

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



# Gain Visibility and Reduce Your Risk Exposure with Splunk Asset and Risk Intelligence

Ethan Gardiner | Senior Global Security Strategist  
BRKSEC-1587

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1587>



Is my network asset  
inventory 60%  
complete and updated  
in the last 30 days?

# SecOps struggle to understand their asset landscape

Rapidly evolving assets, users, devices, applications, and regulatory pressures continue to grow in scale and complexity.



**Incomplete and  
Inaccurate Asset Data**

52% manage 10,000+ assets<sup>1</sup>

<sup>1</sup> SC Magazine, Attack Surface Management: A critical pillar of cybersecurity asset management, Nov 2022

<sup>2</sup> CSO Online, Look for attack surface management to go mainstream in 2022, Jon Oltsik, Feb 2022

<sup>3</sup> The True Cost of Non-Compliance, Savivyt, May 2022

# SecOps struggle to understand their asset landscape

Rapidly evolving assets, users, devices, applications, and regulatory pressures continue to grow in scale and complexity.



## Incomplete and Inaccurate Asset Data

52% manage 10,000+ assets<sup>1</sup>



## Lengthy Security Investigation

69% experienced an attack targeting unknown, or poorly managed assets<sup>2</sup>

<sup>1</sup> SC Magazine, Attack Surface Management: A critical pillar of cybersecurity asset management, Nov 2022

<sup>2</sup> CSO Online, Look for attack surface management to go mainstream in 2022, Jon Oltsik, Feb 2022

<sup>3</sup> The True Cost of Non-Compliance, Savivint, May 2022

# SecOps struggle to understand their asset landscape

Rapidly evolving assets, users, devices, applications, and regulatory pressures continue to grow in scale and complexity.



## Incomplete and Inaccurate Asset Data

52% manage 10,000+ assets<sup>1</sup>



## Lengthy Security Investigation

69% experienced an attack targeting unknown, or poorly managed assets<sup>2</sup>



## Gaps in compliance

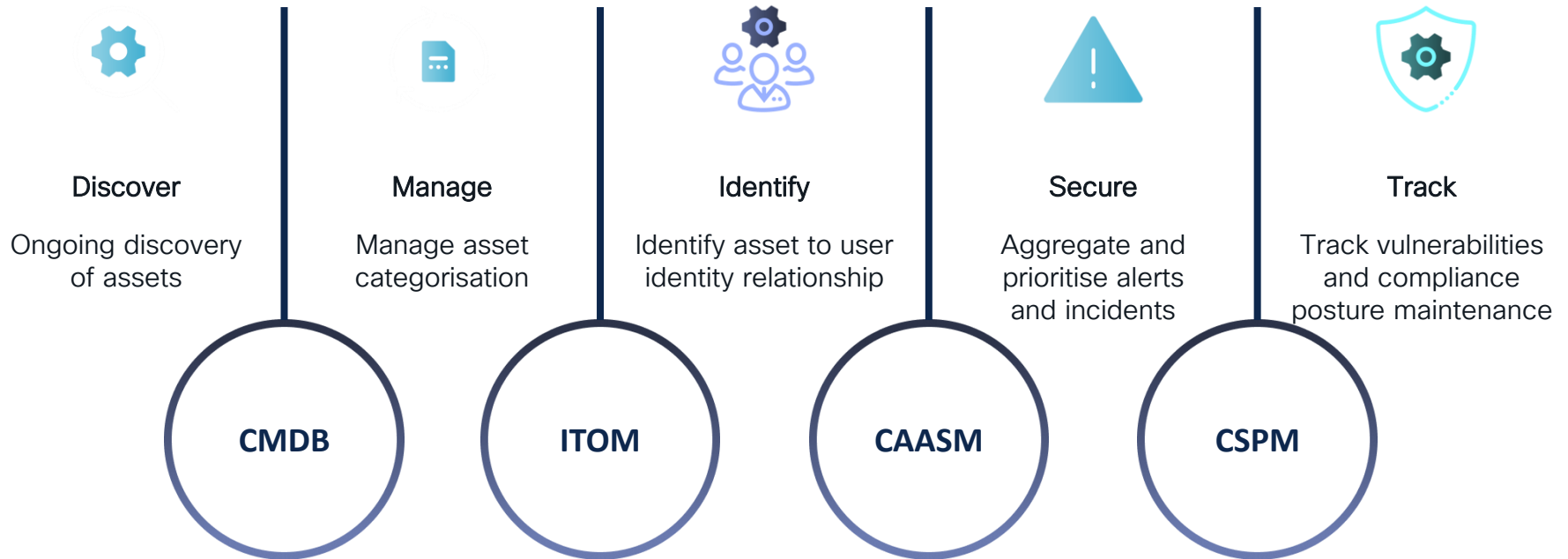
\$4M average revenue loss due to compliance failures<sup>3</sup>

<sup>1</sup> SC Magazine, Attack Surface Management: A critical pillar of cybersecurity asset management, Nov 2022

<sup>2</sup> CSO Online, Look for attack surface management to go mainstream in 2022, Jon Oltsik, Feb 2022

<sup>3</sup> The True Cost of Non-Compliance, Savivnt, May 2022

# Many tools to attempt to address this problem



# Traditional asset management tools are falling short

## What you get...



Fragmented visibility and insights

0010  
01010  
0101

Incomplete, inaccurate, outdated data



Disconnected tools and data sources

69%

of organisations have experienced an attack targeting unknown or unmanaged assets<sup>1</sup>

# What is needed?



Comprehensive asset visibility

---



Continuous updates to asset inventory to ensure it's never stale

---



An accurate, single source of truth



How do you  
close this divide?

You need a  
new approach.

