Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on May 21, 2024 and its most recent report on Form 10-K filed on September 7, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

A Comprehensive Guide to the Latest Splunk Security Innovations

SEC1467B

.conf24 splunk>

Bring on the future.

Who Are We?

Tony Paterra

VP, Product Management
Security Products
Splunk

Shail Talati

Sr. Director, Product Management
Enterprise Security
Splunk

splunk> .conf24

Persistent Security Operations Challenges

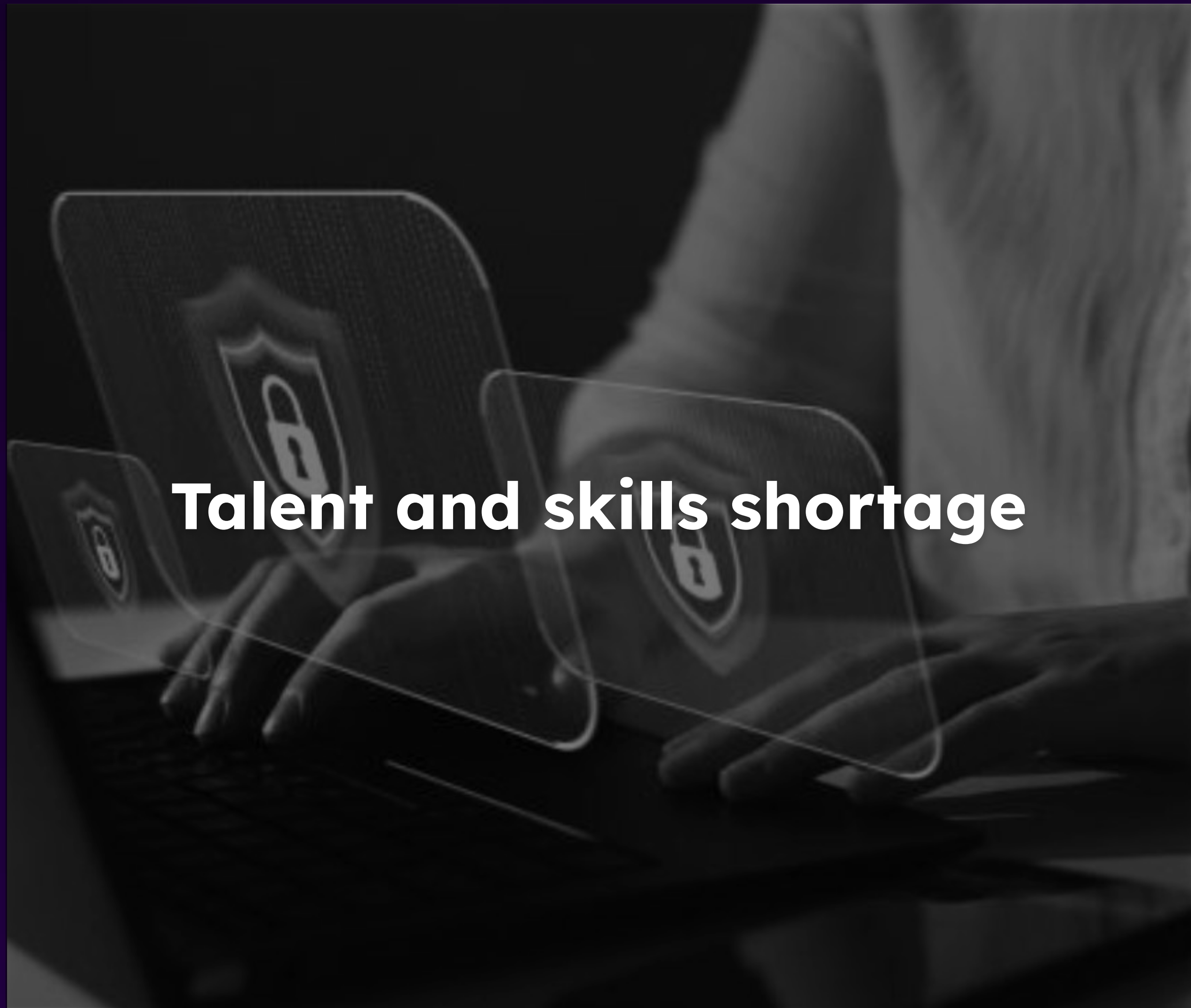
Source: ESG SOC Trends Report 2023

Expanding attack surface

Siloed tools, teams, data & workflows

Growing attack volumes

Compliance mandates and requirements



Talent and skills shortage

Splunk Security Focus Areas

2024-25: Powering the SOC of the future with Splunk Security

Unify TDIR with Automated Workflows

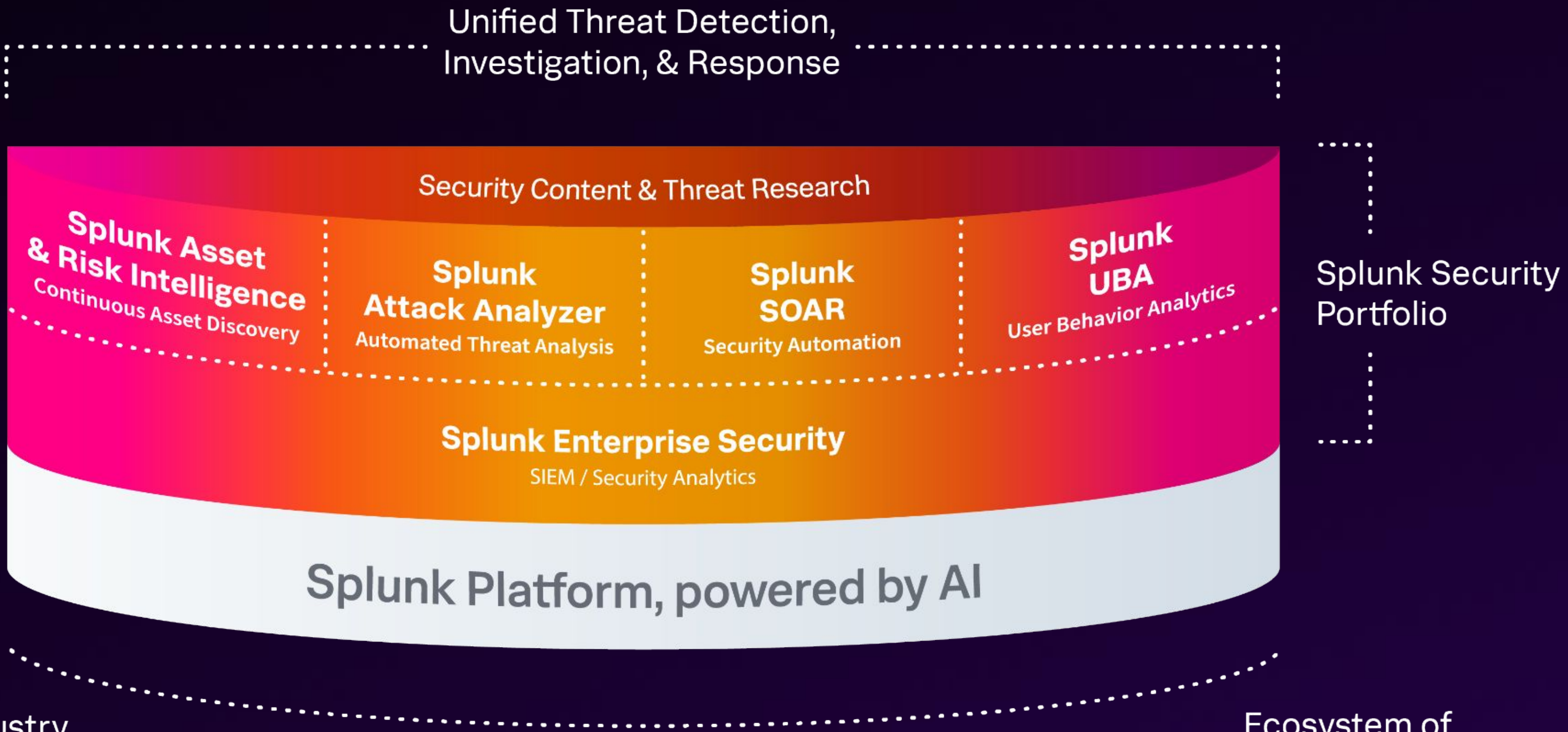
Transform **Detection Engineering**

Gain Asset Visibility to Address **Risk and Compliance**

Embrace **Federated** Data Access and Analytics

Leverage AI for Guided Security Operations

Powering the SOC of the future with the leading TDIR solution


Unified Threat Detection, Investigation, & Response
Security Content & Threat Research
Splunk Asset & Risk Intelligence
Continuous Asset Discovery
Splunk Attack Analyzer
Automated Threat Analysis
Splunk SOAR
Security Automation
Splunk UBA
User Behavior Analytics
Splunk Enterprise Security
SIEM / Security Analytics
Splunk Platform, powered by AI
Splunk Security Portfolio

