HARVARD UNIVERSITY
Information Technology

Transforming Vulnerability Management

From One Size-Fits-All to Truly Risk-Based

Security Camp
7 Aug 2025

Agenda

Welcome and Introductions

The Problem We Faced

Solution Design and Implementation

Demonstration

Lessons Learned

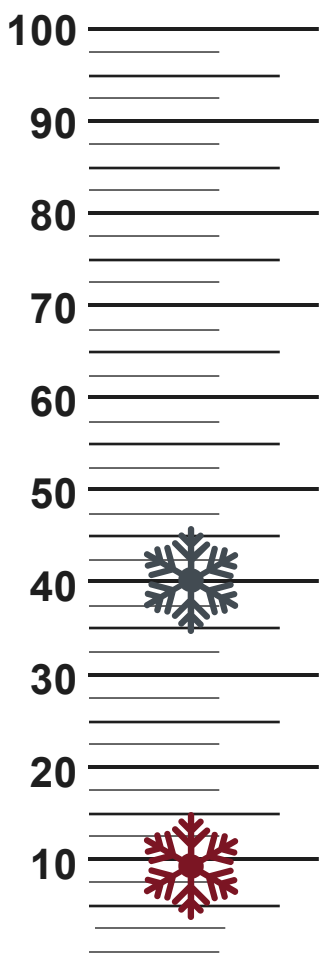
Conclusion and Q&A

Introductions

John Sorel, Sr. Security Engineer, Harvard University

Todd Conetta, Project Manager, Harvard University; SEI, Inc.

Journey of the Mind to Beat the Heat (New England Style)



Which month sees the most Snow?

February

What's the average annual snowfall in Boston?

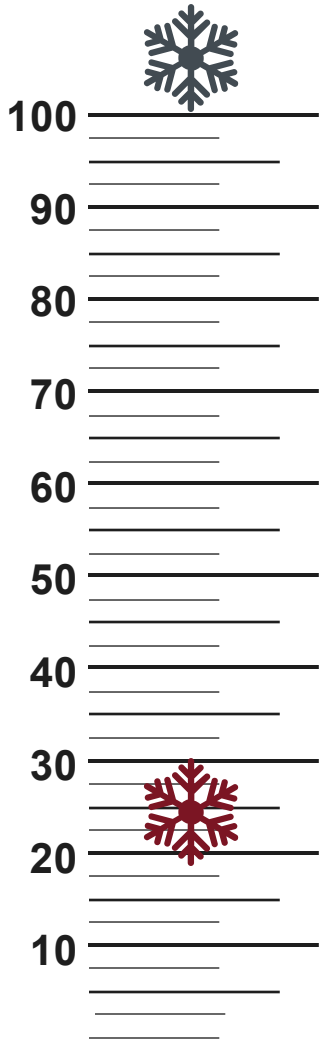
~40 inches

Average biggest snowfall of the year?

~9.5 inches

https://www.extremeweatherwatch.com/cities/boston/most-yearly-snow, https://www.currentresults.com/Yearly-Weather/USA/MA/Boston/extreme-annual-boston-snowfall.php

Journey of the Mind to Beat the Heat (New England Style)



What was the largest snowfall total for one winter?

108 inches

Okay but that was a long time ago, right?

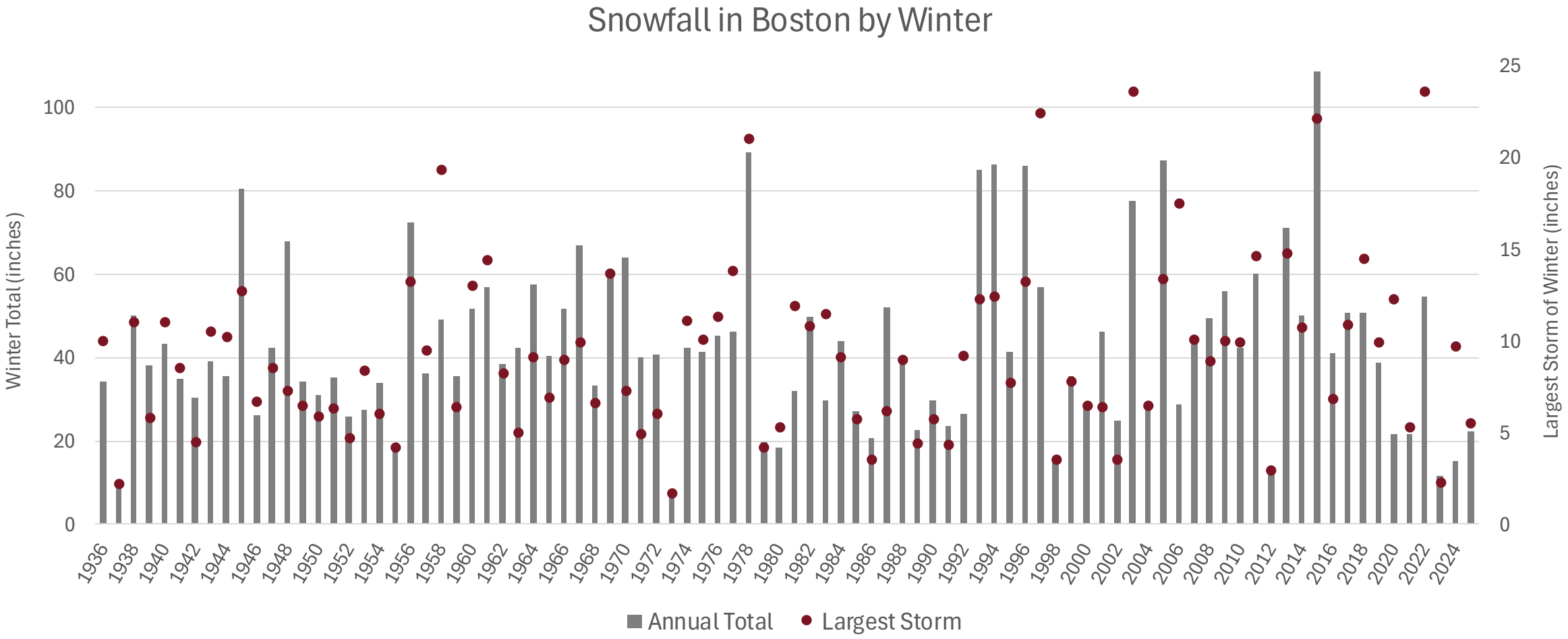
2014 - 2015

So 2015 probably had the worst storm in recent years, too?

No - 23.5 inches 2022

https://www.extremeweatherwatch.com/cities/boston/most-yearly-snow, https://www.currentresults.com/Yearly-Weather/USA/MA/Boston/extreme-annual-boston-snowfall.php

A Historical View of the Data Set



https://www.extremeweatherwatch.com/cities/boston/most-yearly-snow, https://www.currentresults.com/Yearly-Weather/USA/MA/Boston/extreme-annual-boston-snowfall.php

The Problem we Faced: A Vulnerability Whiteout

A Moment of Clarity in the Storm

- 2022 Call-to-Action, named as a top information security risk
- Addressed with an all hands on-deck goal:

  Reduce all critical and high severity vulnerabilities by 75% in Fiscal Year 2023

- Real improvements and impactful change:
  - Established a Community of Practice
  - Pilot processes for exception handling
  - Addressed bottlenecks in patching process
  - Increased use of automation

The Problem we Faced: Initial Success

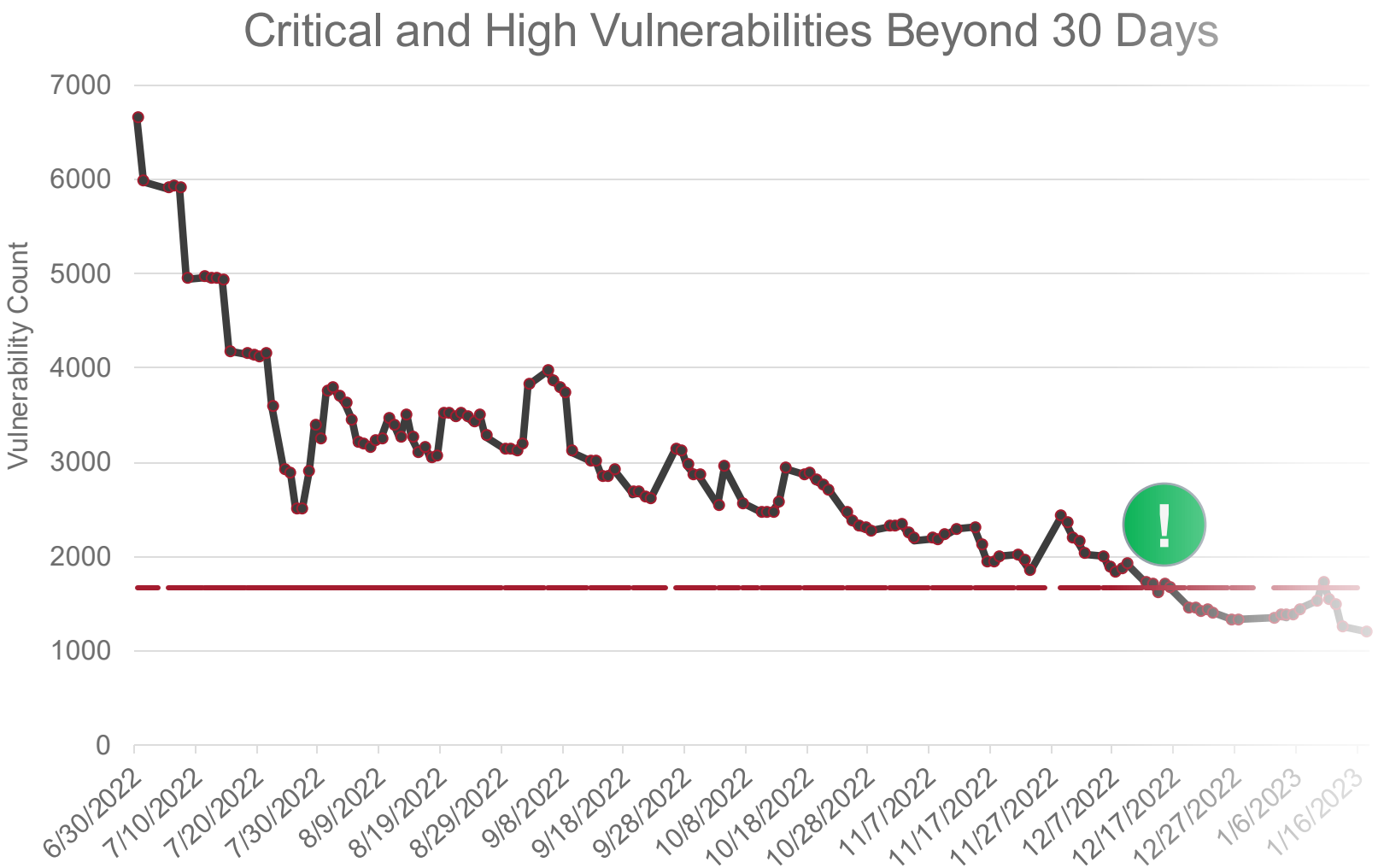


Chart does not represent the entire University, this is one school's counts in FY23

FY23 Success

- Each school significantly reduced their vulnerabilities
- The University reduced by ~78%
- Information sharing, process improvement, better understanding of data

New Challenges Emerge

- Sustaining is actually hard!
- VM fatigue sets in
- Moving up the stack requires new stakeholders and often longer timelines

The Problem we Faced: Tackling What was Next

Evolving Threat Landscape

- Increasing volume and sophistication of threats
- High volume of vulnerabilities
- Limited resources and growing compliance pressures

Challenges with Traditional Approaches

- High-volume, low-priority workload
- Inefficient resource allocation
- Difficulty communicating risk to leadership

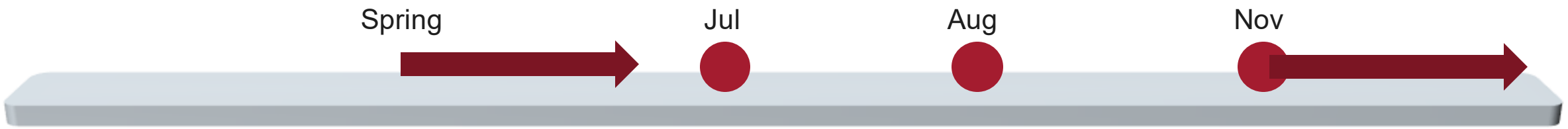
Building a Solution: Establishing a Framework for Execution

Launching a Risk-Based Approach

- Starting FY24: 3-Year Initiative
- Prioritize remediation based on true risk to the University
- Centralize standards to drive consistency across decentralized action
- Engage with partners to lay the foundation for strong stakeholder alignment
- Equip partners with the right toolset

