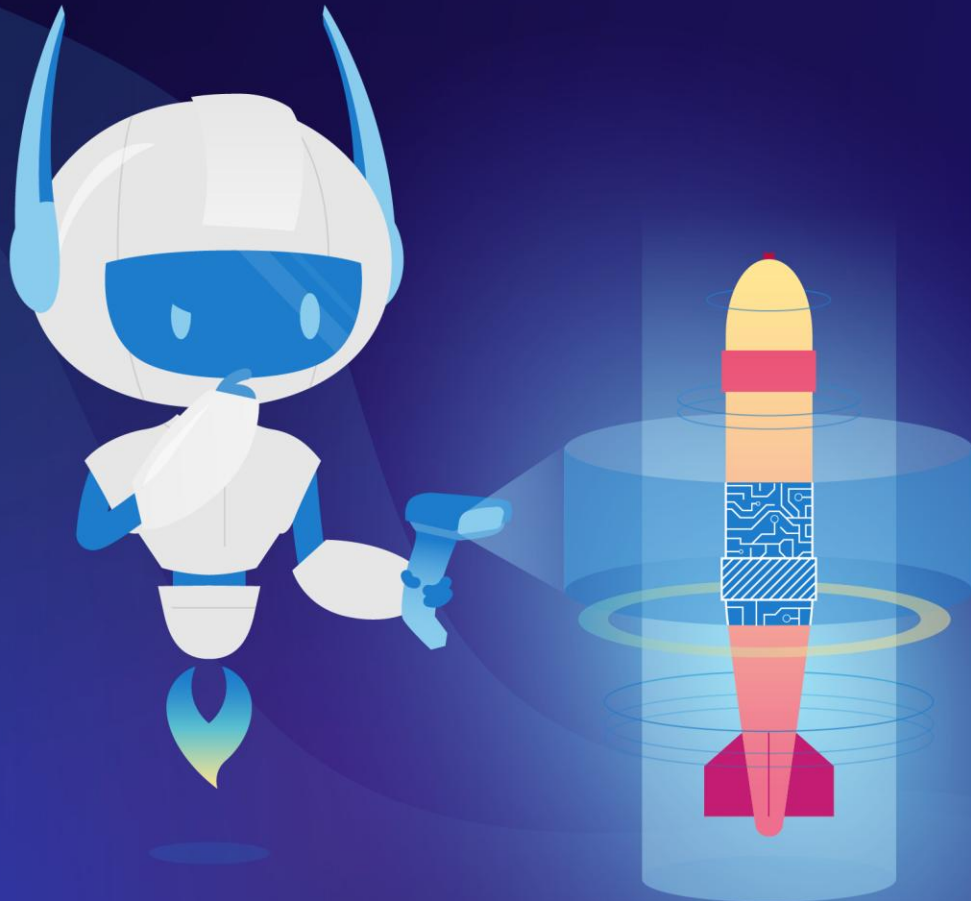


# CERT<sup>2</sup>CONNECT

CYBER & CLOUD SECURITY

TRUSTED SECURITY PARTNER  
FOUNDED IN 2012



**EMPOWER YOUR  
CYBER SECURITY,  
MANAGE YOUR  
SECURITY RISKS**