Recognized industry leadership in security operations

Supported by thousands of Splunkbase apps and integrations

Vibrant community of users and partners

Ecosystem of third-party tools

Splunk® Enterprise Security Innovations

Splunk Security

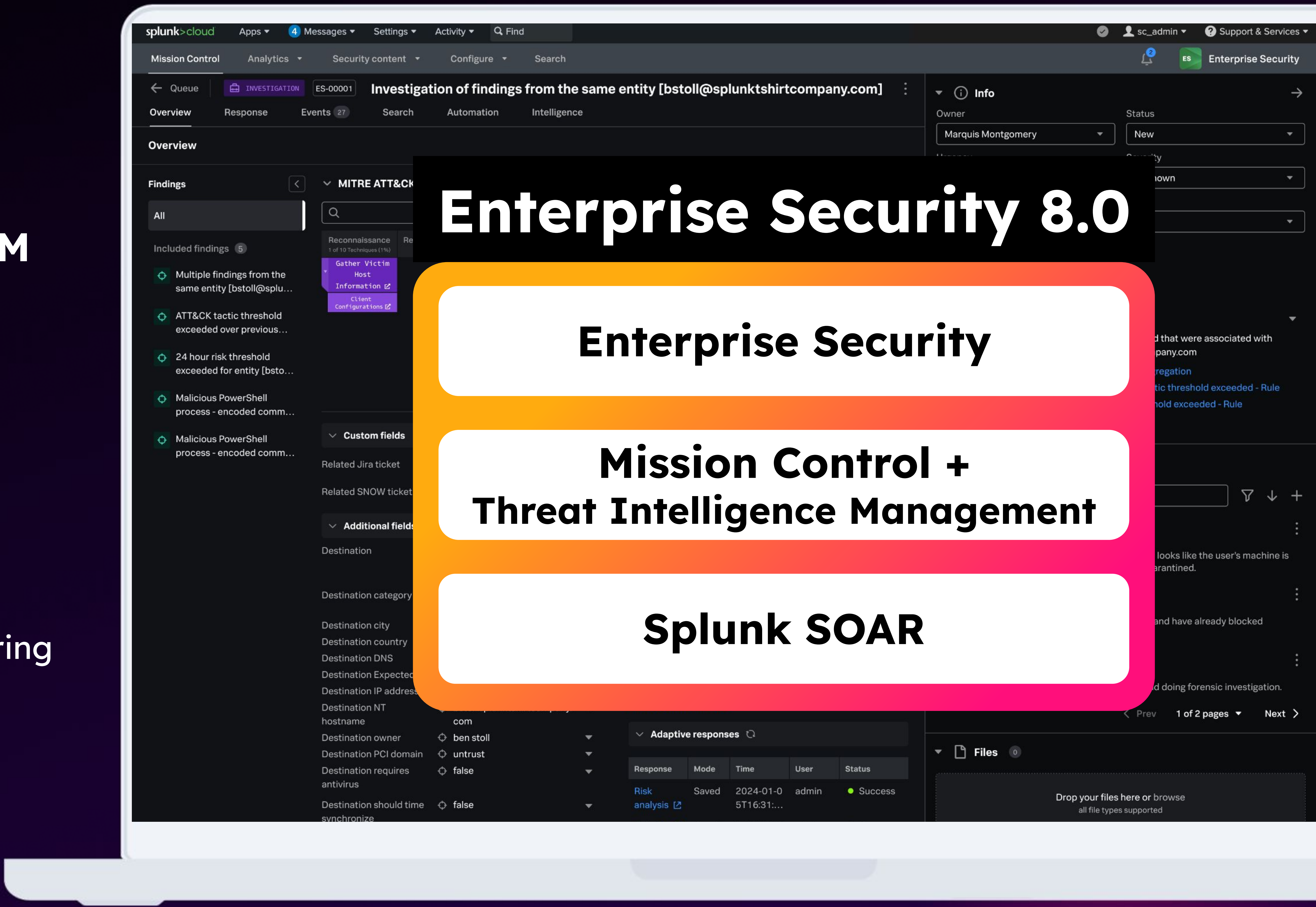
Unify TDIR

Coming Soon

Enterprise Security 8.0

The Market-Leading SIEM to Power the SOC of the Future

- Improved case management capabilities
- Native Splunk® SOAR integration
- Enhanced detection engineering capabilities
- Simplified terminology for security analytics



Investigation of findings from the same entity [bstoll@splunktshirtcompany.com]

Overview

Owner: Marquis Montgomery

Status: New

Included findings 5

- Multiple findings from the same entity [bstoll@splu…
- ATT&CK tactic threshold exceeded over previous…
- 24 hour risk threshold exceeded for entity [bsto…
- Malicious PowerShell process - encoded comm…
- Malicious PowerShell process - encoded comm…

Related Jira ticket

Related SNOW ticket

Destination

Destination category

Destination city

Destination country

Destination DNS

Destination Expected

Destination IP address

Destination NT hostname

Destination owner: ben stoll

Destination PCI domain: untrust

Destination requires antivirus: false

Destination should time synchronize: false

Response	Mode	Time	User	Status
Risk analysis	Saved	2024-01-05T16:31:…	admin	● Success

Drop your files here or browse
all file types supported

Enterprise Security 8.0

Enterprise Security

Mission Control + Threat Intelligence Management

Splunk SOAR

ES 8.0 currently available by private preview only. UI shown is for illustration; not final product.

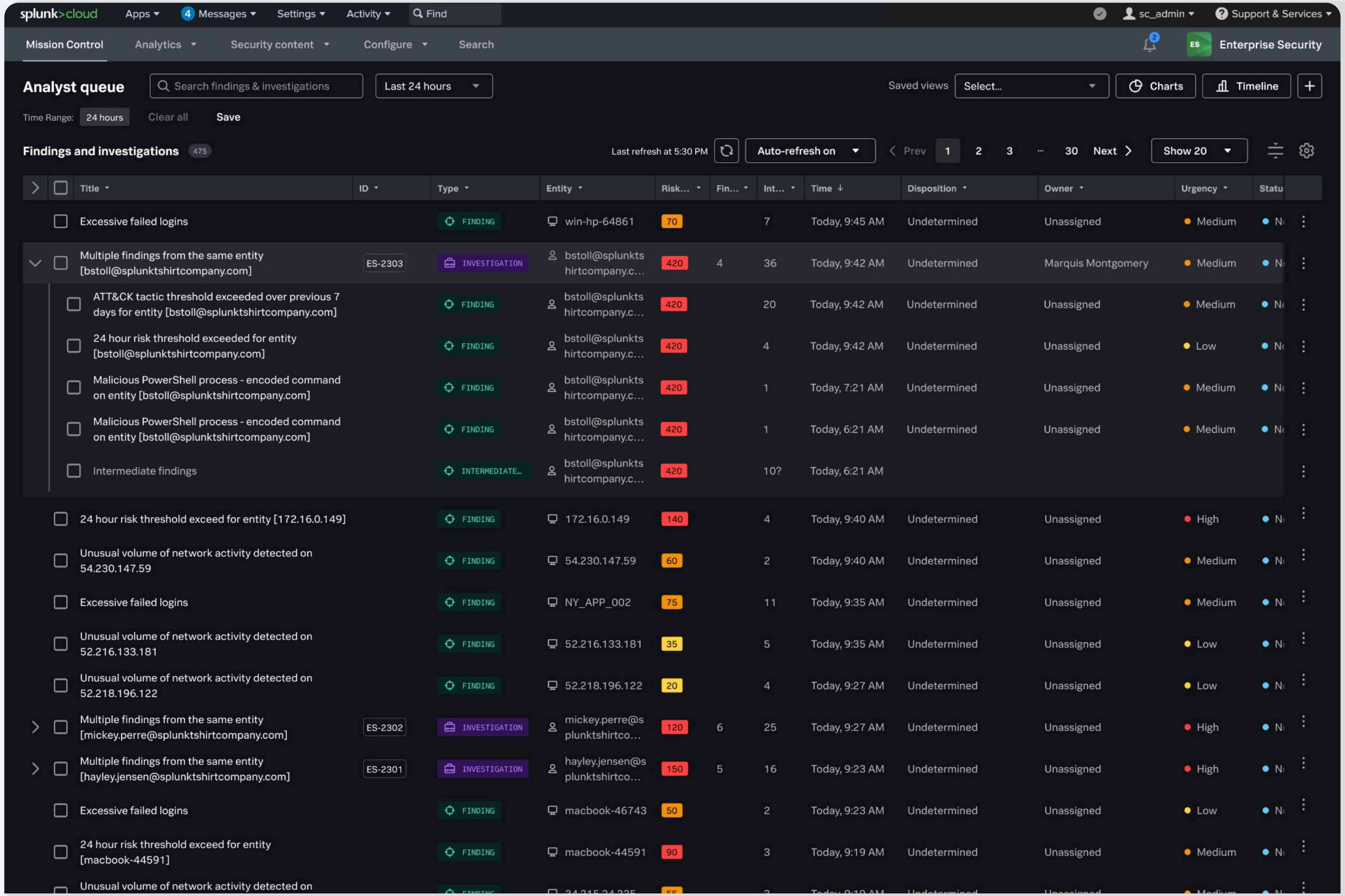
Unify TDIR

Coming Soon

Enterprise Security 8.0

Modern Case Management

- A seamless, completely integrated workflow experience
- Automatically aggregate findings based on predetermined rules
- Aggregate against common security grouping techniques and calculations
- Show analysts a comprehensive view of all related high-fidelity findings in one click



Findings and investigations 475

Last refresh at 5:30 PM

Auto-refresh on

< Prev 1 2 3 ... 30 Next >

Show 20

Title	ID	Type	Entity	Risk...	Fin...	Int...	Time	Disposition	Owner	Urgency	Statu
Excessive failed logins		FINDING	win-hp-64861	70		7	Today, 9:45 AM	Undetermined	Unassigned	● Medium	● N
Multiple findings from the same entity [bstoll@splunktshirtcompany.com]	ES-2303	INVESTIGATION	bstoll@splunkts hirtcompany.c...	420	4	36	Today, 9:42 AM	Undetermined	Marquis Montgomery	● Medium	● N
ATT&CK tactic threshold exceeded over previous 7 days for entity [bstoll@splunktshirtcompany.com]		FINDING	bstoll@splunkts hirtcompany.c...	420		20	Today, 9:42 AM	Undetermined	Unassigned	● Medium	● N
24 hour risk threshold exceeded for entity [bstoll@splunktshirtcompany.com]		FINDING	bstoll@splunkts hirtcompany.c...	420		4	Today, 9:42 AM	Undetermined	Unassigned	● Low	● N
Malicious PowerShell process - encoded command on entity [bstoll@splunktshirtcompany.com]		FINDING	bstoll@splunkts hirtcompany.c...	420		1	Today, 7:21 AM	Undetermined	Unassigned	● Medium	● N
Malicious PowerShell process - encoded command on entity [bstoll@splunktshirtcompany.com]		FINDING	bstoll@splunkts hirtcompany.c...	420		1	Today, 6:21 AM	Undetermined	Unassigned	● Medium	● N
Intermediate findings		INTERMEDIATE...	bstoll@splunkts hirtcompany.c...	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@splunktshirtcompany.com]	ES-2302	INVESTIGATION	mickey.perre@s plunktshirtco...	120	6	25	Today, 9:27 AM	Undetermined	Unassigned	● High	● N
Multiple findings from the same entity [hayley.jensen@splunktshirtcompany.com]	ES-2301	INVESTIGATION	hayley.jensen@s plunktshirtco...	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		FINDING	24.215.24.225	55		3	Today, 9:19 AM	Undetermined	Unassigned	● Medium	● N

Sourced from a customer submission in Splunk Ideas!