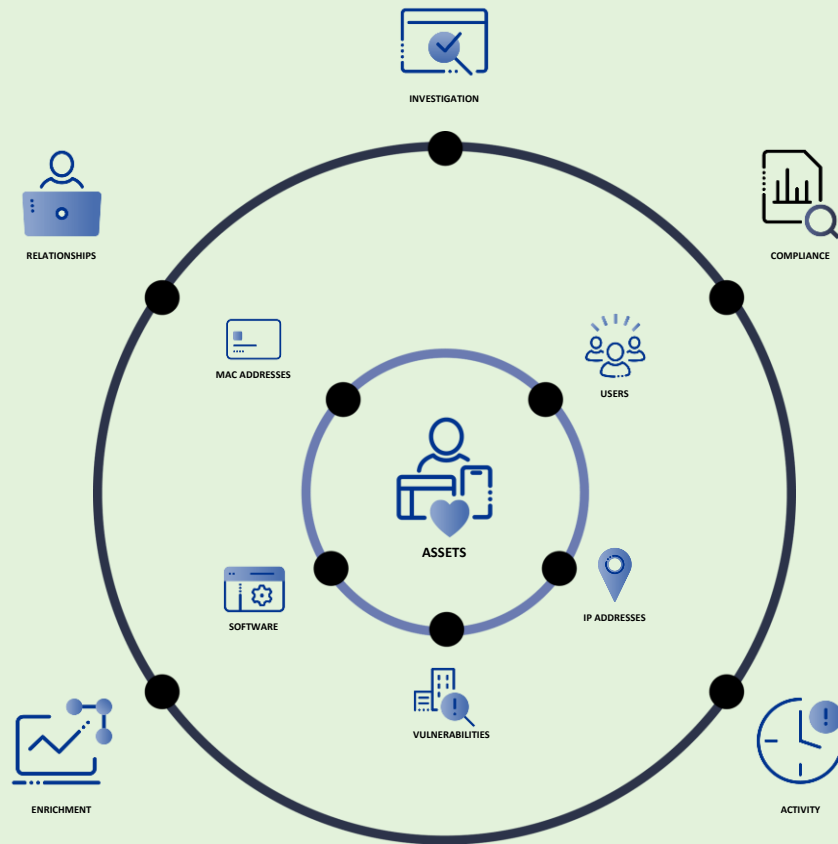


# Introducing Splunk® Asset and Risk Intelligence

Proactive risk mitigation through continuous asset discovery and compliance monitoring.

Continuously **discovers networked assets** (including devices, users, and applications) leveraging the rich data in Splunk.

Asset and Risk Intelligence identifies **compliance violations** and **gaps in security controls** using OOTB and custom frameworks, to **accelerate investigations** and **reduce risk** exposure.



# Empowering SecOps with Splunk Asset and Risk Intelligence



Gain comprehensive asset visibility to reduce risk exposure



Accelerate security investigation with accurate asset context



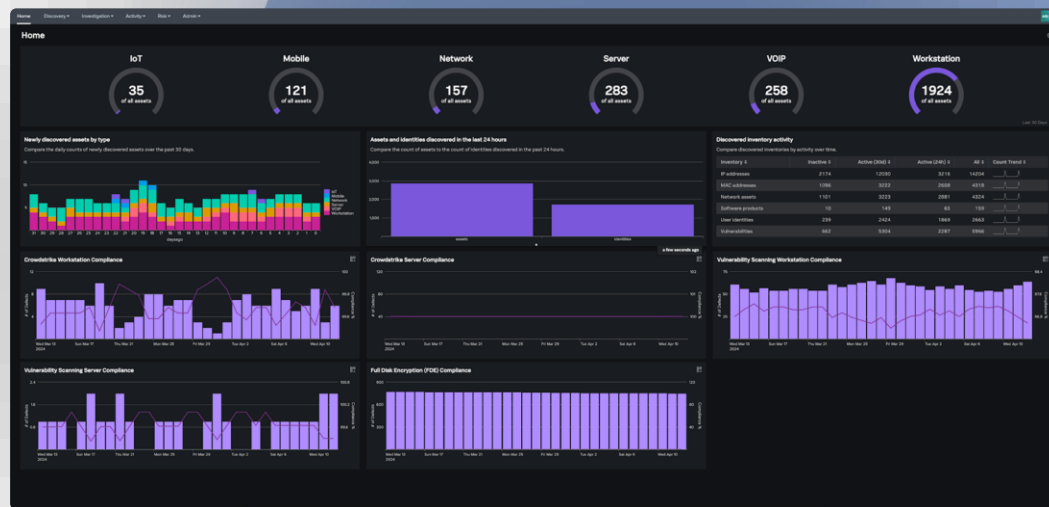
Identify compliance gaps in security controls



