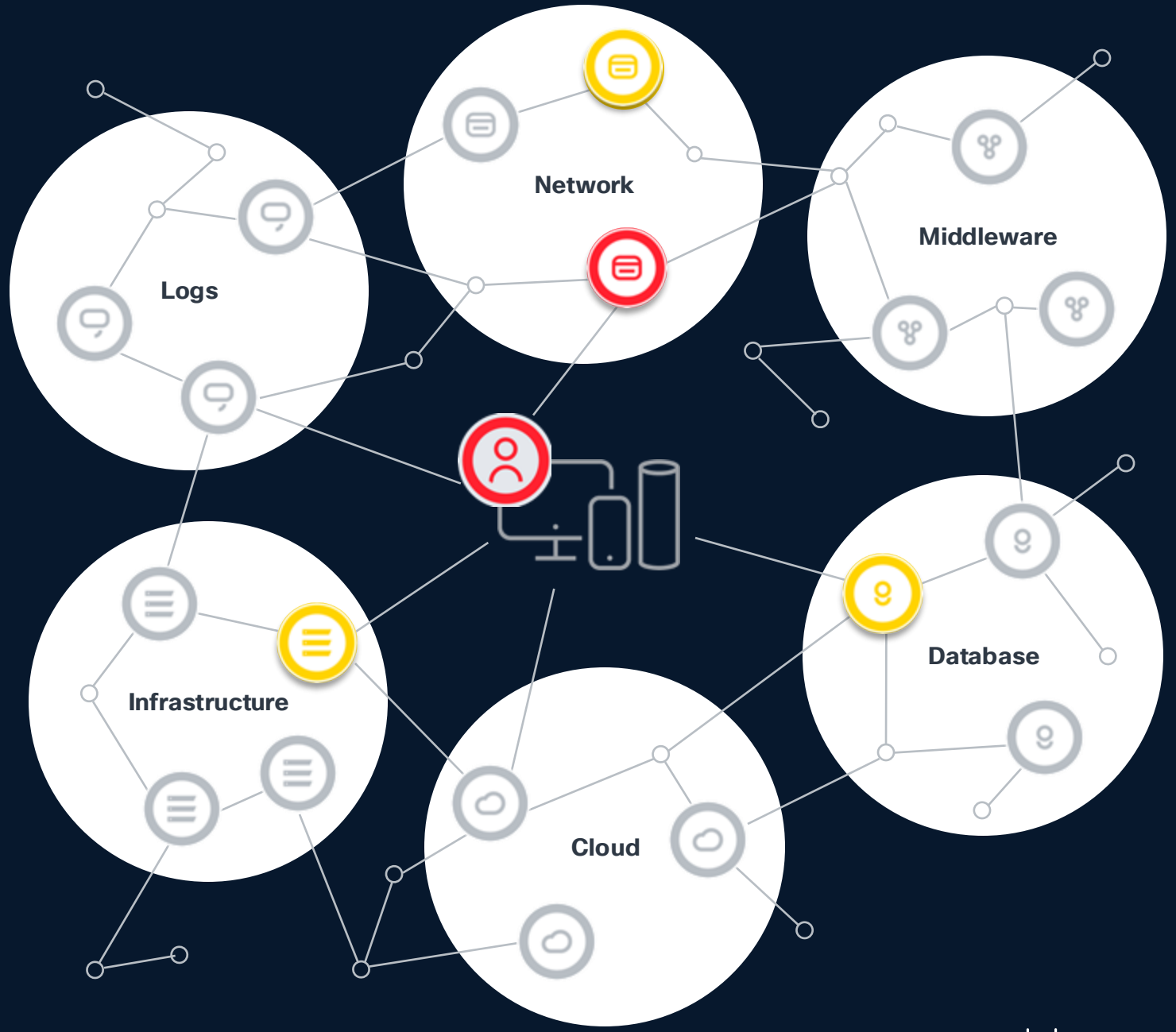
CISCO Connect

Introduction to Splunk Platform for Security & Observability

Robbie Baines, Splunk Observability Specialist

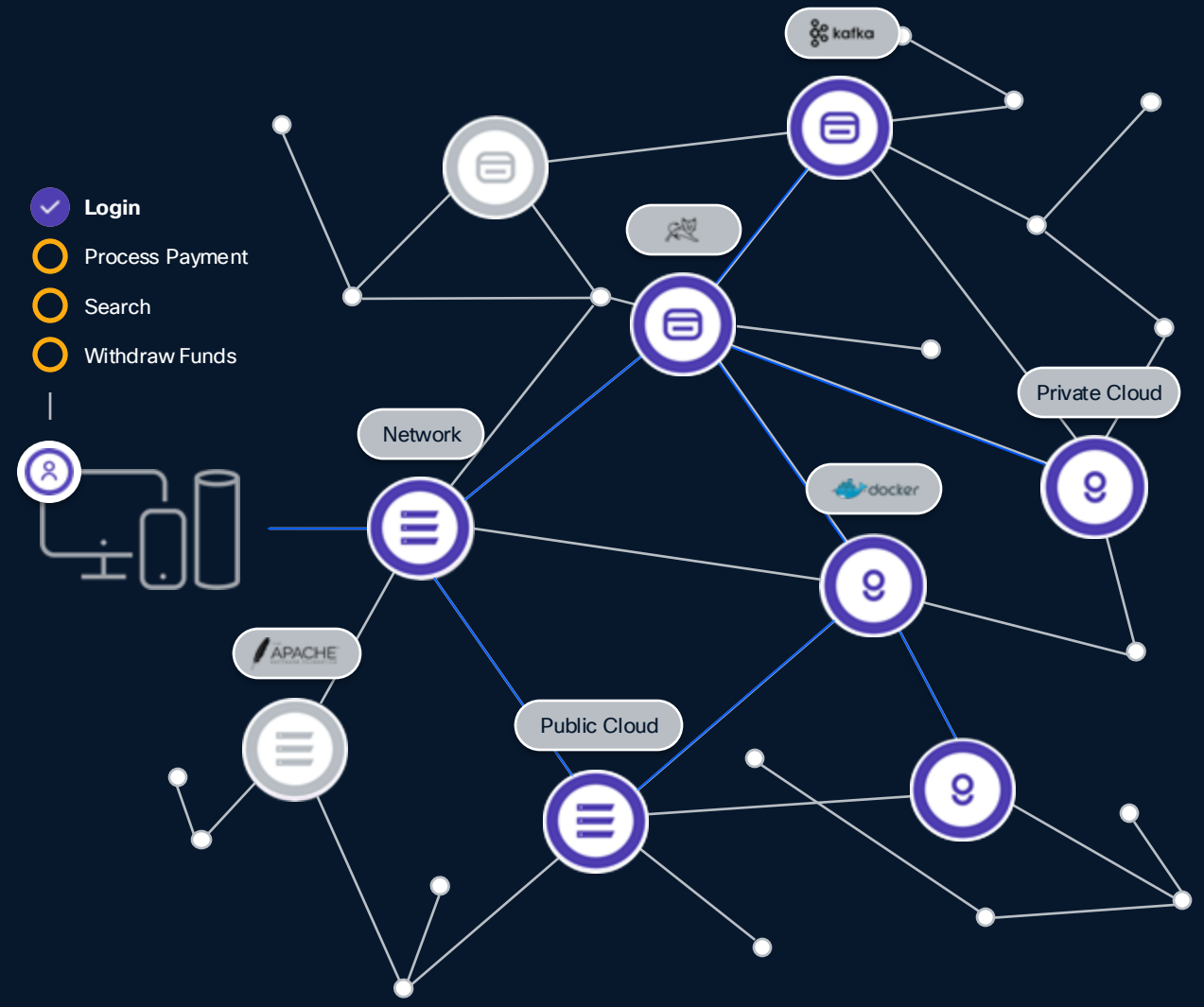
Teams rely on scattered visibility

Disconnected toolchains lead to blind spots for problems that span teams & services