ES 8.0 currently available by private preview only. UI shown is for illustration; not final product.

Unify TDIR

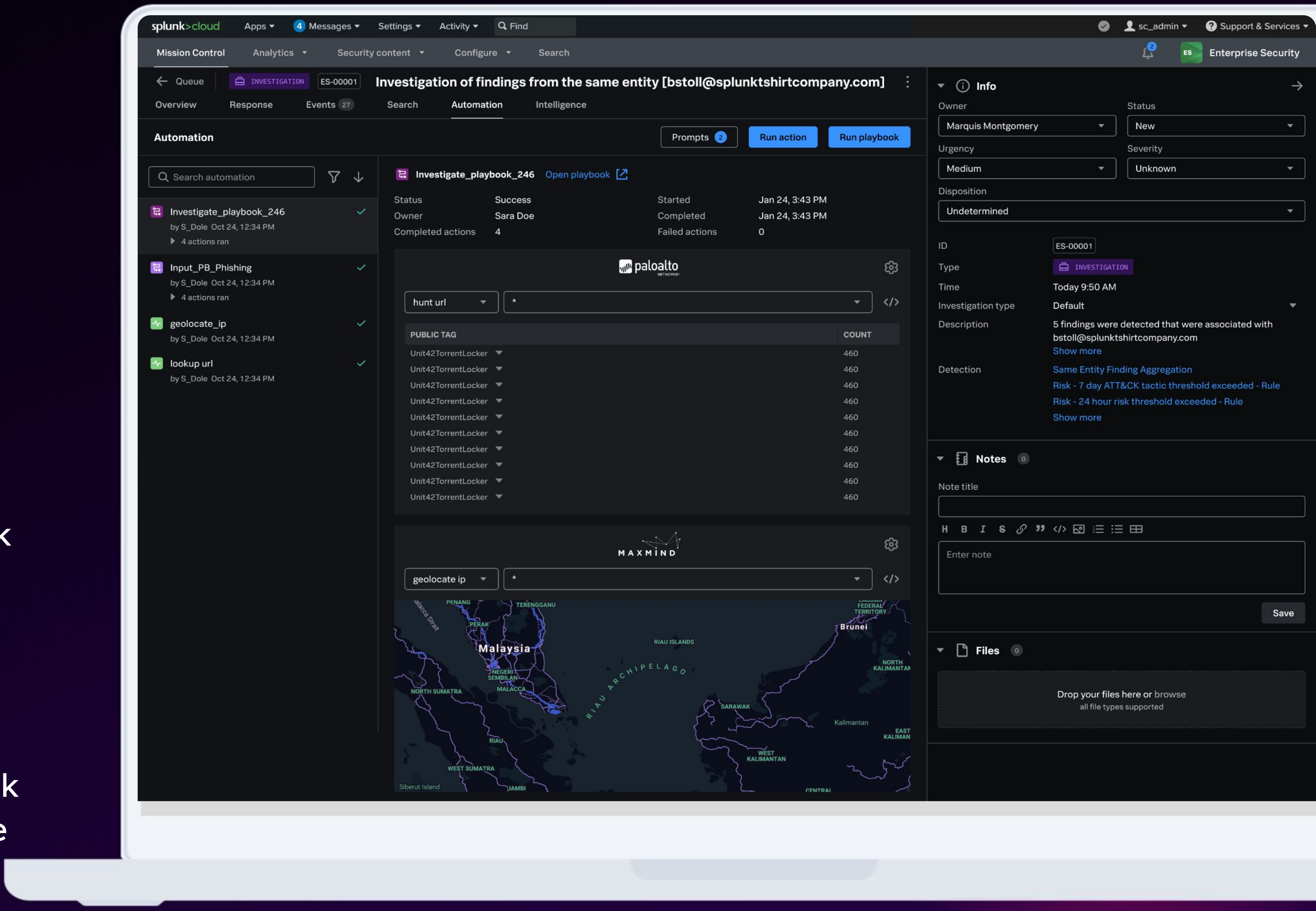
Coming Soon

Enterprise Security 8.0

Native SOAR Integration

- Mission Control embedded directly in Splunk Enterprise Security
- Direct integration with Splunk SOAR playbooks and actions
- Pair SOAR and ES within seconds without worrying about data formats
- Integrate natively with Splunk SOAR from the analyst queue

Sourced from a customer submission in Splunk Ideas!



Investigation of findings from the same entity [bstoll@splunktshirtcompany.com]

Investigate_playbook_246 ✓
by S_Dole Oct 24, 12:34 PM
4 actions ran

Input_PB_Phishing ✓
by S_Dole Oct 24, 12:34 PM
4 actions ran

geolocate_ip ✓
by S_Dole Oct 24, 12:34 PM

lookup url ✓
by S_Dole Oct 24, 12:34 PM

Investigate_playbook_246 Open playbook

Status	Success	Started	Jan 24, 3:43 PM
Owner	Sara Doe	Completed	Jan 24, 3:43 PM
Completed actions	4	Failed actions	0

PUBLIC TAG	COUNT
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460
Unit42TorrentLocker	460

Info

Owner: Marquis Montgomery
Status: New
Urgency: Medium
Severity: Unknown
Disposition: Undetermined

ID: ES-00001
Type: INVESTIGATION
Time: Today 9:50 AM
Investigation type: Default
Description: 5 findings were detected that were associated with bstoll@splunktshirtcompany.com
Show more
Detection: Same Entity Finding Aggregation
Risk - 7 day ATT&CK tactic threshold exceeded - Rule
Risk - 24 hour risk threshold exceeded - Rule
Show more

Notes 0

Note title

Enter note

Save

Files 0

Drop your files here or browse
all file types supported

ES 8.0 currently available by private preview only. UI shown is for illustration; not final product.

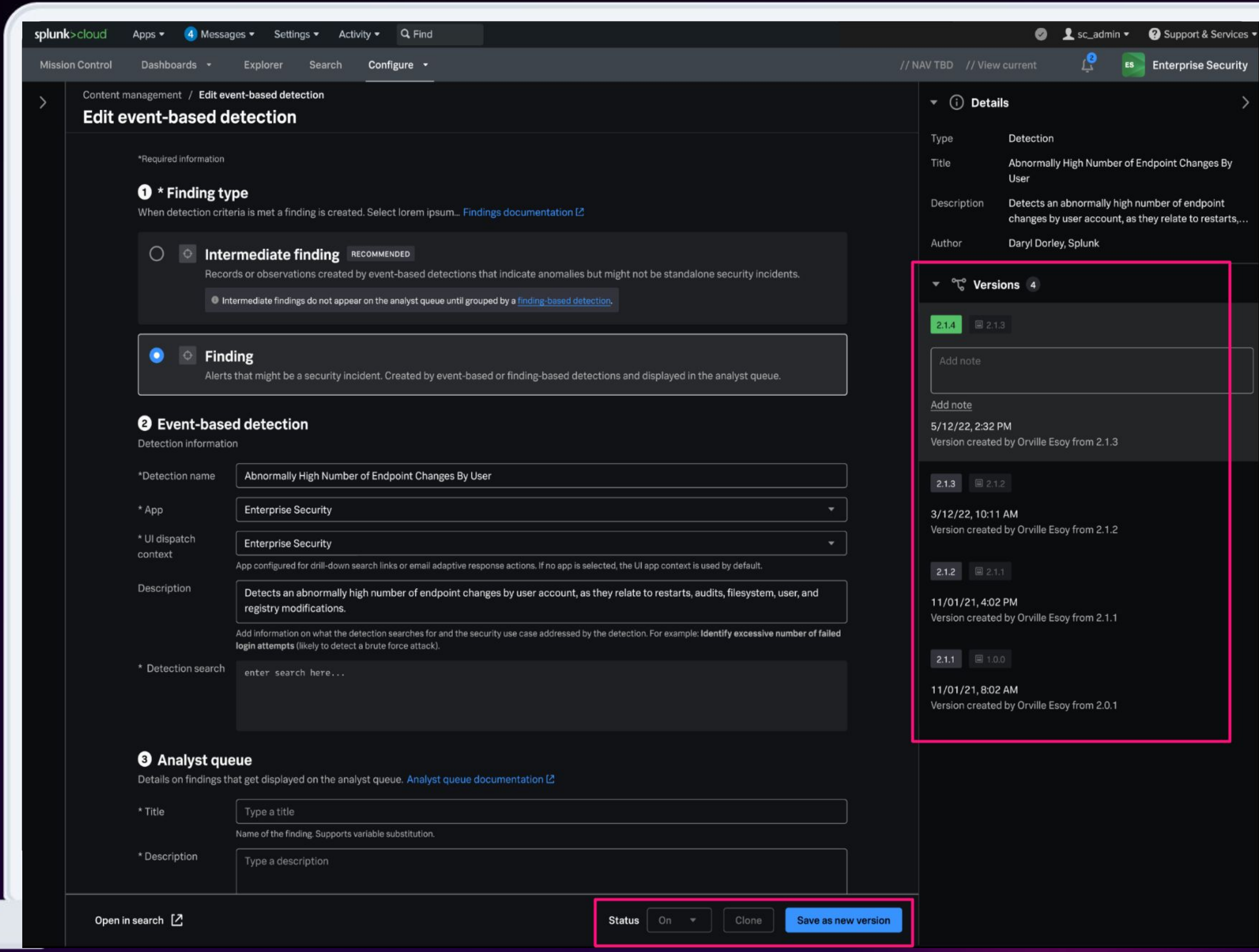
Coming Soon

Enterprise Security 8.0

Enhanced Detection Engineering

- Native support for detection versioning
- Help analysts understand and implement a risk-based alerting (RBA) detection strategy
- Build high-confidence aggregated alerts for investigation

Sourced from a customer submission in Splunk Ideas!



