




Erfolgreiches Vulnerability Management in der Praxis

Manuel Krucker

Manuel Krucker, Cyber Defense Specialist,
SME Vulnerability Management

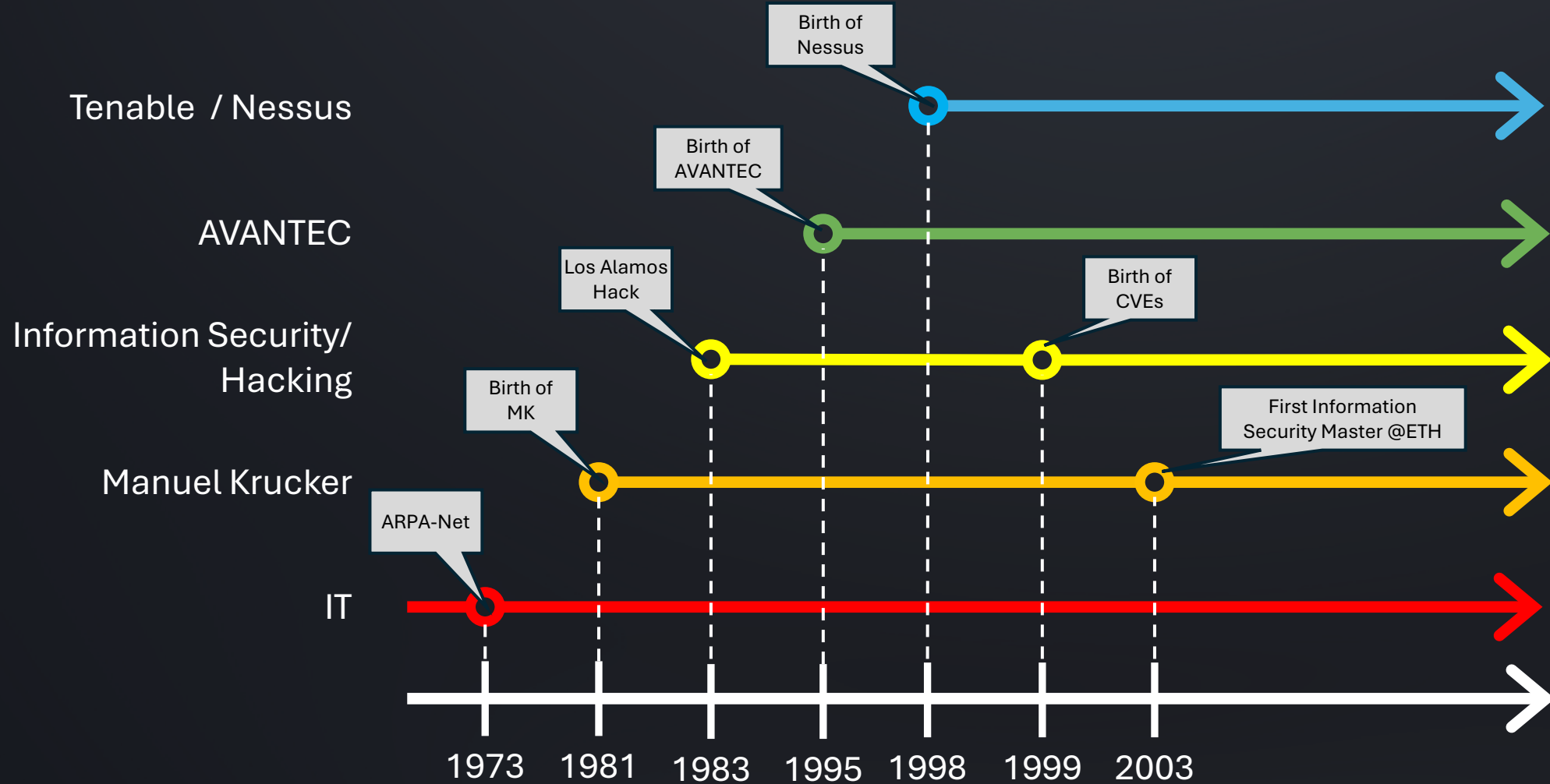


Agenda

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

Einführung

Funny Facts

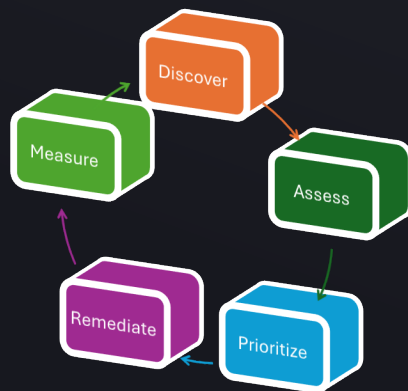


Einführung

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 verschiedenen 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