Business context gets lost

It’s hard to triage performance problems based on business impact



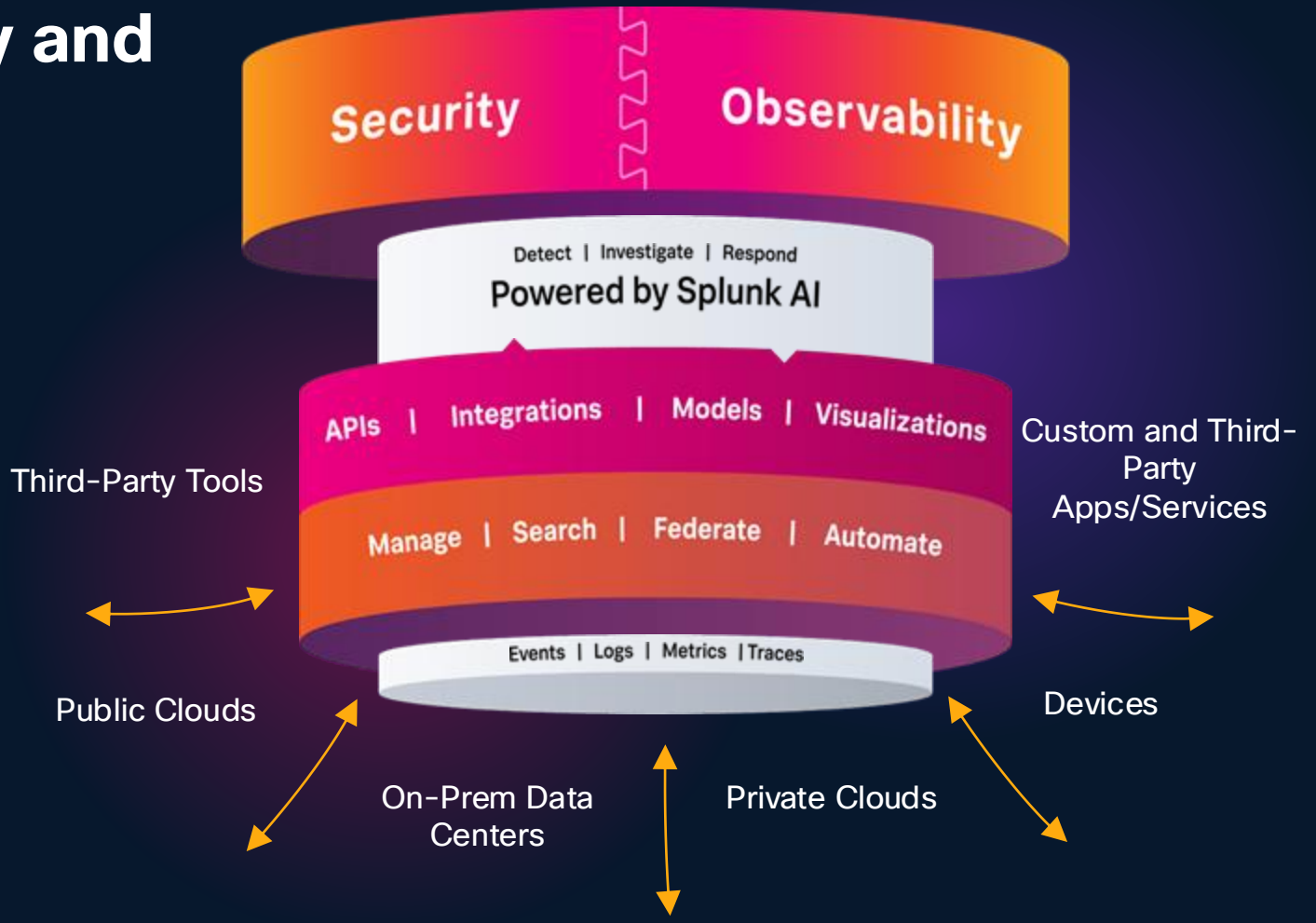
Splunk’s approach to Observability

Ensure the **resilience** of digital systems and reduce the **human toil** of operating them by letting **software** do more of the **heavy lifting,** to **identify problems, find root causes,** and **take corrective action.**

See the **business impact** of every performance problem

cisco

Splunk: The Unified Security and Observability Platform



Splunk Platform

Single source of truth, single resilience platform

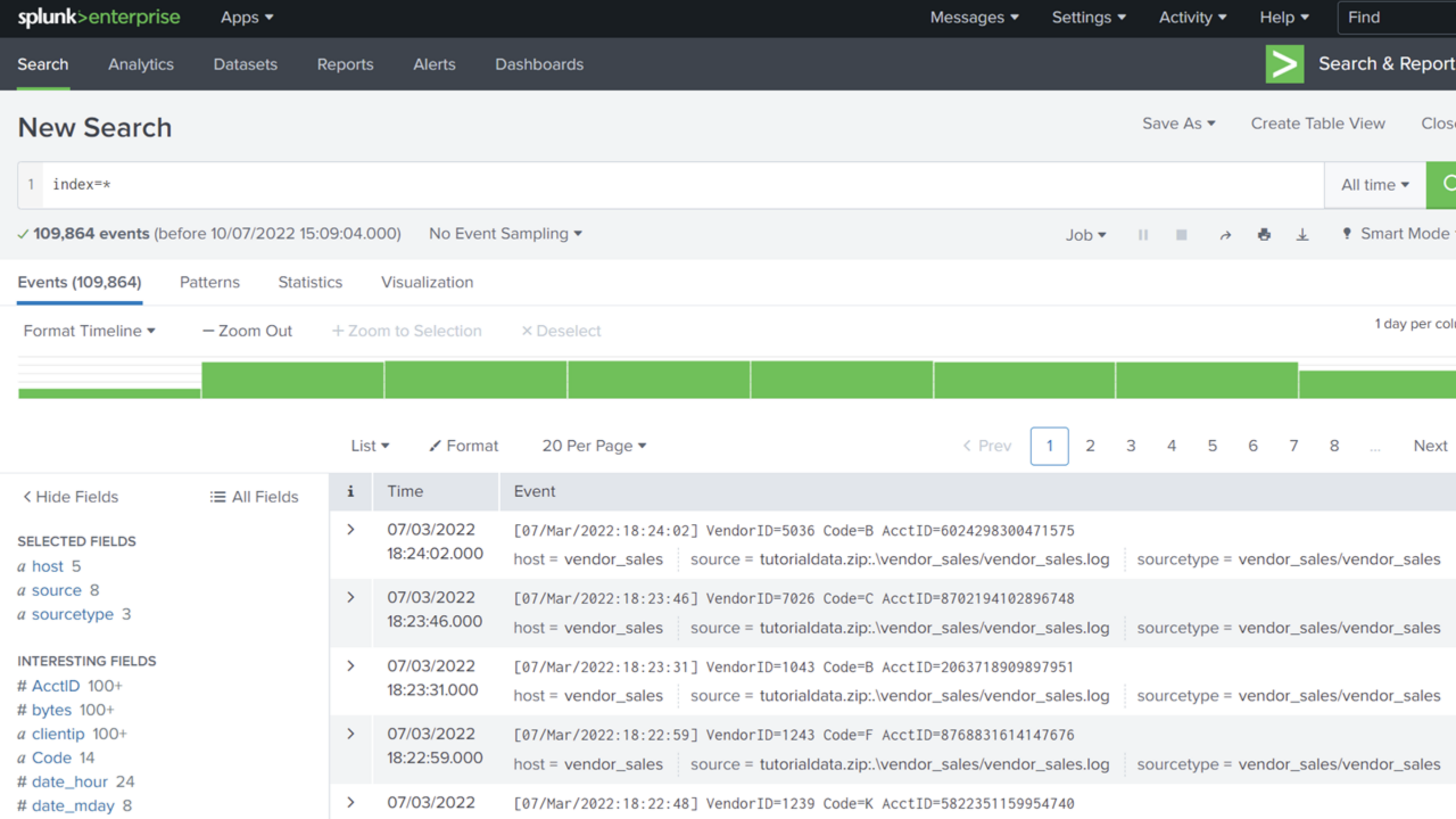
...all teams working together with shared context

Any Data From Any Source

Ask Any Question

- **IT Operations & Cap Planning**
- **Service Delivery**
- **Network, IoT, and Infrastructure**
- **Business Insights**
- **Security & Incident Response**

cisco


splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Report
New Search
Save As
Create Table View
1 index=*
All time
✓ 109,864 events (before 10/07/2022 15:09:04.000)
No Event Sampling
Job
Smart Mode
Events (109,864)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 day per col
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
...
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 5
a source 8
a sourcetype 3
INTERESTING FIELDS
AcctID 100+
bytes 100+
a clientip 100+
a Code 14
date_hour 24
date_mday 8
Time
Event
07/03/2022 18:24:02.000
[07/Mar/2022:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575
host = vendor_sales source = tutorialdata.zip:.\vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
07/03/2022 18:23:46.000
[07/Mar/2022:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748
host = vendor_sales source = tutorialdata.zip:.\vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
07/03/2022 18:23:31.000
[07/Mar/2022:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951
host = vendor_sales source = tutorialdata.zip:.\vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
07/03/2022 18:22:59.000
[07/Mar/2022:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676
host = vendor_sales source = tutorialdata.zip:.\vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
07/03/2022
[07/Mar/2022:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740

