

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Unify Threat Detection, Investigation and Response

David Gamer | Principal Global Security Strategist

BRKSEC-1584

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

Questions?

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

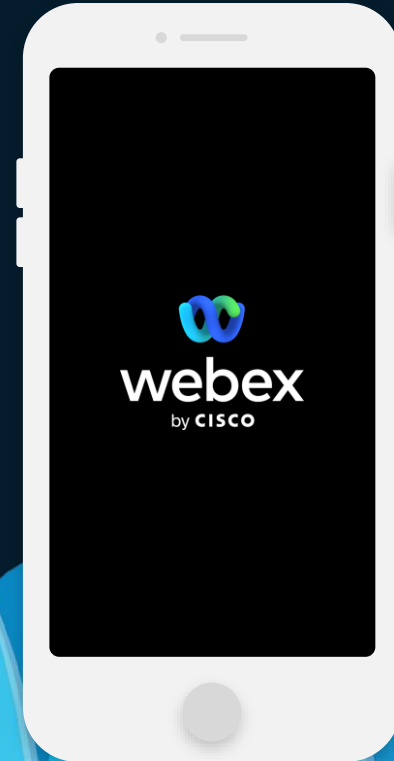
How

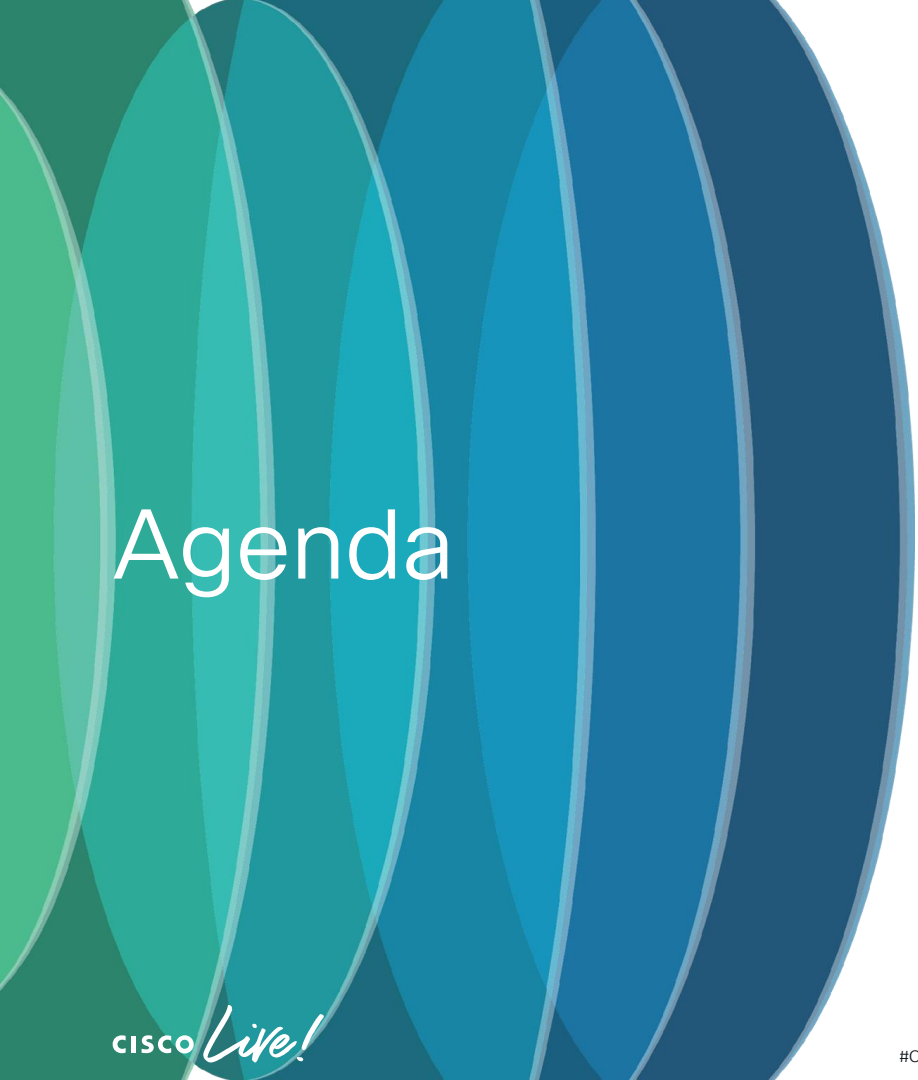
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

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



<https://ciscolive.ciscoevents.com/ciscolivebot/BRKSEC-1584>





Agenda

- The Security Problem
- A Modern Security Operation
- The Data Problem
- Using Data for Operations
- Automation
- Conclusion

#whoami



David Gamer
Principal Global Security
Strategist



Expanding Attack Surface

Persistent Security Operations Challenges

Source: [ESG SOC Trends Report 2023](#)



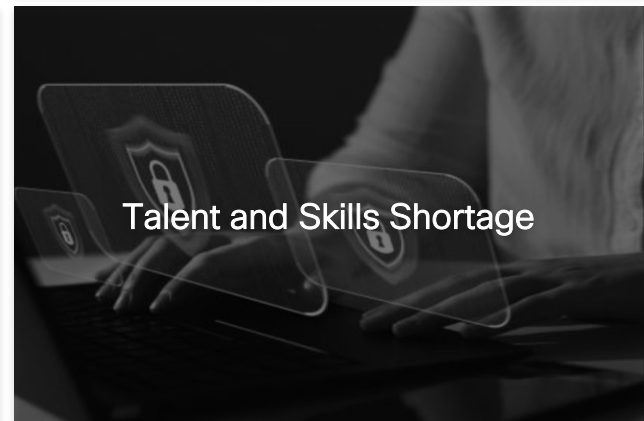
Siloed Tools, Teams, Data & Workflows



Growing Attack Volumes



Compliance Mandates and Requirements



Talent and Skills Shortage

Frequency of Preventable Incidents

2/3

of security leaders experienced an incident that could have been prevented if security operations were improved.

Source: [ESG SOC Trends Report 2023](#)

cisco *Live!*



Driving SOC modernisation

across detection, investigation, and response as a top priority to achieve **digital resilience**.

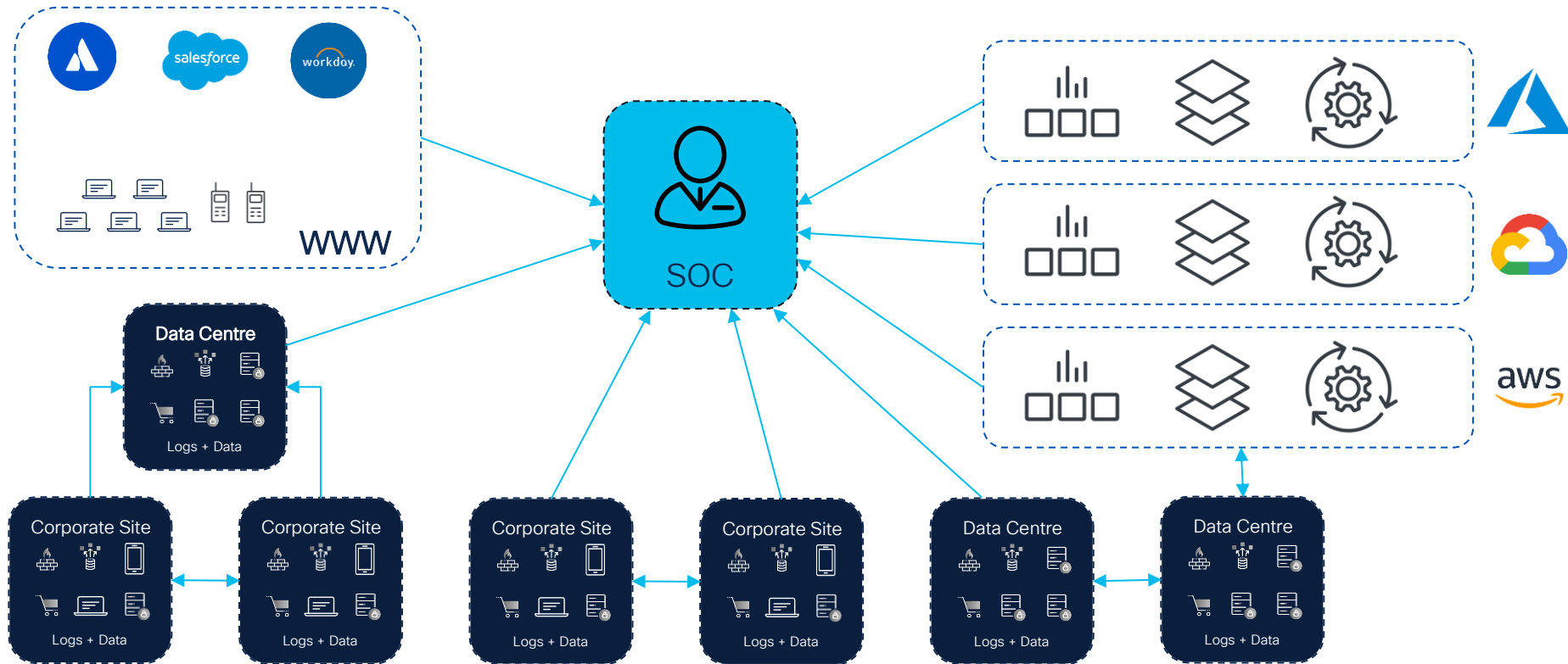
CISCO *Live!*

84%

of organisations claim improving efficacy and efficiency of SecOps is a top 5 priority.

Source: [ESG SOC Trends Report 2023](#)

Secops is simple, right? Not Really...



Key technology shifts in the SOC

Past

- **Limited visibility** across disconnected data sources and relying on ingest only approach hampers ability to identify high-risk threats amidst the digital noise.
- **Reactive threat detection** based on signatures or predefined rules with limited threat intelligence enrichment leading longer attacker dwell times.
- **Reliance on manual efforts** with limited automation for select routine tasks keeping your security team stuck in a reactive mode moving from tool to tool.
- **Lack of AI to help** guide SOC workflows providing no relief for an already overworked and overwhelmed security team.
- **Disjointed** threat detection, investigation, and response limiting MTTD and MTTR.