Content management / Edit event-based detection

Edit event-based detection

*Required information

1 * Finding type

When detection criteria is met a finding is created. Select lorem ipsum... Findings documentation

○ Intermediate finding RECOMMENDED

Records or observations created by event-based detections that indicate anomalies but might not be standalone security incidents.

Intermediate findings do not appear on the analyst queue until grouped by a finding-based detection.

● Finding

Alerts that might be a security incident. Created by event-based or finding-based detections and displayed in the analyst queue.

2 Event-based detection

Detection information

*Detection name: Abnormally High Number of Endpoint Changes By User

* App: Enterprise Security

* UI dispatch context: Enterprise Security

App configured for drill-down search links or email adaptive response actions. If no app is selected, the UI app context is used by default.

Description: Detects an abnormally high number of endpoint changes by user account, as they relate to restarts, audits, filesystem, user, and registry modifications.

Add information on what the detection searches for and the security use case addressed by the detection. For example: **Identify excessive number of failed login attempts** (likely to detect a brute force attack).

* Detection search: enter search here...

3 Analyst queue

Details on findings that get displayed on the analyst queue. Analyst queue documentation

* Title: Type a title

Name of the finding. Supports variable substitution.

* Description: Type a description

Details

Type	Detection
Title	Abnormally High Number of Endpoint Changes By User
Description	Detects an abnormally high number of endpoint changes by user account, as they relate to restarts,...
Author	Daryl Dorley, Splunk

Versions 4

2.1.4 2.1.3

Add note

Add note

5/12/22, 2:32 PM
Version created by Orville Esoy from 2.1.3

2.1.3 2.1.2

3/12/22, 10:11 AM
Version created by Orville Esoy from 2.1.2

2.1.2 2.1.1

11/01/21, 4:02 PM
Version created by Orville Esoy from 2.1.1

2.1.1 1.0.0

11/01/21, 8:02 AM
Version created by Orville Esoy from 2.0.1

ES 8.0 currently available by private preview only. UI shown is for illustration; not final product."

New Innovations with Splunk® Enterprise Security

SEC1209A

PLUS

- Demo Pod
- Keynote Demo
- ES Workshops
- Many ES Sessions (Filter the .conf catalog by Products to see more)

Marquis Montgomery **Jozef Krakora**

.conf24
splunk>

Bring on the future.

AI Assistant in Enterprise Security

Coming Soon

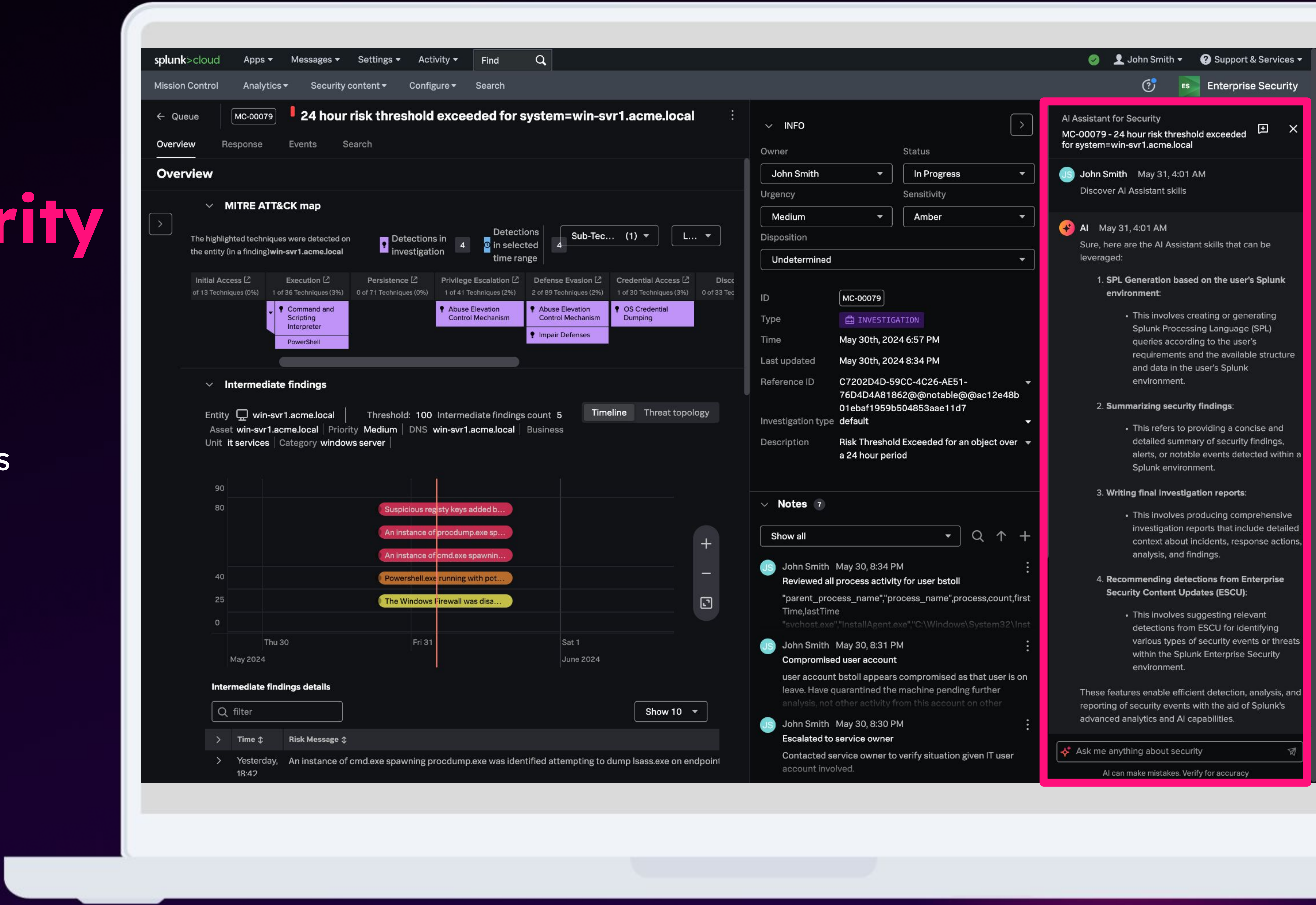
Federated Analytics

Splunk Security Innovations

Coming Soon

AI Assistant in Enterprise Security

- Answer analyst questions to guide daily workflows
- Save time and address threats more rapidly
- Use natural language queries to get answers during investigations



MC-00079 24 hour risk threshold exceeded for system=win-svr1.acme.local

Overview

MITRE ATT&CK map

The highlighted techniques were detected on the entity (in a finding)**win-svr1.acme.local**

Detections in investigation 4

Detections in selected time range 4

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Disc
of 13 Techniques (0%)	1 of 36 Techniques (3%)	0 of 71 Techniques (0%)	1 of 41 Techniques (2%)	2 of 89 Techniques (2%)	1 of 30 Techniques (3%)	0 of 33 Tec
	Command and Scripting Interpreter PowerShell		Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism Impair Defenses	OS Credential Dumping	

Intermediate findings

Entity win-svr1.acme.local | Threshold: 100 Intermediate findings count 5
Asset win-svr1.acme.local | Priority Medium | DNS win-svr1.acme.local | Business Unit it services | Category windows server |

Intermediate findings details

Time	Risk Message
Yesterday, 18:42	An instance of cmd.exe spawning procdump.exe was identified attempting to dump lsass.exe on endpoint

INFO

Owner: John Smith
Status: In Progress
Urgency: Medium
Sensitivity: Amber
Disposition: Undetermined

ID	MC-00079
Type	INVESTIGATION
Time	May 30th, 2024 6:57 PM
Last updated	May 30th, 2024 8:34 PM
Reference ID	C7202D4D-59CC-4C26-AE51-76D4D4A81862@@notable@@ac12e48b01ebaf1959b504853aae11d7
Investigation type	default
Description	Risk Threshold Exceeded for an object over a 24 hour period

Notes 7

John Smith May 30, 8:34 PM
Reviewed all process activity for user bstoll
"parent_process_name","process_name",process,count,firstTime,lastTime
"svchost.exe","InstallAgent.exe","C:\Windows\System32\Inst

John Smith May 30, 8:31 PM
Compromised user account
user account bstoll appears compromised as that user is on leave. Have quarantined the machine pending further analysis, not other activity from this account on other

John Smith May 30, 8:30 PM
Escalated to service owner
Contacted service owner to verify situation given IT user account involved.

