AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Erfolgreiches Vulnerability Management in der Praxis

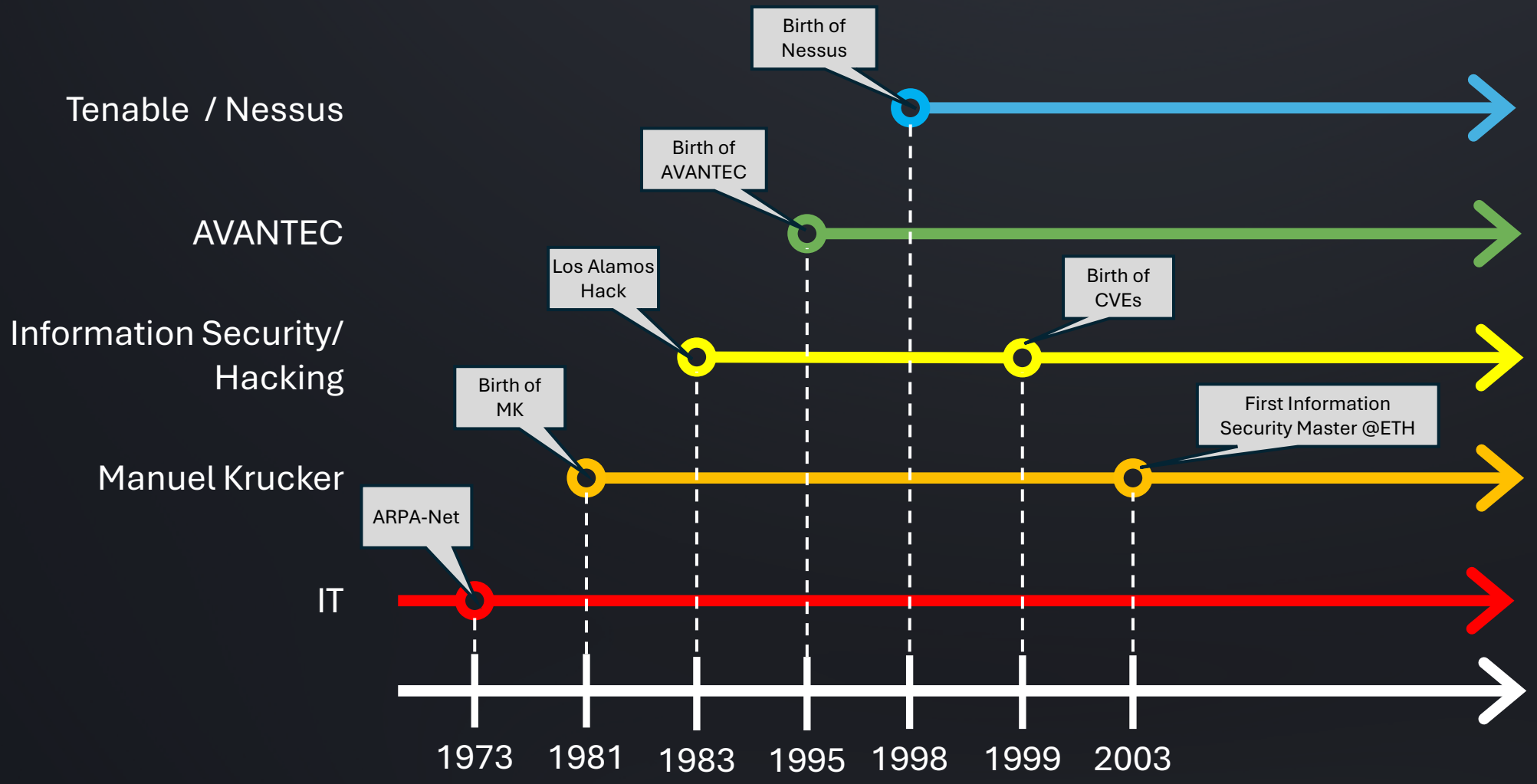
Manuel Krucker
Manuel Krucker, Cyber Defense Specialist,
SME Vulnerability Management

Agenda

1. Einführung
2. Herausforderungen VM
3. AVANTEC Ansatz
4. Zusammenfassung
5. Diskussion

Einführung

Funny Facts

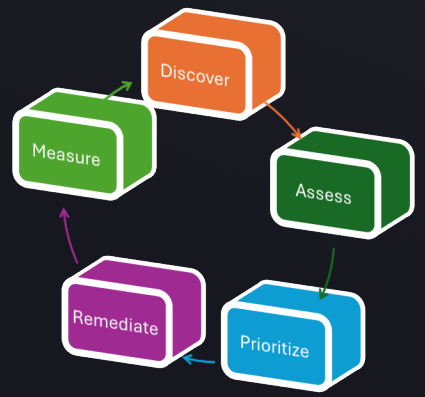


Einführung

Hintergrund Vulnerability Management?

Was ist Vulnerability Management?

ISO 27002 Control «Information about technical vulnerabilities of information systems in use **should be obtained**, the organization's **exposure** to such vulnerabilities should be **evaluated** and **appropriate measures should be taken**. »