Future

- **Comprehensive visibility** across all data, no matter where located with context for full attack-surface coverage with no “weak” signals missed.
- **Proactive threat detection** using AI/ML, risk based approach, and comprehensive threat intelligence stopping advanced attacks and slashing dwell times.
- **Pervasive automation** across threat analysis, containment, response and recovery actions increasing security team’s productivity and efficiency.
- **AI guided SOC workflows** to help increase efficiency and effectiveness of the security team
- **Unified** threat detection, investigation, and response dramatically improving MTTD and MTTR.

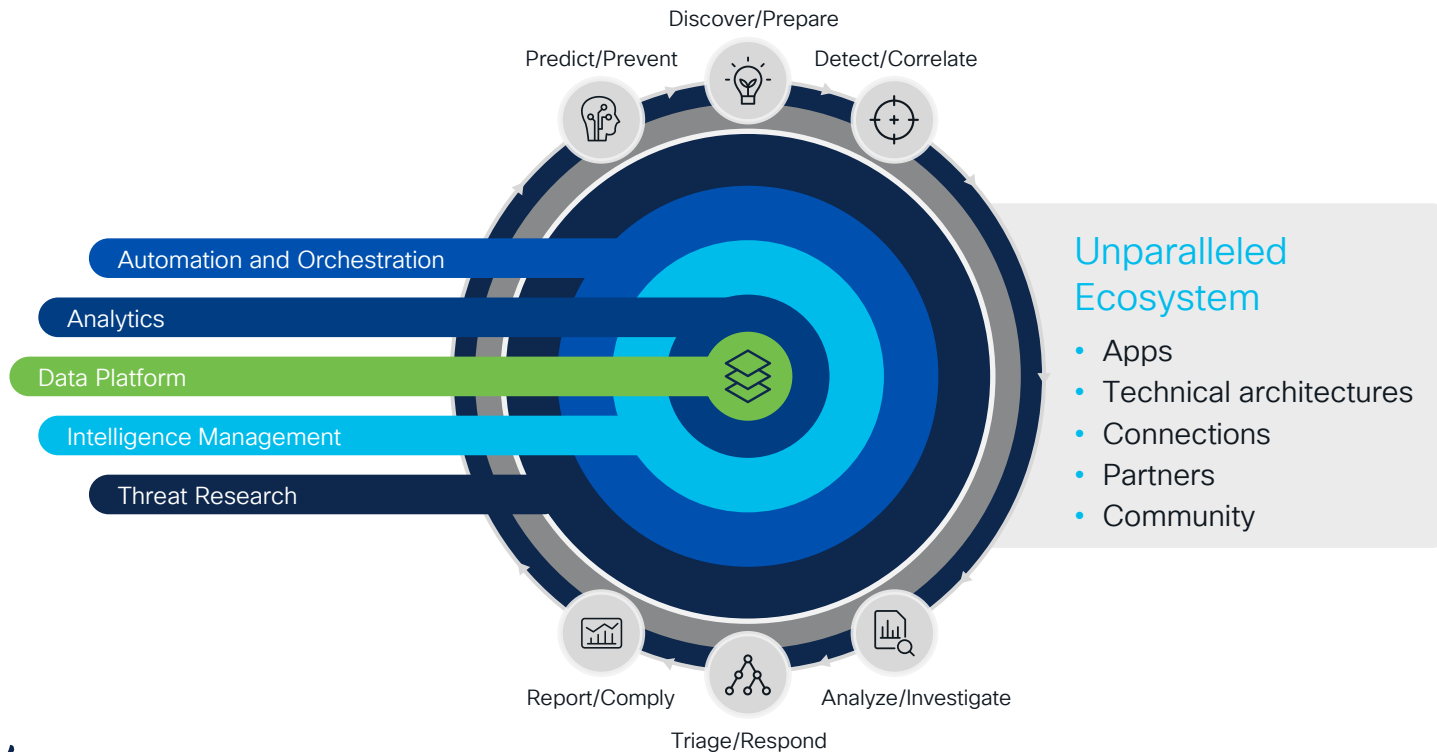
The SOC of the Future

Unified Threat Detection,
Investigation and Response
at the Core.



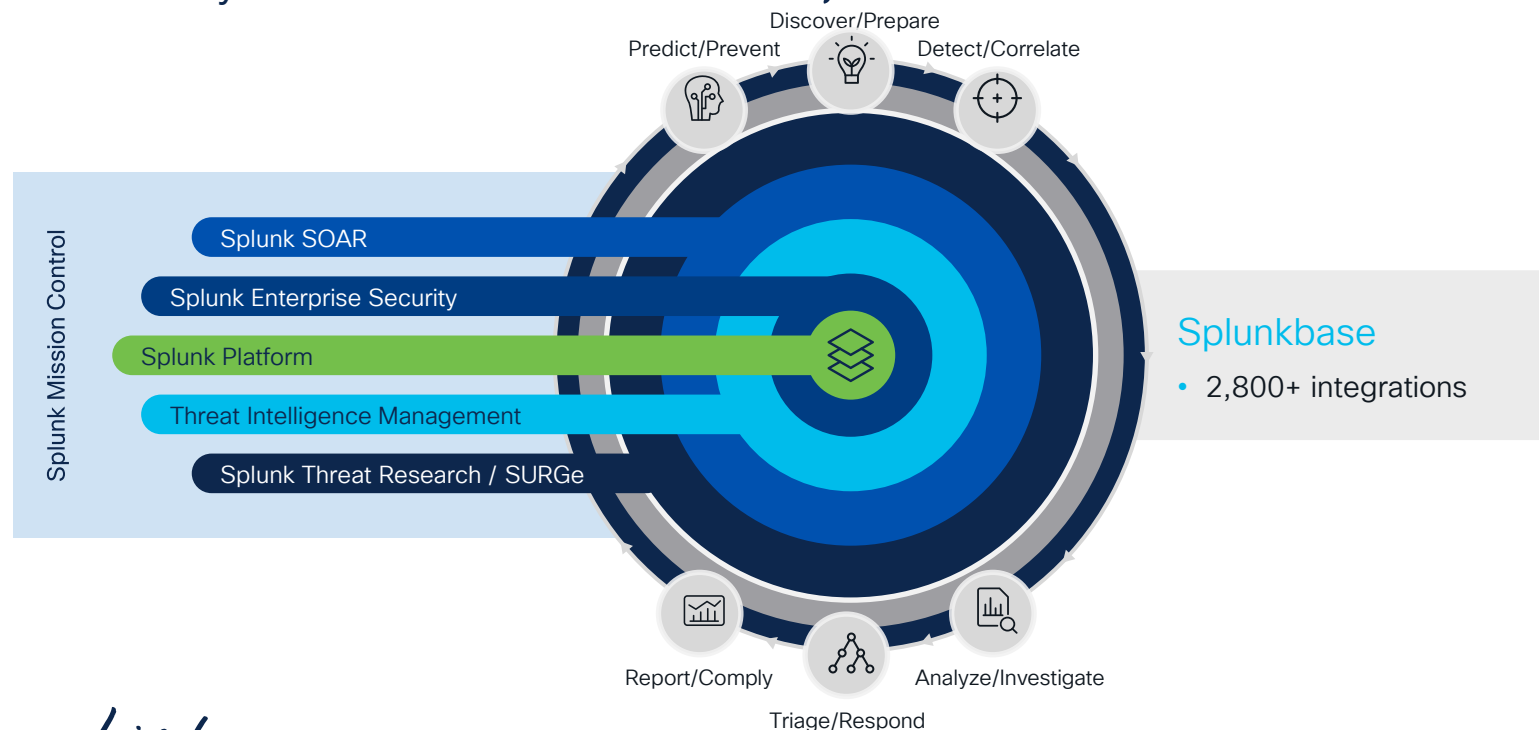
The Data-Centric Modern SOC

Threat Detection, Investigation and Response



Splunk Security for Threat Detection, Investigation and Response

The tools you need to build a modern, data-centric SOC



Splunk Security Focus Areas

2024-25: Key pillars of “SOC of the future”