Seamless integration and deployment with Splunk® Enterprise Security



Bridge the IT and Security gap with seamless ServiceNow® CMDB integration



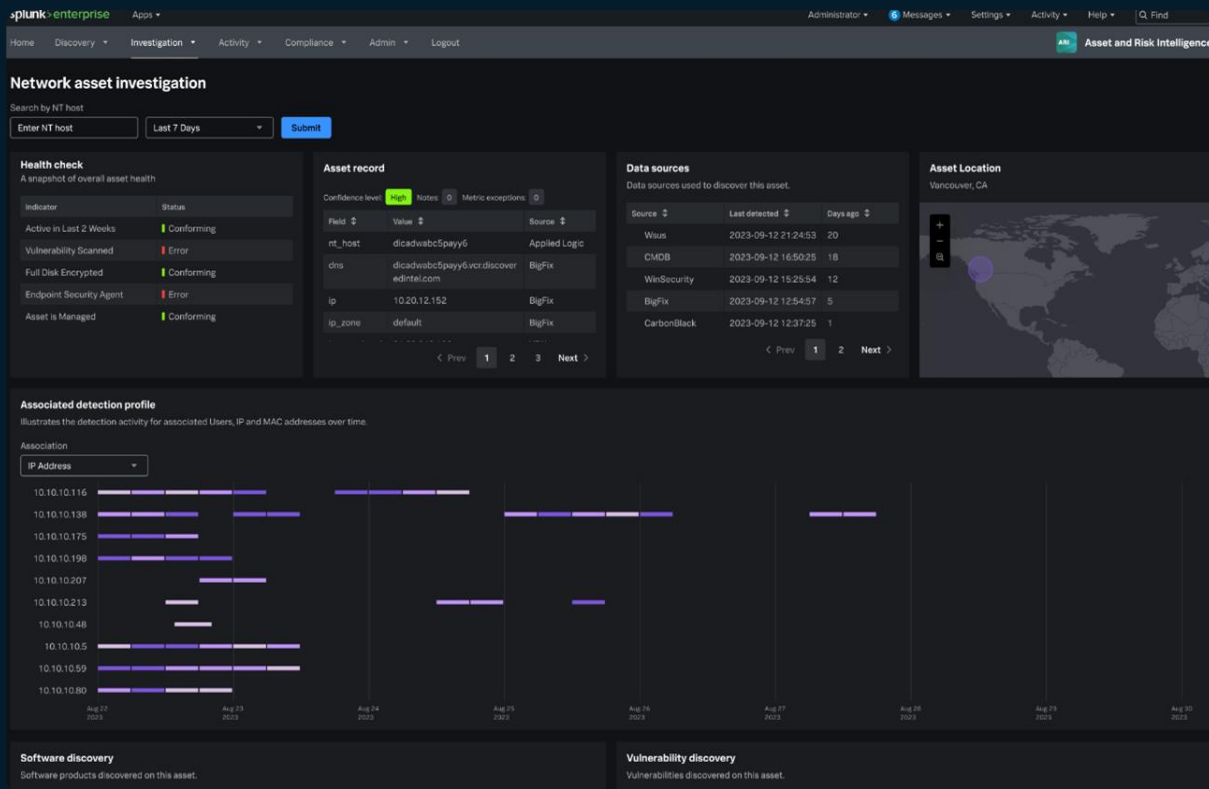
**CISCO** *Live!*

- © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



# Accelerate security investigations

- Perform instant asset investigations
- Gain holistic asset and identity insights
- Dynamic asset risk scoring to power investigations
- Streamline investigative processes



# Augment the power of Splunk enterprise security with asset and risk intelligence

- Gain a thorough understanding of your assets and boost your security posture.

Automatically **populate ES Assets & Identities** Framework with discovered asset information

Provide **comprehensive asset context** for ES notable event **enrichment**

Ensures **accurate attribution of assets and events** during investigations

## Complementing benefits for ES customers

- Continuous asset discovery
- Complete and accurate asset records
- Track asset changes over time
- Investigate asset relationships
- Comprehensive asset and compliance reporting
- Software & vulnerability inventory and discovery

# Bridging the gap: enhancing asset visibility across IT and SecOps.

- With seamless ServiceNow CMDB bi-directional integration.



Update ServiceNow asset records



Identify unmanaged and unknown



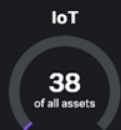
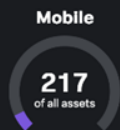
Ensure CMDB data is not stale



Automated endpoint compliance ticketing integration

# Walk Through

**Home**



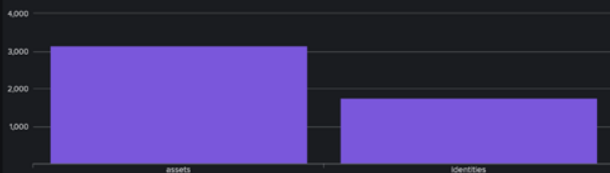
### Newly discovered assets by type

Compare the daily counts of newly discovered assets over the past 30 days.



### Assets and Identities discovered in the last 24 hours

Compare the count of assets to the count of identities discovered in the past 24 hours.

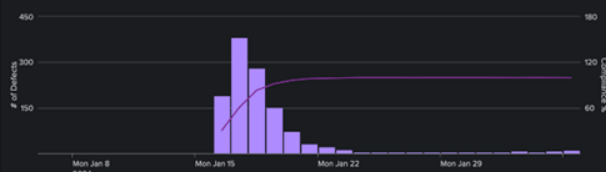


### Discovered inventory activity

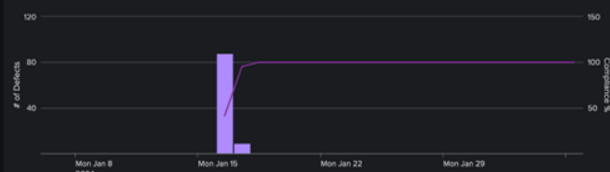
Compare discovered inventories by activity over time.

| Inventory ↕       | Inactive ↕ | Active (30d) ↕ | Active (24h) ↕ | All ↕ | Count Trend ↕ |
|-------------------|------------|----------------|----------------|-------|---------------|
| IP addresses      | 0          | 12081          | 3492           | 12081 |               |
| MAC addresses     | 0          | 3853           | 2860           | 3853  |               |
| Network assets    | 0          | 3859           | 3146           | 3859  |               |
| Software products | 0          | 44             | 30             | 44    |               |
| User identities   | 0          | 2429           | 1946           | 2429  |               |
| Vulnerabilities   | 0          | 4974           | 2116           | 4974  |               |

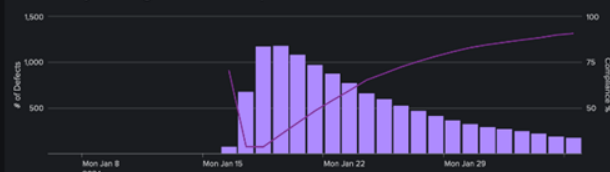
## CrowdStrike Workstation Compliance



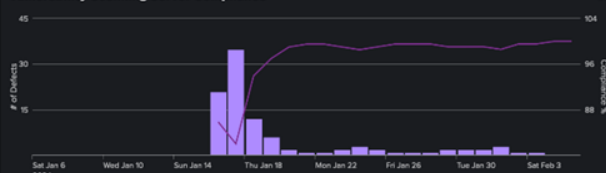
## CrowdStrike Server Compliance



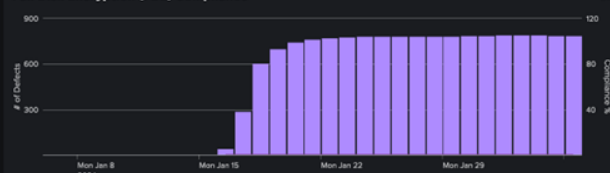
## Vulnerability Scanning Workstation Compliance



## Vulnerability Scanning Server Compliance



## Full Disk Encryption (FDE) Compliance



## ASSET DISCOVERY

## Network asset discovery

No Selected Filter ▾ Show Filters

## CONTINUOUS DISCOVERY

3,207

Discovered network assets

## Total discovered assets by type

Compare the total number of discovered assets for each asset type.