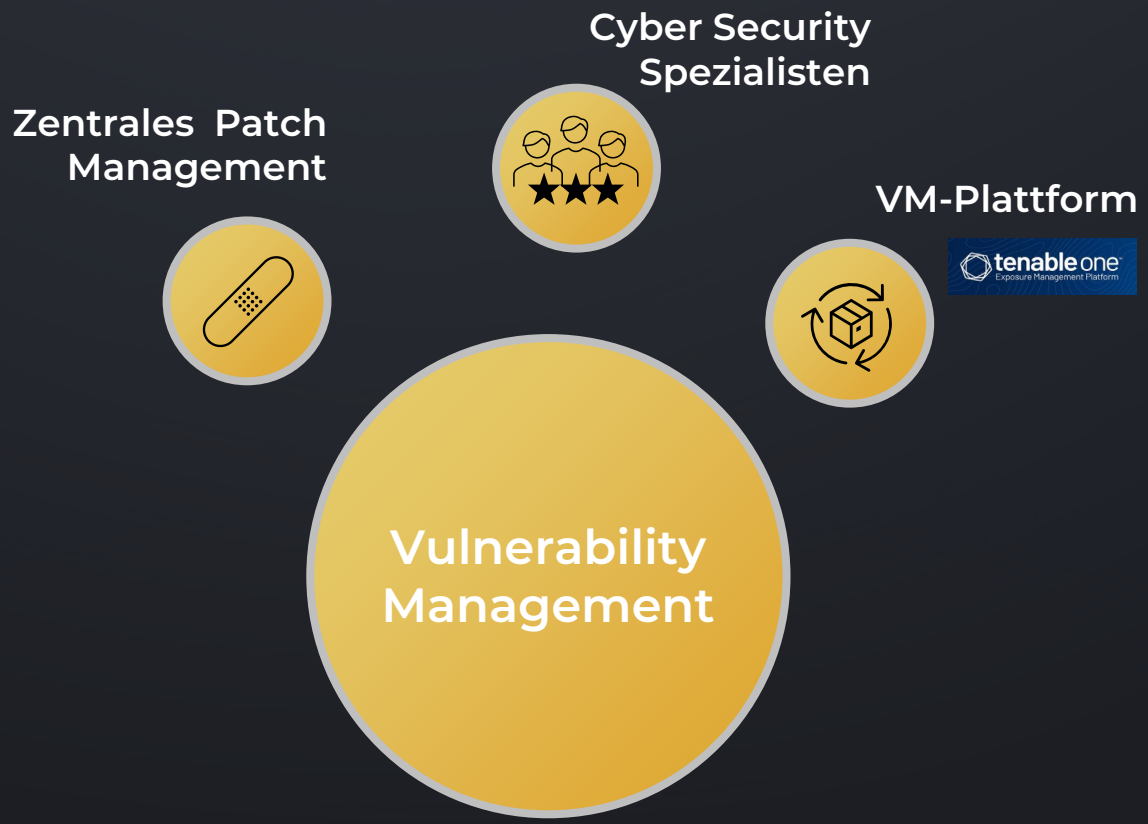


Warum Vulnerability Management?

- ISO 27002 : To prevent exploitation of technical vulnerabilities
- Angriffsfläche ist riesig. Das macht es unmöglich, jede Schwachstelle zu patchen und zu beheben.
- VM schafft einen wiederholbaren, messbaren Prozess, der sich an die Entwicklung der Bedrohungen anpasst.
- VM-Prozess wichtiges Instrument für Controlling der Security Posture – Aktive Anstossung von Security Prozessen
- Compliance verlangt einen Prozess, um die damit einhergehenden Risiken zu reduzieren

Herausforderungen

- Tenable identifiziert tausende von ‘Critical’ und ‘High’ Schwachstellen
- Gewisse Schwachstellen sind schwierig zu beurteilen, z.B. Log4j auf Clients
- Viele Schwachstellen betreffen ähnliche oder gleiche Massnahmen (z.B. Google Chrome) – keine Mehrfachtickets erwünscht (Resignation)
- Die gleichen Schwachstellen betreffen zum Teil verschieden Teams / IT-Dienstleister
- Gewisse Schwachstellen können oder sollen nicht gefixt werden, entsprechende Risiken sollen aber aufgenommen werden
- Kontrolle der täglichen Scans aufwendig
- Bei Reports zeigen nicht die relevanten Informationen
- Etc.



Feature ‘Priorisierung der Findings’

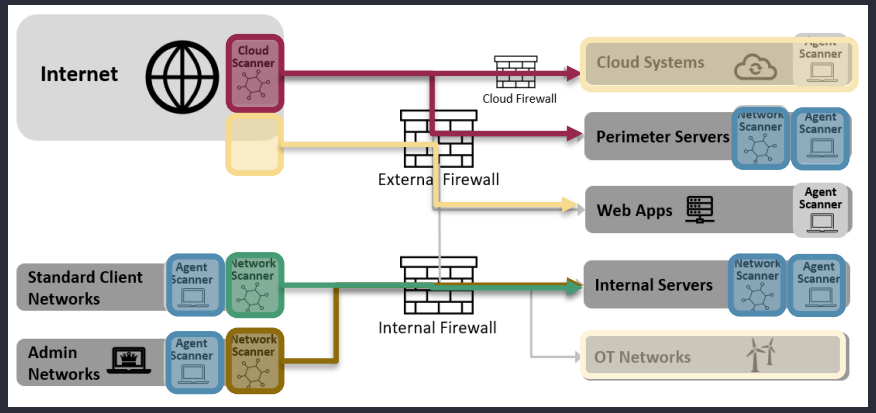
Challenge

Tenable hat tausende von ‘Critical’ und ‘High’ Vulnerabilities

Lösung / Implementierung

- Scans bilden verschiedene Exposure Levels ab
- Exposure Level werden von Severity subtrahiert
- Es gibt Ausnahmen bei hoher Exploitability
- Neu-bewertete Findings in AVANTEC Datenbank
- Alerts/Tickets durch Risiko-basierte AVANTEC Bewertung
- Transparent im Report dokumentiert

Output / Resultat



AVANTEC Competence. Security. Trust.	Critical	High	Medium	Low
	0	0	12,839	49,915

tenable	Tenable Critical	Tenable High	Tenable Medium	Tenable Low
	10,086	22,683	19,644	3,632

Feature ‘Gruppierung der Findings’

AVANTEC
Competence. Security. Trust.

Challenge

Nun haben wir zwar nur noch wenige ‘Critical’ und ‘High’ Risiko-basierte Findings, aber immer noch tausend ‘Medium’ Risiko-basierte Findings

Lösung / Implementierung

- Die Findings müssen sinnvoll gruppiert werden, z.B.
  - Nur 1 Ticket für Google Chrome
  - Nur 1 Ticket für Windows OS Updates
- Implementierung einer AVANTEC eigene *FindingGroup*
- Zusammenfassen von Findings

Output / Resultat

Info	Instances	Findings Top5	Assets Top5	OS Top5
Finding Group: Microsoft Edge First Seen: 2026-03-05	56 Findings 9 Plugins 32 Assets	Microsoft Edge (Chromium) < 146.0.3856.97 Multiple Vulnerabilities (5x) Microsoft Edge (Chromium) < 146.0.3856.84 Multiple Vulnerabilities (3x) Microsoft Edge (Chromium) < 147.0.3912.60 Multiple Vulnerabilities (6x) Microsoft Edge (Chromium) < 146.0.3856.72 Multiple Vulnerabilities (3x) Microsoft Edge (Chromium) < 147.0.3912.86 Multiple Vulnerabilities (32x)	[redacted] (5x) [redacted] (8x) [redacted] (3x) [redacted] (9x) [redacted] (3x)	Microsoft Windows 11 Pro (4x) Microsoft Windows 11 Busi (5x) Microsoft Windows 11 Pro (47x)

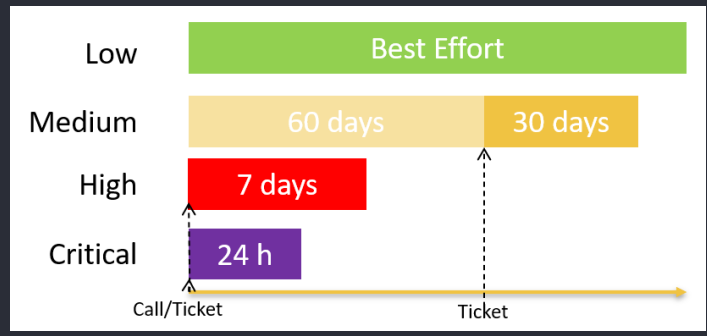
Feature ‘Verzögerung der Tickets’

AVANTEC
Competence. Security. Trust.