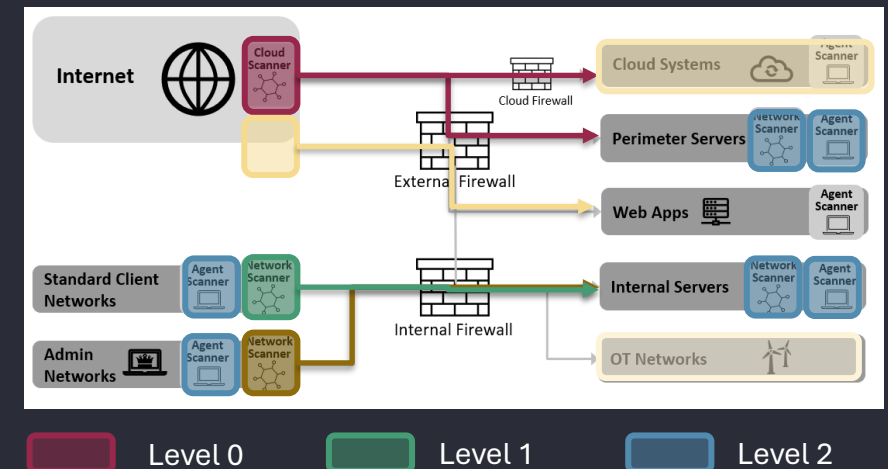


Lösung / Implementierung

- 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	Critical	High	Medium	Low
Competence. Security. Trust.	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'



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

Feature 'Verzögerung der Tickets'



Challenge

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

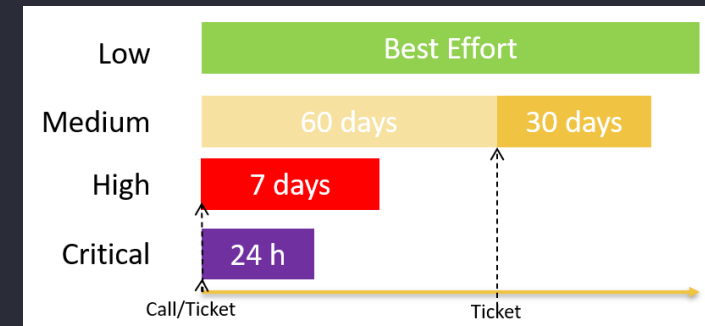


Lösung / Implementierung

- '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



Output / Resultat



Feature 'Ticket Erstellung'



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 - MEDIUM Vulnerability - Apache Tomcat Multiple Vulnerabilities]

AVANTEC Cyber Defense Center 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 (Remediation Zeiten befinden sich 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_...
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: ...

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'



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
<input type="checkbox"/> Level0_NetworkScan_Perimeter-InternetBreakouts Shared	Daily at 1:30 AM	05/06/2026	Completed
<input type="checkbox"/> Level0_NetworkScan_Perimeter-DataCentre Shared	Daily at 12:30 AM	05/06/2026	Completed
<input type="checkbox"/> Level2_AgentScan_Windows-Clients-Standard Shared	Every week on Tuesday, Thursday at 8:0...	05/05/2026	Completed
<input type="checkbox"/> Level2_NetworkScan_...	Every week on Sunday at 2:00 PM	05/03/2026	Completed
<input type="checkbox"/> Level2_NetworkScan_...	Every week on Sunday at 2:00 PM	05/03/2026	Completed
<input type="checkbox"/> Level2_NetworkScan_...	Every week on Sunday at 2:00 PM	05/03/2026	Completed
<input type="checkbox"/> Level2_NetworkScan_...	Every week on Sunday at 2:00 PM	05/03/2026	Completed
<input type="checkbox"/> Level2_NetworkScan_...	Every week on Sunday at 2:00 PM	05/03/2026	Completed
<input type="checkbox"/> Level2_NetworkScan_...	Every week on Sunday at 2:00 PM	05/03/2026	Completed
<input type="checkbox"/> Level2_NetworkScan_...	Every week on Sunday at 2:00 PM	05/03/2026	Completed

Exclusions

NAME ↑	TARGETS
#TCK1 - Telecom Provider Swisscom	
#TCK1 - Licensing Limitations - Firewalls Check Point GAIA	
#TCK1 - Licensing Limitations - Network Switches and Access Points	
#TCK1 - Licensing Limitations - Out of Scope Assets Excel List 26.03.2026	
#TCK1 - Licensing Limitations - Out of Scope Temporary	
#TCK1 - 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	

tenable License Information
Asset License Account Details

Vulnerability Management
Current Score: 99%
Last Update: May 06, 2025 at 09:44 UTC Details

Assets included in subscription	1,800
Assets scanned	1,400
Assets remaining	25
Expired On	March 03, 2025

[Show More](#)

Feature 'Remediation Playbook'



Challenge

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

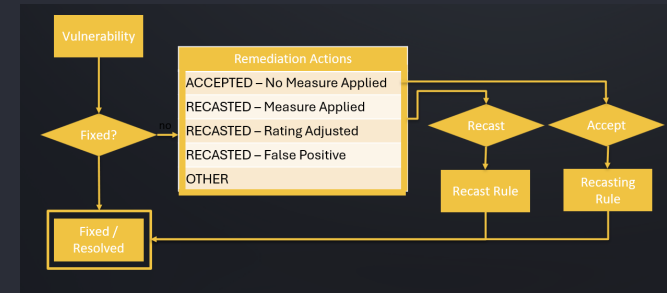


Lösung / Implementierung

- 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

>	<input type="checkbox"/>	#TCK[REDACTED] - Oracle MySQL Connectors (October 2024 CPU)	
>	<input type="checkbox"/>	#TCK[REDACTED] - Unsupported Windows Server 2012	
>	<input type="checkbox"/>	#TCK[REDACTED] IGEL Clients which will be replaced	

Report

Info	Rule Name	Description
Created: 2026-03-30	Rule Action: ACCEPT	Orig. Tenable Severity: CRITICAL
Expires At: 2027-03-28	Last Processed: Apr 30, 2026 @ 02:18:04.960	New Tenable Severity: -
	#TCK[REDACTED] IGEL Clients which will be replaced	Alle IGEL Clients werden durch Wi verwendete Hardware ist für Updat

	Open	Accepted
Critical	0	0
High	0	0
Medium	12,839	2,397
Low	49,915	6

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

AVANTEC
Competence. Security. Trust.