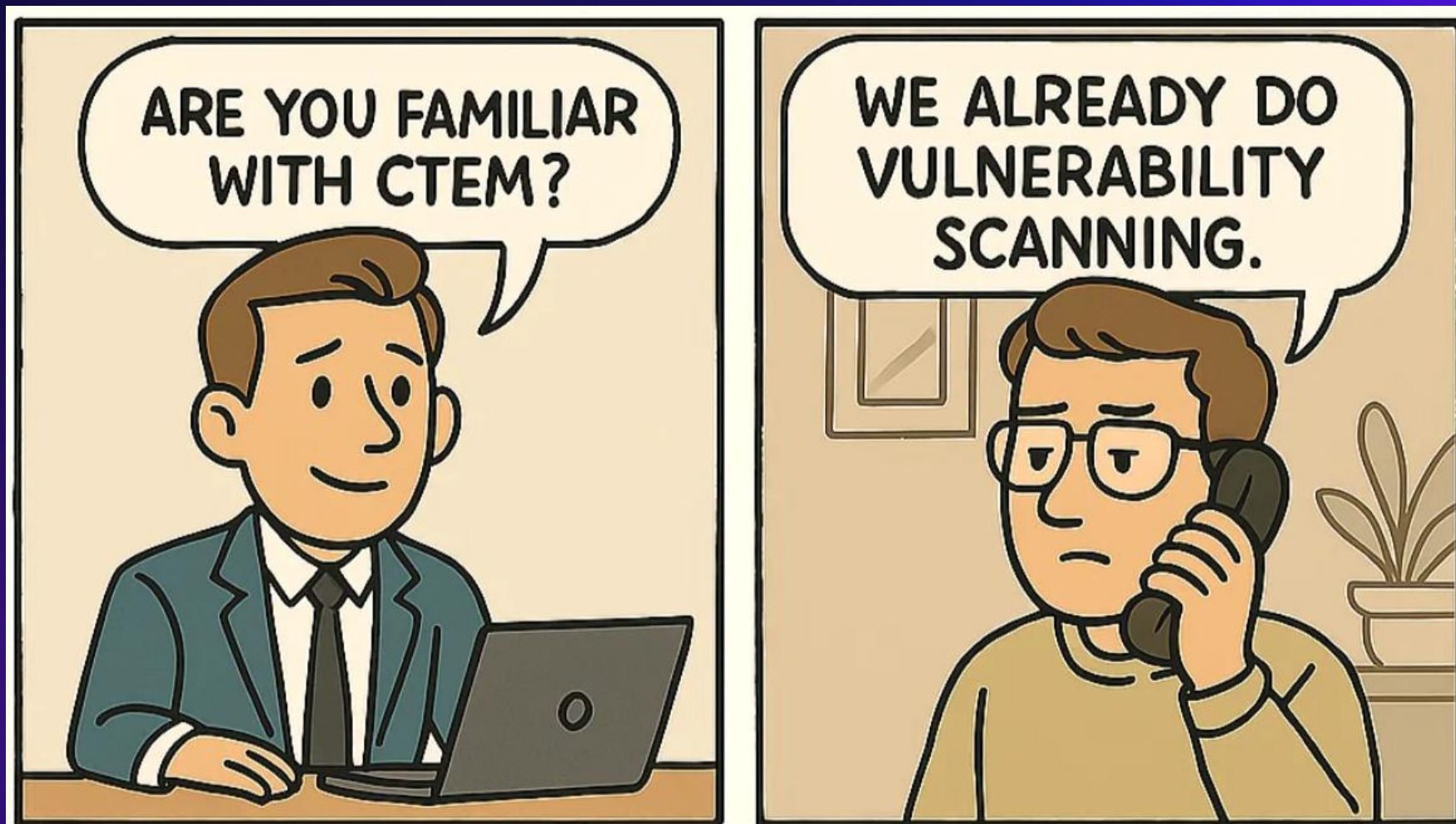
## CONTINUOUSLY IN CONTROL

Due to automated and efficient cyber and appsec security solutions.

Translate cyber risks into business risks.  
Ensure commitment to your plans and priorities.

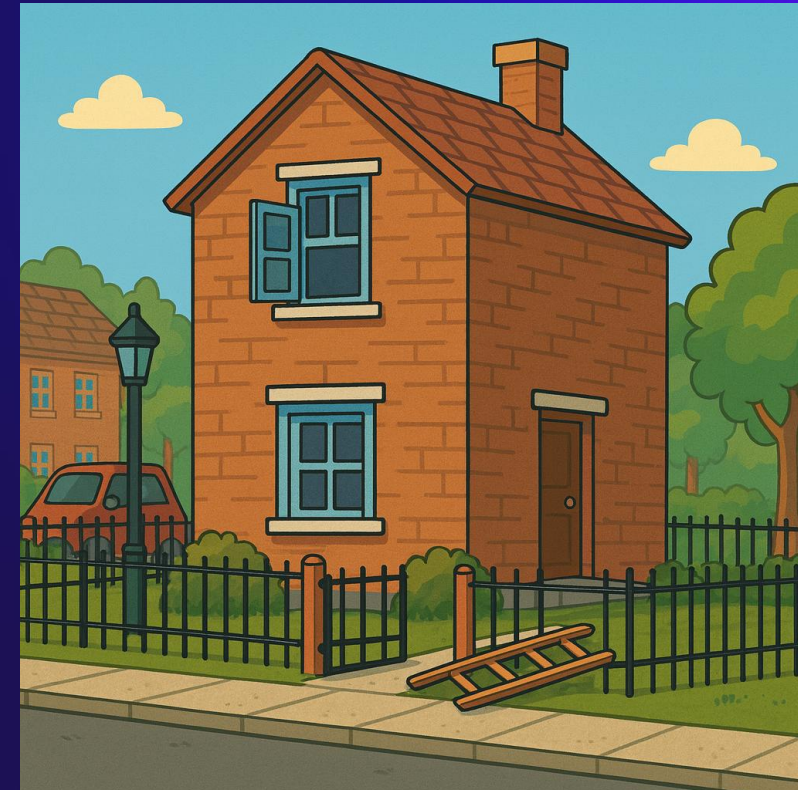
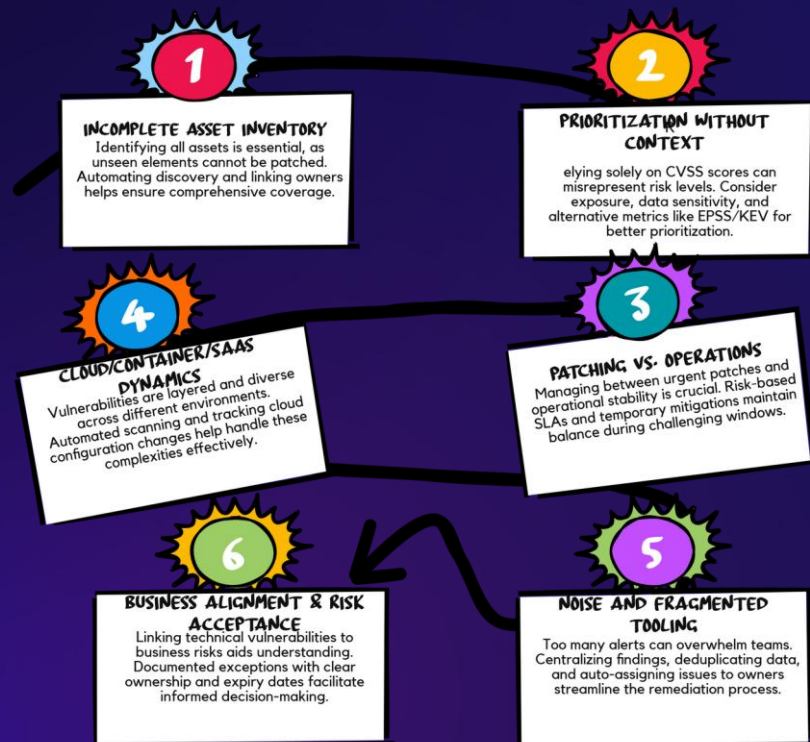
Meet compliance with industry standards and regulations while knowing your security posture instantly.







# Vulnerability management



**CTEM**

# **Continuous Threat Exposure Management**

## Threats



## Vulnerability



## Risk

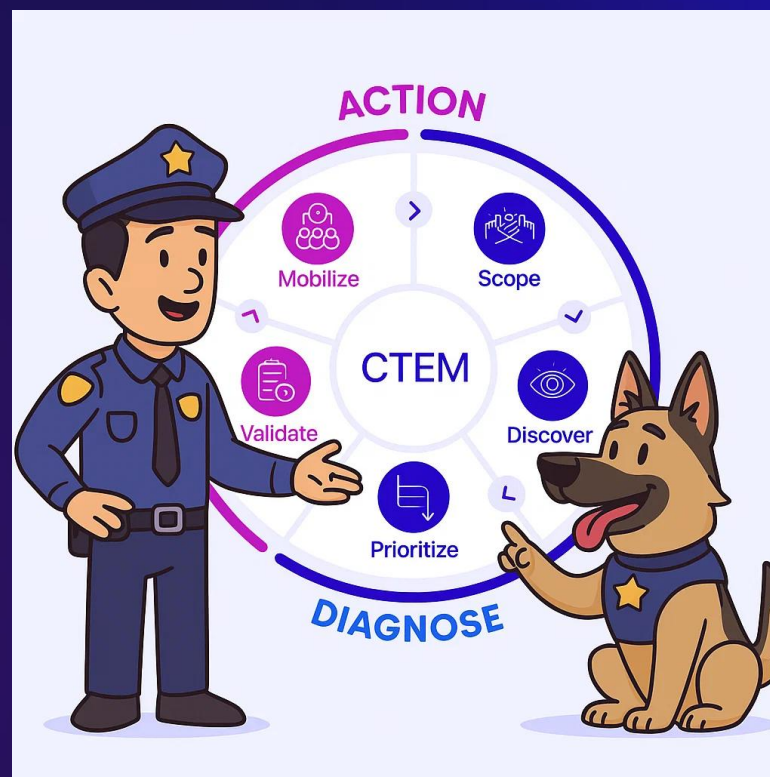






## CTEM

# Continuous Threat Exposure Management





# Scoping



# Scoping

**PROJECT OVERVIEW**

Search

Columns View [Classify Your Companies](#)

Company Name	Sensitivity	Activities	Classification	Risk Assessment	Remediation	Intel Score	Audit Score	Overall Rating
Cert2Connect	Medium	<a href="#">View activity history &gt;</a>	1 Non Classified	2 In progress	3 No open cases	28	60	44
Port comp Demo	Medium	<a href="#">View activity history &gt;</a>	1 Non Classified	2 In progress	3 No open cases	18	-	18
Airport LTD	Medium	<a href="#">View activity history &gt;</a>	1 Non Classified	2 In progress	3 No open cases	32	-	32
calmco	Medium	<a href="#">View activity history &gt;</a>	1 Non Classified	2 In progress	3 No open cases	22	-	22
Movaci	High	<a href="#">View activity history &gt;</a>	1 Classified	2 In progress	3 No open cases	27	-	27

Rows per page: 10 1 - 5 of 5

**ASSESSMENT SUMMARY**

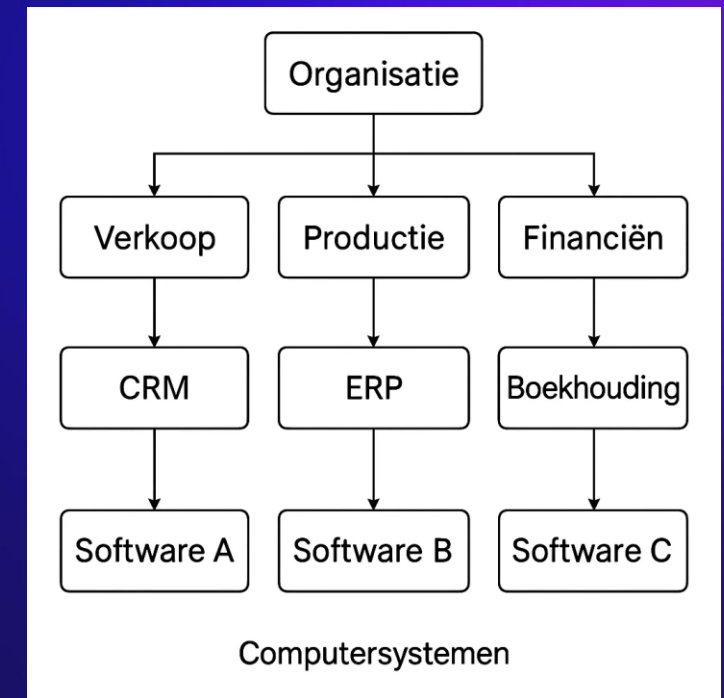
Intelligence Assessment In Progress

In Progress 5

**PROJECT RISK BREAKDOWN**

Average Score By Risk Vector

High Risk Vectors 1



# Discover





# Discover

OPENWMS REPORT

Analysis

Dashboard

Assets

Vulnerabilities

Import

Appliances

User management

Europe/Berlin

Sign out in: 29:37

John Doe

Manage tags

Export

### Assets

▼

Match

All

Host name

IP address

Last scan

Operating system

Tag

IP address

Operating system

Appliance name

Last scan

Asset ID

Criticality

Tags

Action

target-gps-01-debian	192.168.30.52	Debian GNU/Linux 9.3	Lab Network #1 (Greenbone Enterprise 450)	Apr 24, 2025, 09:03:39 AM	af95a207-e38b-ba8e-b9d1-ba02b9b9b9c2	<div><div></div></div>	IoT: Sector 4	<div>🔍</div>
gps-01-macos-pro-max	192.168.123.50	Ubuntu 8.04	Lab Network #1 (Greenbone Enterprise 450)	Apr 24, 2025, 08:44:51 AM	9239a277-6249-ba8e-b9d1-ba02b9b9b9c2	<div><div></div></div>		<div>🔍</div>
target-macos-pro-max	192.168.30.50	Mac OS X / macOS 10.13.6	Lab Network #1 (Greenbone Enterprise 450)	Sep 04, 2023, 05:15:02 PM	af95a207-e38b-ba8e-b9d1-ba02b9b9b9c2	<div><div></div></div>	Department: Marketing +1	<div>🔍</div>
target-gps-01-debian-0-gps-train-greenbone-net	192.168.30.52	Debian GNU/Linux 9	Lab Network #1 (Greenbone Enterprise 450)	Apr 24, 2025, 08:01:56 AM	7a9a2c17b-2249-4336-b9d1-ba02b9b9b9c2	<div><div></div></div>	IoT: Sector 4 +1	<div>🔍</div>
shiroki-target-01-support-greenbone-net	192.168.123.50	Debian GNU/Linux 9	Lab Network #1 (Greenbone Enterprise 450)	Oct 29, 2024, 04:30:12 PM	94a77613e-1274-4336-b9d1-ba02b9b9b9c2	<div><div></div></div>	IoT: Sector 4	<div>🔍</div>
shiroki-target-01-support-greenbone-net	192.168.123.50	Debian GNU/Linux 9	Lab Network #1 (Greenbone Enterprise 450)	Oct 29, 2024, 04:30:07 PM	af95a207-e38b-ba8e-b9d1-ba02b9b9b9c2	<div><div></div></div>	IoT: Sector 4	<div>🔍</div>
shiroki-target-01-support-greenbone-net	192.168.123.50	Debian GNU/Linux 9	Lab Network #1 (Greenbone Enterprise 450)	Sep 04, 2023, 05:10:43 PM	94a77613e-1274-4336-b9d1-ba02b9b9b9c2	<div><div></div></div>		<div>🔍</div>
IoT-01-gps-devnet-greenbone-net	192.168.9.130	Debian GNU/Linux 10	Lab Network #1 (Greenbone Enterprise 450)	Sep 04, 2023, 04:31:59 PM	af95a207-e38b-ba8e-b9d1-ba02b9b9b9c2	<div><div></div></div>	Department: Engineering +1	<div>🔍</div>
gps-01-support-greenbone-net	192.168.123.50	Debian GNU/Linux 8	Lab Network #1 (Greenbone Enterprise 450)	Sep 04, 2023, 04:37:05 PM	af95a207-e38b-ba8e-b9d1-ba02b9b9b9c2	<div><div></div></div>		<div>🔍</div>
gps-01-support-greenbone-net	192.168.123.50	Debian GNU/Linux 8	Lab Network #1 (Greenbone Enterprise 450)	Sep 04, 2023, 04:37:47 PM	94a77613e-1274-4336-b9d1-ba02b9b9b9c2	<div><div></div></div>		<div>🔍</div>