Building a Solution: Timeline

2023



Final stretch for 75% reduction

University-wide Vulnerability Management team established

Team conducts listening tour across schools

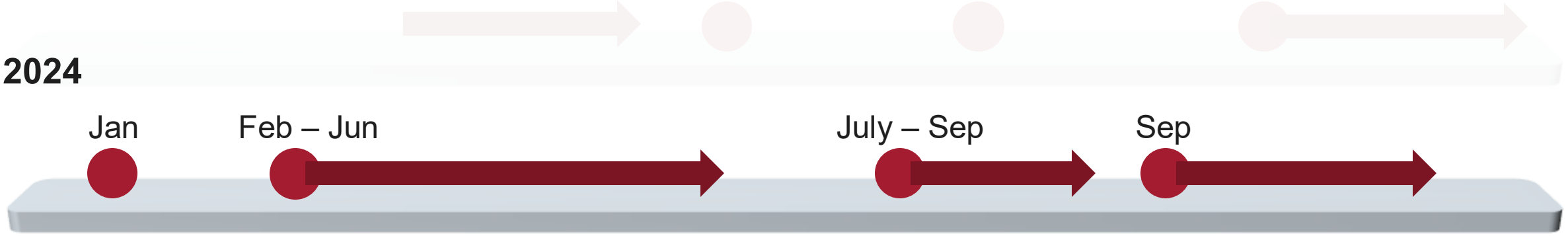
Risk-based vulnerability management (RBVM) pilot approved

RBVM Product Research

Building a Solution: Timeline

2023

2024



Stood up Cyber Asset Attack Surface Management (CAASM) instance

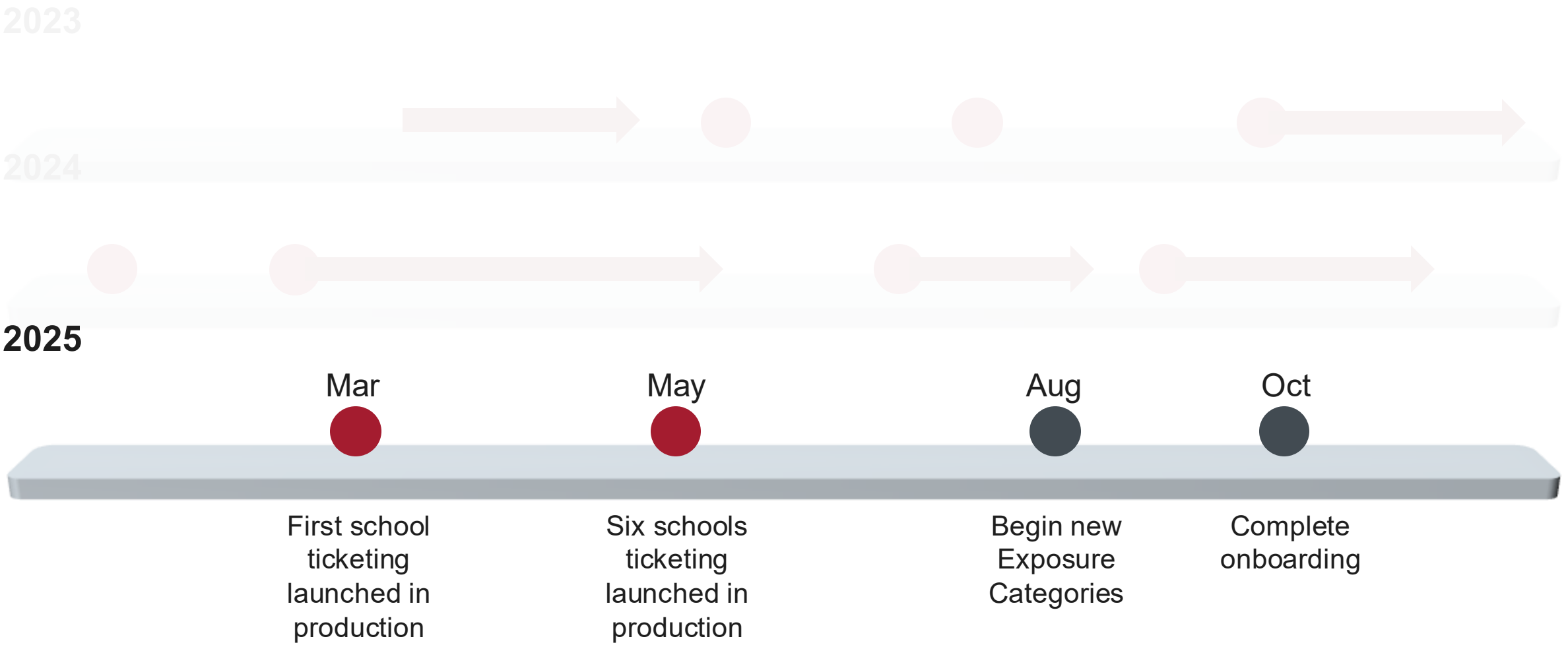
Conducted pilot to demonstrate viability of RBVM and suitability of CAASM platform as primary engine

Shift from pilot to execution planning

University-wide kickoff begin onboarding

Product development + onboarding activities

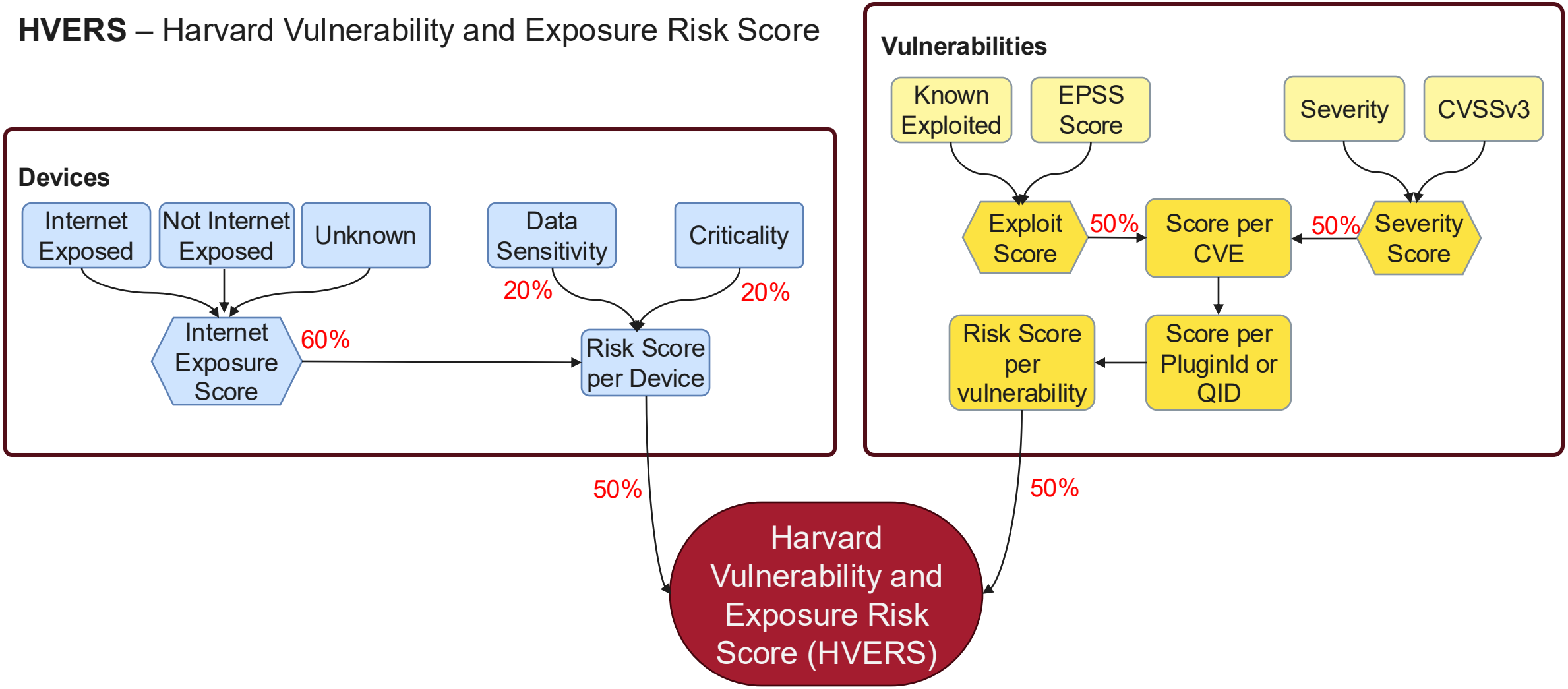
Building a Solution: Timeline



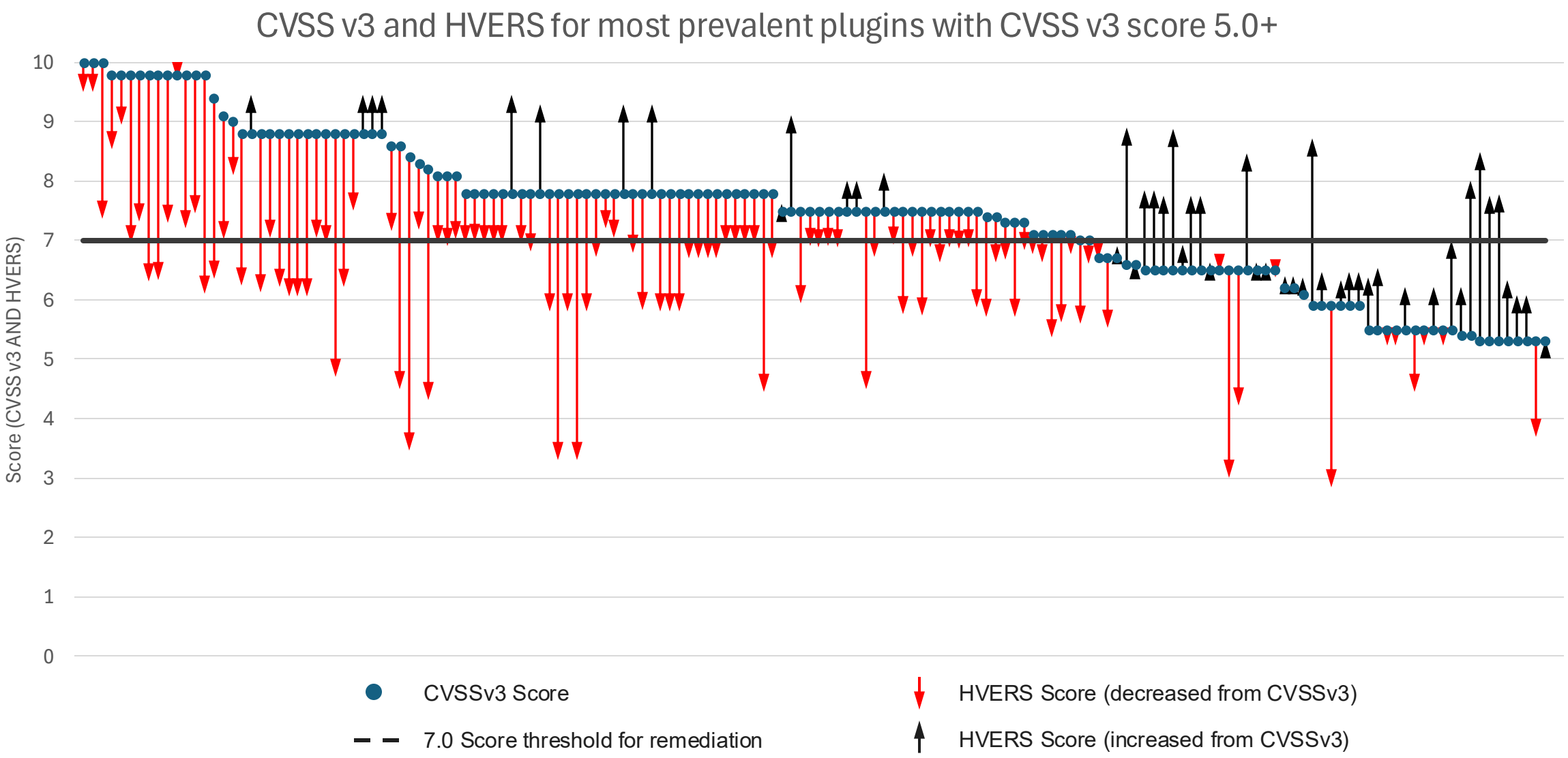
Building a Solution: Timeline

Building a Solution: Calculating HVERS

HVERS – Harvard Vulnerability and Exposure Risk Score



Building a Solution: HVERS v. CVSS (version 3)



How the Solution Works: Demo

We'll cover the following solution components as part of our demo today:

1. Data flow from adapters: Tenable, AWS, Azure, VMWare
2. Dashboard for SMVP Compliance (Security Minimal Viable Product)
3. Dissecting device data, tag values and tag compliance
4. Enforcement Center Action Device Score
5. Vulnerabilities Table
6. Enforcement Center Action Vulnerabilities Score
7. Vulnerabilities Instance Table
8. Enforcement Center Action HVERS score
9. Enforcement Center Action for SNOW/Jira ticket generation
10. Enforcement Center Action for ticket update / Query for autoremediation
11. Exceptions, false positives
12. HVERS Dashboard

Dashboards

Add Dashboard

Search

Favorites
- Axonius Dashboard
- My Dashboard

Public
- UWVM
  - On-Boarded Schools Status
  - Risk Based Vulnerability ...
  - School Status Dashboard
  - UVWM HVERS
  - Vulnerability Tickets
- HUIT
  - HUIT Security Requiremen...
  - Tagging Status for HUIT
- Demo
- Axonius Dashboard

Shared
- All Vulnerabilities
- HVERS - Vulnerabilities

Axonius Dashboard

Add Chart

System Lifecycle

Cycle	2025-05-17 19:00:00 - 2025-05-17 21:00:31
Duration	02:00:31
Next Cycle	2025-05-18 19:00:00

Discovery Log

Latest Discoveries	Started	Completed	Duration
	May 17, 19:00	May 17, 21:00	2hr31sec
	May 16, 19:00	May 16, 21:00	2hr36sec
	May 15, 19:00	May 15, 21:10	2hr 10min 10sec
	May 14, 19:00	May 14, 21:02	2hr 2min 6sec
	May 13, 19:00	May 13, 21:05	2hr 5min 2sec

Adapter Connections Status

Opsview	1		
CSV	3		
CrowdStrike Falcon Dis...	1		
Druva Cloud Platform	1		
Amazon Web Services ...	11		
Atlassian (formerly Atla...	2		
Axonius Users	1		
Checkmarx SAST	1		
Total 33	5	1	70

Device Discovery

CrowdStrike Falcon	35,238 (36,258)
ServiceNow	18,159 (18,280)
Microsoft Active Directory (AD)	15,194 (15,269)
Microsoft Endpoint Configuration Manager (MECM) (formerly SCCM)	11,558 (11,640)

User Discovery

Microsoft Active Directory (AD)	139,481 (140,266)
Atlassian (formerly Atlassian Jira Software)	126,860 (126,971)
Jamf Pro	10,427
Amazon Web Services (AWS)	2,227 (2,233)

Stop Discovery

Adapters

Adapters Fetch History › | Adapter Connections › | Create New Adapter

Search Adapters... | Search Categories... | Search Asset Type...