## Newly discovered assets by type

Compare the daily counts of newly discovered assets over the past 7 days.



## Discovered asset locations

See discovered assets with known locations.



## Asset details

The following list includes all discovered assets. Select a row to further investigate a specific asset.

| asset_type ▾  | os ▾ | nt_host ▾            | ip ▾         | mac ▾        | asset_class ▾ | city ▾    | state ▾ | country ▾ | user_id ▾     | firstdetect ▾       | lastdetect ▾        | age ▾ | classification ▾ | sensitivity ▾ | criticality ▾ |
|---------------|------|----------------------|--------------|--------------|---------------|-----------|---------|-----------|---------------|---------------------|---------------------|-------|------------------|---------------|---------------|
| Uncategorized |      | applewatchcigicbweg0 | 10.20.61.161 | 0088652d98cb |               | Vancouver | BC      | CA        |               | 2024-01-17 15:00:40 | 2024-05-13 17:57:39 | 117   | confidential     | high          | high          |
| Workstation   |      | aricadwabcvzka1      | 10.20.12.13  | 00014a1801f1 | Laptop        | Vancouver | BC      | CA        | ebartell      | 2024-01-16 19:22:55 | 2024-05-13 17:57:36 | 118   | internal         | high          | high          |
| Workstation   |      | aricadwabcvidmtr     | 10.50.11.89  | 4c3275667790 | Laptop        | New York  | NY      | US        | mikolaus      | 2024-01-16 22:24:33 | 2024-05-13 17:57:33 | 118   | internal         | high          | medium        |
| Server        |      | arirsvwdefykdyb      | 10.10.20.222 | 00065bd2d09d |               | Toronto   | ON      | CA        |               | 2024-04-01 10:44:04 | 2024-05-13 17:57:29 | 42    | internal         | low           | low           |
| Workstation   |      | aricadwabcgkaw2      | 10.40.11.241 | 4c32756e0900 | Laptop        | Singapore |         | SG        | bratke-grimes | 2024-04-27 09:24:52 | 2024-05-13 17:57:28 | 16    | internal         | high          | medium        |
| Workstation   |      | aricadwabcnuj1yr     | 10.30.12.114 | 00014a5bf1b9 | Laptop        | London    |         | GB        | kozey         | 2024-01-16 15:13:17 | 2024-05-13 17:57:27 | 118   | internal         | critical      | critical      |

## Network asset investigation

Search by NT host

ericadwbcvzwa1

Submit

## Health check

A snapshot of overall asset health

| Indicator              | Status    |
|------------------------|-----------|
| Active in last 2 weeks | Compliant |
| Endpoint Security      | Compliant |
| Vulnerability Scanned  | Compliant |
| Endpoint Encryption    | Compliant |

## ASSET RECORD POSTURE CHECK

## Record

Confidence level: High Notes: 0 Metric exceptions: 0

| field         | value                                     | source            |
|---------------|-------------------------------------------|-------------------|
| nt_host       | ericadwbcvzwa1                            | Applied Logic     |
| dns           | ericadwbcvzwa1.vcr.splunkshirtcompany.com | QualysGuard       |
| ip            | 10.20.12.13                               | MS_DHCP           |
| ip_zone       | default                                   | MS_DHCP           |
| ip_translated | 68.185.109.201                            | CrowdStrikeDevice |
| mac           | 00014a1801f1                              | MS_DHCP           |
| os            | Windows 8                                 | AriTaAsset        |
| user_id       | ebartell                                  | AriTaAsset        |
| asset_type    | Workstation                               | CrowdStrikeDevice |
| asset_class   | Laptop                                    | Applied Logic     |

Prev 1 2 3 Next

## Data sources

The following data sources have been used by ARI to discover this asset

| source            | last_detected       | daysago |
|-------------------|---------------------|---------|
| MS_DHCP           | 2024-05-13 17:57:36 | 0       |
| AriTaAsset        | 2024-05-13 04:48:29 | 1       |
| CrowdStrikeDevice | 2024-05-13 03:35:56 | 1       |
| WinSecurity       | 2024-05-13 01:39:53 | 1       |
| TenableIOVulns    | 2024-05-12 21:10:50 | 1       |
| TenableIOAssets   | 2024-05-08 06:55:23 | 5       |
| AriTaSoftware     | 2024-05-07 16:03:33 | 6       |
| QualysGuard       | 2024-05-04 04:19:19 | 10      |
| Bluecoat          | 2024-01-28 00:30:24 | 107     |
| JuniperVPN        | 2024-01-26 13:33:10 | 108     |

## Geographic location

Vancouver, CA



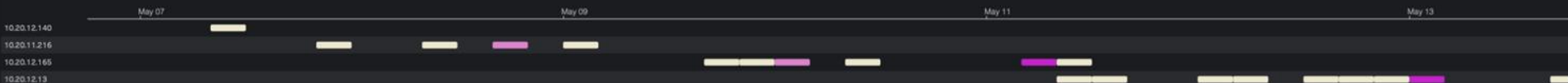
Last 7 days

## Detection activity

Select Association

IP address

Select associated users, IP addresses, or MAC addresses to see their detection activity over time.



## ASSET RELATIONSHIP MAPPING

## Cloud asset insights

Displays insights into the active cloud provisioned assets that have been discovered by ari.

## INACTIVE VS ACTIVE CLOUD ASSETS

4,532

Total cloud assets

3,199

Active cloud assets (past month)

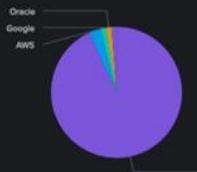
1,333

Inactive cloud assets

5

Cloud providers

## Top cloud providers



## Active vs. inactive cloud assets by provider



## Cloud assets by location



## Top cloud subnets

| subnet     | ip_zone | provider | assets |
|------------|---------|----------|--------|
| 10.40.11.0 | default |          | 161    |
| 10.50.10.0 | default |          | 159    |
| 10.10.11.0 | default |          | 158    |
| 10.30.11.0 | default |          | 154    |
| 10.20.11.0 | default |          | 153    |
| 10.40.12.0 | default |          | 152    |
| 10.50.12.0 | default |          | 152    |
| 10.10.12.0 | default |          | 150    |
| 10.30.12.0 | default |          | 150    |



## Cloud asset detection activity - past month

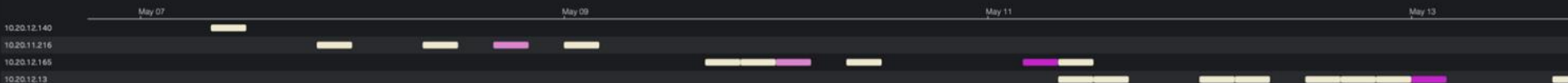
Illustrates the number of Cloud assets actively discovered by ARI on each day over the past month.



Select Association

IP address

Select associated users, IP addresses, or MAC addresses to see their detection activity over time.



## DISCOVERED SOFTWARE

### Discovered software

The following software products have been discovered on this asset

| vendor    | product                                                        | version         | First Detected      | Last Detected       |
|-----------|----------------------------------------------------------------|-----------------|---------------------|---------------------|
| apple     | itunes                                                         | 12.23.24        | 2024-02-16 02:03:27 | 2024-05-07 16:03:33 |
| intel     | intel(r) pro/wireless driver                                   | 16.06.2000.0671 | 2024-02-16 02:03:28 | 2024-05-07 16:03:32 |
| microsoft | internet explorer                                              | 11.0.9600.17031 | 2024-02-16 02:03:27 | 2024-05-07 16:03:32 |
| microsoft | microsoft silverlight                                          | 5.1.30214.0     | 2024-02-16 02:03:32 | 2024-05-07 16:03:32 |
| sony      | valo care                                                      | 8.4.0.14286     | 2024-02-16 02:03:31 | 2024-05-07 16:03:32 |
| oracle    | java 7 update 13 (64-bit)                                      | 7.0.130         | 2024-02-16 02:03:29 | 2024-05-07 16:03:31 |
| microsoft | office 15 click-to-run licensing component                     | 15.0.4605.1003  | 2024-02-16 02:03:30 | 2024-05-07 16:03:31 |
| google    | chrome                                                         | 34.0.1847.116   | 2024-02-16 02:03:28 | 2024-05-07 16:03:30 |
| microsoft | microsoft office shared 64-bit mui (english) 2013              | 15.0.4569.1506  | 2024-02-16 02:03:29 | 2024-05-07 16:03:30 |
| microsoft | microsoft visual c++ 2008 redistributable - x64 9.0.30729.6161 | 9.0.30729.6161  | 2024-02-16 02:03:27 | 2024-05-07 16:03:29 |

&lt; Prev 1 2 3 Next &gt;

### Discovered vulnerabilities

The following vulnerabilities have been discovered on this asset

| signature                                           | port | First Detected      | Last Detected       |
|-----------------------------------------------------|------|---------------------|---------------------|
| apple ios and macos memory corruption vulnerability | 22   | 2024-02-03 04:19:19 | 2024-05-12 21:10:50 |
| microsoft office buffer overflow vulnerability      | 80   | 2024-02-03 04:19:11 | 2024-05-12 21:08:19 |

### Associated MAC addresses

Select a MAC address to open its investigation.

| mac          | mac_vendor       | detections | First associated | Last associated  |
|--------------|------------------|------------|------------------|------------------|
| 00014a1801f1 | Sony Corporation | 100 %      | 2024-01-16 20:33 | 2024-05-13 17:57 |

### Associated user IDs

Select a user ID to open its investigation.

| user_id  | detections | First associated | Last associated  |
|----------|------------|------------------|------------------|
| ebartell | 100 %      | 2024-01-16 19:22 | 2024-05-13 09:54 |

### Associated IP addresses

Select an IP address to open its investigation.

| ip           | detections | First associated | Last associated  |
|--------------|------------|------------------|------------------|
| 10.20.12.13  | 41 %       | 2024-05-11 11:09 | 2024-05-13 17:57 |
| 10.20.12.165 | 33 %       | 2024-05-09 19:15 | 2024-05-11 09:09 |
| 10.20.11.216 | 19 %       | 2024-05-07 21:36 | 2024-05-09 02:35 |
| 10.20.12.140 | 7 %        | 2024-05-04 21:03 | 2024-05-07 08:43 |

## User Identity Investigation

Search by user ID

## Record

Known information about the user ID. Notes: 0 Metric Exceptions: 0

| field            | value                           | source        |
|------------------|---------------------------------|---------------|
| user_id          | ebartell                        | Applied Logic |
| user_first       | Eleazar                         | Applied Logic |
| user_last        | Bartell                         | Applied Logic |
| user_category    | Employee                        | Applied Logic |
| user_email       | ebartell@splunkshirtcompany.com | Applied Logic |
| user_business    | Splunk T-Shirt Company          | Applied Logic |
| user_bunit       | West                            | Applied Logic |
| user_location_id | Vancouver_BC_CA                 | Applied Logic |
| user_priority    | Medium                          | Applied Logic |
| user_start_date  | 2022-04-18                      | Applied Logic |

◀ Prev 1 2 Next ▶

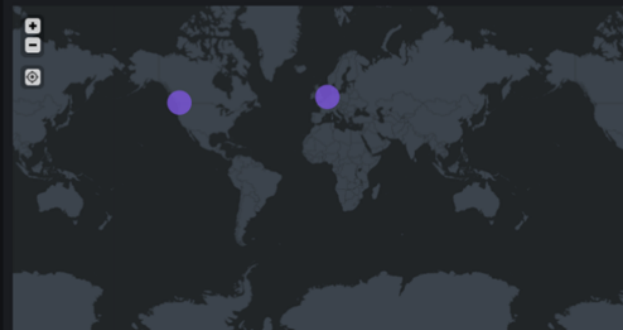
## Data sources

The following data sources have been used by ARI to discover this user ID.

| source      | last_detected       | daysago |
|-------------|---------------------|---------|
| WinSecurity | 2024-05-13 09:54:41 | 0       |
| JuniperVPN  | 2024-05-13 03:39:08 | 1       |
| Bluecoat    | 2024-05-12 16:21:24 | 1       |
| AriTaAsset  | 2024-05-11 04:15:32 | 3       |

## Geographic location

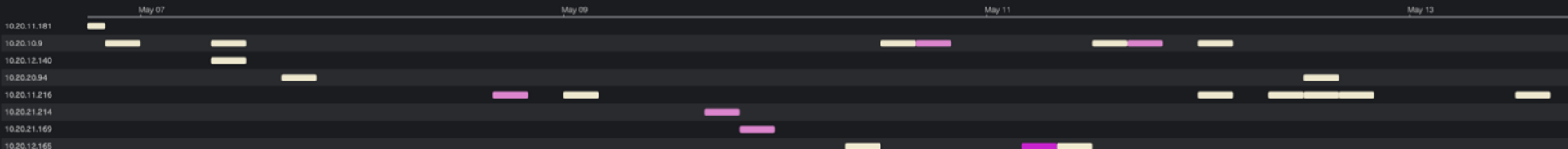
Vancouver, CA

IDENTITY DISCOVERY  
AND ACTIVITY  
DETECTION

## Detection activity

Select association

Illustrates the detection activity for associated network assets, IP and MAC addresses over time.



## Risk scoring insights

Risks detected

Last 30 days

Search by NT host

\*

Asset type

All

## DYNAMIC ASSET RISK SCORING

### Assets with risks

1,234

### Risk rules

1

### Total risks

1,234

### Critical risks

0

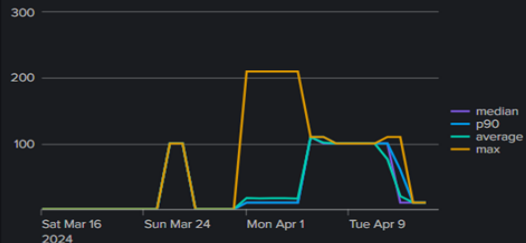
### High risks

0

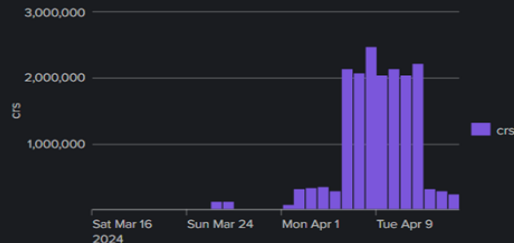
### Avg risk score (CRS)

10

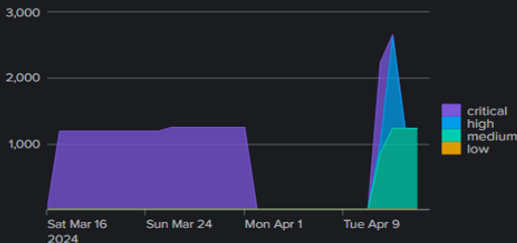
### Composite risk score (CRS) trend



### Total composite risk score (CRS)



### Assets by risk level



Risk levels

All

Risk rules

All

Show only assets with a CRS

Yes

CRS greater than

0

### Asset count by risk scoring rules

| Risk ID | Risk rule | Risk level | Filter type(s) | Last detected       | Assets |
|---------|-----------|------------|----------------|---------------------|--------|
| 0001    | Rule33    | medium     | Asset record   | 2024-04-15 19:21:00 | 1230   |

### Asset detail by risk scoring rules

| nt_host         | asset_type  | crs | Rule33              |
|-----------------|-------------|-----|---------------------|
| dicadwabcylez7g | Workstation | 10  | medium (2024-04-15) |
| dicadwabcg9c9or | Workstation | 10  | medium (2024-04-15) |
| dicadwabc8zhxl  | Workstation | 10  | medium (2024-04-15) |
| dicadwabc9m4etb | Workstation | 10  | medium (2024-04-15) |

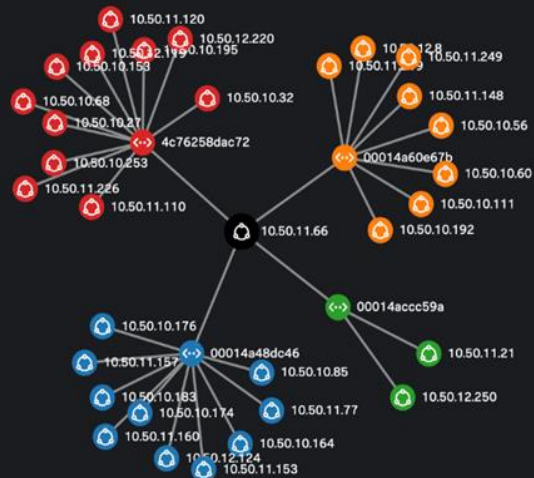
## Attack surface explorer

Visualize relationships between network assets, IPs, users and MACs over time

Time range: Last 30 days
 Source: ip
 Source value: 10.50.11.66
 Zones: default
 Target: mac
 Exclude target values: None
 Relationship degrees: 2 degree
☐ Link Weights
 Submit

### Asset relationship diagram

The following diagram illustrates the key relationships between the selected source and targets, for the selected timeframe.

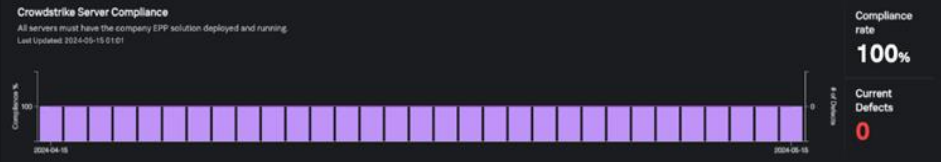


**ATTACK SURFACE  
EXPLORATION**

Metrics posture

-- No Selected Filter --

Show Filters



COMPLIANCE POSTURE  
DISCOVERY

# VULNERABILITY GAP IDENTIFICATION

Home Discovery Investigation Activity Risk Admin

## Vulnerability Scanning Workstation Compliance

0

Exceptions

1,832

Opportunities

63

Defects

1,769

Compliant

96.56%

Compliance %

### Metric description

All workstations must be scanned by the company vulnerability scanner on a regular basis. This metric measures the compliance with this requirement and provides a list of defects for remediation.

