

Vulnerability Management Webinar 2. & 7. Dezember 2021



Risiko-basiertes
Schwachstellenmanagement

Thomas Cueni
Senior Security Engineer



**RANSOMWARE IS THE
MONETIZATION OF
POOR CYBERHYGIENE**

Predict the flaws ransomware will target



AVANTEC
Competence. Security. Trust.

Vulnerability Management Webinar 2. & 7. Dezember 2021



Vulnerability Management Webinar 2. & 7. Dezember 2021

VPR

VULNERABILITY PRIORITY RATING

Leverages supervised machine learning algorithms to calculate the priority of a vulnerability based on the real threat posed.

Key Drivers include

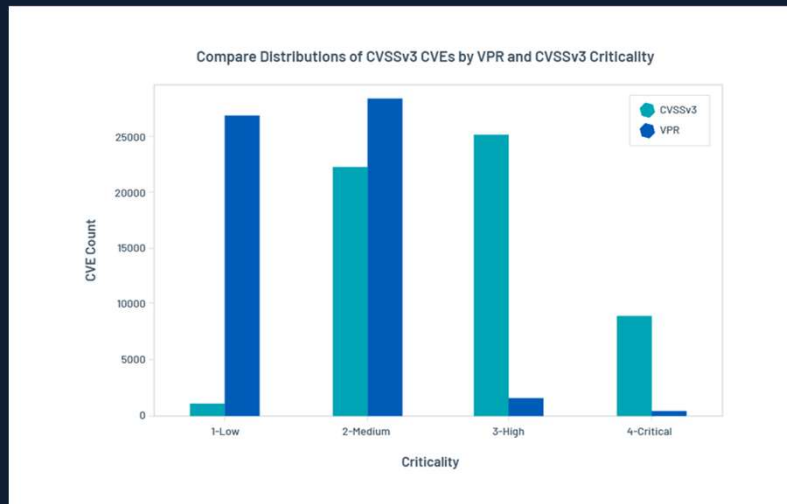
- Threat Recency
- Threat Intensity
- Exploitability
- Vulnerability Age
- Threat Sources

VPR Framework

- CVSS Impact Score**
Captures the effects of a successfully exploited vulnerability (CIA)
- ML Threat Score**
Captures the likelihood a vulnerability will be targeted for exploitation in the near term
- VPR**
A dynamic rating that captures the risk posed by a vulnerability

Vulnerability Management Webinar 2. & 7. Dezember 2021

VPR vs CVSS: Severity Distribution



VPR vs CVSS: Attacks in the Wild

CVE	RF	VT	SW	VPR 2019	CVSSv3 SCORE
CVE-2017-5638		Y		10	10
CVE-2019-10149			Y	9.9	9.8
CVE-2019-0903			Y	9.9	8.8
CVE-2019-2725		Y	Y	9.9	9.8
CVE-2019-0859			Y	9.9	7.8
CVE-2019-3396		Y	Y	9.9	9.8
CVE-2018-20250	Y	Y		9.9	7.8
CVE-2018-15982	Y			9.9	9.8
CVE-2018-8174	Y	Y		9.9	7.5
CVE-2018-7600		Y		9.9	9.8

Compared VPR with CVSS for the most dangerous CVE's of 2019:

- Recorded Future / SonicWall / Verint
- CVE-2019-0859
 - Actively Exploited Zero-Day
- CVE-2018-20250
 - "One of the most widely and rapidly-exploited security flaws of recent times"
- CVE-2018-8174
 - Maze ransomware attack
 - Encrypts & exfiltrates data!



Vulnerability Management Webinar 2. & 7. Dezember 2021

ACR

ASSET CRITICALITY RATING


Leverages algorithms to calculate the criticality of an asset to focus prioritisation efforts.
Key drivers include

- Business Purpose
- Device Type
- Connectivity
- Capabilities
- Location
- 3rd Party Data