Items per page: 10

1 - 10 of 2,303 items

<

1

2

3

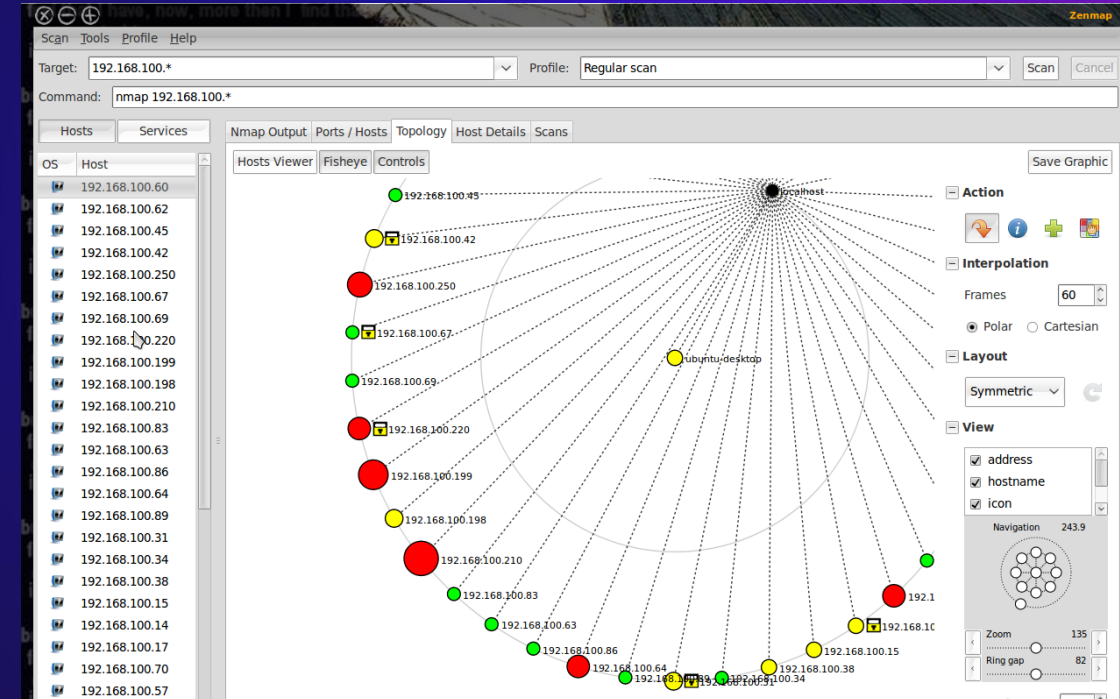
4

5

...

231

>



# Prioritize



Dashboards

Scope

Discover

Validate

Prioritize

Reports

Settings

Vulnerability Prioritization

12.5K

CVEs

CVEs by severity

Critical

High

Medium

Low

Info

CVEs by asset tier

Crown Jewel

574

Tier 1

4.9K

Tier 2

4.9K

Tier 3

1.8K

Unassigned

320

CVEs prevention ratio

Prevented

Not Prevented

27%

Prevention ratio

CVEs exploitability breakdown

All CVEs

13K

Exploited CVEs

541

APT groups exploited

65

APT groups targeted

29

Try searching for...

Date Range

Filters

12,540 results

Select all

Show severity calculation

Columns

Export

<input type="checkbox"/>	CVE ID	CVSS >> Analyzed severity ↑↓	Assets count ↑↓	Asset types	Business context	Testable ↑↓	Prevention ratio ↑↓	Detection ratio ↑↓	Business owner	Exposures count ↑↓	Affects
<input type="checkbox"/>	CVE-2017-8464	8.8 High » 9.2 Critical	2	Host	Finance & Revenue Systems +1	Testable	0%		N/A	2	Micros
<input type="checkbox"/>	CVE-2023-22527	9.8 Critical » 9.2 Critical	1	Host	Identity & Access Management	Testable	13%		N/A	1	Atlassi
<input type="checkbox"/>	CVE-2024-1709	10.0 Critical » 8.8 High	1	Host	Crown Jewels	Testable	38%	8%	N/A	1	
<input type="checkbox"/>	CVE-2013-3900	8.8 High » 8.7 High	24	Host	Compliance Systems +4	Testable			N/A	24	Micros
<input type="checkbox"/>	CVE-2023-38831	7.8 High » 8.7 High	12	Host	Finance & Revenue Systems +2	Testable		0%	N/A	12	
<input type="checkbox"/>	CVE-2024-26169	7.8 High » 8.7 High	5	Host	Finance & Revenue Systems +1	Testable	0%		N/A	5	Micros





SS

Dashboard

Scope

Discover

Validate

Prioritize

Reports

Settings

Exposure Validation

Templates

Attack Simulation

Threat Feed

Assessments

Resources

Quick scenario filters

New scenarios

No pre-requirements

Shared scenarios

Security controls

Antivirus

CDR

CWPP

DLP

SEG

EDR

IPS / IDS

KBS

SIEM

SOAR

WAF

SWG

Platforms

1 item selected

Windows

(1) Selected

Select all

Clear all

☒ Windows

APT Groups

1 item selected

Scattered Spider

(1) Selected

Select all

Clear all

☒ Scattered Spider

Destination country

1 item selected

Netherlands

(1) Selected

Select all

Clear all

☒ Netherlands

Select item

Search scenarios

Date Range

8,975 Scenarios

Select all

+ Create scenario

Interlock Ransomware: Obfuscation and Persistence Techniques

This scenario focuses on the use of obfuscated PowerShell commands and the creation of malicious shortcuts to ensure persistence on a Windows system. It simulates the encoding of commands into Base64 and the creation of a shortcut in the startup folder, which executes the malicious payload upon system reboot. The harmful activities simulated include the use of obfuscation to evade detection and the establishment of persistence through malicious shortcuts, highlighting the tactics employed by attackers to maintain access to compromised systems.

New

HIGH

2 actions

Interlock Ransomware: Malicious Software Installation

This scenario focuses on the installation of remote access tools and the downloading of malicious files using PowerShell. It simulates the installation of AnyDesk and the use of the MsXmI COM object to download files from untrusted sources. The harmful activities simulated include the unauthorized installation of software that can facilitate remote access and the potential downloading of malicious files, which can lead to further exploitation of the system and unauthorized access to sensitive information.

New

HIGH

2 actions

Interlock Ransomware: Malicious File Downloads and Exfiltration

This scenario focuses on the use of various PowerShell methods to download files and exfiltrate sensitive data from a Windows system. It simulates multiple techniques for downloading files, including the use of Invoke-WebRequest and RClone for FTP exfiltration. The harmful activities simulated include the unauthorized downloading of potentially malicious files and the transfer of sensitive data to remote servers, demonstrating how attackers can exploit vulnerabilities to steal information and compromise system integrity.

New

HIGH

2 actions

Interlock Ransomware: Remote Access and File Download

This scenario focuses on the installation of remote access software and the downloading of files using PowerShell to facilitate unauthorized access and data exfiltration. It simulates the installation of ScreenConnect, enabling attackers to remotely control the compromised system, and tests the ability to download files from external sources. The harmful activities simulated include the establishment of a Command and Control (C2) connection through remote access software and the potential theft of sensitive data via file downloads, highlighting the risks associated with unauthorized remote access.

New

HIGH

2 actions

Interlock Ransomware: Keylogging and File Download

This scenario focuses on the deployment of keylogging software and file downloading techniques to capture sensitive information and potentially install further malicious payloads. It simulates the downloading of a keylogger that records user keystrokes, allowing attackers to harvest confidential data such as passwords and personal information. Additionally, it tests the system's defenses against file downloads using PowerShell commands. The harmful activities simulated include the capture of user input through keylogging and the unauthorized downloading of files, which can lead to data breaches and further exploitation of the compromised system.

New

CRITICAL

2 actions

Interlock Ransomware: Registry Persistence and Payload Execution

This scenario focuses on the use of PowerShell to establish persistence and execute malicious payloads on a Windows system. It simulates the creation of a RunOnce registry entry, which ensures that a specified program or script runs at the next system startup, thereby allowing the attacker to maintain access to the system. Additionally, the scenario includes downloading malicious code and executing it, demonstrating how attackers can infiltrate and compromise systems. The harmful activities simulated include the establishment of persistence through registry manipulation, downloading and executing malicious files, and executing obfuscated PowerShell commands, all of which are common tactics used in ransomware attacks.

New

HIGH

4 actions

<

1

2

3

4

5

>



# Remediate





# Remediate

<input type="checkbox"/>	Finding Name	Scenario Name	Timestamp ↑↓	End Time ↑↓	Status ↑↓	Detection
<input type="checkbox"/>	Insufficient Endpoint Security protection	Add New Local Admin User	4/3/2025 03:46:58	4/3/2025 03:47:12	Not Prevented	
<input type="checkbox"/>	Misconfigured security control detection	Add New Local Admin User	4/3/2025 03:46:58	4/3/2025 03:47:12	Not Detected	⊖ No alert or event triggered



add a new user to the local administrators group

Endpoint Detection and Response (EDR) rules monitor and take actions on endpoints. They are used for detecting and responding to threats at the device level, such as unusual file executions or process behaviors.

Cymulate's universal EDR mitigation

EDR RULEHighCopy

'Process.CommandLine CONTAINS "net localgroup administrators" AND Process.CommandLine CONTAINS "/add"

Query translator

»SentinelOne

Copy

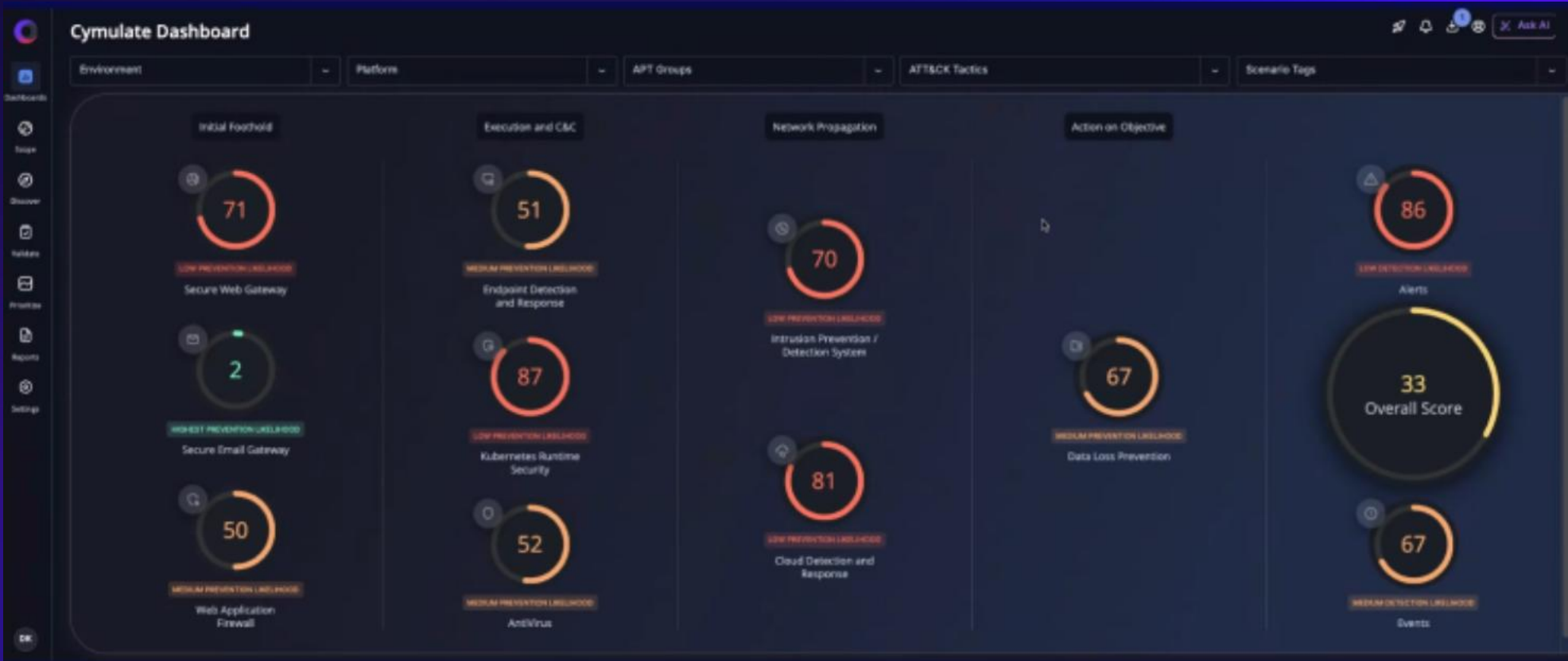
Rule type: Single event "(tgt.process.cmdline contains 'net localgroup administrators' and tgt.process.cmdline contains '/add')"

# Monitor



# Monitor

<input type="checkbox"/>	Finding Name	Scenario Name	Timestamp ↑↓	End Time ↑↓	Status ↑↓	Detection	Previous Status ↑↓
<input type="checkbox"/>		Add New Local Admin User	4/5/2025 03:08:34	4/5/2025 03:09:10	Detected	Alert & Event triggered	Not Detected
<input type="checkbox"/>	Insufficient Endpoint Security protection	Add New Local Admin User	4/5/2025 03:08:34	4/5/2025 03:09:10	Not Prevented		Not Prevented





# Valkuilen van CTEM



# CTEM Program by Cymulate

## Program Overview



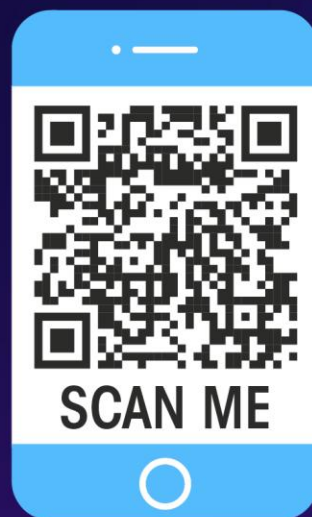
# Vragen?





# CERT<sup>2</sup>CONNECT

CYBER & CLOUD SECURITY



**MEET OUR EXPERTS**

**W** [WWW.CERT2CONNECT.COM](http://WWW.CERT2CONNECT.COM)

**E** [INFO@CERT2CONNECT.COM](mailto:INFO@CERT2CONNECT.COM)

**T** +31 (0)20 8208631



  
**CYBERVEILIG  
NEDERLAND**  
MEMBER