### Opportunities

All workstations discovered on the network in the past 15 days.

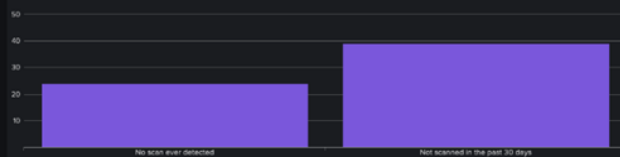
### Defects

Any discovered workstations that have never been vulnerability scanned OR have not been scanned in the past 30 days.

### Compliance vs non-compliance



### Defect reason



### Timeline



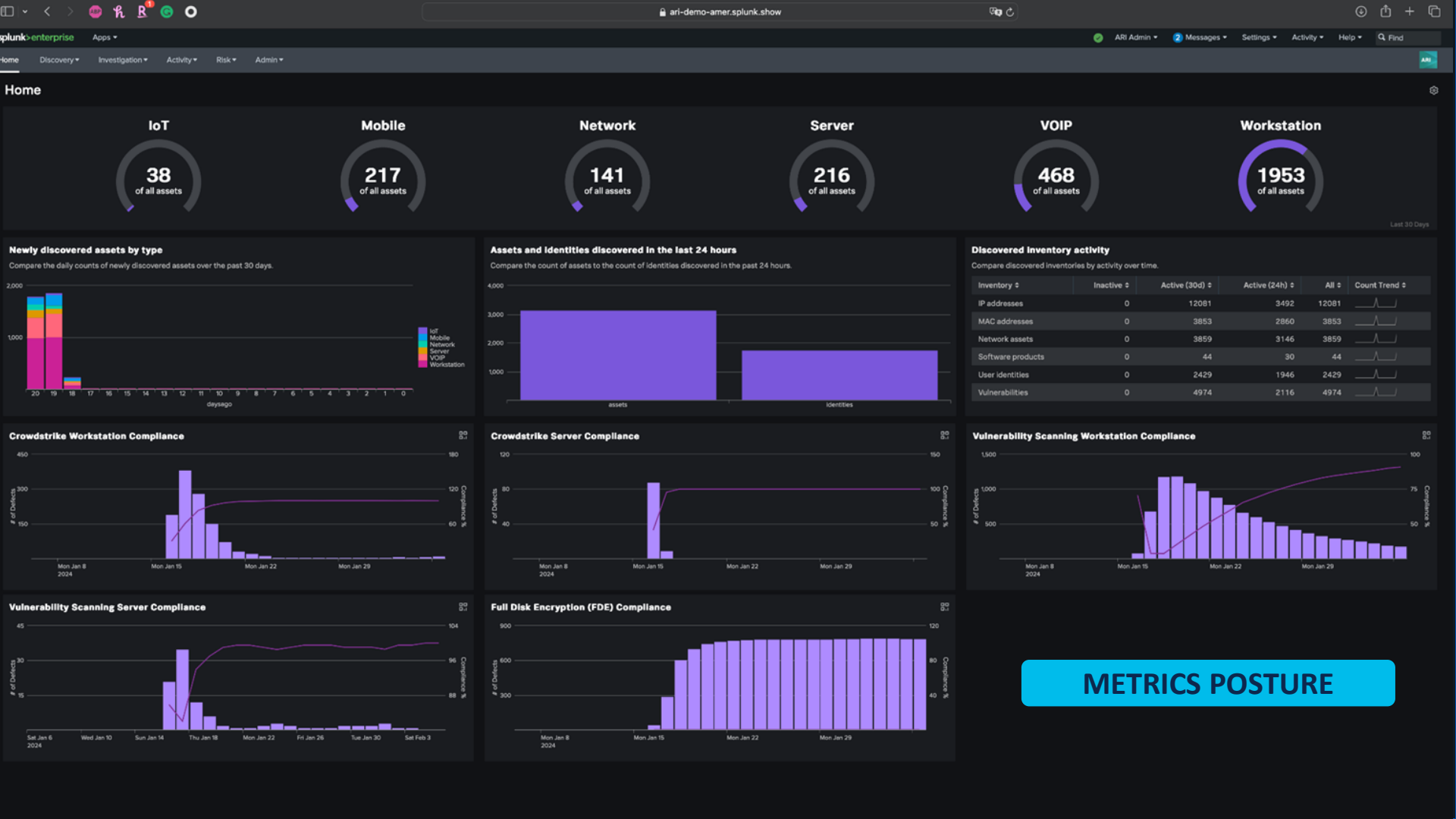
### Defects

Search

Exceptions

\*

|    | nt_host s                | defect_reason s  | os s                            | ip s        | ip_zone s    | lastdetect s | lastdetect_source s | asset_type s        | asset_class s | location_id s | region s         | city s | state s   | country s | user_id s      |
|----|--------------------------|------------------|---------------------------------|-------------|--------------|--------------|---------------------|---------------------|---------------|---------------|------------------|--------|-----------|-----------|----------------|
| 1  | <input type="checkbox"/> | aplmexifcmbp0    | No scan ever detected           |             | 10.20.32.36  | default      | 2024-05-15 16:21:37 |                     | Workstation   | Laptop        | Vancouver Office |        | Vancouver | BC        | CA             |
| 2  | <input type="checkbox"/> | aricadwabc19zt10 | No scan ever detected           | Windows 7   | 10.30.12.142 | default      | 2024-05-15 10:58:26 |                     | Workstation   |               | london           |        | London    | GB        | hbraun         |
| 3  | <input type="checkbox"/> | aricadwabc1uqoj  | No scan ever detected           | Mac OS X 10 | 10.30.11.119 | default      | 2024-05-15 13:51:25 |                     | Workstation   | Laptop        | london           |        | London    | GB        | aprice         |
| 4  | <input type="checkbox"/> | aricadwabc2eamy8 | Not scanned in the past 30 days | Mac OS X 10 | 10.30.10.60  | default      | 2024-05-15 15:37:58 | 2024-04-10 16:45:08 | Workstation   | Laptop        | london           |        | London    | GB        | tsauer-weimann |
| 5  | <input type="checkbox"/> | aricadwabc4ksaum | Not scanned in the past 30 days | Windows 7   | 10.20.10.128 | default      | 2024-05-15 05:50:59 | 2024-04-15 07:10:55 | Workstation   |               | vancouver        |        | Vancouver | BC        | CA             |
| 6  | <input type="checkbox"/> | aricadwabc6h3jxf | Not scanned in the past 30 days | Windows XP  | 10.30.12.11  | default      | 2024-05-15 09:10:56 | 2024-04-14 06:03:37 | Workstation   | Laptop        | london           |        | London    | GB        | pkesster       |
| 7  | <input type="checkbox"/> | aricadwabcakxr3  | Not scanned in the past 30 days | Windows 7   | 10.50.10.178 | default      | 2024-05-15 14:21:53 | 2024-04-14 15:38:00 | Workstation   |               | nyc              |        | New York  | NY        | US             |
| 8  | <input type="checkbox"/> | aricadwabcbrw4m  | Not scanned in the past 30 days | Windows 7   | 10.10.11.143 | default      | 2024-05-15 16:24:20 | 2024-04-10 22:37:01 | Workstation   | Laptop        | toronto          |        | Toronto   | ON        | CA             |
| 9  | <input type="checkbox"/> | aricadwabcorgtw  | No scan ever detected           | Windows 8   | 10.30.11.187 | default      | 2024-05-15 06:18:29 |                     | Workstation   | Laptop        | london           |        | London    | GB        | mwisozk        |
| 10 | <input type="checkbox"/> | aricadwabcourcpd | Not scanned in the past 30 days | Windows XP  | 10.20.11.251 | default      | 2024-05-15 08:42:09 | 2024-04-04 21:12:27 | Workstation   | Laptop        | vancouver        |        | Vancouver | BC        | CA             |



# CYBERSECURITY FRAMEWORK MAPPING

## Add framework

☐ Inactive ✕

Name

CIS Critical Security Controls

ID ⓘ

CISv8

Description

The CIS Controls are a prescriptive, prioritized and simplified set of best practices that can be used to strengthen cybersecurity posture and mitigate the most prevalent cyberattacks against systems and networks.

## Cybersecurity frameworks

Name filter

\*

