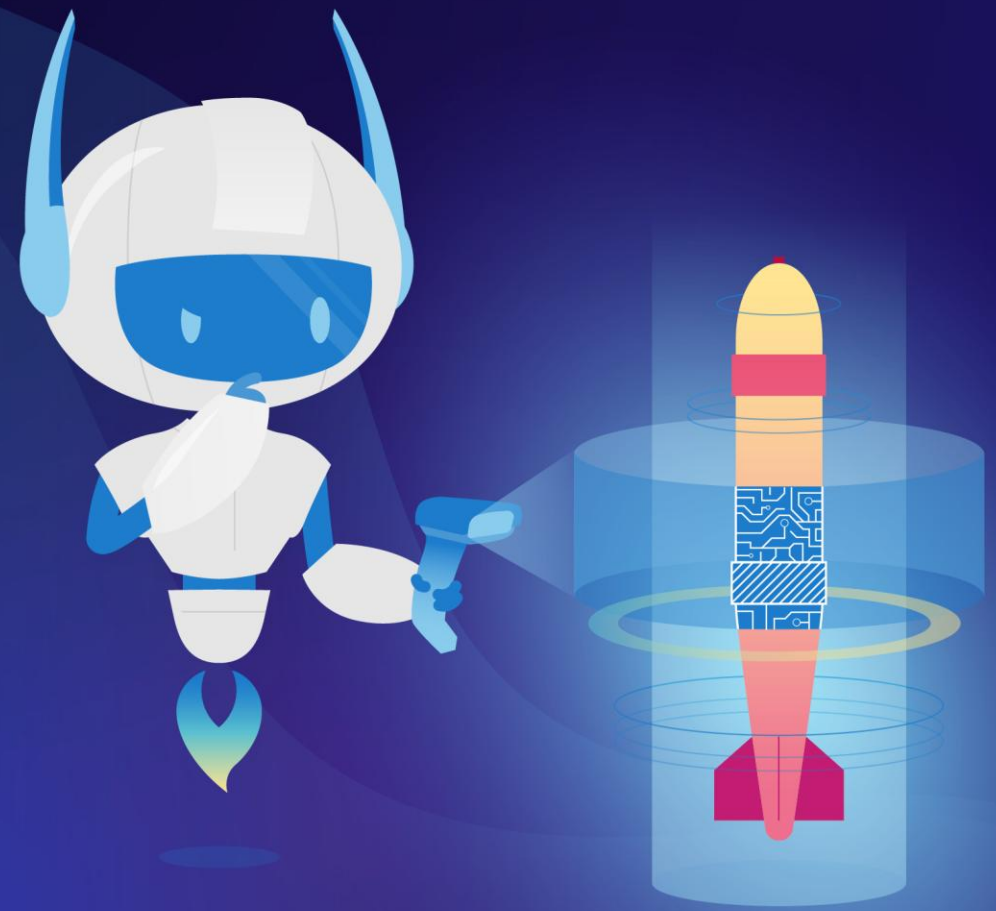


CERT2CONNECT

CYBER & CLOUD SECURITY

TRUSTED SECURITY PARTNER
FOUNDED IN 2012

EMPOWER YOUR CYBER SECURITY, MANAGE YOUR SECURITY RISKS

CYBERVEILIG NEDERLAND
MEMBER

CERT 2 CONNECT

CYBER & CLOUD SECURITY

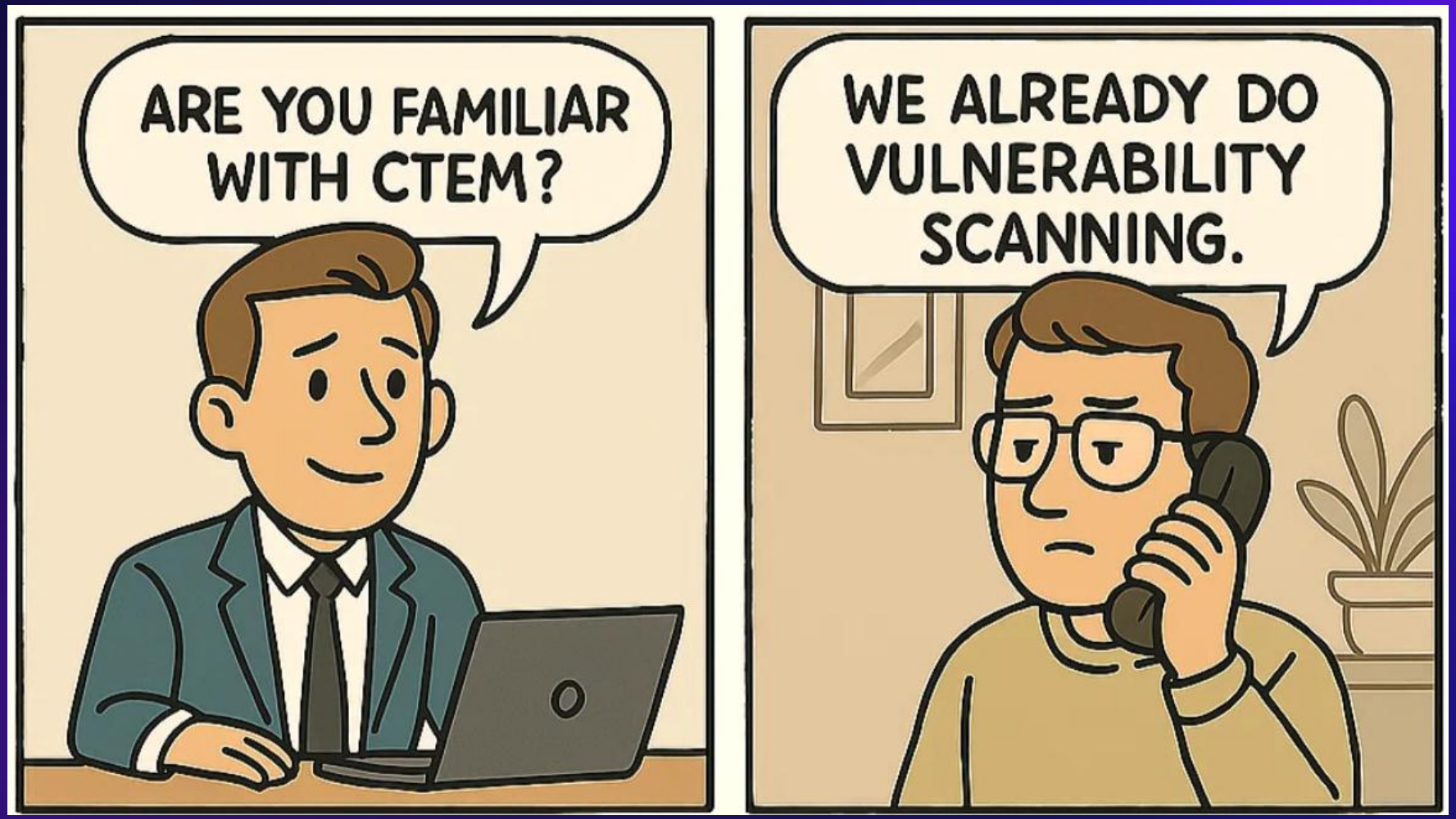