New Search

```
1 index="tutorialdata"
2 | where AcctID like "87%"
```

✓ **684 events** (before 9/12/22 10:56:05.000 PM) No Event Sampling

Events (684) Patterns Statistics Visualization

Format Timeline — Zoom Out + Zoom to Selection × Deselect

List Format 20 Per Page

Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
AcctID 100+
a Code 14
date_hour 24
date_mday 8

i	Time	Event
>	6/11/22 6:23:46.000 PM	[11/Jun/2022:18:23:46] VendorID=7026 Code=C AcctID=870?194102896748 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetyp
>	6/11/22 6:23:46.000 PM	[11/Jun/2022:18:23:46] VendorID=7026 Code=C AcctID=870?194102896748 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetyp
>	6/11/22 6:22:59.000 PM	[11/Jun/2022:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetyp
>	6/11/22 6:22:59.000 PM	[11/Jun/2022:18:22:59] VendorID=1243 Code=F AcctID=876?831614147676 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetyp

Machine Data Contains Critical Insights

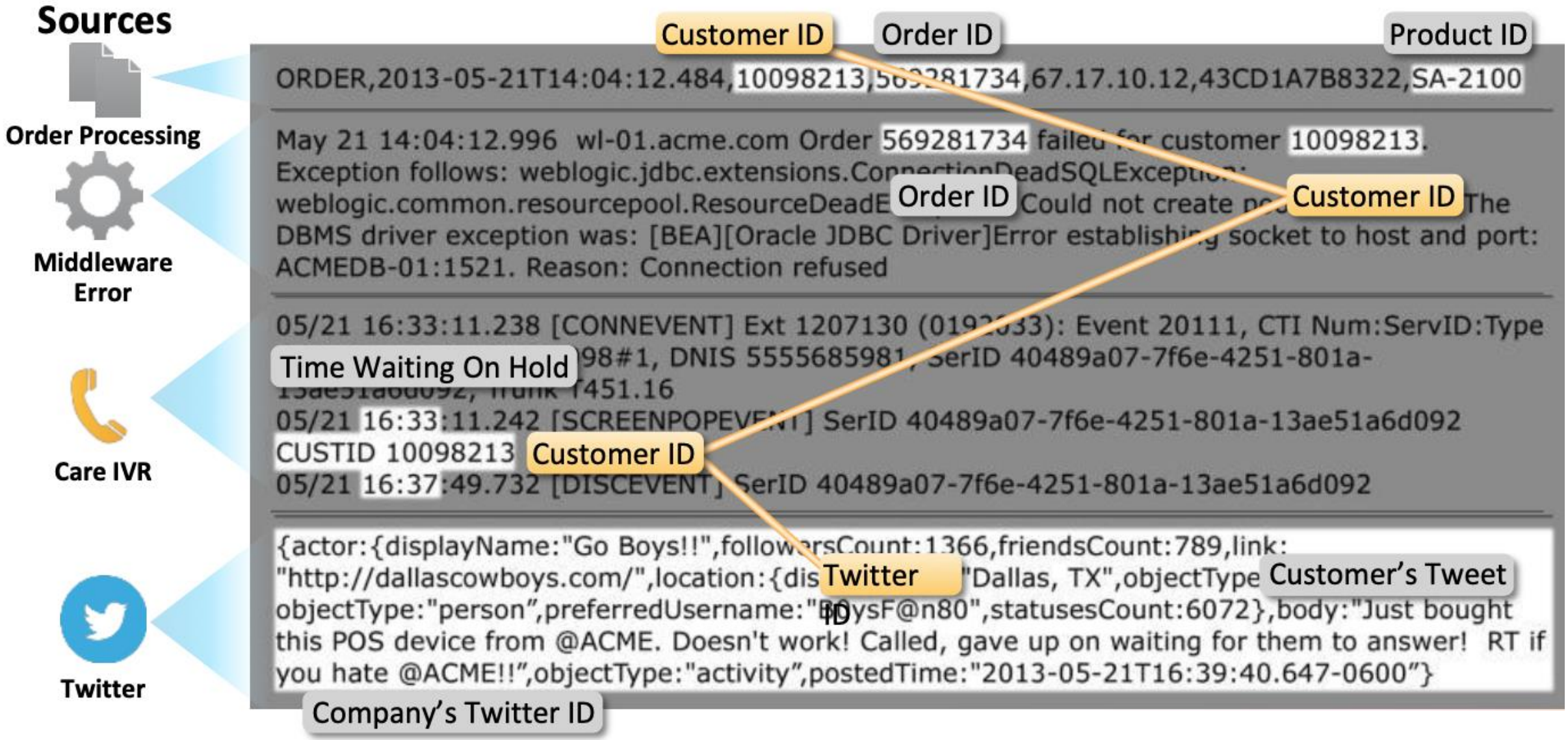


Table of Top 10 Issues

Site: Global

Issue Type	Priority	Count	Severity	Last Occurred	Names	Status	Device Name	IP Address	MAC Address	Family	Role	Site
EIGRP_Peering	P1	5	HIGH	2025-05-12 16:18:25	EIGRP Adjacency Failed on Device "LO-CN" Interface Vlan140 (Interface description: to_PDX_access) with Neighbor 10.93.140.7 EIGRP Adjacency Failed on Device "PDX-MGMT" Interface Vlan32 (Interface description: --) with Neighbor 10.93.141.42 EIGRP Adjacency Failed on Device "PDX-MGMT" Interface Vlan32 (Interface description: --) with Neighbor 10.93.141.41 EIGRP Adjacency Failed on Device "PDX-RO" Interface GigabitEthernet2 (Interface description: TO_CSR2_GI2) with Neighbor 10.93.131.2 EIGRP Adjacency Failed on Device "PDX-CORE" Interface Vlan140 (Interface description: to_PDX_access) with Neighbor 10.93.140.7	active active active active active	LO-CN PDX-MGMT PDX-MGMT PDX-RO PDX-CORE	10.93.141.20 10.93.141.29 10.93.141.29 10.93.141.23 10.93.141.18	30:8b:b2:ba:c2:80 40:14:82:f6:5f:80 40:14:82:f6:5f:80 00:1e:e6:06:0d:00 6c:03:b5:66:60:00	Switches and Hubs Switches and Hubs Switches and Hubs Routers Switches and Hubs	ACCESS ACCESS ACCESS BORDER ROUTER CORE	Global/OR/LO/Floor-3
BGP_Down	P1	2	HIGH	2025-05-12 17:08:44	BGP is down on 'PDX-RO' with neighbor '10.93.141.17' BGP is down on 'PDX-MGMT' with neighbor '10.93.141.41'	active active	PDX-RO PDX-MGMT	10.93.141.23 10.93.141.29	00:1e:e6:06:0d:00 40:14:82:f6:5f:80	Routers Switches and Hubs	BORDER ROUTER ACCESS	Global/OR/PDX/Floor-2
infra_link_down	P1	2	HIGH	2025-05-13 04:01:04	Interface "GigabitEthernet0/0" (Interface description: --) is down on network device "NYC-ACCESS" Interface "GigabitEthernet1/0/18" (Interface description: --) is down on network device "LO-BN"	active active	NYC-ACCESS LO-BN	10.93.141.26 10.93.141.28	30:8b:b2:b5:32:00 90:77:ee:ac:ab:80	Switches and Hubs Switches and Hubs	DISTRIBUTION CORE	Global/NY/NYC/Floor-8
BGP_Flap	P2	2	HIGH	2025-05-12 16:15:17	BGP is Flapping on Device "PDX-RO" with Neighbor 10.93.141.17 BGP is Flapping on Device "PDX-MGMT" with Neighbor 10.93.141.41	active active	PDX-RO PDX-MGMT	10.93.141.23 10.93.141.29	00:1e:e6:06:0d:00 40:14:82:f6:5f:80	Routers Switches and Hubs	BORDER ROUTER ACCESS	Global/OR/PDX/Floor-2
global_ap_disconnect_trigger	P2	1	HIGH	2025-05-12 15:47:58	AP(s) disconnected from WLC on Switch "LO-BN".	active	LO-BN	10.93.141.28	90:77:ee:ac:ab:80	Switches and Hubs	CORE	Global/OR/LO/Floor-3
default_trap_event_trigger	P3	1	HIGH	2025-05-13 04:00:59	Stack member 1 removed from stack.	active	PDX-MGMT	10.93.141.29	40:14:82:f6:5f:80	Switches and Hubs	ACCESS	Global/OR/PDX/Floor-2

Cisco Catalyst Center ▾ | Dashboards ▾ | Search

Overview

Edit | Export ▾ | ...

This dashboard provides an overview of various metrics and statistics in the Cisco Catalyst network.

Time Range: Last 24 hours ▾

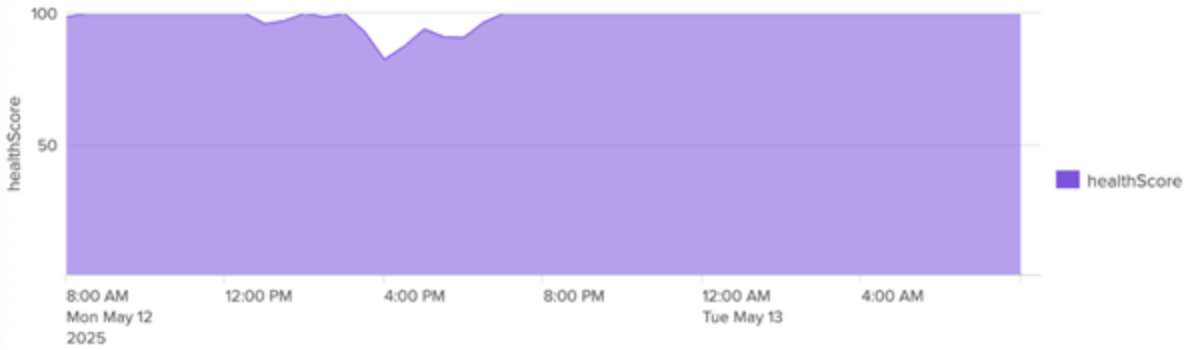
Cisco Catalyst Center Host: https://10.93.141.45 ▾ ×

Site: Global

Submit | Hide Filters

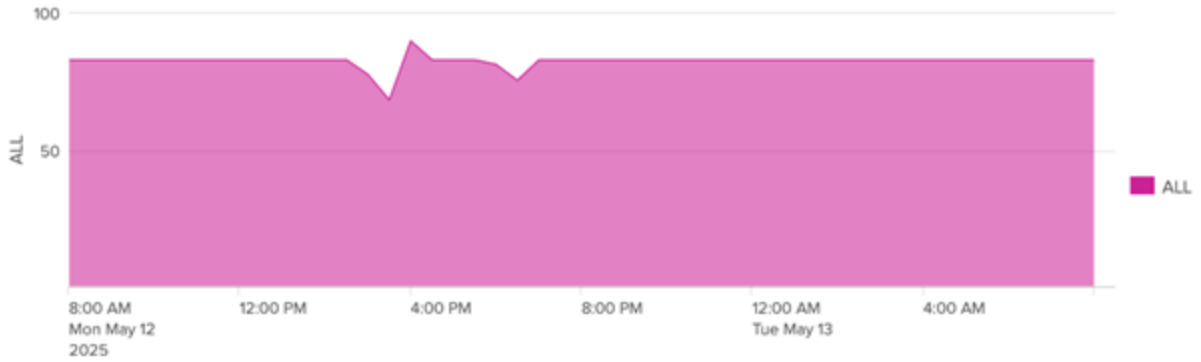
Average Network Health Score

Site: Global



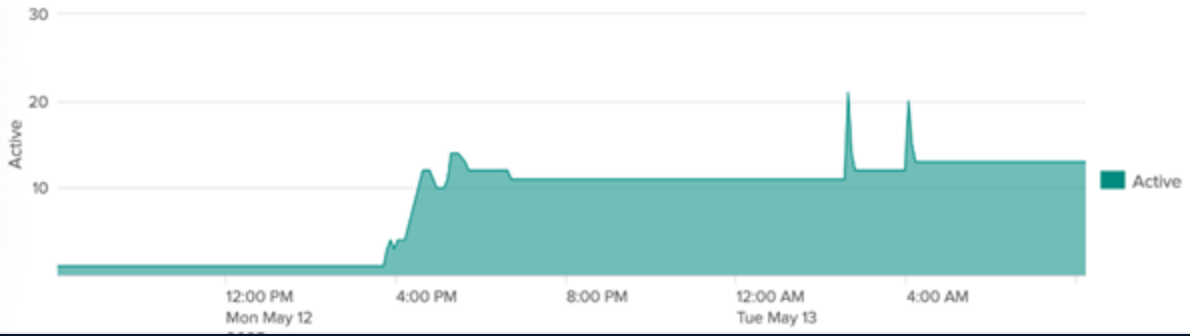
Average Client Health Score

Site: Global



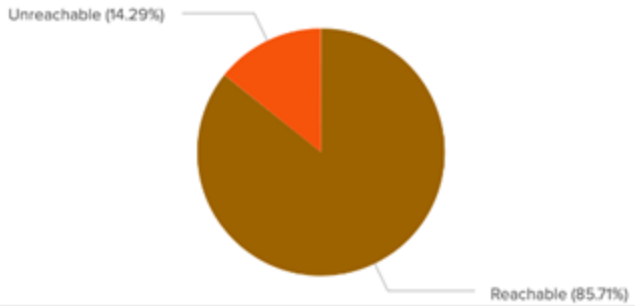
Total Number of Active Issues

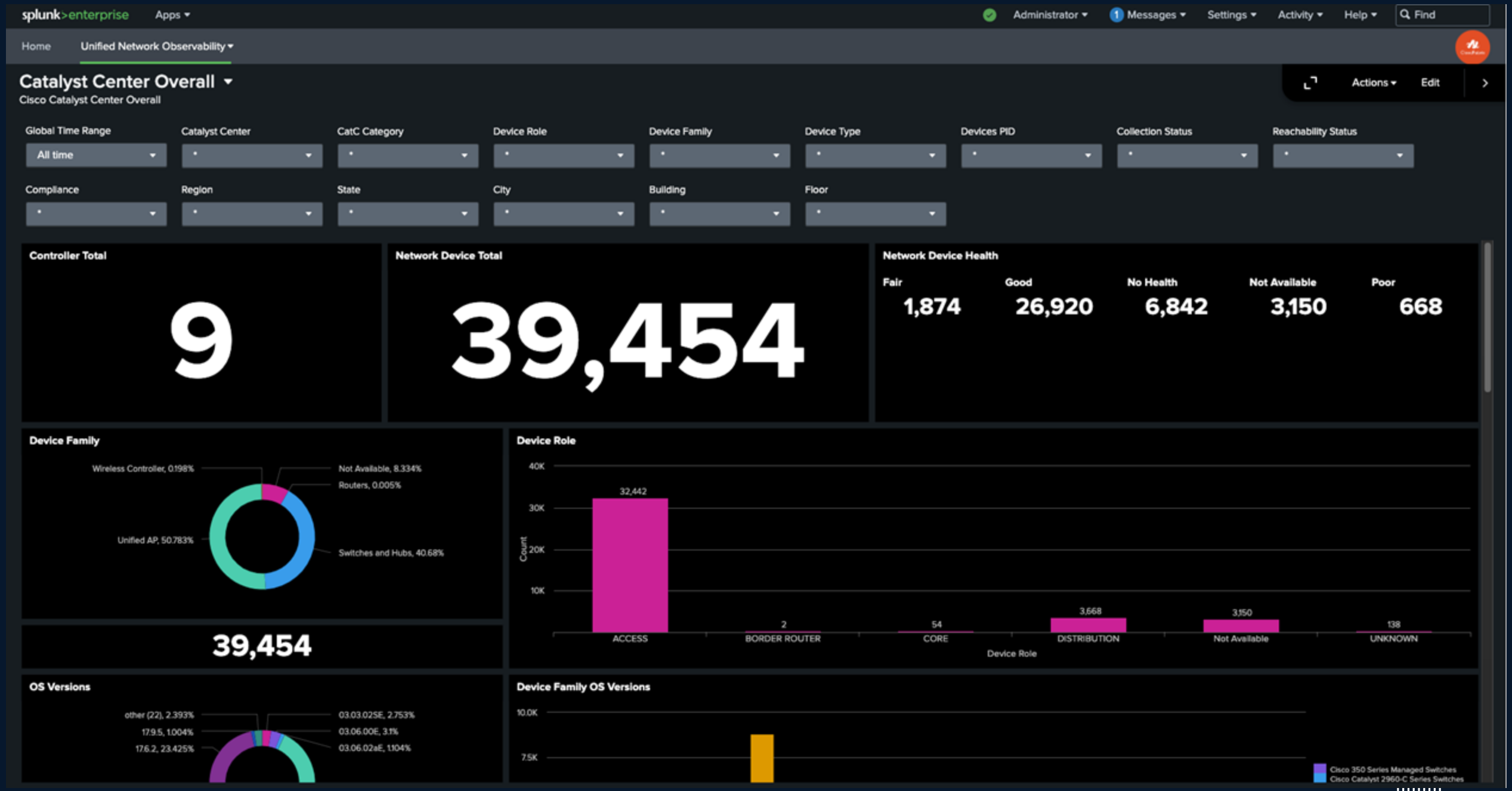
Site: Global



Device Reachability Type Percentages

Site: Global





RWI - Executive Dashboard

Show Filters

Edit Export ...