Challenge

Viele Medium Schwachstellen werden automatisch aktualisiert (z.B. Chrome, Windows Updates), hier möchte man keine Tickets.

Output / Resultat



Lösung / Implementierung

- ‘Medium’ Schwachstellen werden verzögert in der Hoffnung, dass es kein Ticket braucht
- Spätestens nach 60 Tage wird Ticket erstellt
- Ticket beinhaltet aber nur Findings älter als 40 Tage
- SOAR überprüft täglich Findings und löst Tickets aus

Feature ‘Ticket Erstellung’

AVANTEC
Competence. Security. Trust.

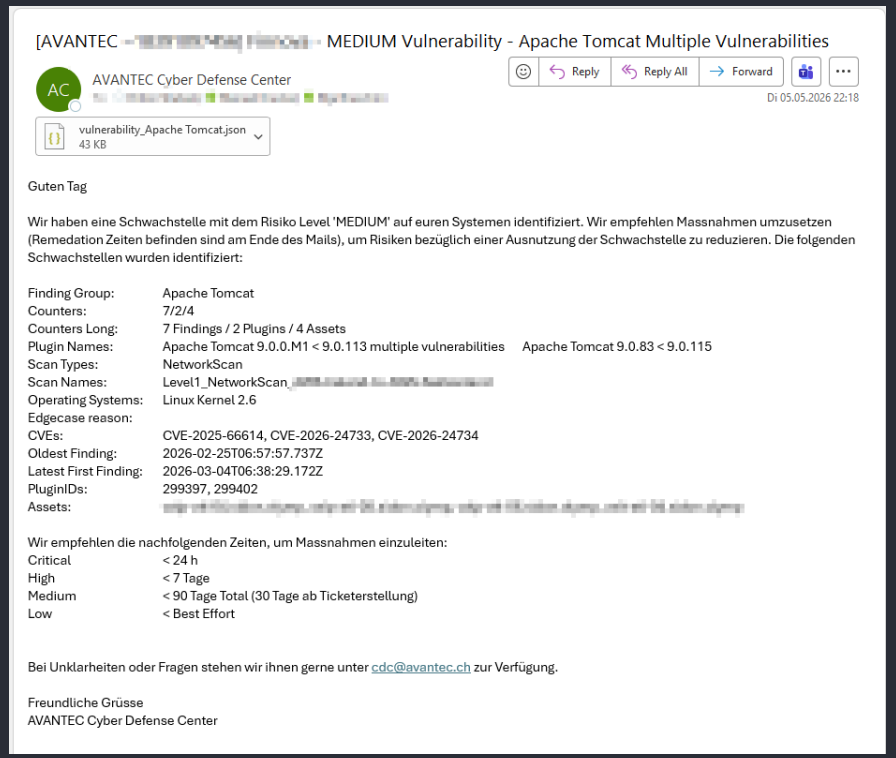
Challenge

Jeder Kunde hat verschiedene IT-Abteilungen, die für Behebung zuständig sind. Zudem möchten Kunden mit dem entsprechenden Ticket Workflows/Validierungen starten.

Lösung / Implementierung

- Ticket wird auf Verantwortliche gesplittet (z.B. Workstations Win/MacOS, Server, Others)
- Ticket Kurzversion – Details im Anhang
- Anhang für kunden-interne Automatisierung
- Anhangformat wählbar (json, csv, etc.)

Output / Resultat



[AVANTEC [redacted] MEDIUM Vulnerability - Apache Tomcat Multiple Vulnerabilities

AC AVANTEC Cyber Defense Center [redacted]

Reply | Reply All | Forward

Di 05.05.2026 22:18

vulnerability_Apache Tomcat.json
43 KB

Guten Tag

Wir haben eine Schwachstelle mit dem Risiko Level 'MEDIUM' auf euren Systemen identifiziert. Wir empfehlen Massnahmen umzusetzen (Remedation Zeiten befinden sind am Ende des Mails), um Risiken bezüglich einer Ausnutzung der Schwachstelle zu reduzieren. Die folgenden Schwachstellen wurden identifiziert:

Finding Group:	Apache Tomcat
Counters:	7/2/4
Counters Long:	7 Findings / 2 Plugins / 4 Assets
Plugin Names:	Apache Tomcat 9.0.0.M1 < 9.0.113 multiple vulnerabilities Apache Tomcat 9.0.83 < 9.0.115
Scan Types:	NetworkScan
Scan Names:	Level1_NetworkScan [redacted]
Operating Systems:	Linux Kernel 2.6
Edgecase reason:	
CVEs:	CVE-2025-66614, CVE-2026-24733, CVE-2026-24734
Oldest Finding:	2026-02-25T06:57:57.737Z
Latest First Finding:	2026-03-04T06:38:29.172Z
PluginIDs:	299397, 299402
Assets:	[redacted]

Wir empfehlen die nachfolgenden Zeiten, um Massnahmen einzuleiten:

Critical	< 24 h
High	< 7 Tage
Medium	< 90 Tage Total (30 Tage ab Ticketerstellung)
Low	< Best Effort

Bei Unklarheiten oder Fragen stehen wir ihnen gerne unter cdc@avantec.ch zur Verfügung.

Freundliche Grüsse
AVANTEC Cyber Defense Center

Feature ‘Scoping’

AVANTEC
Competence. Security. Trust.

Challenge

Es ist wichtig, dass alle relevanten Assets möglichst komplett auf Schwachstellen überprüft werden.