Unified
TDIR with
automated
workflows



World class
detection



Insider
threat,
risk and
compliance



Federation



AI-guided
workflows

Solving the Data Problem

Growing data volume makes it harder to be resilient

\$200M

Yearly cost of **system downtime**

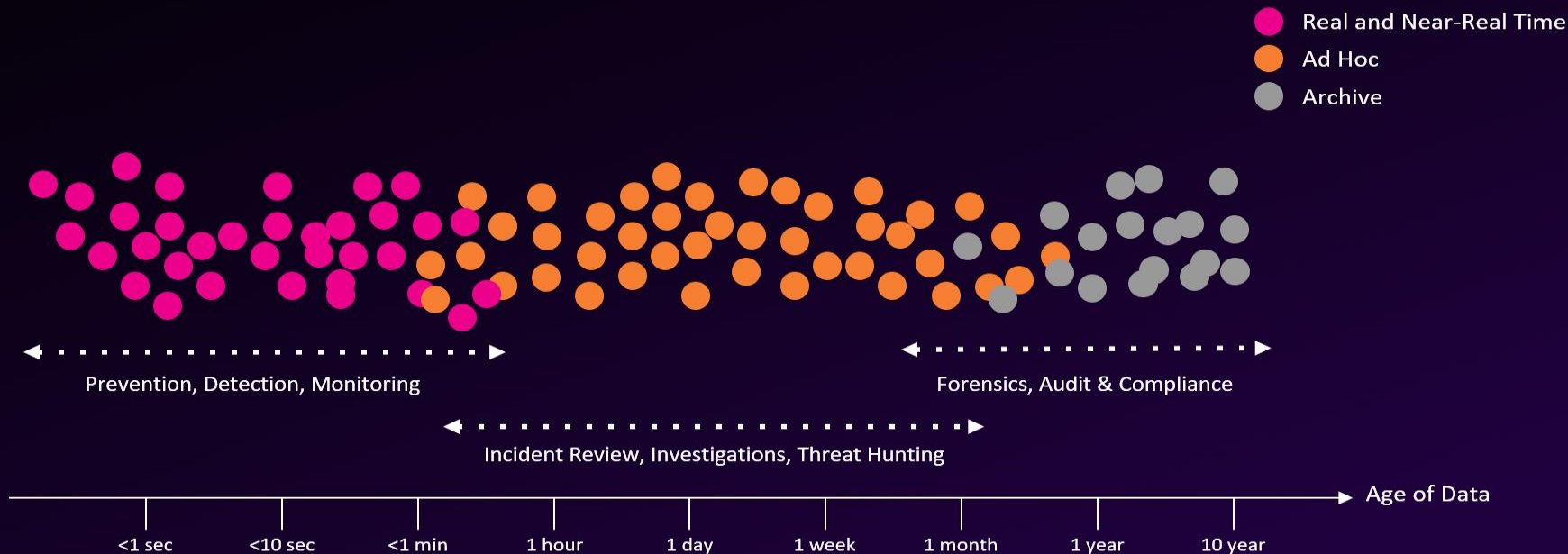
\$4.3M

Average cost of a **data breach**

90%

Of all data created in last 2 years, **AI demand for data accelerating**

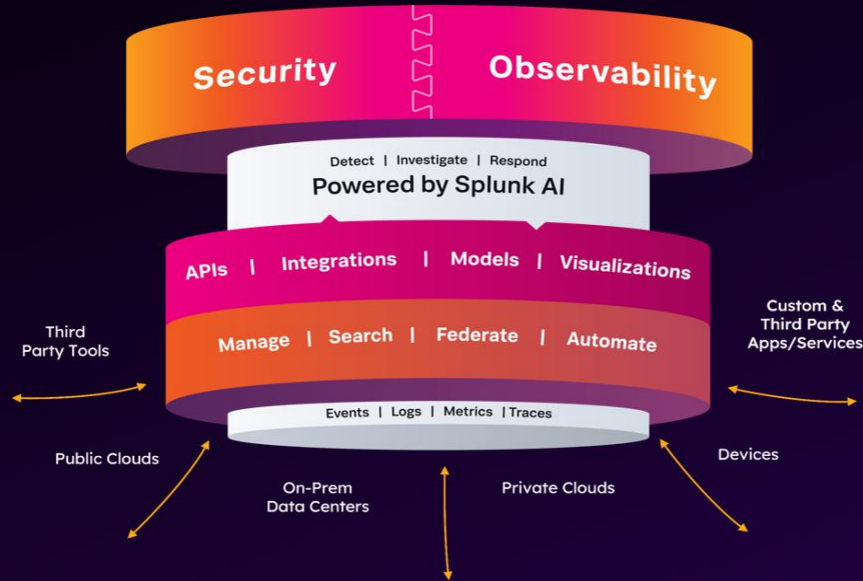
Data value varies by use case



© 2024 SPLUNK INC.

Enabling Enterprise Resilience

The Unified Security and Observability Platform



Access the Right

Data

Apply the Right

Analytics

Accelerate the Right

Actions

© 2024 SPLUNK INC.

CISCO *Live!*

#CiscoLiveAPJC

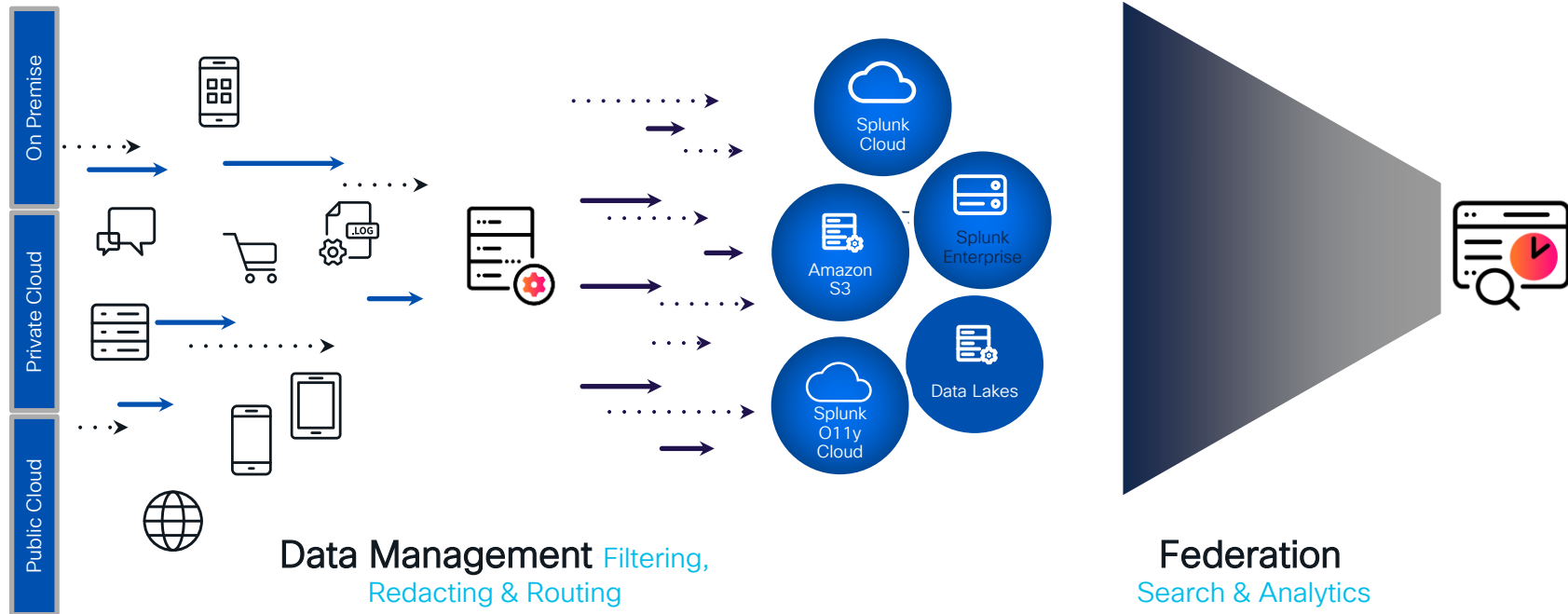
BRKSEC-1584

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

19

Data Management and Federation optimize value

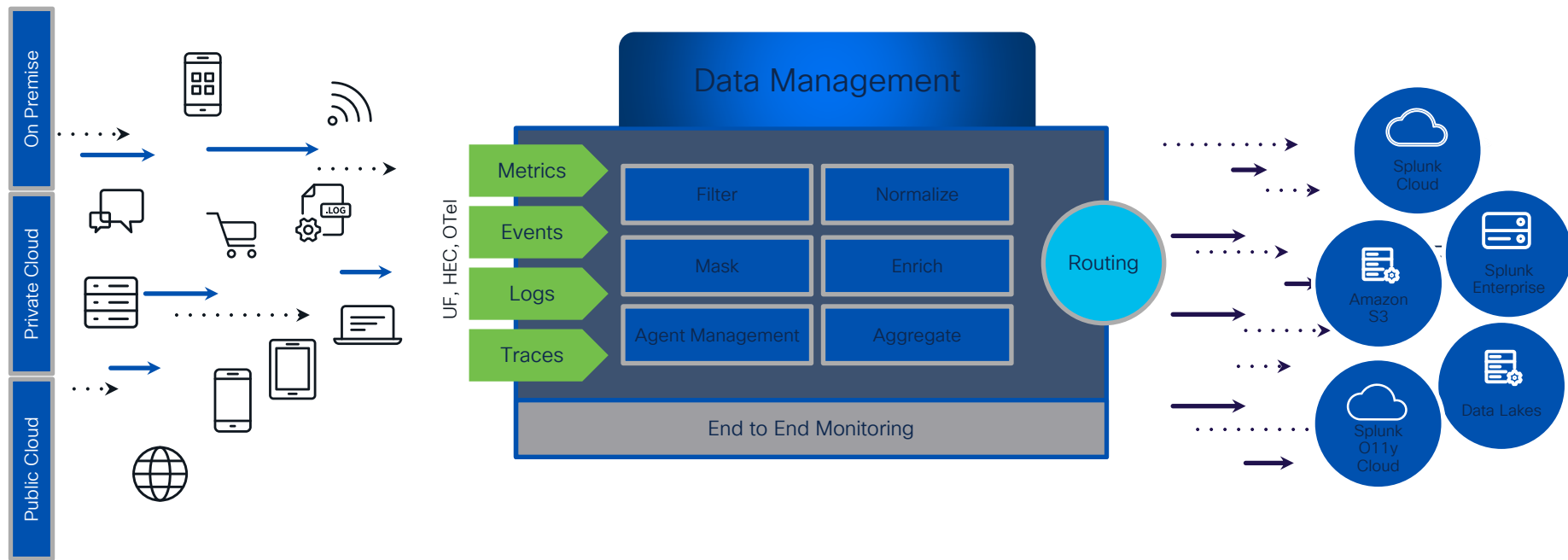
Enable a broader range of use cases and better customer ROI