AI Assistant for Security

MC-00079 - 24 hour risk threshold exceeded for system=win-svr1.acme.local

John Smith May 31, 4:01 AM
Discover AI Assistant skills

AI May 31, 4:01 AM
Sure, here are the AI Assistant skills that can be leveraged:

1. **SPL Generation based on the user's Splunk environment**:
   - This involves creating or generating Splunk Processing Language (SPL) queries according to the user's requirements and the available structure and data in the user's Splunk environment.
2. **Summarizing security findings**:
   - This refers to providing a concise and detailed summary of security findings, alerts, or notable events detected within a Splunk environment.
3. **Writing final investigation reports**:
   - This involves producing comprehensive investigation reports that include detailed context about incidents, response actions, analysis, and findings.
4. **Recommending detections from Enterprise Security Content Updates (ESCU)**:
   - This involves suggesting relevant detections from ESCU for identifying various types of security events or threats within the Splunk Enterprise Security environment.

These features enable efficient detection, analysis, and reporting of security events with the aid of Splunk's advanced analytics and AI capabilities.

Ask me anything about security

AI can make mistakes. Verify for accuracy

Using AI for SecOps Efficiency

The Maverick SOC Analyst's Rooster

SEC1528A

Shail Talati

Senior Director, Product Management
Splunk

James Young

Principal Security Strategist
Splunk

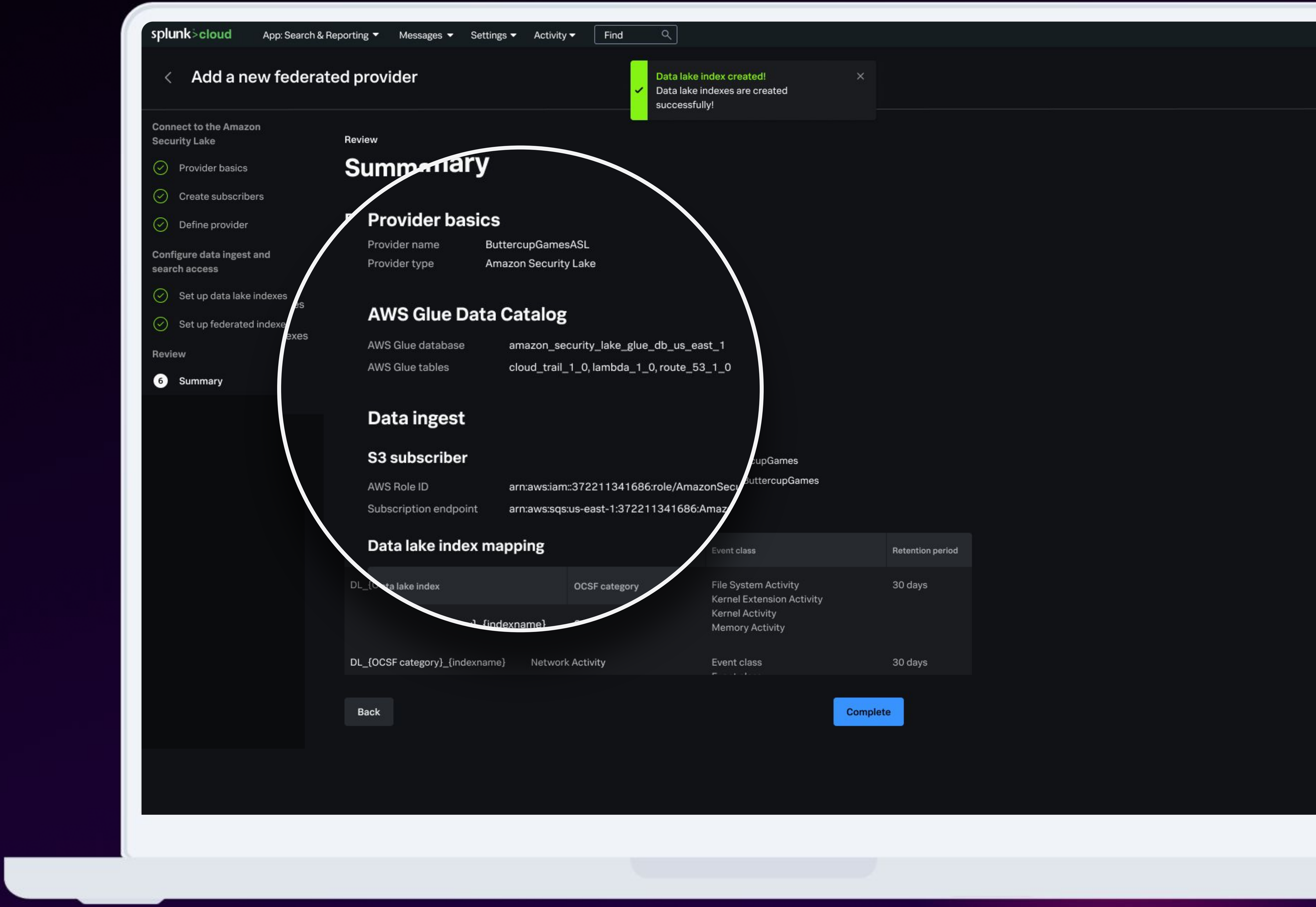
splunk> .conf24

Coming Soon

Federated Analytics

Amazon Security Lake

- Complements ad-hoc Federated Search with near real-time detection
- Manage and analyze data in Amazon Security Lake and Splunk’s AWS detection content
- Implement data tiering and standardization for cost-effective data management



Add a new federated provider

Data lake index created!
Data lake indexes are created successfully!

Connect to the Amazon Security Lake

- ✓ Provider basics
- ✓ Create subscribers
- ✓ Define provider

Configure data ingest and search access

- ✓ Set up data lake indexes
- ✓ Set up federated indexes

Review

- 6 Summary

Review

Summary

Provider basics

Provider name	ButtercupGamesASL
Provider type	Amazon Security Lake

AWS Glue Data Catalog

AWS Glue database	amazon_security_lake_glue_db_us_east_1
AWS Glue tables	cloud_trail_1_0, lambda_1_0, route_53_1_0

Data ingest

S3 subscriber

AWS Role ID	arn:aws:iam::372211341686:role/AmazonSecu
Subscription endpoint	arn:aws:sqs:us-east-1:372211341686:Amaz

cupGames
ButtercupGames

Data lake index mapping

Data lake index	OCSF category	Event class	Retention period
DL_{O		File System Activity Kernel Extension Activity Kernel Activity Memory Activity	30 days
}_{indexname}			
DL_{OCSF category}_{indexname}	Network Activity	Event class	30 days

Use Federated Analytics to Run Security Workloads Against Amazon Security Lake

SEC1212A

Marc Luescher

Sr Solution Architect
AWS

Derek Feriancek

Sr Product Manager, Distributed Search
Splunk

splunk> .conf24

Splunk® SOAR Innovations

Splunk Security

Coming Soon

Unify TDIR

Coming Soon

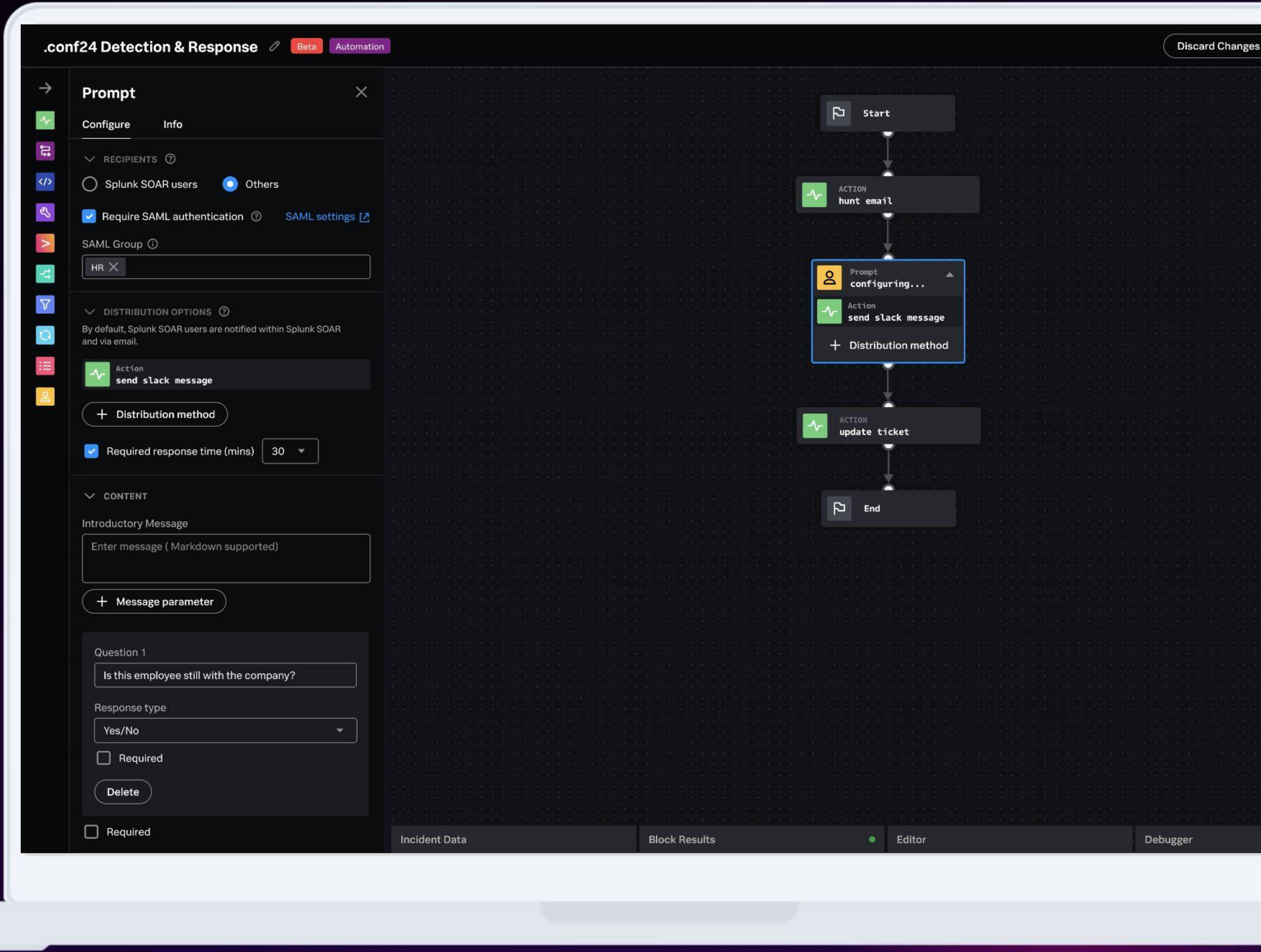
Splunk SOAR

User Response Driven Automation

Improved End User External Prompts

- **Automate Manual Communication Workflows**
  Real-time secure prompts to end-users and other teams that extend beyond the SOC
- **Flexible Method of Delivery**
  Choose from 300+ SOAR integrations to deliver prompts to your hybrid workforce
- **Accelerated Response**
  Take immediate response actions based on response for data loss prevention & phishing workflows

Sourced from a customer submission in Splunk Ideas!



