Agent 002	nbns	{
n	SSH Banner Grab	Agent 002	ssh_banner	{ " " "

mbo digitaal

ulnerability_scan	{ "status": true, "hosts": [{ "IP": "192.168.2.115", "cves": [{ "id": "CVE-2020-1472", "cvss": 10 }] }] }
ulnerability_scan	{ "status": true, "hosts": [{ "IP": "192.168.2.115", "cves": [{ "id": "CVE-2020-1472", "cvss": 10 }] }] }
cess	{ "status": true, "ip": "185.220.101.37" }
cess	{ "status": true, "ip": "185.220.101.99" }
	{ "status": true, "hosts": [{ "IP": "192.168.2.115" }] }
	{ "status": true, "hosts": [{ "IP": "192.168.2.115" }] }
nner	{ "host": "192.168.2.115", "banner": { "host": "192.168.2.115", "port": 22, "key_type": "ssh-ed25519", "fingerprint_md5": "b2:d9:58:14:dd:4c:69:c4:10:16:94:0c:93:6c:da:b9", "fingerprint_sha256": "4a09c526c21befac6651625f3153e34500a9bc286d356a0867f934d2dd40a8a5", "fingerprint_sha256_base64": "SHA256:SgnFJsIb76xmUWJfMVPjRQCpvChtNWoIZ/k00t1AqKU" } }
	{ "host": "192.168.2.115", "banner": { "host": "192.168.2.115", "port": 22, "key_type": "ssh-ed25519"

mbo digitaal

EduC2
Dashboard

Dashboard Jobs Scheduler Events Agents Organizations Download Report Config Logout

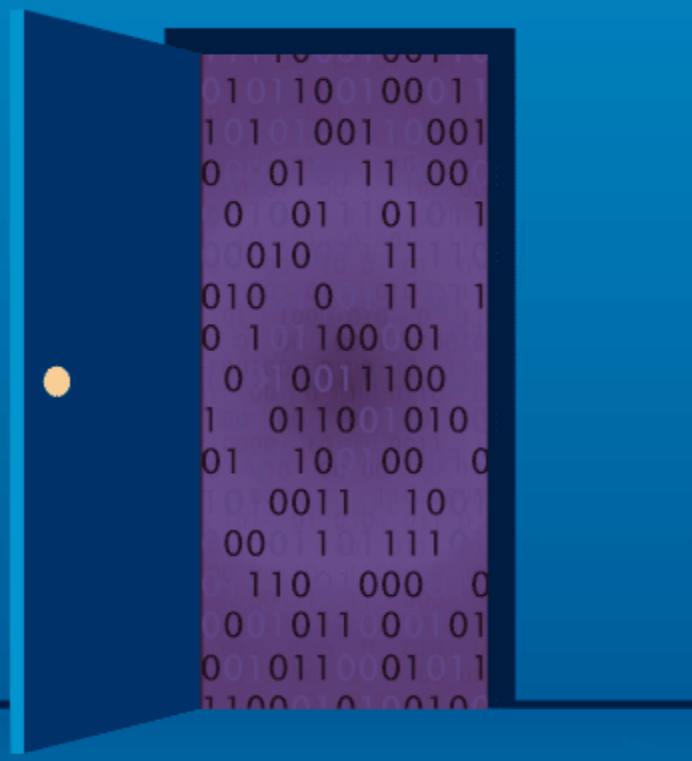
Status	UUID	Created	Organization	Job	Agent	Source	Data
⚠	6924f2e2e5988ea2f991550a	2025-11-25T00:05:54.009000Z	Organization 001	NMAP Vunerability Scan	Agent 001	nmap_vulnerability_scan	{ "status": true, "hosts": [{ "IP": "192.168.2.115", "cves": [{ "id": "CVE-2020-1472", "cvss": 10 }] }] }
⚠	6924f2e0e5988ea2f9915500	2025-11-25T00:05:52.006000Z	Organization 002	NMAP Vunerability Scan	Agent 002	nmap_vulnerability_scan	{ "status": true, "hosts": [{ "IP": "192.168.2.115", "cves": [{ "id": "CVE-2020-1472", "cvss": 10 }] }] }
⚠	6924f289e5988ea2f9915469	2025-11-25T00:04:25.006000Z	Organization 002	Tor Check	Agent 002	tor_access	{ "status": true, "ip": "185.220.101.37" }
⚠	6924f283e5988ea2f9915458	2025-11-25T00:04:19.005000Z	Organization 001	Tor Check	Agent 001	tor_access	{ "status": true, "ip": "185.220.101.99" }
⚠	6924f20ae5988ea2f991532e	2025-11-25T00:02:18.008000Z	Organization 001	Detect NBNS	Agent 001	nbns	{ "status": true, "hosts": [{ "IP": "192.168.2.115" }] }
⚠	6924f208e5988ea2f9915324	2025-11-25T00:02:16.005000Z	Organization 002	Detect NBNS	Agent 002	nbns	{ "status": true, "hosts": [{ "IP": "192.168.2.115" }] }
✓	6924f1cee5988ea2f9915295	2025-11-25T00:01:18.009000Z	Organization 002	SSH Banner Grab	Agent 002	ssh_banner	{ "host": "192.168.2.115", "banner": { "host": "192.168.2.115", "port": 22, "key_type": "ssh-ed25519", "fingerprint_md5": "b2:d9:58:14:dd:4c:69:c4:10:16:94:0c:93:6c:da:b9", "fingerprint_sha256": "4a09c526c21befac6651625f3153e34500a9bc286d356a0867f934d2dd40a8a5", "fingerprint_sha256_base64": "SHA256:SgnFJsIb76xmUWJfMVPjRQCpvChtNWoIZ/k00t1AqKU" } }
✓	6924f1c8e5988ea2f9915284	2025-11-25T00:01:12.009000Z	Organization 001	SSH Banner Grab	Agent 001	ssh_banner	{ "host": "192.168.2.115", "banner": { "host": "192.168.2.115", "port": 22, "key_type": "ssh-ed25519", "fingerprint_md5": "b2:d9:58:14:dd:4c:69:c4:10:16:94:0c:93:6c:da:b9", "fingerprint_sha256": "4a09c526c21befac6651625f3153e34500a9bc286d356a0867f934d2dd40a8a5", "fingerprint_sha256_base64": "SHA256:SgnFJsIb76xmUWJfMVPjRQCpvChtNWoIZ/k00t1AqKU" } }
✓	6924f19ee5988ea2f991521e	2025-11-25T00:00:30Z	Organization 001	Find SMB Shares with Guest Access enabled	Agent 001	open_samba_share	{ "status": false, "host": "192.168.2.115", "port": 445 }
✓	6924f199e5988ea2f991520d	2025-11-25T00:00:25.005000Z	Organization 001	Find SMB Shares with Guest Access enabled	Agent 001	open_samba_share	{ "status": false, "host": "192.168.2.115", "port": 139 }

« ‹ 1 2 3 4 5 › » 10

mbo digitaal

Wat onderzoekt eduC2 nu?