Lösung / Implementierung

- Initialer Onboarding Workshop
- Fahrplan für die Scans
- Host Discovery Scans zur Kontrolle des Scopes
- Automatische Überprüfung ‘Unmanaged Assets’
- Filterung von ähnlichen Assets bei Lizenz-Beschränkungen
- Transparente Ausweisung des Scopes

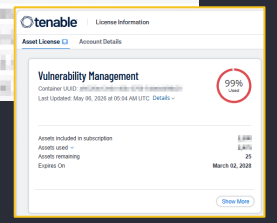
Output / Resultat

Scans

NAME	SCHEDULE	LAST RUN ↓	STATUS
Level0_NetworkScan_Perimeter-InternetBreakouts Shared	Daily at 1:30 AM	05/06/2026	Completed
Level0_NetworkScan_Perimeter-DataCentre Shared	Daily at 12:30 AM	05/06/2026	Completed
Level2_AgentScan_Windows-Clients-Standard Shared	Every week on Tuesday, Thursday at 8:0...	05/05/2026	Completed
Level2_NetworkScan_	Every week on Sunday at 2:00 PM	05/03/2026	Completed
Level2_NetworkScan_	Every week on Sunday at 2:00 PM	05/03/2026	Completed
Level2_NetworkScan_	Every week on Sunday at 2:00 PM	05/03/2026	Completed
Level2_NetworkScan_	Every week on Sunday at 2:00 PM	05/03/2026	Completed
Level2_NetworkScan_	Every week on Sunday at 2:00 PM	05/03/2026	Completed
Level2_NetworkScan_	Every week on Sunday at 2:00 PM	05/03/2026	Completed

Exclusions

NAME ↑	TARGETS
#TCK - Telecom Provider Swisscom	
#TCK - Licensing Limitations - Firewalls Check Point GAiA	
#TCK - Licensing Limitations - Network Switches and Access Points	
#TCK - Licensing Limitations - Out of Scope Assets Excel List 26.03.2026	
#TCK - Licensing Limitations - Out of Scope Temporary	
#TCK - Datenbankverbindungsprobleme während des Schwachstellenscan	
Onboarding - Guest Networks	
Onboarding - MPLS Networks	
Onboarding - Non-route Networks	
Onboarding - Potential Sensitive Networks	
Onboarding - Printers	
Onboarding - Sensitive Networks	
Onboarding - VOIP Networks	



Feature ‘Remediation Playbook’

AVANTEC
Competence. Security. Trust.

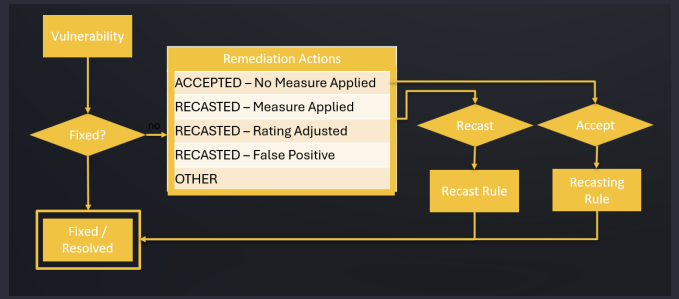
Challenge

Gewisse Schwachstellen können nicht gefixt werden. Sie werden akzeptiert oder es werden anderwärtige Massnahmen implementiert.

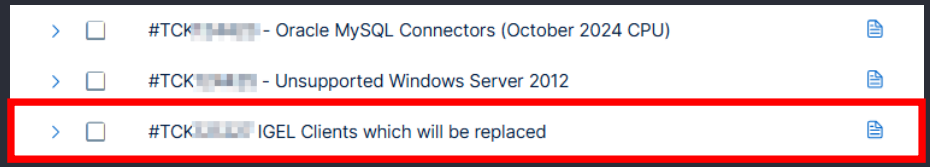
Lösung / Implementierung

- Ein standardisierte ‘Remediation Playbook’ wird verwendet
- Das Playbook ist reduziert auf das Minimum
- Customer Ticket / Security Case dokumentiert alle Ausnahmen
- Accept/Recast Rules in Tenable
- Monthly Report listet alles auf

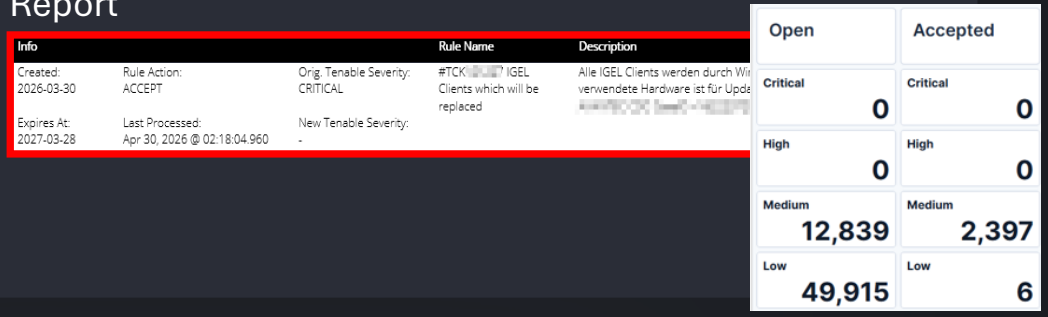
Output / Resultat



Tenable



Report



Features ‘Monthly Report’

- Monatlicher Bericht
- Dashboards für KPIs
- Tabellen mit allen Details

- Inhaltsverzeichnis
  1. Executive Summary
  2. Major Open Vulnerabilities
  3. Remediation Activities
  4. Operations
  5. Medium Vulnerabilities
  6. Low Vulnerabilities

Details Report

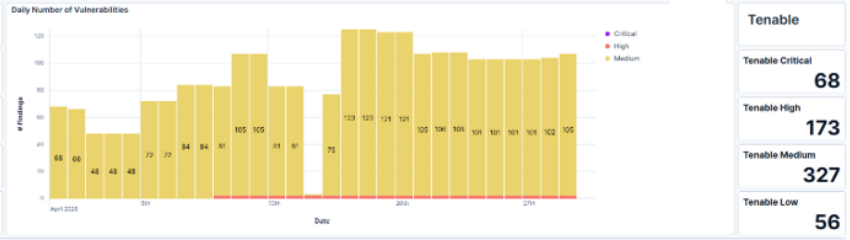
AVANTEC
Competence. Security. Trust.