Configured Adapters (33 of 1128)

Bulk Set Advanced Settings

Amazon Web Services (AWS)
Devices | Users | Vulnerabiliti... +22
Cloud Infra 11

Atlassian (formerly Atlassian Jira Software)
Users | Roles | Groups | Accou...
DevOps | SaaS Management 2

Axonius Users
Users | Roles
ITAM/ITSM 1

Checkmarx SAST
Devices | Users | Business Applica...
AppSec 1

CrowdStrike Falcon
Devices | Users | Vulnerabilitie... +3
EDR/EPP | VA Tool | SaaS Manag... 1

CrowdStrike Falcon Discover
Devices | Users | Software
Networking 1

CSV
Devices | Users | Vulnerabilitie... +3
CMDB 3

Druva Cloud Platform
Devices | Users
DLP 1

F5 BIG-IP iControl
Devices | Domains & URLs | Co... +2
Networking 1

Jamf Pro
Devices | Users | Software | Ac...
MDM/EMM | SaaS Management 1

LogicMonitor
Devices
Infra Monitoring 1

Microsoft Active Directory (AD)
Devices | Users | Groups | ... +4
Directory | IAM 2

Microsoft Azure
Devices | Vulnerabilities | Role... +19
Cloud Infra 1

Microsoft Endpoint Configuration Manager...
Devices | Users | Software
Config/Patch Mgmt 1

Opsview
Devices
Infra Monitoring | RMM 1

Oracle Cloud
Devices | Users | Groups | ... +4

Orca Cloud Visibility Platform
Devices | Users | Vulnerabiliti... +22

PagerDuty
Users | Tickets

Proxmox Virtual Environment (VE)
Devices

Qualys Cloud Platform
Devices | Users | Vulnerabilitie... +3

11

Cloud Infra

Search Settings

Adapter Profile

If the source for an adapter connection is only accessible by an internal network, you must set the relevant Gateway Connection as part of the Adapter Connection settings.

Description

Learn More | Run Adapter Cleanup

Amazon Web Services (AWS) includes a broad set of global cloud based products. It supports EC2, ECS, EKS, IAM, EBS, ELB, RDS, S3, FSx, VPC, Workspaces, Lambda and Route 53

Asset Type

Devices Users Vulnerabilities Software Roles Groups Cloud Security Exposures Compute Services Application Services Networks Load Balancers Databases Containers Object Storage
Network Services File Systems Accounts/Tenants Serverless Functions Disks Compute Images Secrets Certificates Network/Firewall Rules Alerts/Incidents Configurations

Search

All Connections 11

Connection Status	Connection Label	Connection ID	Gateway Name	AWS Access Key ID	Proxy	Use instance profile (attached role)
Successfully connected						No
Successfully connected						Yes
Successfully connected						Yes
Successfully connected						Yes
Successfully connected						Yes
Successfully connected						Yes
Successfully connected						Yes
Successfully connected						No
Successfully connected						No

15

VA Tool

Search Settings

Adapter Profile

If the source for an adapter connection is only accessible by an internal network, you must set the relevant Gateway Connection as part of the Adapter Connection settings.

Description

Learn More | Run Adapter Cleanup

Tenable.sc (formerly SecurityCenter) consolidates and evaluates vulnerability data, prioritizing security risks.

Asset Type

Devices Vulnerabilities Software Alerts/Incidents

Search

All Connections 15

Connection Status	Connection Label	Connection ID	Gateway Name	Tenable.sc domain	User Name	Verify SSL	HTTPS Proxy	Ac
Successfully connected								6c
Successfully connected								bd
Successfully connected								38
Successfully connected								c8
Successfully connected								ac
Successfully connected								f8b
Successfully connected								fba
Successfully connected								cd
Successfully connected								e9

12

Virtualization

Search Settings

Adapter Profile

If the source for an adapter connection is only accessible by an internal network, you must set the relevant Gateway Connection as part of the Adapter Connection settings.

Description

Learn More | Run Adapter Cleanup

VMware ESXi is an enterprise-class, type-1 hypervisor for deploying and serving virtual computers. VMware vSphere is VMware's cloud computing virtualization platform.

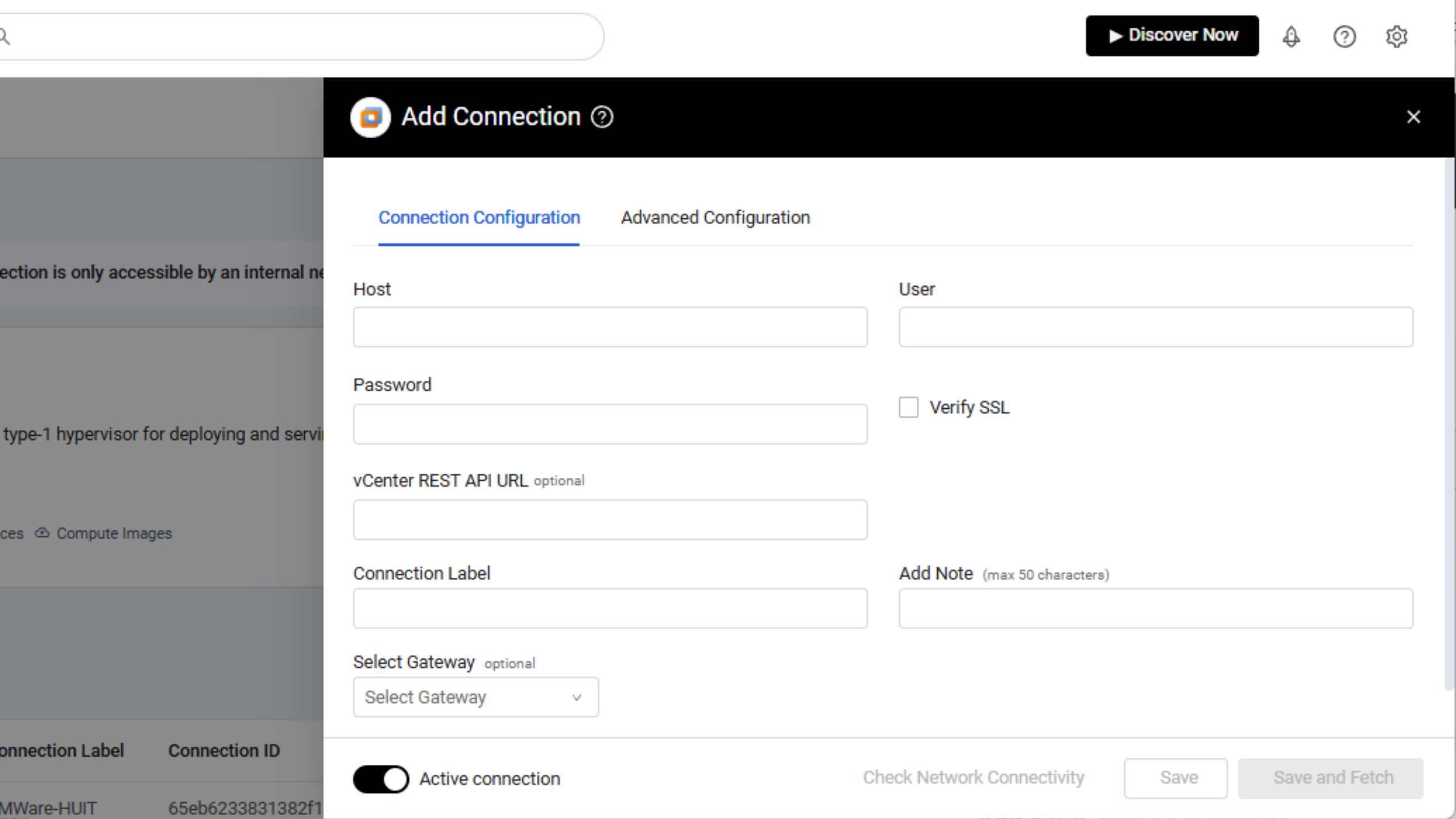
Asset Type

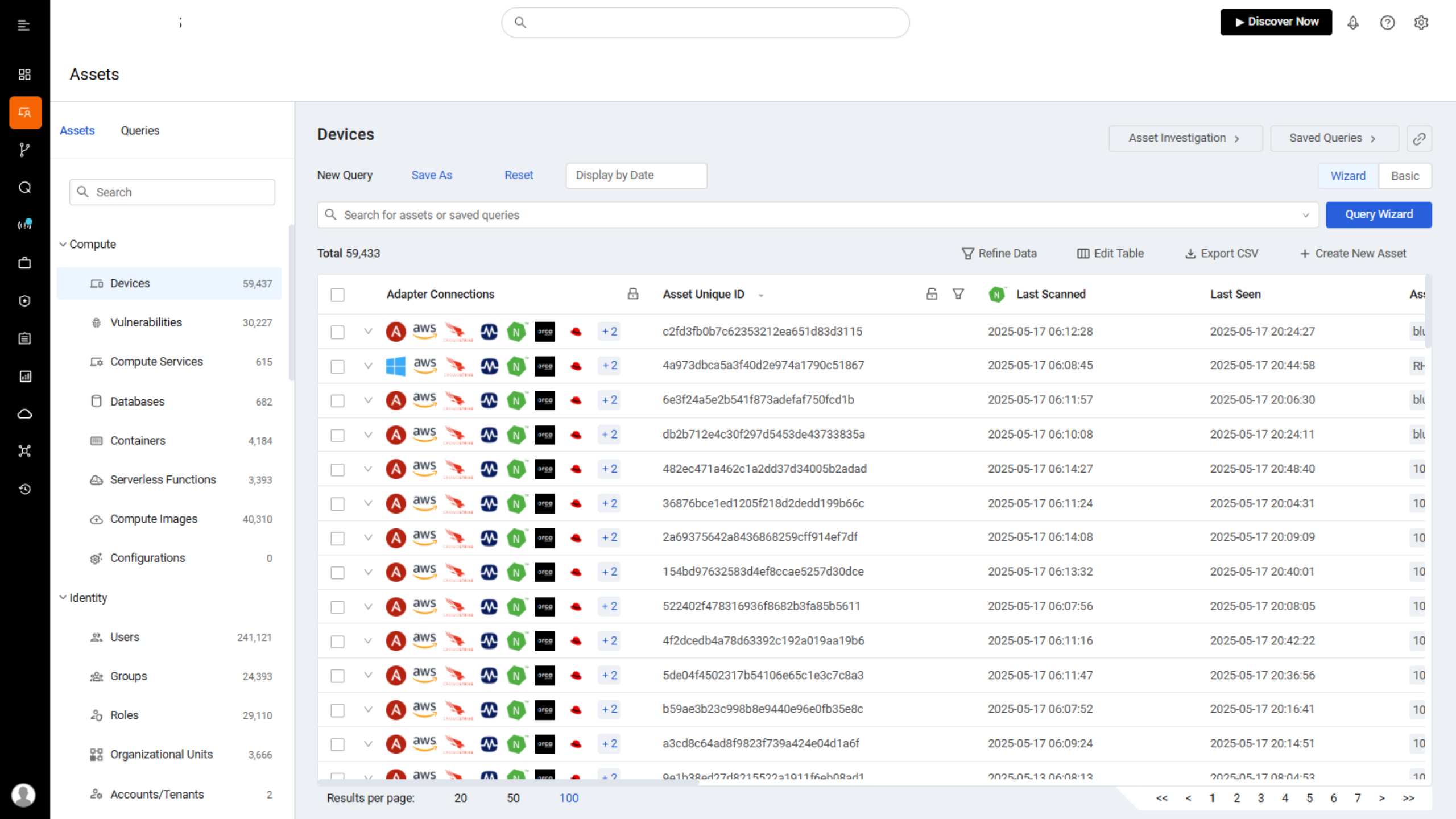
Devices Users Compute Services Compute Images

Search

All Connections 12

Connection Status	Connection Label	Connection ID	Gateway Name	Host	User	Verify SSL	vC
Successfully connected							
Successfully connected							
Successfully connected							
Successfully connected							
Successfully connected							
Successfully connected							
Successfully connected							
Successfully connected							
Successfully connected							


Discover Now
ection is only accessible by an internal ne
type-1 hypervisor for deploying and servi
ces
Compute Images
onnection Label
Connection ID
MWare-HUIT
65eb6233831382f1
Add Connection
Connection Configuration
Advanced Configuration
Host
User
Password
Verify SSL
vCenter REST API URL optional
Connection Label
Add Note (max 50 characters)
Select Gateway optional
Select Gateway
Active connection
Check Network Connectivity
Save
Save and Fetch