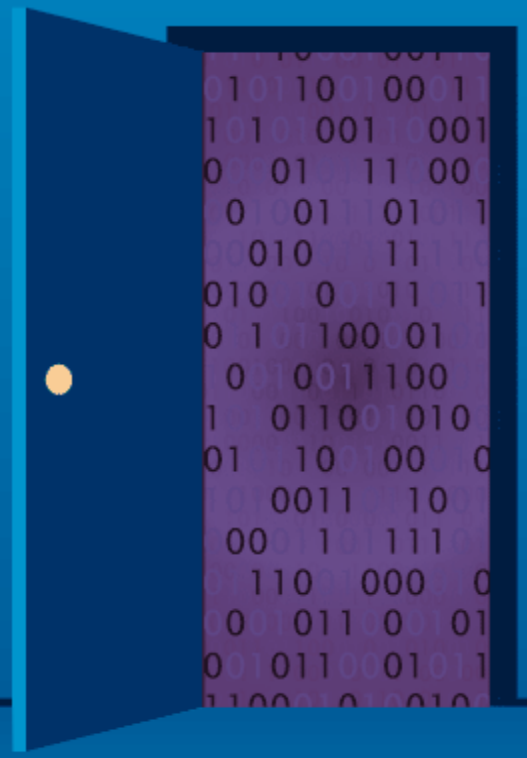
- Detectie van open of onveilige netwerkservices en bestandsdeling
  - Relay aanvallen via Server Message Block (SMB)
- Signalering van verouderde of misbruikbare netwerk- en naamresolutieprotocollen
  - Poisoning via LLMNR, NTB-NS, MDNS
- Lichte kwetsbaarhedenscan op basis van bekende versies van netwerkservices
  - Kwetsbaarheden identificeren via Network Mapper (Nmap):
    - banner grabbing
    - OS detection
    - portscan
    - vulnerability scan (CVSS ≥7.0)
    - SSH fingerprint
- Controle op netwerksegmentatie tussen apparaten en subnetten
- Test op uitgaand verkeer richting verdachte of ongewenste internetbestemmingen
  - bijvoorbeeld The Onion Routing (TOR)



mbo digitaal

Testen EduC2

- Soma College
- Zadkine
- Zone College



Poll (2x)

ahaslides.com/AZ3N8

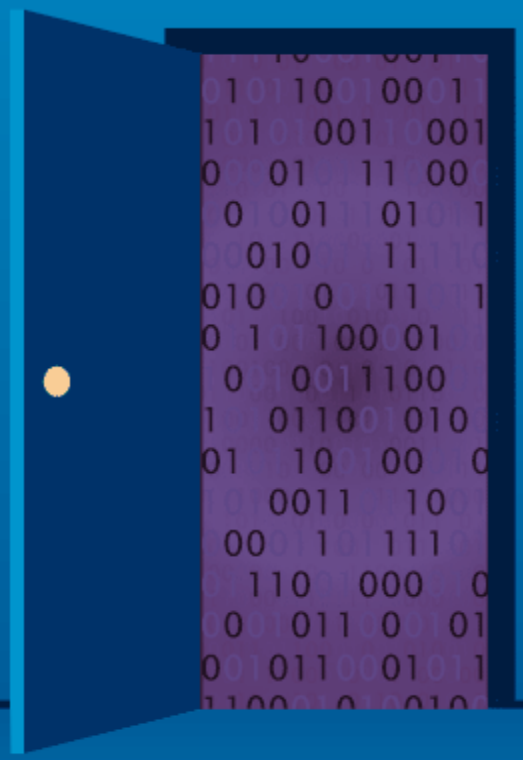
Suggesties voor testmogelijkheden

Welk voorstel is het waardevolst

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.