Smart Data Optimization Enhanced Productivity AI Assistant for SPL

Data Management

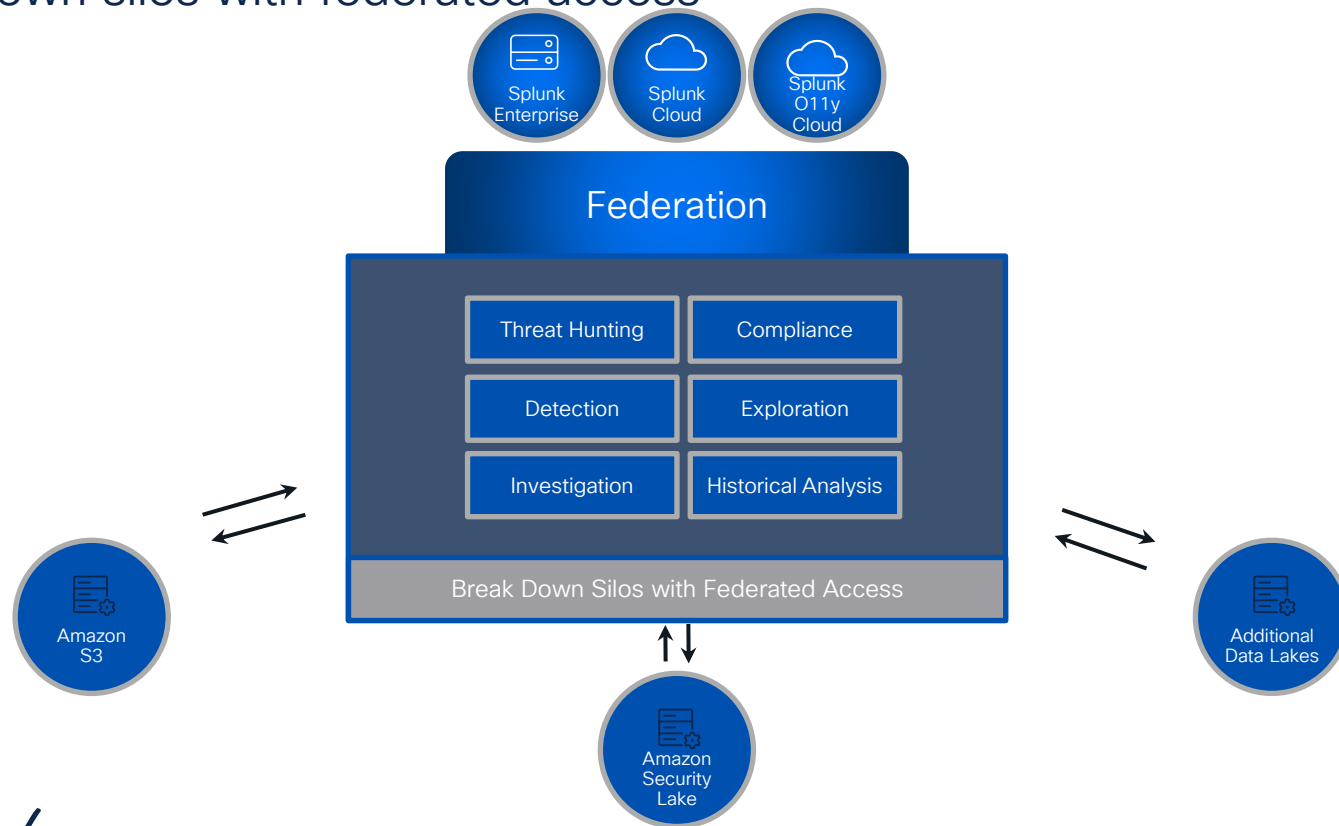
Unified data configuration, processing, and management



Federation

Break down silos with federated access

splunk



Enhance Splunk productivity with AI and ML

Catalyze resilience with easier data management, administration, search and reporting

Embedded AI in your workflows



Optimized data design for admins and data engineers



Faster learning curve in Search and Reporting for analysts



Customizable and embedded AI models for improved Security and IT operations outcomes

Generative AI

Make sense of the signal to improve user productivity and outcomes

Advanced AI

Find the signal from the noise in vast amounts of data

Security use case optimization

With Data Management and Federation

High Performance

Prevention, Detection, Monitoring

- **Search Tier:** Search & Analytics for highest performance with configurable data retention
- **Data Management Capabilities:** Enrich, mask and transform

Performance at Cost

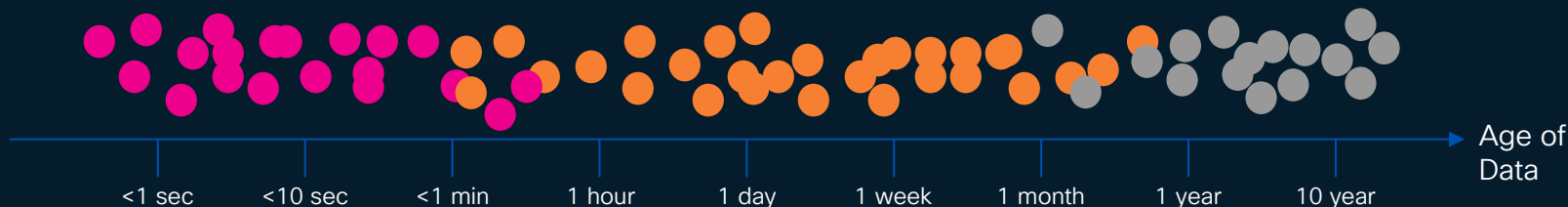
Incident Investigation, Threat Hunting

- **Search Tier:** Federated Analytics for performance on data <30 days, subject to data lake latency
- **Data Management Capabilities:** Ingest Processor Metricization, Lookups

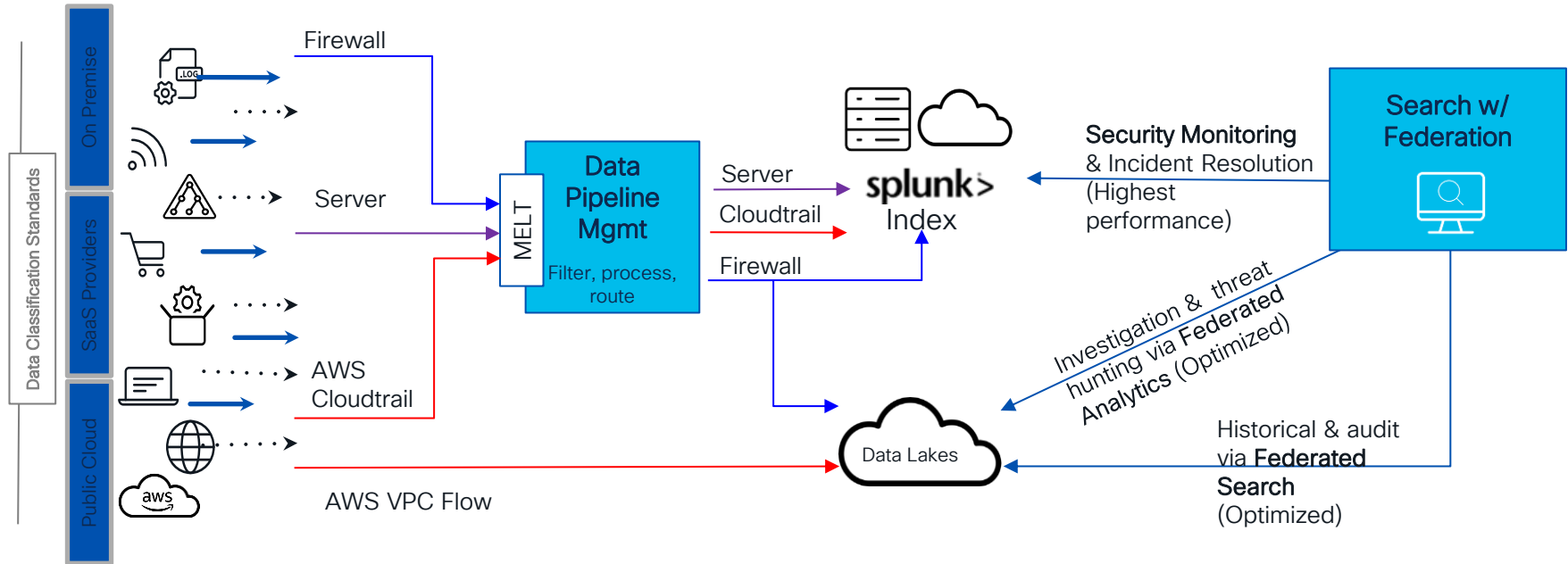
Compliance

Audit, Forensics, Compliance

- **Search Tier:** Federated Search for less performant scanning of archived & long term data
- **Data Management Capabilities:** Filter & Route with Edge Processor



Optimized data design across use cases



Deploy Splunk platform flexibly to meet the needs of your environment

Deploy Splunk platform flexibly to meet the needs of your environment



Using Data for Security Operations

Splunk Enterprise Security is an industry-defining SIEM and security analytics solution **trusted by SOC's around the globe**. Its powerful capabilities enable you to **realize comprehensive visibility, empower accurate detection with context, and fuel operational efficiency**.

splunk>
a CISCO company

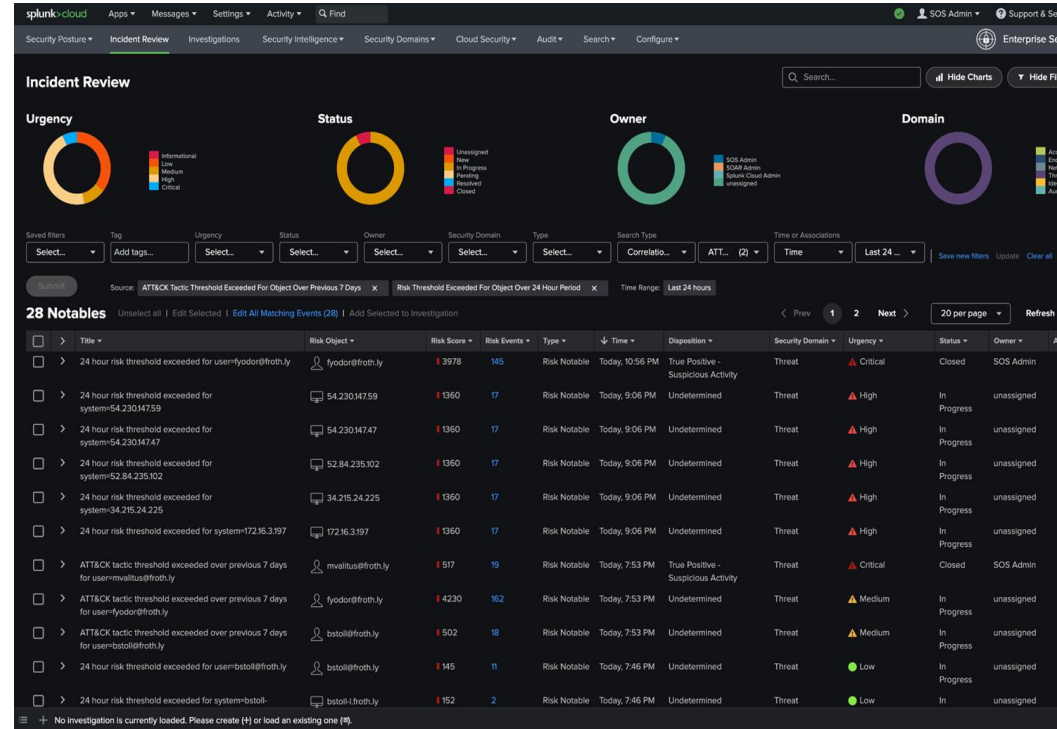


CISCO *Live!*

Realize Comprehensive Visibility

Make sense of data noise and enable fast action

- Ingest, normalize and analyze any data from all enterprise sources using the power of the Splunk Platform, with AI-powered capabilities to find any event anytime at scale
- Gain visibility with Splunk's custom alert actions feature
- Achieve cost-effective data optimization and storage flexibility by choosing to ingest only your key data critical to security use cases



Empower AccurateDetection with Context

Streamline investigations and increase productivity

- Drastically reduce alert volumes by up to 90% with risk-based alerting (RBA)
- Tap into 1,700+ out-of-the-box detections, and leverage detection engineering resources, from Splunk Threat Research to find and remediate threats faster
- Enhance your security program with customizable dashboards, visualizations, and reports

The screenshot shows the Splunk Enterprise Security interface. The top navigation bar includes tabs for Security Posture, Incident Review, Investigations, Glass Tables, Security Intelligence, Security Domains, Audit, Search, Configure, and SA-Investigator. The Incident Review section is active, showing a table of 347 Notables. The table has columns for Title, Risk Object, Aggregated Risk, Risk Events, Type, Created, Disposition, Security Domain, Urgency, Status, Owner, and Action. A notable titled 'Threat Activity Detected (25.204.169.136)' is selected, showing a risk of 410 and a status of New. Below the table, the MITRE ATTACK posture for this notable is displayed, showing a flow from Reconnaissance to Persistence. The detailed view includes a description of the threat activity, a list of additional fields, and a list of related investigations.

