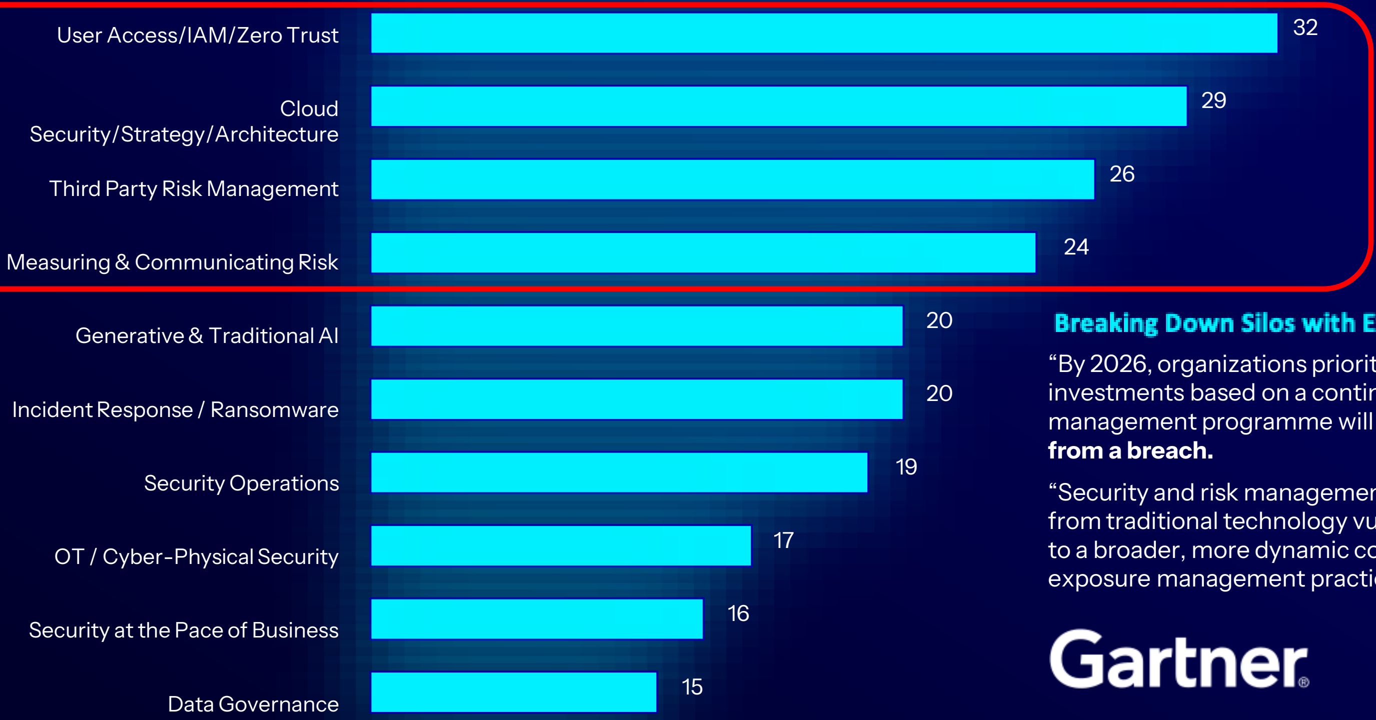
# People don’t hack in: They log in with your credentials

## Embracing Identity Security: The Key to Zero Trust and Continuous Threat Exposure Management

Novan Tambunan
Security Engineer

# 2024 top 10 CISO priorities



Source: Evanta - A Gartner Company

### Breaking Down Silos with Exposure Management

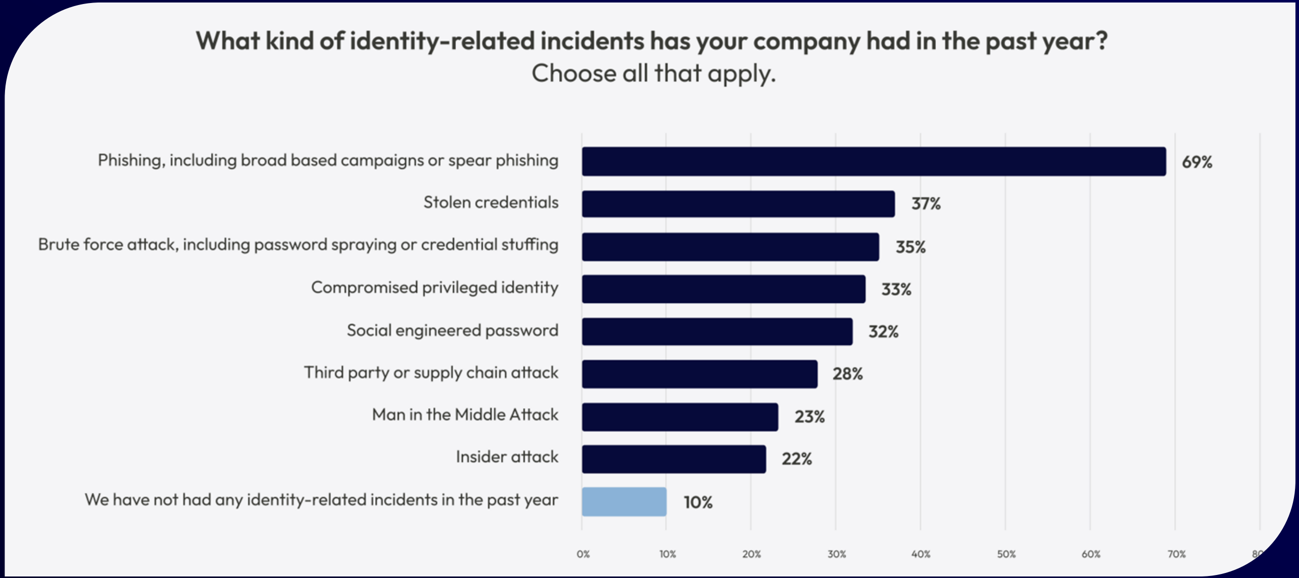
"By 2026, organizations prioritizing their security investments based on a continuous exposure management programme will be **3X less likely to suffer from a breach.**

"Security and risk management leaders should…pivot from traditional technology vulnerability management to a broader, more dynamic continuous threat and exposure management practice."

Gartner

tenable

# Identity Attacks are on the RISE



What kind of identity-related incidents has your company had in the past year?
Choose all that apply.

Source: https://www.idsalliance.org/white-paper/2024-trends-in-securing-digital-identities/

" **84%** of identity stakeholders said incidents directly impacted their business."
– IDSA Survey

" **91%** of ***companies invoked incident response for an identity-related incident in the past year.*** "
– IDSA Survey

# How Identity Sprawl Fuels Attacks

Identity is challenging and dynamic!
Rapid adoption of Cloud, SaaS, and remote work is fragmenting and expanding the attack surface.

### How identity sprawl manifests:

1. Blind spots—too many identities to monitor across multiple providers (AD, Entra ID, Okta…)
1. Hygiene—too many weaknesses to discover and track (misconfigurations, excessive permissions).
1. Risk—too much risk to assess and remediate in time