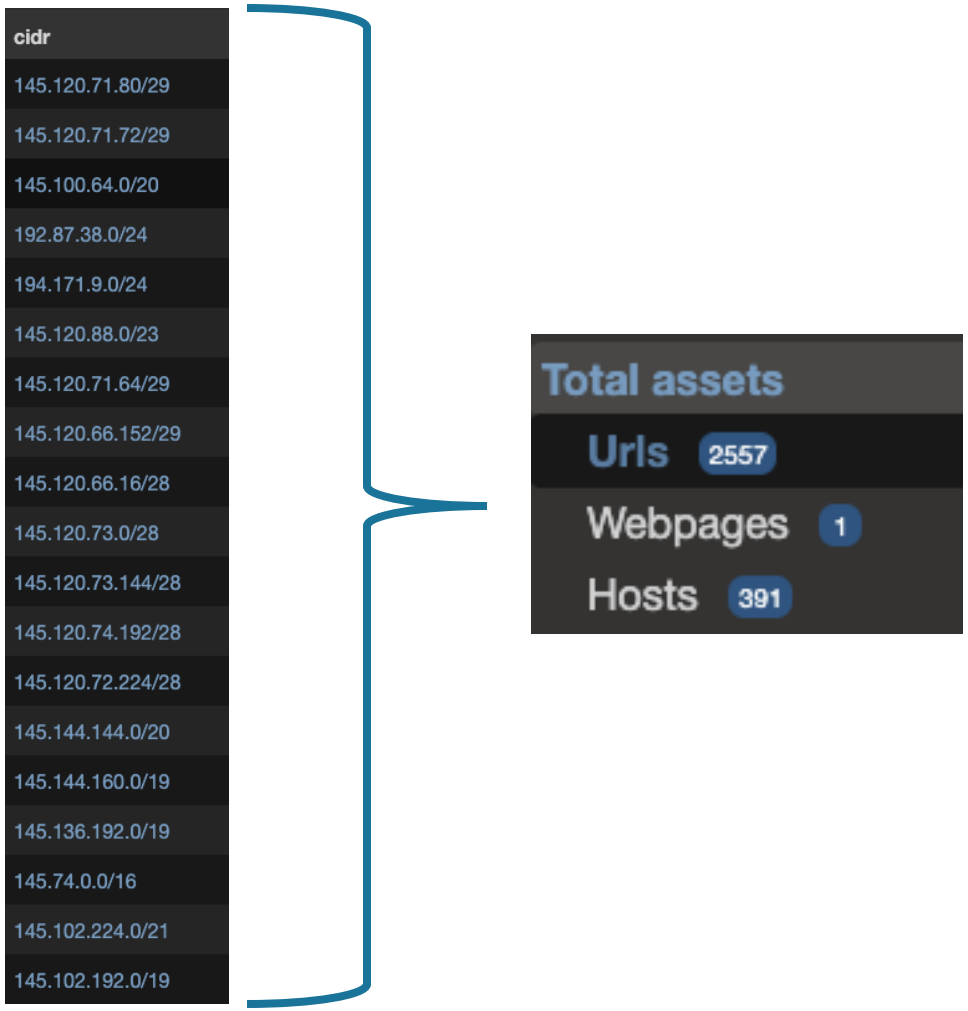
mbo digitaal

Attack Surface Management

cidr	asn	asn_name	tags	first_seen	last_seen
145.120.71.80/29	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 15:24:06 UTC
145.120.71.72/29	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 15:24:06 UTC
145.100.64.0/20	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 15:24:06 UTC
192.87.38.0/24	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-11-11 11:33:49 UTC	2025-12-08 12:23:05 UTC
194.171.9.0/24	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-11-11 11:36:15 UTC	2025-12-08 12:23:05 UTC
145.120.88.0/23	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 10:51:28 UTC
145.120.71.64/29	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 10:51:28 UTC
145.120.66.152/29	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 10:12:12 UTC
145.120.66.16/28	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 10:12:12 UTC
145.120.73.0/28	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 10:12:12 UTC
145.120.73.144/28	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 09:50:13 UTC
145.120.74.192/28	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 09:50:13 UTC
145.120.72.224/28	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-10-24 09:19:16 UTC	2025-12-08 09:50:13 UTC
145.144.144.0/20	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-11-11 11:36:15 UTC	2025-12-07 09:16:55 UTC
145.144.160.0/19	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-11-11 11:36:15 UTC	2025-12-07 09:16:55 UTC
145.136.192.0/19	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-11-11 11:36:15 UTC	2025-12-07 09:16:55 UTC
145.74.0.0/16	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-11-11 10:54:14 UTC	2025-12-06 12:33:55 UTC
145.102.224.0/21	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-11-11 10:54:14 UTC	2025-12-06 12:33:55 UTC
145.102.192.0/19	1103	SURFNET-NL SURFnet, The Netherlands, NL		2025-11-11 10:54:14 UTC	2025-12-06 12:33:55 UTC