AVANTEC VMS Service – Monthly Report 2026.04

Table of Contents

1. Executive Summary.....	4
2. Major Open Vulnerabilities.....	5
2.1 KPIs.....	5
2.2 Critical Vulnerabilities Open.....	6
2.3 High Vulnerabilities Open.....	6
2.4 Medium Vulnerabilities Open.....	6
2.5 Accepted Findings.....	24
3. Remediation Activities.....	25
3.1 KPIs.....	25
3.2 Closed Cases.....	25
3.3 Recasting Rules.....	29
3.4 Remediation Alerts.....	32
4. Operations.....	33
4.1 KPIs.....	33
4.2 Operational Cases.....	34
4.3 Assets and Networks in Scope / Out of Scope.....	34
4.4 Scanners and Scans.....	34
5. Medium Vulnerabilities Open.....	45
5.1 KPIs.....	45
5.2 Medium Vulnerabilities Open - Aggregated.....	46
6. Low Vulnerabilities Open.....	56
6.1 KPIs.....	56
6.2 Low Vulnerabilities Open - Aggregated.....	57

Page 2/94

Risk

Compliance

Operations

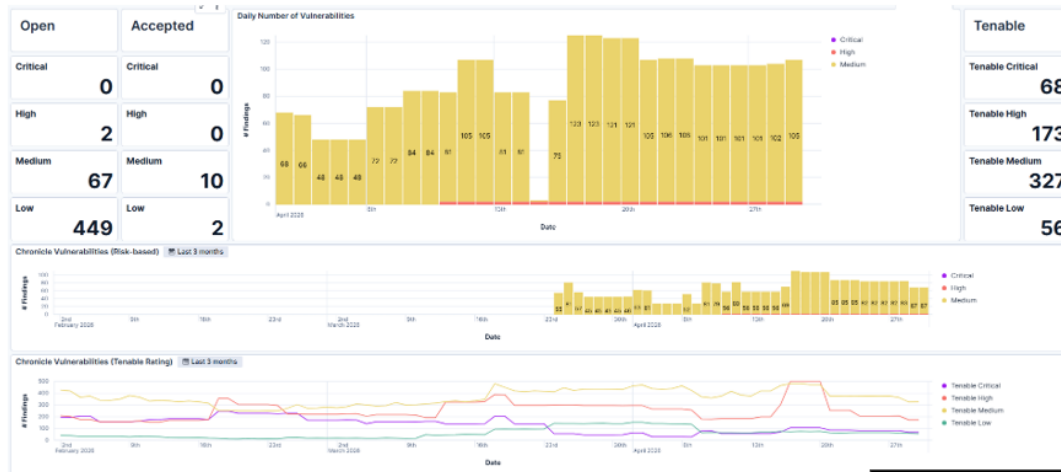
Completeness

Details Report

AVANTEC VMS Service – Monthly Report 2026.04

2. Major Open Vulnerabilities

2.1 KPIs



AVANTEC AG – Cyber Defense Center – Heinrichstrasse 267 – CH-8005 Zürich – Tel. 044 457 13 13 – cdc@avantec.ch



AVANTEC VMS Service – Monthly Report 2026.04

4. Operations

4.1 KPIs



AVANTEC AG – Cyber Defense Center – Heinrichstrasse 267 – CH-8005 Zürich – Tel. 044 457 13 13 – cdc@avantec.ch

Page 14/51

Info	CaseID/Ticket	Titel	OS Top5	Assets Top5	Number of Findings
Date: 2025-12-18	TicketID: 1642534504	ASP.NET Core Vulnerability - ASP.NET Core SEoL - 104 Endpoints affected	Microsoft Windows 11 Ente Microsoft Windows 11 Pro Microsoft Windows Server	192.168.1.101 192.168.1.102 192.168.1.103 192.168.1.104 192.168.1.105	open: 9 fixed: 73 accepted: 0 recasted: 0
Days Open: 80	CaseID: ~1642534504	Scan Source: AGENT			
Date: 2025-12-18	TicketID: 16425357328	Microsoft Teams Vulnerability - Microsoft Teams < 1.6.0.18681 RCE - 102 Endpoints affected	Microsoft Windows 11 Ente Microsoft Windows 11 Pro	192.168.1.101 192.168.1.102 192.168.1.103 192.168.1.104 192.168.1.105	open: 83 fixed: 0 accepted: 0 recasted: 0
Days Open: 80	CaseID: ~16425357328	Scan Source: AGENT			
Date: 2025-12-18	TicketID: 16957677672	Windows 10 Version 1607 / Windows Server 2016 Security Update Vulnerability - Multiple Vulnerabilities - 8 Endpoints affected	Microsoft Windows Server	192.168.1.101 192.168.1.102 192.168.1.103 192.168.1.104 192.168.1.105	open: 18 fixed: 0 accepted: 0 recasted: 0
Days Open: 80	CaseID: ~16957677672	Scan Source: AGENT			