**$30M**
in financial impact

### Identity Sprawl Aides Attacks

🔍 Blind Spots → Unseen Attack Paths

🔓 Weak Hygiene → Exploitable Misconfigurations

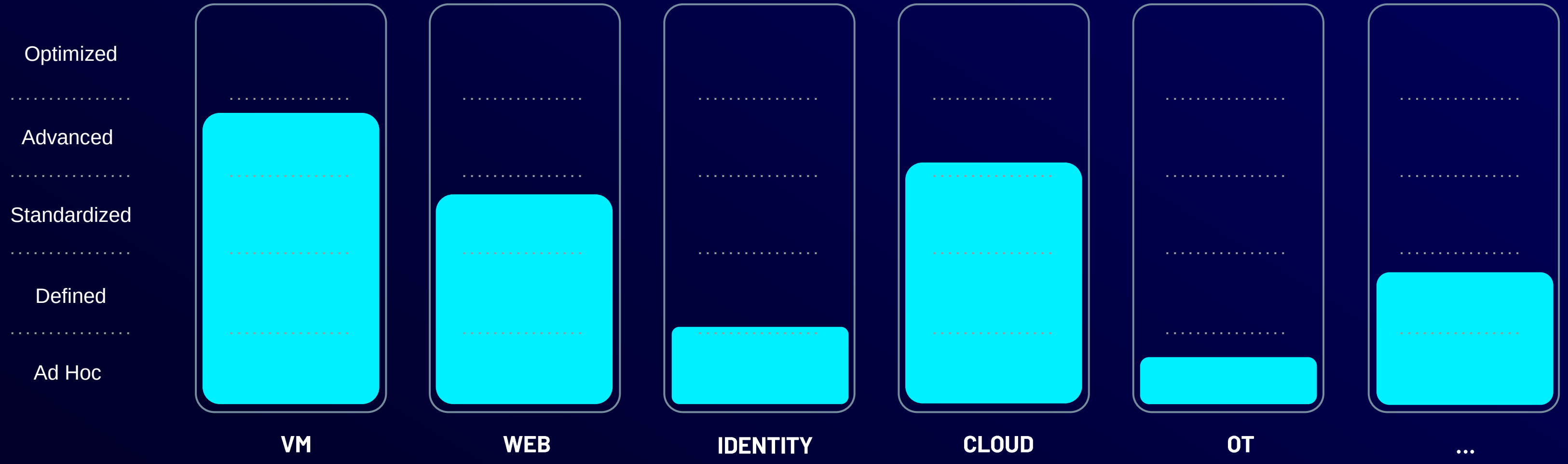
⚠️ Unquantified Risk → Delayed Response

⏳ Slow Remediation → Extended Dwell Time

tenable

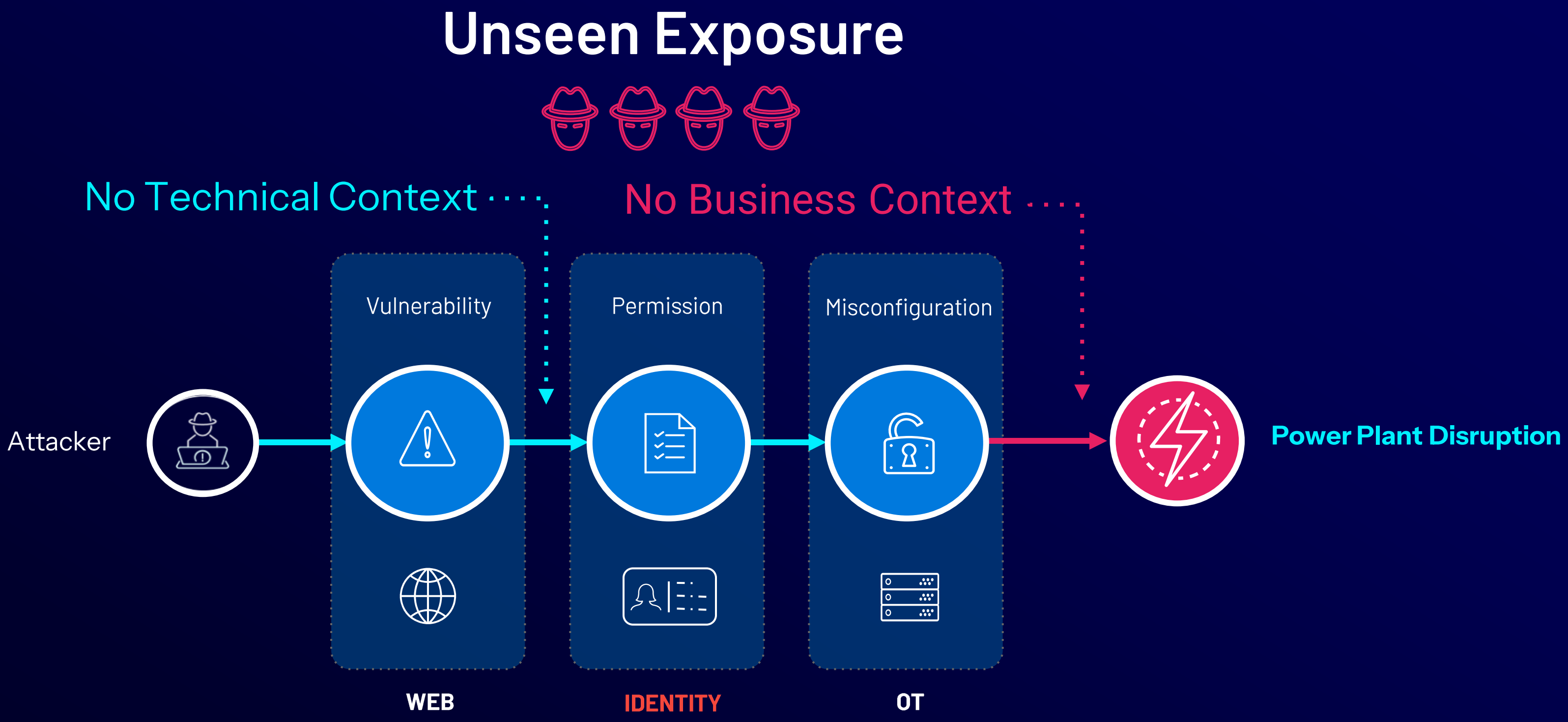
# Today: Proactive security is siloed – with varied levels of maturity....

How does this align
with your reality?

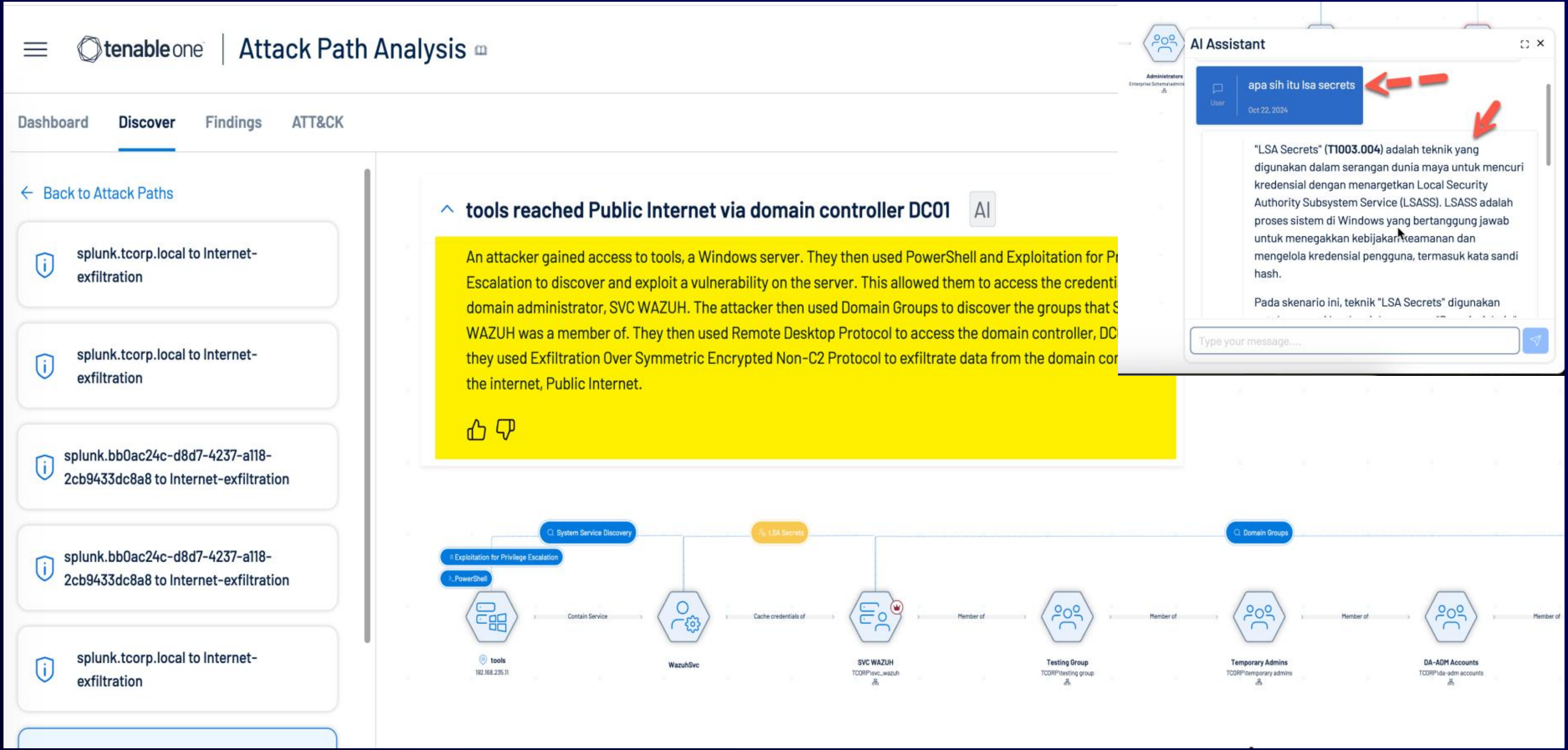


tenable

# Challenge: Attackers don’t honor silos...



# UNIFY INSIGHTS - Share context and prioritize true exposure



## tools reached Public Internet via domain controller DC01 AI

An attacker gained access to tools, a Windows server. They then used PowerShell and Exploitation for Pr
Escalation to discover and exploit a vulnerability on the server. This allowed them to access the credenti
domain administrator, SVC WAZUH. The attacker then used Domain Groups to discover the groups that S
WAZUH was a member of. They then used Remote Desktop Protocol to access the domain controller, DC
they used Exfiltration Over Symmetric Encrypted Non-C2 Protocol to exfiltrate data from the domain co
the internet, Public Internet.

**AI Assistant**

apa sih itu lsa secrets

Oct 22, 2024

"LSA Secrets" (**T1003.004**) adalah teknik yang digunakan dalam serangan dunia maya untuk mencuri kredensial dengan menargetkan Local Security Authority Subsystem Service (LSASS). LSASS adalah proses sistem di Windows yang bertanggung jawab untuk menegakkan kebijakan keamanan dan mengelola kredensial pengguna, termasuk kata sandi hash.

Pada skenario ini, teknik "LSA Secrets" digunakan

Type your message....

# SolarWinds Breach TTPs: On Prem to Cloud Compromise

**Total Impact:** $90 Billion

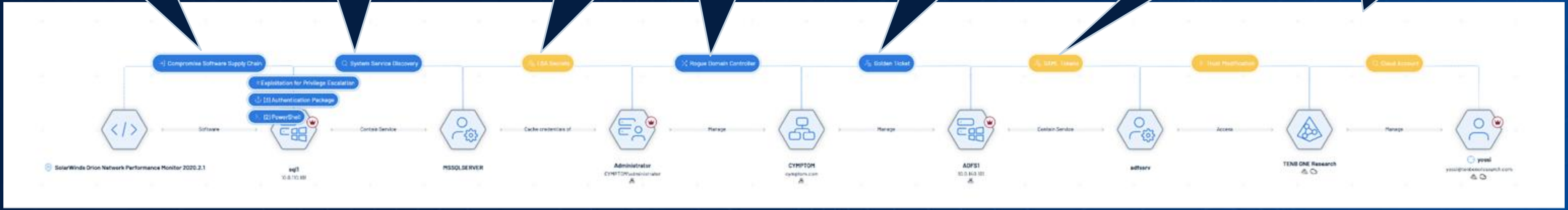
**Type:** Supply Chain Compromise

**Material Impact:** 11% of annual revenue, Espionage, Exfiltrated Data

**Domains:** Identity, VM, Cloud

**Sponsor:** APT29, Russia

**Important Note:** Pure play cloud security can not detect or prevent this attack, because it lacks Identity & VM context on premises.



Initial machine privileges via compromised Orion software

Target discovery using System Service Discovery

Elevate privileges by accessing admin credentials via LSA Secrets

Use admin privileges to create a rogue domain controller

Elevate permissions to compromise Active Directory Federated Services

Generate SAML tokens to become Azure admin

Gain trusted admin access to Azure Cloud

# NotPetya: Identity/IT to OT Compromise

**Total Impact:** $10 Billion

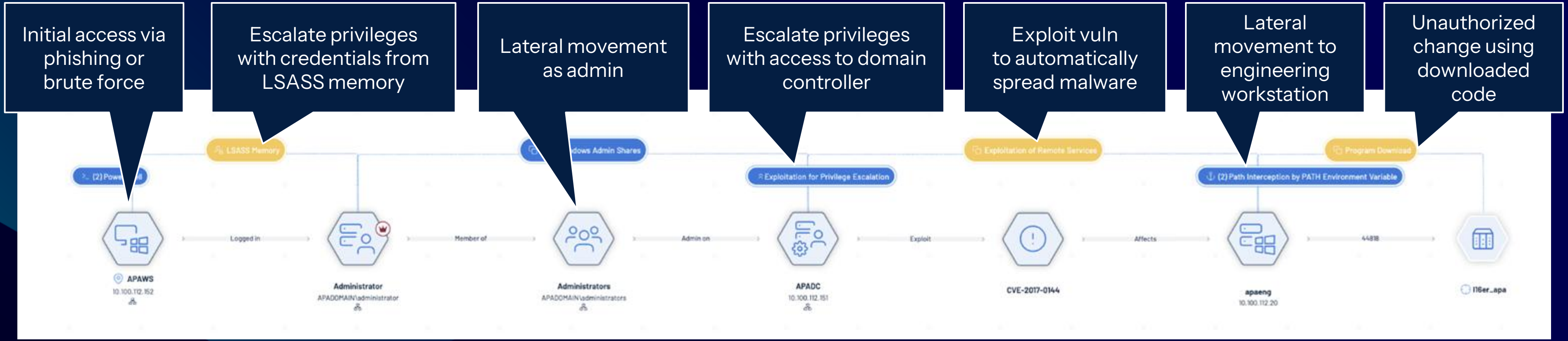
**Type:** Malware

**Material Impact**: Destroyed Data,
Disrupted Operations/Critical Infra

**Domains:** OT, Identity, VM

**Sponsor:** Sandworm, Russia GRU

**Key Takeaway:**
Pure-play OT security cannot detect or prevent this attack because tools lack Identity & IT context.



Initial access via phishing or brute force

Escalate privileges with credentials from LSASS memory

Lateral movement as admin

Escalate privileges with access to domain controller

Exploit vuln to automatically spread malware

Lateral movement to engineering workstation

Unauthorized change using downloaded code

tenable

# Octo Tempest (2023)

Financially-motivated ransomware group (= Scattered Spider = UNC3944 = Muddled Libra)

“For identity-based persistence, Octo Tempest targets federated identity providers using tools like AADInternals to federate existing domains, or spoof legitimate domains by adding and then federating new domains. The threat actor then abuses this federation to generate forged valid security assertion markup language (SAML) tokens for any user of the target tenant with claims that have MFA satisfied, a technique known as Golden SAML.

Similar techniques have also been observed using Okta as their source of truth identity provider, leveraging Okta Org2Org functionality to impersonate any desired user account.”

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction (Microsoft, Oct 2023)

# Storm-0501 (2024)

Financially-motivated ransomware group

“Following a successful pivot from the on-premises environment to the cloud through the compromised Microsoft Entra Connect Sync user account or the cloud admin account compromised through cloud session hijacking [...]

Once Global Administrator access is available for Storm-0501, we observed them creating a persistent backdoor access for later use by creating a new federated domain in the tenant. This backdoor enables an attacker to sign in as any user of the Microsoft Entra ID tenant in hand [...]”

Storm-0501: Ransomware attacks expanding to hybrid cloud environments (Microsoft, Sep 2024)

# Storm-0501 (2024)

Financially-motivated ransomware group

"The threat actor used the open-source tool AADInternals, and its Microsoft Entra ID capabilities to create the backdoor. [...] If the target domain is managed, then the attackers need to convert it to a federated one and provide a root certificate to sign future tokens upon user authentication and authorization processes. If the target domain is already federated, then the attackers need to add the root certificate as "NextSigningCertificate".

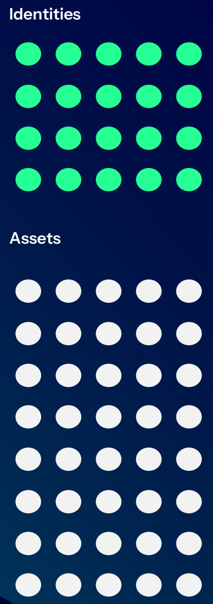
[...] The threat actor uses the AADInternals commands [...] which can be used to impersonate any user in the organization and bypass MFA to sign in to any application. [...]"

Storm-0501: Ransomware attacks expanding to hybrid cloud environments (Microsoft, Sep 2024)

# To scale, we must approach security from an attacker’s perspective…

Discover the **Attack Surface**

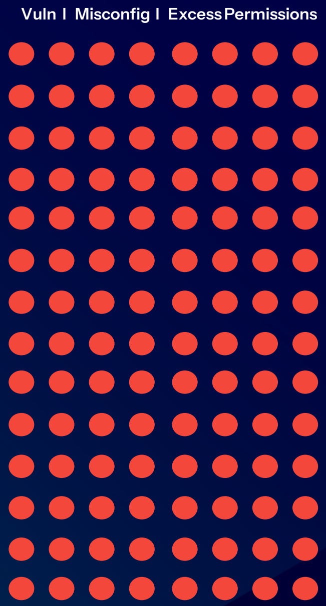
1



*Identify external & internal facing assets & identities*

Identify **Preventable Risk**

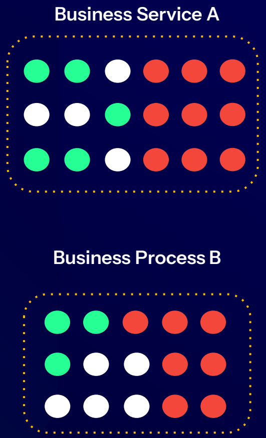
2



*Detect 3 forms of risk used to gain access & move laterally*

Align with **Business Context**

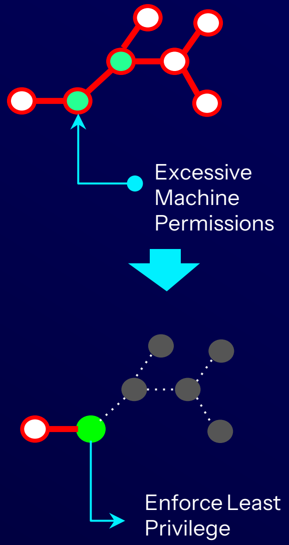
3



*Link assets, identities & risk to business to focus on what matters*

Remediate **True Exposure**

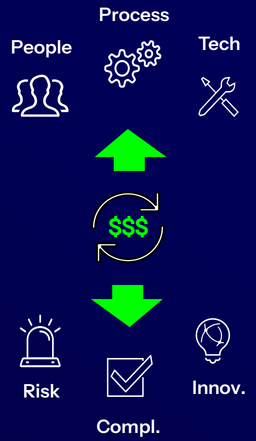
4



*Assess attack path viability and choke points for remediation*

Continuously **Optimize Investments**

5



*Measure and prioritize resources for better outcomes*

# Tenable One

## exposure management platform

### UNIFY VISION

See all your assets & risks across the attack surface

### UNIFY INSIGHT

Gain critical context to prioritize true exposure

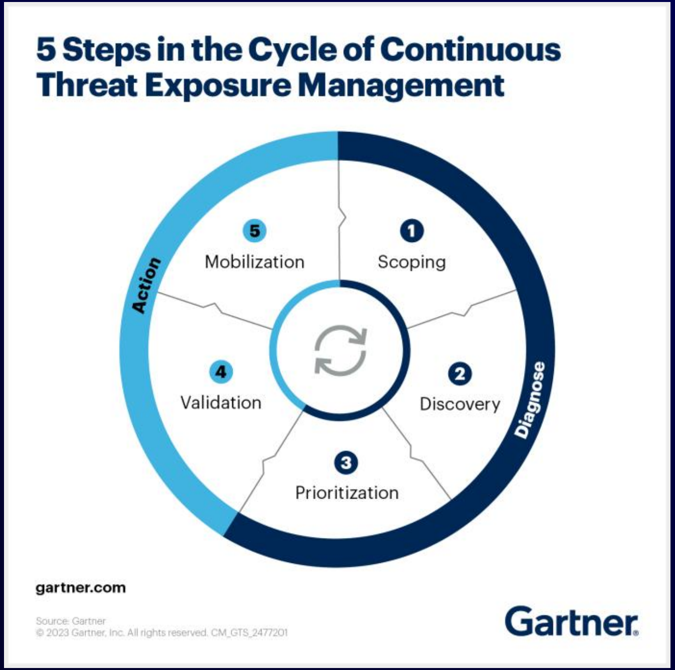
### UNIFY ACTION

Mobilize response across teams to eradicate risk

- Multi-cloud
- Federated identities
- Hybrid applications
- Unmanaged devices
- OT and IoT
- Private cloud and IT

tenable

# Gartner defines CTEM as a program (not a platform)…



5 Steps in the Cycle of Continuous Threat Exposure Management

Source: Gartner
© 2023 Gartner, Inc. All rights reserved. CM_GTS_2477201

## Continuous Threat Exposure Management (CTEM)

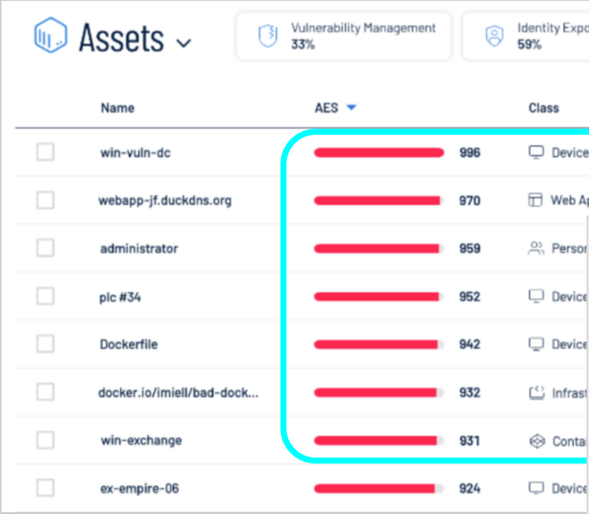
*Set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exploitability and exposure of an enterprise's digital and physical assets.*