TITLE	RISK OBJECT	AGGREGATED RISK	RISK EVENTS	TYPE	CREATED	DISPOSITION	SECURITY DOMAIN	URGENCY	STATUS	OWNER	ACTION
ATT&CK tactic threshold exceeded over previous 7 days for user-John Doe	John Doe	160	9	Risk Notable	Today, 12:51 AM	Undetermined	Threat	Medium	New	Glenn Gallen	
Threat Activity Detected (25.204.169.136)	--	--	--	Notable	Today, 12:50 AM	Undetermined	Threat	Low	New	Glenn Gallen	
24 hour risk threshold exceeded for system-Adam's Desktop	Adam's Desktop	410	9	Risk Notable	Today, 12:50 AM	Undetermined	Threat	High	New	Unassigned	

MITRE ATTACK Posture for this Notable

The highlighted techniques were detected on the risk object Adam's Desktop

Reconnaissance (2 of 7 Techniques (28%))

- Get Victim Identity
- Enumerate Employee Names
- Get Victim Host Information
- Client Configurations

Initial Access (2 of 3 Techniques (67%))

- Drive-by Compromise
- Phishing
- Spamming
- Attachment
- Spamming Link

Execution (2 of 18 Techniques (11%))

- Account Manipulation
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Persistence (2 of 14 Techniques (14%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Privilege Escalation (2 of 14 Techniques (14%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Defense Evasion (2 of 14 Techniques (14%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Credential Access (2 of 14 Techniques (14%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Discovery (2 of 27 Techniques (7%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Lateral Movement (2 of 17 Techniques (12%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Collection (2 of 17 Techniques (12%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Command and Control (2 of 17 Techniques (12%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Exfiltration (2 of 17 Techniques (12%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Impact (2 of 17 Techniques (12%))

- Desktop Registration
- Browser Extensions
- Control Triggered Execution
- Change Default File Association
- Powercat Profile

Description:

Threat activity (25.204.169.136) was discovered in the "dest" field based on threat intelligence available in the ip_intel collection

Additional Fields

Field	Value	Action
Category	Threat Intelligence	
Destination	25.204.169.136	45
Destination Expected	false	
Destination PCI Domain	untrust	
Destination Requires Antivirus	false	
Destination Should Time Synchronize	false	
Destination Should Update	false	
Destination Should Update	false	
Kill Chain Phase	None	
MITRE ATTACK Tactic ID	TA0001	
MITRE ATTACK Tactic	TA0001 - Initial Access	
MITRE ATTACK Technique ID	T1071	
MITRE ATTACK Technique	T1071	
MITRE ATTACK Technique	T1071 - Application Layer Protocol	

Related Investigations:

Currently not associated with any investigation.

Correlation Search:

Threat List Activity - Rule

History:

View all review activity for this Notable Event

History:

View all threat activity involving dest="25.204.169.136"

Original Event:

```
{
  "time": 1615100000,
  "search_name": "Threat - Source And Destination Matches - Threat Gen",
  "search_name": "Threat Gen",
  "info_min_time": 1614980600,
  "info_max_time": 1614983300,
  "info_search_time": 1614983300,
  "src": "14.113.104.194",
  "dest": "25.204.169.136",
  "weight": 1,
  "threat_match_field": "dest",
  "threat_match_value": "25.204.169.136",
  "orig_sourcetype": "stream:http",
  "threat_keyblocklist_login",
  "threat_collection_key": "blocklist_login|25.0.0-25.255.255"
}
```

Adaptive Responses:

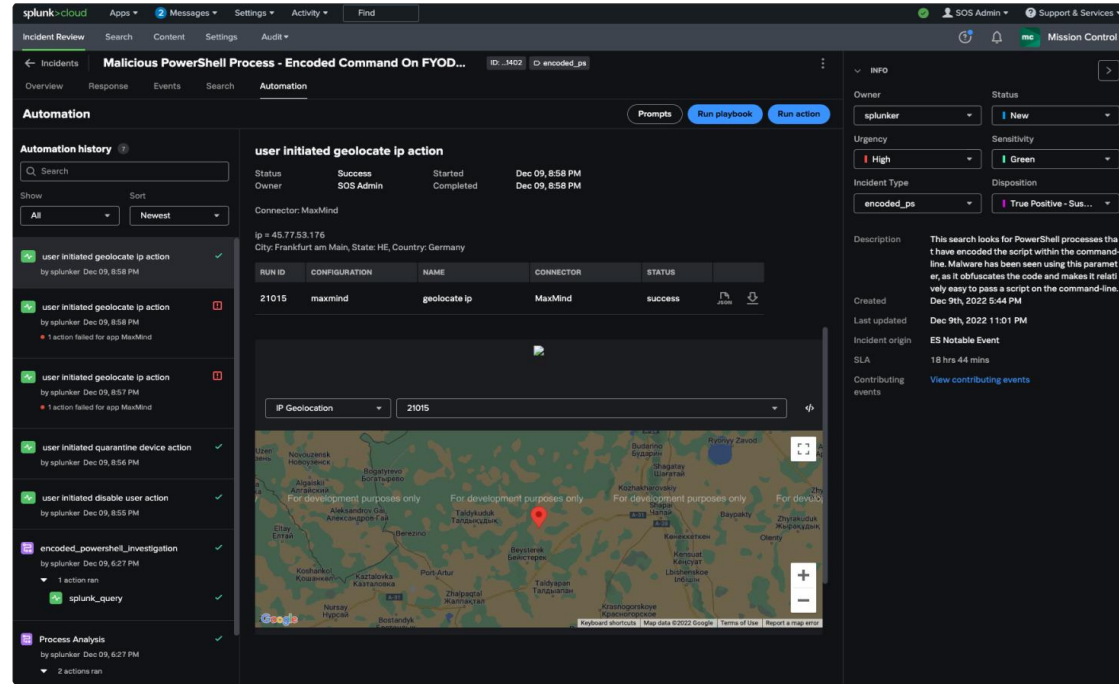
Unable to load the adaptive responses. error

View Adaptive Response Invocations

Fuel Operational Efficiency

Unify threat detection, investigation and response workflows

- **Centralize your workflows** across detection, investigation and response, and align to response templates and industry-standard frameworks like MITRE ATT&CK using the Mission Control feature
- **Increase SOC efficiency** by collaborating with the Splunk Answers community, and access Splunk's partner network of 2,200+ partners
- **Collect, search, monitor and analyze data** using a centralized solution to help meet increasingly complex
 - compliance requirements



Splunk® Enterprise Security 8.0

Splunk Enterprise Security 8.0

The SIEM Powering the SOC of the Future

As the market-leader in SIEM, Splunk Enterprise Security 8.0 revolutionizes the SOC workflow experience, enabling security analysts to seamlessly detect what matters, investigate holistically, and respond rapidly.

Splunk Enterprise Security 8.0

Market-Leading SIEM for the SOC of the Future



Complete TDIR within
Splunk Enterprise
Security



Modern Aggregation
and Triage
Capabilities



Enhanced Detections



Simplified
Terminology for
Security Analytics

Complete TDIR within Splunk Enterprise Security

A seamless, completely integrated workflow experience

With Splunk SOAR* natively integrated in Splunk Enterprise Security, it offers a unified work surface with direct integration of playbooks and actions to dramatically improve the mean time to detect and respond to incidents.

*Feature integration still requires a paid Splunk SOAR subscription

The screenshot displays the 'Analyst queue' in Splunk Enterprise Security. It shows a table of findings and investigations with columns for Title, ID, Type, Entity, Risk, Fin..., Int..., Time, Disposition, Owner, Urgency, and Status. The table is filtered for the last 24 hours and shows various findings such as 'Excessive failed logins', 'Multiple findings from the same entity', and '24 hour risk threshold exceeded for entity'.

Title	ID	Type	Entity	Risk	Fin...	Int...	Time	Disposition	Owner	Urgency	Status
Excessive failed logins		FINDING	win-hp-64861	30	7		Today, 9:45 AM	Undetermined	Unassigned	Medium	N
Multiple findings from the same entity [bstoll@splunkshircompany.com]	ES-2303	INVESTIGATION	bstoll@splunkshircompany.com	420	4	36	Today, 9:42 AM	Undetermined	Marquis Montgomery	Medium	N
ATT&CK tactic threshold exceeded over previous 7 days for entity [bstoll@splunkshircompany.com]		FINDING	bstoll@splunkshircompany.com	420		20	Today, 9:42 AM	Undetermined	Unassigned	Medium	N
24 hour risk threshold exceeded for entity [bstoll@splunkshircompany.com]		FINDING	bstoll@splunkshircompany.com	420		4	Today, 9:42 AM	Undetermined	Unassigned	Low	N
Malicious PowerShell process - encoded command on entity [bstoll@splunkshircompany.com]		FINDING	bstoll@splunkshircompany.com	420		1	Today, 7:21 AM	Undetermined	Unassigned	Medium	N
Malicious PowerShell process - encoded command on entity [bstoll@splunkshircompany.com]		FINDING	bstoll@splunkshircompany.com	420		1	Today, 6:21 AM	Undetermined	Unassigned	Medium	N
Intermediate findings		INTERMEDIATE	bstoll@splunkshircompany.com	420		10?	Today, 6:21 AM				
24 hour risk threshold exceed for entity [172.16.0.149]		FINDING	172.16.0.149	140		4	Today, 9:40 AM	Undetermined	Unassigned	High	N
Unusual volume of network activity detected on 54.230.147.59		FINDING	54.230.147.59	60		2	Today, 9:40 AM	Undetermined	Unassigned	Medium	N
Excessive failed logins		FINDING	NY_APP_002	75		11	Today, 9:35 AM	Undetermined	Unassigned	Medium	N
Unusual volume of network activity detected on 52.216.133.181		FINDING	52.216.133.181	35		5	Today, 9:35 AM	Undetermined	Unassigned	Low	N
Unusual volume of network activity detected on 52.218.196.122		FINDING	52.218.196.122	20		4	Today, 9:27 AM	Undetermined	Unassigned	Low	N
Multiple findings from the same entity [mickey.perre@splunkshircompany.com]	ES-2302	INVESTIGATION	mickey.perre@splunkshircompany.com	120		6	Today, 9:27 AM	Undetermined	Unassigned	High	N
Multiple findings from the same entity [hayley.jensen@splunkshircompany.com]	ES-2301	INVESTIGATION	hayley.jensen@splunkshircompany.com	150		5	Today, 9:23 AM	Undetermined	Unassigned	High	N
Excessive failed logins		FINDING	macbook-46743	50		2	Today, 9:23 AM	Undetermined	Unassigned	Low	N
24 hour risk threshold exceed for entity [macbook-44591]		FINDING	macbook-44591	90		3	Today, 9:19 AM	Undetermined	Unassigned	Medium	N
Unusual volume of network activity detected on 54.230.147.59		FINDING	54.230.147.59	60		2	Today, 9:19 AM	Undetermined	Unassigned	Medium	N

Modern Aggregation and Triage Capabilities

Automatically aggregate findings with just one click using predetermined rules that harness common security grouping techniques and calculations.

The screenshot displays the Splunk Cloud Analyst queue interface. The top navigation bar includes links for Mission Control, Analytics, Security content, Configure, and Search. The main section is titled 'Analyst queue' and features a search bar, a time range selector (set to 'Last 24 hours'), and a 'Save' button. Below this, a table lists findings and investigations. A specific finding is expanded, showing a list of related events. On the right, a detailed view of the selected finding is shown, including its title, owner, status, urgency, severity, and various attributes like detection time, entity, and destination.

Findings and investigations	Time Range	Clear all	Save
Multiple findings from the same entity [bstoll@splunkshirtcompany.com]	Last 24 hours		
Excessive failed logins			
ATT&CK tactic threshold exceeded over previous 7 days for entity [bstoll@splunkshirtcompany.com]			
24 hour risk threshold exceeded for entity [bstoll@splunkshirtcompany.com]			
Malicious PowerShell process - encoded command on entity [bstoll@splunkshirtcompany.com]			
Malicious PowerShell process - encoded command on entity [bstoll@splunkshirtcompany.com]			
Intermediate findings			
24 hour risk threshold exceed for entity [172.16.0.149]			
Unusual volume of network activity detected on 54.230.147.59			
Excessive failed logins			
Unusual volume of network activity detected on 52.216.133.181			
Unusual volume of network activity detected on 52.218.196.122			
Multiple findings from the same entity [mickeyperre@splunkshirtcompany.com]			
Multiple findings from the same entity [hayleyjensen@splunkshirtcompany.com]			
Excessive failed logins			

Multiple findings from the same entity [bstoll@splunkshirtcompany.com]
4 findings were detected that were associated with bstoll@splunkshirtcompany.com

Owner: Marquis Montgomery | Status: New | Urgency: Medium

Severity: Medium | Disposition: Undetermined

Time: Today, 9:42 AM

Detection: Same Entity Finding Aggregation

Entity: bstoll@splunkshirtcompany.com

Original Splunk source: Access - Geographically Improbable Access Detected Demo - Rule BA - System Process Running from Unexpected Location - Rule

Annotation framework: mitre_attack

Destination: bstoll@splunkshirtcompany.com

Destination category: workstation windows

Destination city: San Francisco

Destination country: US

Destination DNS: bstoll

Destination Expected: false

Destination IP address: 10.0.1.4

Destination NT hostname: bstoll.splunkshirtcompany.com

Destination owner: ben stoll

Destination PCI domain: untrust

Destination requires antivirus: false

Destination should time synchronize: false

Destination should update: false

File hash: 586EF56F4D8963DD546163AC31C865D7

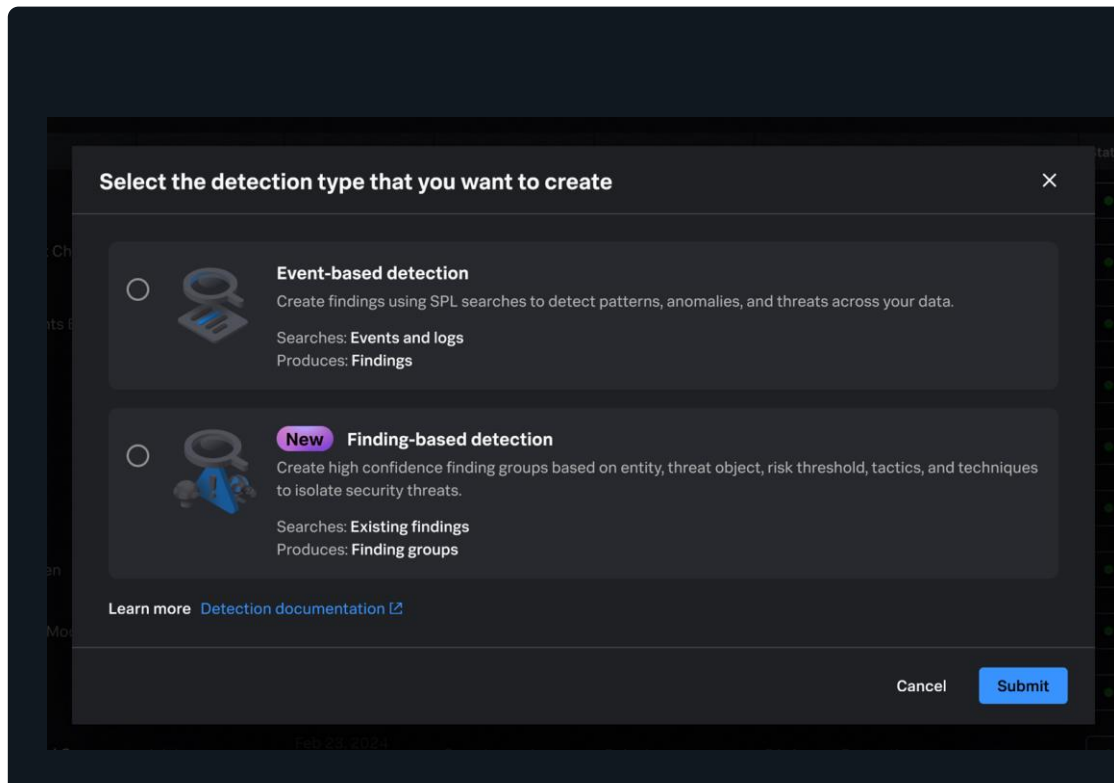
Process: powershell.exe

Entity bunit: americas

Entity category: technical

Enhanced Detections

Enhanced detection capabilities empower analysts to comprehend and employ a risk-based alerting strategy, offering the flexibility to create high-confidence aggregated alerts for thorough investigations.



Simplified Terminology for Security Analytics

Streamlined terminology across detection, findings, and investigations workflows significantly improves the analyst's experience by aligning to the Open Cybersecurity Schema Framework (OCSF).

The screenshot displays the 'Analyst queue' in Splunk Cloud, showing a list of findings and investigations. The interface includes a search bar, filters for time range (Last 24 hours), and various action buttons like 'Charts', 'Timeline', and 'Show 20'. The table below represents the data shown in the queue.

Findings and Investigations	ID	Type	Entity	Risk	Fin...	Int...	Time	Disposition	Owner	Urgency	Status
Excessive failed logins		FINDING	win-hp-64861	70		7	Today, 9:45 AM	Undetermined	Unassigned	Medium	N
Multiple findings from the same entity [bstoll@splunkthirtcompany.com]		INVESTIGATION	bstoll@splunkthirtcompany.com	420	4	36	Today, 9:42 AM	Undetermined	Unassigned	Medium	N
24 hour risk threshold exceed for entity [172.16.0.149]		FINDING	172.16.0.149	140		4	Today, 9:40 AM	Undetermined	Unassigned	High	N
Unusual volume of network activity detected on 54.230.147.59		FINDING	54.230.147.59	60		2	Today, 9:40 AM	Undetermined	Unassigned	Medium	N
Excessive failed logins		FINDING	NY_APP_002	75		11	Today, 9:35 AM	Undetermined	Unassigned	Medium	N
Unusual volume of network activity detected on 52.216.133.181		FINDING	52.216.133.181	35		5	Today, 9:35 AM	Undetermined	Unassigned	Low	N
Unusual volume of network activity detected on 52.218.196.122		FINDING	52.218.196.122	20		4	Today, 9:27 AM	Undetermined	Unassigned	Low	N
Multiple findings from the same entity [mickey.perre@splunkthirtcompany.com]		INVESTIGATION	mickey.perre@splunkthirtcompany.com	120	6	25	Today, 9:27 AM	Undetermined	Unassigned	High	N
Multiple findings from the same entity [hayley.jensen@splunkthirtcompany.com]		INVESTIGATION	hayley.jensen@splunkthirtcompany.com	150	5	16	Today, 9:23 AM	Undetermined	Unassigned	High	N
Excessive failed logins		FINDING	macbook-46743	50		2	Today, 9:23 AM	Undetermined	Unassigned	Low	N
24 hour risk threshold exceed for entity [macbook-44591]		FINDING	macbook-44591	90		3	Today, 9:19 AM	Undetermined	Unassigned	Medium	N
Unusual volume of network activity detected on 34.215.24.225		FINDING	34.215.24.225	55		3	Today, 9:19 AM	Undetermined	Unassigned	Medium	N
24 hour risk threshold exceed for entity [win-hp-85570]		FINDING	win-hp-85570	65		5	Today, 9:19 AM	Undetermined	Unassigned	Medium	N
Unusual volume of network activity detected on 172.16.0.127		FINDING	172.16.0.127	60		3	Today, 9:15 AM	Undetermined	Unassigned	Medium	N
Excessive failed logins		FINDING	win-lenovo-15782	70		8	Today, 9:15 AM	Undetermined	Unassigned	Low	N
Excessive failed logins		FINDING	win-lenovo-15565	70		7	Today, 9:12 AM	Undetermined	Unassigned	Low	N

Splunk Enterprise Security Use Cases



Security Monitoring

make decisions and
reduce risk



Incident Management

fast and flexible search
and reporting



Compliance

pass audits with
minimal effort

Splunk Recognized as a Leader

2024 Gartner® Magic Quadrant™ for Security Information and Event Management

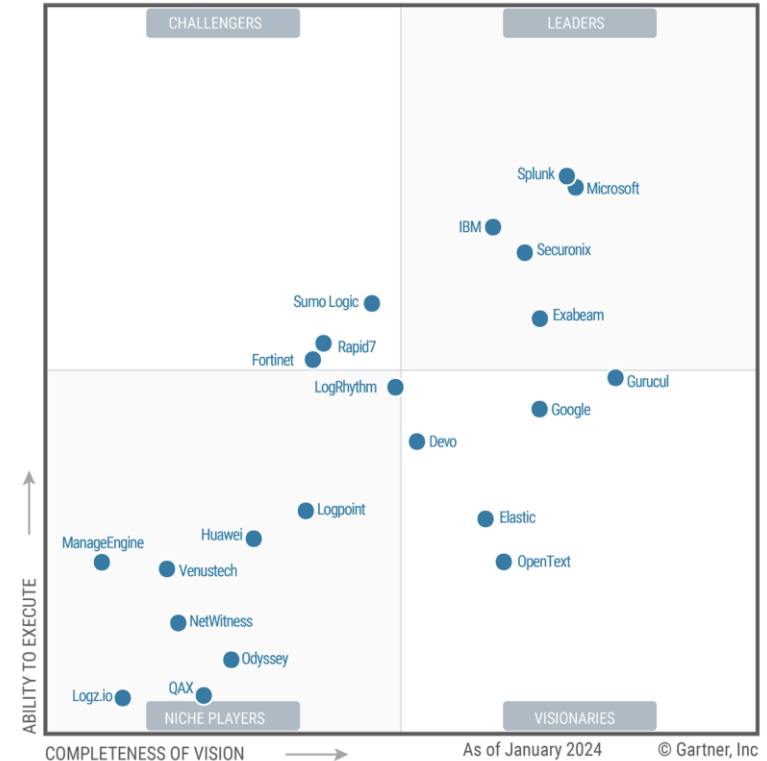
- Splunk named a **Leader** for the **10th consecutive time**
- Recognized consistently in the SIEM report based on its Completeness of Vision and Ability to Execute

GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Splunk.

Figure 1: Magic Quadrant for Security Information and Event Management

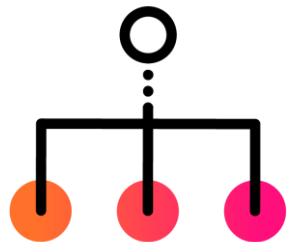


Automation

Splunk SOAR provides security orchestration, automation and response capabilities that allow security analysts to **work smarter by automating repetitive tasks; respond to security incidents faster** with automated alert triage, investigation, and response; and **strengthen defenses by connecting and coordinating complex workflows** across their team and tools.

Automate So You Can Innovate

with Splunk SOAR



Bring Order to a
Chaotic SOC



Force Multiply Your
Team



Respond with Speed
and Accuracy

Bring Order to a Chaotic SOC

Streamline investigations and increase productivity

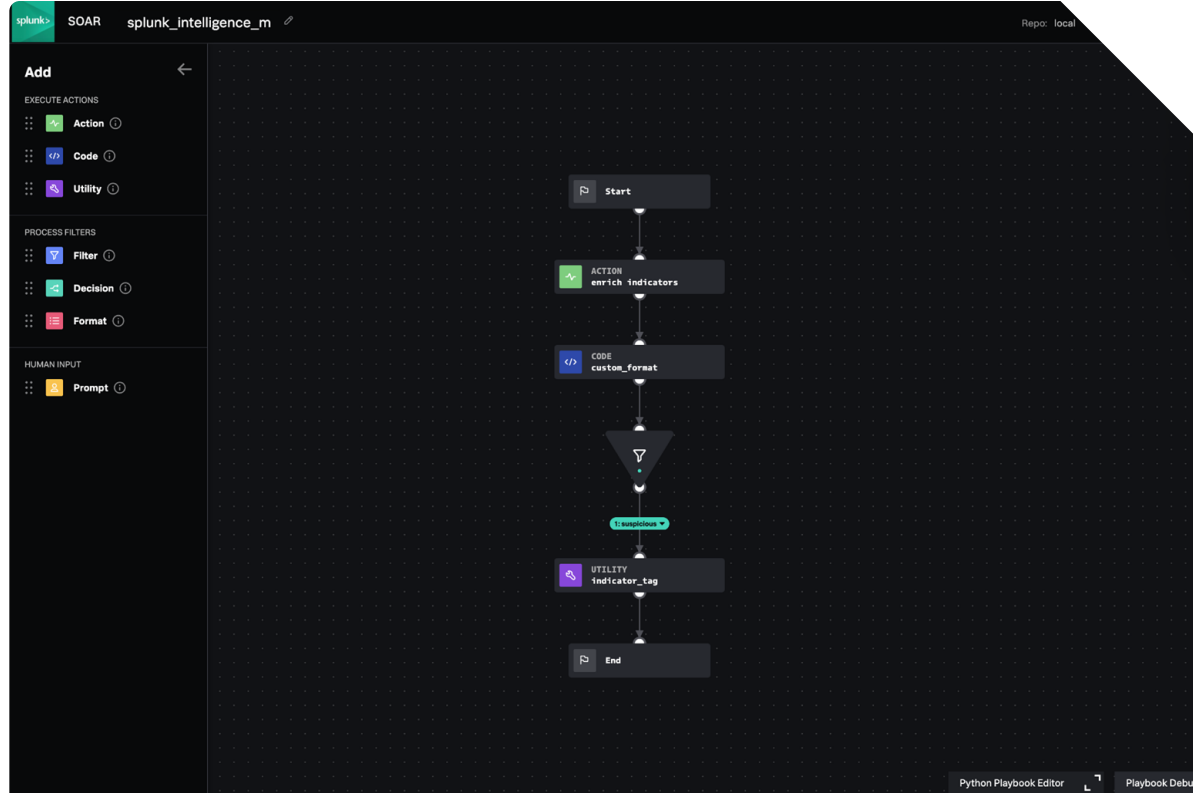
- **Get more out of your security stack** with the ability to integrate across 300+ third-party tools with support for 2,800+ automated actions
- **Develop apps easily** to tackle the use cases that matter most to your organization
- **Visualize and validate SOC efficiency** with highly customizable dashboards providing the top of mind information you and your Security C-Suite need to know



Force Multiply Your Team

Leverage automation so your team can do more with less

- **Make a team of 10 feel Like 20** with the power of orchestration and automation to help you execute tasks quickly and more efficiently
- **Take prioritized action** as threats are sorted by overall priority and sensitivity scores
- **Actionize your data** by automating investigation and response actions, enhanced by the valuable telemetry from your other security tools



Respond with Speed and Accuracy

Automate security workflows in seconds to reduce MTTR

- **Automate with ease** and conquer complex workflows with a variety of prebuilt and customizable playbooks
- **Respond with threat context** based on key input parameters and automate a series of actions to respond to common threats
- **Foster collaborative investigations** with case management and workbook functions to help keep your team informed at all times

The screenshot displays the Splunk Enterprise Security interface for a threat investigation. The top navigation bar shows the threat ID 'risk_notable' and the rule 'Threat - RIR - 7 Day ATT&CK Tactic Threshold Exceeded Demo - Rule: fyodor@froth.ly'. The left sidebar contains a 'Workbook' section with tabs for 'Activity', 'Workbook', and 'Guidance'. The 'Workbook' tab is active, showing a list of tasks: 'Investigate' (0/3), 'Preprocess' (assigned to no one), 'Render Verdict' (assigned to no one), and 'risk_notable_verdict'. The main panel displays the '[Auto-Generated] Notable Event Summary' for the threat. It includes a task note, phase information, and a summary of the risk score (4328.0 points). Below this, a timeline of events is shown, including Windows process execution, PowerShell commands, network activity, and login attempts. The interface also features a 'MITRE' section with initial access, execution, lateral movement, and exfiltration details.

Splunk® SOAR 6.3.x

Splunk SOAR Has Evolved

Splunk SOAR 6.3.0 and 6.3.1 provide integrated automation for unified threat detection, investigation and response to drive superior outcomes for the SOC.

SIEM and SOAR

Unify security workflows with Splunk Enterprise Security

Collaborative SecOps

Prompt-driven automation streamlines response workflows

Guided Automation

Overlays real incident data atop logical sequencing for easier playbook building

Easy UI Navigation

Wayfinder feature offers streamlined discovery and navigation experience

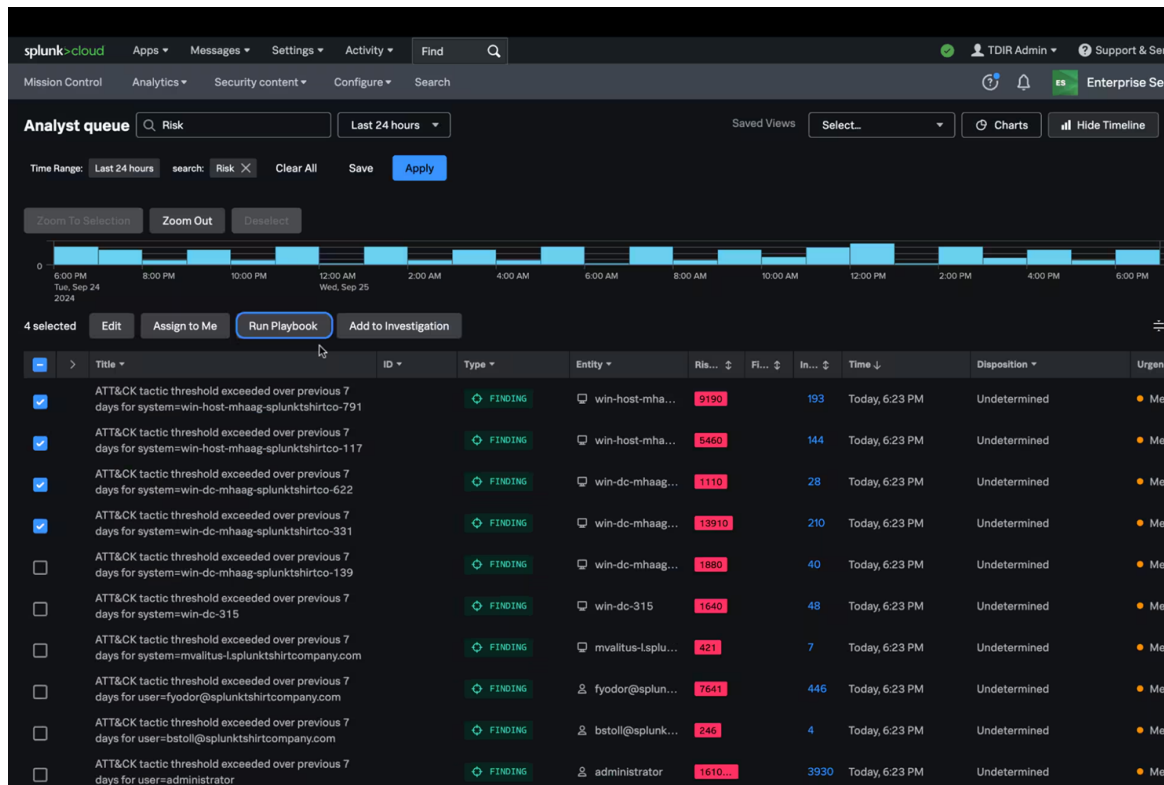
Splunk SOAR is also FedRAMP Moderate Certified

SIEM and SOAR: a Match Made in Heaven

Splunk SOAR features now come fully integrated* with Splunk Enterprise Security 8.0.

- Pair Splunk SOAR and Splunk Enterprise Security within seconds without worrying about data formats
- Playbooks and actions are now directly integrated within the Splunk Enterprise Security analyst queue
- Run playbooks and see the results without leaving the Splunk Enterprise Security interface
- Automation Rules feature in Splunk Enterprise Security ensures that playbooks run automatically when your selected detections produce findings

*Feature integration still requires a paid Splunk SOAR subscription and paid Splunk Enterprise Security subscription.



Collaborative SecOps

Prompt-driven automation lets you send real-time, secure prompts to teams outside the SOC to streamline response workflows and resolve security incidents faster.

- Effective communication with teams like IT, Network Security, HR, Legal, and end-users is crucial for informed security decisions.
- However, much of this communication occurs out-of-band, reducing SOC responsiveness.
- Prompt-driven automation streamlines these interactions for a more agile and inclusive security strategy.
- Deliver prompts through any ITOps, ChatOps or Ticketing applications

The screenshot displays the Splunk SOAR interface for configuring a prompt-driven automation workflow. The left sidebar shows the 'splunk>' logo and various icons. The main panel is titled 'SOAR' and 'Autobahn - VPE2 Phis'. It features a 'PROMPT' section with a 'prompt_analyst' prompt. Below this, there are tabs for 'Configure', 'Info', and 'Stats'. The 'Configure' tab is active, showing settings for 'RECIPIENTS' and 'DISTRIBUTION'. Under 'RECIPIENTS', the 'Others' radio button is selected. Under 'DISTRIBUTION', the 'ACTION' is set to 'send message'. The 'Required response time (mins)' is set to 1440. The right panel shows a workflow diagram in the 'Python Playbook Editor'. The workflow starts with a decision diamond, followed by a '1: is_malicious' condition. If true, it triggers a 'PROMPT prompt_analyst' action, which then leads to a 'DISTRIBUTION method' step. This is followed by another decision diamond, which branches into '1: open_event' and '2: close_event'. The '1: open_event' branch leads to a 'UTILITY set_status_open' action, and the '2: close_event' branch leads to a 'UTILITY set_status_closed' action.

Guided Automation

Playbook building is now easier than ever.

Guided automation unlocks a whole new visual experience overlaying real incident data atop the logical sequencing in a playbook. Analysts can drastically reduce the time to build automation and improve accuracy.

- Leverage intuitive at-a-glance data visualizations that show data in the context of specific security investigations
- Build faster with suggested actions to quickly add the right action blocks, filters, and prompts with a single click
- Build accurately by visualizing results rooted in real data from individual blocks

The screenshot displays the Splunk SOAR Guided Automation interface. On the left, a visual flowchart shows the playbook logic: **Start** → **PLAYBOOK dispatch account disable** → a decision diamond → **UTILITY observable check comment** (if **observable_not_exist**) or **CODE normalized observable filter** (if **observable_exist**) → **FORMAT merge report**. On the right, the **Data preview** panel shows the execution context: **ID-2: ID-2: User Scenario Rule Title gtbob...**. Below this, the **Block results** section shows the execution of the **dispatch_account_disable** block by **soar_local_admin** on September 26th, 2024, at 8:48:40 am. The **Data** section displays the results in a structured format:

```

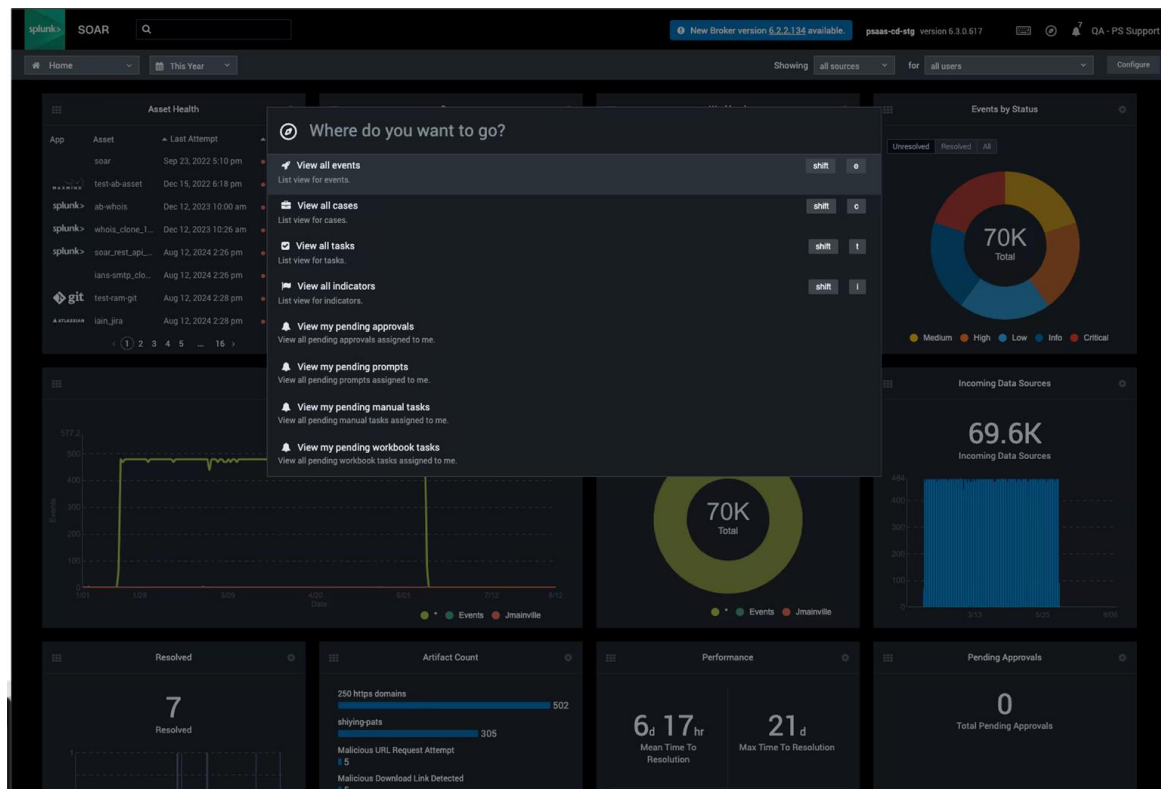
Results
  ✓ dispatch_account_disable: 1 item
  ✓ playbook_output: 7 items
    ✓ custom_function_result: 1 item
      ✓ 0: 3 items
        id: 7
        name: find_matching_playbooks
        status: success
      message
      name: dispatch_account_disable
      playbook: community/dispatch_input_playbooks
      playbook_run_id: 15
  
```

Easy UI Navigation

Wayfinder is a powerful new feature that offers a streamlined discovery and navigation experience within the Splunk SOAR interface.

With keyboard shortcuts, you can now instantly access key incidents, playbooks, and critical information for a smoother and efficient experience.

- **Keyboard-driven navigation:** Skip the menus and jump directly to what you need with the "." key
- **Dynamic content discovery:** Easily search for tasks, playbooks, or pages, with Wayfinder surfacing relevant results as you type
- **Metadata-rich guidance:** Results are accompanied with helpful metadata, ensuring you quickly reach the right destination



Splunk SOAR Use Cases



Automate Containment & Response Actions

to improve investigation and response times



Orchestrate Response Workflows

to reduce operational friction and increase efficiency

Splunk Recognized as a Leader

In the 2023 KuppingerCole Leadership Compass for SOAR

- Splunk SOAR was recognized as an Overall Leader, Product Leader and Market Leader

Other Awards and Recognition

- 2023 TrustRadius Award for Best Software for Enterprise (SIEM and SOAR)
- 2023 TrustRadius Award for Mid-Market Businesses (SIEM and SOAR)
- Fast Mover in the 2023 GigaOm Radar for SOAR





Let's show it in Action!

CISCO *Live!*

#CiscoLiveAPJC

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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC