Welcome

Splunk Tech Talks | Security Edition

Thanks for your patience! We will begin momentarily.

- All lines are muted as this session is being recorded and will be shared with all attendees.
- Please submit your questions to the Q&A option. We will address them during the session, at the end and afterward.
- Video replay will be available on Splunk Community Tech Talks.

Thank you for attending!

Splunk Enterprise Security 8

The Essential Upgrade for Threat Detection, Investigation, and Response

Thursday, November 6, 2025

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 February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 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.

splunk>
a CISCO company

Speakers

Drew Church

Global Security Product Specialist

Brandon Tansey

Global Security Product Specialist

Topics

- Notable Changes (between ES 7 and ES 8*)
  - Terminology
- ES 8 Key Benefits and Features
- Enterprise Security Editions
- Important Considerations
  - Deprecated features & limitations
  - Known issues
  - Architectural nuances
  - REST API Support

**Up to v8.2*

Notable Changes

Terminology

Updated ES Taxonomy & Terminology

Changes from <=7.3 to 8

* = Conceptual difference

<=ES 7.3	ES 8
Correlation search, correlation rule, risk rule	Event-based detection
Risk incident rule*	Finding-based detection
Notable (notable event, risk rotable)	Finding
Comment*	Note
MC incident, ES investigation*	Investigation
Risk event	Intermediate finding
Splunk events	Events
Alerts	Third-party Alerts

For more information on the changed terms, see Glossary and Splunk Enterprise Security terminology.

Updated ES Taxonomy & Terminology

Changes from <=7.3 to 8

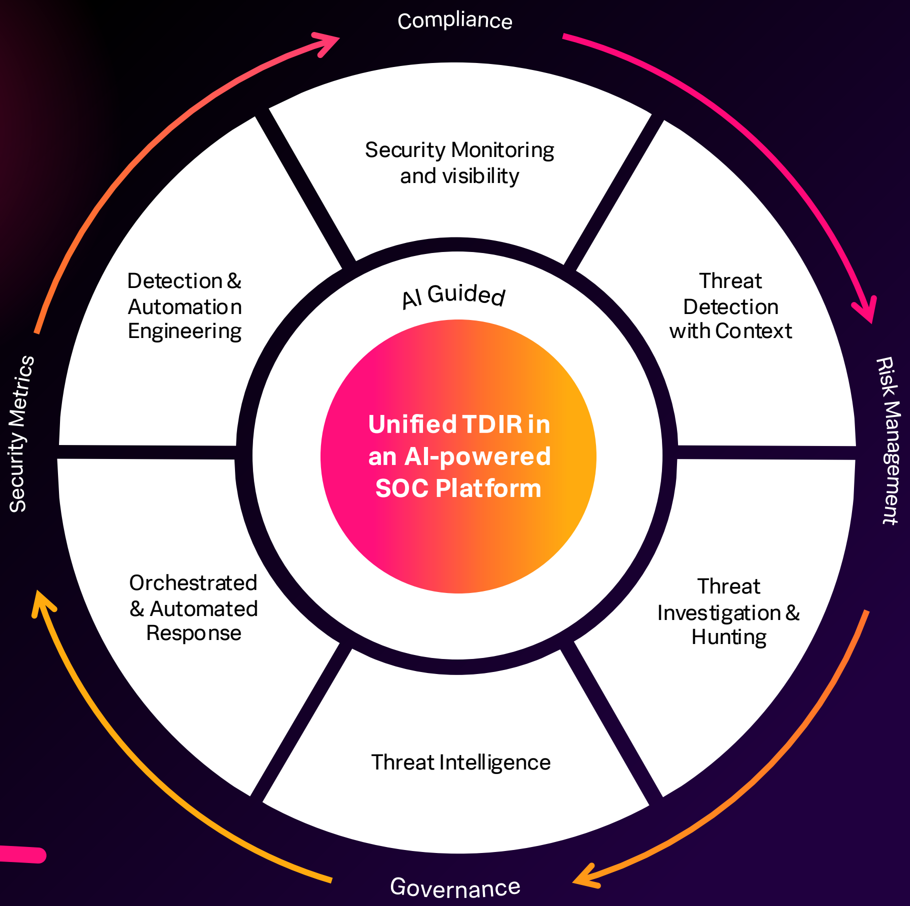
<=ES 7.3	ES 8
Incident Review	(Mission Control) Analyst Queue
MC incident details page	Investigation details page
Risk object	Entity (any identity, asset, user or device)
Response plan, Response template	Response plan
Indicator, Threat artifact	Indicator
Threat-matching searches	Threat-match detections
Threat match, threat activity	Threat findings
Artifact, evidence	Artifact

For more information on the changed terms, see Glossary and Splunk Enterprise Security terminology.

The SOC Reimagined

A human + AI partnership to harness massive volumes of data and:

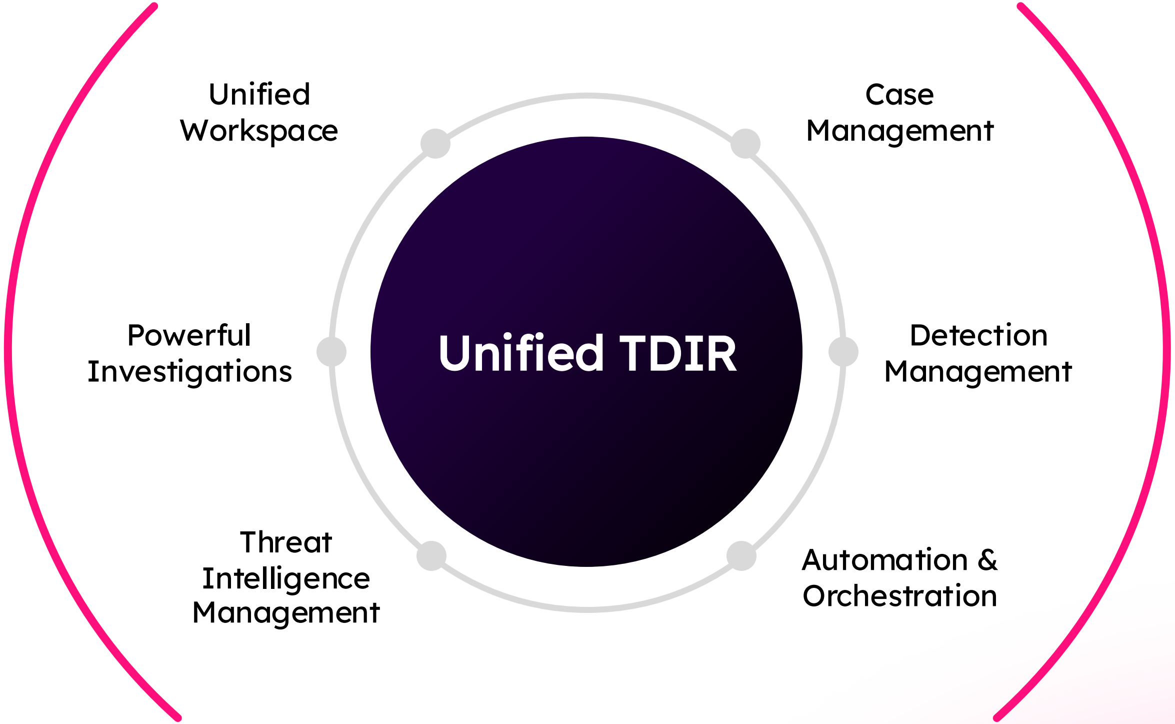
- Focus on the threats that matter most.
- Accelerate detection and response.
- Enable digital resilience for the business.



Compliance
Risk Management
Governance
Security Metrics
Security Monitoring and visibility
Threat Detection with Context
Threat Investigation & Hunting
Threat Intelligence
Orchestrated & Automated Response
Detection & Automation Engineering
AI Guided
Unified TDIR in an AI-powered SOC Platform

Unified Analyst Experience to Accelerate TDIR

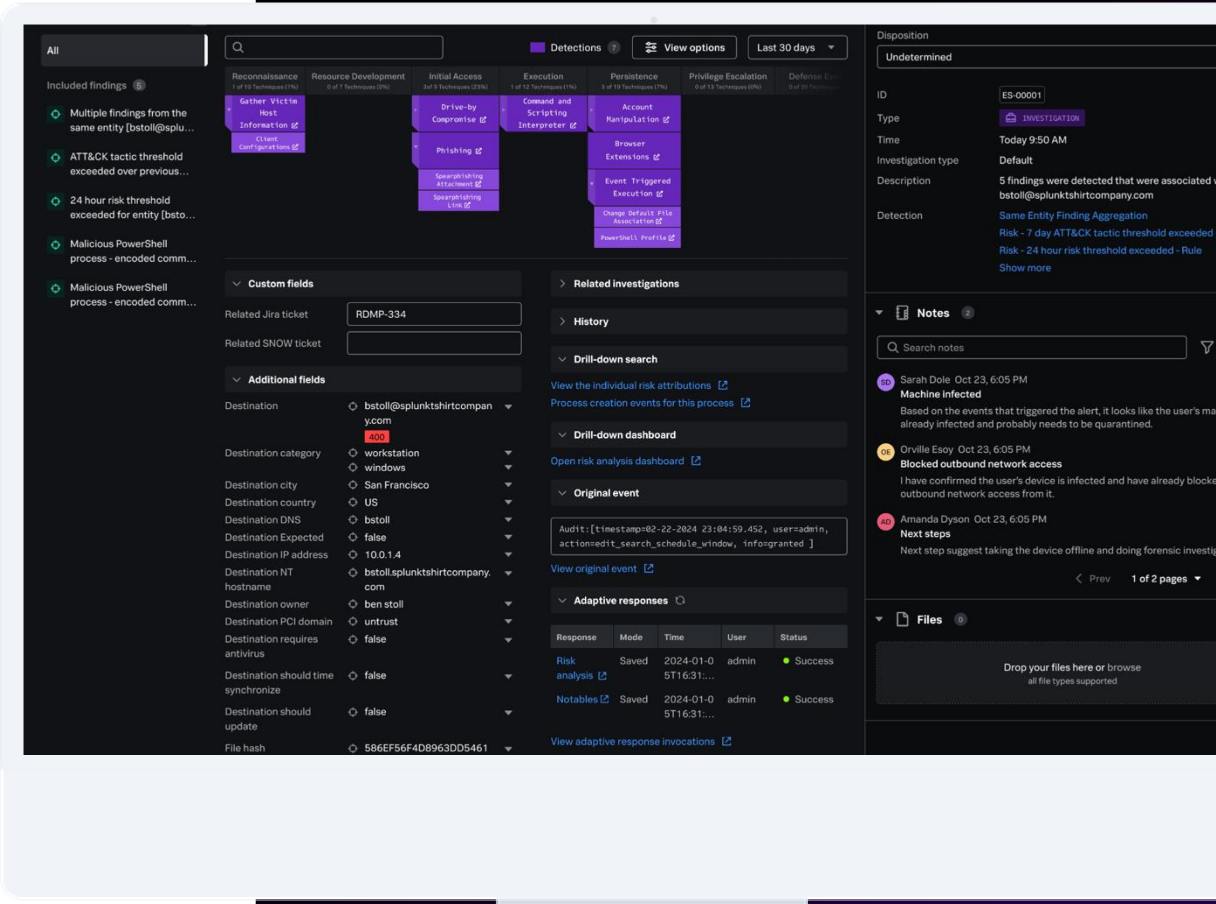
Coordination and collaboration across the TDIR lifecycle



Splunk Enterprise Security

The AI Powered SecOps Platform

- **Unlock full-fidelity visibility** and control of your security data wherever it lives.
- **Deliver the best analyst experience** and tooling with unified TDIR.
- **Accelerate the SOC** with built-in AI and Agentics across every layer.



All

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…

Detections 7 | View options | Last 30 days

Reconnaissance 1 of 10 Techniques (1%)	Resource Development 0 of 7 Techniques (0%)	Initial Access 3of 9 Techniques (23%)	Execution 1 of 12 Techniques (1%)	Persistence 3 of 19 Techniques (7%)	Privilege Escalation 0 of 13 Techniques (0%)	Defense E
Gather Victim Host Information		Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation		
Client Configurations		Phishing		Browser Extensions		
		Spearphishing Attachment		Event Triggered Execution		
		Spearphishing Link		Change Default File Association		
				PowerShell Profile		

Custom fields

Related Jira ticket: RDMP-334

Related SNOW ticket:

Additional fields

Destination: bstoll@splunktshirtcompany.com 400
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.splunktshirtcompany.com
Destination owner: ben stoll
Destination PCI domain: untrust
Destination requires antivirus: false
Destination should time synchronize: false
Destination should update: false
File hash: 586EF56F4D8963DD5461

Related investigations

History

Drill-down search

View the individual risk attributions

Process creation events for this process

Drill-down dashboard

Open risk analysis dashboard

Original event

```
Audit:[timestamp=02-22-2024 23:04:59.452, user=admin,
action=edit_search_schedule_window, info=granted ]
```

View original event

Adaptive responses

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

View adaptive response invocations

Disposition: Undetermined

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

Notes 2

Search notes

SD Sarah Dole Oct 23, 6:05 PM
Machine infected
Based on the events that triggered the alert, it looks like the user's ma already infected and probably needs to be quarantined.

OE Orville Esoy Oct 23, 6:05 PM
Blocked outbound network access
I have confirmed the user's device is infected and have already blocke outbound network access from it.

AD Amanda Dyson Oct 23, 6:05 PM
Next steps
Next step suggest taking the device offline and doing forensic investi

< Prev 1 of 2 pages

Files 0

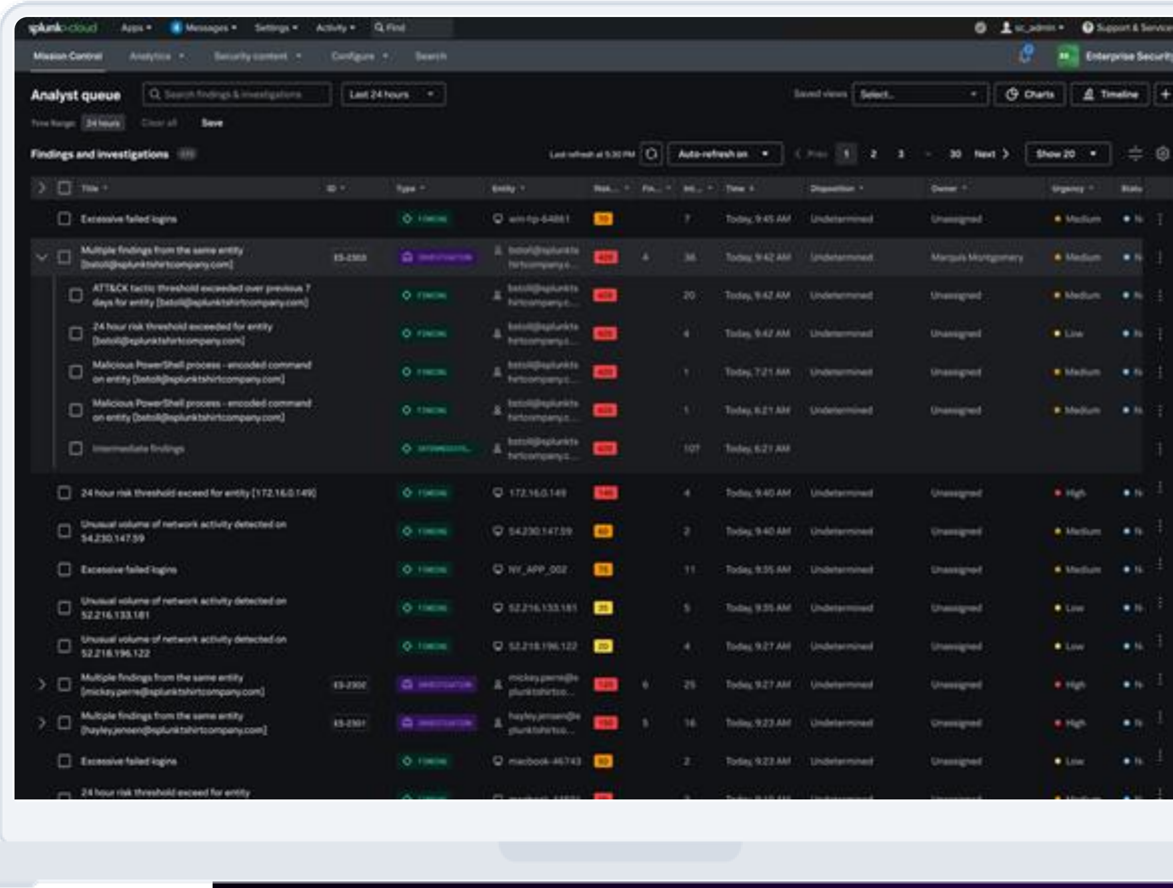
Drop your files here or browse
all file types supported

© 2025 SPLUNK LLC

Unlock Full Fidelity Visibility

Make sense of all data and enable fast action

- Ingest, federate, and normalize **data from any source**, cloud, or OT for unified visibility.
- Optimize data routing, filtering, and storage to **control costs and maintain full access** for compliance and analysis.
- Enrich every alert **with integrated Cisco Talos and Splunk threat intelligence** for faster, more precise triage.
- Stay ahead with **world-class detections**—rule-based, AI-driven, and custom—continuously updated and mapped to MITRE ATT&CK.
- New — Deploy, test, and monitor detections faster with **Detection Studio***, enabling seamless coverage and quick gap closure.
- **Proactively address risk with RBA**, correlating weak signals, reducing false positives, and accelerating triage.



Analyst queue

Findings and investigations

Title	ID	Type	Entity	Risk...	Fin...	Int...	Time	Disposition	Owner	Urgency	Statu
Excessive failed logins		FINDING	win-ftp-64881	[illegible]		7	Today, 9:45 AM	Undetermined	Unassigned	Medium	N
Multiple findings from the same entity [batoll@splunktshirtcompany.com]	ES-2303	INVESTIGATION	batoll@splunkts hirtcompany.c...	[illegible]	4	36	Today, 9:42 AM	Undetermined	Marquis Montgomery	Medium	N
ATT&CK tactic threshold exceeded over previous 7 days for entity [batoll@splunktshirtcompany.com]		FINDING	batoll@splunkts hirtcompany.c...	[illegible]		20	Today, 9:42 AM	Undetermined	Unassigned	Medium	N
24 hour risk threshold exceeded for entity [batoll@splunktshirtcompany.com]		FINDING	batoll@splunkts hirtcompany.c...	[illegible]		4	Today, 9:42 AM	Undetermined	Unassigned	Low	N
Malicious PowerShell process - encoded command on entity [batoll@splunktshirtcompany.com]		FINDING	batoll@splunkts hirtcompany.c...	[illegible]		1	Today, 7:21 AM	Undetermined	Unassigned	Medium	N
Malicious PowerShell process - encoded command on entity [batoll@splunktshirtcompany.com]		FINDING	batoll@splunkts hirtcompany.c...	[illegible]		1	Today, 6:21 AM	Undetermined	Unassigned	Medium	N
Intermediate findings		INTERMEDIATE...	batoll@splunkts hirtcompany.c...	[illegible]		107	Today, 6:21 AM				
24 hour risk threshold exceed for entity [172.16.0.149]		FINDING	172.16.0.149	[illegible]		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...	[illegible]	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...	[illegible]	5	16	Today, 9:23 AM	Undetermined	Unassigned	High	N
Excessive failed logins		FINDING	macbook-46743	80		2	Today, 9:23 AM	Undetermined	Unassigned	Low	N
24 hour risk threshold exceed for entity		[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	Undetermined	Unassigned	Medium	N

*In Alpha

Deliver the Best Analyst Experience

Unify threat detection, investigation and response (TDIR) workflows

New

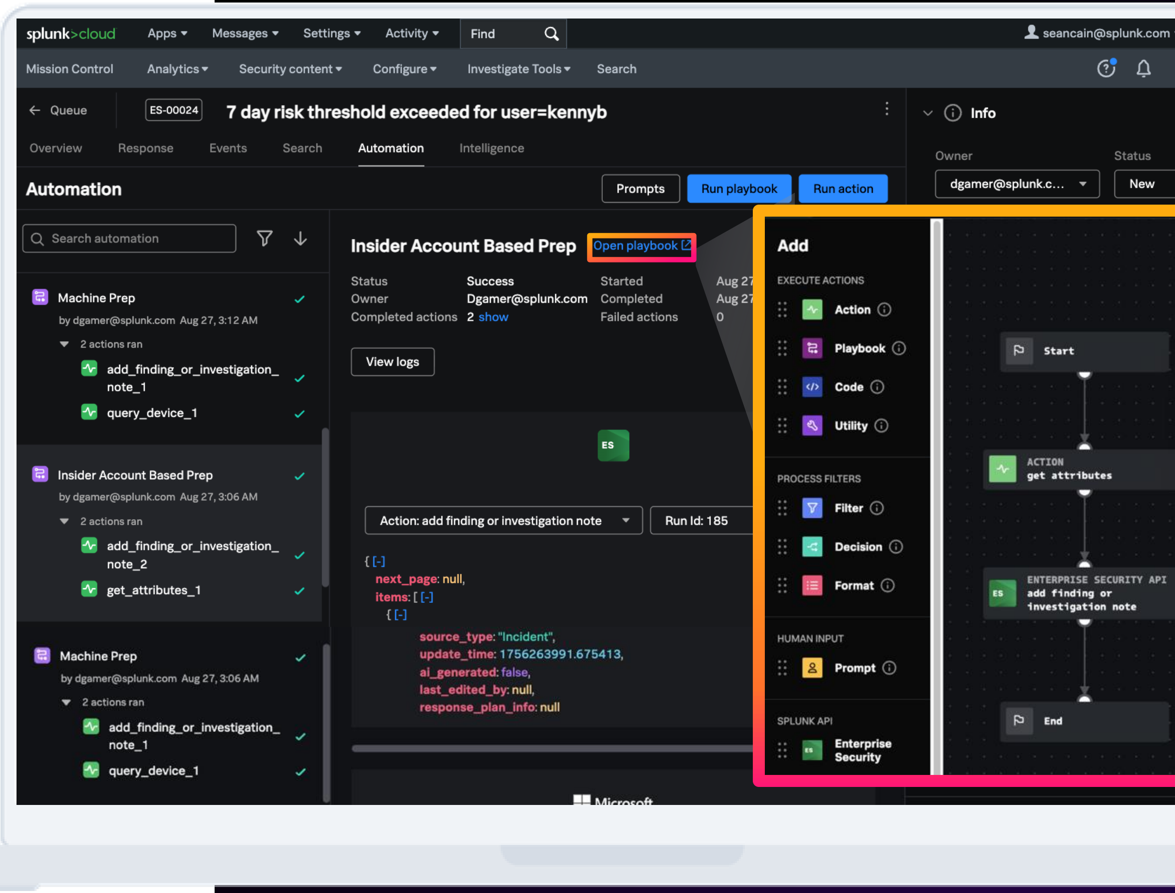
- **Get integrated, end-to-end TDIR workflows** with native SIEM, SOAR, UEBA, and threat intelligence for faster value and a unified analyst experience.

New

- **Empower every analyst with embedded SOAR*** and case management to standardize playbooks, cut errors, and automate triage and response.

New

- **Detect and mitigate insider threats with UEBA***, which baselines activity and elevates risky behaviors for rapid, confident action.



7 day risk threshold exceeded for user=kennyb

Machine Prep ✓
by dgamer@splunk.com Aug 27, 3:12 AM
2 actions ran
add_finding_or_investigation_note_1 ✓
query_device_1 ✓

Insider Account Based Prep ✓
by dgamer@splunk.com Aug 27, 3:06 AM
2 actions ran
add_finding_or_investigation_note_2 ✓
get_attributes_1 ✓

Machine Prep ✓
by dgamer@splunk.com Aug 27, 3:06 AM
2 actions ran
add_finding_or_investigation_note_1 ✓
query_device_1 ✓

Insider Account Based Prep

Status Success
Owner Dgamer@splunk.com
Completed actions 2 show
Started Aug 27
Completed Aug 27
Failed actions 0

Action: add finding or investigation note
Run Id: 185

```
{[-]
 next_page: null,
 items: [ [-]
  {[-]
     source_type: "Incident",
     update_time: 1756263991.675413,
     ai_generated: false,
     last_edited_by: null,
     response_plan_info: null
```

*In controlled availability

Accelerate the SOC

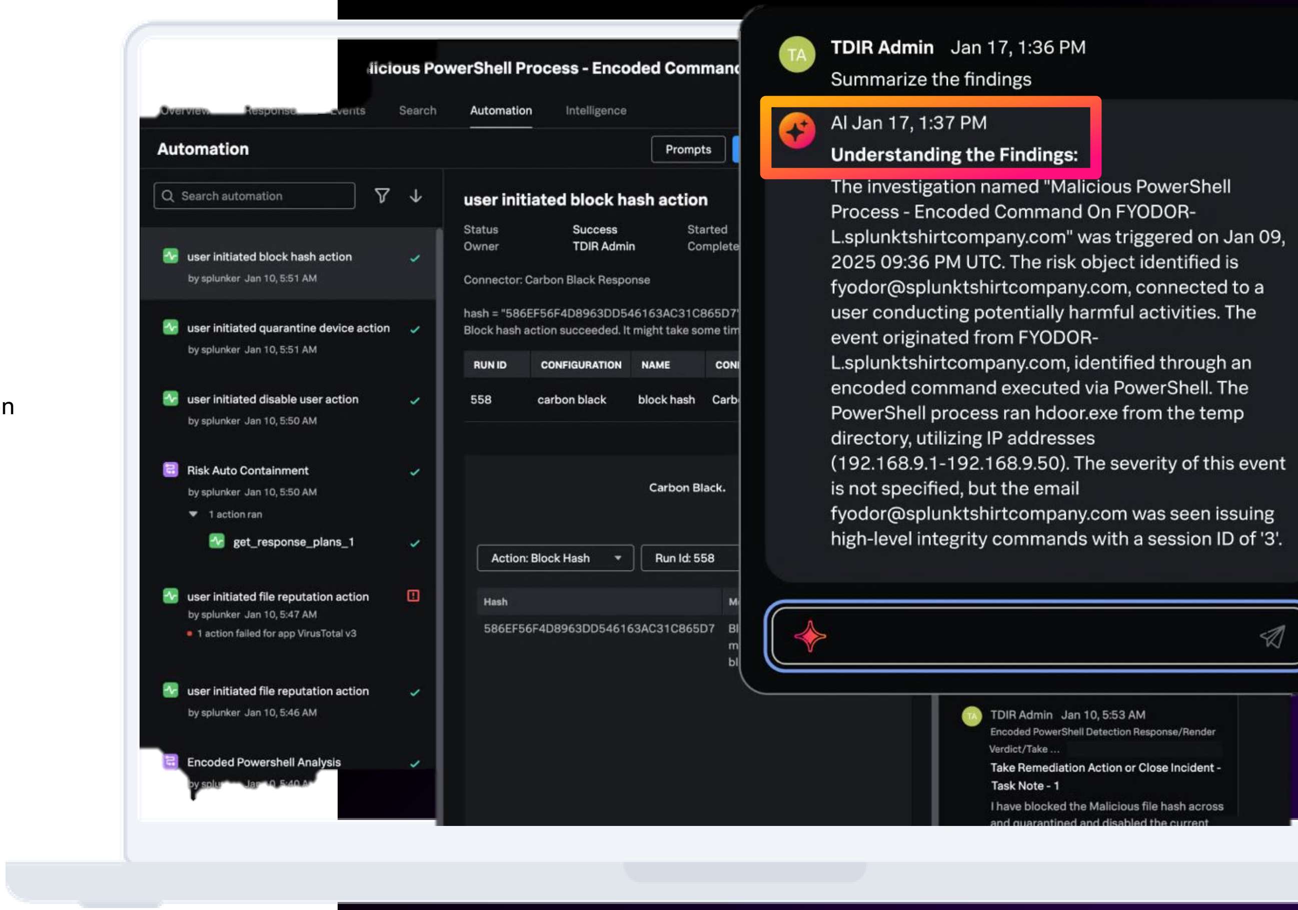
Use built-in AI and Agentics across every layer

Triage and Investigation

- CA Use **AI Assistants*** to generate SPL queries, summarize findings, and provide investigation and remediation guidance from natural language.
- Alpha Let **Triage Agents**** evaluate, prioritize, and explain alerts, reducing workload and highlighting critical issues.

Automation and Response

- Alpha Accelerate automation with **AI Playbook Authoring**** that turns plain language into tested SOAR playbooks—no deep VPE expertise needed.
- Alpha Rely on **Autonomous Response Agents**** to execute response actions in security tools based on set instructions.



licious PowerShell Process - Encoded Command

Automation

user initiated block hash action ✓
by splunker Jan 10, 5:51 AM

user initiated quarantine device action ✓
by splunker Jan 10, 5:51 AM

user initiated disable user action ✓
by splunker Jan 10, 5:50 AM

Risk Auto Containment ✓
by splunker Jan 10, 5:50 AM
1 action ran
get_response_plans_1 ✓

user initiated file reputation action !
by splunker Jan 10, 5:47 AM
1 action failed for app VirusTotal v3

user initiated file reputation action ✓
by splunker Jan 10, 5:46 AM

Encoded Powershell Analysis ✓
by splunker Jan 10, 5:40 AM

user initiated block hash action

Status Success Started
Owner TDIR Admin Complete

Connector: Carbon Black Response

hash = "586EF56F4D8963DD546163AC31C865D7"
Block hash action succeeded. It might take some tim

RUN ID	CONFIGURATION	NAME	CONI
558	carbon black	block hash	Carb

Carbon Black.

Action: Block Hash
Run Id: 558

Hash	M
586EF56F4D8963DD546163AC31C865D7	Bl m bl

TA TDIR Admin Jan 17, 1:36 PM
Summarize the findings

AI Jan 17, 1:37 PM
Understanding the Findings:
The investigation named "Malicious PowerShell Process - Encoded Command On FYODOR-L.splunktshirtcompany.com" was triggered on Jan 09, 2025 09:36 PM UTC. The risk object identified is fyodor@splunktshirtcompany.com, connected to a user conducting potentially harmful activities. The event originated from FYODOR-L.splunktshirtcompany.com, identified through an encoded command executed via PowerShell. The PowerShell process ran hdoor.exe from the temp directory, utilizing IP addresses (192.168.9.1-192.168.9.50). The severity of this event is not specified, but the email fyodor@splunktshirtcompany.com was seen issuing high-level integrity commands with a session ID of '3'.

TA TDIR Admin Jan 10, 5:53 AM
Encoded PowerShell Detection Response/Render Verdict/Take ...
Take Remediation Action or Close Incident - Task Note - 1
I have blocked the Malicious file hash across and quarantined and disabled the current

* In Controlled Availability
**In Alpha

Enterprise Security Editions

**Up to v8.2*

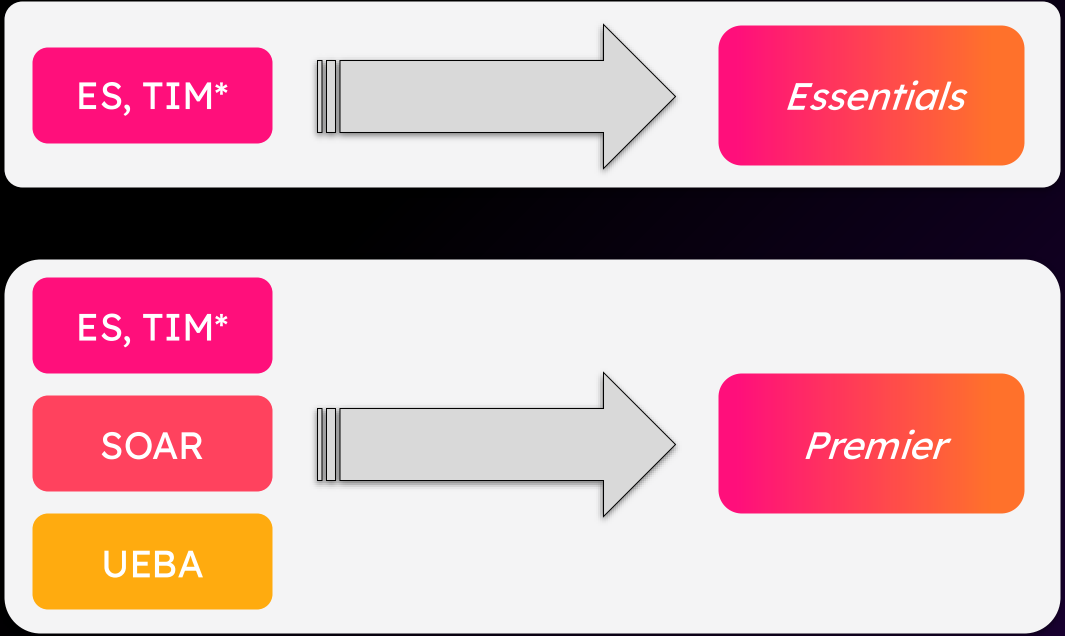
One SecOps Platform, Available in Two Editions

Use Case	Essentials Edition	Premier Edition
Security Monitoring	Get a unified view across all environments for clearer threat visibility and faster, data-driven response	
Threat Detection	Tackle unknown and known threats with a range of detections (correlations, rule-based, AI/ML, and custom)	**Elevate Threat Detection with AI** to easily understand and fine tune detection rules*
Threat Investigation	Leverage the unified Mission Control interface to rapidly analyze, identify and investigate threats for an effective response	Accelerate investigation through **automated playbooks** and amplify human expertise with the **Triage Agent*** to automatically enriches alerts with more context.
Threat Hunting	Use findings and searches to identify malicious activity and mitigate attacks before they escalate	Enhance threat hunting by leveraging **UEBA's ML-driven behavioral insights** and accelerate evidence gathering and response with **1-click automated runbooks**
Automation	Use one time Adaptive Response actions for basic orchestration or integrate with a SOAR product for full spectrum automation	Accelerate response time, minimize human error, and ensure consistent enforcement of security policies. **Available OOTB for every person in the SOC**
Insider Threat Detection	Requires manual implementation or integration with a separate product	Mitigate insider threat in real time using : **OOTB, proven, and scalable ML models, fully integrated in investigation workflows**

*In Alpha

Individual Products → Platform with Editions

A single, integrated platform with capabilities and features supporting TDIR



ES, TIM* → *Essentials*

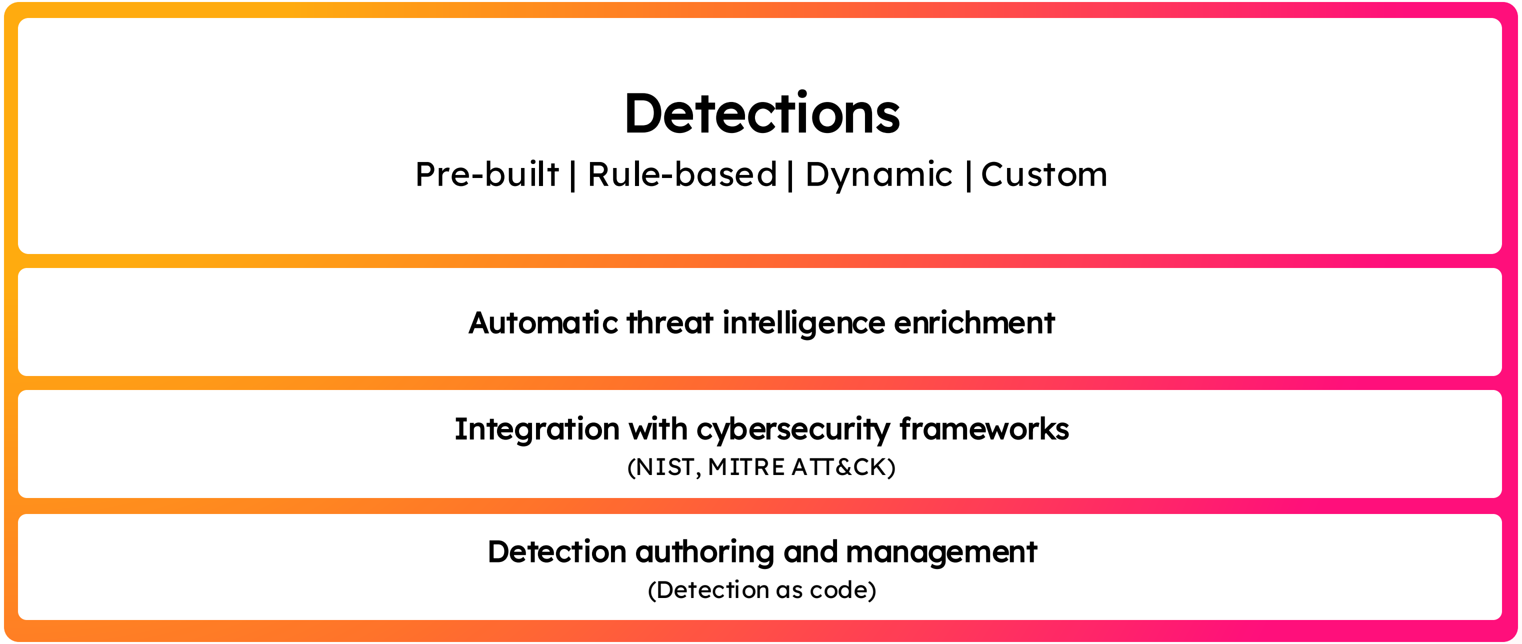
ES, TIM*
SOAR
UEBA
→ *Premier*

⚠ *Not the same as Splunk Security Essentials (SSE)!*

**Cloud only at this time*

Threat Detection

At the core of a TDIR platform are detections



Detections

Pre-built | Rule-based | Dynamic | Custom

Automatic threat intelligence enrichment

Integration with cybersecurity frameworks
(NIST, MITRE ATT&CK)

Detection authoring and management
(Detection as code)

A Mix of Detection Capabilities

Pre-built detections

- 1,700+ Curated Detections by Splunk Threat Research
- 225+ Analytic Stories
- 75+ Automation Playbooks

Rule-based detections

- Event-based Detections
- Findings-based Detections
- Adaptive Response Actions
- Automation Rules and SOAR Playbooks

Dynamic detections

- ML-based Detections
- User (and Entity) Behavior Analytics
- Risk-Based Alerting

Custom detections

- Fully customizable built-in detections
- Full flexibility to create custom detections
- Machine Learning Toolkit

Automatic threat intelligence enrichment

(Threat Intelligence Management, Talos Threat Intelligence, 3rd Party)

Integration with cybersecurity frameworks

(Threat Topology Visualization, MITRE ATT&CK, NIST CSF 2.0, Cyber Kill Chain®)

Detection authoring and management

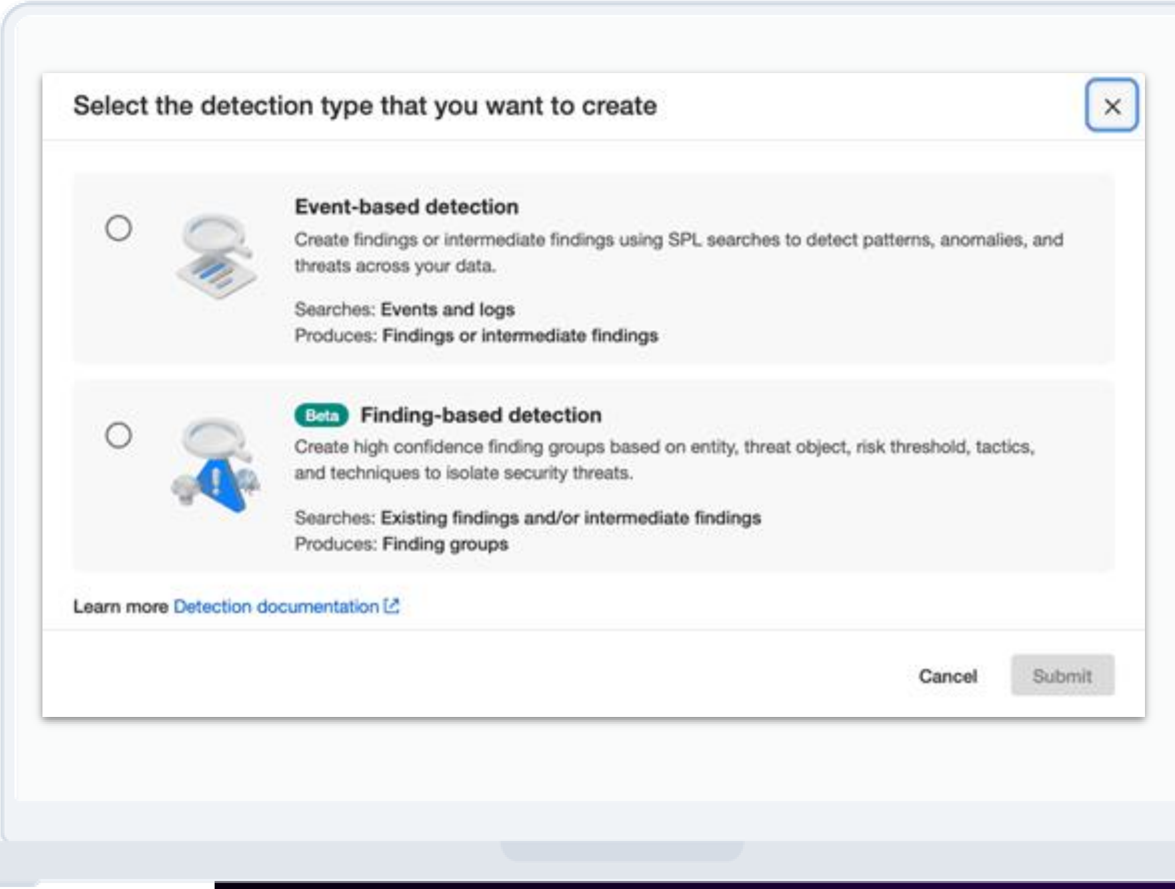
(Automatic Detection Versioning, Open Source Tools)

Detection Authoring and Management

- **Detection Management:** Detection engineers harness the redesigned detection editors to easily track and monitor changes
- **Noise Reduction:** Detection engineers now capture entity and risk context with all detections, and finding-based detections enable aggregation of findings

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.



Select the detection type that you want to create

○ **Event-based detection**

Create findings or intermediate findings using SPL searches to detect patterns, anomalies, and threats across your data.

Searches: Events and logs
Produces: Findings or intermediate findings

○ Beta **Finding-based detection**

Create high confidence finding groups based on entity, threat object, risk threshold, tactics, and techniques to isolate security threats.

Searches: Existing findings and/or intermediate findings
Produces: Finding groups

Learn more Detection documentation

Event-Based Detections

Analysts can choose if the detection outputs a **finding** or an **intermediate finding**

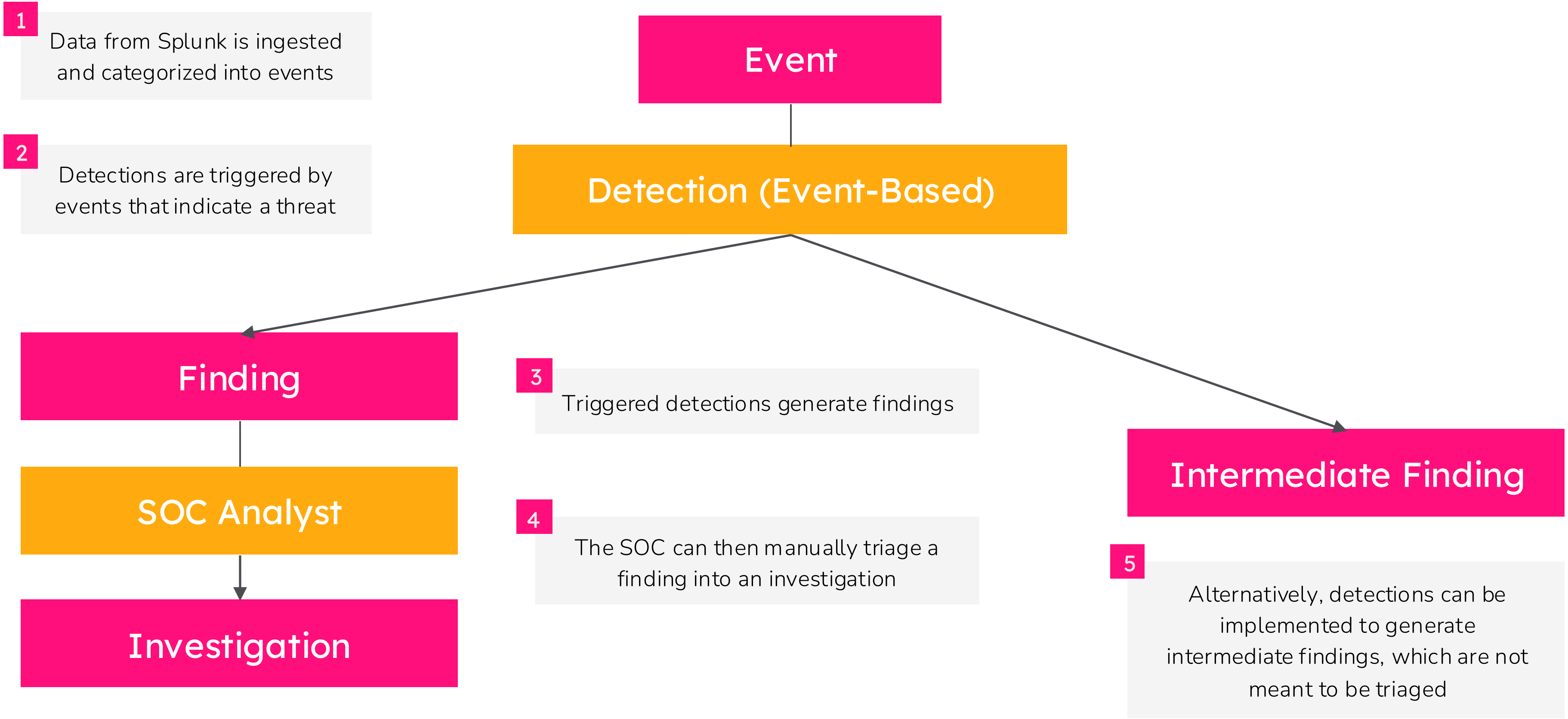
Findings

- Combine the features of notable events and risk events into a single object
- Represent one or more anomalous incidents or alerts
- Metadata about the detection including tactics, techniques, confidence, impact, risk score, and threat objects are included
- View and triage in the Analyst Queue
- Manually created or automatically generated by detections
- Can be a group of alerts or a standalone alert

Intermediate Findings

- Records or observations that indicate anomalies but might not be standalone security incidents
- Not available in the queue to triage
- Can appear identical to findings in style, format, and metadata based on the data stored in the index
- Might be used as input by advanced finding-based detections to discover potential security incidents with high fidelity and confidence

ES 8 Workflow: Event-Based Detections



Event

Detection (Event-Based)

Finding

SOC Analyst

Investigation

Intermediate Finding

1 Data from Splunk is ingested and categorized into events

2 Detections are triggered by events that indicate a threat

3 Triggered detections generate findings

4 The SOC can then manually triage a finding into an investigation

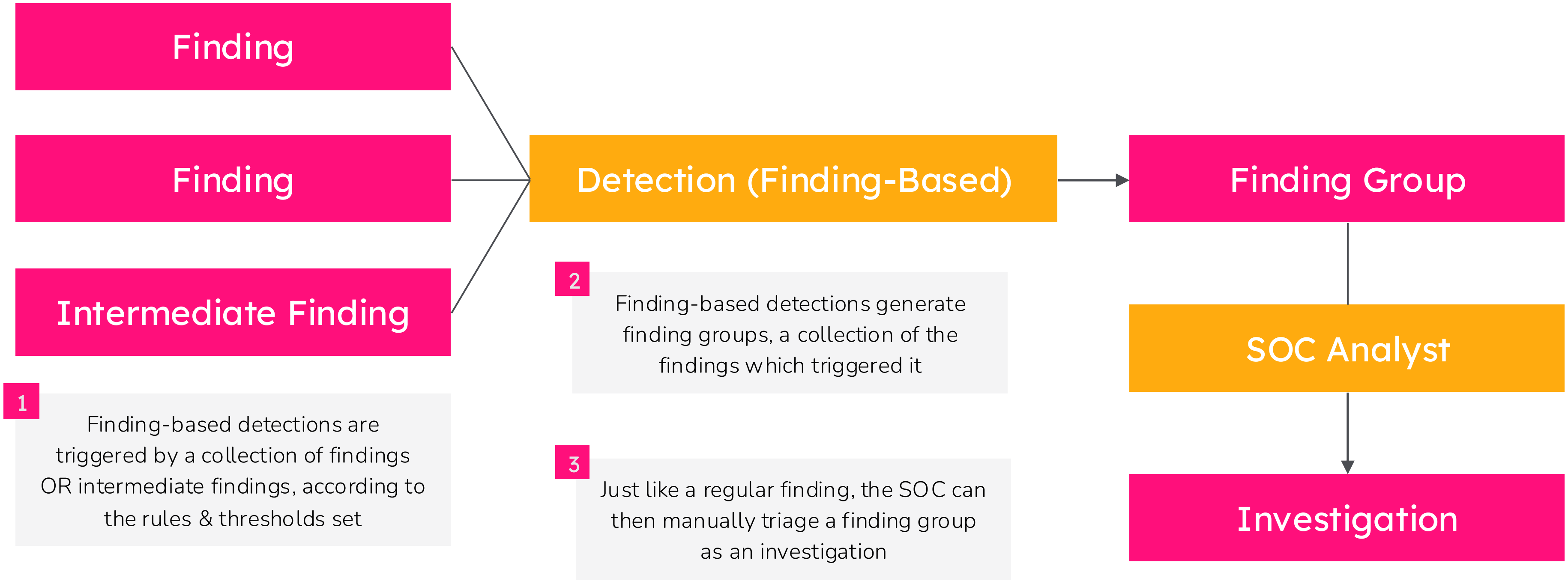
5 Alternatively, detections can be implemented to generate intermediate findings, which are not meant to be triaged

Finding-Based Detections (Beta)

NOTE: Finding-based detections in Splunk Enterprise Security are currently released as a preview feature.

- Similar to **risk incident rules**
- Based on findings, as opposed to events
- Can incorporate **findings, intermediate findings**, or **both**
- Output the findings and intermediate findings that triggered them, as a **finding group**
- Finding groups show up in the analyst queue and can be triaged into investigations

ES 8 Workflow: Finding-Based Detections



Finding

Finding

Intermediate Finding

Detection (Finding-Based)

Finding Group

SOC Analyst

Investigation

1 Finding-based detections are triggered by a collection of findings OR intermediate findings, according to the rules & thresholds set

2 Finding-based detections generate finding groups, a collection of the findings which triggered it

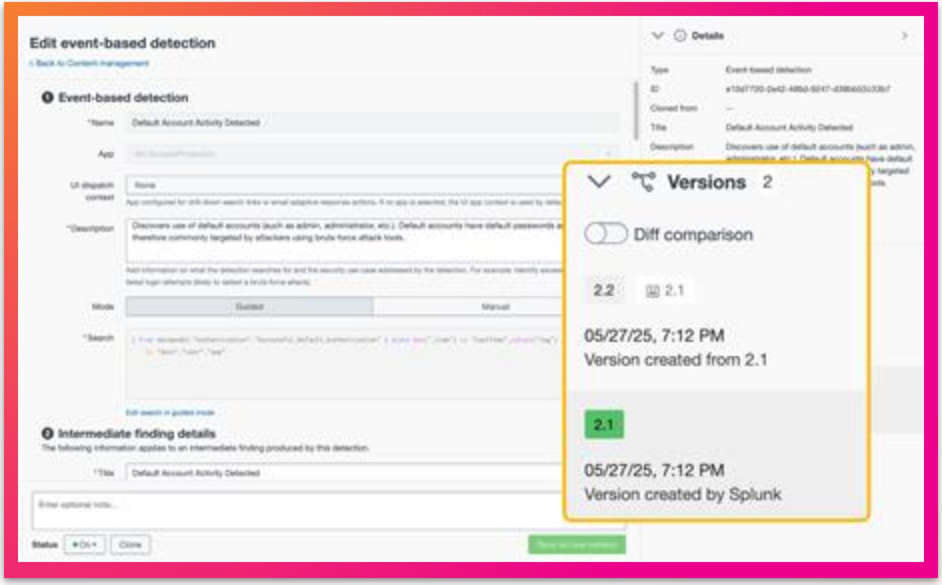
3 Just like a regular finding, the SOC can then manually triage a finding group as an investigation

Tuning of Detections

Detection Versioning

Analysts can now use versioning to keep track of their history editing the detection

- **Versioning and content pipelines** so that content engineers can more easily build and maintain a content development lifecycle
- **Rollback to any version** so that an older version is be used while changes are saved to newer versions
- **Relationships** clearly connect original source to customized detections
- **Change history** captured for audit purposes (who, what, when..)
- **Content archiving** as a means to retire security detections without losing historical context
- **Notes enforcement** available for new versions are created



Edit event-based detection

‹ Back to Content management

❶ Event-based detection

*Name: Default Account Activity Detected

App: [illegible]

UI dispatch context: None

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

*Description: Discovers use of default accounts (such as admin, administrator, etc.). Default accounts have default passwords a[illegible] therefore commonly targeted by attackers using brute force attack tools.

Add information on what the detection searches for and the security use case addressed by the detection. For example: Identify excess[illegible] failed login attempts (likely to detect a brute-force attack).

Mode: Guided | Manual

*Search: [illegible]

Edit search in guided mode

❷ Intermediate finding details

The following information applies to an intermediate finding produced by this detection.

*Title: Default Account Activity Detected

Enter optional note...

Status: ● On ▾ | Clone | [illegible]

Details

Type	Event-based detection
ID	[illegible]
Cloned from	—
Title	Default Account Activity Detected
Description	Discovers use of default accounts (such as admin, administrator, etc.). Default accounts have default [illegible] targeted [illegible]

Versions 2

○ Diff comparison

2.2 | 2.1

05/27/25, 7:12 PM
Version created from 2.1

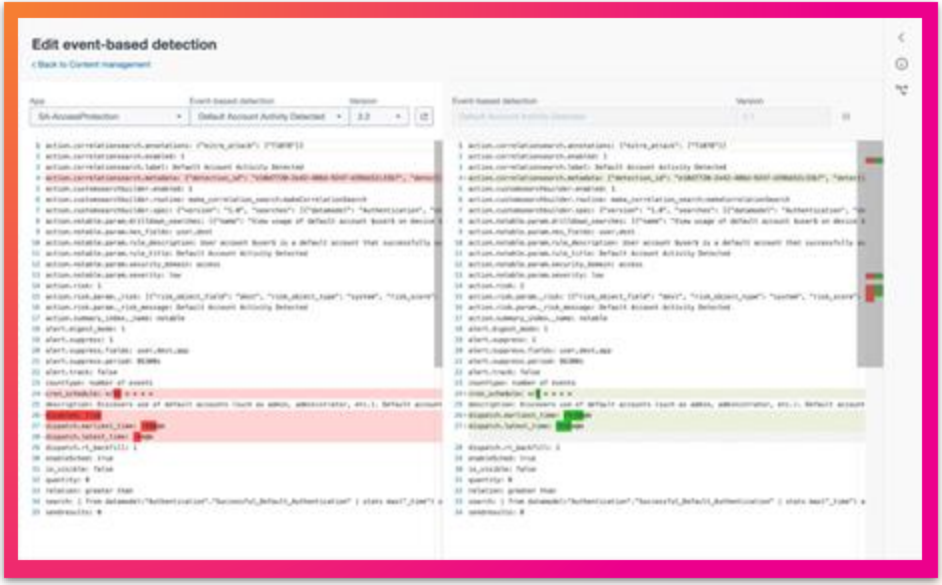
2.1

05/27/25, 7:12 PM
Version created by Splunk

Detection Diffing

Line-by-line tracking for changes in detections

- Detection editors now allows **side-by-side** comparison of detections
- Differences between detections **highlighted** clearly
- Users can **compare to other detections** as well as prior versions of the same detection



Edit event-based detection

< Back to Content management

App: SA-AccessProtection

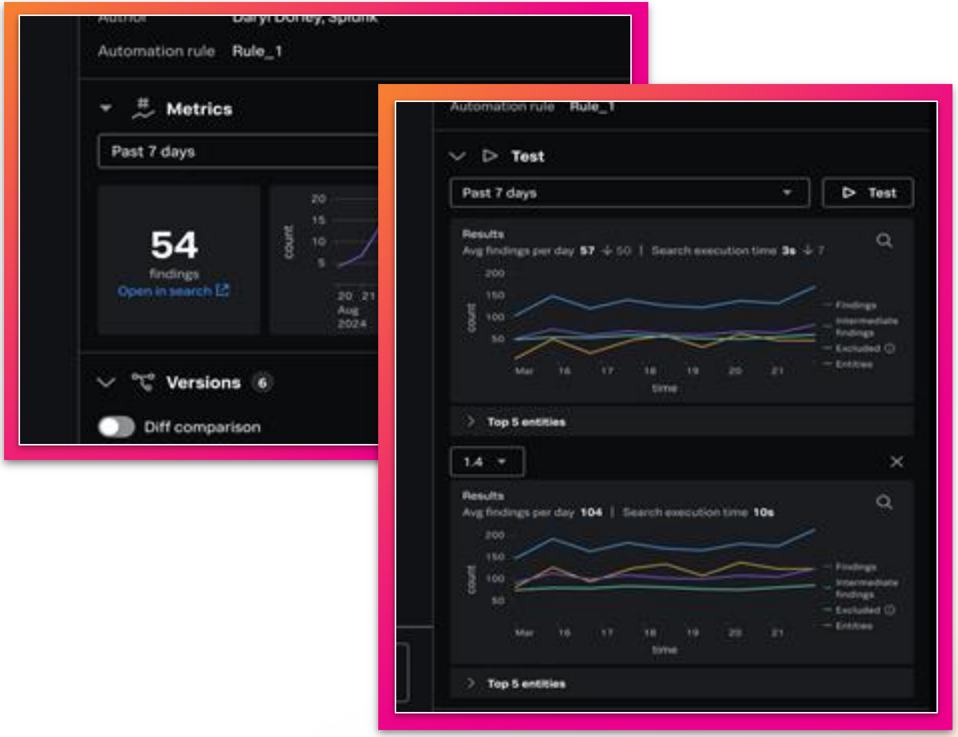
Event-based detection: Default Account Activity Detected

Version: 3.2

Detection In-Editor Testing (Beta)

Native ability to validate SPL searches directly in the Detection Editor

- **Quickly see** how many Findings or Intermediate Findings a rule would generate over a defined time window
- Identify overly broad or narrow detections before they're deployed, **reducing false positives and missed threats**
- Streamline detection tuning for new analysts by giving **immediate feedback** during detection creation



Author Daryl Dorley, Splunk

Automation rule Rule_1

Past 7 days

54 findings

Diff comparison

Automation rule Rule_1

Past 7 days

Results

Avg findings per day 57 ↓ 50 | Search execution time 3s ↓ 7

1.4

Results

Avg findings per day 104 | Search execution time 10s

Investigation

Case Management

Structured and efficient way to manage security incidents from detection to resolution

Workflow Management

Centralized and streamlined workflows for incident response, from initial triage to remediation.

Increased Efficiency

Native integration with Splunk SOAR to automate repetitive tasks and workflows to help SOC analysts become more efficient and productive.

Better Collaboration

Enhanced communication and collaboration among SOC analysts, incident responders, and other relevant teams.

Reduced Risk

Threat prioritization based on risk level, type of threat, the assets and identities affected, and the potential for damage.

Enhanced Compliance

Clear audit trail of security incidents and their handling, making it easier to demonstrate compliance to regulatory bodies.

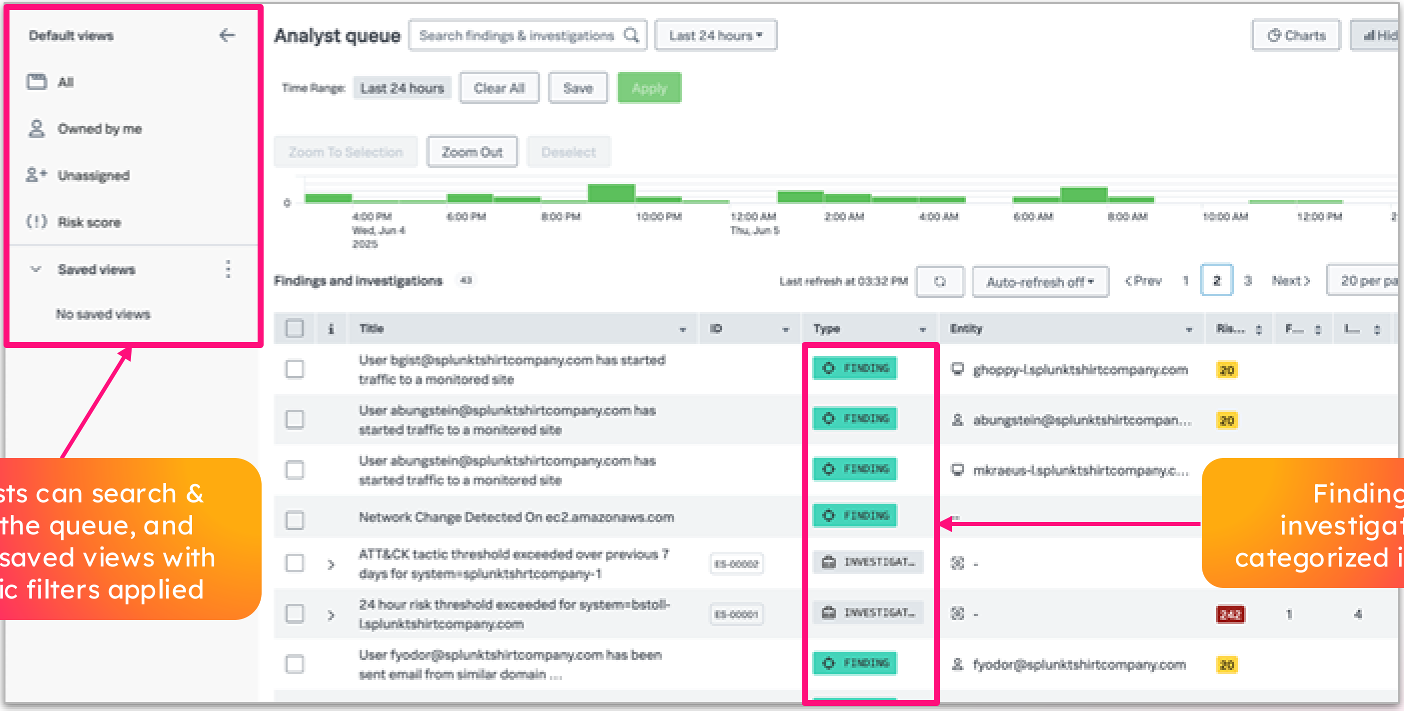
Case Management

Case Management Workflow

- **Triage:** Analysts leverage the redesigned analyst queue to search, sort, filter, and inspect findings
- **Investigate:** Suspicious findings can be flagged, grouped, and reviewed via the new investigations feature
- **Respond:** Native SOAR integration and MC response plans offer numerous pathways to respond to threats both manually and via automation

Analyst Queue

Centralized location for SOC analysts to view findings and investigations



Time Range: Last 24 hours

Findings and investigations 43

Last refresh at 03:32 PM

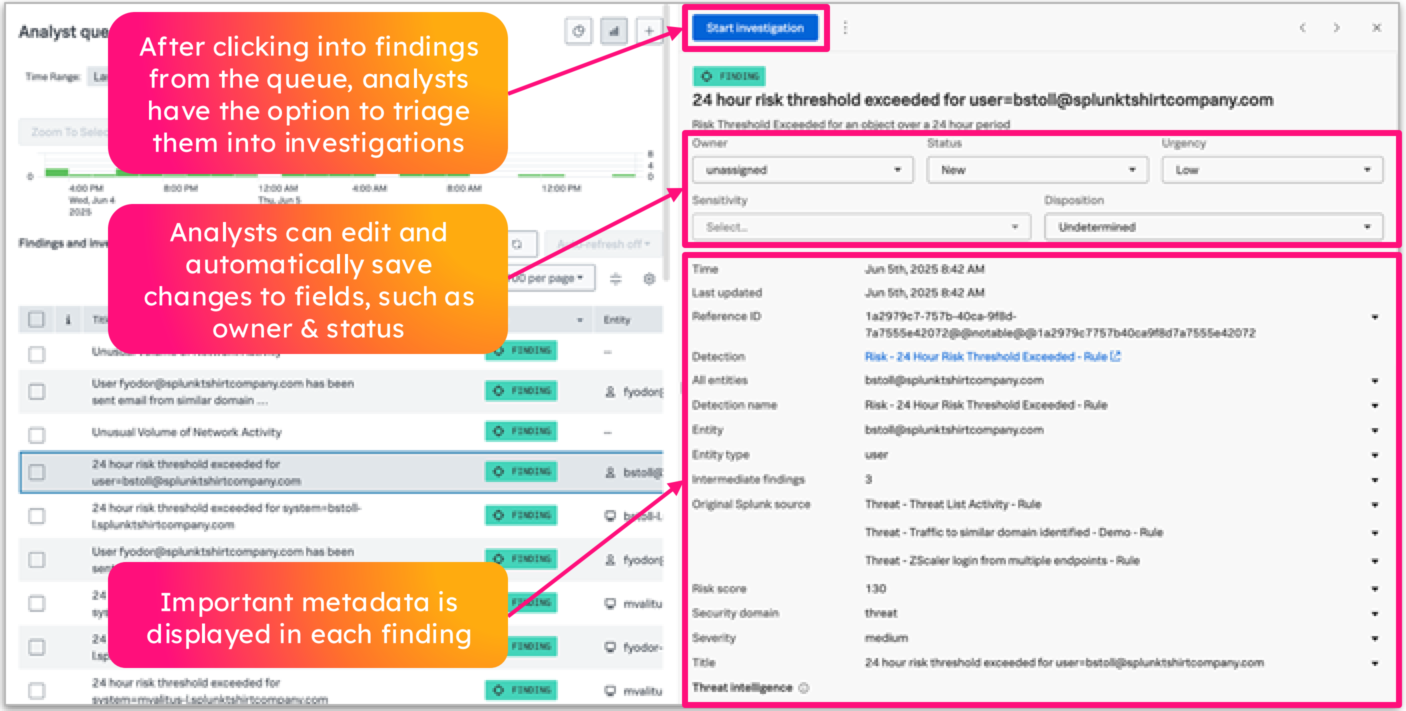
□	i	Title	ID	Type	Entity	Ris...	F...	I...
□		User bgist@splunktshirtcompany.com has started traffic to a monitored site		FINDING	ghoppy-l.splunktshirtcompany.com	20		
□		User abungstein@splunktshirtcompany.com has started traffic to a monitored site		FINDING	abungstein@splunktshirtcompan...	20		
□		User abungstein@splunktshirtcompany.com has started traffic to a monitored site		FINDING	mkraeus-l.splunktshirtcompany.c...			
□		Network Change Detected On ec2.amazonaws.com		FINDING	--			
□	>	ATT&CK tactic threshold exceeded over previous 7 days for system=splunktshrtcompany-1	ES-00002	INVESTIGAT...	-			
□	>	24 hour risk threshold exceeded for system=bstoll-l.splunktshirtcompany.com	ES-00001	INVESTIGAT...	-	242	1	4
□		User fyodor@splunktshirtcompany.com has been sent email from similar domain ...		FINDING	fyodor@splunktshirtcompany.com	20		

Analysts can search & filter the queue, and create saved views with specific filters applied

Findings and investigations are categorized in the queue

Findings

Contain what was observed, which entity was impacted, and relevant detection metadata



Unusual Volume of Network Activity

User fyodor@splunktshirtcompany.com has been sent email from similar domain ... fyodor

Unusual Volume of Network Activity

24 hour risk threshold exceeded for user=bstoll@splunktshirtcompany.com bstoll@

24 hour risk threshold exceeded for system=bstoll-l.splunktshirtcompany.com bstoll-l.

User fyodor@splunktshirtcompany.com has been sen fyodor

24 sys mvalitu

24 l.sp fyodor-

24 hour risk threshold exceeded for system=mvalitus-l.splunktshirtcompany.com mvalitu

Start investigation

FINDING

24 hour risk threshold exceeded for user=bstoll@splunktshirtcompany.com

Risk Threshold Exceeded for an object over a 24 hour period

Owner: unassigned
Status: New
Urgency: Low
Sensitivity: Select...
Disposition: Undetermined

Time	Jun 5th, 2025 8:42 AM
Last updated	Jun 5th, 2025 8:42 AM
Reference ID	1a2979c7-757b-40ca-9f8d-7a7555e42072@@notable@@1a2979c7757b40ca9f8d7a7555e42072
Detection	Risk - 24 Hour Risk Threshold Exceeded - Rule
All entities	bstoll@splunktshirtcompany.com
Detection name	Risk - 24 Hour Risk Threshold Exceeded - Rule
Entity	bstoll@splunktshirtcompany.com
Entity type	user
Intermediate findings	3
Original Splunk source	Threat - Threat List Activity - Rule Threat - Traffic to similar domain identified - Demo - Rule Threat - ZScaler login from multiple endpoints - Rule
Risk score	130
Security domain	threat
Severity	medium
Title	24 hour risk threshold exceeded for user=bstoll@splunktshirtcompany.com

Threat intelligence

After clicking into findings from the queue, analysts have the option to triage them into investigations

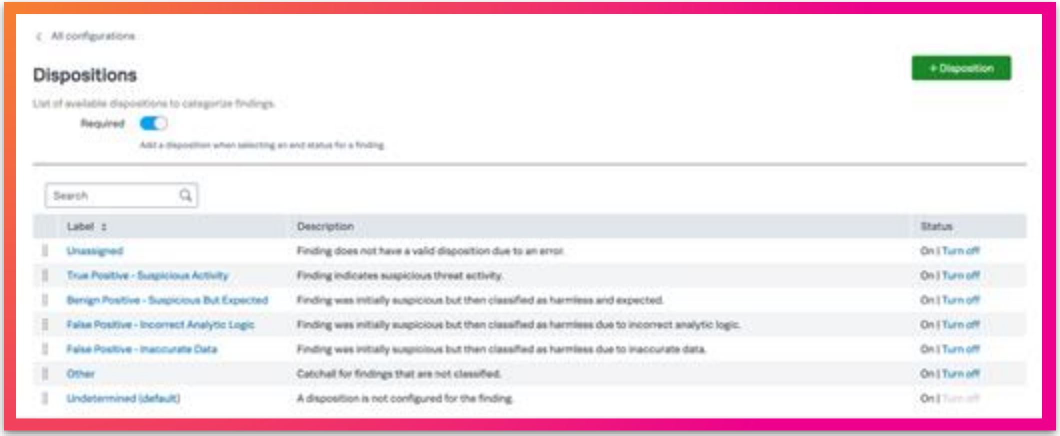
Analysts can edit and automatically save changes to fields, such as owner & status

Important metadata is displayed in each finding

The Power of Dispositions

https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.2/investigations/configure-dispositions-for-findings-in-splunk-enterprise-security

- Classification is necessary for effective tuning
- Improve detection context and accuracy
- Classify findings and investigations based on the threat level associated with them
- Define custom categories based on the actual work performed by incident responders
- Option to mandate entering a disposition before closing a finding



Dispositions

List of available dispositions to categorize findings.

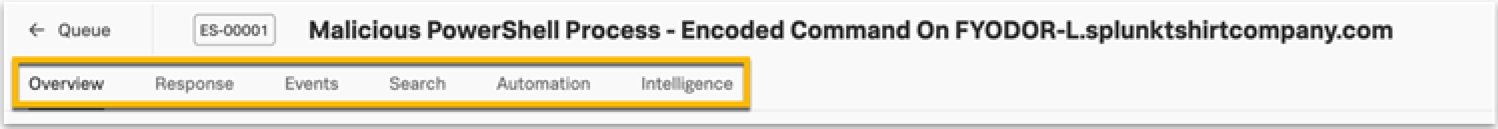
Required: ●

Add a disposition when selecting an end status for a finding.

Label	Description	Status
Unassigned	Finding does not have a valid disposition due to an error.	On | Turn off
True Positive - Suspicious Activity	Finding indicates suspicious threat activity.	On | Turn off
Benign Positive - Suspicious But Expected	Finding was initially suspicious but then classified as harmless and expected.	On | Turn off
False Positive - Incorrect Analytic Logic	Finding was initially suspicious but then classified as harmless due to incorrect analytic logic.	On | Turn off
False Positive - Inaccurate Data	Finding was initially suspicious but then classified as harmless due to inaccurate data.	On | Turn off
Other	Catchall for findings that are not classified.	On | Turn off
Undetermined (default)	A disposition is not configured for the finding.	On | Turn off

Investigation Tabs

Triage individual findings, multiple findings, or finding groups


← Queue
ES-00001
Malicious PowerShell Process - Encoded Command On FYODOR-L.splunktshirtcompany.com
Overview
Response
Events
Search
Automation
Intelligence

Overview: View the data associated with an investigation (e.g., original event, drill-down search, detection, custom fields, additional fields, history)

Response: Use the phases and tasks of a response plan to guide the investigation

Events: Add events to investigations, providing a link between raw data and the ongoing investigation

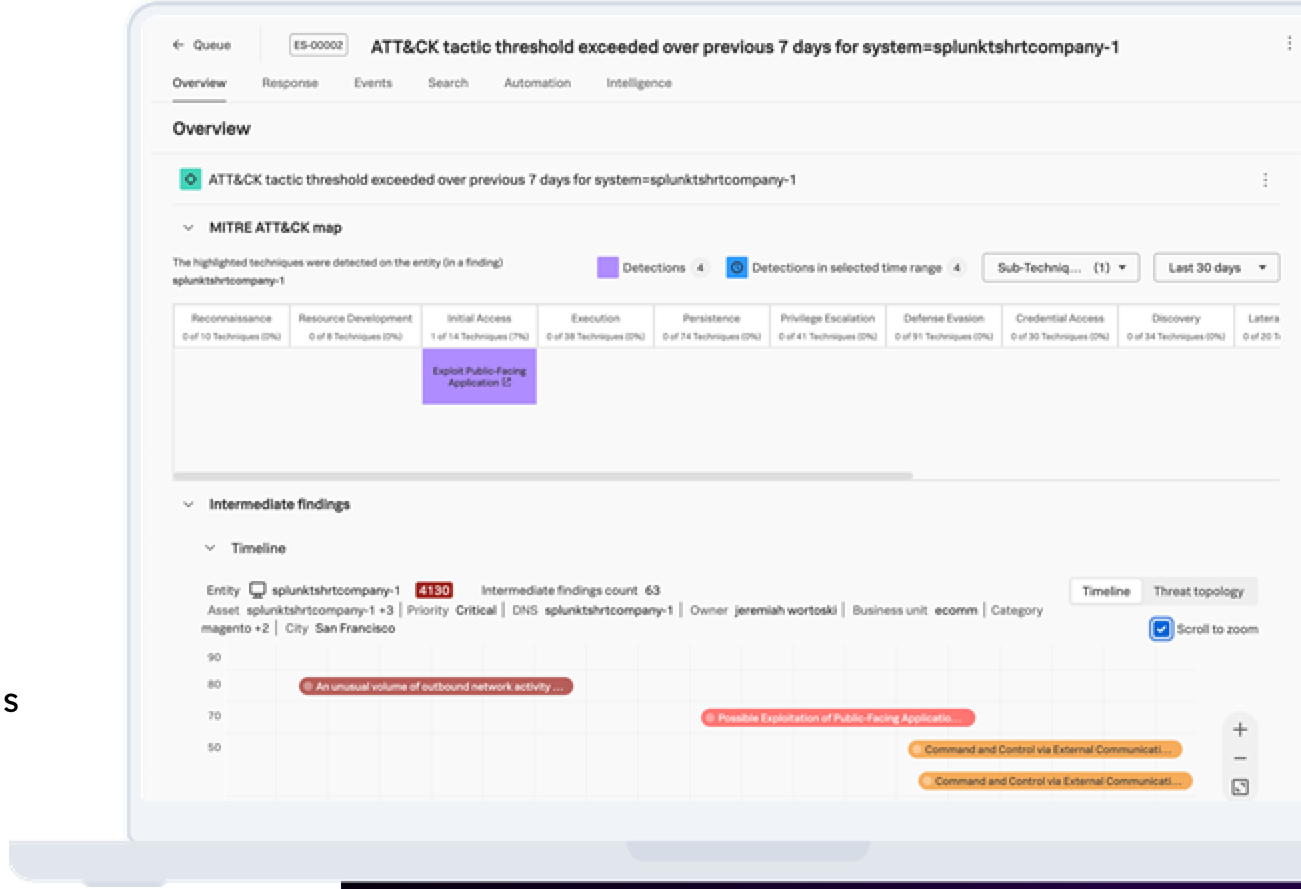
Search: Conduct searches within the investigation context, exploring relevant data and identifying additional findings

Automation: Automate investigation response with actions and playbooks

Intelligence: Integration with threat intelligence feeds, enriching detection rules and observables

Investigation
Overview

- Events
- Included findings
- MITRE ATT&CK map
- Intermediate findings
    - Timeline
    - Threat topology
    - Details
- Drill-down searches & dashboards
- Adaptive responses
- Custom & Additional fields
- MITRE ATT&CK TTPs
- Threat intelligence



ATT&CK tactic threshold exceeded over previous 7 days for system=splunktshrtcompany-1

Overview

ATT&CK tactic threshold exceeded over previous 7 days for system=splunktshrtcompany-1

MITRE ATT&CK map

The highlighted techniques were detected on the entity (in a finding) splunktshrtcompany-1

🟪 Detections 4 | Detections in selected time range 4 | Sub-Techniq... (1) ▾ | Last 30 days ▾

Reconnaissance 0 of 10 Techniques (0%)	Resource Development 0 of 8 Techniques (0%)	Initial Access 1 of 14 Techniques (7%)	Execution 0 of 38 Techniques (0%)	Persistence 0 of 74 Techniques (0%)	Privilege Escalation 0 of 41 Techniques (0%)	Defense Evasion 0 of 91 Techniques (0%)	Credential Access 0 of 30 Techniques (0%)	Discovery 0 of 34 Techniques (0%)	Latera 0 of 20 T
		Exploit Public-Facing Application							

Intermediate findings

Timeline

Entity splunktshrtcompany-1 4130 Intermediate findings count 63

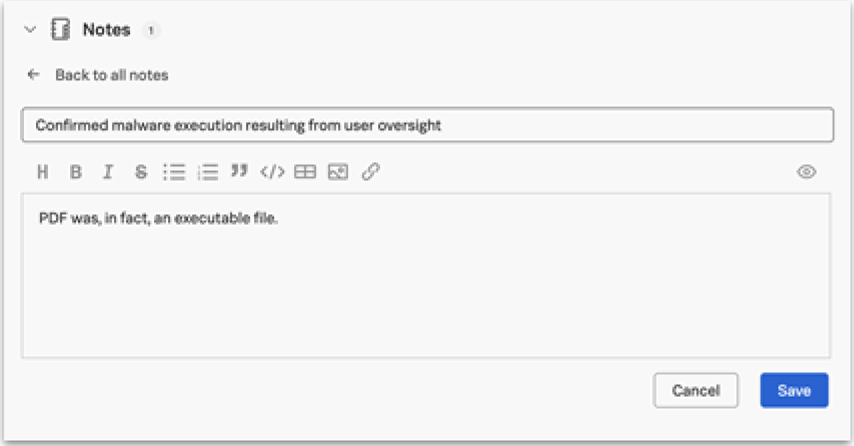
Asset splunktshrtcompany-1 +3 | Priority Critical | DNS splunktshrtcompany-1 | Owner jeremiah wortoski | Business unit ecomm | Category magento +2 | City San Francisco

Timeline
Threat topology
☑ Scroll to zoom
90
80
70
50
An unusual volume of outbound network activity ...
Possible Exploitation of Public-Facing Applicatio...
Command and Control via External Communicati...
Command and Control via External Communicati...
+
−

Notes

Record investigation details or add attachments

- General, Finding and Response notes
- Format text, add code block, table, files/images, and links
- All file types supported
- The maximum file size is 4 MB
- Make files available to Splunk SOAR
  - **SOAR** displays next to the name of files available in Splunk SOAR
- Delete files from ES, SOAR, or both



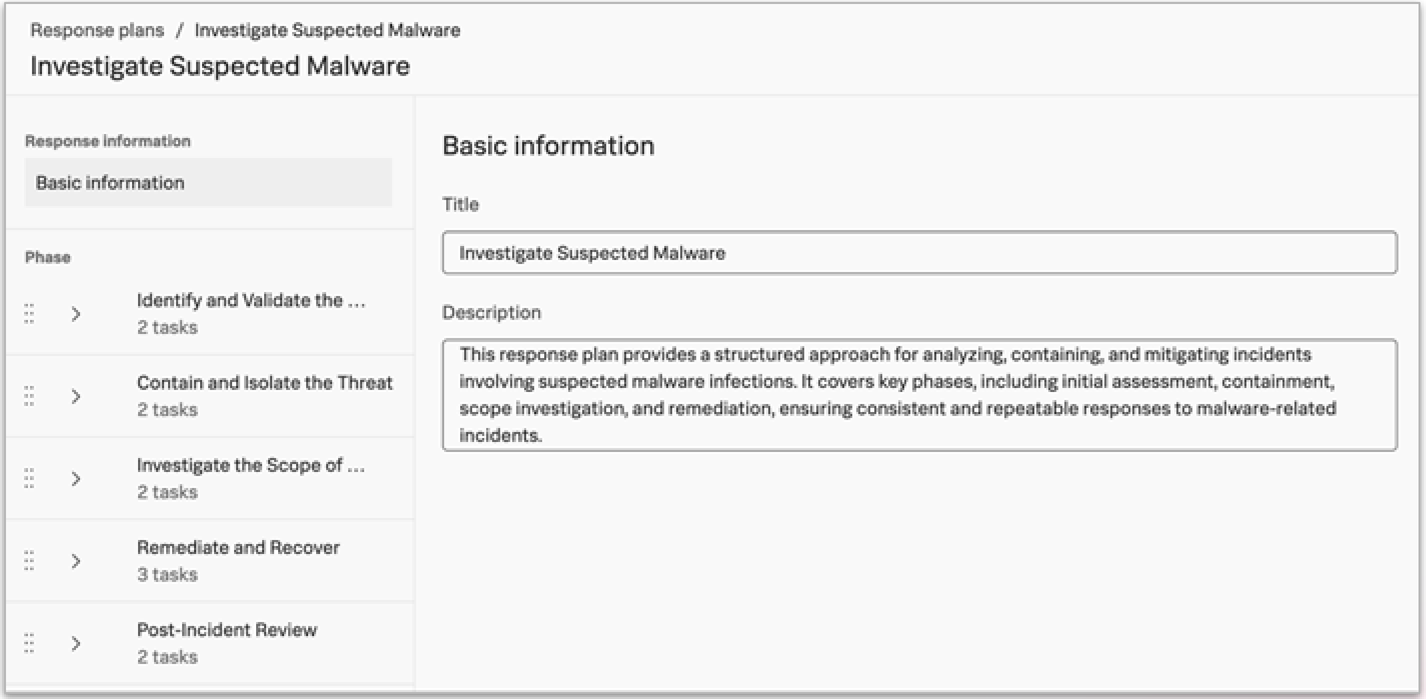
Confirmed malware execution resulting from user oversight

PDF was, in fact, an executable file.

Notes can serve multiple purposes, including post-incident reviews, ensuring compliance, facilitating training, and preserving the chain of custody.

Response Plans

Standardize tasks and phases when investigating findings



Investigate Suspected Malware

- Identify and Validate the ... 2 tasks
- Contain and Isolate the Threat 2 tasks
- Investigate the Scope of ... 2 tasks
- Remediate and Recover 3 tasks
- Post-Incident Review 2 tasks

Basic information

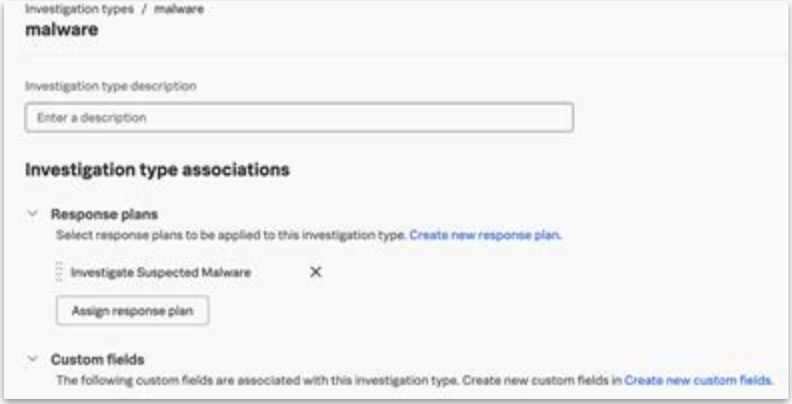
Title: Investigate Suspected Malware

Description: This response plan provides a structured approach for analyzing, containing, and mitigating incidents involving suspected malware infections. It covers key phases, including initial assessment, containment, scope investigation, and remediation, ensuring consistent and repeatable responses to malware-related incidents.

Investigation Type Associations

Standardize tasks and phases when investigating findings

1 Create **Investigation type** to associate investigations with custom fields and response plans



Investigation types / malware

malware

Investigation type description

Enter a description

Investigation type associations

Response plans

Select response plans to be applied to this investigation type. Create new response plan.

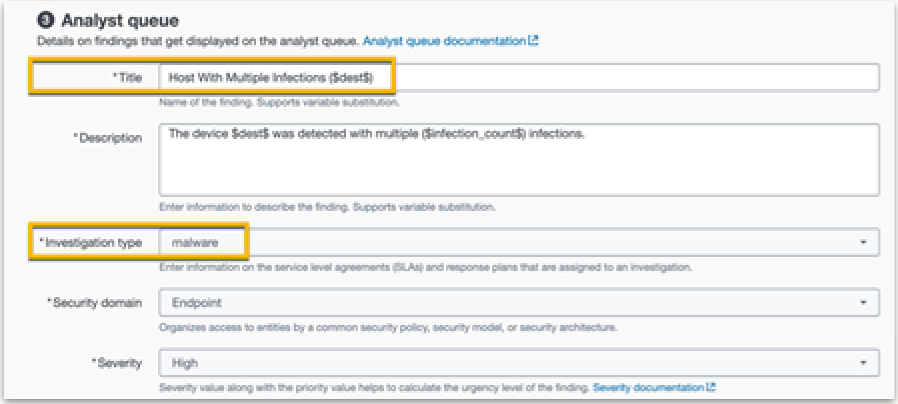
Investigate Suspected Malware ✕

Assign response plan

Custom fields

The following custom fields are associated with this investigation type. Create new custom fields in Create new custom fields.

2 Associate Investigation type with detection



Analyst queue

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

*Title: Host With Multiple Infections ($dest$)

Name of the finding. Supports variable substitution.

*Description: The device $dest$ was detected with multiple ($infection_count$) infections.

Enter information to describe the finding. Supports variable substitution.

*Investigation type: malware

Enter information on the service level agreements (SLAs) and response plans that are assigned to an investigation.

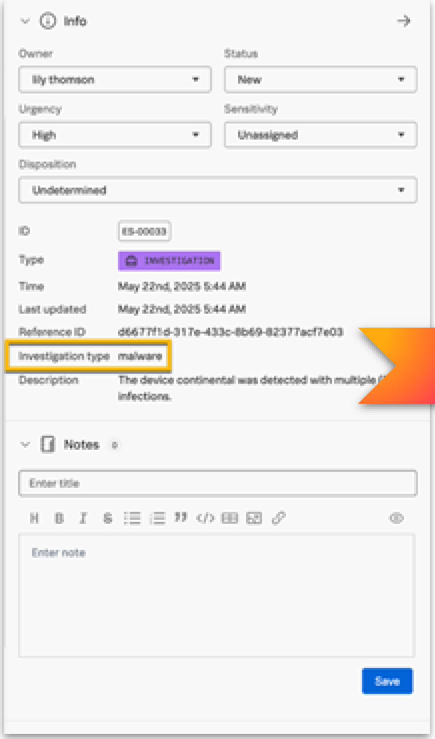
*Security domain: Endpoint

Organizes access to entities by a common security policy, security model, or security architecture.

*Severity: High

Severity value along with the priority value helps to calculate the urgency level of the finding. Severity documentation

Associated Investigation Type with Response Plan



Owner: lily thomson

Status: New

Urgency: High

Sensitivity: Unassigned

Disposition: Undetermined

ID: ES-00033

Type: INVESTIGATION

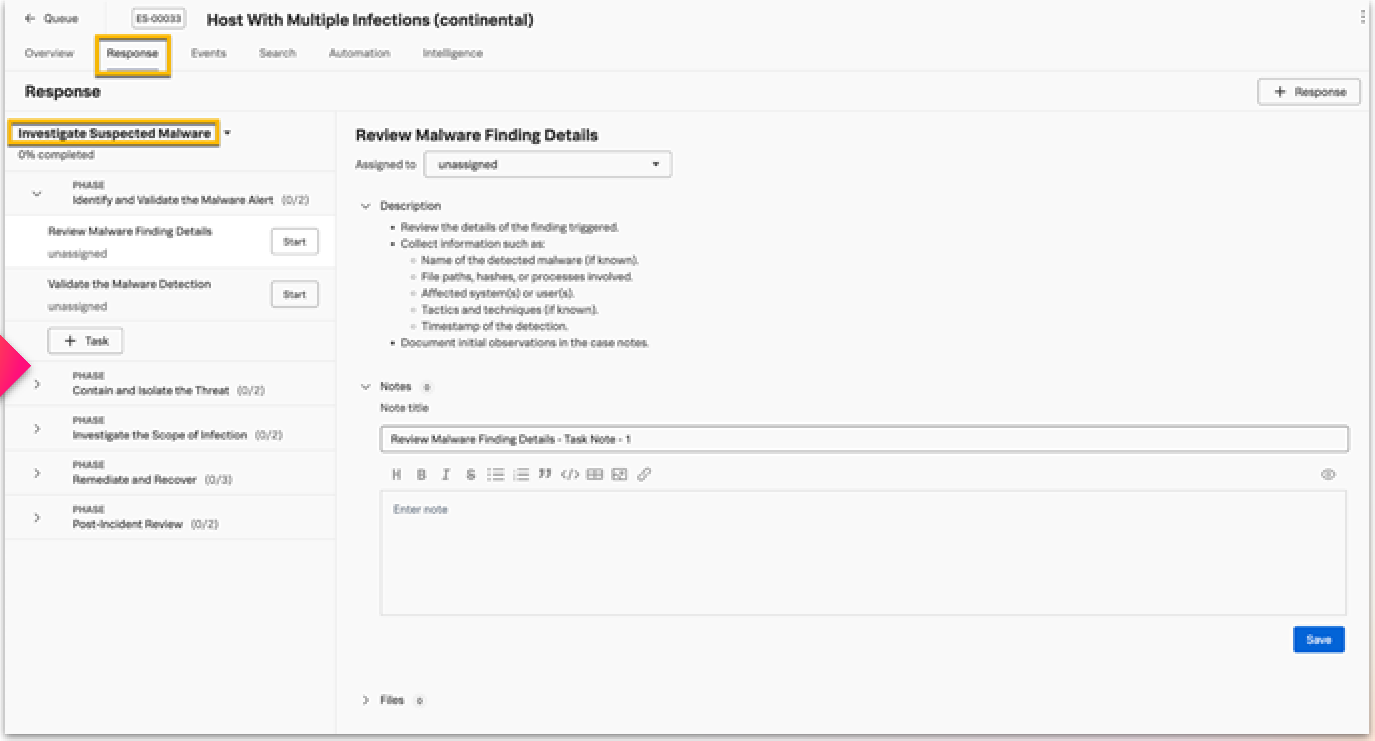
Time: May 22nd, 2025 5:44 AM

Last updated: May 22nd, 2025 5:44 AM

Reference ID: d6677f1d-317e-433c-8b69-82377acf7e03

Investigation type: malware

Description: The device continental was detected with multiple infections.



Host With Multiple Infections (continental)

Response

Investigate Suspected Malware

0% completed

- PHASE: Identify and Validate the Malware Alert (0/2)
  - Review Malware Finding Details, unassigned, Start
  - Validate the Malware Detection, unassigned, Start
  - + Task
- PHASE: Contain and Isolate the Threat (0/2)
- PHASE: Investigate the Scope of Infection (0/2)
- PHASE: Remediate and Recover (0/3)
- PHASE: Post-Incident Review (0/2)

Review Malware Finding Details

Assigned to: unassigned

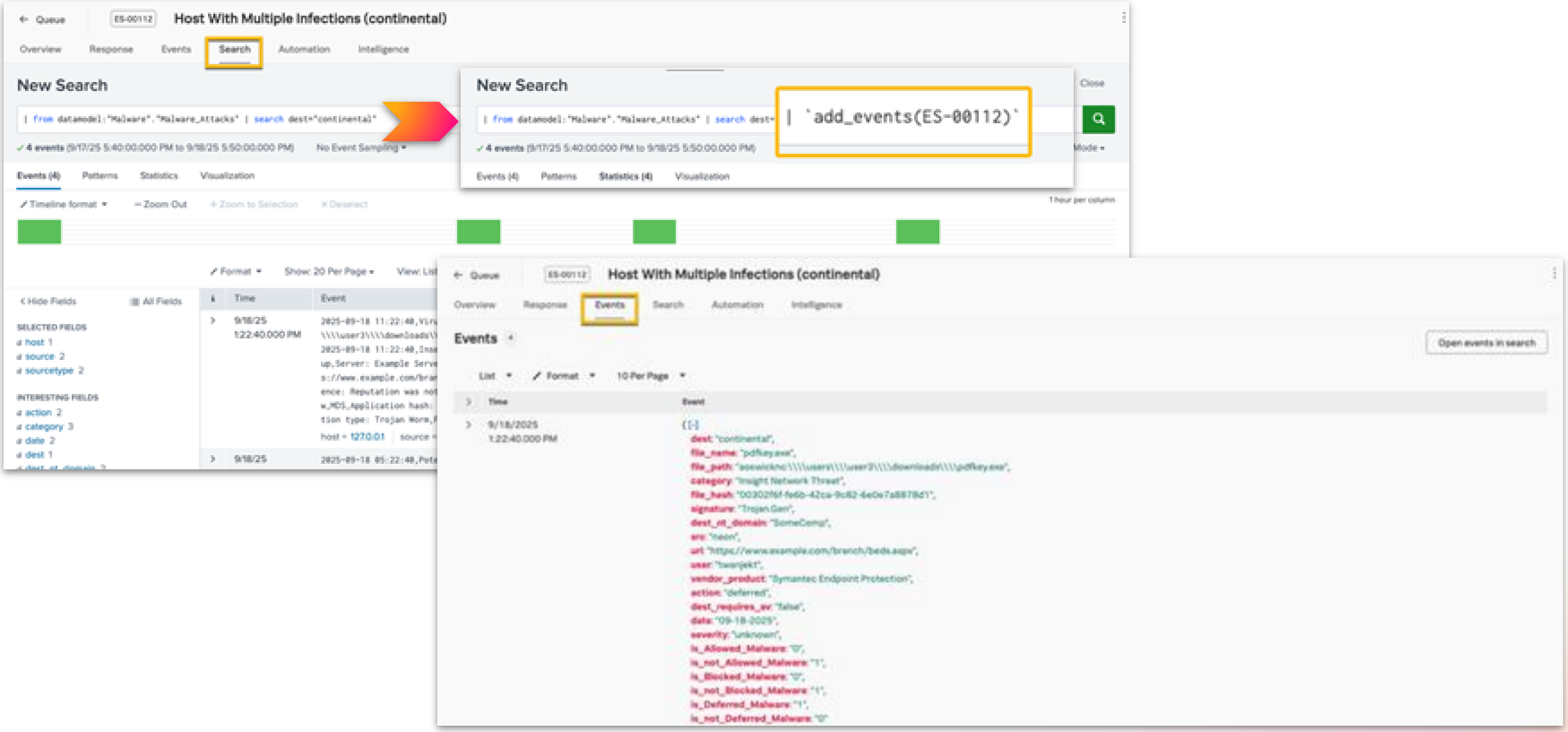
Description

- Review the details of the finding triggered.
- Collect information such as:
  - Name of the detected malware (if known).
  - File paths, hashes, or processes involved.
  - Affected system(s) or user(s).
  - Tactics and techniques (if known).
  - Timestamp of the detection.
- Document initial observations in the case notes.

Notes 0

Note title: Review Malware Finding Details - Task Note - 1

Associate Related Event(s) via Search to the Investigation



New Search

```
| from datamodel:"Malware"."Malware_Attacks" | search dest="continental"
```

✓ 4 events (9/17/25 5:40:00.000 PM to 9/18/25 5:50:00.000 PM)   No Event Sampling ▾

New Search

```
| from datamodel:"Malware"."Malware_Attacks" | search dest="continental" | `add_events(ES-00112)`
```

✓ 4 events (9/17/25 5:40:00.000 PM to 9/18/25 5:50:00.000 PM)

SELECTED FIELDS
- a host 1
- a source 2
- a sourcetype 2

INTERESTING FIELDS
- a action 2
- a category 3
- a date 2
- a dest 1
- a dest_nt_domain 2

Time	Event
9/18/25 1:22:40.000 PM	2025-09-18 11:22:40,Vir \\\\user3\\\\downloads\\ 2025-09-18 11:22:40,Inse up,Server: Example Serve s://www.example.com/bran ence: Reputation was not w_MD5,Application hash: tion type: Trojan Horse,F host = 127.0.0.1 source =
9/18/25	2025-09-18 05:22:40,Pote

Events

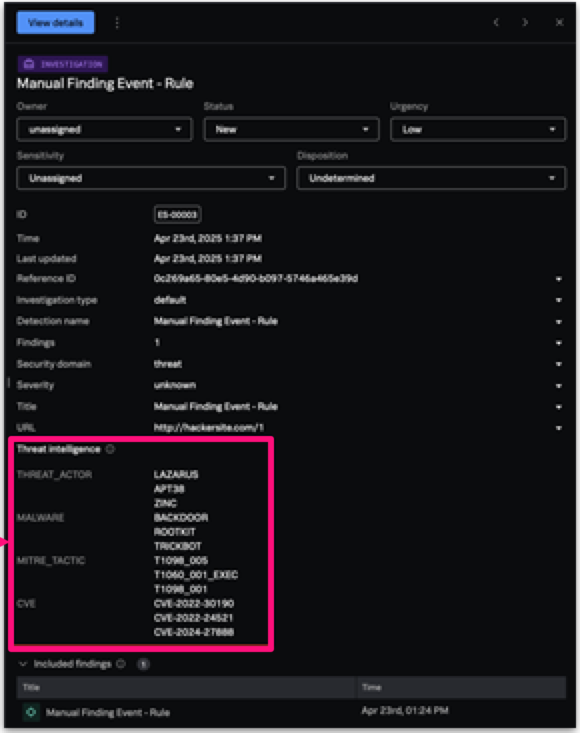
Time	Event
9/18/2025 1:22:40.000 PM	{ [-]

```
{ [-]
   dest: "continental",
   file_name: "pdfkey.exe",
   file_path: "scewickno\\\\users\\\\user3\\\\downloads\\\\pdfkey.exe",
   category: "Insight Network Threat",
   file_hash: "00302f6f-fe6b-42ca-9c82-6e0e7a8878d1",
   signature: "Trojan.Gen",
   dest_nt_domain: "SomeComp",
   src: "neon",
   url: "https://www.example.com/branch/beds.aspx",
   user: "twanjekt",
   vendor_product: "Symantec Endpoint Protection",
   action: "deferred",
   dest_requires_av: "false",
   date: "09-18-2025",
   severity: "unknown",
   is_Allowed_Malware: "0",
   is_not_Allowed_Malware: "1",
   is_Blocked_Malware: "0",
   is_not_Blocked_Malware: "1",
   is_Deferred_Malware: "1",
   is_not_Deferred_Malware: "0"
```

Threat Intelligence Management

***Splunk Cloud (commercial) on AWS only, where available*

Threat Intelligence Summary



Manual Finding Event - Rule

Owner: unassigned
Status: New
Urgency: Low
Sensitivity: Unassigned
Disposition: Undetermined

ID	ES-00003
Time	Apr 23rd, 2025 1:37 PM
Last updated	Apr 23rd, 2025 1:37 PM
Reference ID	0c269a65-80e5-4d90-b097-5746a465e39d
Investigation type	default
Detection name	Manual Finding Event - Rule
Findings	1
Security domain	threat
Severity	unknown
Title	Manual Finding Event - Rule
URL	http://hackersite.com/1

Threat intelligence

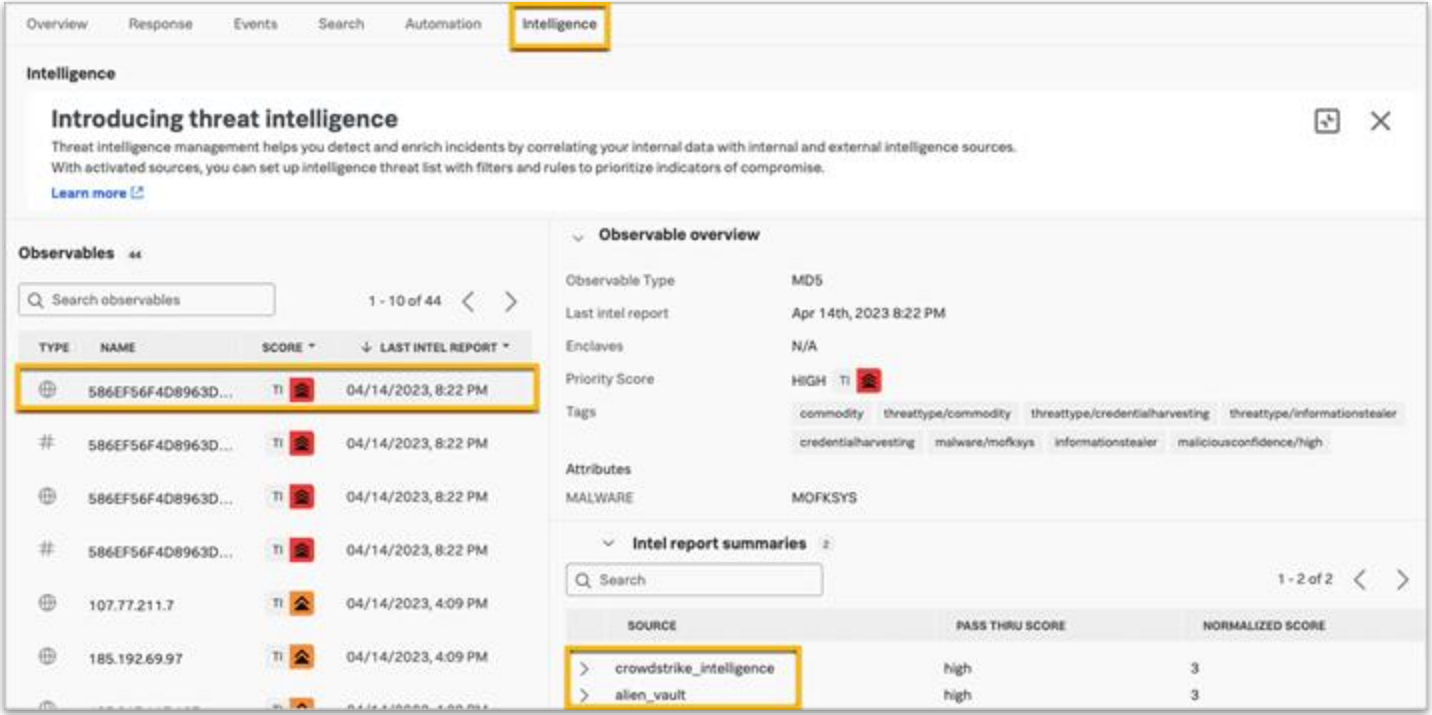
THREAT_ACTOR	LAZARUS APT38 ZINC
MALWARE	BACKDOOR ROOTKIT TRICKBOT
MITRE_TACTIC	T1098_005 T1060_001_EXEC T1098_001
CVE	CVE-2022-30190 CVE-2022-24521 CVE-2024-27888

Included findings 1

Title	Time
Manual Finding Event - Rule	Apr 23rd, 01:24 PM

Contains information regarding threat **actors, malware, MITRE ATT&CK** Tactics, and **CVEs** related to this Finding / Investigation.

Intelligence Tab



Intelligence

Introducing threat intelligence

Threat intelligence management helps you detect and enrich incidents by correlating your internal data with internal and external intelligence sources. With activated sources, you can set up intelligence threat list with filters and rules to prioritize indicators of compromise.

Learn more

Observables 44

TYPE	NAME	SCORE	LAST INTEL REPORT
⊕	586EF56F4D8963D...	TI	04/14/2023, 8:22 PM
#	586EF56F4D8963D...	TI	04/14/2023, 8:22 PM
⊕	586EF56F4D8963D...	TI	04/14/2023, 8:22 PM
#	586EF56F4D8963D...	TI	04/14/2023, 8:22 PM
⊕	107.77.211.7	TI	04/14/2023, 4:09 PM
⊕	185.192.69.97	TI	04/14/2023, 4:09 PM

Observable overview

Observable Type	MD5
Last intel report	Apr 14th, 2023 8:22 PM
Enclaves	N/A
Priority Score	HIGH TI
Tags	commodity threattype/commodity threattype/credentialharvesting threattype/informationstealer credentialharvesting malware/mofksys informationstealer maliciousconfidence/high

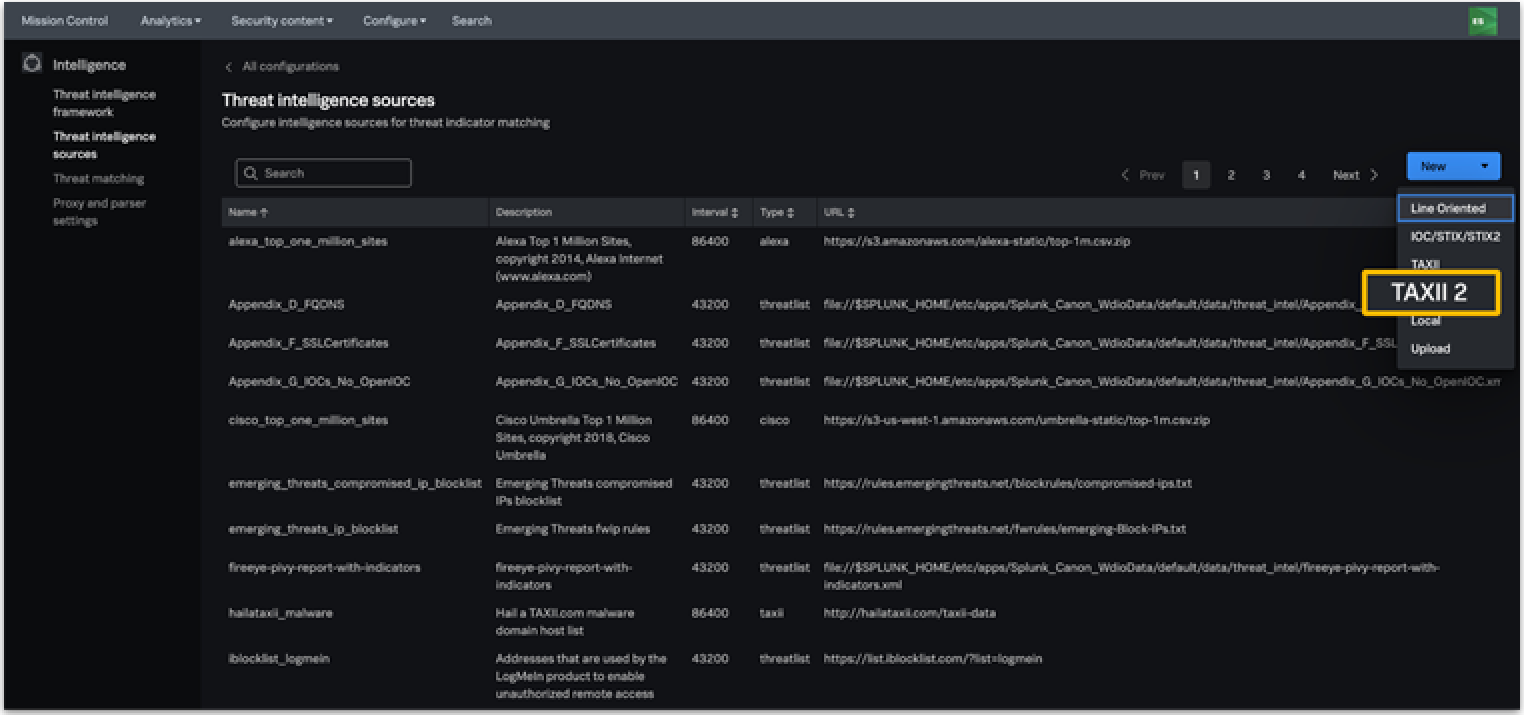
Attributes

MALWARE	MOFKSYS

Intel report summaries 2

SOURCE	PASS THRU SCORE	NORMALIZED SCORE
crowdstrike_intelligence	high	3
alien_vault	high	3