Discover Now
Assets
Assets
Queries
Search
Compute
Devices 59,437
Vulnerabilities 30,227
Compute Services 615
Databases 682
Containers 4,184
Serverless Functions 3,393
Compute Images 40,310
Configurations 0
Identity
Users 241,121
Groups 24,393
Roles 29,110
Organizational Units 3,666
Accounts/Tenants 2
Devices
Asset Investigation
Saved Queries
New Query
Save As
Reset
Display by Date
Wizard
Basic
Search for assets or saved queries
Query Wizard
Total 59,433
Refine Data
Edit Table
Export CSV
Create New Asset
Adapter Connections
Asset Unique ID
Last Scanned
Last Seen
+2
c2fd3fb0b7c62353212ea651d83d3115 2025-05-17 06:12:28 2025-05-17 20:24:27
4a973dbca5a3f40d2e974a1790c51867 2025-05-17 06:08:45 2025-05-17 20:44:58
6e3f24a5e2b541f873adefaf750fcd1b 2025-05-17 06:11:57 2025-05-17 20:06:30
db2b712e4c30f297d5453de43733835a 2025-05-17 06:10:08 2025-05-17 20:24:11
482ec471a462c1a2dd37d34005b2adad 2025-05-17 06:14:27 2025-05-17 20:48:40
36876bce1ed1205f218d2dedd199b66c 2025-05-17 06:11:24 2025-05-17 20:04:31
2a69375642a8436868259cff914ef7df 2025-05-17 06:14:08 2025-05-17 20:09:09
154bd97632583d4ef8ccae5257d30dce 2025-05-17 06:13:32 2025-05-17 20:40:01
522402f478316936f8682b3fa85b5611 2025-05-17 06:07:56 2025-05-17 20:08:05
4f2dcedb4a78d63392c192a019aa19b6 2025-05-17 06:11:16 2025-05-17 20:42:22
5de04f4502317b54106e65c1e3c7c8a3 2025-05-17 06:11:47 2025-05-17 20:36:56
b59ae3b23c998b8e9440e96e0fb35e8c 2025-05-17 06:07:52 2025-05-17 20:16:41
a3cd8c64ad8f9823f739a424e04d1a6f 2025-05-17 06:09:24 2025-05-17 20:14:51
Results per page: 20 50 100
<< < 1 2 3 4 5 6 7 > >>

Linux

Linux Red Hat 8.10

Last seen 27 minute...

Search

- Asset Fields
  - All Fields
  - Aggregated Fields
  - Preferred Fields
  - Tags
- Tables
- Adapter Connections
  - Amazon Web Services (AWS...
  - CrowdStrike Falcon - CS Falc...
  - EC: Artifacts
  - LogicMonitor - LogicMonitor
  - Orca Cloud Visibility Platfor...
  - Red Hat Automation Controll...
  - Red Hat Satellite - RHEL Sate...
  - Tenable Nessus - Nessus Ma...
  - Tenable.sc (SecurityCenter) -...
  - Wiz.io - Harvard-Wiz-PoV
  - Custom Data

All Fields

Search | Adapter Connections | Reset

Total 546 | Edit Table

Field Name	Value	Adapter Connections
Asset Unique ID	c2fd3fb0b7c62353212ea651d83d3115	
Asset Unique ID History	New Asset Unique ID: 9f50b1ea7b2de862ba5da2a9... Change Time: 2024-06-14 15:05:40 Change Reason: Asset Unlink Change Details: The +9	
Asset Short Unique ID	3271376816	
Asset Name	[redacted]	+4
Host Name	[redacted]	+4
Internal Axon Hash	0f7be3e087a11d6f9f81bb57739febcd 84c2d1b7ace4bc4780926e0845600232 +7	+4
Description	imported Automatically discovered	
First Seen	2018-06-18 13:28:36 (2525 Days)	+2
Last Seen	2025-05-17 21:08:32 (0 Days)	+3
Is Latest Last Seen (per adapter)	Yes	+3
Last Seen (agents)	2025-05-17 20:24:27 (0 Days) 2025-05-17 18:35:08 (0 Days) +1	
Fetch Time	2025-05-17 21:11:17 (0 Days)	+4
From Last Fetch	Yes	+4
Not Fetched Count	0	+4
First Fetch Time	2024-06-15 14:26:10 (336 Days)	+4
Public IPs	[redacted]	
Open Ports	Protocol: TCP Port Number: 22 +11	
Network Interfaces	[redacted]	+3
OS: Type	Linux	+2

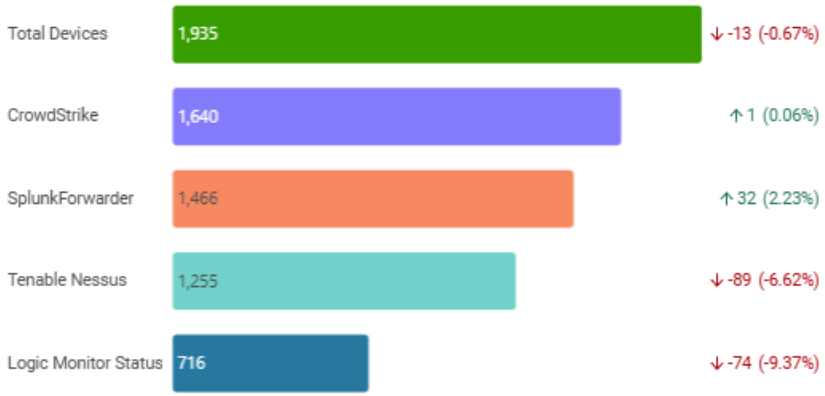
Results per page: 20 50 100

<< < 1 2 3 4 5 6 > >>

SMVP Compliance Status

Filter | Add Chart

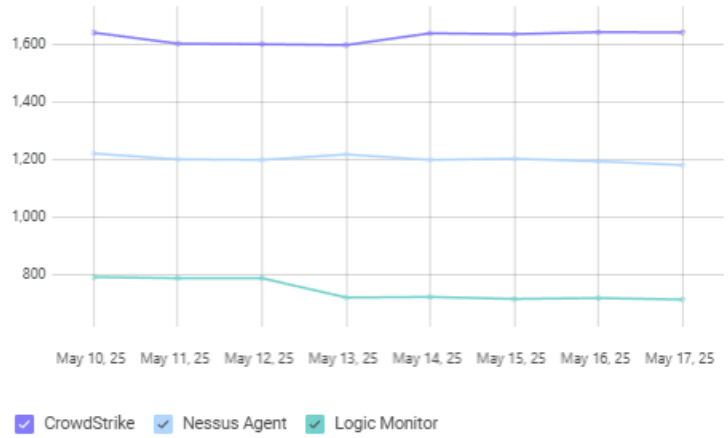
SMVP Compliance Status



143 (-2%) since 7 days ago

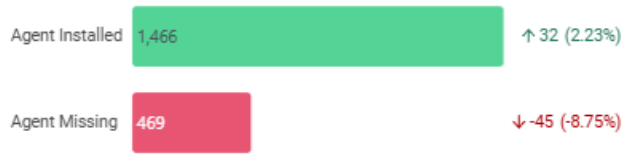
10/page 1 / 1

SMVP Compliance Status Trend



Date range: May 10, 2025 - May 17, 2025

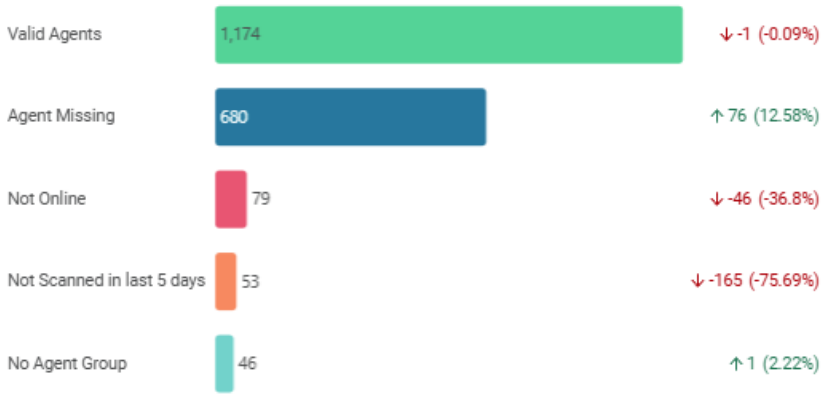
SplunkForwarder Agent Status



13 (-0.67%) since 7 days ago

10/page 1 / 1

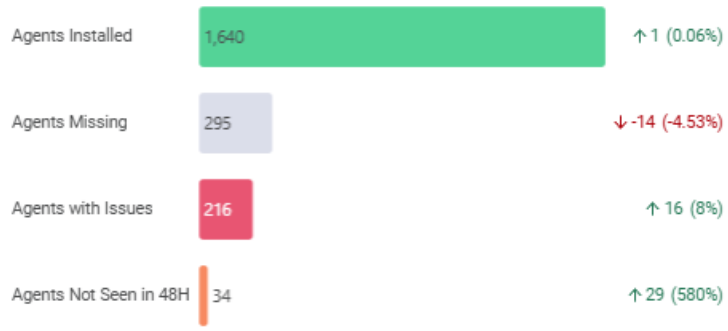
Nessus Agent Status (status' overlap)



135 (-6.23%) since 7 days ago

10/page 1 / 1

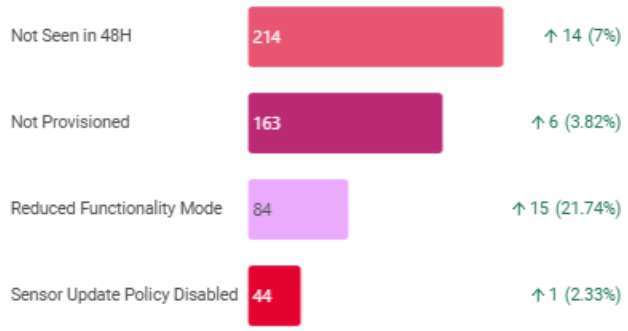
CrowdStrike Agent Status



32 (+1.49%) since 7 days ago

10/page 1 / 1

CrowdStrike Issues



36 (+7.68%) since 7 days ago

10/page 1 / 1

Search

Favorites
- Axonius Dashboard
- My Dashboard

Public
- UWVM
  - On-Boarded Schools Status
  - Risk Based Vulnerability M...
  - School Status Dashboard
  - UVWM HVERS
  - Vulnerability Tickets
- HUIT
  - HUIT Security Requirement...
  - Tagging Status for HUIT
- Demo
- Axonius Dashboard

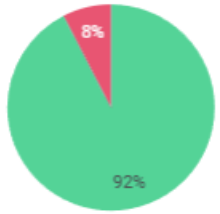
Shared
- All Vulnerabilities
- HVERS - Vulnerabilities
- SMVP Compliance Status
- Tagging Metrics

Private

Tagging Metrics

Filter | Add Chart

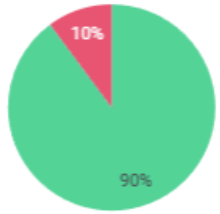
Use of Hosted_By Tag



Hosted_By Tags	1,789 (92%)
Hosted_By Tag Missing	146 (8%)

Total 1935 (2 items)

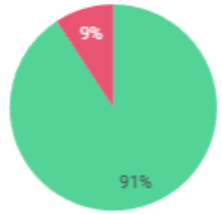
Use of Environment Tag



Environment Tags	1,739 (90%)
Environment Tag Missing	196 (10%)

Total 1935 (2 items)

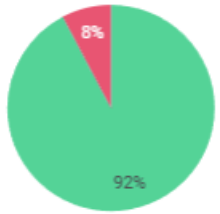
Use of Product Tag



Product Tag	1,757 (91%)
Product Tag Missing	178 (9%)

Total 1935 (2 items)

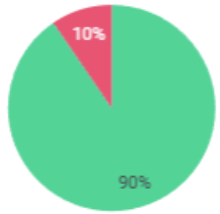
Use of Data_Class Tag



Data_Class Tags	1,786 (92%)
Data_Class Tag Missing	149 (8%)

Total 1935 (2 items)

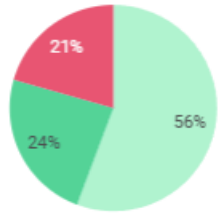
Use of Criticality Tag



Criticality Tags	1,751 (90%)
Criticality Tag Missing	184 (10%)

Total 1935 (2 items)

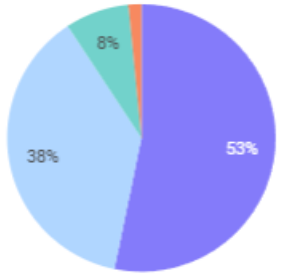
Internet Exposure Tags



Not Internet Facing	1,078 (56%)
Internet Facing	459 (24%)
Not Tagged	398 (21%)

Total 1935 (3 items)

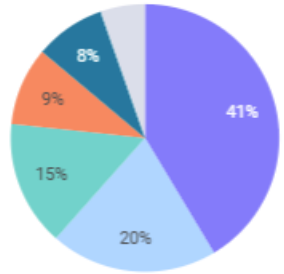
Data_Class Values



NONLEVEL4	1,030 (53%)
LEVEL4	726 (38%)
No Value	149 (8%)
L4	30 (2%)

Total 1935 (4 items)