Active VPN Sessions

2,451

Description: Current number of connected workers.

Active Zoom Meetings

419

Description: Current number of Zoom meetings.

Most Popular App Today

Salesforce

718 Unique Users Accessed the App Today

Description: Most popular apps accessed today.

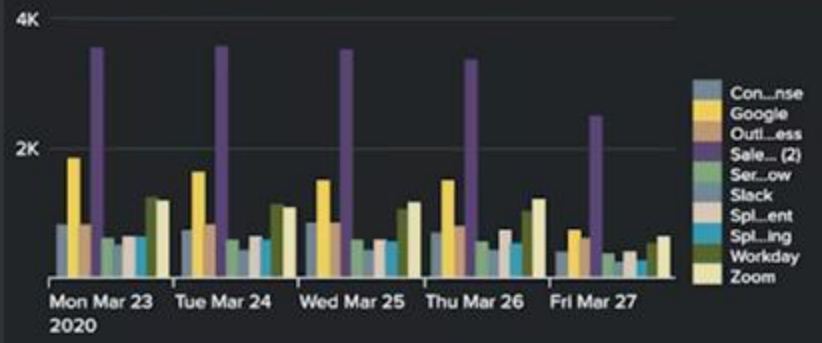
Number of VPN Logins

Description: Number of workers connecting to VPN over time on a daily basis.

Number of Zoom Meetings

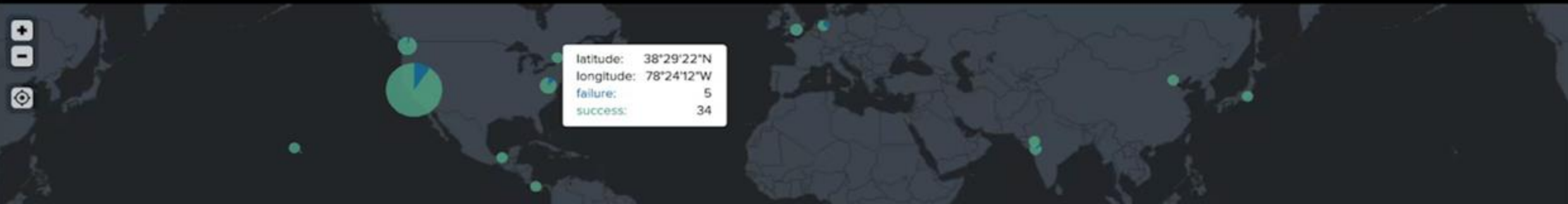
Description: Number of Zoom Meetings created over time on a daily basis.

Top Apps



Description: Top applications accessed over time.

Connected Workforce by Location



Estimated Billing - Current Month

Edit | More Info

Account ID: × All

Currency: USD

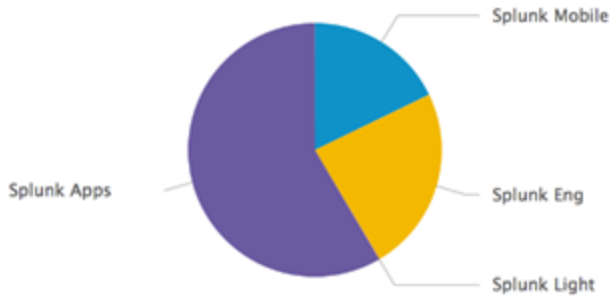
Estimated Cost - Month to Date

$33,419

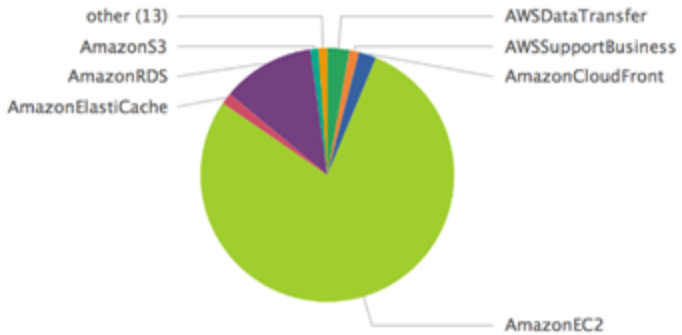
Total Projected Cost - This Month

$41,373

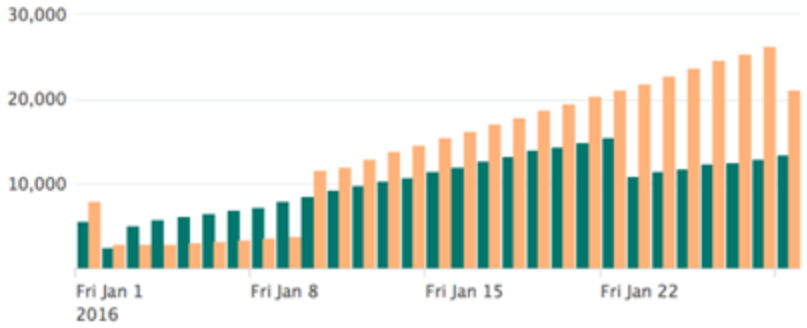
Estimated Cost by Account



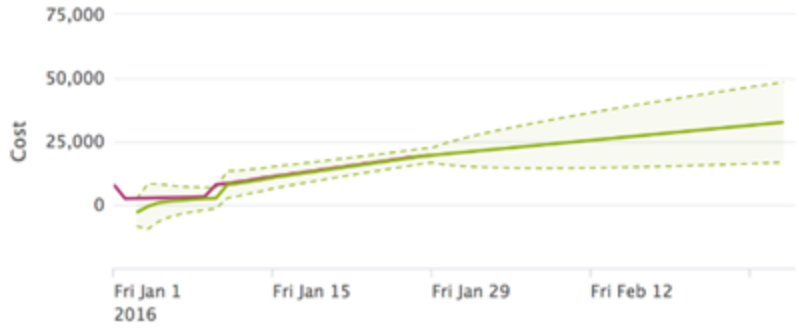
Estimated Cost by Service



Month over Month Comparison - Daily Cost



Cost Projection Over Time



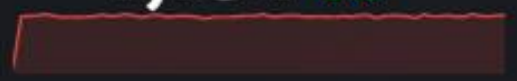
Estimated Cost by Account and Service - Month to Date

Account ID	Account Name	Service	Cost	Percentage
737126726831	Splunk Cloud OPS	AmazonEC2	$13928	41.68%
063605715280	Splunk Mobile	AmazonEC2	$5565	16.65%
111353726070			$3940	11.79%
111353726070		AmazonEC2	$3571	10.69%
737126726831	Splunk	AmazonRDS	$3445	10.31%

Data Center Sensors

Power Utilization

4,151 0%



Updated a few seconds ago

Water Capacity

102% ↓ -5%

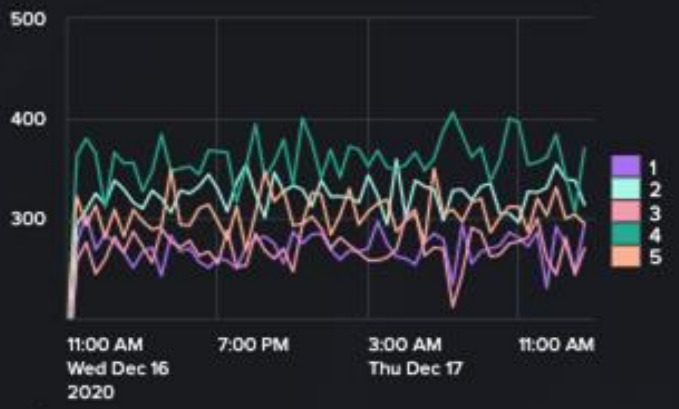
Updated a few seconds ago

Room Temperature

106° ↓ -4

Updated a few seconds ago

Power Usage



Server Room Heatmap

Anomalies Detected

System	Rack	Devices	Value
Power	2	PDU-02	3400
Power	2	PDU-07	2375
Power	2	PDU-12	2245

Host	Priority	Rack	Row
mysql-02	High	2	A
storage_web...	Medium	2	A
storage_exc...	High	2	C
db-01	Critical	2	A
websphere-01	Medium	2	A
websphere-01	Medium	2	A

‹ Prev 1 2 Next ›

splunk>enterprise Apps ▾ | Administrator ▾ | Messages ▾ | Settings ▾ | Activity ▾ | Help ▾ | Find

Overview | Working Dashboards ▾ | Inspirational Dashboards ▾ | Cloud Platforms | Useful Datasets ▾ | Electricity Carbon Intensity ▾ | Documentation ▾ | All Objects ▾ | Sustainability Toolkit for Splunk

Unified Sustainability Dashboard

The Splunk T_Shirt Co.

Energy Cost

To Date This Year

$95,729

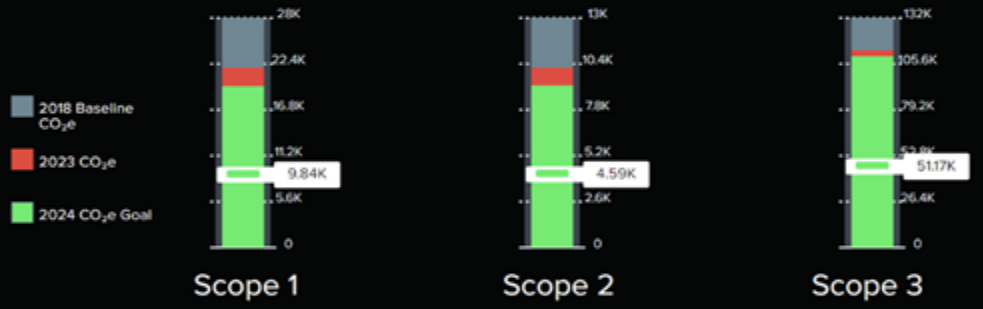
Total CO_2e

To Date This Year

134,020kg

CO_2e Emissions

Year To Date



This Year

Last Year

Realtime Performance

Last 4 hours

	Buildings	End User Devices	Data Centers	Factories
CO_2e kg	3,804	1,465	6,893	7,306
Energy kWh	2,808	1,213	5,285	5,534
Energy $	896	520	1,144	1,009

Splunk Observability

Meeting customers where they are

Traditional environments

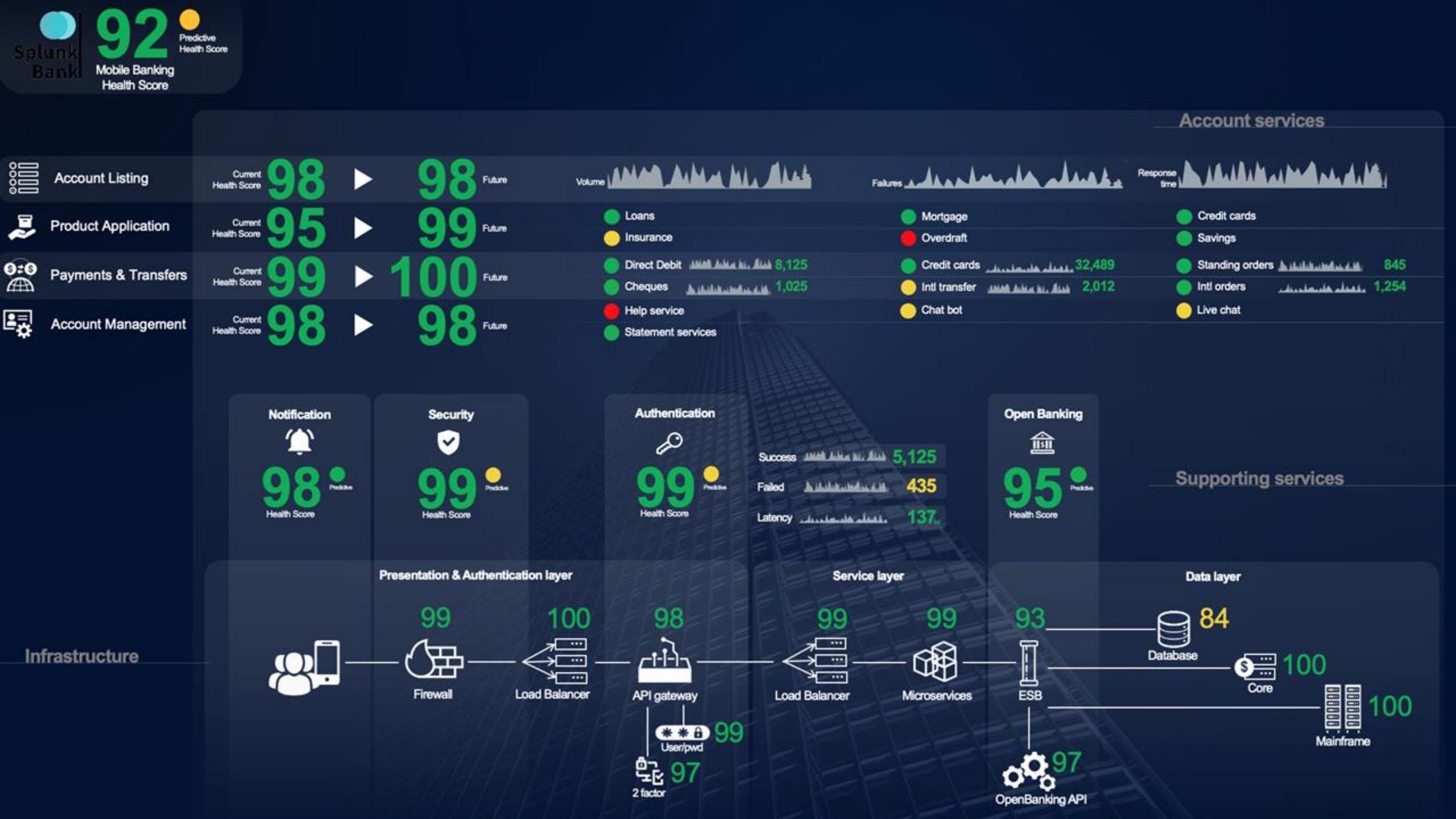
Unified Observability Experience

- APM
- Infrastructure Monitoring
- Digital Experience Monitoring
- Business Insights
- Application Security
- Observability for AI
- Network Observability

Splunk Platform

Cloud native environments

cisco


Splunk Bank
92
Predictive Health Score
Mobile Banking Health Score
Account services
Account Listing
Current Health Score 98
98 Future
Volume
Failures
Response time
Product Application
Current Health Score 95
99 Future
Loans
Insurance
Mortgage
Overdraft
Credit cards
Savings
Payments & Transfers
Current Health Score 99
100 Future
Direct Debit 8,125
Cheques 1,025
Credit cards 32,489
Intl transfer 2,012
Standing orders 845
Intl orders 1,254
Account Management
Current Health Score 98
98 Future
Help service
Statement services
Chat bot
Live chat
Notification
98 Predictive Health Score
Security
99 Predictive Health Score
Authentication
99 Predictive Health Score
Success 5,125
Failed 435
Latency 137
Open Banking
95 Predictive Health Score
Supporting services
Infrastructure
Presentation & Authentication layer
Service layer
Data layer
99
100
98
99
99
93
84
Firewall
Load Balancer
API gateway
Load Balancer
Microservices
ESB
Database
100
Core
100
Mainframe
99
User/pwd
97
2 factor
97
OpenBanking API

IT Services

Global Time Range

Last 24 hours

splunk> a cisco company

IT Services Dashboard

84 Overall Health Score

77 Predictive Health Score

Users 110

Overall IT Health Scores of all Locations

Location	Emails	Documents	Phone Calls	IT Health Score
Zurich	57	27	63	48
Vienna	617	109	33	86
Luxembourg	1222	190	27	90
Dubai	541	111	28	95
London	912	118	40	95

< Prev 1 2 Next >

IT Services

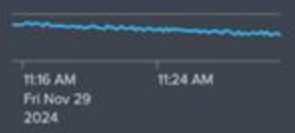
92 Service Health Score

Email

73 Health Score

Phishing Mails 5..

Total Emails 108

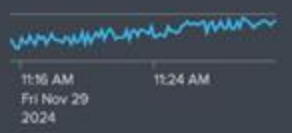


COMS

94 Health Score

Failed Downloads 13..