Weitere Features

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

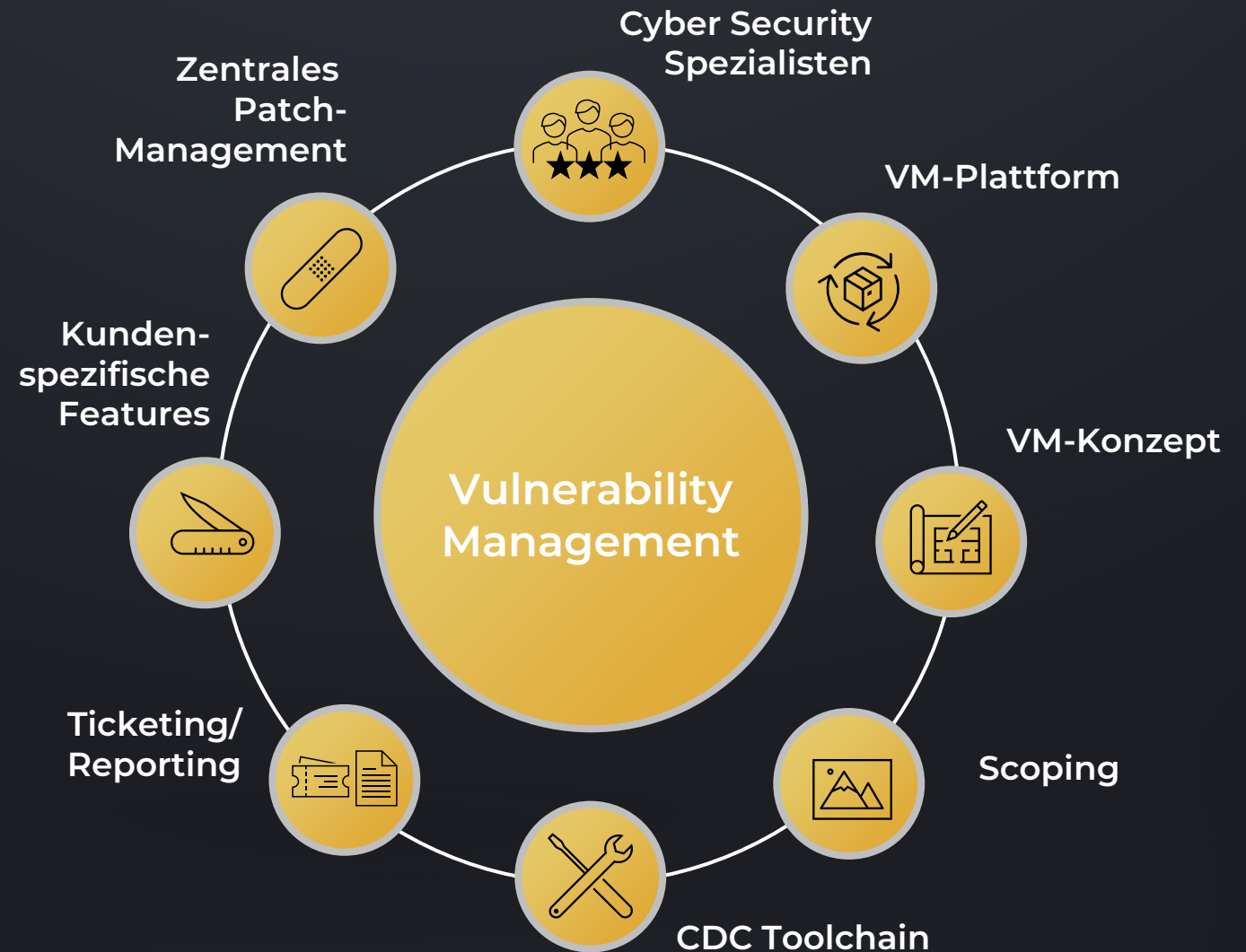
Die meisten dieser Features sind mittels SOAR Workflows implementiert

Antwort: Was braucht es für ein gutes VM?

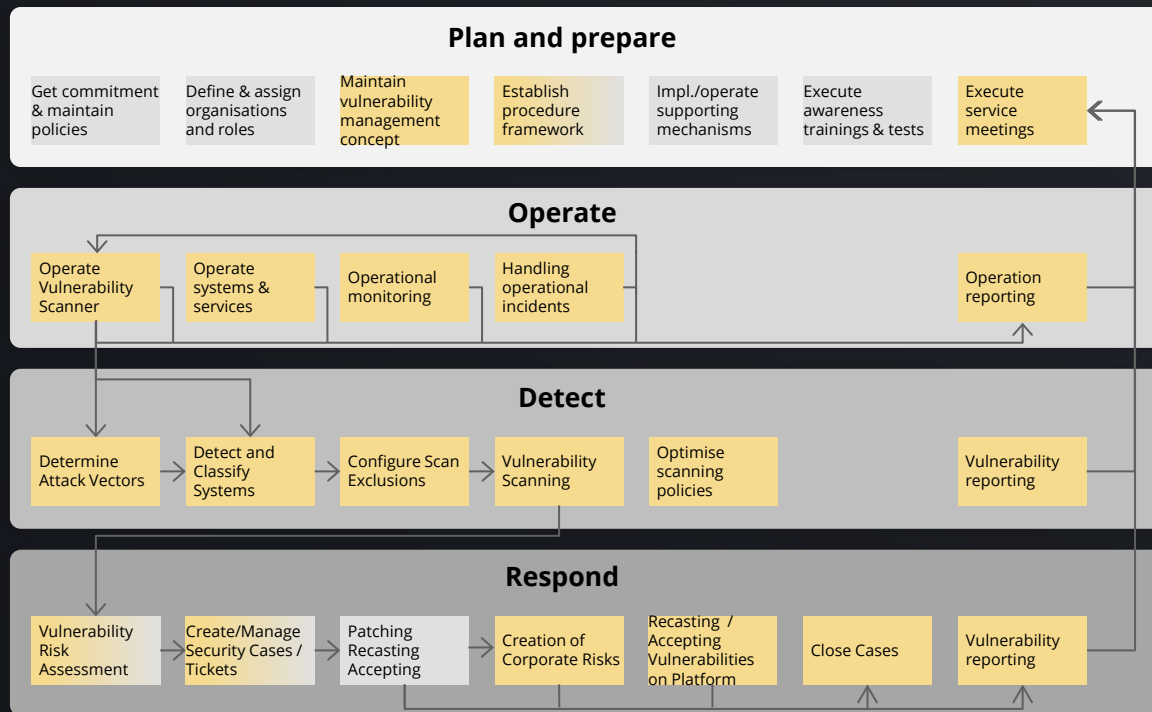


Antwort: Was braucht es für ein gutes VM?

- 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



■ SOC ■ IT/IT Security ■ Together

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.:

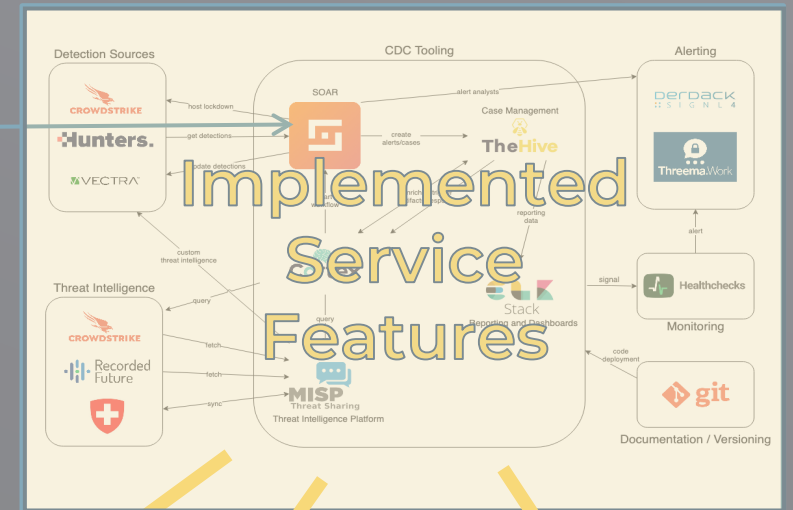
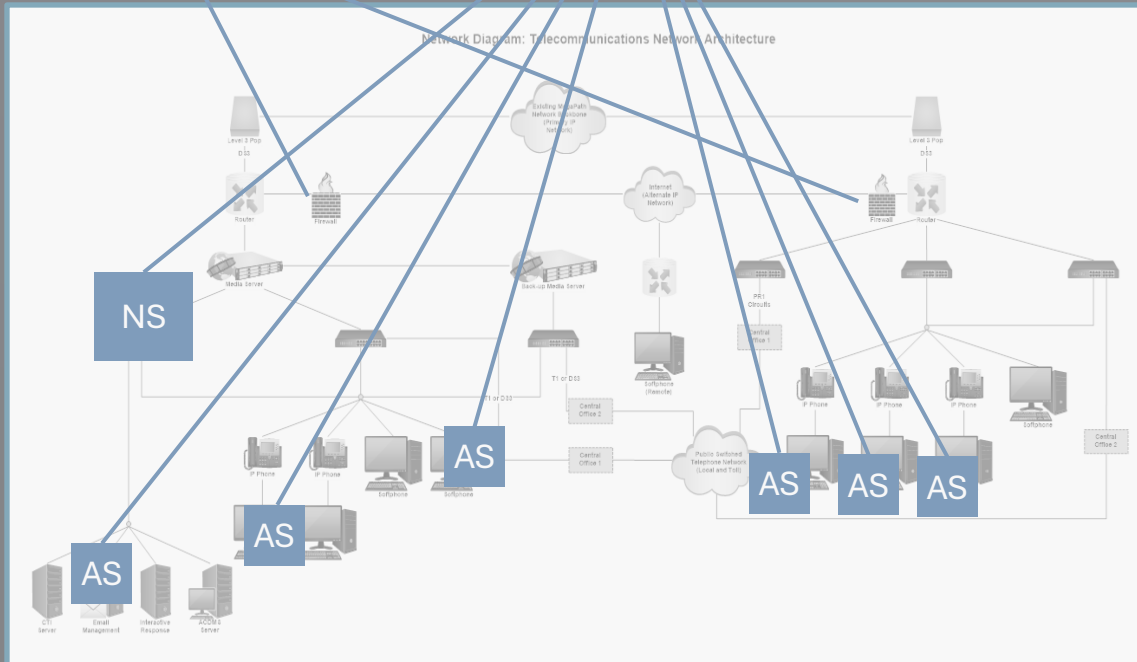
- Maintain Cases
- Fix / Accept / Recast
- Reporting

So sieht der Service aus

AVANTEC

tenable one™
Exposure Management Platform

Cloud Scanner



Calls



Tickets

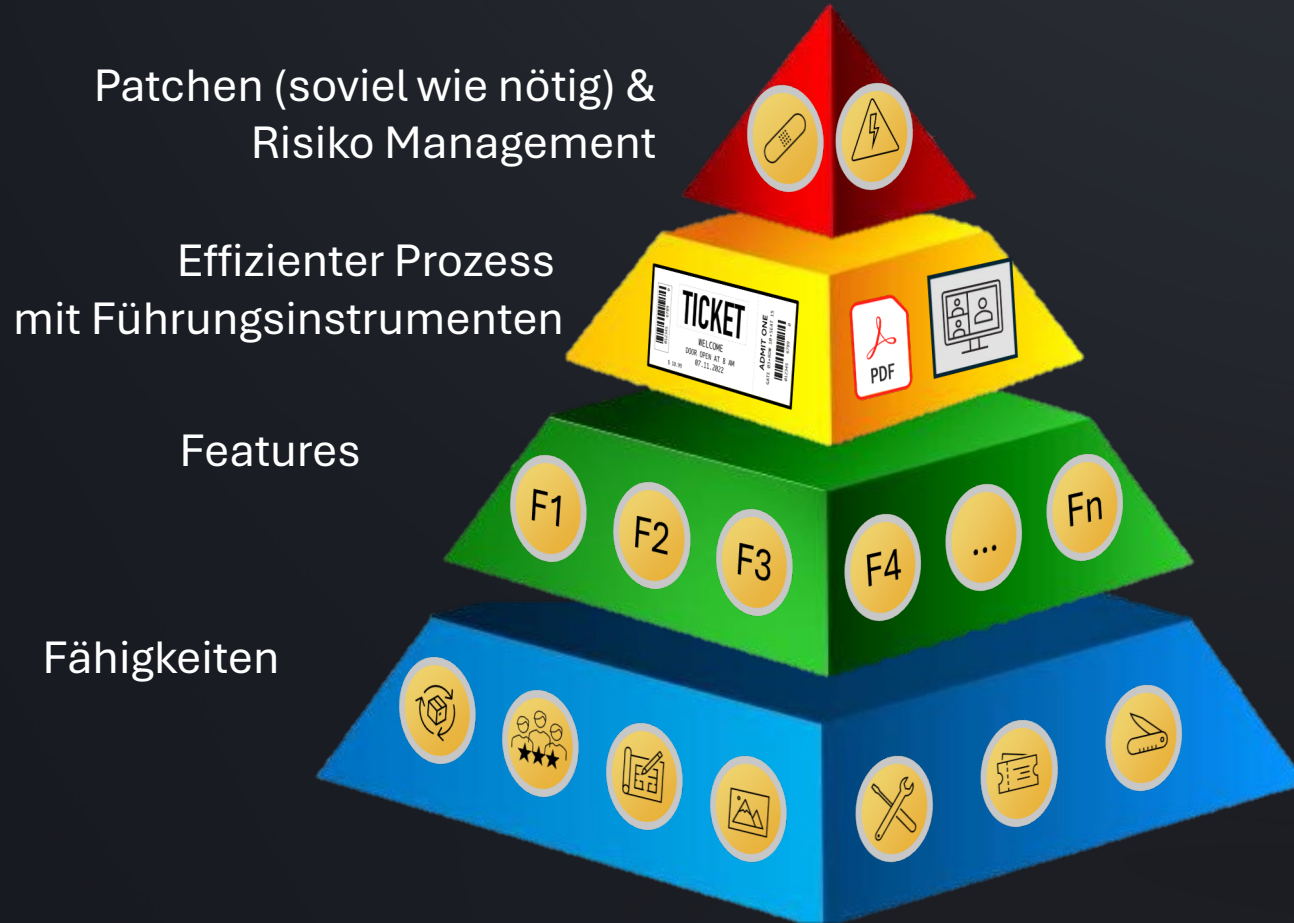


Reports



Meetings

Zusammenfassung



- Vulnerability Management
Schlüsselement 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

- 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



DANKKE



Nächste Session 13:00

Session 2

Was ist PAM mit Zero Standing Privileges (ZSP)?

Produkt:  BeyondTrust

Referenten: Michael Scherzinger, Jessica Warland

Frei, 4. OG

Kontrolle und Schutz im Zeitalter von KI – Der Zscaler-Ansatz für GenAI Security

Produkt:  zscaler

Referent: Jonas Kugler

Odermatt, 4. OG

Disaster Recovery im Cloud-Zeitalter

Produkt:  zscaler

Referent: Matthias Geiser

Lehmann Steingruber, 5. OG

How to secure AI – Ein strategischer Überblick

Produkte: Diverse

Referent: Georg Hegyi

Cancellara, 4. OG

Tenable Cloud Security

Major Features

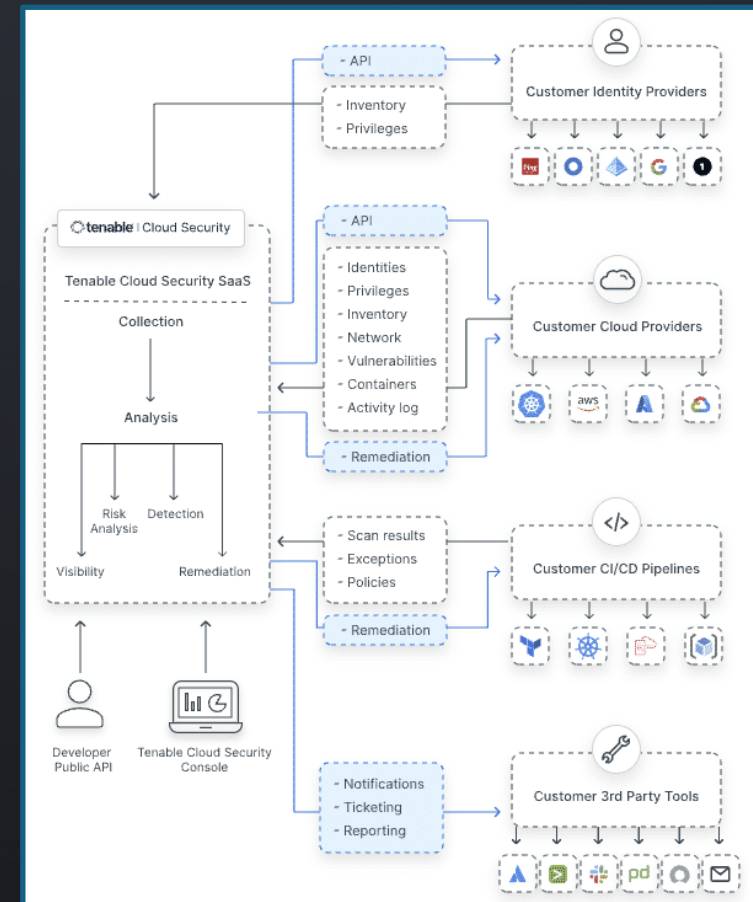
- **CIEM - Cloud Infrastructure Entitlement Management**
Identity and Access Management Risk Portion
- **CSPM - Cloud Security Posture Management**
General measurement of security compliance and best practice configuration
- **CWP - Cloud Workload Protection**
Checking the Workloads in the clouds for 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 - Kubernetes Posture Management**
Security in Containers, are they configured according best practices, what identities are configured

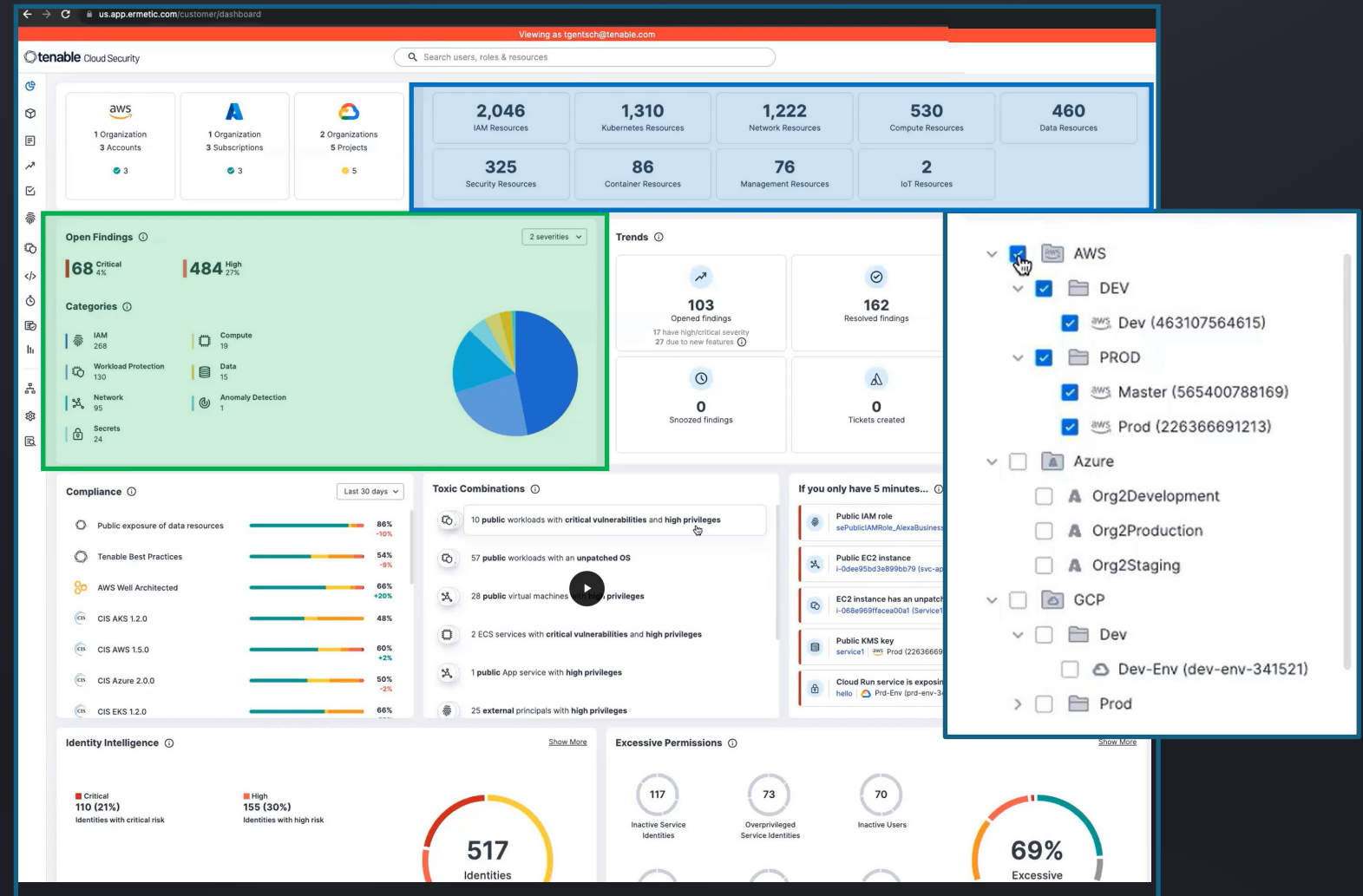
How Tenable does it

- 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

- 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

Toxic Combinations ⓘ

- 10 public workloads with critical vulnerabilities and high privileges
 - aws | 5 EC2 Instances
 - 1 Virtual Machine with unpatched OS
 - 4 VM Instances with high privileges
- 2 ECS services with critical vulnerabilities and high privileges
- 1 public App service with high privileges
- 25 external principals with high privileges

tenable Cloud Security

Search users, roles & resources

INVENTORY - AWS

Name	Account	Network Exposure	Network Exposure Scope	Vulnerability Severity	Labels	Privileged	Items		
Name	Created	State	Operating System	Network Exposure	Network Exposure Scope	Exposed Ports	Vulnerabilities	Last Scan Time	Key Pair
i-068e969ffacea00a1 (Service1) Dev	-	Running	Amazon Linux 2 (Karoo)	Internet (direct)	All IPs	SSH 22	1 91 420 199	2023-11-12 05:26	-
i-Qaa5563edbbc057fe (AwesomeRequesterWebServer) Prod	May 21, 2023	Running	Ubuntu 22.04	Internet (direct)	All IPs	HTTP 80 ±1	2 17 125 94	2023-11-12 05:34	-
i-0cbe616b1cb44bdbd (Web App EC2 Instance) Prod	-	Running	Amazon Linux 2 (Karoo)	Internet (direct)	All IPs	HTTP 80 ±1	3 114 494 207	2023-11-12 05:30	open-ssh-...
i-0d85e2b1aa03ae107 (AnotherAwesomeRequestMak... Prod	May 21, 2023	Running	Ubuntu 22.04	Internet (direct)	All IPs	HTTPS 443 ±1	2 17 125 94	2023-11-12 05:26	-
i-0dee95bd3e899bb79 (svc-api-server) Dev	Feb 22, 2023	Running	Amazon Linux 2 (Karoo)	Internet (direct)	All IPs	HTTP 80 ±4	2 83 175 91	2023-11-12 05:26	service2-ke...

- IAM
 - IAM Groups: 6
 - IAM Policies: 321
 - IAM Roles: 271
 - IAM Users: 52
 - Root Users: 3
 - Service Control Policies: 8
 - SSO Groups: 4
 - SSO Permission Sets: 12
 - SSO Users: 30
- Compute
 - Auto Scaling Groups: 16
 - EBS Snapshots: 62
 - EBS Volumes: 109
 - EC2 Instances: 95**
 - EC2 Machine Images: 56
 - Elastic Beanstalk Environments: 3
 - Lambda Functions: 31
 - Launch Configurations: 12
 - Launch Templates: 6
- Containers
 - Container Images: 9
 - ECR Repositories: 5
 - ECS Services: 7

Demo Example: Outside Threats

Viewing as tgentsch@tenable.com

tenable Cloud Security

IDENTITY INTELLIGENCE

517 Identities 21% Critical

36 Federated Identities 11% Critical

355 Service Identities 19% Critical

162 Users 27% Critical

41 3rd Party Identities 3rd 20% Critical

Name x Originator Type x Risk x Categories x Labels x + 517 Items

Cloud	Name	Originators	Last Activity	Risk	Permissions			Findings	Labels
					Categories	Services	Resources		
aws	FindingsFixer IAM User Prod	-	Jan 28, 2021	High	PE PM DA IM R	365	2.2K	4	Admin Inactive No MFA
aws	Users IAM Role Prod	JohnnyMcFly IAM User Dev	Nov 10, 2023	High	PE PM DA IM R	365	2.2K	5	Admin Anomaly Excess Access Keys
aws	CICDUser IAM User Prod	-	Nov 13, 2023	High	PE PM DA IM R	365	2.2K	3	Ad... Access Ke... Excessi...
aws	danecs IAM User Prod	-	Feb 4, 2023	High	PE PM DA IM R	365	2.2K	3	Admin Inactive Access Keys
aws	DarrenBerg IAM User Prod	-	Never	High	PE PM DA IM R	365	2.2K	3	Admin Inactive No MFA
aws	dorBUser IAM User Prod	-	Oct 21, 2021	High	PE PM DA IM R	365	2.2K	2	Admin Inactive Access Keys