| ID ↕          | Name ↕                         | Description ↕                                                                                                                                                                                                                                                                                                         | Categories ↕                                                                                     |
|---------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| CISv8         | CIS Critical Security Controls | The CIS Controls are a prescriptive, prioritized and simplified set of best practices that can be used to strengthen cybersecurity posture and mitigate the most prevalent cyberattacks against systems and networks.                                                                                                 | Inventory and Control of Enterprise Assets                                                       |
| HIPAA         | HIPAA                          | The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. | Administrative safeguards<br>Physical Safeguards<br>Technical safeguards                         |
| ISO27001_2022 | ISO/IEC 27001:2022             | The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.                                                                                             | Organizational controls<br>People controls<br>Technical controls<br>Technological Controls       |
| NIST_CSFv2    | NIST CSF v2                    | The NIST Cybersecurity Framework (CSF) is based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risks. It is widely used by public and private organizations of all sectors and sizes around the world.                                                  | Detect - Adverse Event Analysis<br>Detect - Continuous Monitoring<br>Identify - Asset Management |

## NIST CSF v2 posture

– No Selected Filter –

Hide Filters

Filter name

My saved filter

☒ Make public

Categories

Detect - Continuous Monitoring ✕

Identify - Asset Management ✕

Protect - Data Security ✕

Metrics

All ✕

Search

Save as new filter

Reset filter

Controls

All ✕

## HIPAA posture

– No Selected Filter –

Show Filters

### Asset Management - Server

All servers must be in the company asset management solution (CMDB).  
Last updated: 2024-04-25 01:01



Compliance rate

97.5%

Current defects

11

### Asset Management - Workstation

All workstations must be in the company asset management solution (CMDB).  
Last updated: 2024-04-25 01:01



Compliance rate

78.46%

Current defects

317

### Data Loss Prevention - Server

All servers must have Data Loss Prevention (DLP) software deployed and running.  
Last updated: 2024-04-25 01:01



Compliance rate

0%

Current defects

454

### Data Loss Prevention - Workstation

All workstations must have Data Loss Prevention (DLP) software deployed and running.  
Last updated: 2024-04-25 01:01



Compliance rate

99.66%

Current defects

5

### Log Collection - Workstations

All workstations must be logging to a central log management system.  
Last updated: 2024-04-25 01:01



Compliance rate

0%

Current defects

2173

### Malware Protection - Servers

All servers must have malware protection deployed and running.  
Last updated: 2024-04-25 01:01



Compliance rate

98.9%

Current defects

5

# Next steps

## Demo



Stop by the Splunk stations to learn more

## Evaluate



Reach out to your sales team to learn how to get an evaluation

## Got a question?



Come find me and have a chat!

# Keynote Deep Dives

**Wednesday**  
**10:30am – 11:30am**



Experiences Amplified:  
How AI Can Fuel Better Employee and Customer Experiences

**Level 1**  
**Room 106**



Smart, Secure, Seamless:  
Transforming Experiences with Next-Generation Networking

**Level 2**  
**Room 204**



Harness a Bold New Era:  
Transform Data Centre and Service Provider Connectivity

**Level 2**  
**Room 203**



Securing User to Application and Everything in Between

**Level 2**  
**Melbourne Room 2**



Unlocking Digital Resilience through Unified Observability

**The HUB**  
**Centre Stage**

# Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

---



Complete your surveys in the **Cisco Live mobile app**.

---



# Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



# Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC