ACCESS42

Cybersecurity

Think BIG. Secure the World!

ACCESS42
Cybersecurity

VULNERABILITY MANAGEMENT

In de praktijk

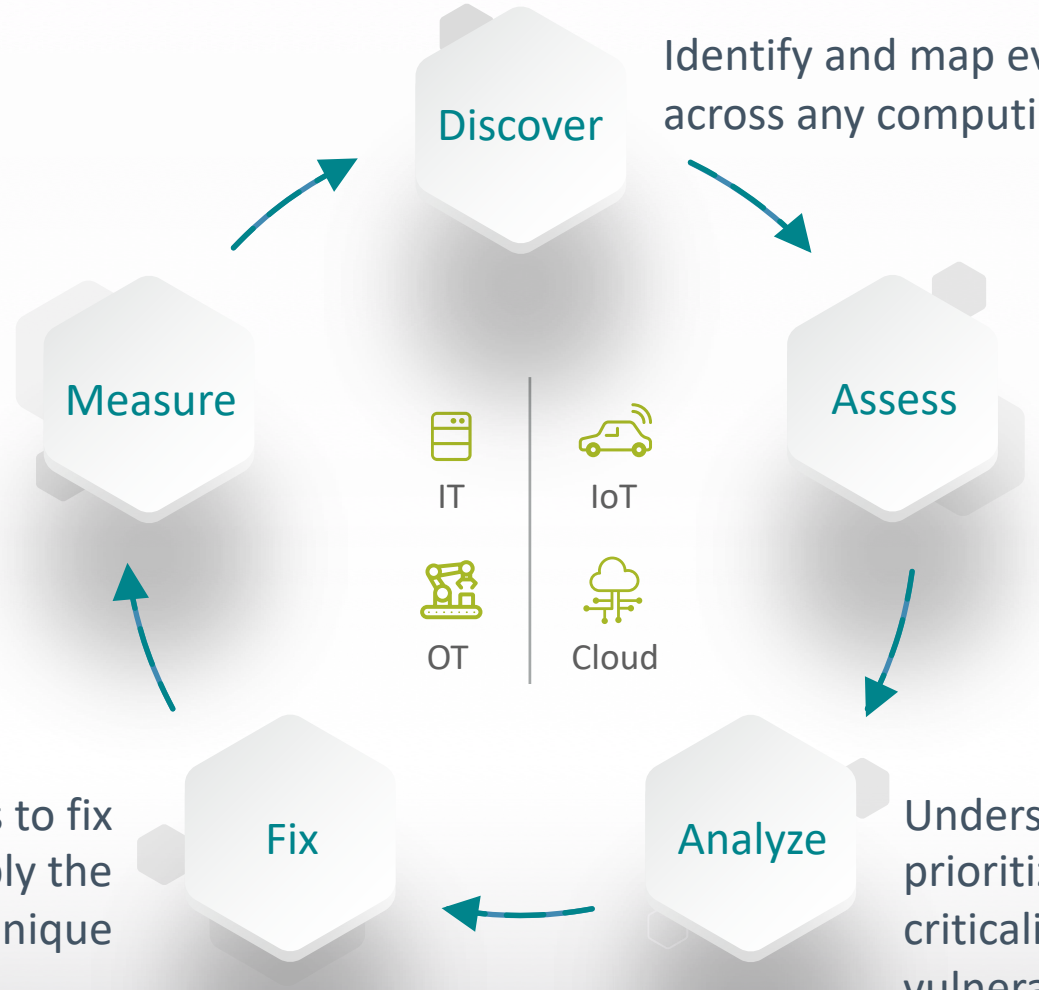
Ronald Kingma, CISSP

Wie ben ik?

- Ronald Kingma, CISSP
  - *Security Specialist*
  - *Access42*
  - *@ronaldkingma*

ACCESS42 Cybersecurity

Vulnerability Management



Identify and map every asset across any computing environment

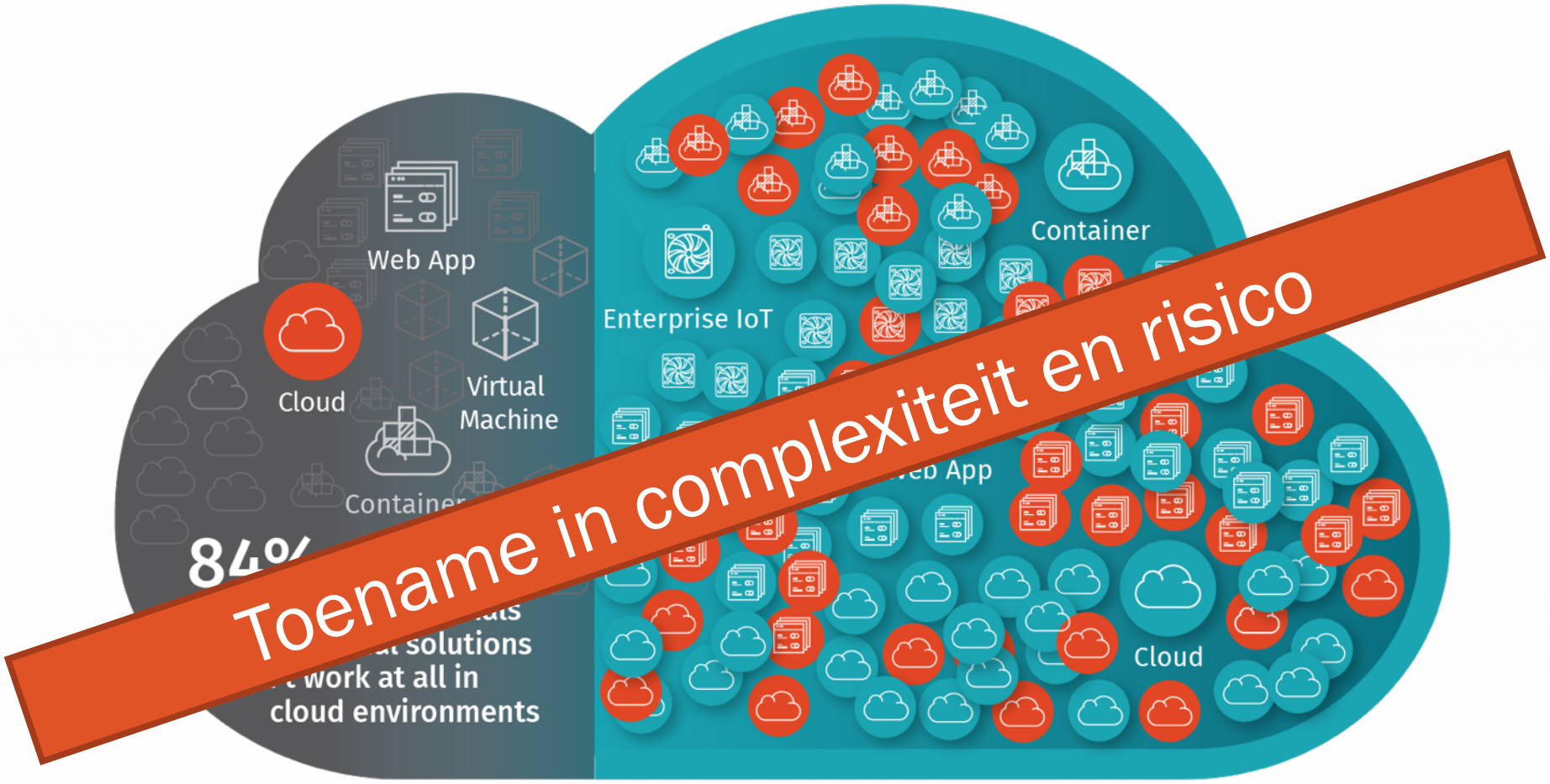
Understand the state of all assets, including vulnerabilities, misconfigurations and other health indicators

Understand exposures in context, to prioritize remediation based on asset criticality, threat context and vulnerability severity

Prioritize which exposures to fix first, if at all, and apply the appropriate remediation technique

Model and analyze cyber exposure to make better business and technology decisions

ACCESS42 Cybersecurity



TRADITIONAL VM

Lack of visibility into infrastructure security

CYBER EXPOSURE

Achieve accurate visibility and insight into dynamic cloud infrastructure

ACCESS42 Cybersecurity

Network Scan

‹ Back to My Scans

Configure | Audit Trail | Launch | Export

Dashboard | Hosts 54 | Vulnerabilities 1564 | Remediations 391 | History 160

TRENDING: Previous Scan

CURRENT VULNERABILITIES

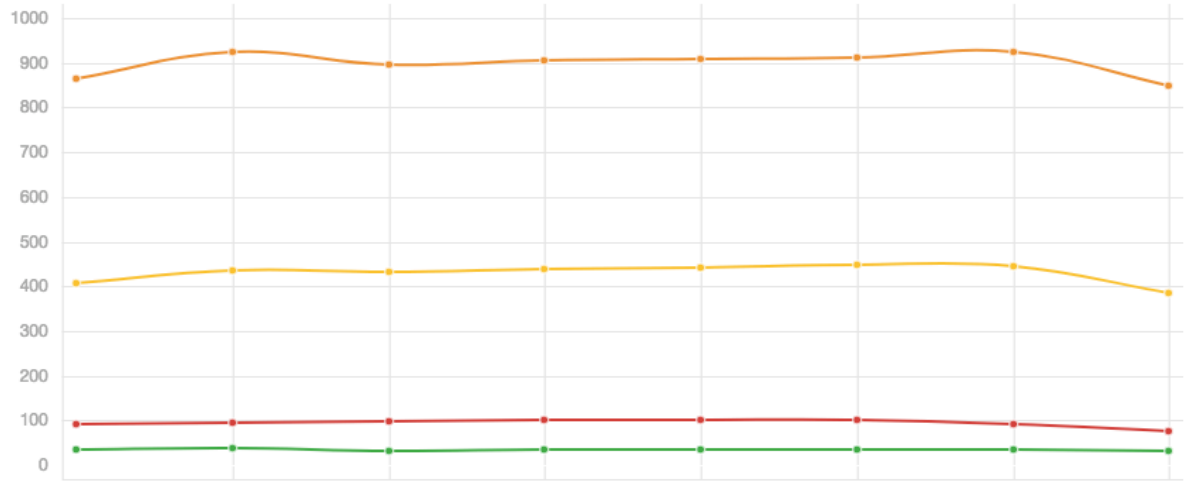
CRITICAL	HIGH	MEDIUM	LOW	INFO
75 (-18)	849 (-74)	384 (-60)	31 (-3)	225 (-26)

OPERATING SYSTEMS

VULNERABILITIES

AUTHENTICATION

VULNERABILITIES OVER TIME



TOP VULNERABILITIES

CRITICAL	MS17-010: Security Update for Microsoft Window...	6
CRITICAL	MS17-012: Security Update for Microsoft Window...	6
CRITICAL	KB4343899: Windows 7 and Windows Server 200...	5
CRITICAL	MS15-034: Vulnerability in HTTP.sys Could Allow R...	5
CRITICAL	MS16-077: Security Update for WPAD (3165191)	5
CRITICAL	MS17-010: Security Update for Microsoft Window...	5
CRITICAL	Microsoft Malware Protection Engine < 1.1.14405....	4
CRITICAL	MS Security Advisory 4022344: Security Update fo...	4

Probleem

- Er zijn verschillende ideeën over kwetsbaarheden en het risico

Vulnerability Researcher

Vendor/Developer

Organisatie

Gebruikers

Overheid/Compliance/Regulering

Risk based security

- Alles is belangrijk, waar moet ik beginnen?
- CVE en CVSS
- Risico's worden geclassifceerd op basis van CVSS (v2 of v3)

CVSS v2.0 Ratings

SEVERITY	BASE SCORE RANGE
LOW	0.0 - 3.9
MEDIUM	4.0 - 6.9
HIGH	7.0 - 10.0

CVSS v3.0 Ratings

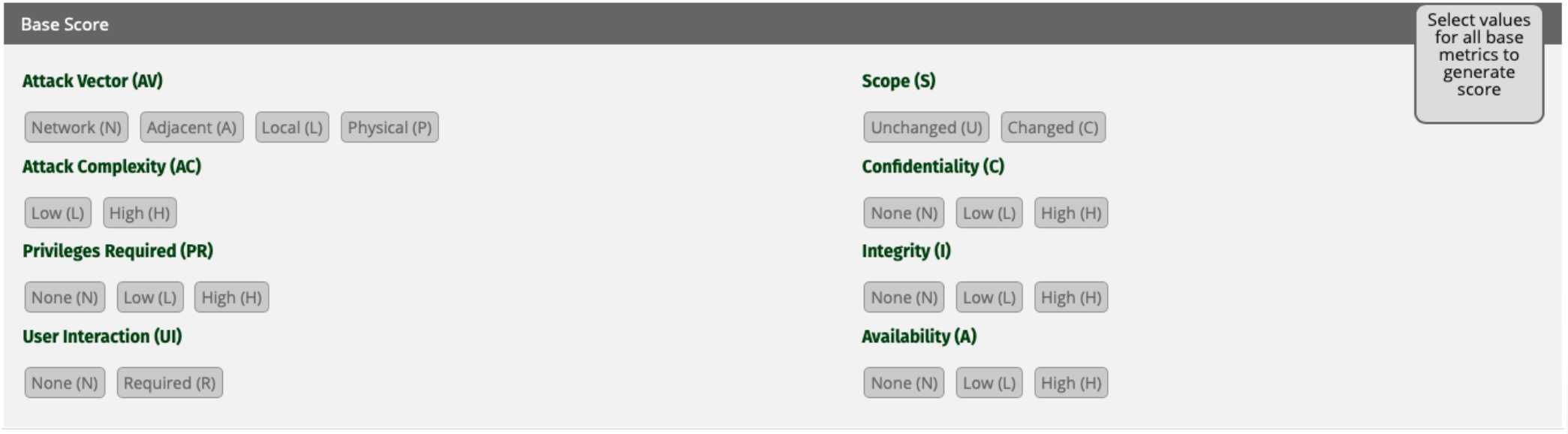
SEVERITY	BASE SCORE RANGE
NONE	0.0
LOW	0.1 - 3.9
MEDIUM	4.0 - 6.9
HIGH	7.0 - 8.9
CRITICAL	9.0 - 10.0

ACCESS42 Cybersecurity

Vuln ID	Summary	CVSS Severity
CVE-2019-11678	The "default reports" feature in Zoho ManageEngine Firewall Analyzer before 12.3 Build 123218 is vulnerable to SQL Injection. **Published:** May 02, 2019; 10:29:00 AM -04:00	*V3:* 9.8 CRITICAL *V2:* 7.5 HIGH
CVE-2019-11625	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/emailingRequest.php. A remote background administrator privilege user (or a user with permission to manage emailing) could exploit the vulnerability to obtain database sensitive information. **Published:** April 30, 2019; 04:29:02 PM -04:00	*V3:* 4.9 MEDIUM *V2:* 4.0 MEDIUM
CVE-2019-11623	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/configurationRequest.php when action=siteweb. A remote background administrator privilege user (or a user with permission to manage configuration siteweb) could exploit the vulnerability to obtain database sensitive information. **Published:** April 30, 2019; 04:29:02 PM -04:00	*V3:* 4.9 MEDIUM *V2:* 4.0 MEDIUM
CVE-2019-11622	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/modulecategoryRequest.php. A remote background administrator privilege user (or a user with permission to manage modulecategory) could exploit the vulnerability to obtain database sensitive information via modulecategory_edit_titre. **Published:** April 30, 2019; 04:29:02 PM -04:00	*V3:* 4.9 MEDIUM *V2:* 4.0 MEDIUM
CVE-2019-11621	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/configurationRequest.php when action=network. A remote background administrator privilege user (or a user with permission to manage network configuration) could exploit the vulnerability to obtain database sensitive information. **Published:** April 30, 2019; 04:29:02 PM -04:00	*V3:* 4.9 MEDIUM *V2:* 4.0 MEDIUM
CVE-2019-11620	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/modulecategoryRequest.php. A remote background administrator privilege user (or a user with permission to manage modulecategory) could exploit the vulnerability to obtain database sensitive information via	*V3:* 4.9 MEDIUM *V2:* 4.0 MEDIUM

Classificatie

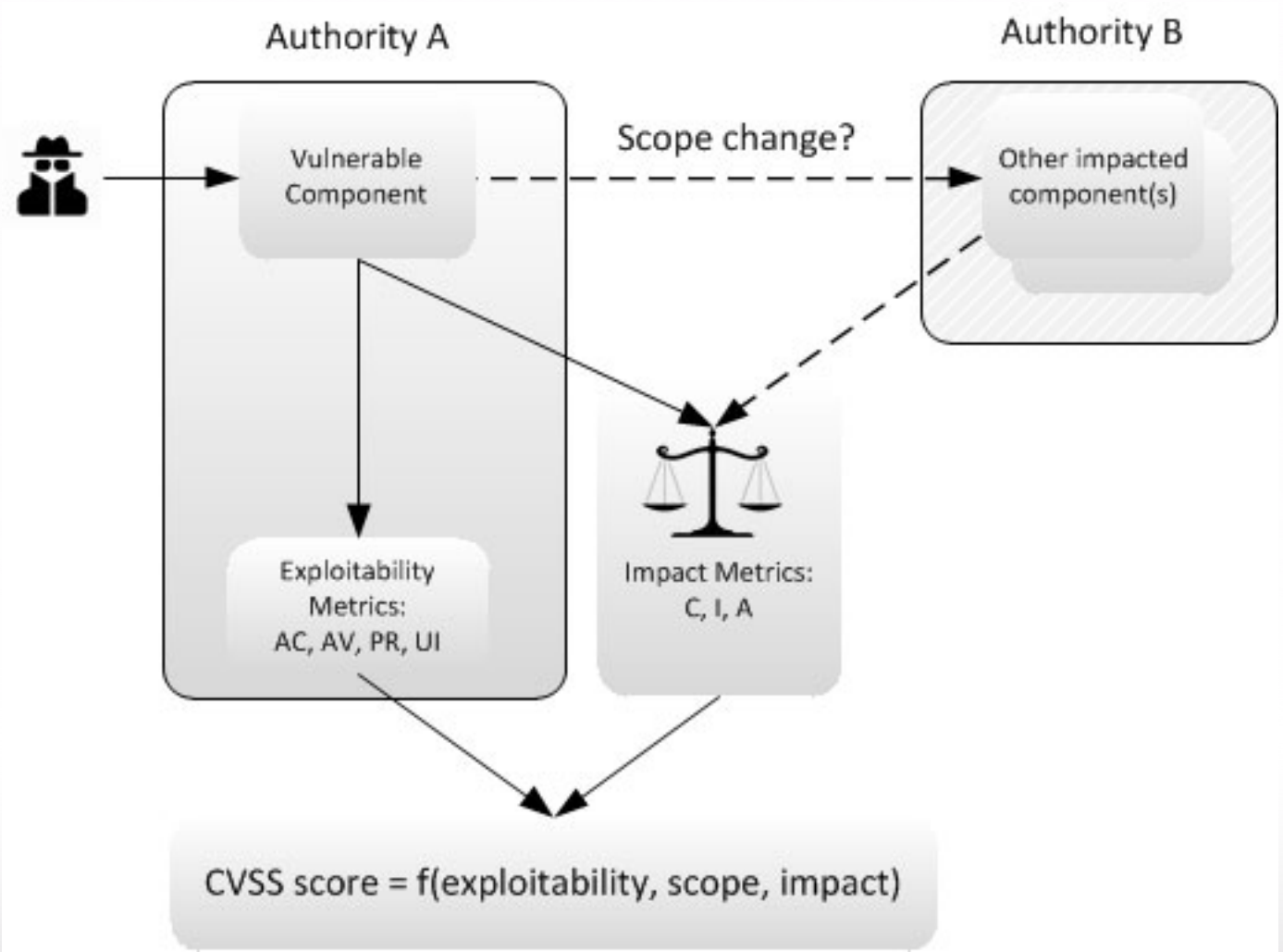
- Standaard worden kwetsbaarheden geclassificeerd met de Base Score



Geen kennis van de omgeving

- Waar staat het device?
- Zijn er andere maatregelen?
- CIA (BIV) classificatie van het device (en de data)?
- Onderdeel van een keten?
- Keten van kwetsbaarheden?
- Etc. etc.

Scope


Authority A
Authority B
Vulnerable Component
Scope change?
Other impacted component(s)
Exploitability Metrics: AC, AV, PR, UI
Impact Metrics: C, I, A
CVSS score = f(exploitability, scope, impact)

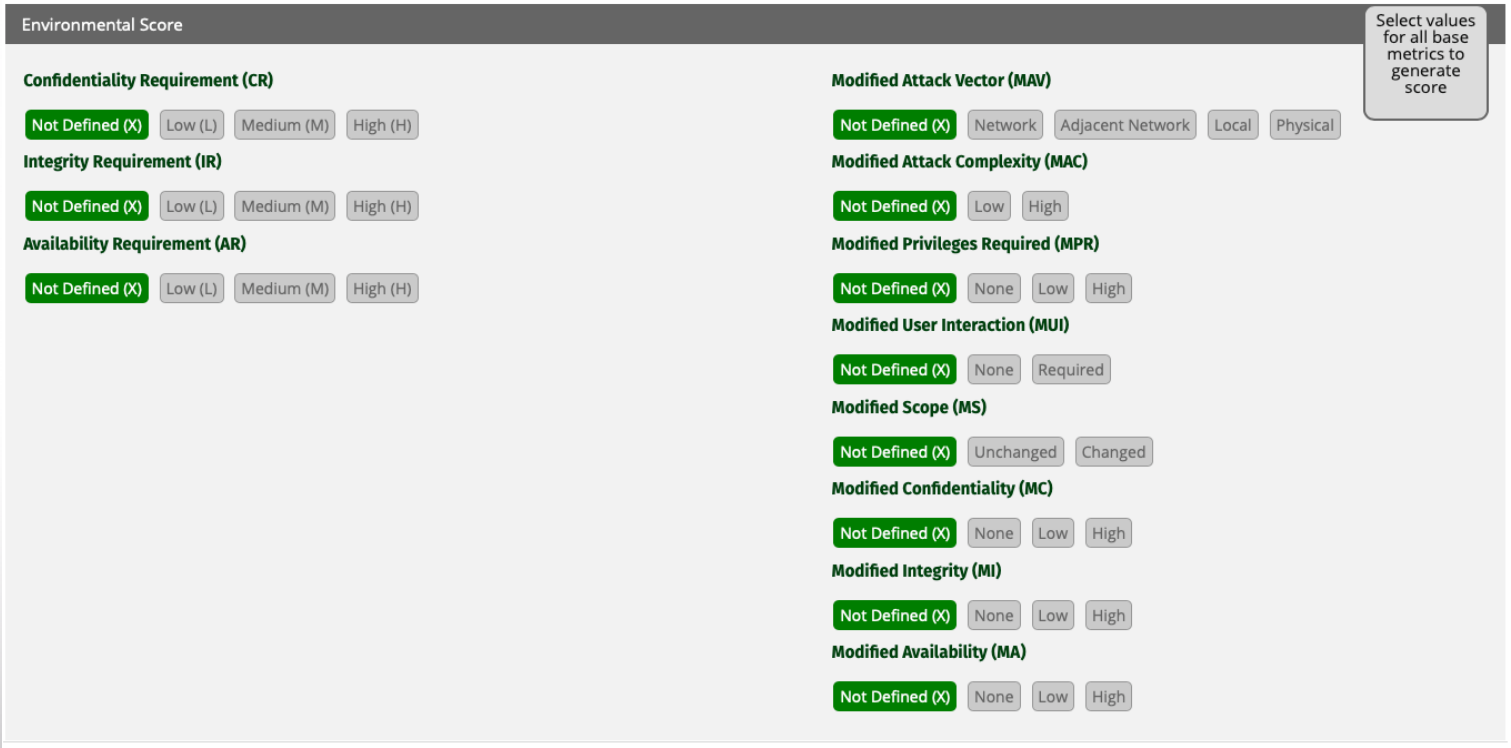
Temporal Score

- Huidige status (eventuele) exploits
- Patches/Workarounds
- Vertrouwen in de omschrijving van een kwetsbaarheid

ACCESS42 Cybersecurity

Environmental Score

- Aanpassing van de CVSS score op basis van de asset classificatie
- Additionele maatregelen



ACCESS42 Cybersecurity

Voorbeeld: Hyper-V vSMB Remote Code Execution Vulnerability

CVE-2019-0786 Detail

Current Description

An elevation of privilege vulnerability exists in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to open a specially crafted file over the SMB protocol on the same machine, aka 'SMB Server Elevation of Privilege Vulnerability'.

Source: MITRE
Description Last Modified: 04/09/2019
+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS v2.0 Severity and Metrics:
Base Score: 7.5 HIGH
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

ACCESS42 Cybersecurity

Base Score

9.8
(Critical)

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Environmental Score

7.4 (High)

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

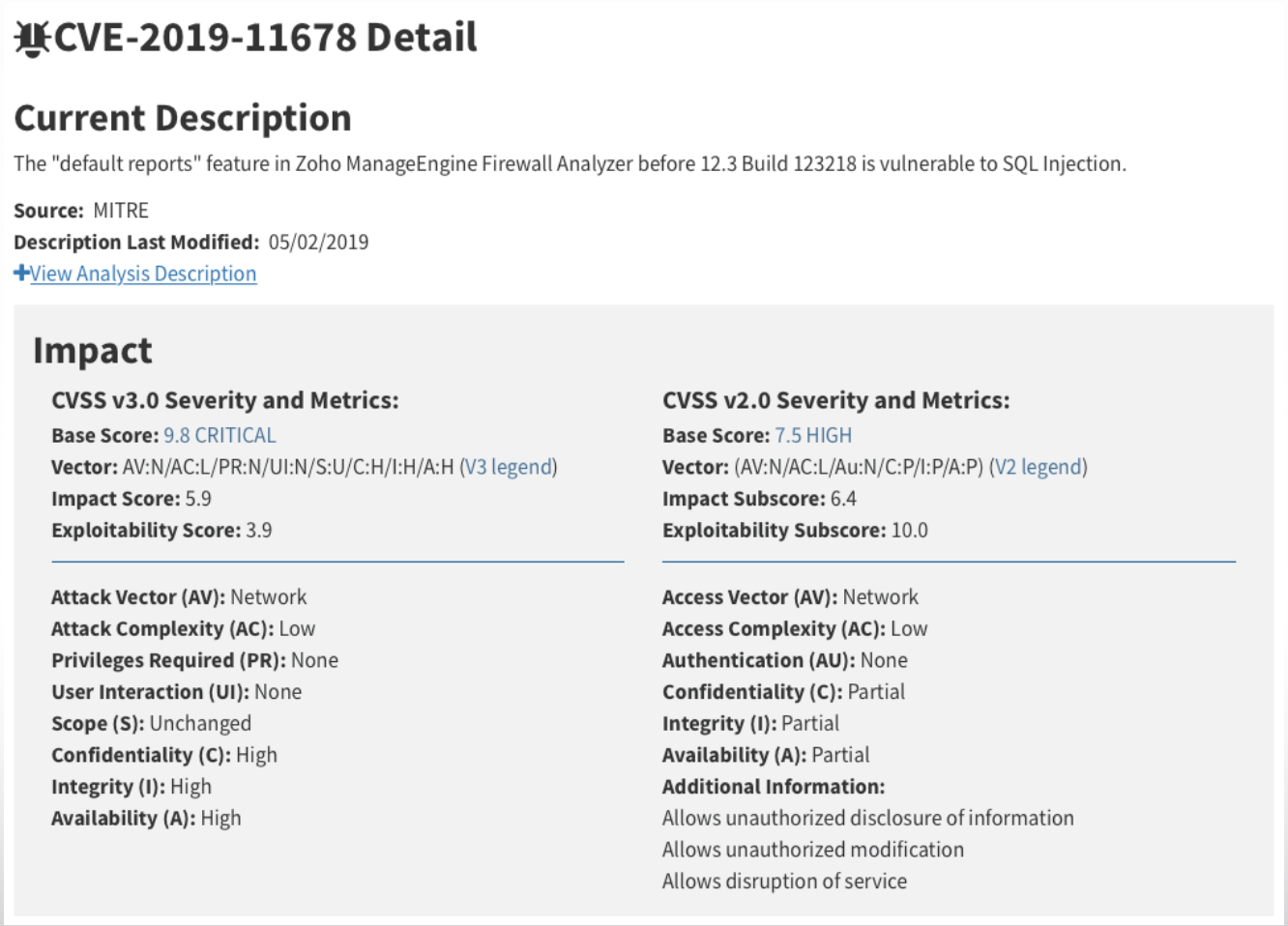
Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

Voorbeeld: The "default reports" feature in Zoho ManageEngine Firewall Analyzer



CVE-2019-11678 Detail

Current Description

The "default reports" feature in Zoho ManageEngine Firewall Analyzer before 12.3 Build 123218 is vulnerable to SQL Injection.

Source: MITRE
Description Last Modified: 05/02/2019
View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS v2.0 Severity and Metrics:
Base Score: 7.5 HIGH
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

ACCESS42 Cybersecurity

Base Score	9.8 (Critical)

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

None (N) | Low (L) | High (H)

Availability (A)

None (N) | Low (L) | High (H)

Temporal Score

9.0 (Critical)

Exploit Code Maturity (E)

Not Defined (X) | **Unproven (U)** | Proof-of-Concept (P) | Functional (F) | High (H)

Remediation Level (RL)

Not Defined (X) | Official Fix (O) | Temporary Fix (T) | Workaround (W) | Unavailable (U)

Report Confidence (RC)

Not Defined (X) | Unknown (U) | Reasonable (R) | Confirmed (C)

Environmental Score

6.9 (Medium)

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | **Adjacent Network** | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | **High**

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

Modified Integrity (MI)

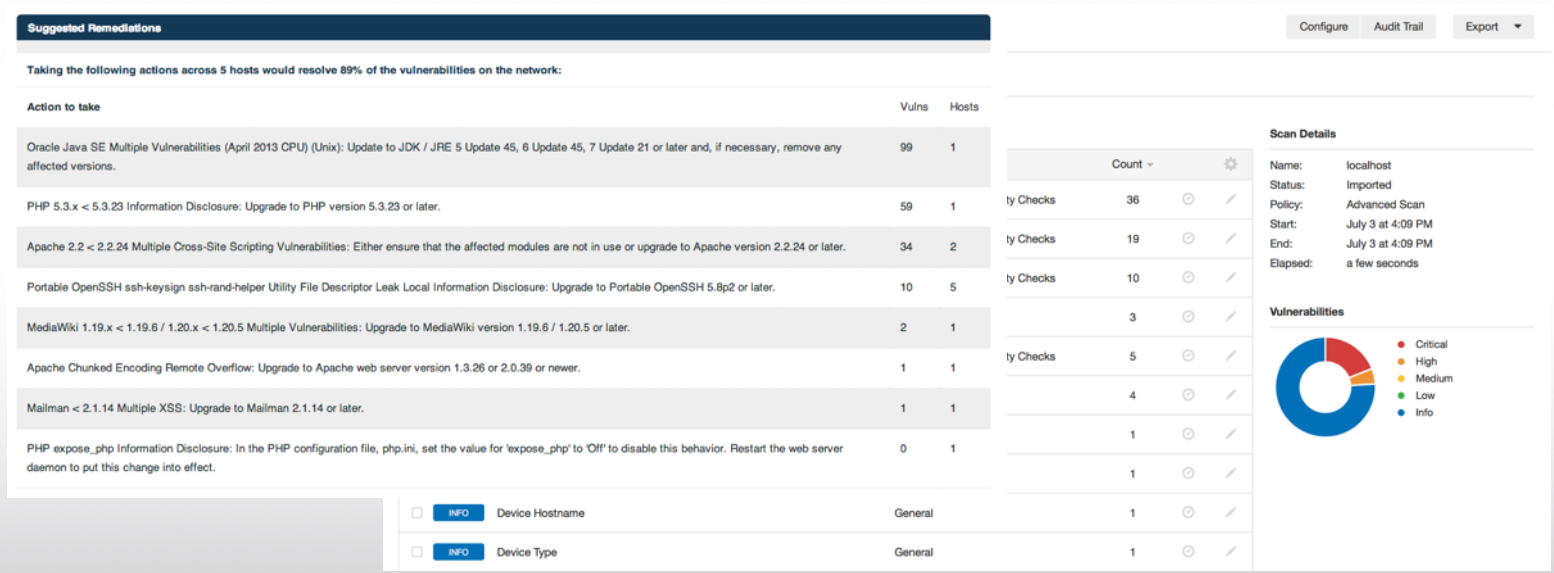
Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

Remediation summary

- Groepeer kwetsbaarheden (en ontdubbel deze)
- Bepaal het risico voor jouw organisatie
- Stel een top X op met hoogste prioriteiten



Suggested Remediations

Taking the following actions across 5 hosts would resolve 89% of the vulnerabilities on the network:

Action to take	Vulns	Hosts
Oracle Java SE Multiple Vulnerabilities (April 2013 CPU) (Unix): Update to JDK / JRE 5 Update 45, 6 Update 45, 7 Update 21 or later and, if necessary, remove any affected versions.	99	1
PHP 5.3.x < 5.3.23 Information Disclosure: Upgrade to PHP version 5.3.23 or later.	59	1
Apache 2.2 < 2.2.24 Multiple Cross-Site Scripting Vulnerabilities: Either ensure that the affected modules are not in use or upgrade to Apache version 2.2.24 or later.	34	2
Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure: Upgrade to Portable OpenSSH 5.8p2 or later.	10	5
MediaWiki 1.19.x < 1.19.6 / 1.20.x < 1.20.5 Multiple Vulnerabilities: Upgrade to MediaWiki version 1.19.6 / 1.20.5 or later.	2	1
Apache Chunked Encoding Remote Overflow: Upgrade to Apache web server version 1.3.26 or 2.0.39 or newer.	1	1
Mailman < 2.1.14 Multiple XSS: Upgrade to Mailman 2.1.14 or later.	1	1
PHP expose_php Information Disclosure: In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.	0	1

Configure | Audit Trail | Export

Count

ty Checks	36	
ty Checks	19	
ty Checks	10	
	3	
ty Checks	5	
	4	
	1	
	1	
INFO Device Hostname	General	1
INFO Device Type	General	1

Scan Details

Name:	localhost
Status:	Imported
Policy:	Advanced Scan
Start:	July 3 at 4:09 PM
End:	July 3 at 4:09 PM
Elapsed:	a few seconds