CONTINUOUSLY IN CONTROL

Due to automated and efficient cyber and appsec security solutions.

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

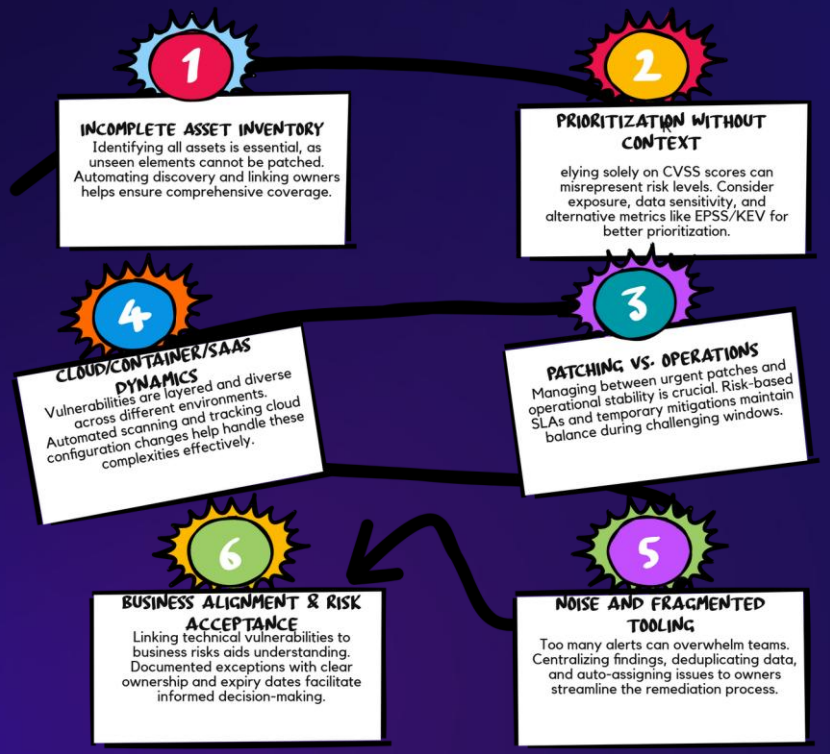
Meet compliance with industry standards and regulations while knowing your security posture instantly.

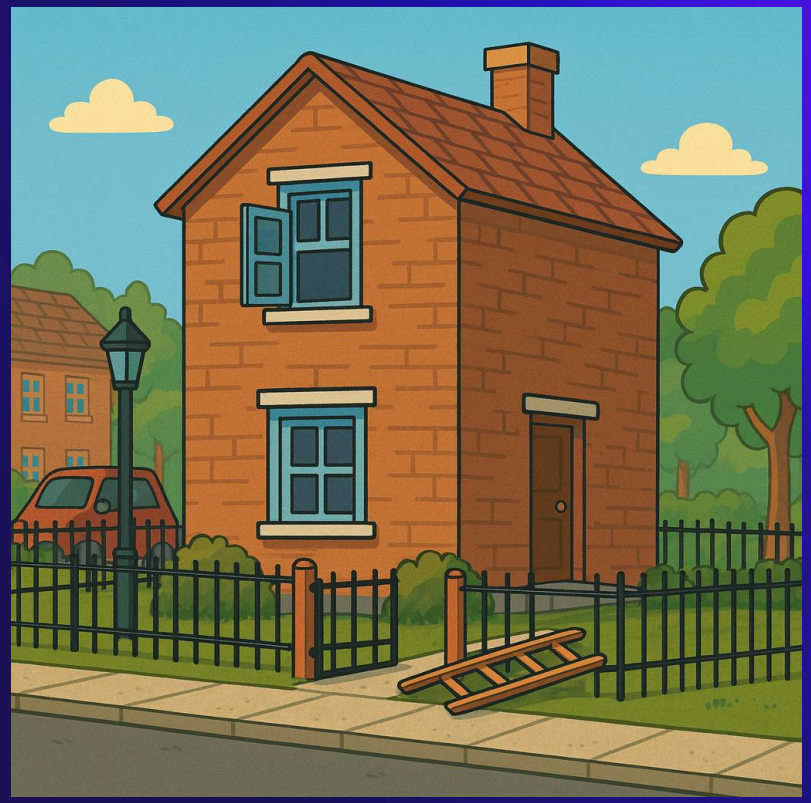
CERT2CONNECT
CYBER & CLOUD SECURITY



CERT2CONNECT
CYBER & CLOUD SECURITY

Vulnerability management





CERT2CONNECT
CYBER & CLOUD SECURITY

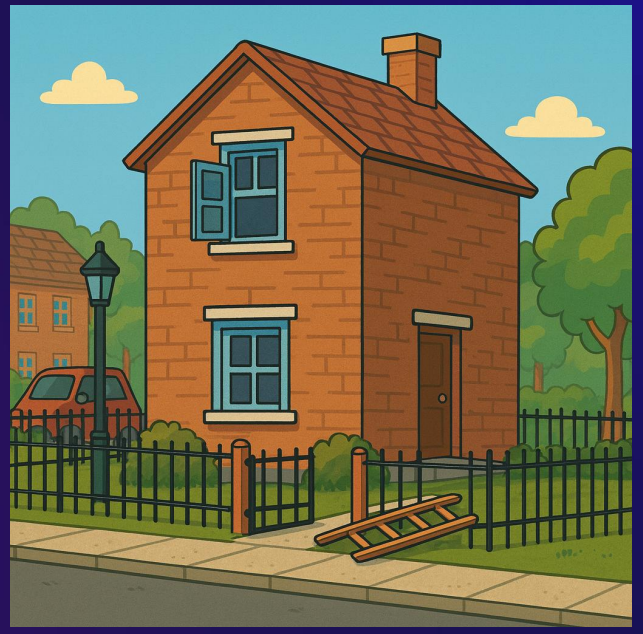
CTEM

Continuous Threat Exposure Management

CERT2CONNECT
CYBER & CLOUD SECURITY

Threats

Vulnerability



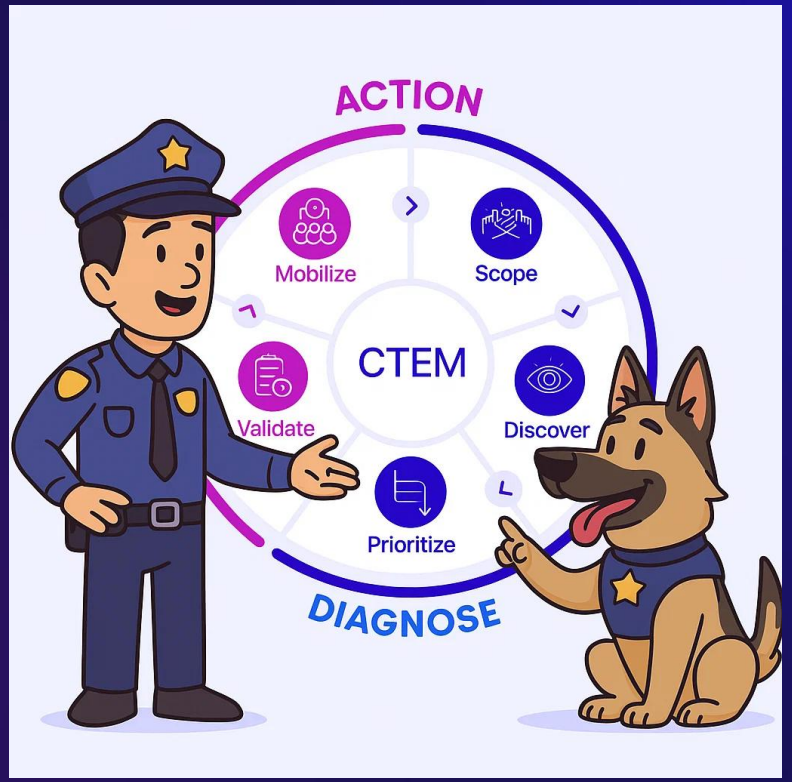
Risk


LEVERANCIER
ONZE ORGANISATIE
KLANT

CERT2CONNECT
CYBER & CLOUD SECURITY

CTEM

Continuous Threat Exposure Management

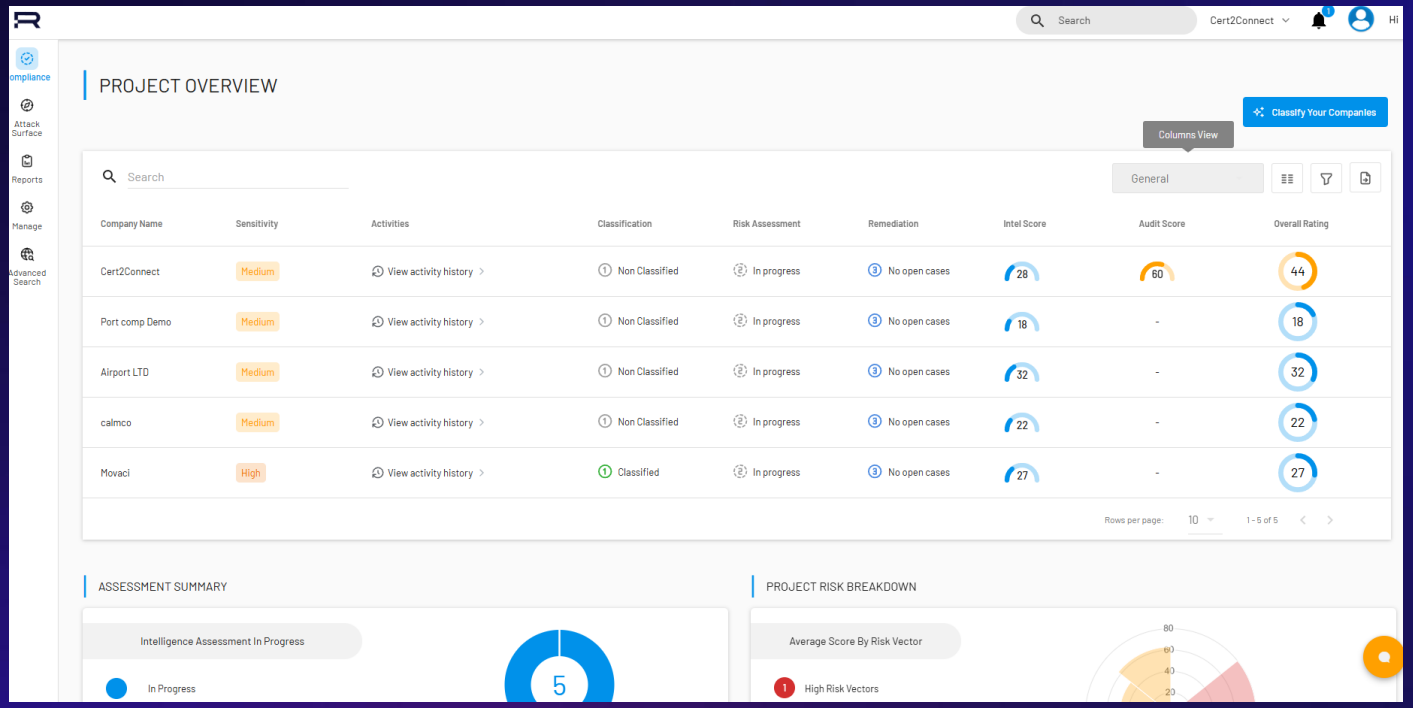


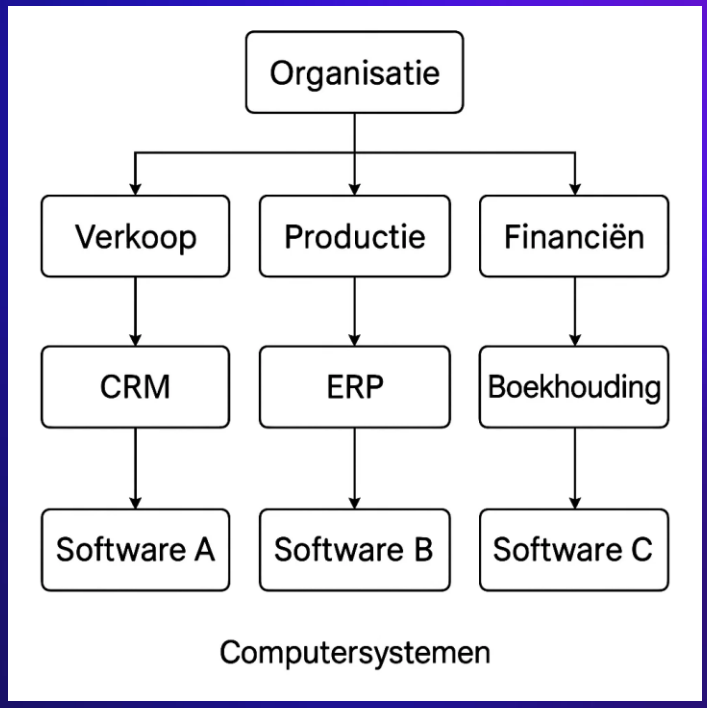
CERT2CONNECT
CYBER & CLOUD SECURITY

Scoping

CERT2CONNECT
CYBER & CLOUD SECURITY

Scoping



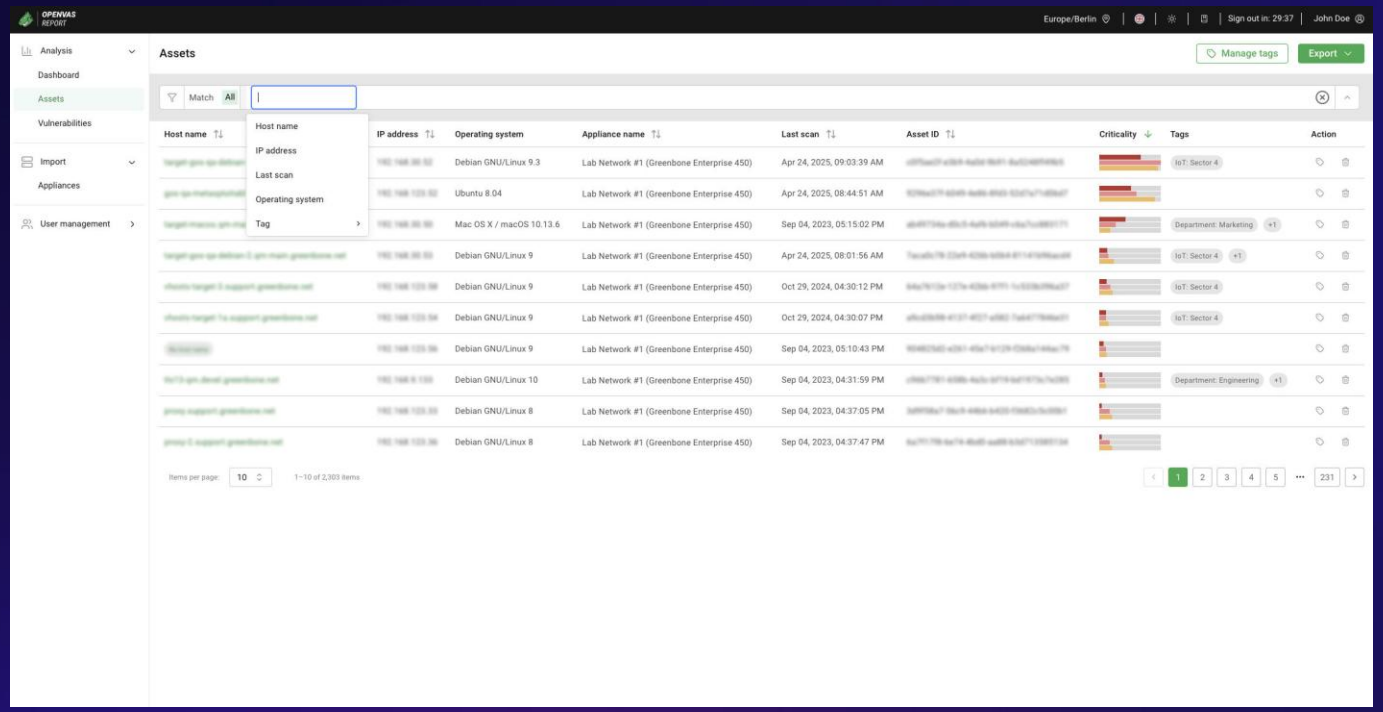


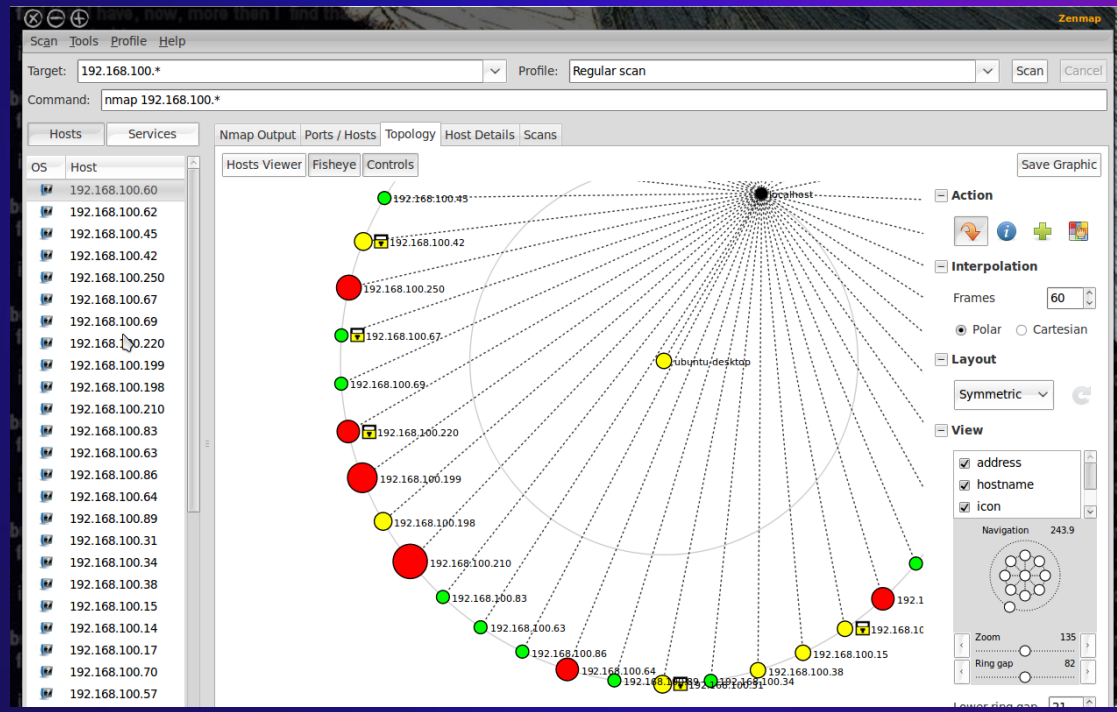
CERT2CONNECT
CYBER & CLOUD SECURITY

Discover

CERT 2 CONNECT
CYBER & CLOUD SECURITY

Discover



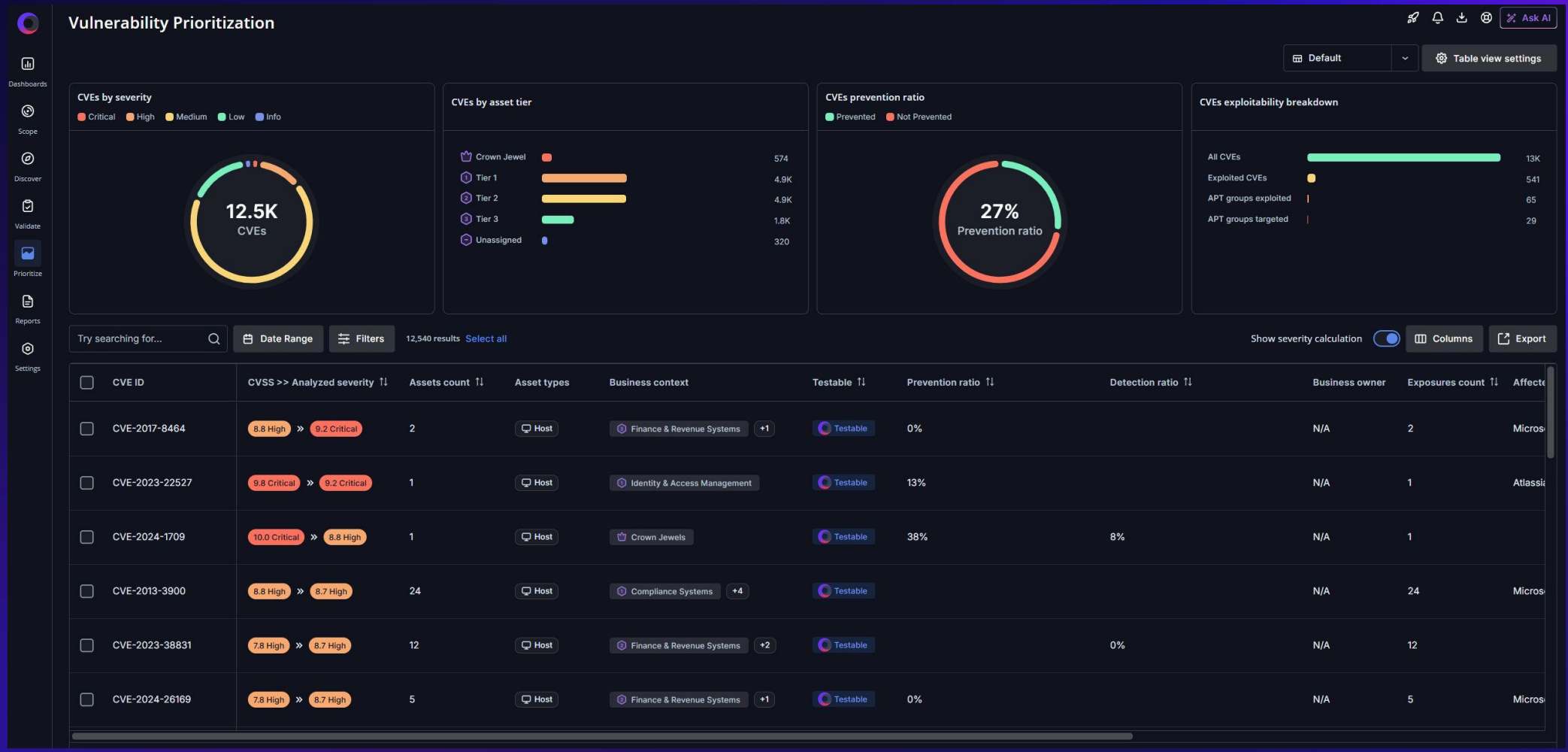


CERT2CONNECT
CYBER & CLOUD SECURITY

Prioritize

CERT 2 CONNECT
CYBER & CLOUD SECURITY

Prioritize

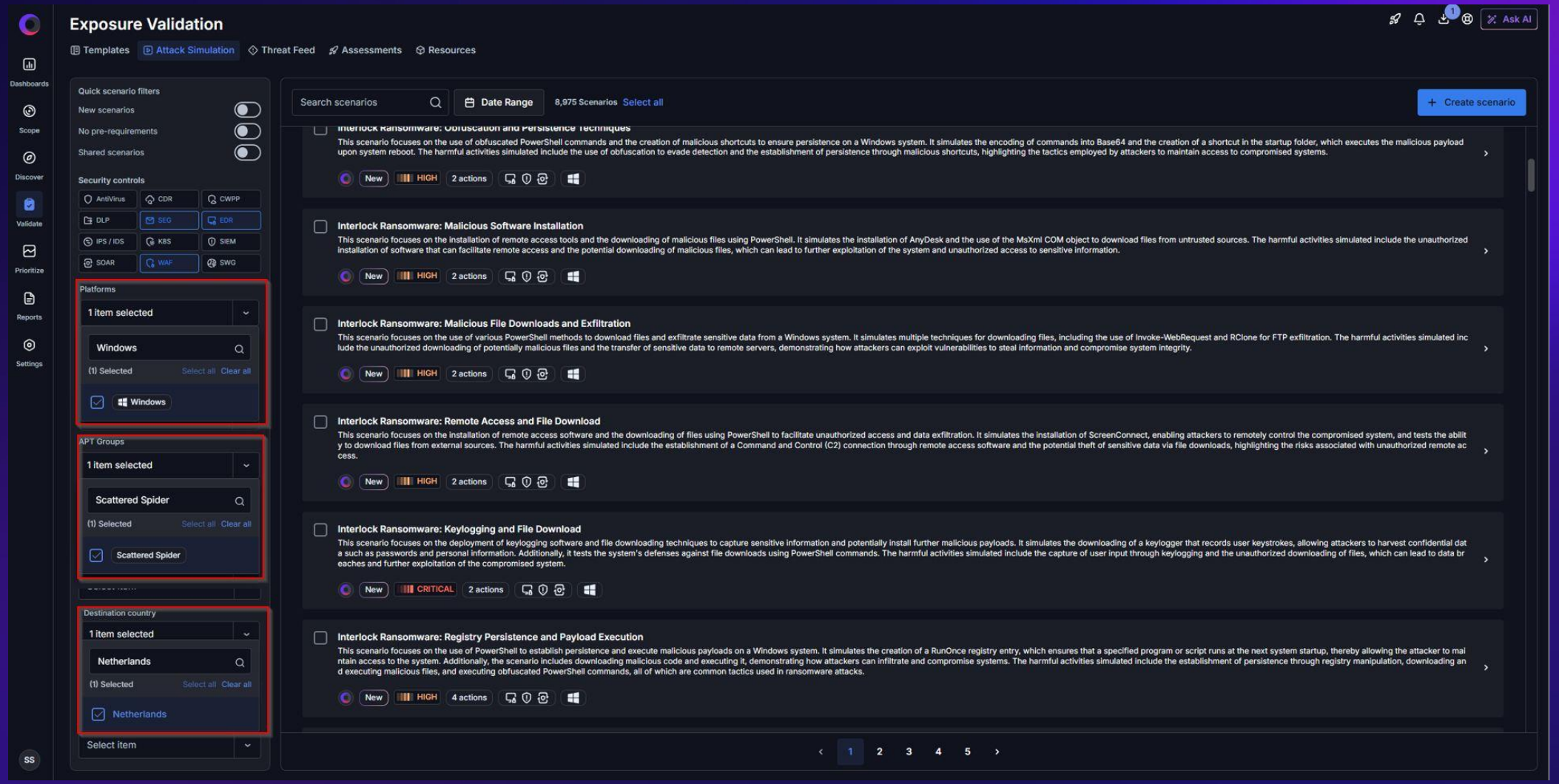


CERT2CONNECT
CYBER & CLOUD SECURITY

Validate

CERT 2 CONNECT
CYBER & CLOUD SECURITY

Validate



CERT2CONNECT
CYBER & CLOUD SECURITY

Remediate

CERT2CONNECT
CYBER & CLOUD SECURITY

Remediate

Finding Name	Scenario Name	Timestamp	End Time	Status	Detection
Insufficient Endpoint Security protection	Add New Local Admin User	4/3/2025 03:46:58	4/3/2025 03:47:12	Not Prevented	
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 RULE High Copy

'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')"

CERT2CONNECT
CYBER & CLOUD SECURITY

Monitor

CERT 2 CONNECT
CYBER & CLOUD SECURITY

Monitor

Finding Name	Scenario Name	Timestamp	End Time	Status	Detection	Previous Status
	Add New Local Admin User	4/5/2025 03:08:34	4/5/2025 03:09:10	Detected	Alert & Event triggered	Not Detected
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

CERT2CONNECT
CYBER & CLOUD SECURITY

Valkuilen van CTEM

Ontbreken validatiefase

Test ontdekte kwetsbaarheden op waarheidsgetrouwe exploitatiemogelijkheden.

Geen koppeling risicobeheer

Verbind kwetsbaarheden met bedrijfsrisico's voor betere prioritering.

Overvolle backlog

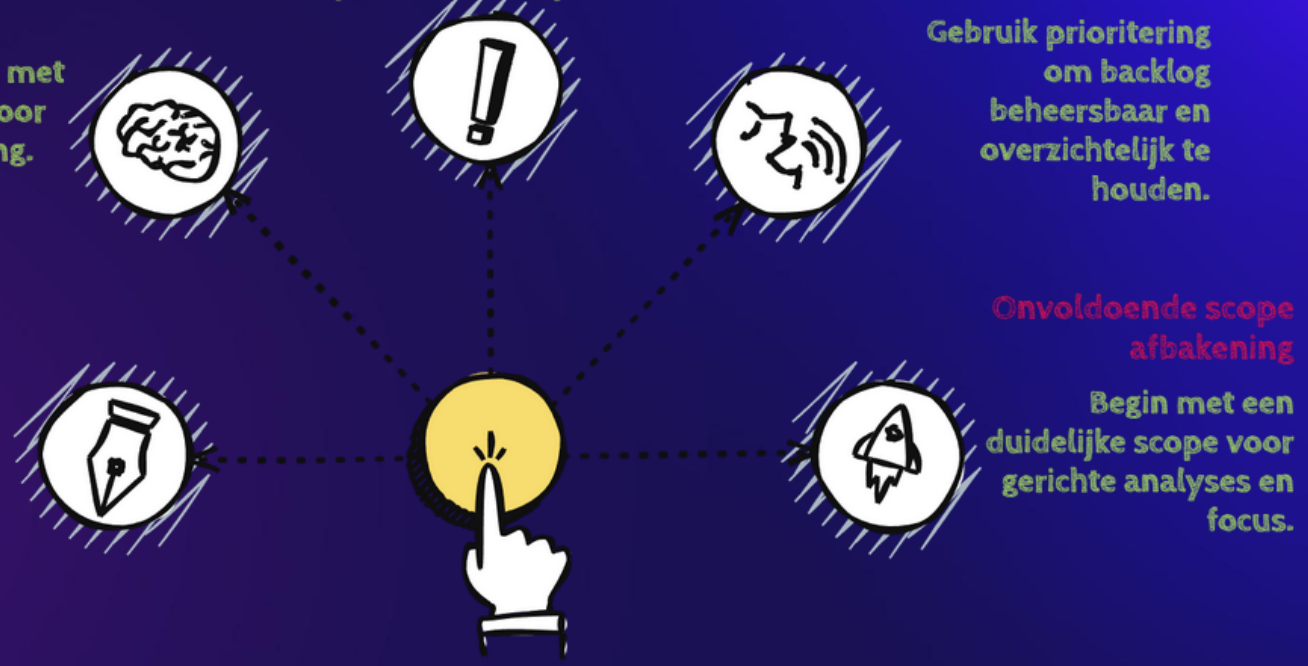
Gebruik prioritering om backlog beheersbaar en overzichtelijk te houden.

Tool versus proces

CTEM moet als proces gezien worden, niet enkel als tool.

Onvoldoende scope afbakening

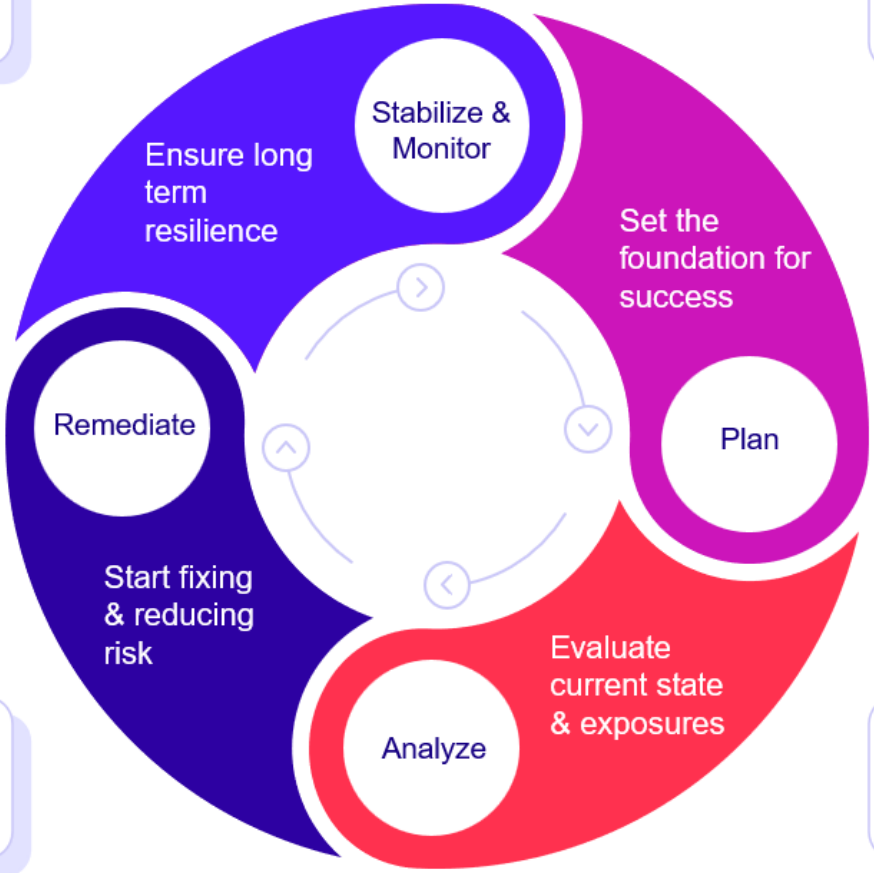
Begin met een duidelijke scope voor gerichte analyses en focus.



CERT2CONNECT
CYBER & CLOUD SECURITY

CTEM Program by Cymulate

Program Overview



01 Drift Monitoring
Watch for deviations from baseline due to emerging threats.

02 Continuous Assessment
Regularly reassess risks in a dynamic landscape.

01 IoC Remediation
Quick wins—automated or manual resolution.

02 Broader Remediation
Address deeper issues and minimize the gaps.

01 Scoping
Align on priorities, reporting metrics, and action plans.

02 Initial Assessment
Understand the baseline and identify quick wins.

03 Baseline Capturing
Define your new secure state.

01 Gap Analysis
Identify where your defenses fall short.

02 Prioritize Risks
Focus on what matters most based on criticality and exposure.

CERT2CONNECT
CYBER & CLOUD SECURITY

Vragen?

CERT2CONNECT

CYBER & CLOUD SECURITY

SCAN ME

CYBERVEILIG NEDERLAND MEMBER

MEET OUR EXPERTS

W WWW.CERT2CONNECT.COM

E INFO@CERT2CONNECT.COM

T +31 (0)20 8208631