1. *Scoping: Align on what is important to the business.*
2. *Discovery: Identify assets and risk across the attack surface.*
3. *Prioritization: Determine risks likely to be exploited for impact.*
4. *Validation: Verify whether attackers can exploit existing controls.*
5. *Mobilization: Communicate and remediate risk*

Gartner's first published use of EM was in 2022

# UNIFY VISION - Streamline hygiene and investigation

## Cross-domain Inventory + Normalization



Assets

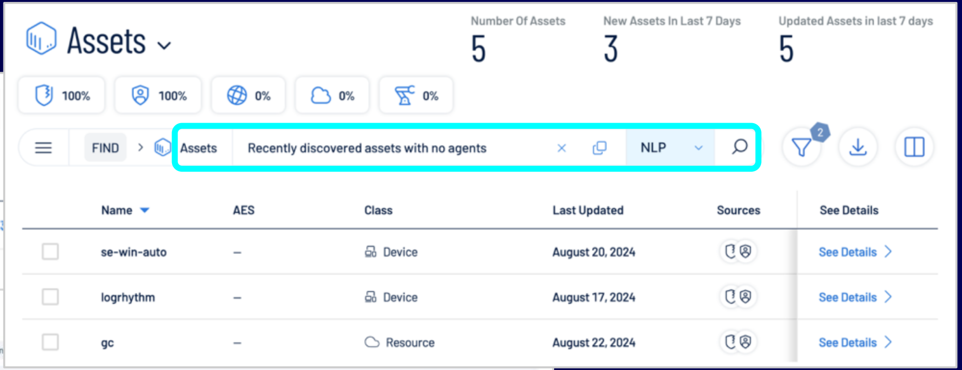
Vulnerability Management 33%

Identity Exposure 59%

Web Application Security <1%

| | Name | AES | Class | Weaknesses |
|---|---|---|---|---|
| □ | win-vuln-dc | 996 | Device | |
| □ | webapp-jf.duckdns.org | 970 | Web Application | |
| □ | administrator | 959 | Persor | |
| □ | plc #34 | 952 | Device | |
| □ | Dockerfile | 942 | Device | |
| □ | docker.io/imiell/bad-dock... | 932 | Infras | |
| □ | win-exchange | 931 | Conta | |
| □ | ex-empire-06 | 924 | Device | |

## AI - Natural Language Search



Assets

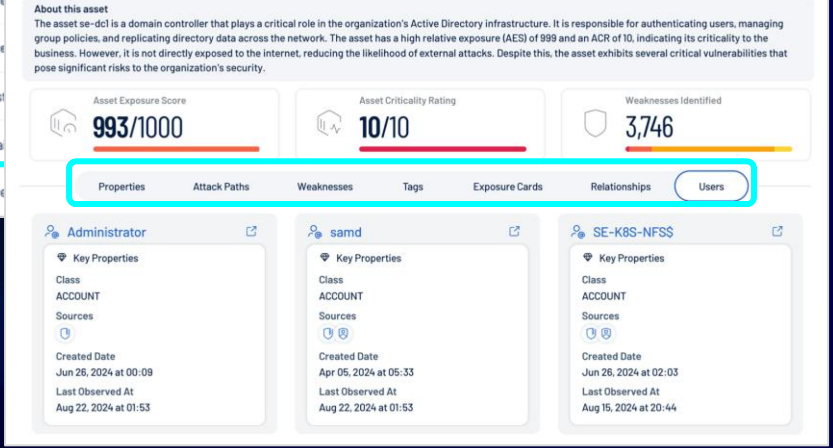
| Number Of Assets | New Assets In Last 7 Days | Updated Assets in last 7 days |
|---|---|---|
| 5 | 3 | 5 |

100% 100% 0% 0% 0%

FIND > Assets | Recently discovered assets with no agents | NLP

| | Name | AES | Class | Last Updated | Sources | See Details |
|---|---|---|---|---|---|---|
| □ | se-win-auto | – | Device | August 20, 2024 | | See Details > |
| □ | logrhythm | – | Device | August 17, 2024 | | See Details > |
| □ | gc | – | Resource | August 22, 2024 | | See Details > |

*Recently discovered assets with no agent*



se-dc1

DEVICE | 1 SOURCE | Data Breach and Tamperin

About this asset

The asset se-dc1 is a domain controller that plays a critical role in the organization's Active Directory infrastructure. It is responsible for authenticating users, managing group policies, and replicating directory data across the network. The asset has a high relative exposure (AES) of 999 and an ACR of 10, indicating its criticality to the business. However, it is not directly exposed to the internet, reducing the likelihood of external attacks. Despite this, the asset exhibits several critical vulnerabilities that pose significant risks to the organization's security.

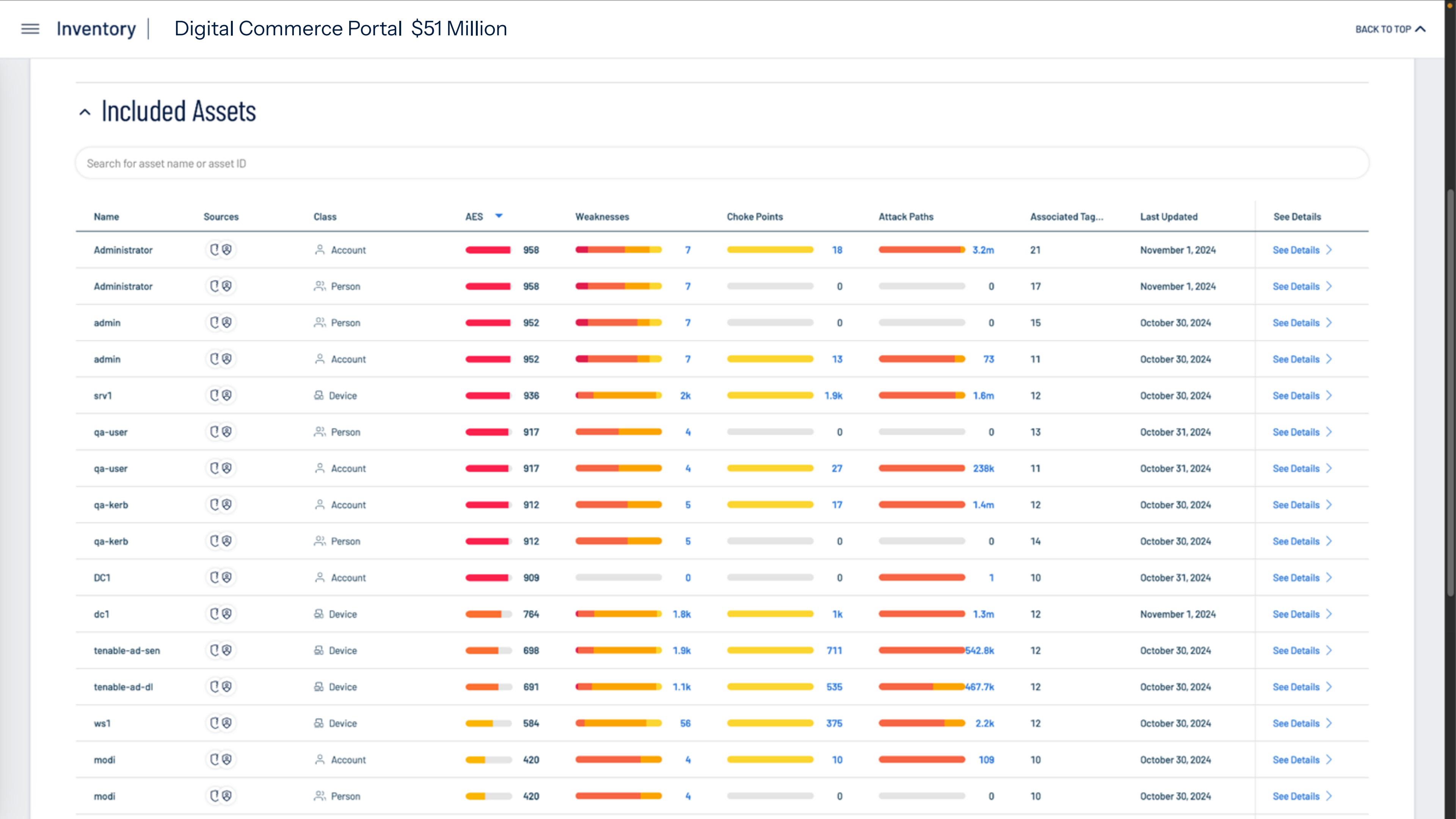
| Asset Exposure Score | Asset Criticality Rating | Weaknesses Identified |
|---|---|---|
| 993/1000 | 10/10 | 3,746 |

Properties | Attack Paths | Weaknesses | Tags | Exposure Cards | Relationships | Users

| | Administrator | samd | SE-K8S-NFS$ |
|---|---|---|---|
| Key Properties | | | |
| Class | ACCOUNT | ACCOUNT | ACCOUNT |
| Sources | | | |
| Created Date | Jun 26, 2024 at 00:09 | Apr 05, 2024 at 05:33 | Jun 26, 2024 at 02:03 |
| Last Observed At | Aug 22, 2024 at 01:53 | Aug 22, 2024 at 01:53 | Aug 15, 2024 at 20:44 |

## Asset Details, Users & Relationships

tenable



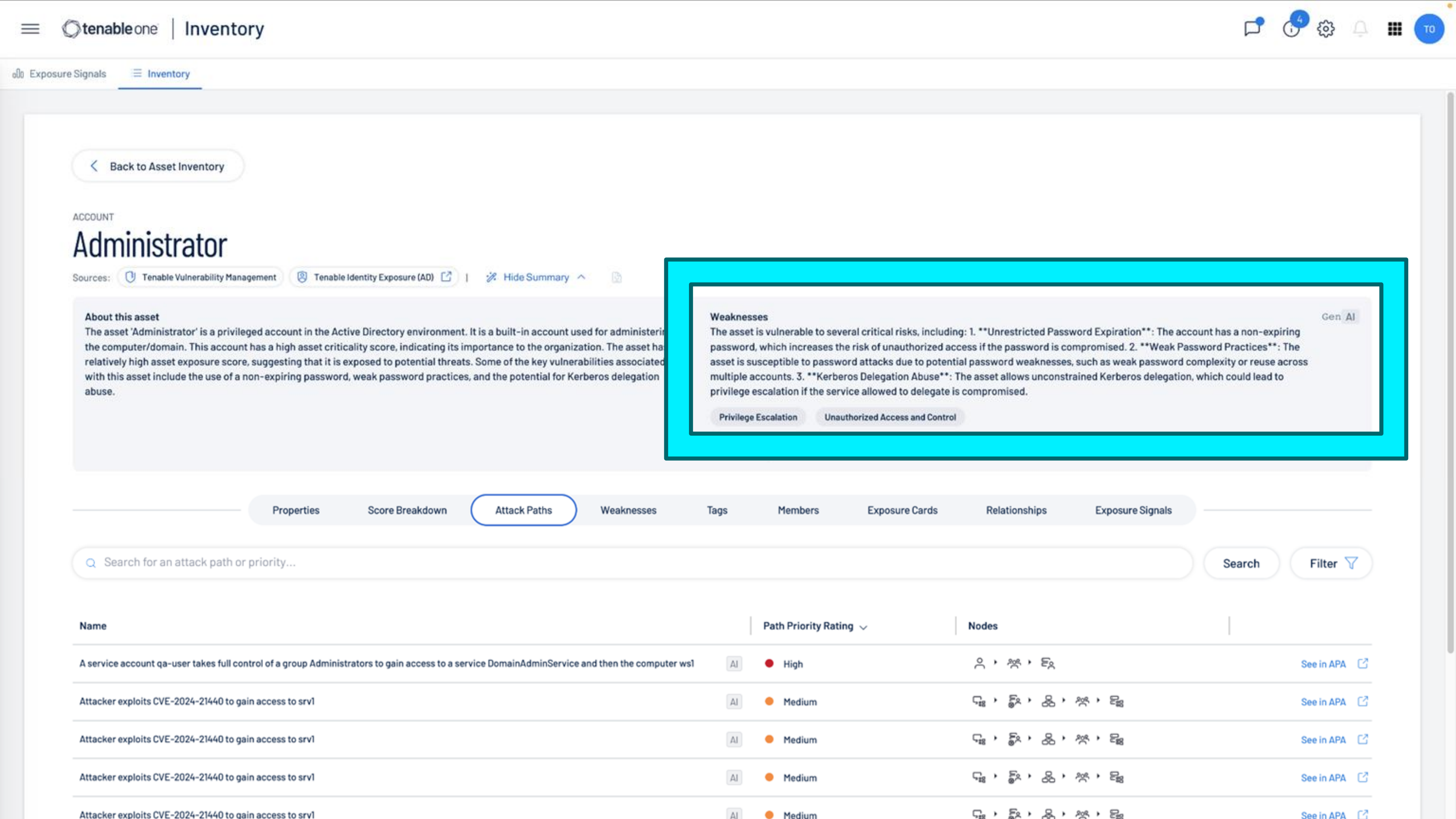
Inventory | Digital Commerce Portal $51 Million

BACK TO TOP

## Included Assets

Search for asset name or asset ID

| Name | Sources | Class | AES | Weaknesses | Choke Points | Attack Paths | Associated Tag... | Last Updated | See Details |
|---|---|---|---|---|---|---|---|---|---|
| Administrator | | Account | 958 | 7 | 18 | 3.2m | 21 | November 1, 2024 | See Details |
| Administrator | | Person | 958 | 7 | 0 | 0 | 17 | November 1, 2024 | See Details |
| admin | | Person | 952 | 7 | 0 | 0 | 15 | October 30, 2024 | See Details |
| admin | | Account | 952 | 7 | 13 | 73 | 11 | October 30, 2024 | See Details |
| srv1 | | Device | 936 | 2k | 1.9k | 1.6m | 12 | October 30, 2024 | See Details |
| qa-user | | Person | 917 | 4 | 0 | 0 | 13 | October 31, 2024 | See Details |
| qa-user | | Account | 917 | 4 | 27 | 238k | 11 | October 31, 2024 | See Details |
| qa-kerb | | Account | 912 | 5 | 17 | 1.4m | 12 | October 30, 2024 | See Details |
| qa-kerb | | Person | 912 | 5 | 0 | 0 | 14 | October 30, 2024 | See Details |
| DC1 | | Account | 909 | 0 | 0 | 1 | 10 | October 31, 2024 | See Details |
| dc1 | | Device | 764 | 1.8k | 1k | 1.3m | 12 | November 1, 2024 | See Details |
| tenable-ad-sen | | Device | 698 | 1.9k | 711 | 542.8k | 12 | October 30, 2024 | See Details |
| tenable-ad-dl | | Device | 691 | 1.1k | 535 | 467.7k | 12 | October 30, 2024 | See Details |
| ws1 | | Device | 584 | 56 | 375 | 2.2k | 12 | October 30, 2024 | See Details |
| modi | | Account | 420 | 4 | 10 | 109 | 10 | October 30, 2024 | See Details |
| modi | | Person | 420 | 4 | 0 | 0 | 10 | October 30, 2024 | See Details |



ACCOUNT

# Administrator

Sources: Tenable Vulnerability Management | Tenable Identity Exposure (AD) | Hide Summary

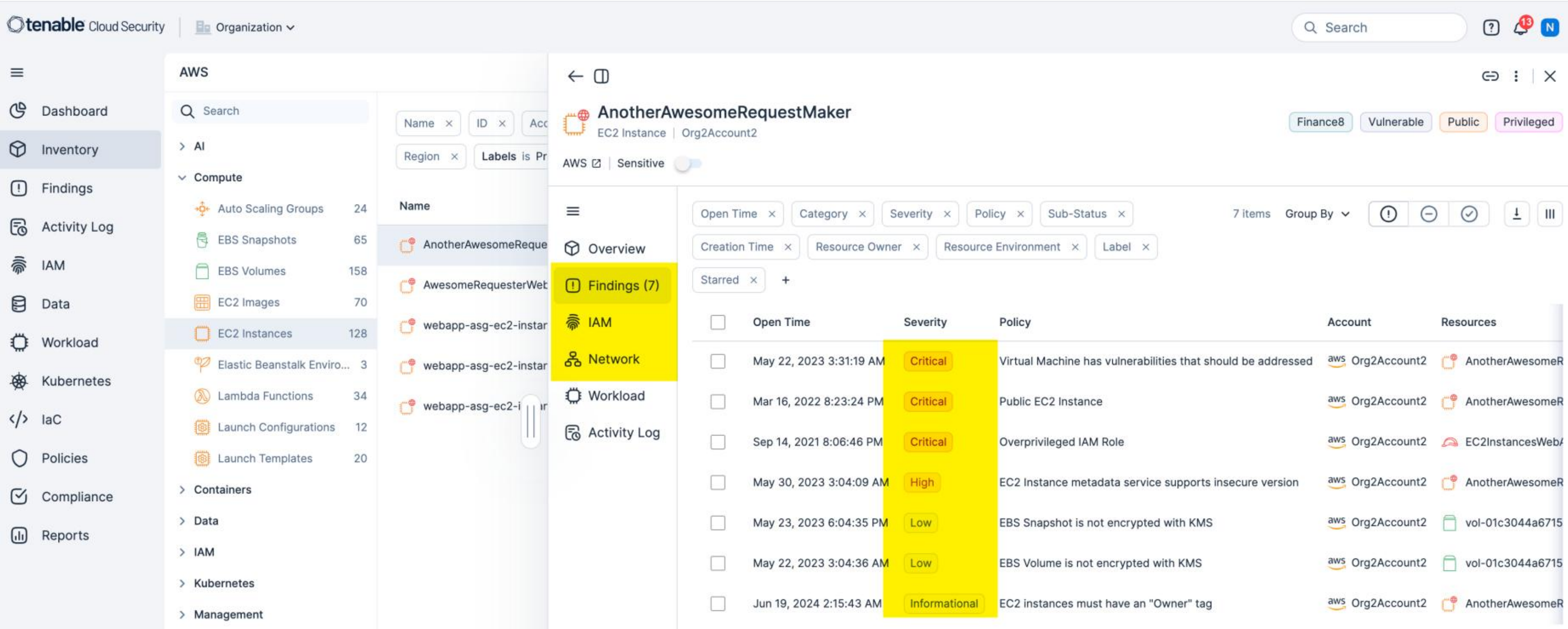
**About this asset**
The asset 'Administrator' is a privileged account in the Active Directory environment. It is a built-in account used for administeri the computer/domain. This account has a high asset criticality score, indicating its importance to the organization. The asset ha relatively high asset exposure score, suggesting that it is exposed to potential threats. Some of the key vulnerabilities associated with this asset include the use of a non-expiring password, weak password practices, and the potential for Kerberos delegation abuse.

**Weaknesses** Gen AI
The asset is vulnerable to several critical risks, including: 1. **Unrestricted Password Expiration**: The account has a non-expiring password, which increases the risk of unauthorized access if the password is compromised. 2. **Weak Password Practices**: The asset is susceptible to password attacks due to potential password weaknesses, such as weak password complexity or reuse across multiple accounts. 3. **Kerberos Delegation Abuse**: The asset allows unconstrained Kerberos delegation, which could lead to privilege escalation if the service allowed to delegate is compromised.

Privilege Escalation | Unauthorized Access and Control

| Name | | Path Priority Rating | Nodes | |
|---|---|---|---|---|
| A service account qa-user takes full control of a group Administrators to gain access to a service DomainAdminService and then the computer ws1 | AI | ● High | | See in APA |
| Attacker exploits CVE-2024-21440 to gain access to srv1 | AI | ● Medium | | See in APA |
| Attacker exploits CVE-2024-21440 to gain access to srv1 | AI | ● Medium | | See in APA |
| Attacker exploits CVE-2024-21440 to gain access to srv1 | AI | ● Medium | | See in APA |
| Attacker exploits CVE-2024-21440 to gain access to srv1 | AI | ● Medium | | See in APA |

# UNIFY INSIGHTS - Share context and prioritize true exposure



| Compute | |
|---|---|
| Auto Scaling Groups | 24 |
| EBS Snapshots | 65 |
| EBS Volumes | 158 |
| EC2 Images | 70 |
| EC2 Instances | 128 |
| Elastic Beanstalk Enviro... | 3 |
| Lambda Functions | 34 |
| Launch Configurations | 12 |
| Launch Templates | 20 |

Name
- AnotherAwesomeReque
- AwesomeRequesterWet
- webapp-asg-ec2-instar
- webapp-asg-ec2-instar
- webapp-asg-ec2-i

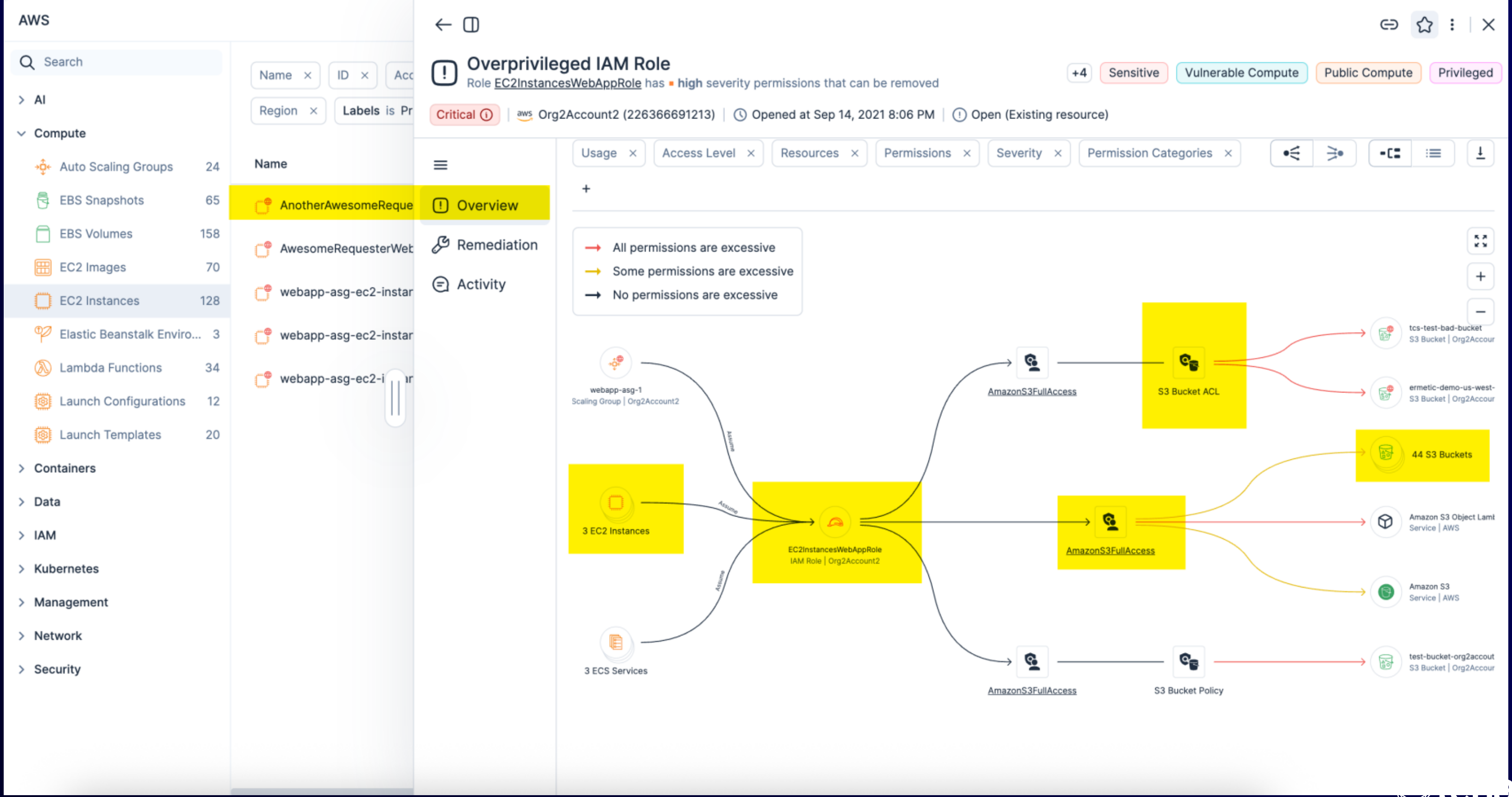
AnotherAwesomeRequestMaker
EC2 Instance | Org2Account2

Finance8 Vulnerable Public Privileged

AWS | Sensitive

| ☐ | Open Time | Severity | Policy | Account | Resources |
|---|---|---|---|---|---|
| ☐ | May 22, 2023 3:31:19 AM | Critical | Virtual Machine has vulnerabilities that should be addressed | aws Org2Account2 | AnotherAwesomeR |
| ☐ | Mar 16, 2022 8:23:24 PM | Critical | Public EC2 Instance | aws Org2Account2 | AnotherAwesomeR |
| ☐ | Sep 14, 2021 8:06:46 PM | Critical | Overprivileged IAM Role | aws Org2Account2 | EC2InstancesWeb/ |
| ☐ | May 30, 2023 3:04:09 AM | High | EC2 Instance metadata service supports insecure version | aws Org2Account2 | AnotherAwesomeR |
| ☐ | May 23, 2023 6:04:35 PM | Low | EBS Snapshot is not encrypted with KMS | aws Org2Account2 | vol-01c3044a6715 |
| ☐ | May 22, 2023 3:04:36 AM | Low | EBS Volume is not encrypted with KMS | aws Org2Account2 | vol-01c3044a6715 |
| ☐ | Jun 19, 2024 2:15:43 AM | Informational | EC2 instances must have an "Owner" tag | aws Org2Account2 | AnotherAwesomeR |

# UNIFY INSIGHTS - Share context and prioritize true exposure



**Overprivileged IAM Role**

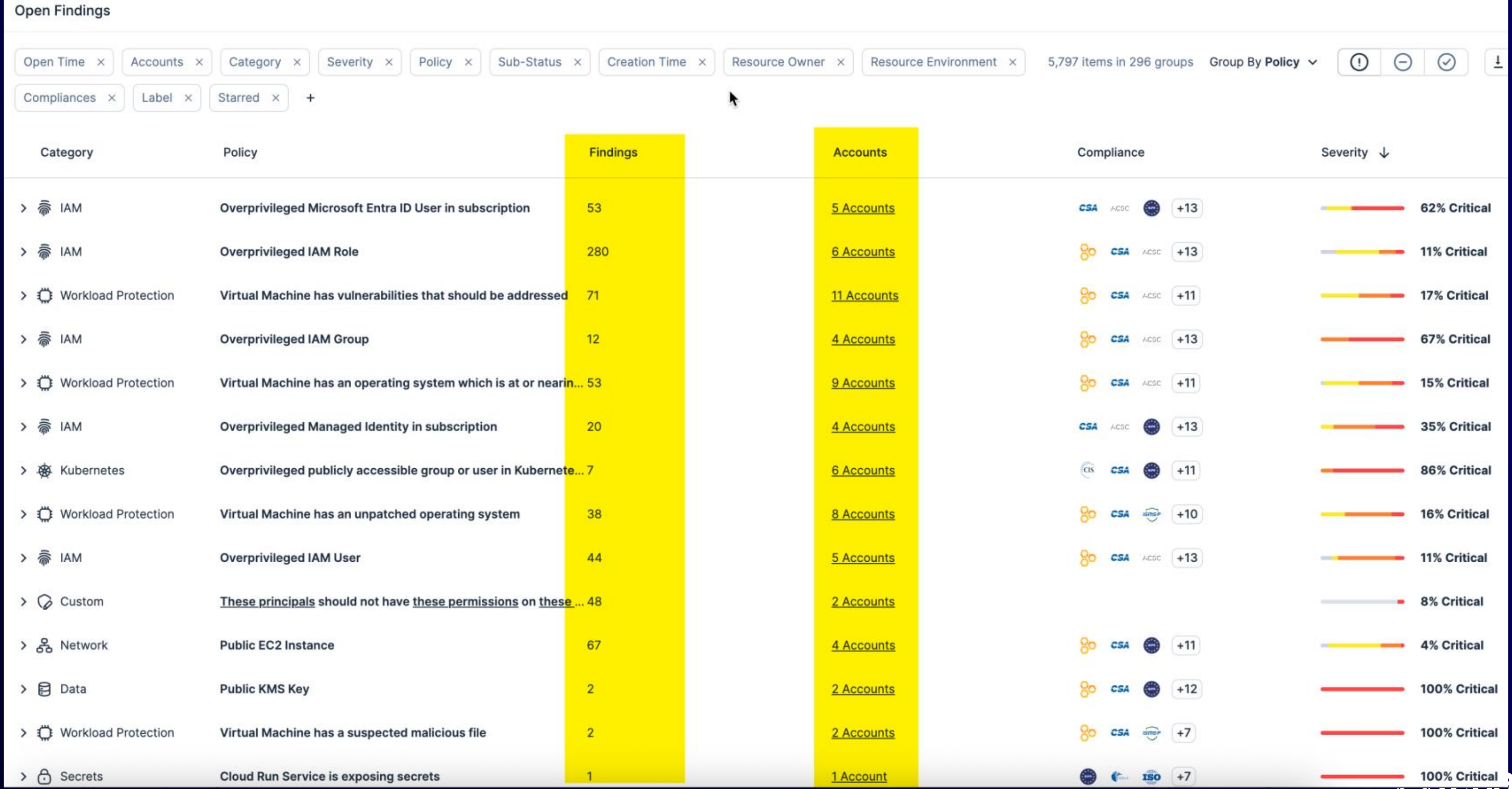
Role EC2InstancesWebAppRole has ▪ high severity permissions that can be removed

+4 Sensitive Vulnerable Compute Public Compute Privileged

Critical ⓘ | aws Org2Account2 (226366691213) | Opened at Sep 14, 2021 8:06 PM | Open (Existing resource)

→ All permissions are excessive
→ Some permissions are excessive
→ No permissions are excessive

# UNIFY INSIGHTS - Share context and prioritize true exposure



Open Findings

Open Time × | Accounts × | Category × | Severity × | Policy × | Sub-Status × | Creation Time × | Resource Owner × | Resource Environment × | Compliances × | Label × | Starred × | +

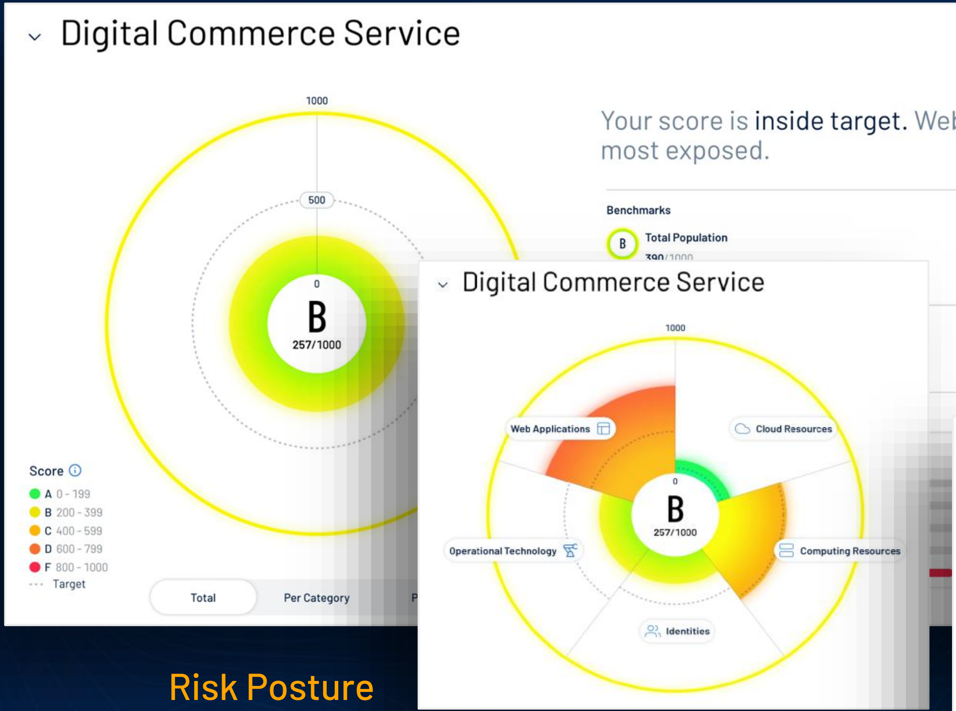
5,797 items in 296 groups

Group By **Policy**

| Category | Policy | Findings | Accounts | Compliance | Severity ↓ |
|---|---|---|---|---|---|
| IAM | Overprivileged Microsoft Entra ID User in subscription | 53 | 5 Accounts | CSA ACSC +13 | 62% Critical |
| IAM | Overprivileged IAM Role | 280 | 6 Accounts | CSA ACSC +13 | 11% Critical |
| Workload Protection | Virtual Machine has vulnerabilities that should be addressed | 71 | 11 Accounts | CSA ACSC +11 | 17% Critical |
| IAM | Overprivileged IAM Group | 12 | 4 Accounts | CSA ACSC +13 | 67% Critical |
| Workload Protection | Virtual Machine has an operating system which is at or nearin... | 53 | 9 Accounts | CSA ACSC +11 | 15% Critical |
| IAM | Overprivileged Managed Identity in subscription | 20 | 4 Accounts | CSA ACSC +13 | 35% Critical |
| Kubernetes | Overprivileged publicly accessible group or user in Kubernete... | 7 | 6 Accounts | CIS CSA +11 | 86% Critical |
| Workload Protection | Virtual Machine has an unpatched operating system | 38 | 8 Accounts | CSA ISMS-P +10 | 16% Critical |
| IAM | Overprivileged IAM User | 44 | 5 Accounts | CSA ACSC +13 | 11% Critical |
| Custom | These principals should not have these permissions on these ... | 48 | 2 Accounts | | 8% Critical |
| Network | Public EC2 Instance | 67 | 4 Accounts | CSA +11 | 4% Critical |
| Data | Public KMS Key | 2 | 2 Accounts | CSA +12 | 100% Critical |
| Workload Protection | Virtual Machine has a suspected malicious file | 2 | 2 Accounts | CSA ISMS-P +7 | 100% Critical |
| Secrets | Cloud Run Service is exposing secrets | 1 | 1 Account | ISO +7 | 100% Critical |

# UNIFY ACTION – Optimize risk posture and investments

Focus on Critical Apps, Locations, Processes



Digital Commerce Service

Your score is inside target. Web Applications is most exposed.

Benchmarks

B Total Population 390/1000

Score

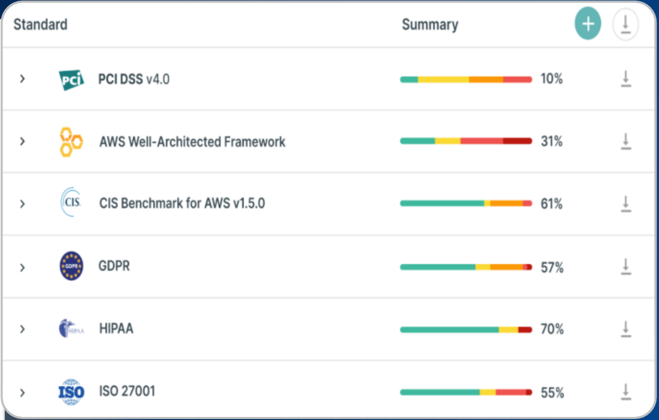
- 🟢 A 0 - 199
- 🟡 B 200 - 399
- 🟠 C 400 - 599
- 🟠 D 600 - 799
- 🔴 F 800 - 1000
- --- Target

Digital Commerce Service

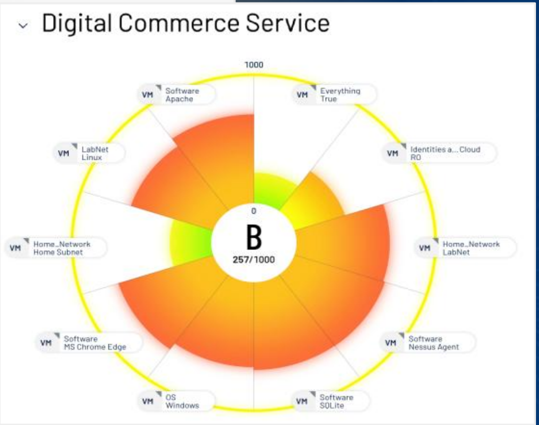
Risk Posture by Domain

Understand domain exposure

Communicate compliance posture



| Standard | Summary |
|---|---|
| PCI DSS v4.0 | 10% |
| AWS Well-Architected Framework | 31% |
| CIS Benchmark for AWS v1.5.0 | 61% |
| GDPR | 57% |
| HIPAA | 70% |
| ISO 27001 | 55% |



Digital Commerce Service

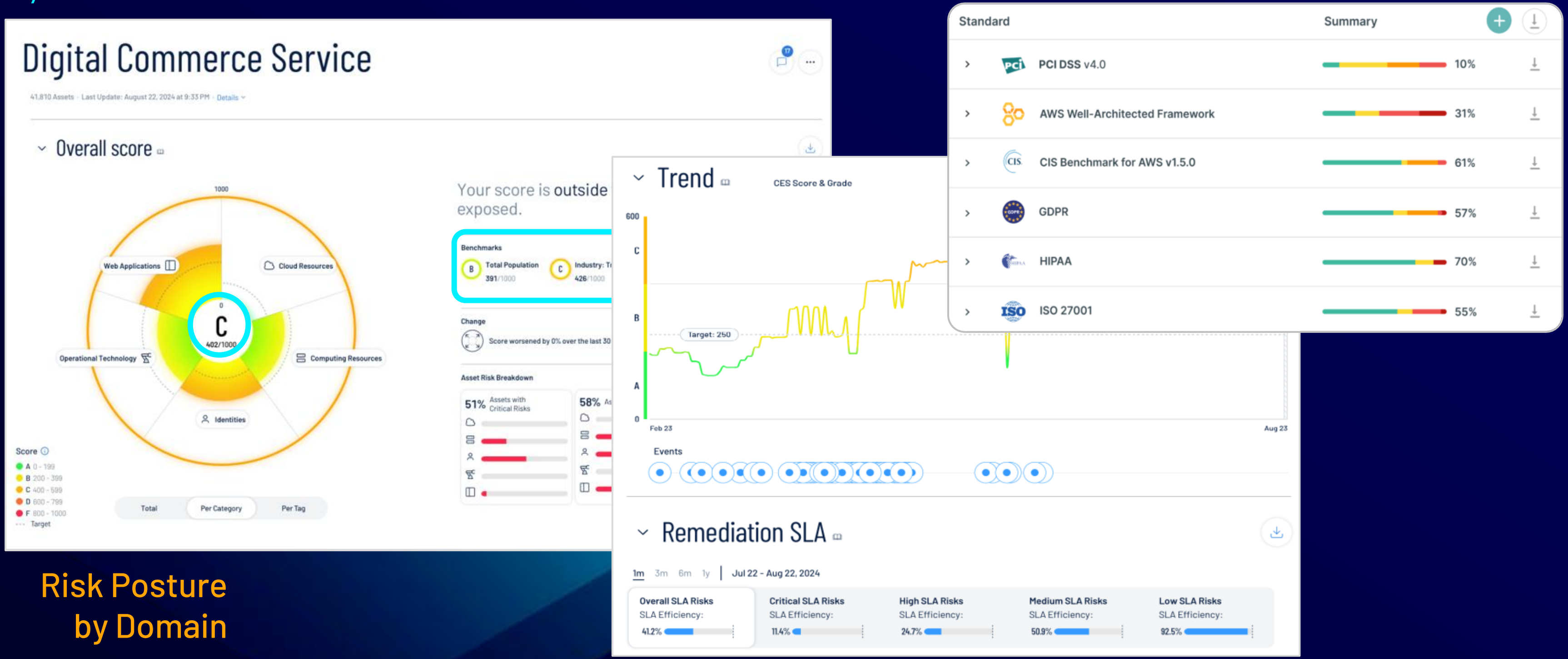
Risk Posture by Tag

tenable

# **UNIFY ACTION** – Optimize risk posture and investments

Cyber Risk Posture

Compliance



## Digital Commerce Service

41,810 Assets · Last Update: August 22, 2024 at 9:33 PM · Details

### Overall score

Your score is outside exposed.

Benchmarks
B Total Population 391/1000
C Industry: T 426/1000

Change
Score worsened by 0% over the last 30

Asset Risk Breakdown
51% Assets with Critical Risks
58% A

Score
● A 0 - 199
● B 200 - 399
● C 400 - 599
● D 600 - 799
● F 800 - 1000
Target

### Trend

CES Score & Grade

| Standard | Summary |
|---|---|
| PCI DSS v4.0 | 10% |
| AWS Well-Architected Framework | 31% |
| CIS Benchmark for AWS v1.5.0 | 61% |
| GDPR | 57% |
| HIPAA | 70% |
| ISO 27001 | 55% |

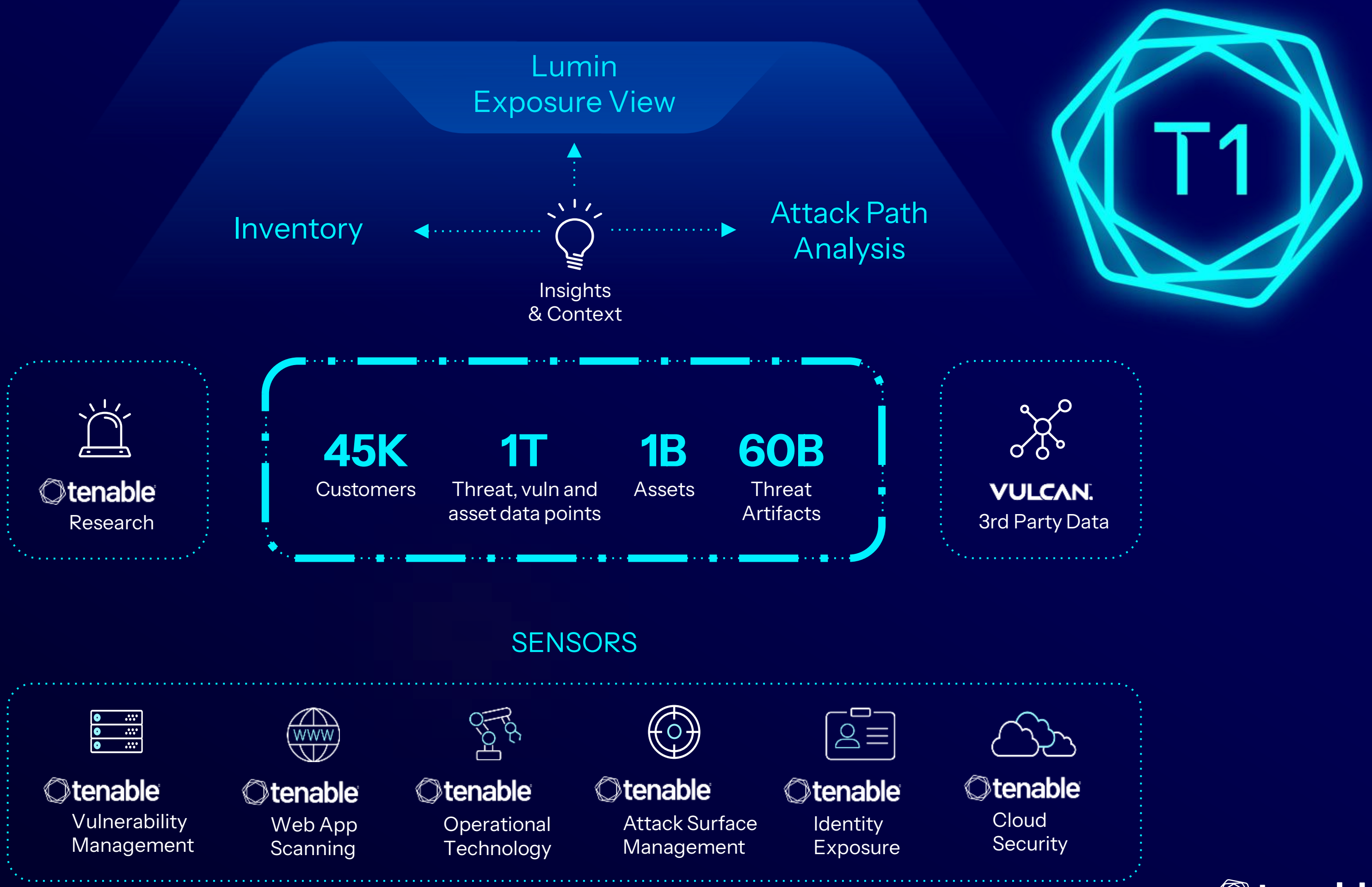
### Remediation SLA

1m 3m 6m 1y | Jul 22 - Aug 22, 2024

| Overall SLA Risks | Critical SLA Risks | High SLA Risks | Medium SLA Risks | Low SLA Risks |
|---|---|---|---|---|
| SLA Efficiency: | SLA Efficiency: | SLA Efficiency: | SLA Efficiency: | SLA Efficiency: |
| 41.2% | 11.4% | 24.7% | 50.9% | 92.5% |

Risk Posture
by Domain

Key Performance Indicators



Lumin
Exposure View

Inventory

Insights
& Context

Attack Path
Analysis

T1

tenable
Research

**45K**
Customers

**1T**
Threat, vuln and
asset data points

**1B**
Assets

**60B**
Threat
Artifacts

VULCAN.
3rd Party Data

SENSORS

tenable
Vulnerability
Management

tenable
Web App
Scanning

tenable
Operational
Technology

tenable
Attack Surface
Management

tenable
Identity
Exposure

tenable
Cloud
Security

# Tenable One Case Study: Expected Security Operations Outcomes

| Requirements | Current Scenario | Outcome Target |
|---|---|---|
| **Time to Assess** and Correlate all Risk Findings | 1-2 Days | Less than 6 Hours |
| **Time to prioritize** on Risk Treatment | 5 hours | 10 Minutes |
| **Forensics** Capacity | 6 IOC/day | 120 IOC/day |
| Consoles | More than 3 | 1-2 |
| **Support** Handling/Respond | 1 Days | Less than 3 hours |

## EFFICACY

- ➢ Average Time assess all digital assets reduces dwell time to less than 6 hours.
- ➢ Full use of Threat Intel and Artificial Intelligence gives customer a higher confidence that security is effective with very low false Positive rate

## EFFICENCY

- ➢ 66% reduction in technology components reduces that cost of security.
- ➢ 85% decrease in manual effort allows customer to repurpose the analysts to harder tasks.
- ➢ 350% increase in IOC handling capacity with Attack Path analysis

tenable

tenable®

Your Exposure Ends Here