.conf24 Detection & Response

Prompt

RECIPIENTS

○ Splunk SOAR users ● Others

☑ Require SAML authentication

SAML Group: HR

DISTRIBUTION OPTIONS

By default, Splunk SOAR users are notified within Splunk SOAR and via email.

Action: send slack message

☑ Required response time (mins): 30

CONTENT

Introductory Message: Enter message (Markdown supported)

Question 1: Is this employee still with the company?

Response type: Yes/No

☐ Required

☐ Required

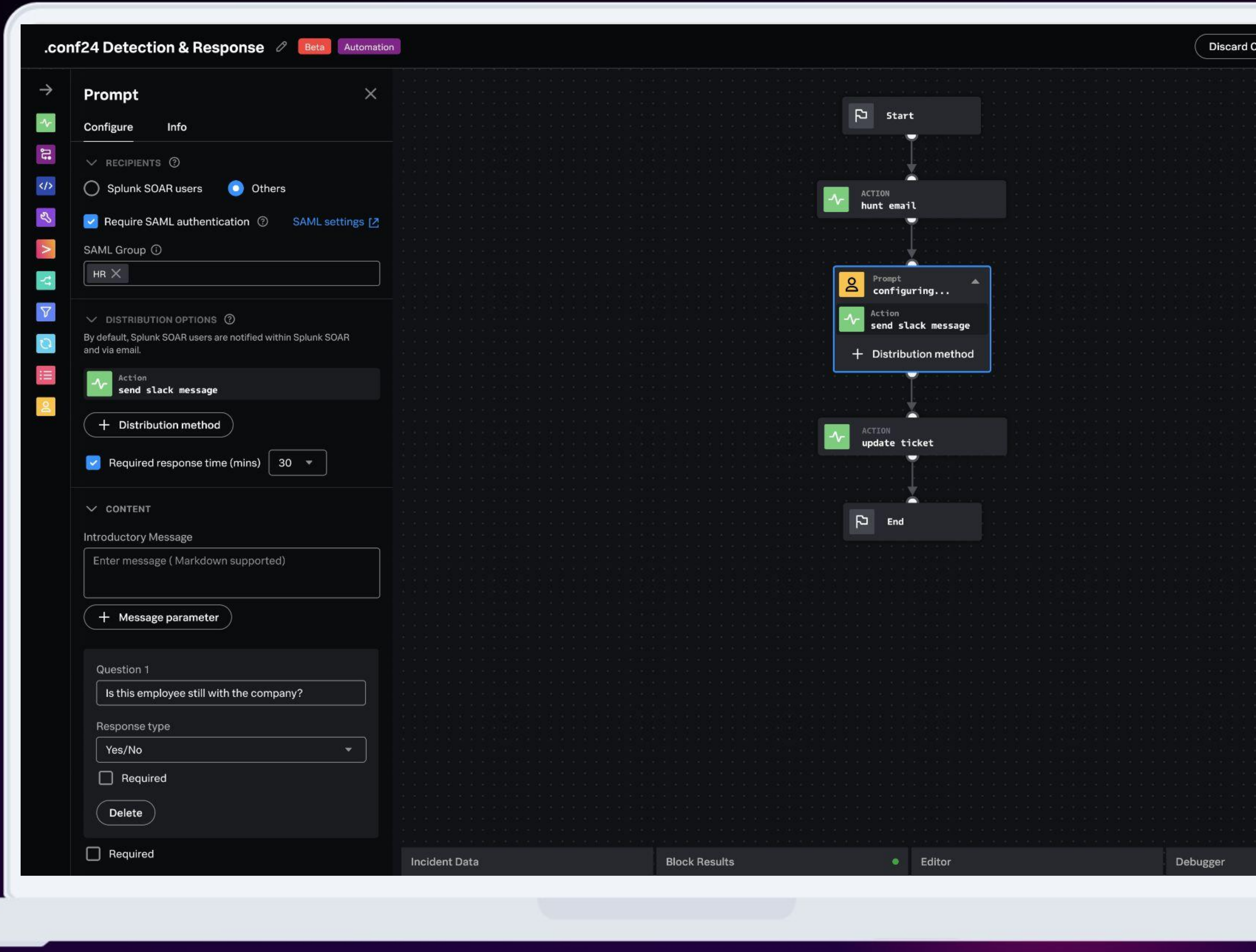
Unify TDIR

Coming Soon

Splunk SOAR

Guided Automation

- **Build Easier** with intuitive at-a-glance data visualization that shows actual data in investigations
- **Build Faster** with suggested actions to quickly add the right action blocks in a single click
- **Build Accurately** by visualizing results from individual blocks to build with confidence



.conf24 Detection & Response Beta Automation

Prompt

Configure Info

RECIPIENTS

○ Splunk SOAR users ● Others

☑ Require SAML authentication SAML settings

SAML Group: HR

DISTRIBUTION OPTIONS

By default, Splunk SOAR users are notified within Splunk SOAR and via email.

Action send slack message

+ Distribution method

☑ Required response time (mins) 30

CONTENT

Introductory Message: Enter message (Markdown supported)

+ Message parameter

Question 1: Is this employee still with the company?

Response type: Yes/No

□ Required

Delete

□ Required

What's New in Splunk® SOAR

SEC1562A

Mandeep Singh Sandhu

Senior Director of Product Management
Splunk

Nick Astor

Product Manager
Splunk

splunk> .conf24

Splunk® Attack Analyzer

Splunk Security

Splunk Attack Analyzer

Automated Threat Analysis

- Take the manual work out of phishing and malware analysis
- Realize consistent, high-quality threat analysis
- SOAR integration to automate end-to-end threat analysis and response

Phishing Alerts

EDR Alerts

SWG/Proxy Alerts

> “Our previous solution used to take 3x the time to analyze and would be wrong on 1 of every 4 analyses. With Attack Analyzer, we haven’t had a false positive in ~6 months and complete most analysis in under 5 mins.

Cybersecurity Architect at US Insurance Company

66% reduction in investigation time

90+% reduction in false positives

Dramatically improved and accelerated threat investigation and analysis

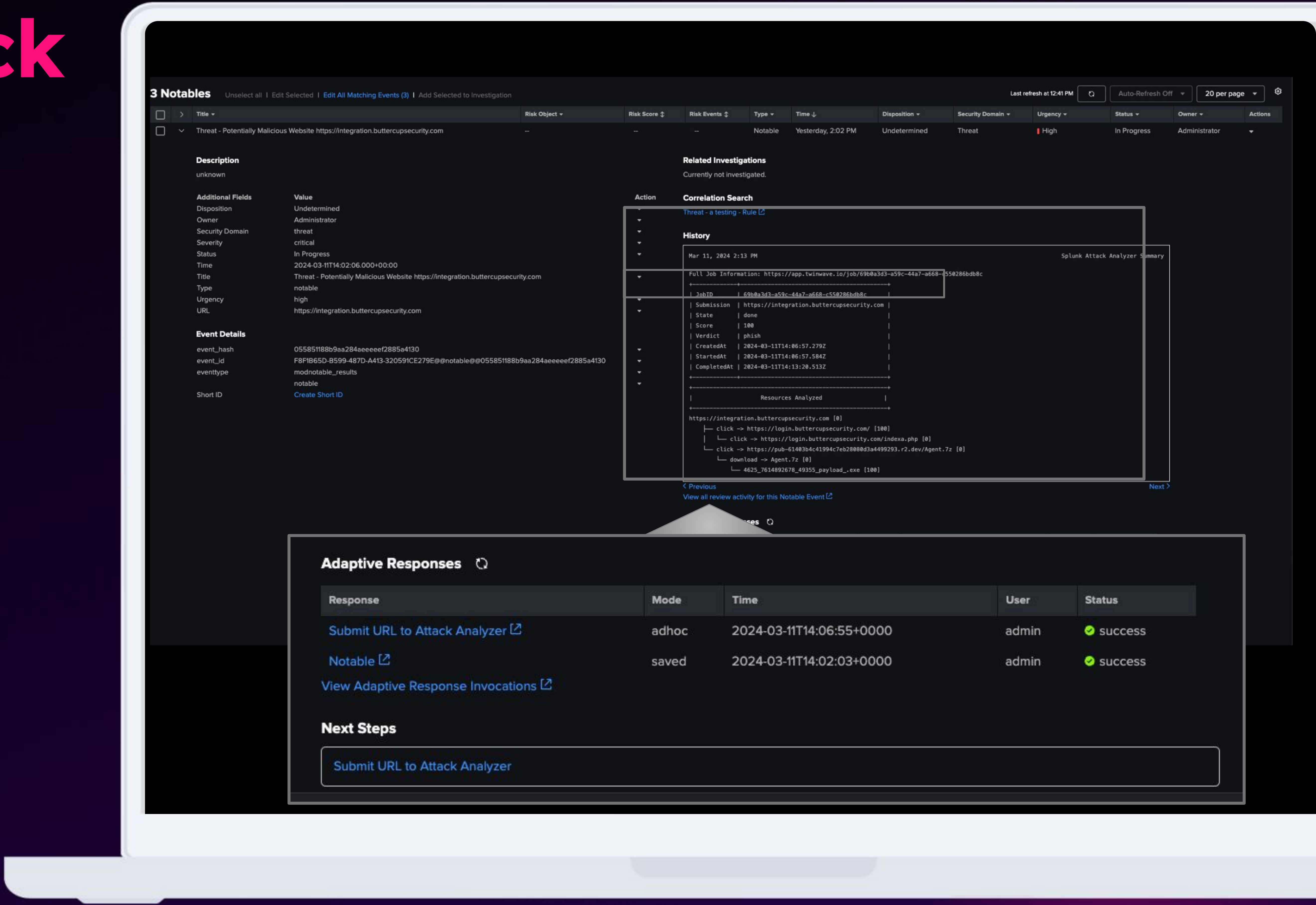
Source:
https://www.splunk.com/en_us/customers/success-stories/southern-farm-bureau-life-insurance-company.html