Total Documents 1,405



Phone

94 Health Score

Call Drops 27

Total Calls 11

Applications

93 Application Health Score

Cloud

Azure 99 Health Score

Microsoft 365 92 Health Score

Teams 93 Health Score

Salesforce 93 Health Score

Azure AD 93 Health Score

On-premise

Exchange 54 Health Score

SharePoint 92 Health Score

Kubernetes 93 Health Score

Unify 99 Health Score

Network

92 Health Score

Firewall 92 Health Score

Switch 97 Health Score

Web Server 96 Health Score

Router 92 Health Score

Access Points 93 Health Score

VPN 93 Health Score

Virtualization

96 Health Score

VMware VM 95 Health Score

Citrix 96 Health Score

Hyper-V 99 Health Score

NetScaler 99 Health Score

On-premise Infrastructure

45 Health Score

Windows Server 22 Health Score

CPU Utilization 98.6%

Memory Utilization 99.2%

*nix Server 92 Health Score

CPU Utilization 20.4%

Memory Utilization 33.1%

Database & Storage

93 Health Score

Database Throughput 295 queries/sec ↑2

Storage Utilization 73.7%

TimeRange
Last 60 minutes

splunk> turn data into doing

Warehouse Management

96 Overall Health Score

92 Predictive Health Score

#Goods Receipts pcs 1,930

#Users 183

OTIF On-time In-full 98

#On-time Shipments lines 955

ServiceNow Tickets

Change Events 1,219

#Priority 1 8

Delivery → Goods Receipt → Warehouse → Goods Issue → Shipment

#On-time Shipments 98.0%

Infrastructure

92 Health Score | Uptime 99.0% | #Disconnections 6

Warehouse Management

SAP — #Orders 723

ConnectShip — 96 Health Score

FedEx — 98 Health Score

Oracle DB — 98 Health Score

Active Directory — 97 Health Score — #Login Failures 8

SQL Server — 77 Health Score

97 Health Score — Voice Picking

97 Health Score — Print Server

Printers — Ink 38% | #Queued Files 6

Devices | #off 4

off, 3% | on, 97%

98 Health Score — Warehouse Access Points

99 Health Score — Voice Pick RF Devices

97 Health Score — Mobile RF Devices

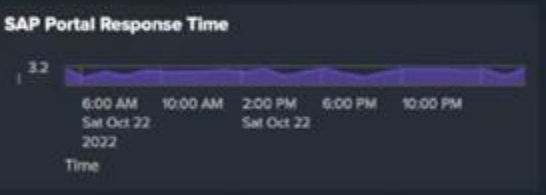
Network — 96 Health Score

The Splunk T_Shirt Co.

Order to Cash Service

Total Value of Open Orders **11.32m**

Presentation



Application

Infrastructure

SAP Predicted Health Score

New Order Acquisition in last hour **290** 0%

Goods Issue in last hour **232** ↓-3%

Invoice Creation in last hour **240** ↓-4%

Sales Orders in last hour **88** ↑9%

Splunk Security

Powering the SOC of the future with the leading TDIR solution

Traditional environments

Unified threat detection, investigation & response

Splunk Asset & Risk Intelligence	Splunk Attack Analyzer	Splunk SOAR	Splunk Enterprise Security
Continuous asset discovery	Automated threat analysis	Security automation	SIEM

Splunk Platform

Cloud native environments

cisco

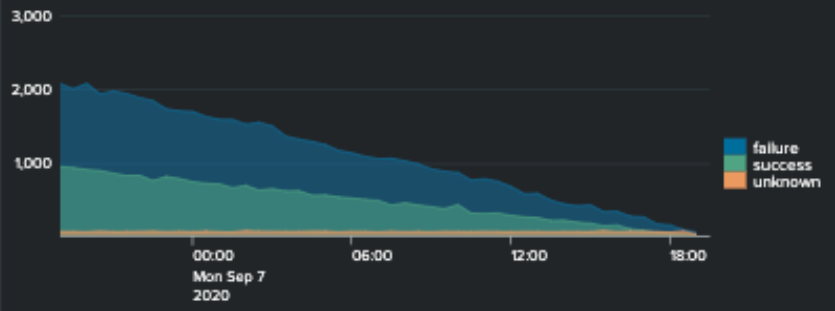
All Authentications

Show Filters

Edit | Export | ...

Failed Authentications	Successful Authentications	Applications	Users
53,233	23,277	5	206

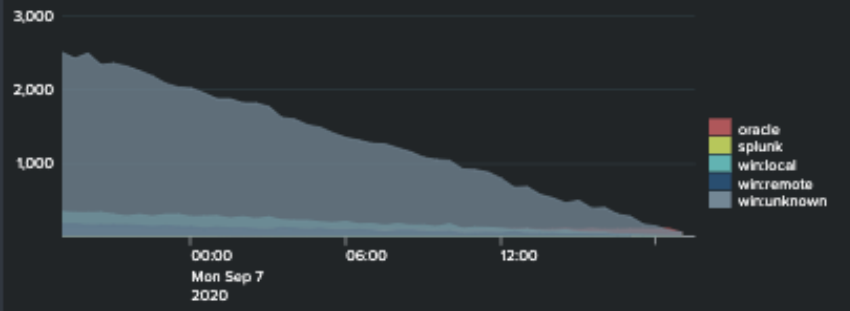
Access over Time by Action



Authentication Attempts by Application

app	count
splunk	2
win:remote	3724
oracle	4527
win:local	8267
win:unknown	62892

Access over Time by App



Top Authentications by Source

src	sparkline	count
oracle-test-host		1008
192.168.1.121		930
192.168.1.120		860
10.9.8.8		845
10.9.8.7		840
NY_APP_002		714
win-hp-68859		708

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Top Authentication Sources by Unique User Count

src	sparkline	user_count
win-lenovo-62060		99
macbook-74273		98
win-hp-30230		98
win-lenovo-13171		98
NY_DB_103		97
macbook-13273		97
win-lenovo-81712		97

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Security Posture

Edit | Export | ...

High Severity Intrusion Alerts v Previous 24 Hrs

2,776 ↗ 1,978

Infected Hosts v Previous 24 Hrs

54 ↗ 1

Malware Signatures v Previous 24 Hrs

13 ↗ 3

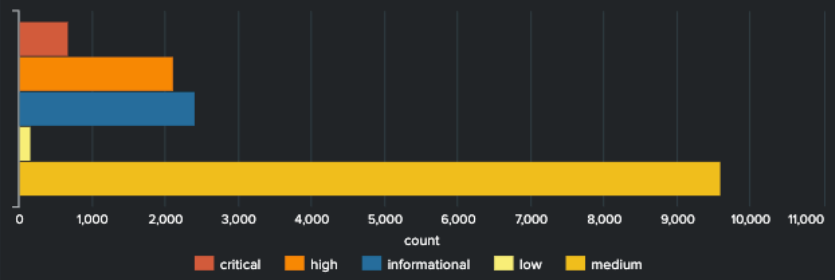
Hosts and Devices Reporting

234 ↘ -1

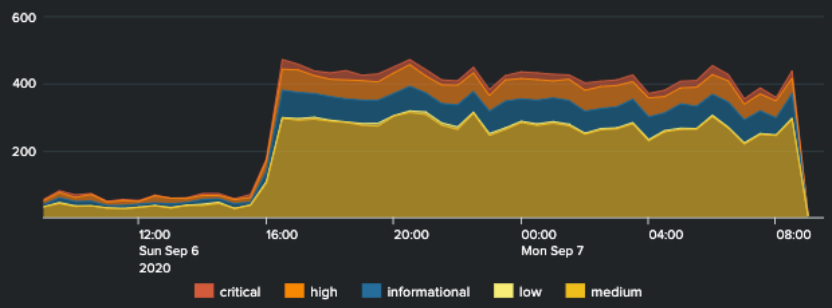
Accounts Monitored

211 ↘ -30

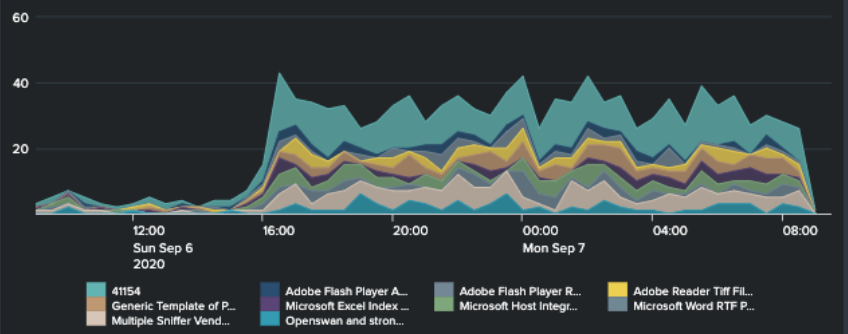
Intrusion Alerts by Severity



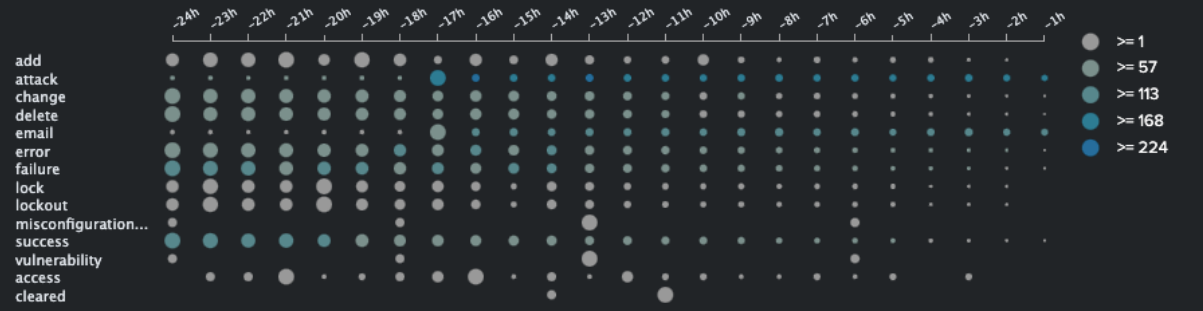
Intrusion Alerts over Time



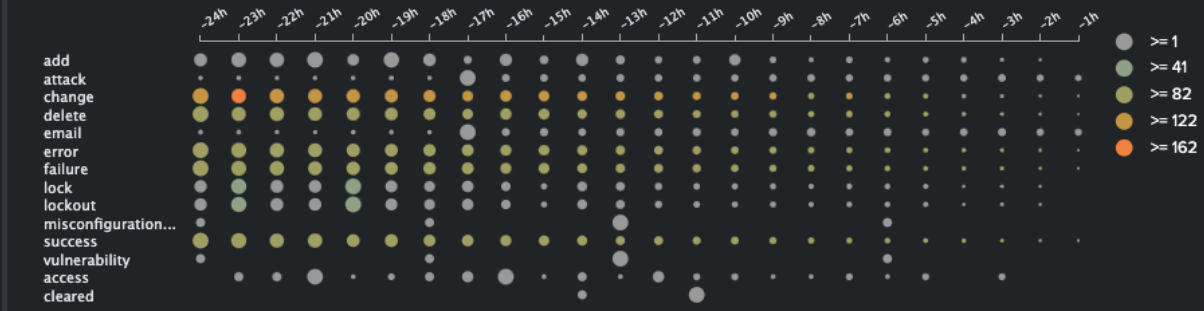
Top 10 Critical/High Severity Intrusion Alerts



360 View by Accounts: Event Types over Time



360 View by Hosts: Event Types over Time



cisco

Global Time Range: Sep 18, 2022 2:00 P...

Single #1 Selection: Count Of Security Ev...

Timechart Selection: By Domain

Table Selection: By Rule Name

splunk > Enterprise Security
Security Operations Executive Overview

Security Posture

408 ↑33	7 ↓-2	2 0	10 0
Total Case Count	Investigations Opened	UBA Anomalies Detected	New Infections Detected

Click For Data Glossary

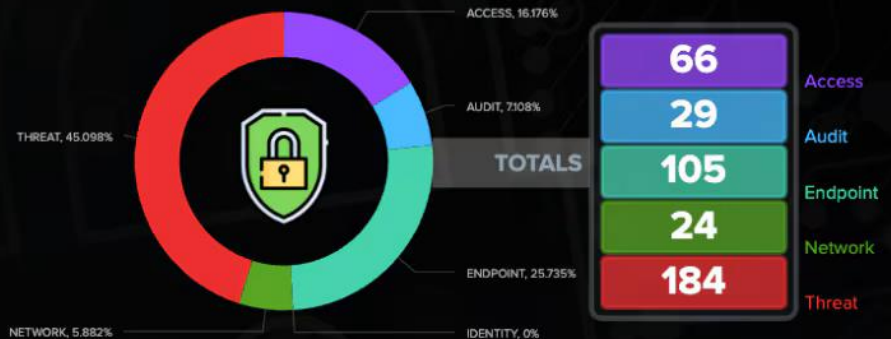
Overall Security Posture

- CRITICAL
- HIGH
- MODERATE
- LOW

Summary Of Security Events By Urgency

This is a summary of all security events, broken out by urgency, in your Splunk ES environment.

Summary Of Security Events By ES Domain



This is a summary of all security events, broken out by Enterprise Security Domain, in your Splunk ES environment.

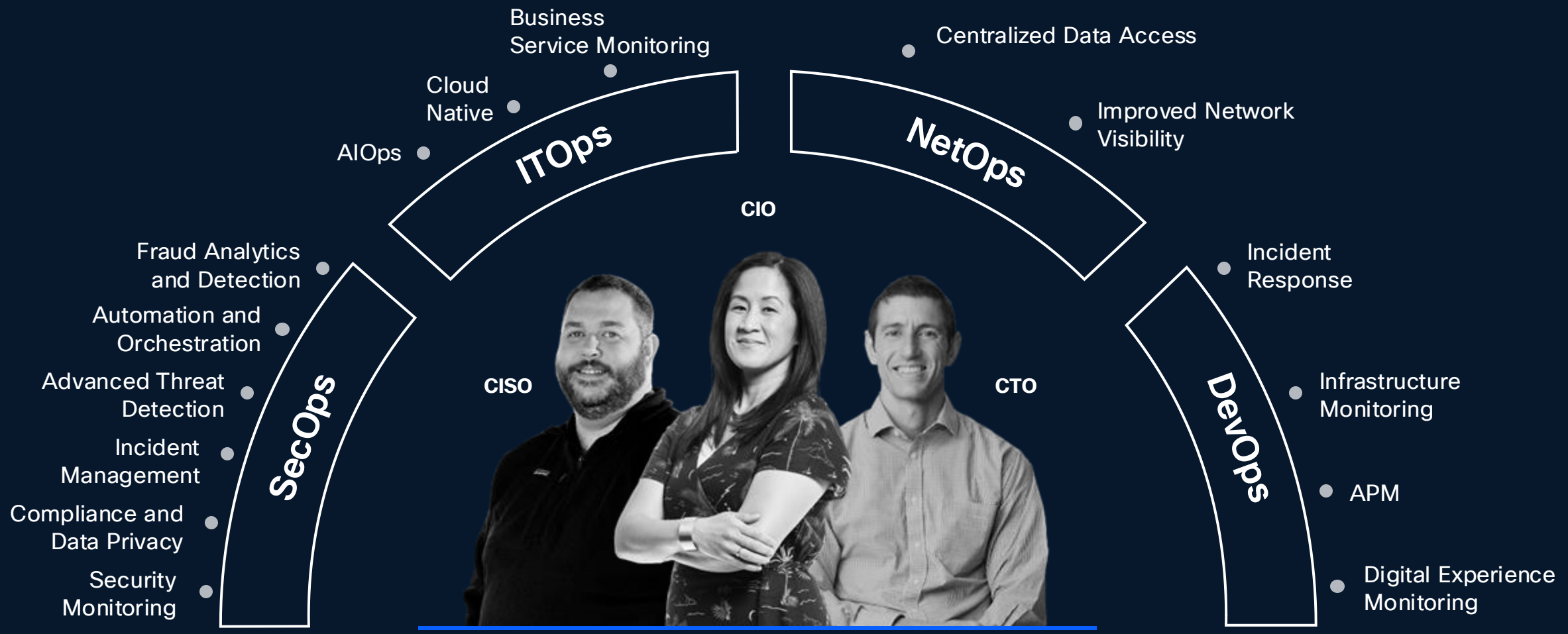
Timeline Of Security Events By Security Domain

Summary Of Security Events By Rule Name

This table is a detailed listing of top security events by security domain.

rule_name	security_domain	sparkline	count
Risk Threshold Exceeded For Object Over 24 Hour Period	threat		178
Host With Multiple Infections	endpoint		101
Excessive Failed Logins	access		66
Personally Identifiable Information Detected	audit		29
Abnormally High Number of HTTP Method Events By Src	network		24

We bring your teams together



The Unified Data Platform

Thank you