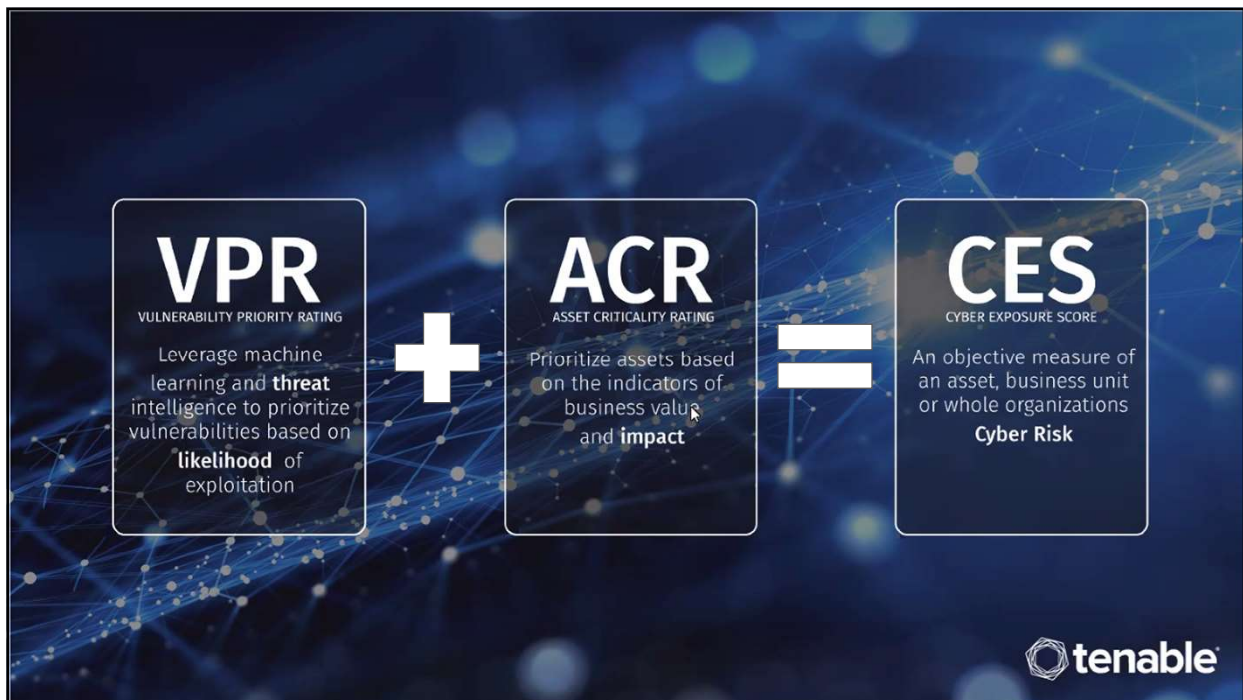
ACR Components

Internet Exposure > Device Type > Capabilities

Is the asset internet accessible? > What type of device is the asset? > What is the purpose of the asset?



Vulnerability Management Webinar 2. & 7. Dezember 2021



CES Overview

CES measures the cyber risk for an individual asset / group of assets

- 0 to 1000 (most exposed)
- Function of ACR & VPR
- Trending & Benchmarking



tenable

Vulnerability Management Webinar 2. & 7. Dezember 2021

Risk Management Metrics 2



Business System Risk
Focus First On
What Matters Most:
Assets & Vulns

Process Integrity Risk
Am I Smart Or Lucky?
Assessment & Remediation
Maturity

+

Assessment Maturity

Measuring Process Integrity Risk

Ensure adequate asset assessment and vulnerability remediation by quantifying and comparing how well you are assessing your environment. Key drivers include:

- Scan Frequency
- Scan Depth
- Remediation Effectiveness

Vulnerability Management Webinar 2. & 7. Dezember 2021

Remediation Maturity

Measuring Process Integrity Risk

Measure speed and efficiency in remediating vulnerabilities.
Benchmark against industry peers. Key drivers include:



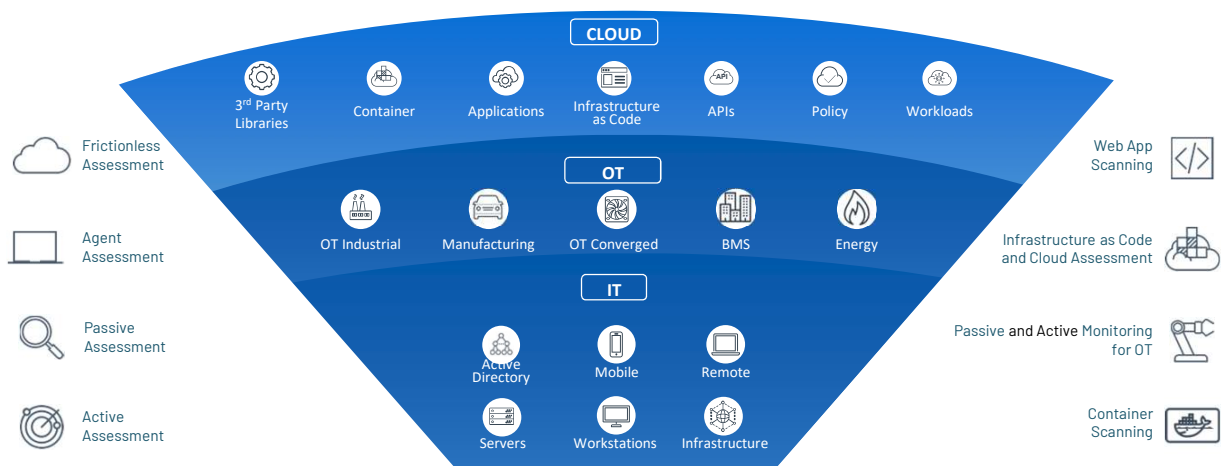
Remediation
Responsiveness



Remediation
Coverage

VISIBILITY OF THE MODERN ATTACK SURFACE

With adaptive approaches to assessing assets and devices across the infrastructure



 **tenable**

AVANTEC
Competence. Security. Trust.

Vulnerability Management Webinar 2. & 7. Dezember 2021

Gartner

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

"BY 2022, ORGANIZATIONS
THAT USE THE RISK-BASED
VULNERABILITY
MANAGEMENT METHOD WILL
SUFFER 80% FEWER
BREACHES.*"

* Gartner, A Guide to Choosing a Vulnerability Assessment Solution, Prateek Bhajanka, Mitchell Schneider, Craig Lawson, April 3, 2019.



AVANTEC
Competence. Security. Trust.

Vulnerability Management Webinar 2. & 7. Dezember 2021

VISIBILITY ACROSS EVERY ATTACK SURFACE

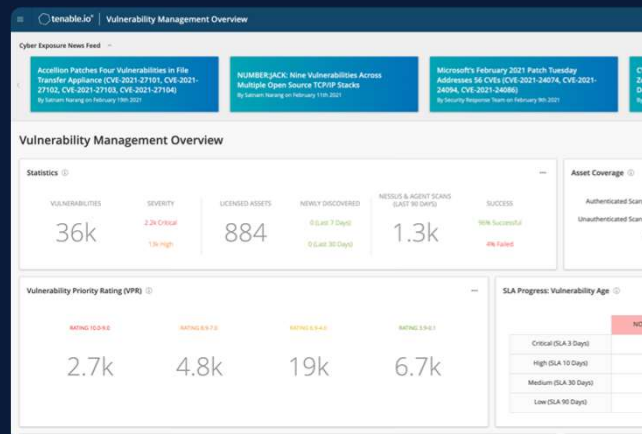
		<p>Detect and Remediate Security Flaws in Your Infrastructure as Code and Running Cloud</p>
<p>Cloud Native Risk-Based Vulnerability Management.</p>	<p>Calculate, Communicate and Compare your Risks and Exposures.</p>	<p>Secure Your Active Directory and Disrupt Attacks.</p>
<p>A Simple, Scalable Approach to Dynamic Application Security Testing.</p>	<p>Gain Visibility into the Security of Container Images.</p>	<p>Gain Complete Visibility, Security and Control of Your Operational Environments.</p>
		<p>See Everything. Predict What Matters. Managed On-Prem.</p>



See everything. Predict what matters.

Managed in the Cloud.

Tenable.io is an integral component of the Tenable Cyber Exposure Platform that provides actionable insight into your entire infrastructure's attack surface.



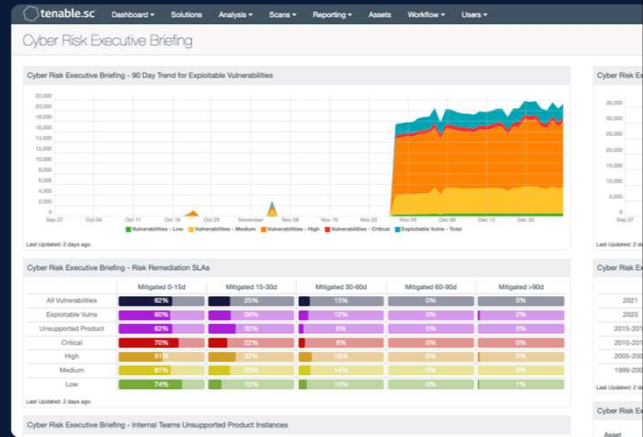
Vulnerability Management Webinar 2. & 7. Dezember 2021



See everything. Predict what matters.

Managed On-Prem.

Get a risk-based view of your IT, security and compliance posture so you can quickly identify, investigate and prioritize vulnerabilities.




Get the operational technology security you need. Reduce the risk you don't.

Tenable.ot protects industrial networks from cyber threats, malicious insiders and human error. With threat detection and mitigation, asset inventory, vulnerability management and configuration control, Tenable's ICS security capabilities identify and predictively prioritize threats and vulnerabilities to maximize the safety and reliability of your operational technology environment.

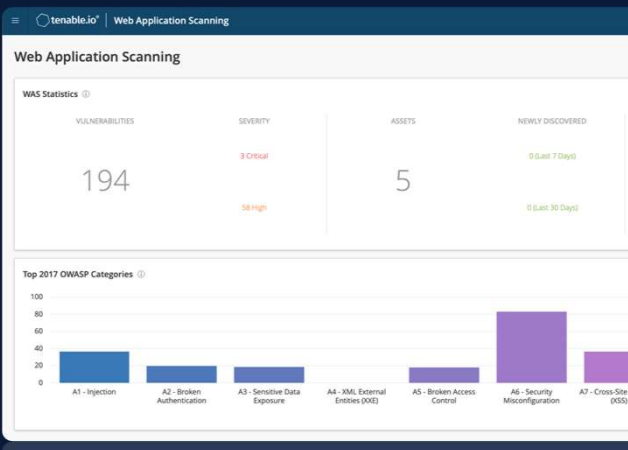
Name	Risk Score	IP/MAC	Family	Firmware	Location
Assembly Line_A #12	10	192.168.9.137 192.168.9.95	CompactLogix	28.011	Production Floor 4
Assembly Line_B #17	10	192.168.1.202	MicroLogix 1400	2.015	Assembly line 1
Assembly Line_A #16	10	192.168.10.6	CompactLogix 1375	30.011	Assembly line 1
Production Units Line A #12	10	192.168.10.89 192.168.9.137	CompactLogix	28.011	Production Floor 4
Assembly Line_A #19	10	192.168.9.95	SUC3	3.013	3rd fl.
Production Units Line A #9	10	192.168.9.27	ControlLogix 5560	20.005	Production Floor 4
Production Units Line B #1	10	192.168.2.211	ControlLogix 5560	20.013	Plant
Production Units Line D #10	10	192.168.10.36	CompactLogix 1375	28.011	Assembly line 2
Schneider PLC	10	192.168.4.46	SE Motionium Unity	1.21	Production Floor 6
Production Units Line B #5	10	192.168.7.46	SE Motionium M560	2.76	Assembly line 2
Shop Floor #7	10	192.168.4.70	SE Quantum Unity	2.20	Production Floor 4
Shop Floor #8	10	192.168.3.65	SE Motionium M560	2.76	Assembly line 1
Shop Floor #1	10	192.168.7.136	SE Motionium M560	2.76	3rd fl.
Production Units Line A #7	10	192.168.10.36	SE Motionium M560	2.76	Assembly line 1

Vulnerability Management Webinar 2. & 7. Dezember 2021



Unified Visibility. Built By Tenable Research.

Create new scans in seconds and get actionable results in minutes with Tenable.io Web App Scanning
Take advantage of web application security built by the largest vulnerability research team in the industry.




Web Application Scanning

WAS Statistics

VULNERABILITIES	SEVERITY	ASSETS	NEWLY DISCOVERED
194	3 Critical 18 High	5	0 (Last 7 Days) 0 (Last 30 Days)

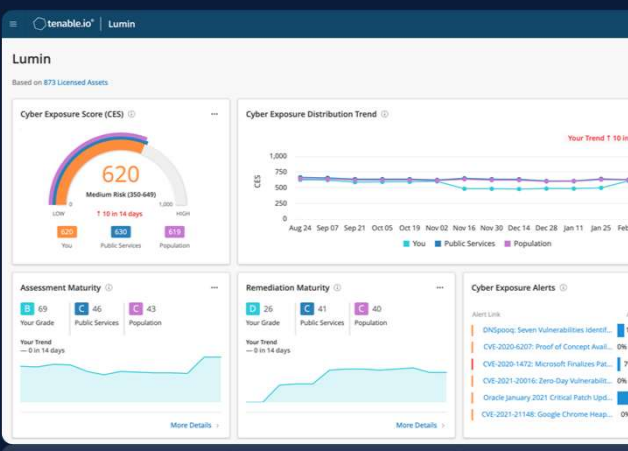
Top 2017 OWASP Categories

Category	Count
A1 - Injection	~35
A2 - Broken Authentication	~25
A3 - Sensitive Data Exposure	~20
A4 - XML External Entities (XXE)	~15
A5 - Broken Access Control	~10
A6 - Security Misconfiguration	~85
A7 - Cross-Site Scripting (XSS)	~35



**How secure is the business?
Meet your Cyber Exposure Score**

For the first time ever, you can visualize and explore your Cyber Exposure, track risk reduction over time, and benchmark against your peers.



Lumin

Based on 873 Licensed Assets

Cyber Exposure Score (CES)

620
Medium Risk (300-649)

Trend: ↑ 10 in 14 days

Comparison: You (620), Public Services (630), Population (617)

Cyber Exposure Distribution Trend

Line chart showing CES over time from Aug 24 to Feb 1. Your trend is highlighted in red, showing an increase from ~750 to ~1000.

Assessment Maturity

Your Grade: 69
Public Services: 46
Population: 43

Trend: ↑ 6 in 14 days

Remediation Maturity

Your Grade: 26
Public Services: 41
Population: 40

Trend: ↑ 8 in 14 days

Cyber Exposure Alerts

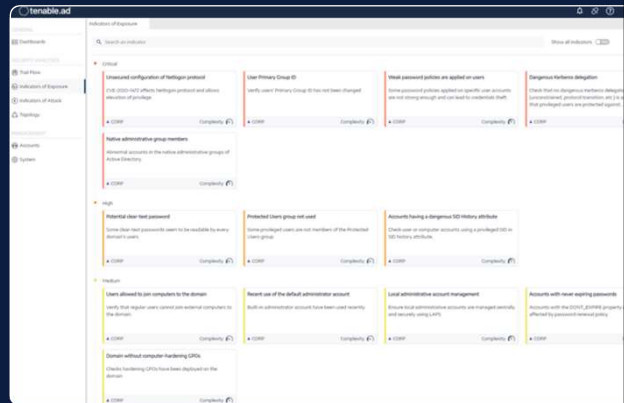
- DNSSpoof: Seven Vulnerabilities Identif... 0%
- CVE-2020-6207: Proof of Concept Avail... 0%
- CVE-2020-1472: Microsoft Finalizes Pat... 7%
- CVE-2021-20016: Zero-Day Vulnerabilit... 0%
- Oracle January 2021 Critical Patch Upd... 0%
- CVE-2021-21148: Google Chrome Hea... 0%

Vulnerability Management Webinar 2. & 7. Dezember 2021



**No Privilege Escalation.
No Lateral Movement.
No Next Step.**

By combining Risk-based Vulnerability Management and Active Directory Security, Tenable enables you to disrupt the attack path, ensuring attackers struggle to find a foothold and have no next step if they do.



**Secure Infrastructure as Code for
Flawless Clouds**

We are witnessing the rise of the Infrastructure as Code (IaC) movement, and to support this movement, cybersecurity needs to innovate with Security as Code.

Assess Infrastructure as Code before deployment and identify drift at runtime to secure the cloud at the speed of code.