Criticality Tag Values



NON-CRITICAL	801 (41%)
IMPORTANT	389 (20%)
CRITICAL	293 (15%)
No Value	183 (9%)
FOUNDATIONAL / LIFE SAFETY	164 (8%)
MISSION CRITICAL	104 (5%)

Total 1934 (6 items)

Assets

Assets Queries

Search

- Compute
  - Devices 59,437
  - Vulnerabilities 31,009
  - Compute Services 615
  - Databases 682
  - Containers 4,184
  - Serverless Functions 3,393
  - Compute Images 40,310
  - Configurations 0
- Identity
  - Users 241,121
  - Groups 24,393
  - Roles 29,110
  - Organizational Units 3,666
  - Accounts/Tenants 2

Devices

Asset Investigation › | Saved Queries ›

New Query | Save As | Reset | EC Actions | Display by Date | Wizard | Basic

({{QueryID=67af5bcf39e758bbc2e82605}}) and (("adapters_data.gui.custom_internet_facing" == ({"$exists":true,"$ne":null}))) and ("specific_data.data.axonius_risk_score" > 0)

Query Wizard

Total 1,101

Refine Data | Edit Table | Export CSV | + Create New Asset

Preferred OS: Type and Distribution	Axonius Risk Score	Criticality_Tag	Data_Class_Tag	Internet_facing
Linux Red Hat 8.10	7.00	IMPORTANT	LEVEL4	Yes
Linux Red Hat 8.10	5.00	IMPORTANT	NONLEVEL4	Yes
Linux Red Hat 8.10	2.00	NON-CRITICAL	LEVEL4	No
Linux Red Hat 8.10	2.00	NON-CRITICAL	LEVEL4	No
Linux Red Hat 8.10	2.00	IMPORTANT	LEVEL4	No
Linux Red Hat 8.10	5.00	IMPORTANT	NONLEVEL4	Yes
Windows Server 2019	5.00	NON-CRITICAL	NONLEVEL4	Yes
Windows Server 2019	5.00	NON-CRITICAL	NONLEVEL4	Yes
Windows Server 2019	8.00	CRITICAL	NONLEVEL4	Yes
Windows Server 2019	8.00	CRITICAL	NONLEVEL4	Yes
Windows Server 2016	5.00	NON-CRITICAL	NONLEVEL4	Yes
Windows Server 2016	5.00	NON-CRITICAL	NONLEVEL4	Yes
Windows Server 2016	10.00	CRITICAL	LEVEL4	Yes
Windows Server 2016	8.00	CRITICAL	NONLEVEL4	Yes

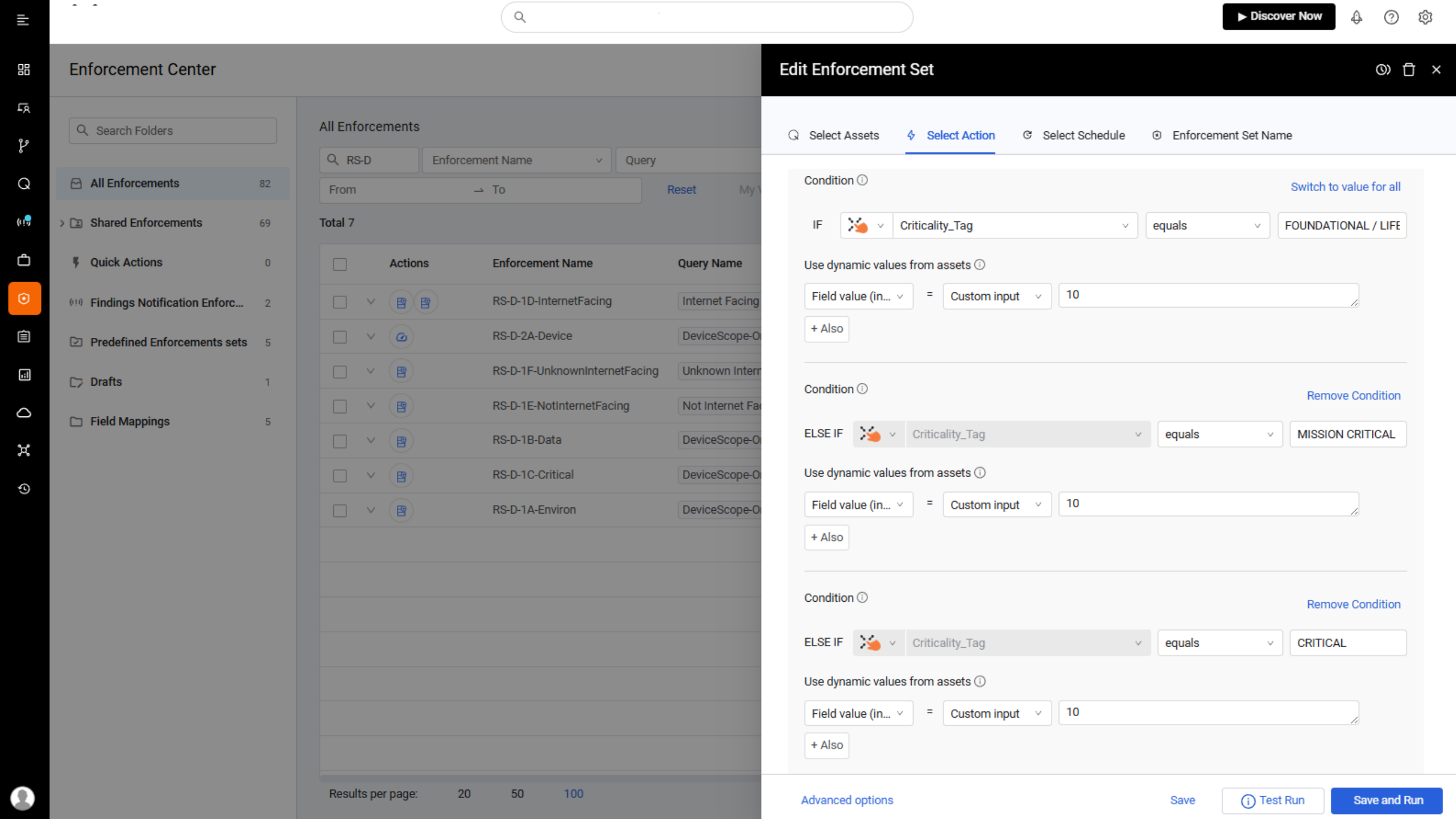
Results per page: 20 50 100

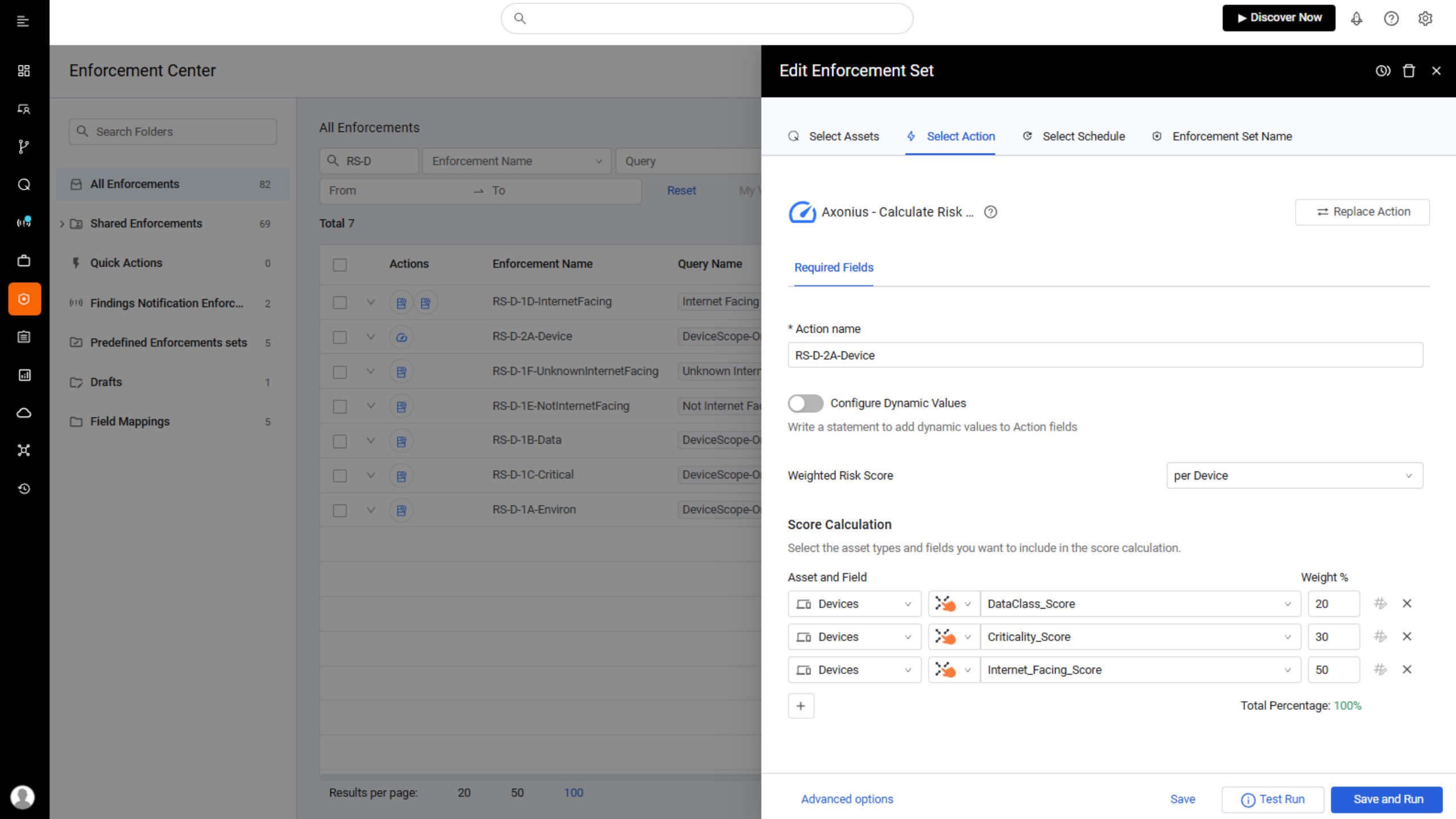
<< < 1 2 3 4 5 6 7 > >>

Total 7

Import

Actions	Enforcement Name	Query Name	Scheduling Type	Last Run Status	Last Run
	RS-D-1D-InternetFacing	Internet Facing for Onboarded Schools	Every 12 hours	Completed	2025-05-17 20:00:23
	RS-D-2A-Device	DeviceScope-Onboarded Schools	Every 1 days; at 06:00	Partially	2025-05-17 02:00:18
	RS-D-1F-UnknownInternetFacing	Unknown Internet Facing Devices for Onboarded Schools	Every 12 hours	Completed	2025-05-17 20:00:21
	RS-D-1E-NotInternetFacing	Not Internet Facing Devices for Onboarded Schools	Every 12 hours	Completed	2025-05-17 20:00:21
	RS-D-1B-Data	DeviceScope-Onboarded Schools	Every 1 days; at 05:15	Completed	2025-05-17 01:15:03
	RS-D-1C-Critical	DeviceScope-Onboarded Schools	Every 1 days; at 05:20	Completed	2025-05-17 01:20:02
	RS-D-1A-Environ	DeviceScope-Onboarded Schools	Every 1 days; at 05:05	Completed	2025-05-17 01:05:02


Discover Now
Enforcement Center
Search Folders
All Enforcements 82
Shared Enforcements 69
Quick Actions 0
Findings Notification Enforc... 2
Predefined Enforcements sets 5
Drafts 1
Field Mappings 5
All Enforcements
RS-D
Enforcement Name
Query
From
To
Reset
Total 7
Actions
Enforcement Name
Query Name
RS-D-1D-InternetFacing
Internet Facing
RS-D-2A-Device
RS-D-1F-UnknownInternetFacing
RS-D-1E-NotInternetFacing
RS-D-1B-Data
RS-D-1C-Critical
RS-D-1A-Environ
Results per page: 20 50 100
Edit Enforcement Set
Select Assets
Select Action
Select Schedule
Enforcement Set Name
Condition
Switch to value for all
IF
Criticality_Tag
equals
FOUNDATIONAL / LIFE
Use dynamic values from assets
Field value (in...
=
Custom input
10
+ Also
Condition
Remove Condition
ELSE IF
Criticality_Tag
equals
MISSION CRITICAL
Use dynamic values from assets
Field value (in...
=
Custom input
10
+ Also
Condition
Remove Condition
ELSE IF
Criticality_Tag
equals
CRITICAL
Use dynamic values from assets
Field value (in...
=
Custom input
10
+ Also
Advanced options
Save
Test Run
Save and Run


Discover Now
Enforcement Center
Search Folders
All Enforcements 82
Shared Enforcements 69
Quick Actions 0
Findings Notification Enforc... 2
Predefined Enforcements sets 5
Drafts 1
Field Mappings 5
All Enforcements
RS-D
Enforcement Name
Query
From
To
Reset
Total 7
Actions
Enforcement Name
Query Name
RS-D-1D-InternetFacing
Internet Facing
RS-D-2A-Device
RS-D-1F-UnknownInternetFacing
RS-D-1E-NotInternetFacing
RS-D-1B-Data
RS-D-1C-Critical
RS-D-1A-Environ
Results per page: 20 50 100
Edit Enforcement Set
Select Assets
Select Action
Select Schedule
Enforcement Set Name
Axonius - Calculate Risk ...
Replace Action
Required Fields
* Action name
RS-D-2A-Device
Configure Dynamic Values
Write a statement to add dynamic values to Action fields
Weighted Risk Score
per Device
Score Calculation
Select the asset types and fields you want to include in the score calculation.
Asset and Field
Weight %
Devices
DataClass_Score
20
Devices
Criticality_Score
30
Devices
Internet_Facing_Score
50
Total Percentage: 100%
Advanced options
Save
Test Run
Save and Run

Assets

Assets | Queries

Search

- Compute
  - Devices 59,437
  - Vulnerabilities 31,009
  - Compute Services 615
  - Databases 682
  - Containers 4,184
  - Serverless Functions 3,393
  - Compute Images 40,310
  - Configurations 0
- Identity
  - Users 241,121
  - Groups 24,393
  - Roles 29,110
  - Organizational Units 3,666
  - Accounts/Tenants 2

Vulnerabilities

Repository › | Exclusion Rules › | Saved Queries ›

New Query | Save As | Reset | EC Actions | Display by Date | Wizard | Basic

{"vulnerabilities":"(\"specific_data.data.axonius_risk_score\" > 9)","devices":""}

Query Wizard

Total 443 | Unique Device Count 2,569 | Last updated: 2025-05-17 22:35:29

Refine Data | Edit Table | Export CSV

Vuln ID	Axonius Risk Score	Device Count	Tenable Vulnerability: Plugin	
Plugin-157118	9.19	5	CentOS 7 : httpd (RHSA-2022:0143)	Critic
Plugin-181349	9.40	5	Mozilla Firefox < 117.0.1	High
Plugin-182134	9.40	5	Mozilla Firefox < 118.0.1	High
Plugin-187705	9.40	5	Rocky Linux 8 : webkit2gtk3 (RLSA-2023:7716)	High
Plugin-201085	9.55	5	OpenSSL 3.0.0 < 3.0.15 Vulnerability	Critic
Plugin-201351	9.50	5	Canonical Ubuntu Linux SEoL (16.04.x)	Critic
Plugin-205456	9.29	5	KB5041160: Windows Server 2022 / Azure Stack HCI 22...	Critic
Plugin-206897	9.40	5	KB5042881: Windows Server 2022 / Azure Stack HCI 22...	Critic
Plugin-209245	9.55	5	Oracle MySQL Connectors (October 2024 CPU)	Critic
Plugin-210866	9.40	5	KB5046616: Windows Server 2022 / Azure Stack HCI 22...	Critic
Plugin-234293	9.90	5	RHEL 8 : tomcat (RHSA-2025:3683)	Critic
Plugin-234649	9.05	5	RHEL 7 : postgresql (RHSA-2025:3978)	High
Plugin-73756	9.50	5	Microsoft SQL Server Unsupported Version Detection (re...	Critic

Results per page: 20 50 100

<< < 1 2 3 4 5 > >>

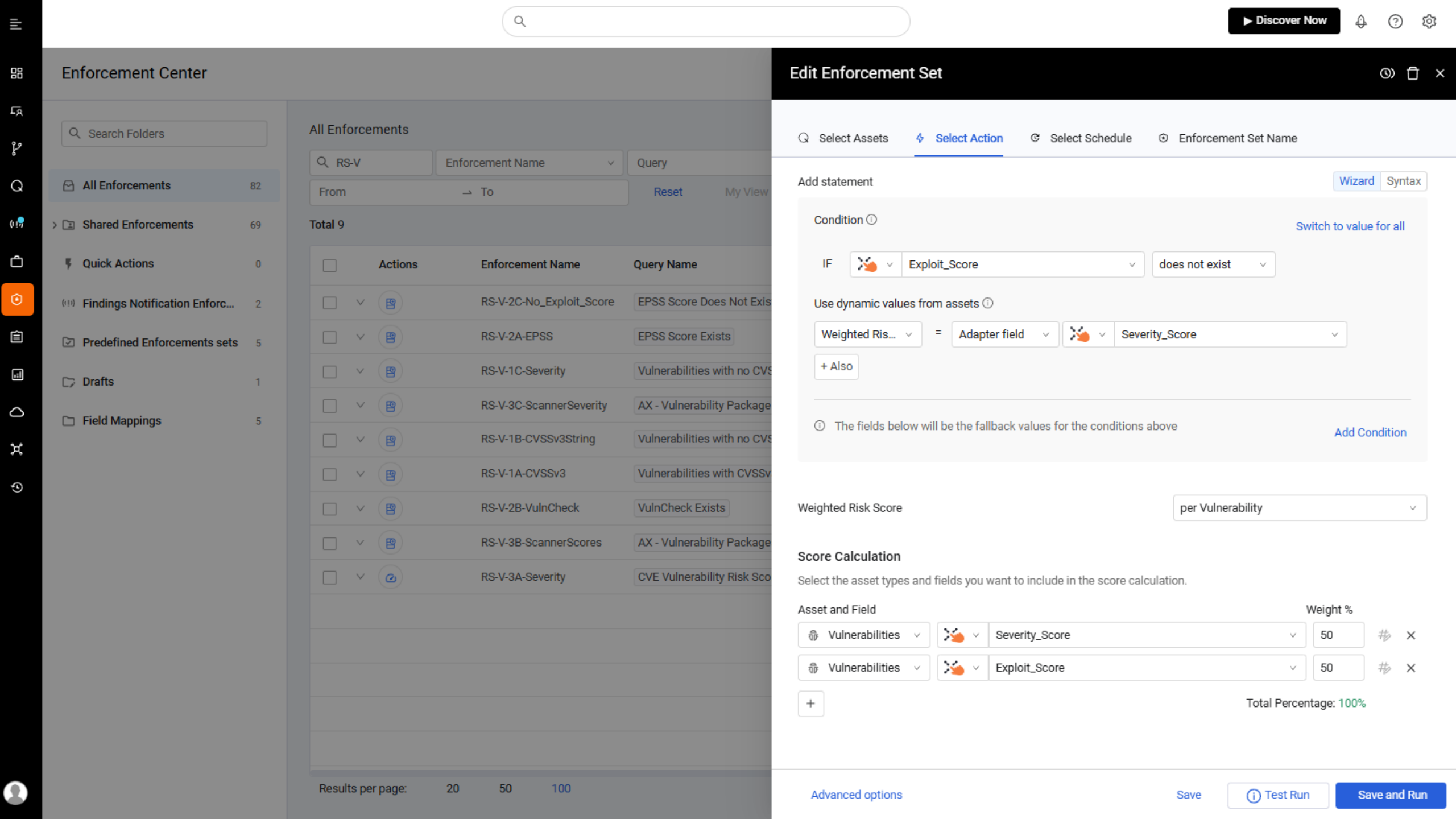
Total 9

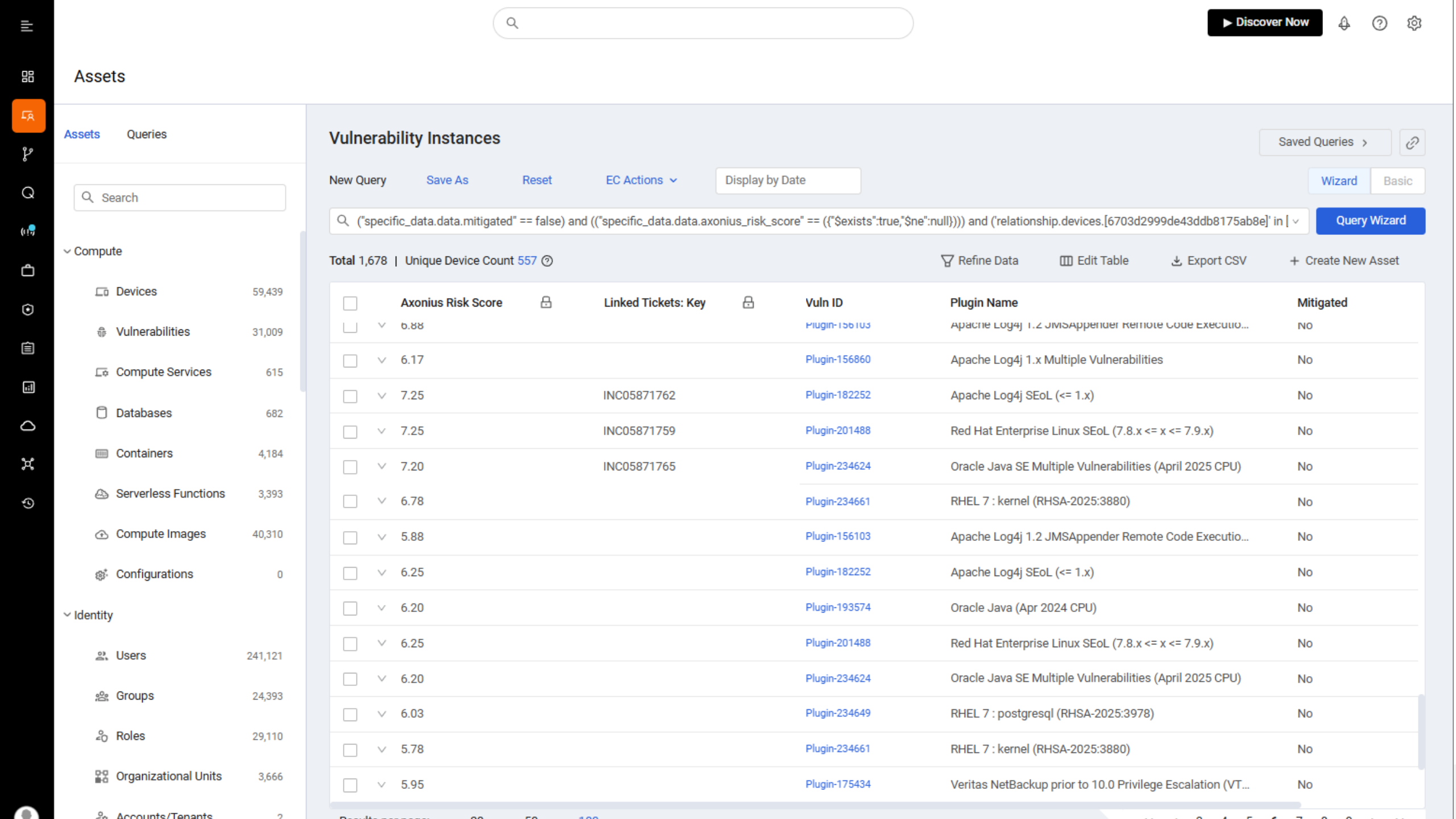
Import

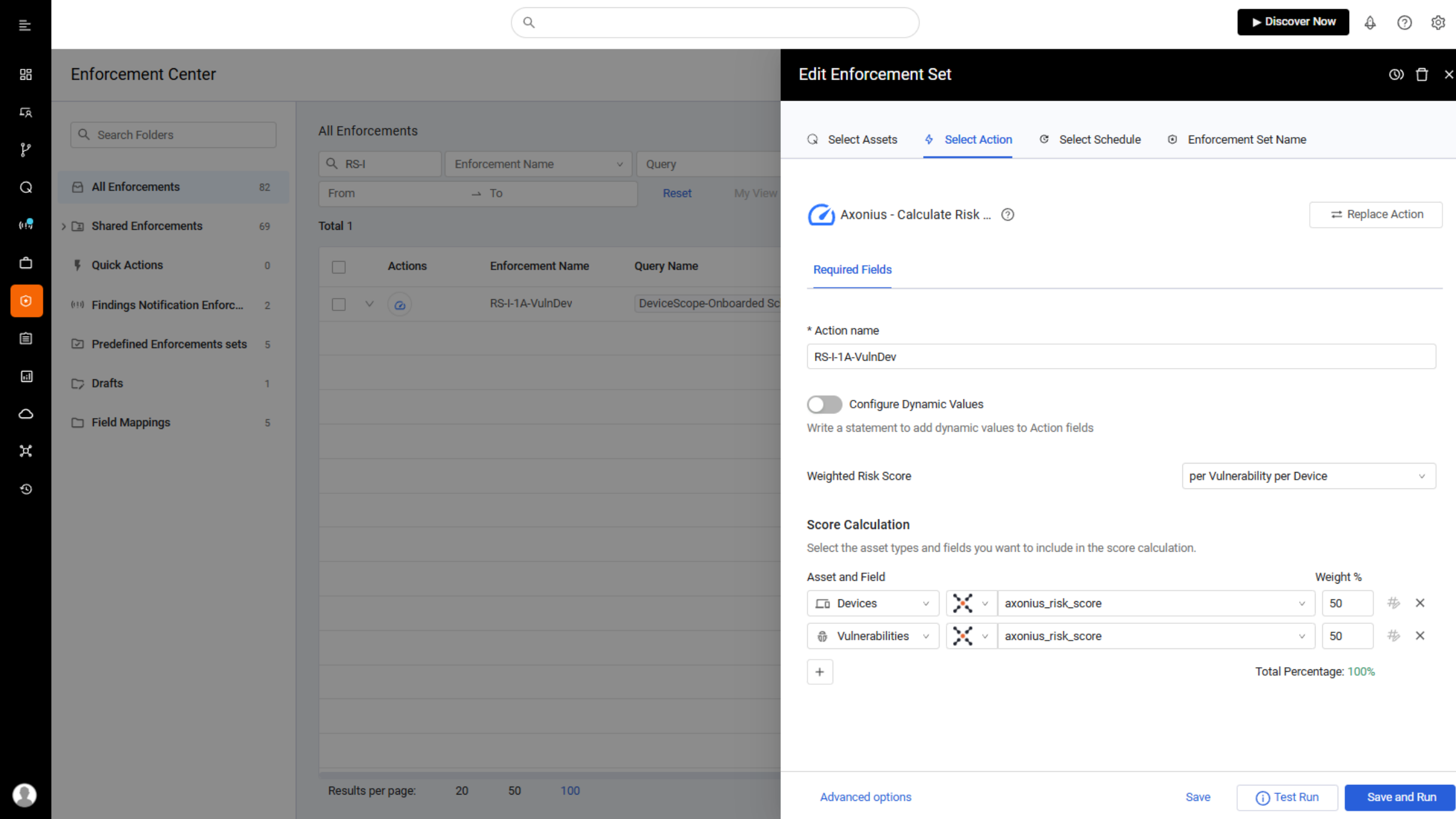
Actions	Enforcement Name	Query Name	Scheduling Type	Last Run Status	Last Run	Next Run
	RS-V-2C-No_Exploit_Score	EPSS Score Does Not Exist	Every 3 hours	Completed	2025-05-17 20:00:19	2025-05-17 23:00:0(
	RS-V-2A-EPSS	EPSS Score Exists	Every 8 hours	Completed	2025-05-17 20:00:41	2025-05-18 04:00:0(
	RS-V-1C-Severity	Vulnerabilities with no CVSSv3 Score or String	Every 6 hours	Completed	2025-05-17 20:00:26	2025-05-18 02:00:0(
	RS-V-3C-ScannerSeverity	AX - Vulnerability Package - No CVE List	Every 12 hours	Completed	2025-05-17 20:00:18	2025-05-18 08:00:0(
	RS-V-1B-CVSSv3String	Vulnerabilities with no CVSSv3 Score	Every 6 hours	Completed	2025-05-17 20:00:25	2025-05-18 02:00:0(
	RS-V-1A-CVSSv3	Vulnerabilities with CVSSv3 scores	Every 6 hours	Partially	2025-05-17 20:00:38	2025-05-18 02:00:0(
	RS-V-2B-VulnCheck	VulnCheck Exists	Every 3 hours	Completed	2025-05-17 20:00:21	2025-05-17 23:00:0(
	RS-V-3B-ScannerScores	AX - Vulnerability Packages	Every 1 days; at 22:45	Partially	2025-05-17 18:45:11	2025-05-18 18:45:0(
	RS-V-3A-Severity	CVE Vulnerability Risk Score Scope	Every 1 days; at 22:30	Partially	2025-05-17 18:30:34	2025-05-18 18:30:0(

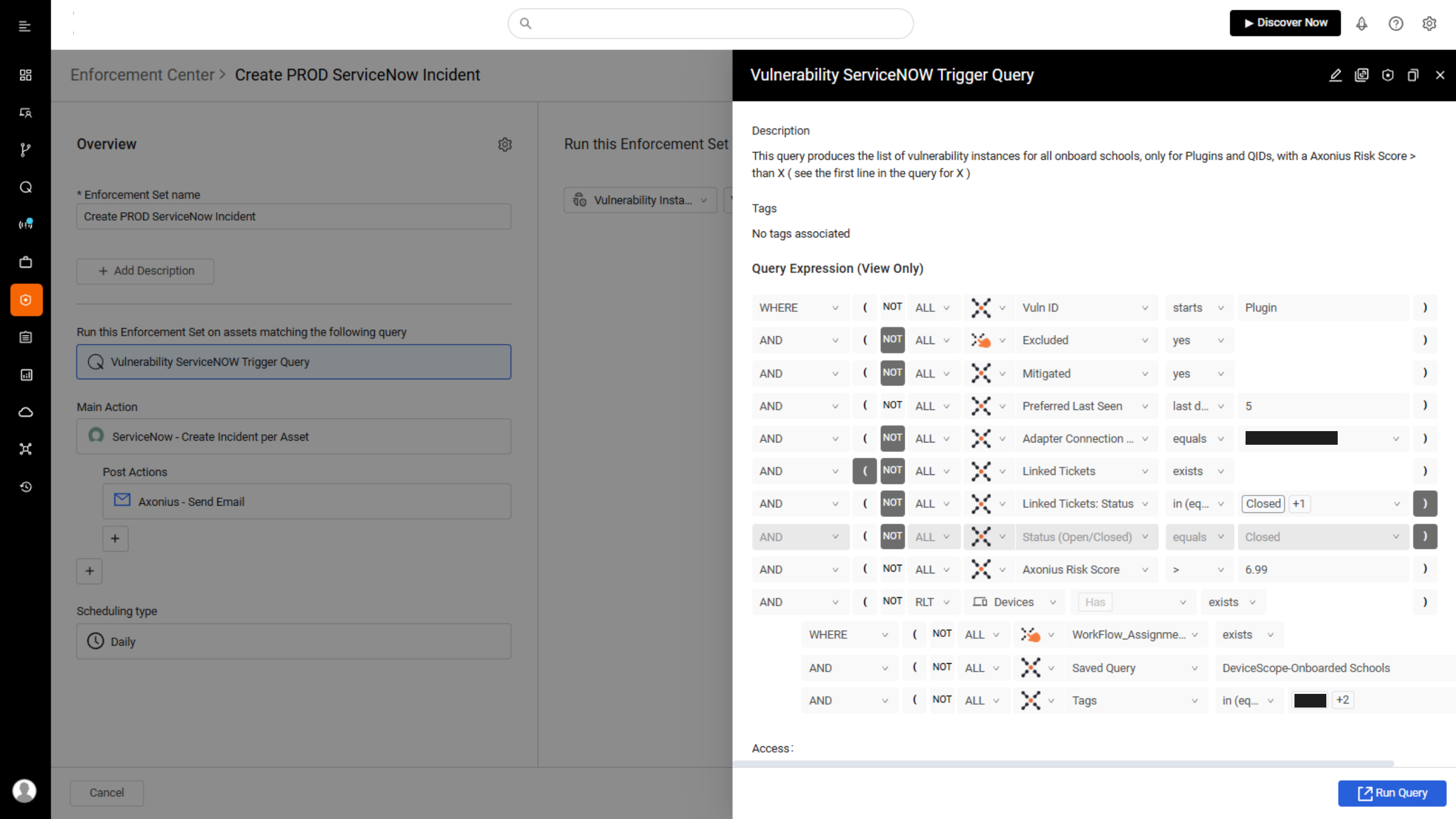
Results per page: 20 50 100

<< < 1 > >>


Discover Now
Enforcement Center
Search Folders
All Enforcements 82
Shared Enforcements 69
Quick Actions 0
Findings Notification Enforc... 2
Predefined Enforcements sets 5
Drafts 1
Field Mappings 5
All Enforcements
RS-V
Enforcement Name
Query
From
To
Reset
My View
Total 9
Actions
Enforcement Name
Query Name
RS-V-2C-No_Exploit_Score
EPSS Score Does Not Exis
RS-V-2A-EPSS
EPSS Score Exists
RS-V-1C-Severity
Vulnerabilities with no CVS
RS-V-3C-ScannerSeverity
AX - Vulnerability Package
RS-V-1B-CVSSv3String
Vulnerabilities with no CVS
RS-V-1A-CVSSv3
Vulnerabilities with CVSSv
RS-V-2B-VulnCheck
VulnCheck Exists
RS-V-3B-ScannerScores
AX - Vulnerability Package
RS-V-3A-Severity
CVE Vulnerability Risk Sco
Results per page: 20 50 100
Edit Enforcement Set
Select Assets
Select Action
Select Schedule
Enforcement Set Name
Add statement
Wizard
Syntax
Condition
Switch to value for all
IF
Exploit_Score
does not exist
Use dynamic values from assets
Weighted Ris...
=
Adapter field
Severity_Score
+ Also
The fields below will be the fallback values for the conditions above
Add Condition
Weighted Risk Score
per Vulnerability
Score Calculation
Select the asset types and fields you want to include in the score calculation.
Asset and Field
Weight %
Vulnerabilities
Severity_Score
50
Vulnerabilities
Exploit_Score
50
Total Percentage: 100%
Advanced options
Save
Test Run
Save and Run


Discover Now
Assets
Assets
Queries
Search
Compute
Devices 59,439
Vulnerabilities 31,009
Compute Services 615
Databases 682
Containers 4,184
Serverless Functions 3,393
Compute Images 40,310
Configurations 0
Identity
Users 241,121
Groups 24,393
Roles 29,110
Organizational Units 3,666
Vulnerability Instances
Saved Queries
New Query
Save As
Reset
EC Actions
Display by Date
Wizard
Basic
("specific_data.data.mitigated" == false) and (("specific_data.data.axonius_risk_score" == ({"$exists":true,"$ne":null}))) and ('relationship.devices.[6703d2999de43ddb8175ab8e]' in [
Query Wizard
Total 1,678 | Unique Device Count 557
Refine Data
Edit Table
Export CSV
Create New Asset
Axonius Risk Score
Linked Tickets: Key
Vuln ID
Plugin Name
Mitigated
6.88 Plugin-156103 Apache Log4j 1.2 JMSAppender Remote Code Executio... No
6.17 Plugin-156860 Apache Log4j 1.x Multiple Vulnerabilities No
7.25 INC05871762 Plugin-182252 Apache Log4j SEoL (<= 1.x) No
7.25 INC05871759 Plugin-201488 Red Hat Enterprise Linux SEoL (7.8.x <= x <= 7.9.x) No
7.20 INC05871765 Plugin-234624 Oracle Java SE Multiple Vulnerabilities (April 2025 CPU) No
6.78 Plugin-234661 RHEL 7 : kernel (RHSA-2025:3880) No
5.88 Plugin-156103 Apache Log4j 1.2 JMSAppender Remote Code Executio... No
6.25 Plugin-182252 Apache Log4j SEoL (<= 1.x) No
6.20 Plugin-193574 Oracle Java (Apr 2024 CPU) No
6.25 Plugin-201488 Red Hat Enterprise Linux SEoL (7.8.x <= x <= 7.9.x) No
6.20 Plugin-234624 Oracle Java SE Multiple Vulnerabilities (April 2025 CPU) No
6.03 Plugin-234649 RHEL 7 : postgresql (RHSA-2025:3978) No
5.78 Plugin-234661 RHEL 7 : kernel (RHSA-2025:3880) No
5.95 Plugin-175434 Veritas NetBackup prior to 10.0 Privilege Escalation (VT... No


Discover Now
Enforcement Center
Search Folders
All Enforcements 82
Shared Enforcements 69
Quick Actions 0
Findings Notification Enforc... 2
Predefined Enforcements sets 5
Drafts 1
Field Mappings 5
All Enforcements
RS-I
Enforcement Name
Query
From
To
Reset
My View
Total 1
Actions
Enforcement Name
Query Name
RS-I-1A-VulnDev
DeviceScope-Onboarded Sc
Results per page: 20 50 100
Edit Enforcement Set
Select Assets
Select Action
Select Schedule
Enforcement Set Name
Axonius - Calculate Risk ...
Replace Action
Required Fields
* Action name
RS-I-1A-VulnDev
Configure Dynamic Values
Write a statement to add dynamic values to Action fields
Weighted Risk Score
per Vulnerability per Device
Score Calculation
Select the asset types and fields you want to include in the score calculation.
Asset and Field
Weight %
Devices
axonius_risk_score
50
Vulnerabilities
axonius_risk_score
50
Total Percentage: 100%
Advanced options
Save
Test Run
Save and Run


▶ Discover Now
Enforcement Center > Create PROD ServiceNow Incident
Overview
* Enforcement Set name
Create PROD ServiceNow Incident
+ Add Description
Run this Enforcement Set on assets matching the following query
Vulnerability ServiceNOW Trigger Query
Main Action
ServiceNow - Create Incident per Asset
Post Actions
Axonius - Send Email
Scheduling type
Daily
Run this Enforcement Set
Vulnerability Insta...
Cancel
Vulnerability ServiceNOW Trigger Query
Description
This query produces the list of vulnerability instances for all onboard schools, only for Plugins and QIDs, with a Axonius Risk Score > than X (see the first line in the query for X)
Tags
No tags associated
Query Expression (View Only)
WHERE (NOT ALL Vuln ID starts Plugin)
AND (NOT ALL Excluded yes)
AND (NOT ALL Mitigated yes)
AND (NOT ALL Preferred Last Seen last d... 5)
AND (NOT ALL Adapter Connection ... equals [redacted])
AND (NOT ALL Linked Tickets exists)
AND (NOT ALL Linked Tickets: Status in (eq... Closed +1)
AND (NOT ALL Status (Open/Closed) equals Closed)
AND (NOT ALL Axonius Risk Score > 6.99)
AND (NOT RLT Devices Has exists)
WHERE (NOT ALL WorkFlow_Assignme... exists
AND (NOT ALL Saved Query DeviceScope-Onboarded Schools
AND (NOT ALL Tags in (eq... [redacted] +2
Access:
Run Query

Incident
INC05888147

Discuss Save Update and Return Assign to me Resolve

Number	INC05888147	Status	New
* Customer	Axonius API	Impact	3 - Single group
Call back number		Urgency	3 - Work not affected
Location		Priority	4 - Normal
Contact Type	External System	Assignment Group	[redacted]
* Service	Secure Computing > Vulnerability Managem	Assigned to	
* Category	Server-based Remediation	Customer watch list	
External ticket ID			Email the customer

* Short description: Axonius Vulnerabilty | [redacted] PluginID: 235616 | Microsoft Edge (Chromium) < 136.0.3240.64 (CVE-2025-4372)

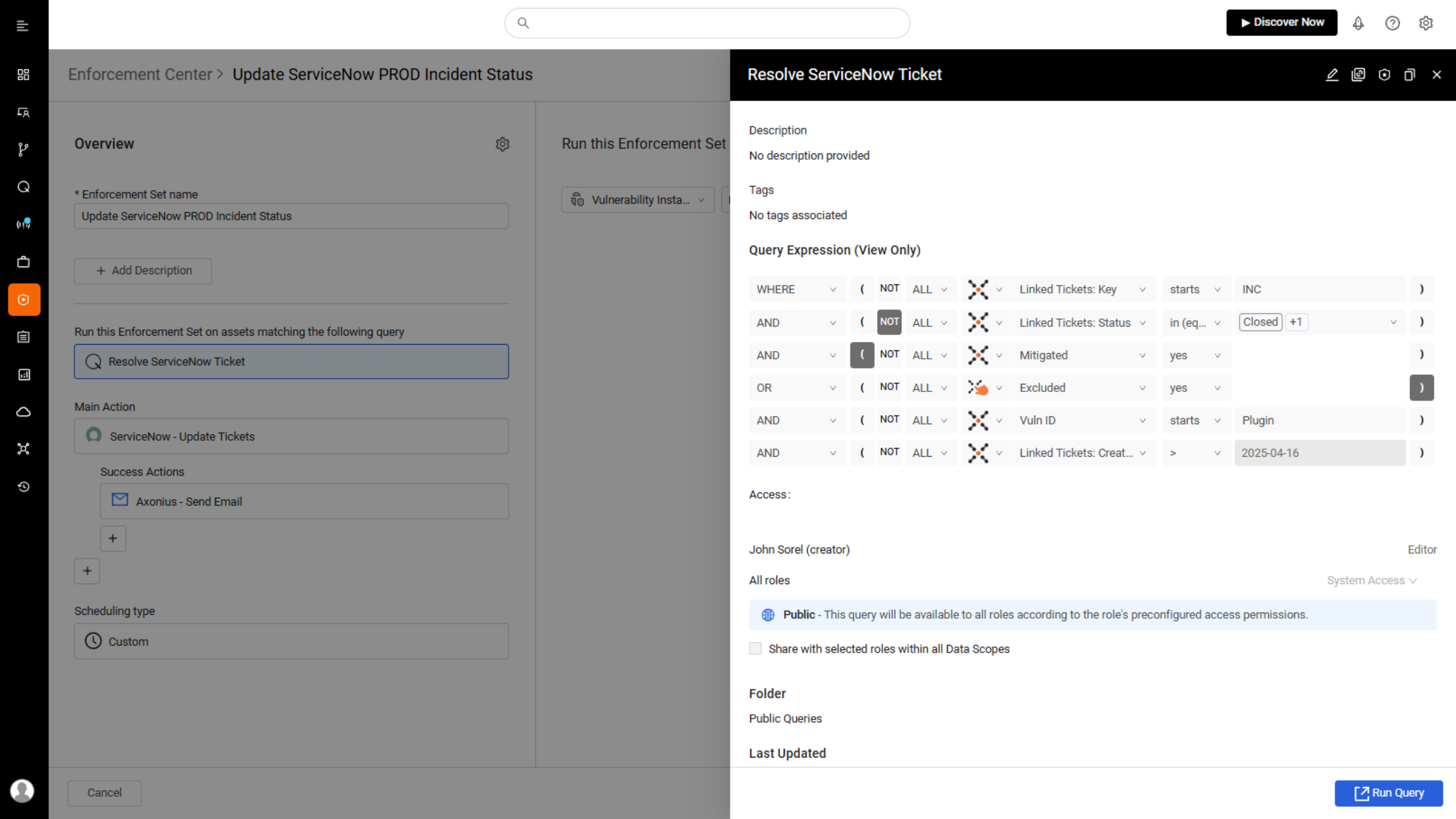
* Description:

Hostname: [redacted]
IP: [redacted]
Vulnerability Name: Microsoft Edge (Chromium) < 136.0.3240.64 (CVE-2025-4372)
PluginID: 235616
Plugin Info: https://www.tenable.com/plugins/nessus/235616
Harvard Risk Score: 7.2
Severity: High
First Seen: 2025-05-11T06:01:20.000Z
Last Seen: 2025-05-11T06:01:20.000Z
Vulnerability Publication Date: 2025-05-06T16:00:00.000Z
Scan Result: <plugin_output>
Path : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 135.0.3179.66
Fixed version : 136.0.3240.64
</plugin_output>
Remediation: Upgrade to Microsoft Edge version 136.0.3240.64 or later.

Disable Notifications

Related Search Results >

Notes | Resolution Information


Discover Now
Enforcement Center > Update ServiceNow PROD Incident Status
Overview
* Enforcement Set name
Update ServiceNow PROD Incident Status
+ Add Description
Run this Enforcement Set on assets matching the following query
Resolve ServiceNow Ticket
Main Action
ServiceNow - Update Tickets
Success Actions
Axonius - Send Email
Scheduling type
Custom
Run this Enforcement Set
Vulnerability Insta...
Cancel
Resolve ServiceNow Ticket
Description
No description provided
Tags
No tags associated
Query Expression (View Only)
WHERE (NOT ALL Linked Tickets: Key starts INC)
AND (NOT ALL Linked Tickets: Status in (eq... Closed +1)
AND (NOT ALL Mitigated yes)
OR (NOT ALL Excluded yes)
AND (NOT ALL Vuln ID starts Plugin)
AND (NOT ALL Linked Tickets: Creat... > 2025-04-16)
Access:
John Sorel (creator)
Editor
All roles
System Access
Public - This query will be available to all roles according to the role's preconfigured access permissions.
Share with selected roles within all Data Scopes
Folder
Public Queries
Last Updated
Run Query

Overview

* Enforcement Set name

Update ServiceNow PROD Incident Status

+ Add Description

Run this Enforcement Set on assets matching the following query

Resolve ServiceNow Ticket

Main Action

ServiceNow - Update Tickets

Success Actions

Axonius - Send Email

Scheduling type

Custom

Main Action: ServiceNow - Update Tickets

Test Connection | Replace Action

Required Fields | Ticket Main Settings | Ticket Additional Settings | Additional Fields

* Action name

Resolve Incident

Configure Dynamic Values

Write a statement to add dynamic values to Action fields

Use stored credentials from ServiceNow adapter

Select Adapter Connection

ServiceNow-Prod

*Compute Node

Primary

Assets

Assets | Queries

Search

- Secrets 0
- Application Resources

Tickets

- Tickets 75

Exposures

- Cloud Security Exposur... 83,358
- Vulnerability Instanc... 1,520,379

Network

- Networks 0
- Load Balancers 369
- Network Services 4,696
- Network Devices 162
- Network/Firewall Rules 14,449

Vulnerability Instances

Saved Queries

New Query [Edited] | Save As | Reset | EC Actions | Display by Date | Wizard | Basic

("specific_data.data.cve_id" == regex("^Plugin", "i")) and ("adapters_data.gui.is_excluded" == true) and not ("specific_data.data.mitigated" == true) and ("specific_dat

Query Wizard

Total 9 | Unique Device Count 8

Refine Data | Edit Table | Export CSV | + Create New Asset

Axonius Ris...	Vuln ID	Plugin Name	Excluded	Exclusion Reason
9.12	Plugin-156103	Apache Log4j 1.2 JMSAppender Remote ...	Yes	Not using JMS Appender
8.12	Plugin-156103	Apache Log4j 1.2 JMSAppender Remote ...	Yes	Not using JMS Appender
8.12	Plugin-156103	Apache Log4j 1.2 JMSAppender Remote ...	Yes	Not using JMS Appender
7.88	Plugin-156103	Apache Log4j 1.2 JMSAppender Remote ...	Yes	Not using JMS Appender
7.25	Plugin-182252	Apache Log4j SEoL (<= 1.x)	Yes	
7.25	Plugin-201488	Red Hat Enterprise Linux SEoL (7.8.x <= x...	Yes	
8.00	Plugin-201425	CentOS SEoL (7.x)	Yes	
7.88	Plugin-156103	Apache Log4j 1.2 JMSAppender Remote ...	Yes	Not using JMS Appender
7.88	Plugin-156103	Apache Log4j 1.2 JMSAppender Remote ...	Yes	Not using JMS Appender

Results per page: 20 50 100

<< < 1 > >>

Search

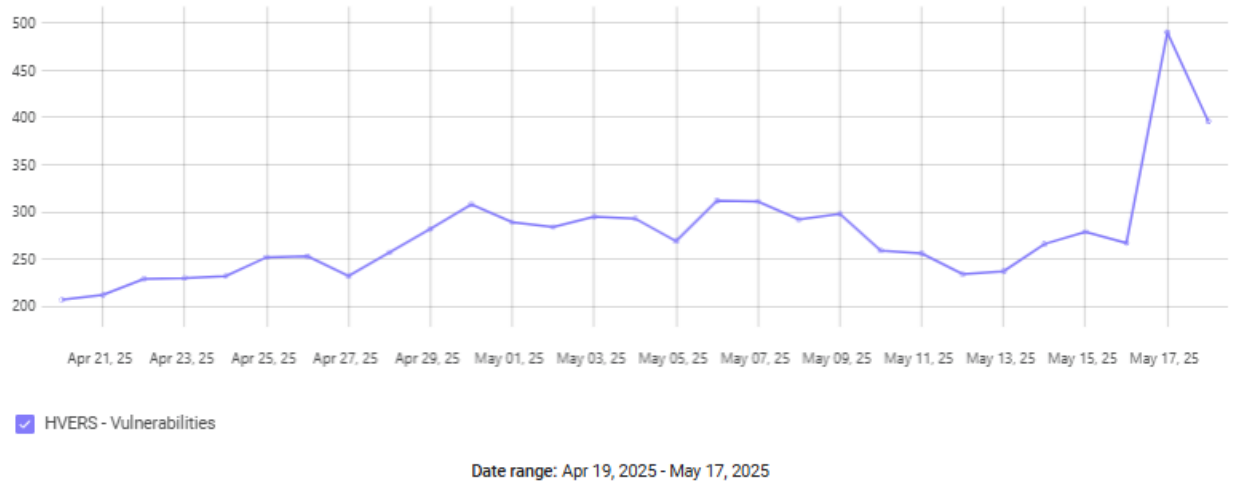
Favorites
- Axonius Dashboard
- My Dashboard

Public
- UWVM
  - On-Boarded Schools Status
  - Risk Based Vulnerability ...
  - School Status Dashboard
  - UVWM HVERS
  - Vulnerability Tickets
- HUIT
  - HUIT Security Requireme...
  - Tagging Status for HUIT
- Demo
- Axonius Dashboard

Shared
- All Vulnerabilities
- HVERS - Vulnerabilities
- SMVP Compliance Status
- Tagging Metrics

HVERS - Vulnerabilities

Filter | Add Chart



Date range: Apr 19, 2025 - May 17, 2025

Excluded Vulnerabilities

Total 33 (1 items)

↑ 1 (+3.12%) since 7 days ago

10/page 1 / 1

Vulnerability List Above HVERS Threshold

Axonius Risk Score	Preferred Hostname	Linked Tickets: Key	CVE ID	CVE Severity	Plugin Name	Plugin Output	Plugin Solution	Pl
7.00			Plugin-182252	CRITICAL	Apache Log4j SEoL (...	Path : C:\Program Fil...	Upgrade to a version...	A
7.00			Plugin-182252	CRITICAL	Apache Log4j SEoL (...	Path : /u01/DWC/D...	Upgrade to a version...	A
7.00			Plugin-40435	HIGH	MS09-035: Vulnerabi...	The following Visual ...	Microsoft has releas...	A
7.00			Plugin-234942	HIGH	Amazon Linux 2023 ...	Remote package ins...	Run 'dnf update kern...	T
7.00			Plugin-235852	HIGH	Security Update for ...	Path : C:\Program Fil...	Update .NET Core, re...	T
7.00			Plugin-235852	HIGH	Security Update for ...	Path : C:\Program Fil...	Update .NET Core, re...	T
7.00			Plugin-235852	HIGH	Security Update for ...	Path : C:\Program Fil...	Update .NET Core, re...	T
7.00			Plugin-235852	HIGH	Security Update for ...	Path : C:\Program Fil...	Update .NET Core, re...	T

Lessons Learned

- **Cultural Shift > Technology Change:** New mindset around vulnerability = potential business risk.
- **Clear Risk Language:** Translating technical risk into operational terms for leadership.
- **Piloting is Key:** Start small, scale after success.
- **Data Quality Matters:** Garbage in = garbage out. Asset inventories needed upgrades first
- **Celebrate Wins:** Even small improvements kept momentum.

Lessons Learned: Spotlight on Change Management

1. Engaged partners early
2. Communicated with a consistent message
3. Took hands-on approach to training and design workshops
4. Leadership adopted role of change champions
5. Promoted feedback loop to drive continuous improvement

Conclusion

- Risk-based vulnerability management (RBVM) EQUALS smarter security
- RBVM is a culture shift, every day is an opportunity to build on risk awareness
- Thank You!
- Open for Questions

Contact Information

HUIT Information Security and Data Privacy, University-wide Vulnerability Management (UWVM)

John Sorel: john_sorel@harvard.edu

Todd Conetta: todd_conetta@harvard.edu