2. Major Open Vulnerabilities

2.1 KPIs

Open		Accepted	
Critical	0	Critical	0
High	2	High	0
Medium	67	Medium	10
Low	449	Low	2

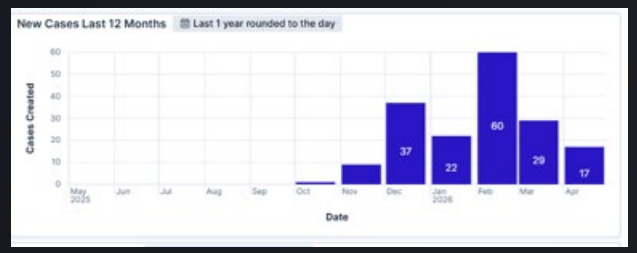
Tenable	
Tenable Critical	68
Tenable High	173
Tenable Medium	327
Tenable Low	56



4. Operations

4.1 KPIs

Executed Scans	Aborted Scans	Number of Scanners
264	3	1



Info	CaseID/Ticket	Titel	OS Top5	Assets Top5	Number of Findings	
Date: 20[redacted]	TicketID: [redacted]	ASP.NET Core Vulnerability - ASP.NET Core SEoL - 104 Endpoints affected	Microsoft Windows 11 Ente Microsoft Windows 11 Pro Microsoft Windows Server	[redacted]	open: fixed: accepted: recasted:	9 73 0 0
Days Open: 80	CaseID: ~16425345040	Scan Source: AGENT				
Date: 20[redacted]	TicketID: [redacted]	Microsoft Teams Vulnerability - Microsoft Teams < 1.6.0.18681 RCE - 102 Endpoints affected	Microsoft Windows 11 Ente Microsoft Windows 11 Pro	[redacted]	open: fixed: accepted: recasted:	83 0 0 0
Days Open: 80	CaseID: ~16425357328	Scan Source: AGENT				
Date: 20[redacted]	TicketID: [redacted]	Windows 10 Version 1607 / Windows Server 2016 Security Update Vulnerability - Multiple Vulnerabilities - 8 Endpoints affected	Microsoft Windows Server	[redacted]	open: fixed: accepted: recasted:	18 0 0 0
Days Open: 80	CaseID: ~16957677672	Scan Source: AGENT				

Weitere Features

AVANTEC
Competence. Security. Trust.

- Initial Baselining
- Mandanten-übergreifende False Positive Propagation
- Alarmierung bei ‘Failed Scans’
- Alarmierung bei ‘Unmanaged Assets running tenable sensor’
- Tägliche Aktualisierung der Tickets
- Etc.

Die meisten dieser Features sind mittels SOAR Workflows implementiert

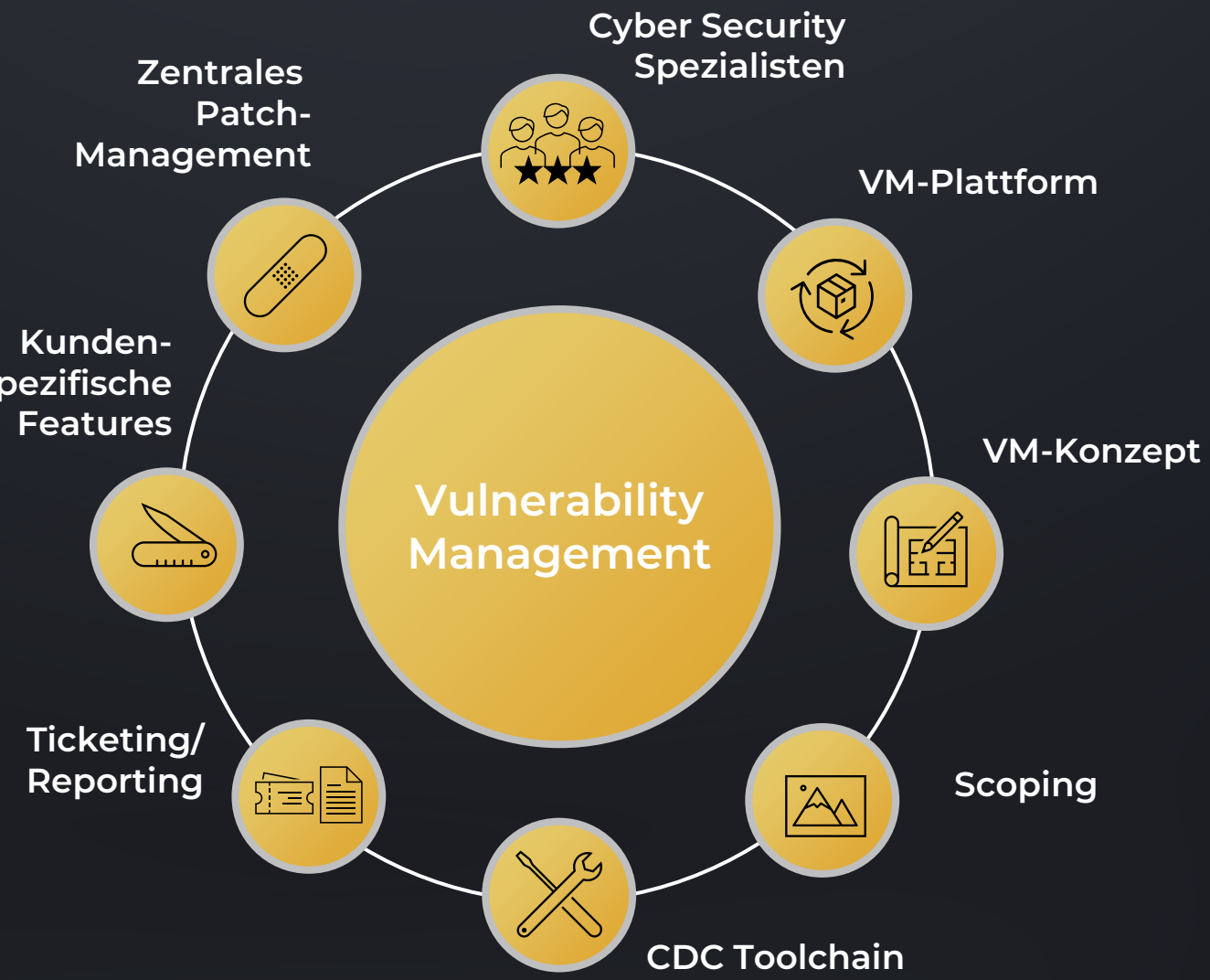
Antwort: Was braucht es für ein gutes VM?

AVANTEC
Competence. Security. Trust.

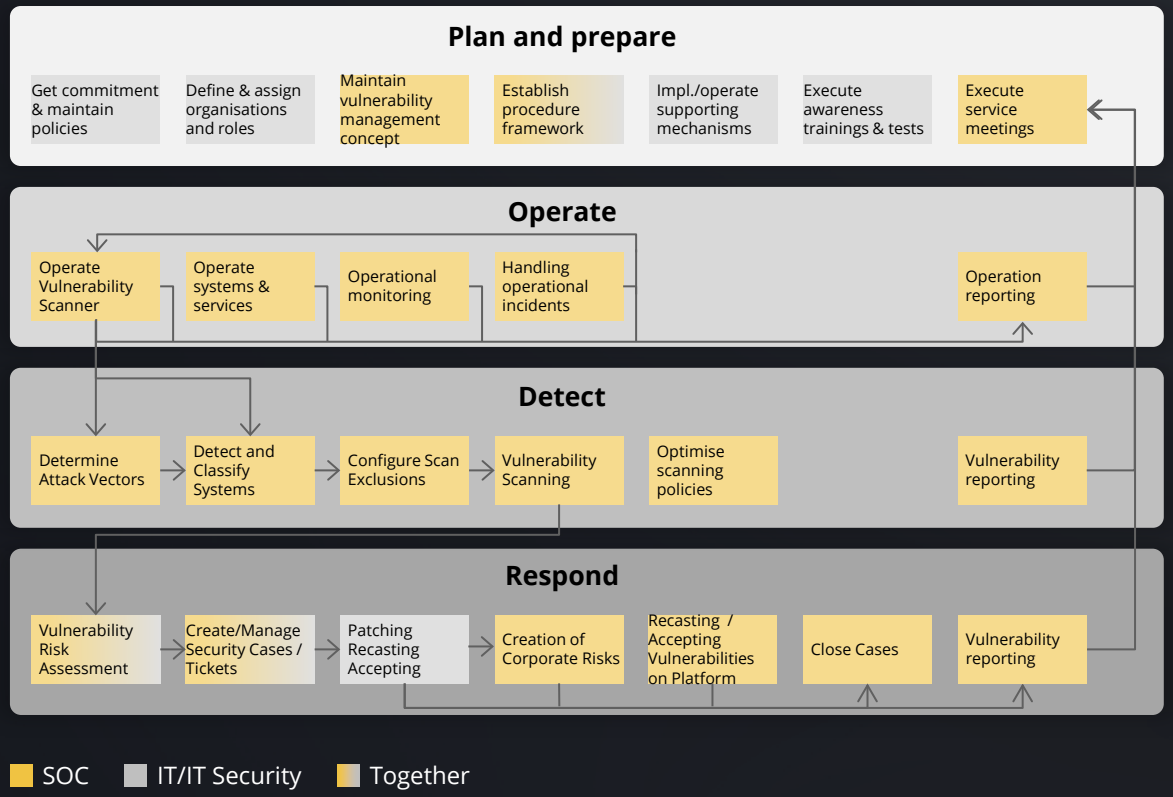
Antwort: Was braucht es für ein gutes VM?

AVANTEC
Competence. Security. Trust.

- Mit diesen Fähigkeiten sind wir in der Lage, sinnvolle Service Features zu implementieren
- Ein erster Schritt ist Lösungen für Herausforderungen zu entwickeln
- Danach werden manuelle Tätigkeiten Schritt für Schritt automatisiert
  - Repetitive Tätigkeiten werden identifiziert
  - Tätigkeiten werden spezifiziert
  - Tätigkeiten werden mittels CDC Toolchain automatisiert
- Aufwendige Automatisierung “lohnt” sich, da alle Mandanten profitieren



Vulnerability Management Process



High Level Process Specification

Plan and Prepare, e.g.:
- Get Commitment
- Assign Roles

Operate, e.g.:
- Operate Systems and Services

Detect, e.g.:
- Classify Systems
- Configure/Execute Scans

Respond, e.g.:
- Maintain Cases
- Fix / Accept / Recast
- Reporting

So sieht der Service aus

AVANTEC
Competence. Security. Trust.

AVANTEC

tenable one
Exposure Management Platform

Cloud Scanner

NS

AS

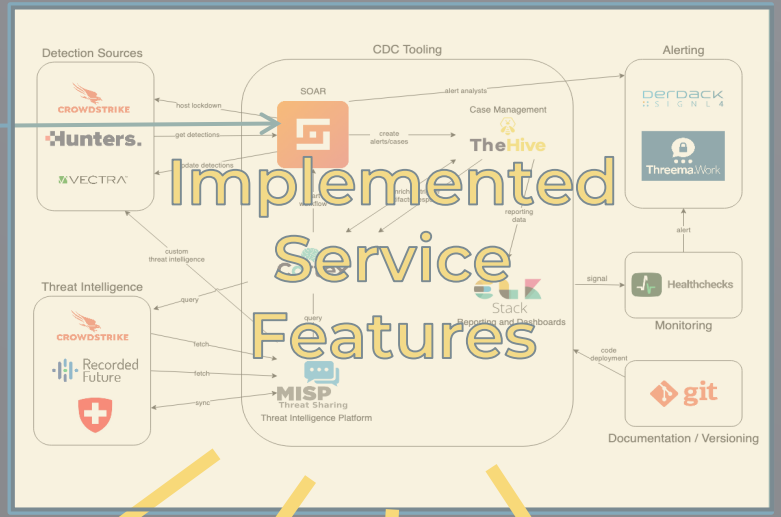
AS

AS

AS

AS

AS



Calls

Tickets

Reports

Meetings

Zusammenfassung

AVANTEC
Competence. Security. Trust.

Patchen (soviel wie nötig) &
Risiko Management

Effizienter Prozess
mit Führungsinstrumenten

Features

Fähigkeiten

- **Vulnerability Management** Schlüsselelement für effektive Cyber Security
- **Vulnerability Management** Produkte unterstützen, weisen aber auch Limitation auf und sind aufwendig im Betrieb
- Effizienter VM-Prozess benötigt Features & Knowhow von Vulnerability Profis
- Die Grundlage für Features sind umfangreiche Fähigkeiten
- Erfolgreicher VM-Prozess braucht Führungsinstrumente (Tickets, Report, Meetings)
- Kunden sollen sich auf das Patchen der relevanten Schwachstellen fokussieren – das ist immer noch sehr viel Arbeit

Danksagung

AVANTEC
Competence. Security. Trust.

- Partner
  - Tenable Plattform macht einen super Job
- Team: Wir haben ein tolles CDC-Team generell, aber auch für das Vulnerability Management
  - Tobias Balschun – Operativer Leiter Cyber Defence Center
  - Abdi Ciise & Eljia Bruschini - Vulnerability Management SME
  - Drilon Shabani – Implementierung Workflows im SOAR
  - Alle CDC-Mitglieder bringen Inputs für Vulnerability Management
  - Christian Grob – Co-CEO und Head of Security Service
- Last But not Least – oder das Salz in der Suppe – Unsere Kunden
  - Beide können voneinander profitieren und Zusammenarbeit ist ein Win-Win
  - Wir brauchen die Inputs / Anregungen / Wünsche von unseren Kunden

- Noch Fragen? Wir sind gerne für Sie da!

- Lass sie sich helfen beim Thema Vulnerability Management! Wir sind bereit!

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

DANKE

BeyondTrust · CHECK POINT · CROWDSTRIKE · digicert · netskope · THALES · tenable · xorlab · zscaler

AVANTEC
Competence. Security. Trust.

Nächste Session 13:00

Session 2

Was ist PAM mit Zero Standing Privileges (ZSP)? — Frei, 4. OG

Produkt: BeyondTrust
Referenten: Michael Scherzinger, Jessica Warland

Kontrolle und Schutz im Zeitalter von KI – Der Zscaler-Ansatz für GenAI Security — Odermatt, 4. OG

Produkt: zscaler
Referent: Jonas Kugler

Disaster Recovery im Cloud-Zeitalter — Lehmann Steingruber, 5. OG

Produkt: zscaler
Referent: Matthias Geiser

How to secure AI – Ein strategischer Überblick — Cancellara, 4. OG

Produkte: Diverse
Referent: Georg Hegyi

Tenable Cloud Security

AVANTEC
Competence. Security. Trust.

Major Features

- CIEM - Cloud Infrastructure Entitlement Management
  Identity and Access Management Risk Portion
- CSPM - Cloud Security Posture Management
  General measurement of security compliance and best practice configuration
- CWP - Cloud Workload Protection
  Checking the Workloads in the clouds for vulnerability and patch status

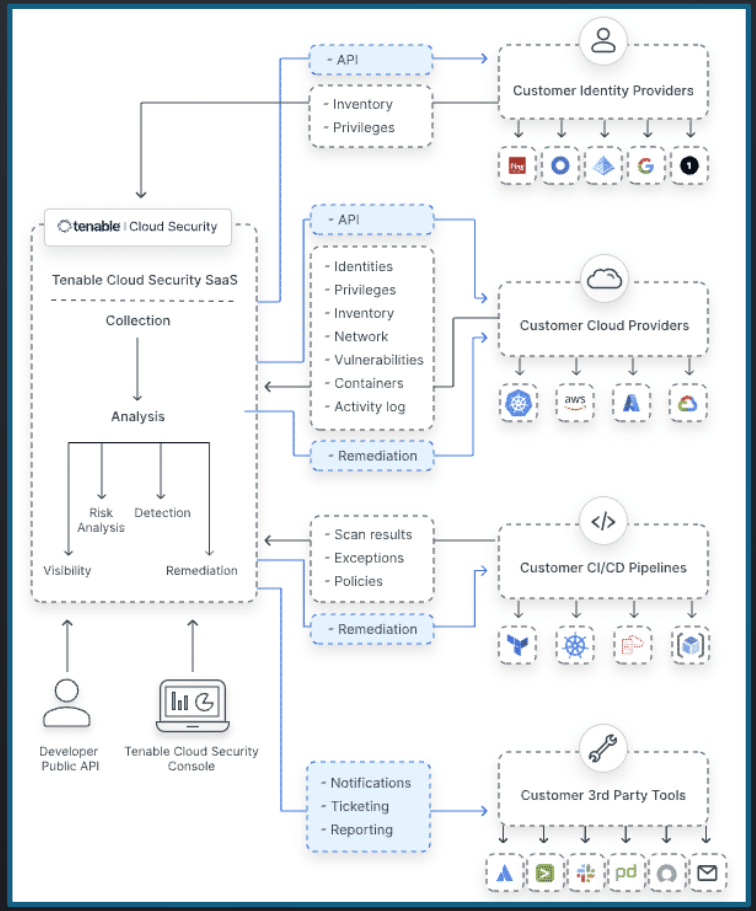
Minor Features

- IaC - Infrastructure as Code
  Identify risk in the code
- CDR - Cloud Detection and Response
  Look at behavior and logs in the cloud, forensic investigations
- KSPM - Kubernetics Posture Management
  Security in Containers, are they configured according best practices, what identities are configured

How Tenable does it

AVANTEC
Competence. Security. Trust.

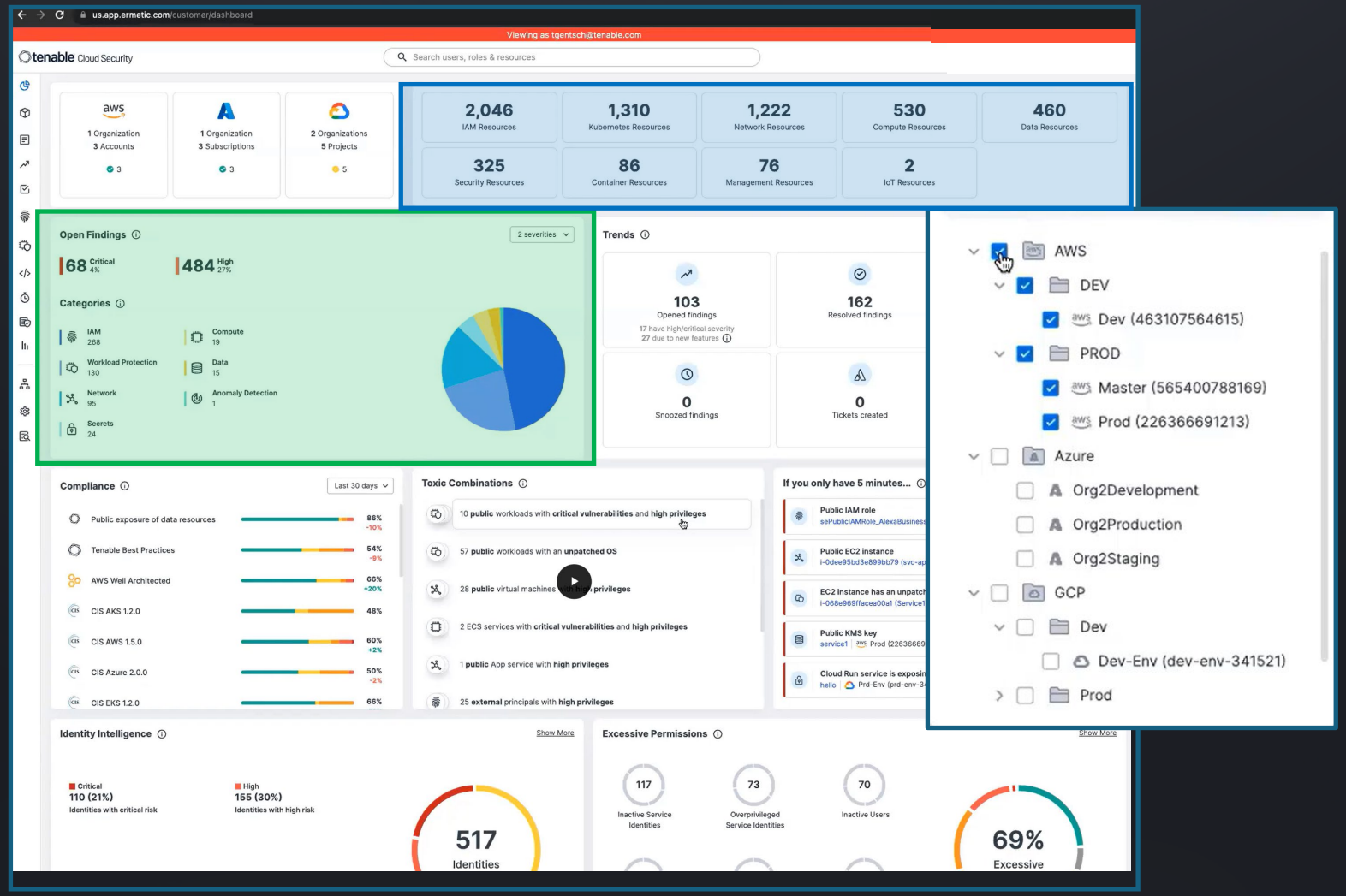
- Agentless, API-based SaaS solution
- Supports the leading Cloud Service Providers
- Deep interoperability with cloud-based Identity Providers (IdP)
- Integrates with popular DevOps, IT, and Security products
- Custom integrations with webhook and API
- Support infrastructure-as-Code (IaC) and CI/CD pipelines
- Natively integrates into organizational process



Demo Example: Cloud Dashboard

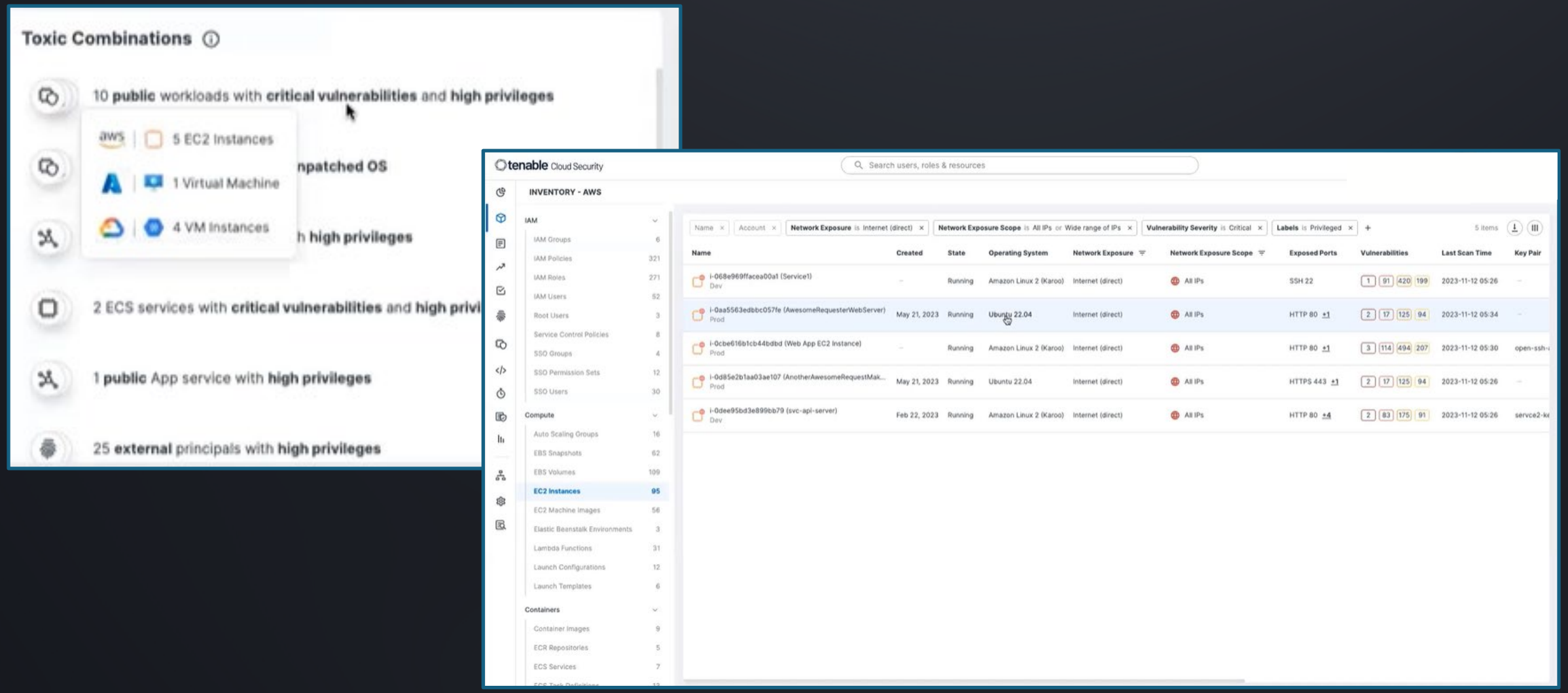
AVANTEC
Competence. Security. Trust.

- Cloud Provider
- Filter for subsections
- Navigation Bar
- Inventory Cloud Resources
  - IAM Resources
  - Compute Resources
  - Data Resources
  - Kubernetes Resources
  - ...
- Nice Widgets:
  - Open Findings
  - Trends
  - Compliance
  - Toxic Combinations



Demo Example: Toxic Combinations

AVANTEC
Competence. Security. Trust.



Demo Example: Outside Threats

AVANTEC
Competence. Security. Trust.