Splunk Attack Analyzer

Splunk App for Splunk Attack Analyzer

Enhance Splunk® Enterprise Security (ES) findings with automated analysis of URLs.

Splunkbase link



3 Notables Unselect all | Edit Selected | Edit All Matching Events (3) | Add Selected to Investigation

Last refresh at 12:41 PM | Auto-Refresh Off | 20 per page

□	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
□	Threat - Potentially Malicious Website https://integration.buttercupsecurity.com	--	--	--	Notable	Yesterday, 2:02 PM	Undetermined	Threat	High	In Progress	Administrator	

Description

unknown

Additional Fields	Value
Disposition	Undetermined
Owner	Administrator
Security Domain	threat
Severity	critical
Status	In Progress
Time	2024-03-11T14:02:06.000+00:00
Title	Threat - Potentially Malicious Website https://integration.buttercupsecurity.com
Type	notable
Urgency	high
URL	https://integration.buttercupsecurity.com

Event Details

event_hash	055851188b9aa284aeeeeef2885a4130
event_id	F8F1B65D-B599-487D-A413-320591CE279E@@notable@@055851188b9aa284aeeeeef2885a4130
eventtype	modnotable_results notable
Short ID	Create Short ID

Related Investigations

Currently not investigated.

Correlation Search

Threat - a testing - Rule

History

```
Mar 11, 2024 2:13 PM                                                    Splunk Attack Analyzer Summary

Full Job Information: https://app.twinwave.io/job/69b0a3d3-a59c-44a7-a668-c550286bdb8c
+-------------+------------------------------------------+
| JobID       | 69b0a3d3-a59c-44a7-a668-c550286bdb8c     |
| Submission  | https://integration.buttercupsecurity.com |
| State       | done                                     |
| Score       | 100                                      |
| Verdict     | phish                                    |
| CreatedAt   | 2024-03-11T14:06:57.279Z                 |
| StartedAt   | 2024-03-11T14:06:57.584Z                 |
| CompletedAt | 2024-03-11T14:13:20.513Z                 |
+-------------+------------------------------------------+
+--------------------------------------------------------+
|                   Resources Analyzed                   |
+--------------------------------------------------------+
https://integration.buttercupsecurity.com [0]
    ├── click -> https://login.buttercupsecurity.com/ [100]
    │   └── click -> https://login.buttercupsecurity.com/indexa.php [0]
    └── click -> https://pub-61403b4c41994c7eb28080d3a4499293.r2.dev/Agent.7z [0]
        └── download -> Agent.7z [0]
            └── 4625_7614892678_49355_payload_.exe [100]
```

< Previous Next >

View all review activity for this Notable Event

Adaptive Responses

Response	Mode	Time	User	Status
Submit URL to Attack Analyzer	adhoc	2024-03-11T14:06:55+0000	admin	✓ success
Notable	saved	2024-03-11T14:02:03+0000	admin	✓ success

View Adaptive Response Invocations

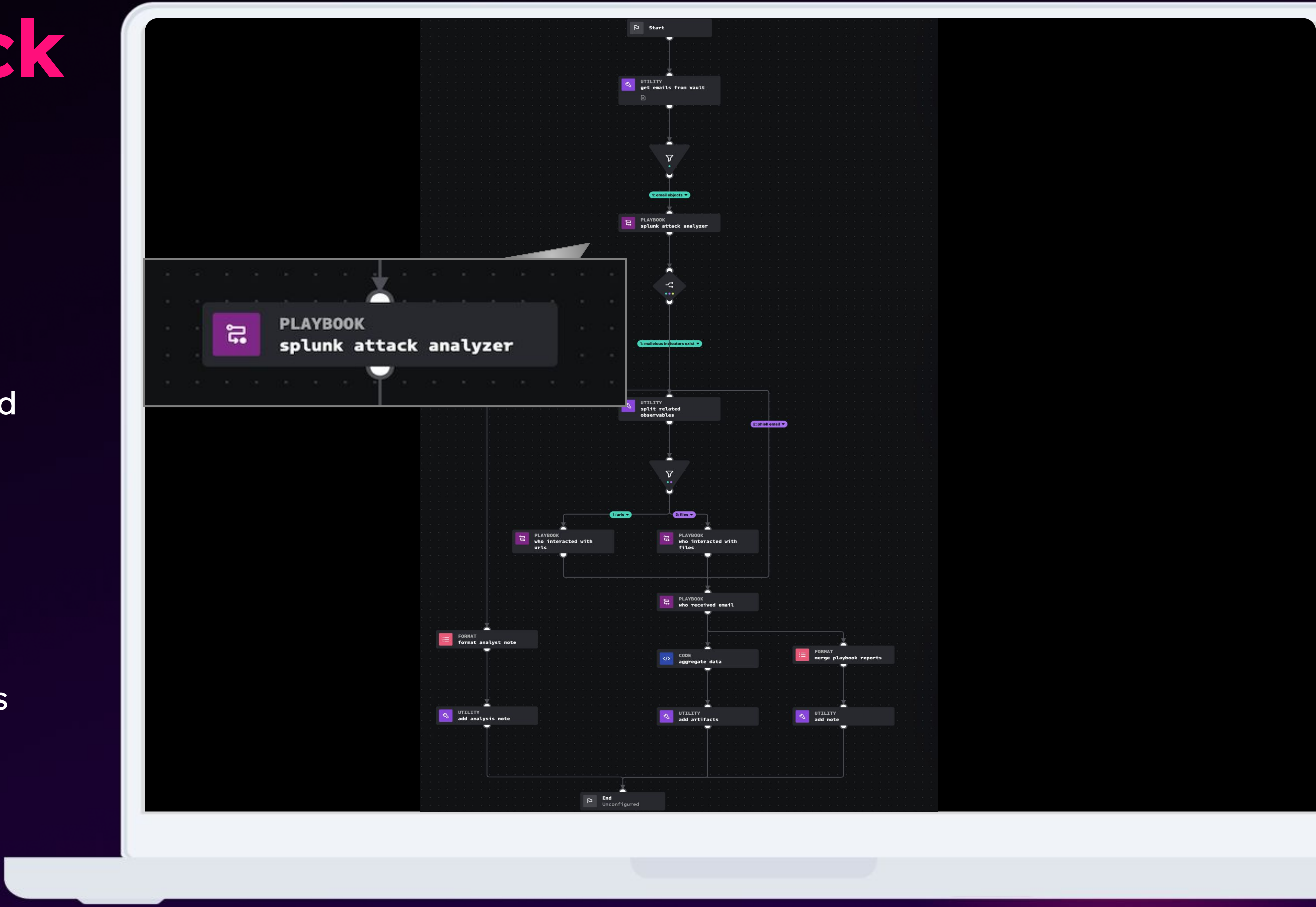
Next Steps

Submit URL to Attack Analyzer

Splunk Attack Analyzer

Simplify Threat Analysis Playbooks

- Eliminate manual analysis and response actions
- Simplify intricate playbooks that utilize diverse threat analysis products
- Build intelligent automation for end-to-end threat analysis and response



Join our Attack Analyzer Customer Panel session SEC1174B at .conf24 to learn more.

Neal Iyer

Moderator
Sr. Principal Product Manager
Splunk

Brandon Platter

Principal Security Engineer
Citizens Bank

Francisco Zuazo

Supervisor, Global Security Operations
Carnival Corporation

Tony Iacobelli

Sr. Manager,
Advanced Response Team
Splunk

splunk> .conf24

Splunk® Asset and Risk Intelligence Innovation

Splunk Security

SecOps teams 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[1]

Lengthy Security Investigations

69% experienced an attack targeting unknown, or poorly managed assets[2]

Gaps in compliance $4M average revenue

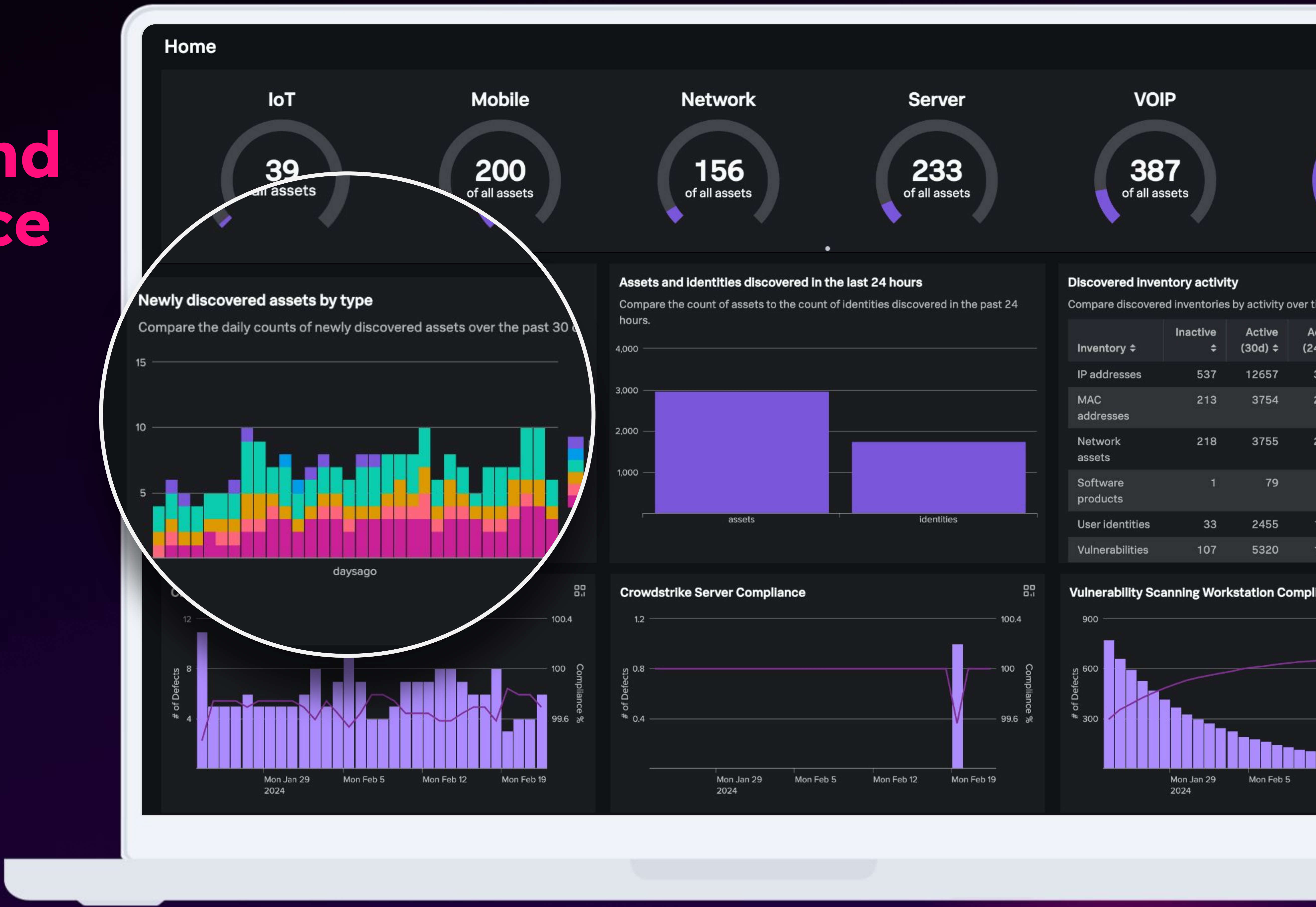
$4M average revenue loss due to compliance audit failures[3]

[1] SC Magazine, Attack Surface Management: A critical pillar of cybersecurity asset management, Nov 2022
[2] CSO Online, Look for attack surface management to go mainstream in 2022, Jon Oltsik, Feb 2022
[3] The True Cost of Non-Compliance, Savivynt, May 2022

Splunk Asset and Risk Intelligence

New - Early Access

- Gain comprehensive asset visibility to reduce risk exposure
- Accelerate investigation with more accurate asset context
- Identify compliance gaps in security controls



Newly discovered assets by type

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

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 t

Inventory ⇕	Inactive ⇕	Active (30d) ⇕
IP addresses	537	12657
MAC addresses	213	3754
Network assets	218	3755
Software products	1	79
User identities	33	2455
Vulnerabilities	107	5320

Crowdstrike Server Compliance

Vulnerability Scanning Workstation Compl

Empowering SecOps with Splunk® Asset and Risk Intelligence

Patriz Regalado

Director, Security Product Marketing
Splunk

Madhura Kumar

Director, Product Manager Compliance
Splunk

A New Era of Continuous Asset Discovery and Compliance

SEC1145A

splunk> .conf24

Cisco Talos | Splunk

&

Cisco XDR | Splunk

Splunk Security Products Labs

Advancing innovation within the Splunk Security portfolio by rapidly prototyping capabilities to support our customer's security operations.

OT Security Add-On for Splunk

Splunkbase Link

Splunk App for Fraud Analytics

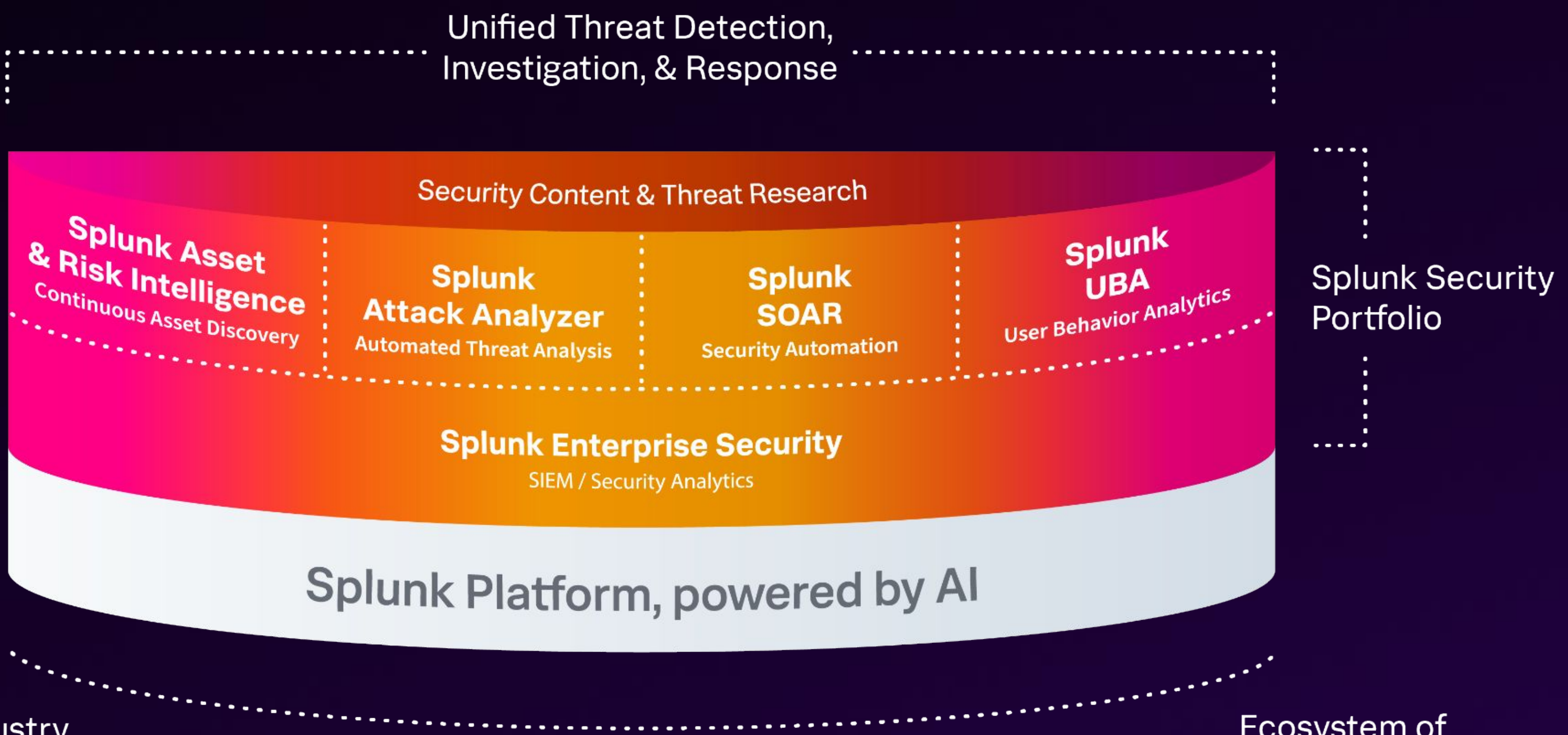
Splunkbase Link

Compliance Essentials for Splunk

Splunkbase Link

Cisco Talos Integration

Powering the SOC of the future with the leading TDIR solution



Unified Threat Detection, Investigation, & Response
Security Content & Threat Research
Splunk Asset & Risk Intelligence
Continuous Asset Discovery
Splunk Attack Analyzer
Automated Threat Analysis
Splunk SOAR
Security Automation
Splunk UBA
User Behavior Analytics
Splunk Enterprise Security
SIEM / Security Analytics
Splunk Security Portfolio
Splunk Platform, powered by AI

Recognized industry leadership in security operations

Supported by thousands of Splunkbase apps and integrations

Vibrant community of users and partners

Ecosystem of third-party tools

Thank You - Learn More

Topic	Session
Splunk Enterprise Security 8.0	SEC1209A: New Innovations with Splunk® Enterprise Security
Splunk SOAR	SEC1562A: What's New in Splunk® SOAR
Splunk Attack Analyzer	SEC1174B: Splunk® Attack Analyzer Customer Panel with Carnival and Citizens Bank
Splunk Asset & Risk Intelligence	SEC1145A: Empowering SecOps with Splunk® Asset and Risk Intelligence
Federated Analytics	SEC1212A: A Federated Approach to Running Security Workloads Against Amazon Security Lake
Splunk AI Assistant for Security	SEC1528A: Using AI for SecOps Efficiency

Questions?