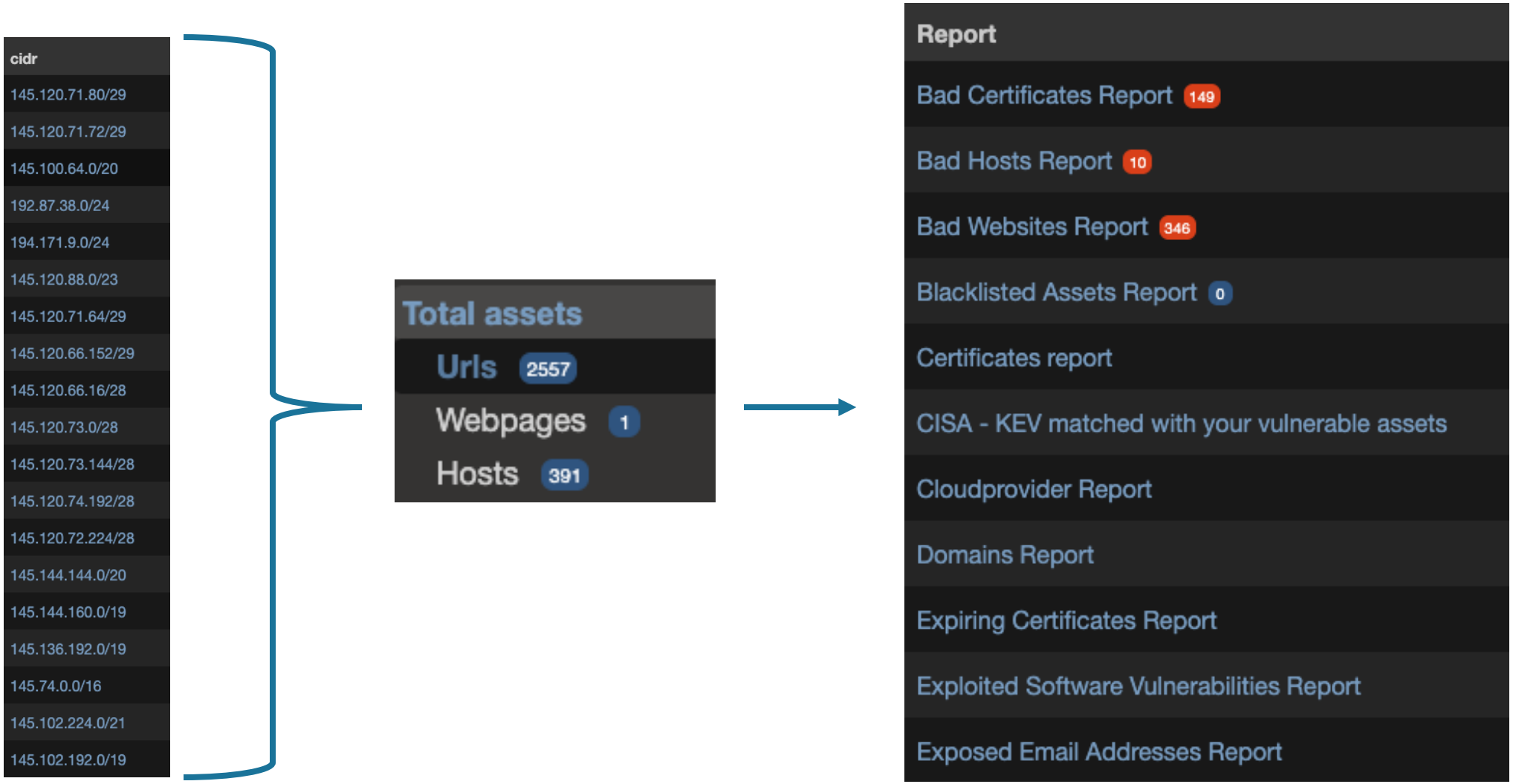
mbo digitaal

Attack Surface Management



mbo digitaal

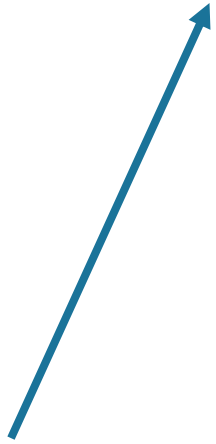
Attack Surface Management



mbo digitaal

Attack Surface Management

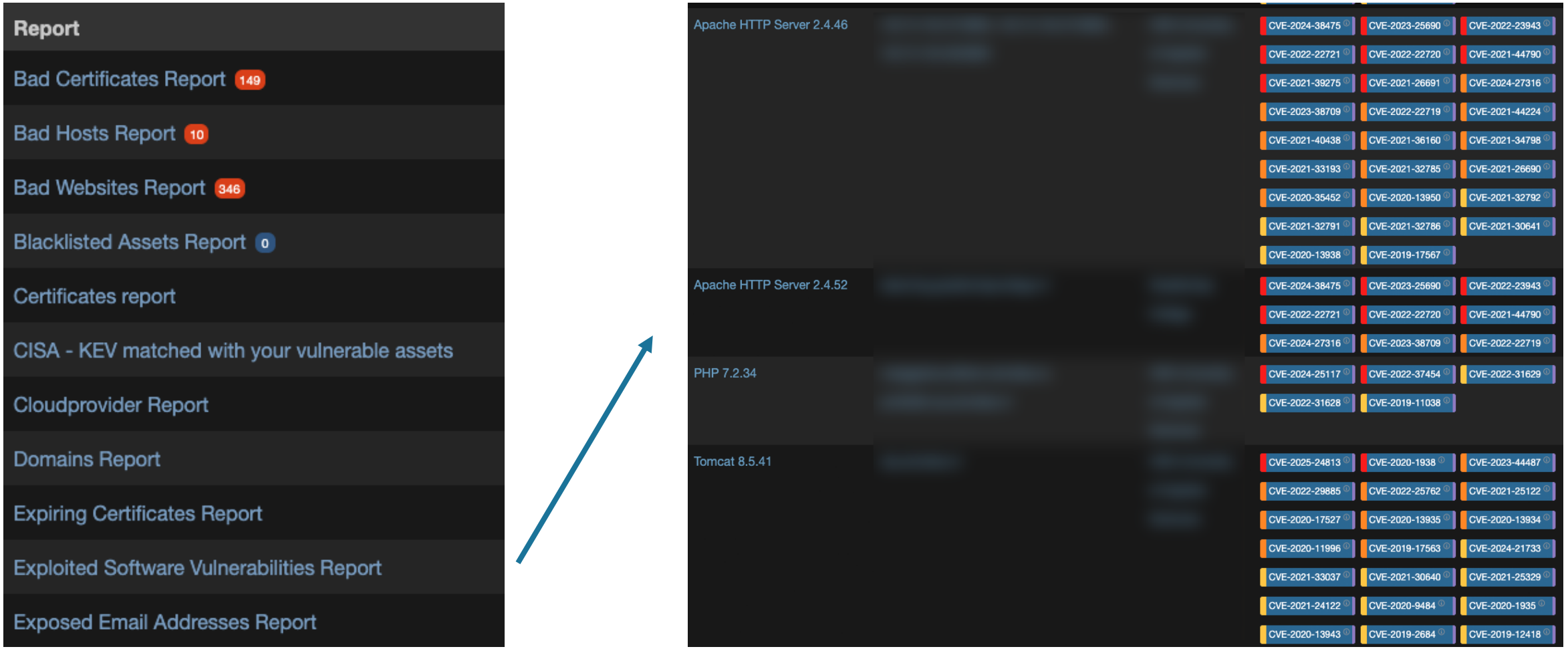
Report
Bad Certificates Report 149
Bad Hosts Report 10
Bad Websites Report 346
Blacklisted Assets Report 0
Certificates report
CISA - KEV matched with your vulnerable assets
Cloudprovider Report
Domains Report
Expiring Certificates Report
Exploited Software Vulnerabilities Report
Exposed Email Addresses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

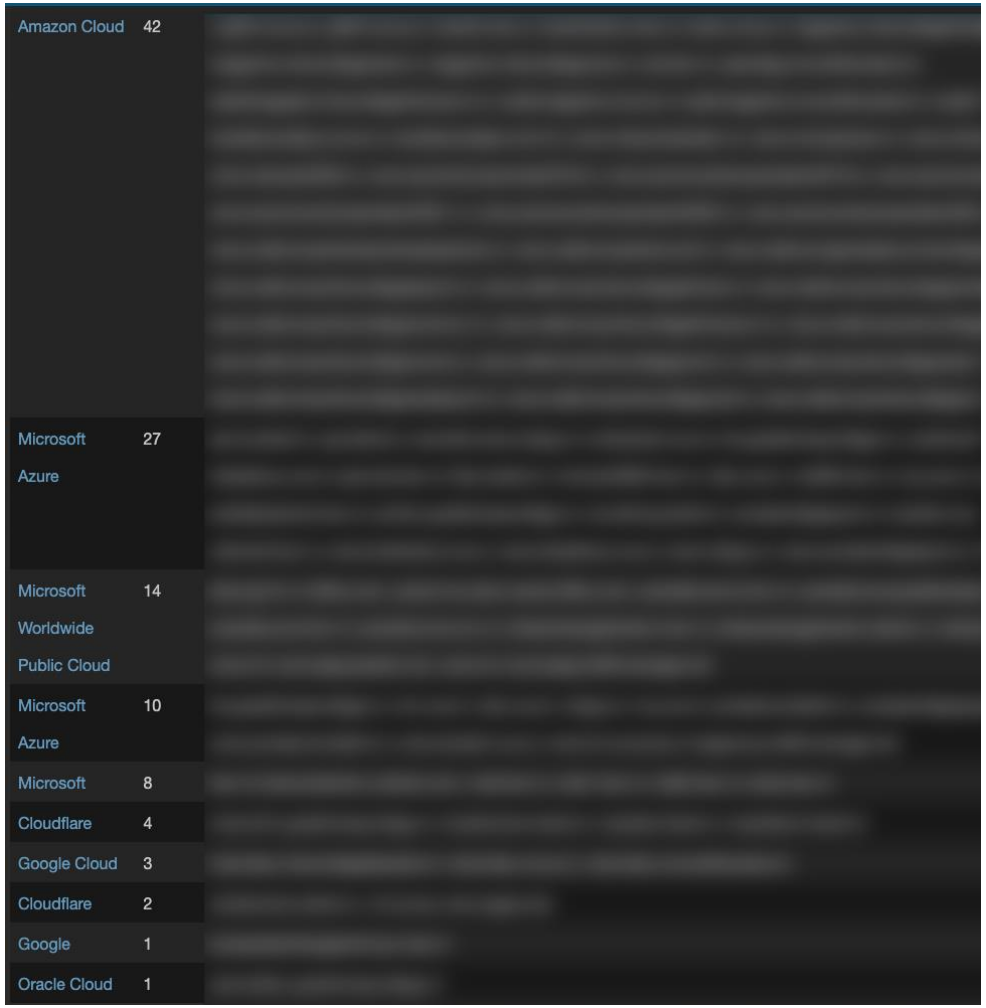
Attack Surface Management



mbo digitaal

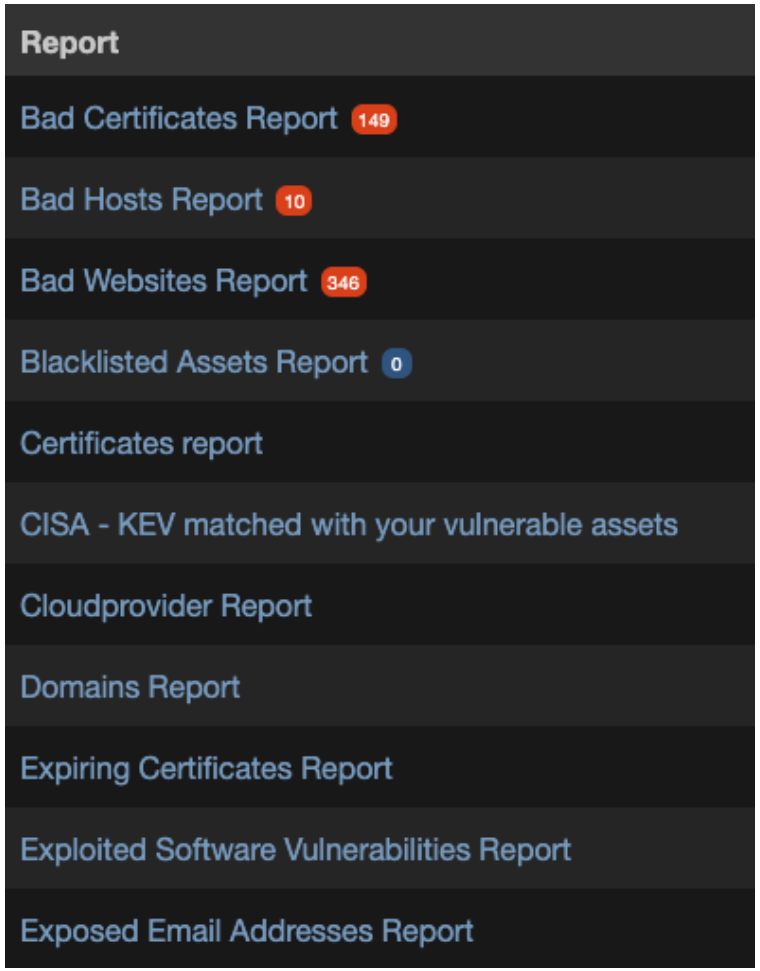
Attack Surface Management

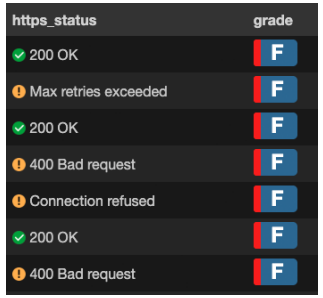
Report
Bad Certificates Report 149
Bad Hosts Report 10
Bad Websites Report 346
Blacklisted Assets Report 0
Certificates report
CISA - KEV matched with your vulnerable assets
Cloudprovider Report
Domains Report
Expiring Certificates Report
Exploited Software Vulnerabilities Report
Exposed Email Addresses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

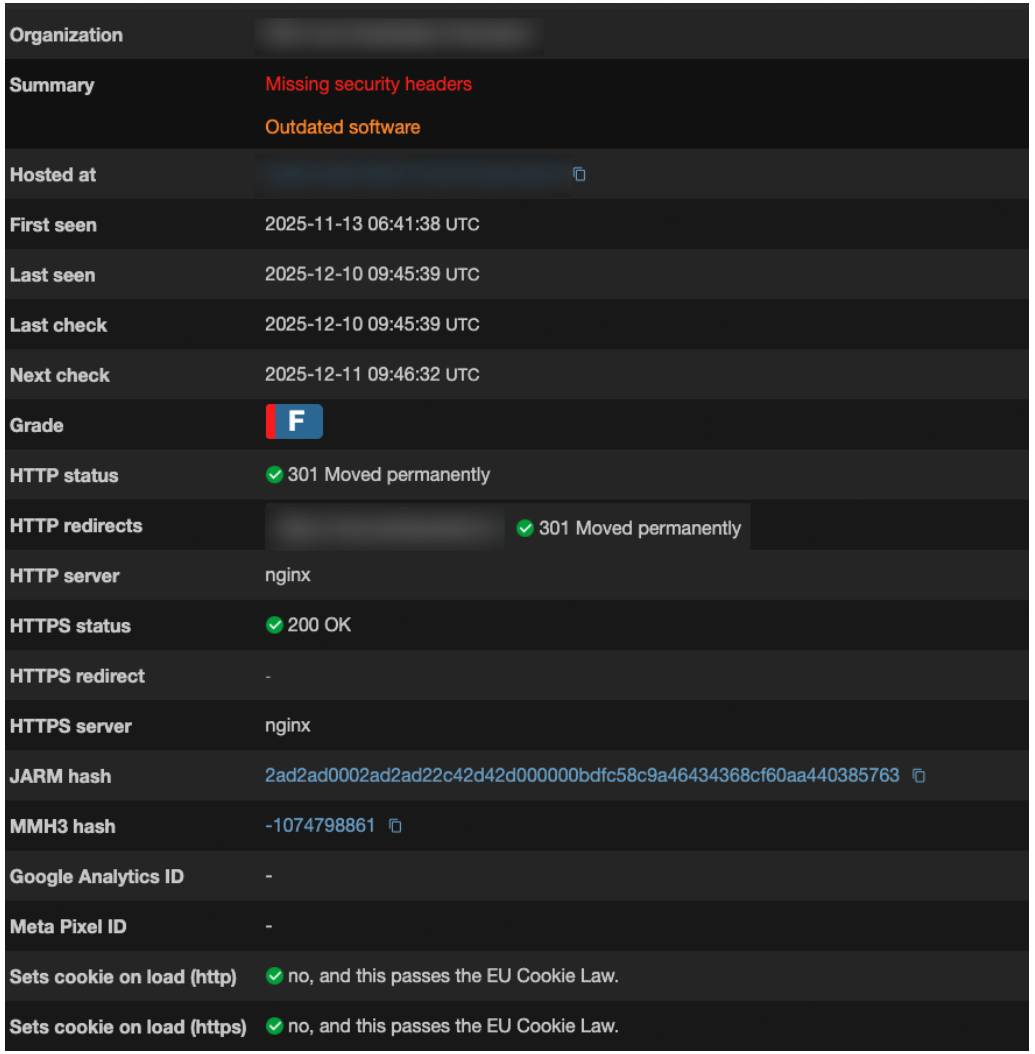


mbo digitaal

Attack Surface Management







Poll (2x)