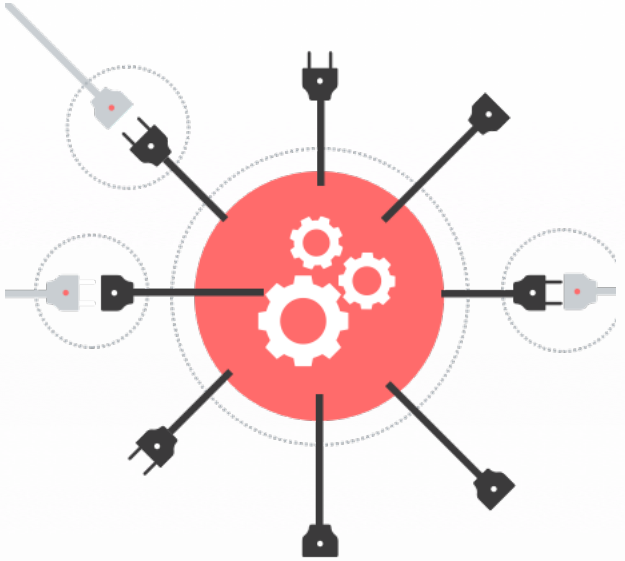
Vulnerabilities

ACCESS42 Cybersecurity

Samenwerken / Requirements (voorbeelden)

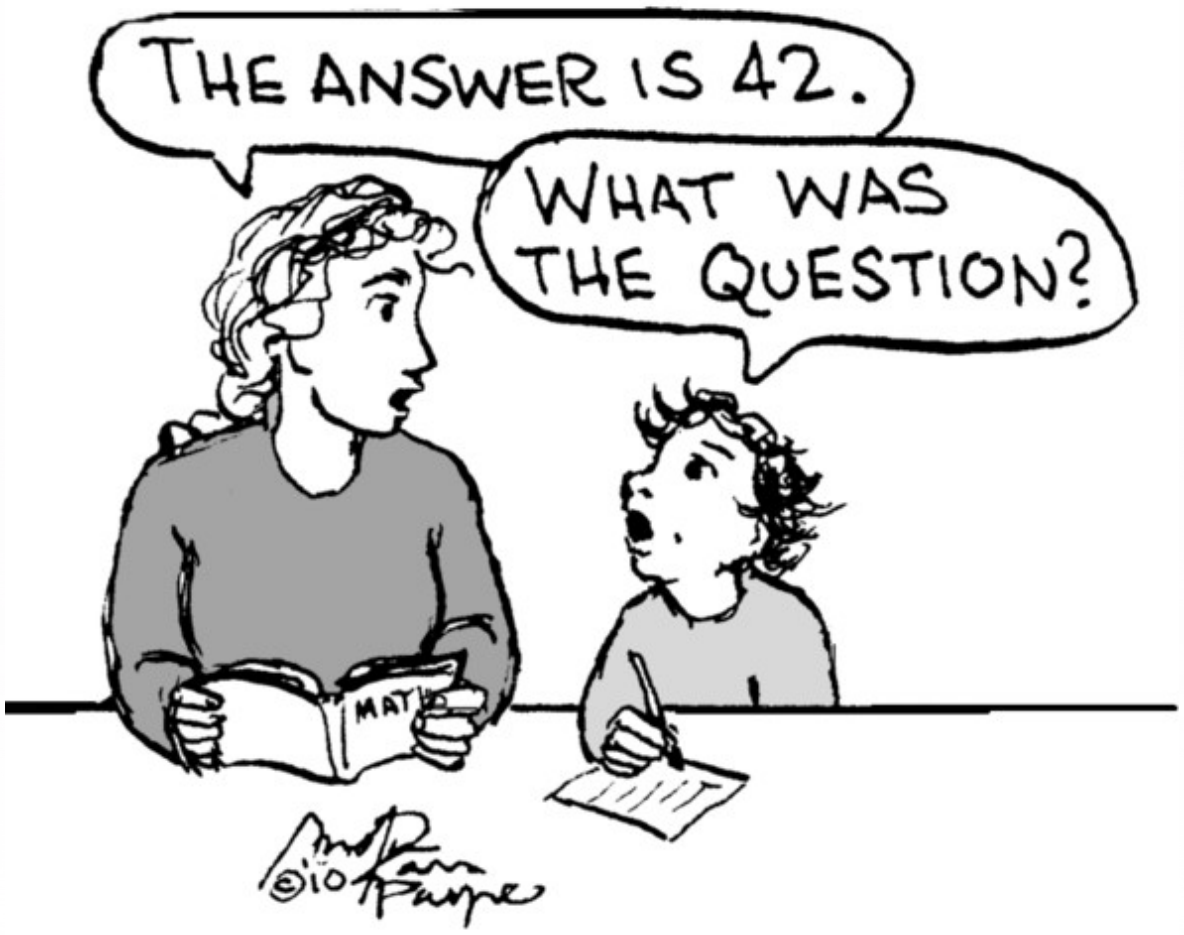
- CMDB
- CIA /BIV
- Patchmanagement

Het ideale VM proces



- Integratie Vulnerability Scanner / Management tool
  - *Meerdere scanners?*
  - *API driven connectors*
- Automatische prioritering van kwetsbaarheden
  - *Koppelingen met CMDB?*
- Integratie met ticketing systeem (incident/change)
  - *Koppelingen met ticketing systeem?*
- Automatische bevestiging of kwetsbaarheid is opgelost
  - *Koppeling terug naar VM*

ACCESS42 Cybersecurity


THE ANSWER IS 42.
WHAT WAS THE QUESTION?
MAT
©10