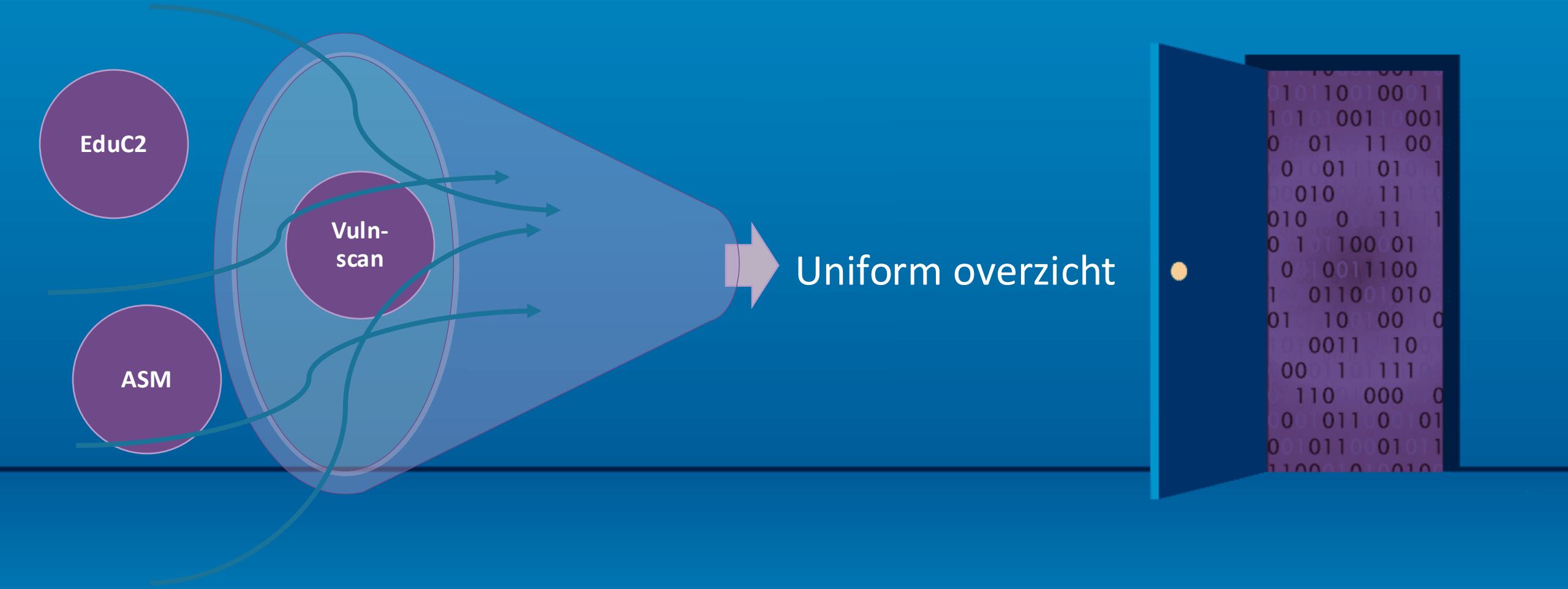
ahaslides.com/AZ3N8

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

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

mbo digitaal

Meerdere diensten

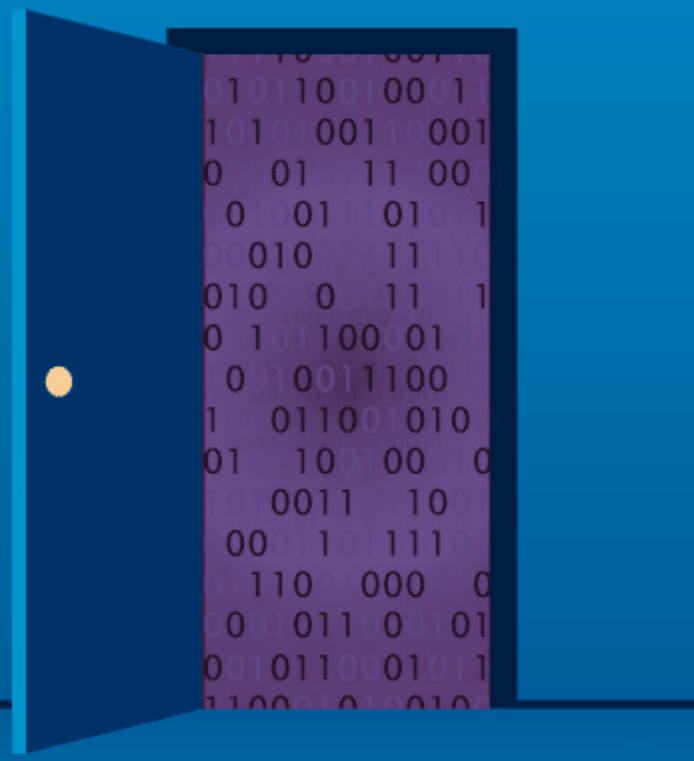


mbo digitaal

Initiatief weerbaarheidstesten – ‘projectmanagement’

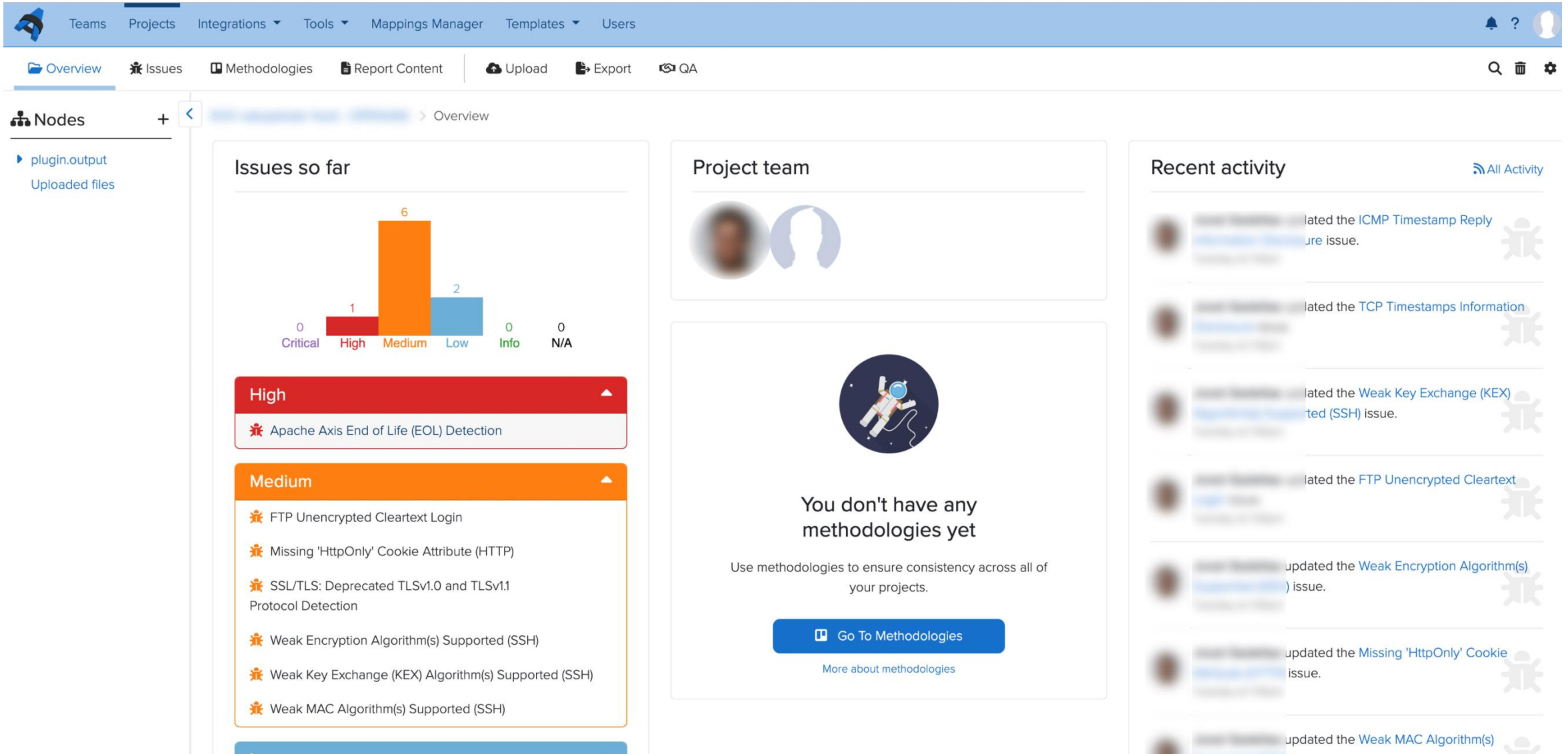
Geleerd bij het ‘van check tot hack’ traject.

10 instellingen x 5/6 checks = 🤯



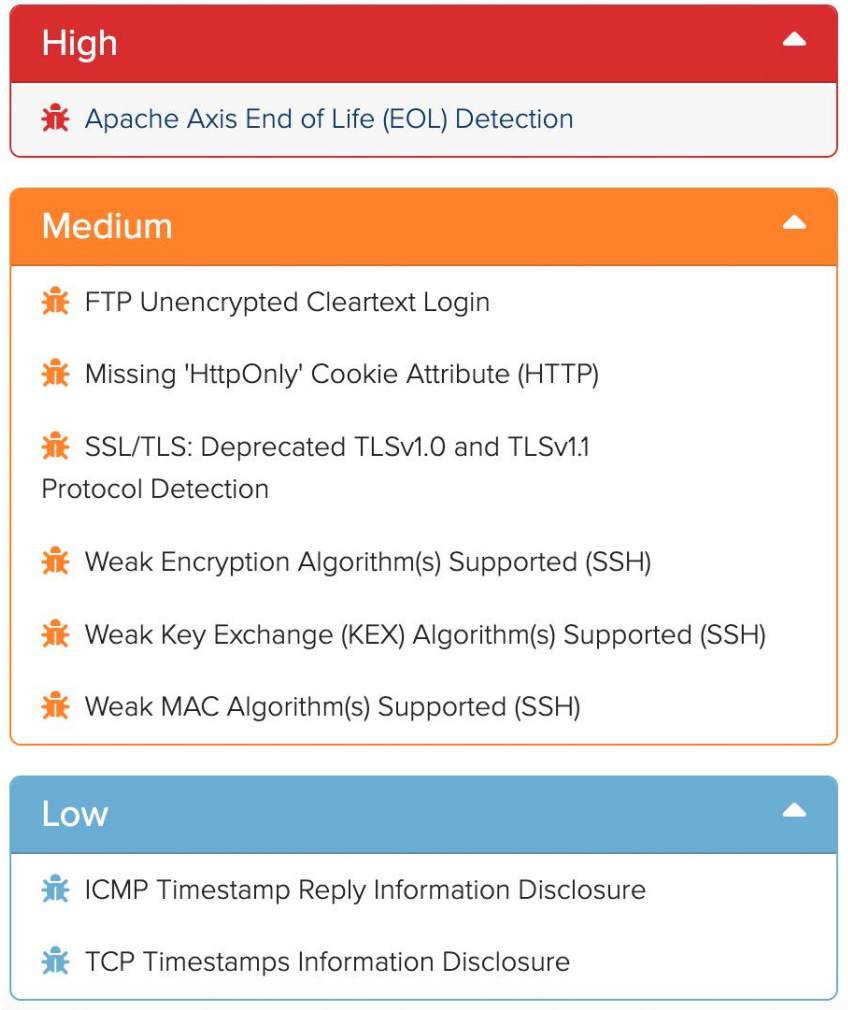
mbo digitaal

Bevindingen



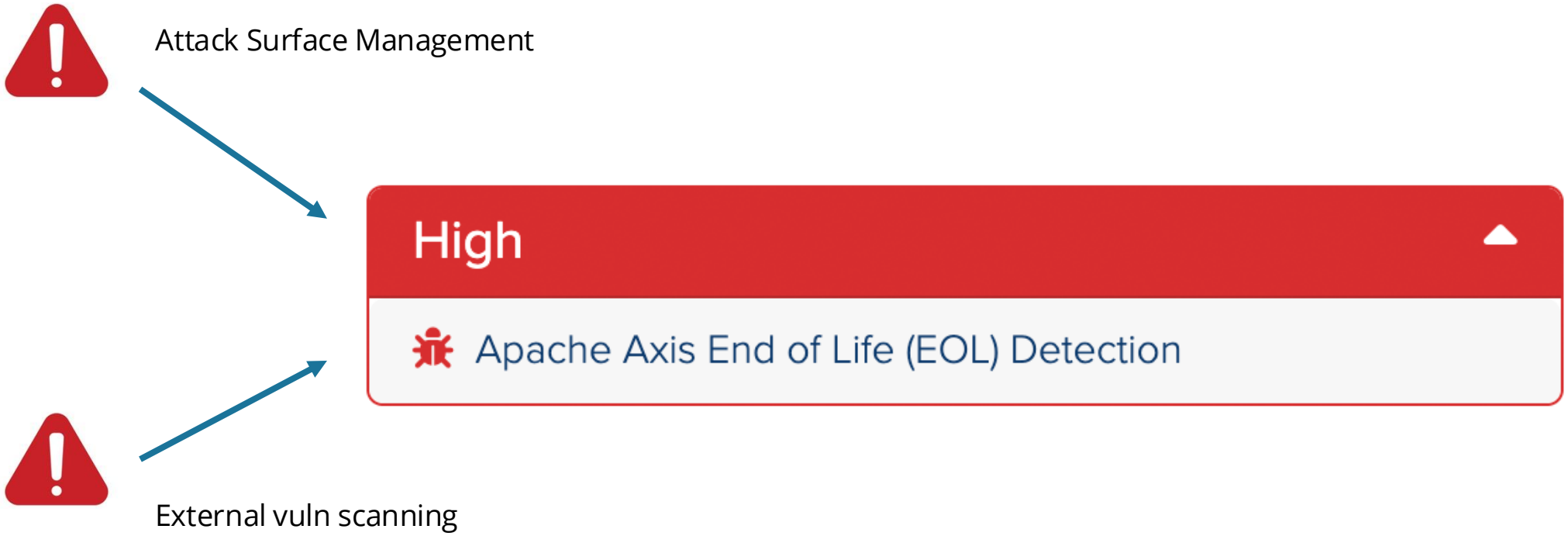
mbo digitaal

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.

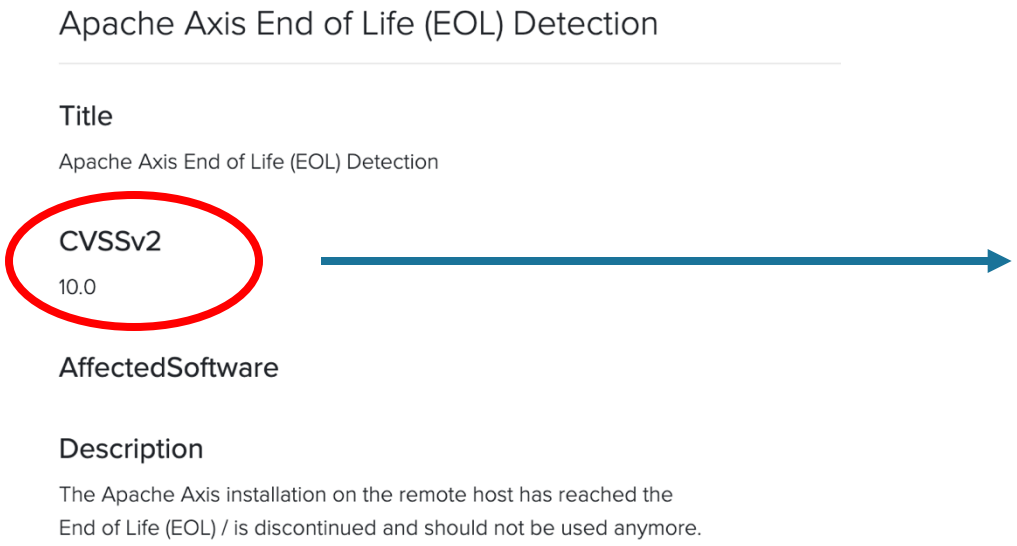
Recommendation

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.

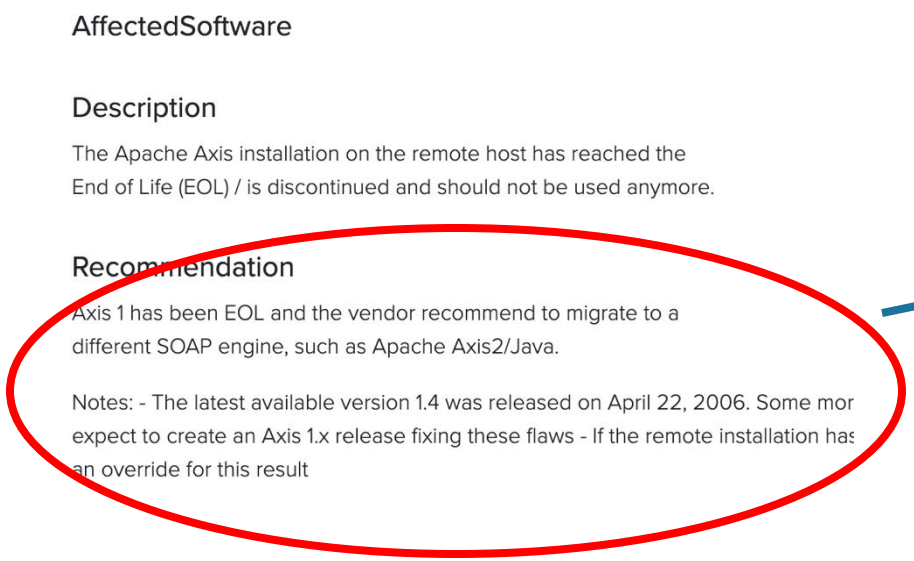
Er zijn ook kwetsbaarheden waar geen CVSS-score voor bestaat. Dit komt vooral voor bij **misconfiguraties** en ontbrekende (of niet nageleefde) **policies**. In dergelijke gevallen passen we een prioriteringsmodel toe, hierbij hanteren we de volgende categorieën:

- 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.

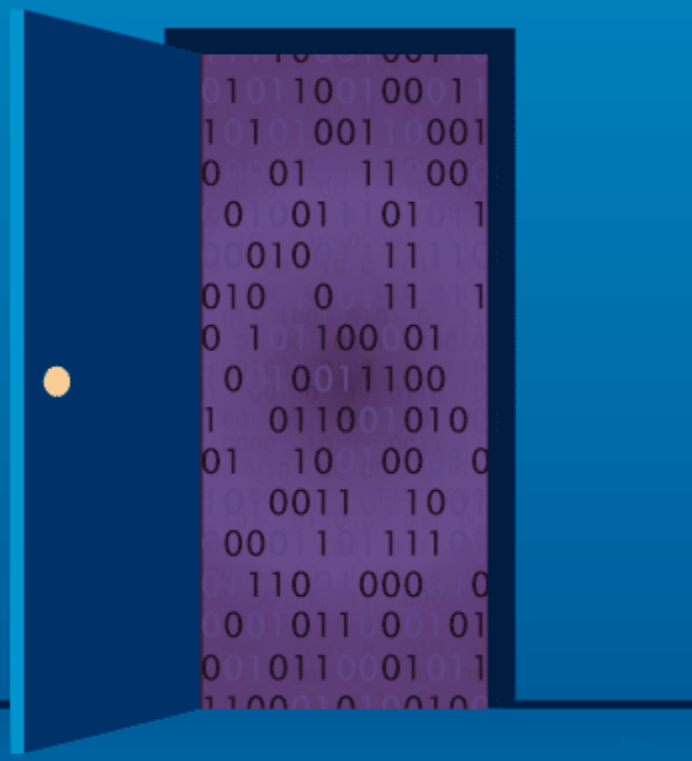
- Richtlijnen per type misconfiguratie (bijv. policies, cloud resources).
- Best practices gebaseerd op CIS-benchmarks of interne baseline-standaarden.
- Heldere instructies voor beheerteams over hoe het probleem te verhelpen is.
- Eventuele workarounds of tijdelijke mitigerende maatregelen wanneer patches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

mbo digitaal

Toekomst

Ontwikkelen detecties EduC2.
Ontwikkelen normalisatie.
Ontwikkelen handelingsperspectief.

En het inrichten van alle bijbehorende processen.



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.