TAXII 2 Client in Threat Intel Framework (TIF)



Threat intelligence sources

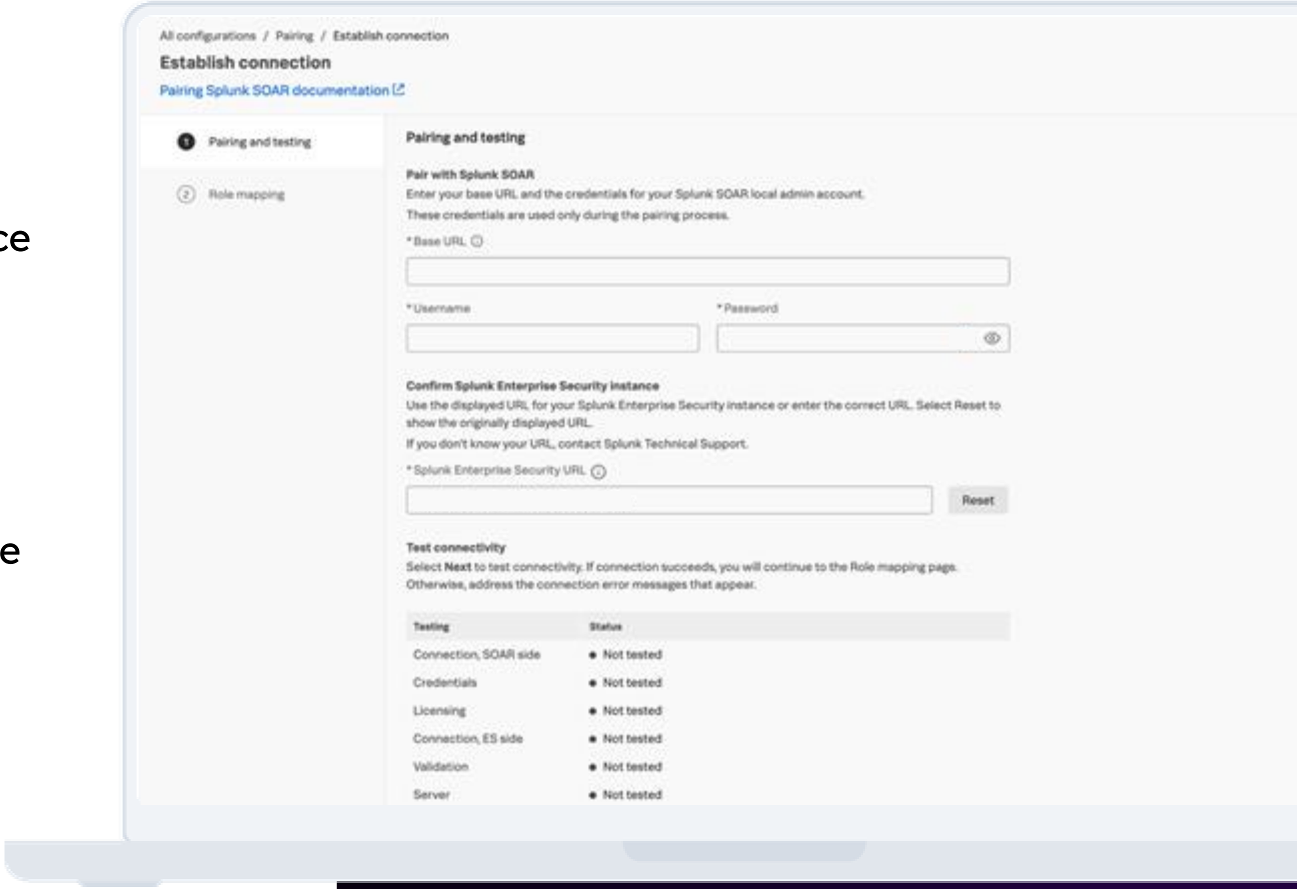
Configure intelligence sources for threat indicator matching

Name ↑	Description	Interval ⇕	Type ⇕	URL ⇕
alexa_top_one_million_sites	Alexa Top 1 Million Sites, copyright 2014, Alexa Internet (www.alexa.com)	86400	alexa	https://s3.amazonaws.com/alexa-static/top-1m.csv.zip
Appendix_D_FQDNS	Appendix_D_FQDNS	43200	threatlist	file://$SPLUNK_HOME/etc/apps/Splunk_Canon_WdioData/default/data/threat_intel/Appendix_
Appendix_F_SSLCertificates	Appendix_F_SSLCertificates	43200	threatlist	file://$SPLUNK_HOME/etc/apps/Splunk_Canon_WdioData/default/data/threat_intel/Appendix_F_SSL
Appendix_G_IOCs_No_OpenIOC	Appendix_G_IOCs_No_OpenIOC	43200	threatlist	file://$SPLUNK_HOME/etc/apps/Splunk_Canon_WdioData/default/data/threat_intel/Appendix_G_IOCs_No_OpenIOC.xm
cisco_top_one_million_sites	Cisco Umbrella Top 1 Million Sites, copyright 2018, Cisco Umbrella	86400	cisco	https://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip
emerging_threats_compromised_ip_blocklist	Emerging Threats compromised IPs blocklist	43200	threatlist	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
emerging_threats_ip_blocklist	Emerging Threats fwip rules	43200	threatlist	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
fireeye-pivy-report-with-indicators	fireeye-pivy-report-with-indicators	43200	threatlist	file://$SPLUNK_HOME/etc/apps/Splunk_Canon_WdioData/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml
hailataxii_malware	Hail a TAXII.com malware domain host list	86400	taxii	http://hailataxii.com/taxii-data
iblocklist_logmein	Addresses that are used by the LogMeIn product to enable unauthorized remote access	43200	threatlist	https://list.iblocklist.com/?list=logmein

Response

Self-Service Pairing

- Rapid pairing experience
- Does not clutter your existing SOAR case management
- Gives you immediate access to the new native SOAR integration in ES



All configurations / Pairing / Establish connection

Establish connection

Pairing Splunk SOAR documentation

Pairing and testing

Pair with Splunk SOAR

Enter your base URL and the credentials for your Splunk SOAR local admin account.

These credentials are used only during the pairing process.

* Base URL

* Username

* Password

Confirm Splunk Enterprise Security instance

Use the displayed URL for your Splunk Enterprise Security instance or enter the correct URL. Select Reset to show the originally displayed URL.

If you don't know your URL, contact Splunk Technical Support.

* Splunk Enterprise Security URL

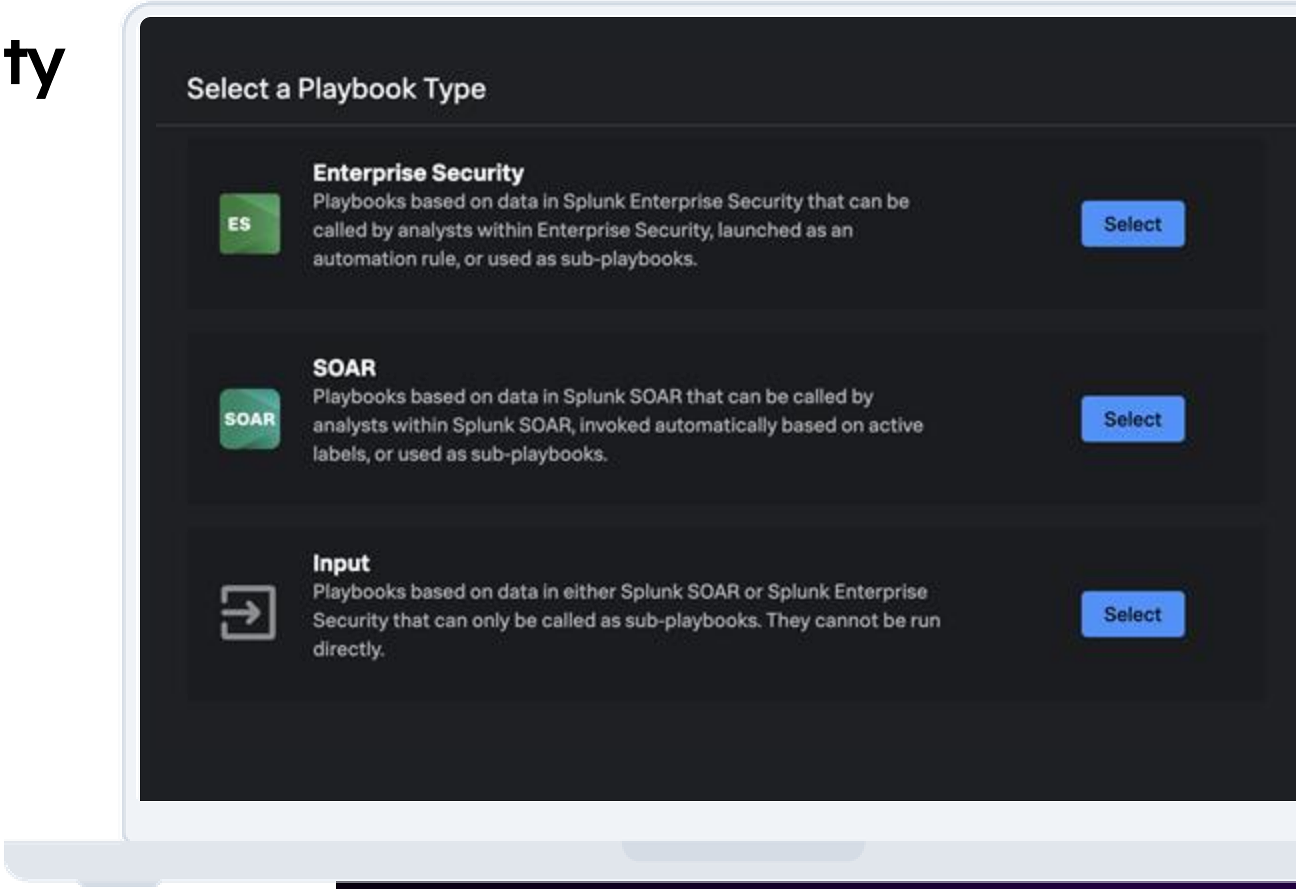
Test connectivity

Select **Next** to test connectivity. If connection succeeds, you will continue to the Role mapping page. Otherwise, address the connection error messages that appear.

Testing	Status
Connection, SOAR side	● Not tested
Credentials	● Not tested
Licensing	● Not tested
Connection, ES side	● Not tested
Validation	● Not tested
Server	● Not tested

Enterprise Security Playbook Type

- New type of playbook for Mission Control investigations
- New data paths
- Debug directly against Mission Control data



Select a Playbook Type

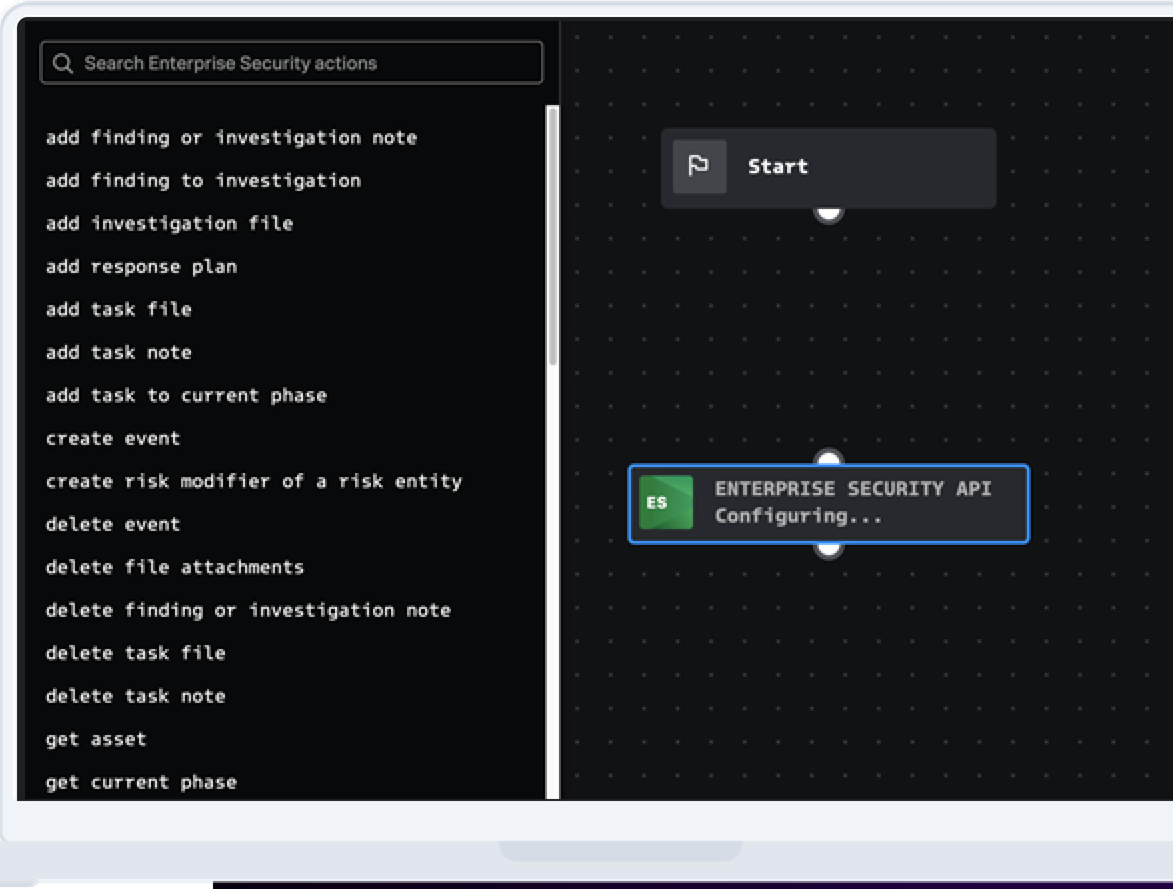
Enterprise Security
Playbooks based on data in Splunk Enterprise Security that can be called by analysts within Enterprise Security, launched as an automation rule, or used as sub-playbooks.

SOAR
Playbooks based on data in Splunk SOAR that can be called by analysts within Splunk SOAR, invoked automatically based on active labels, or used as sub-playbooks.

Input
Playbooks based on data in either Splunk SOAR or Splunk Enterprise Security that can only be called as sub-playbooks. They cannot be run directly.

ES Connector for SOAR

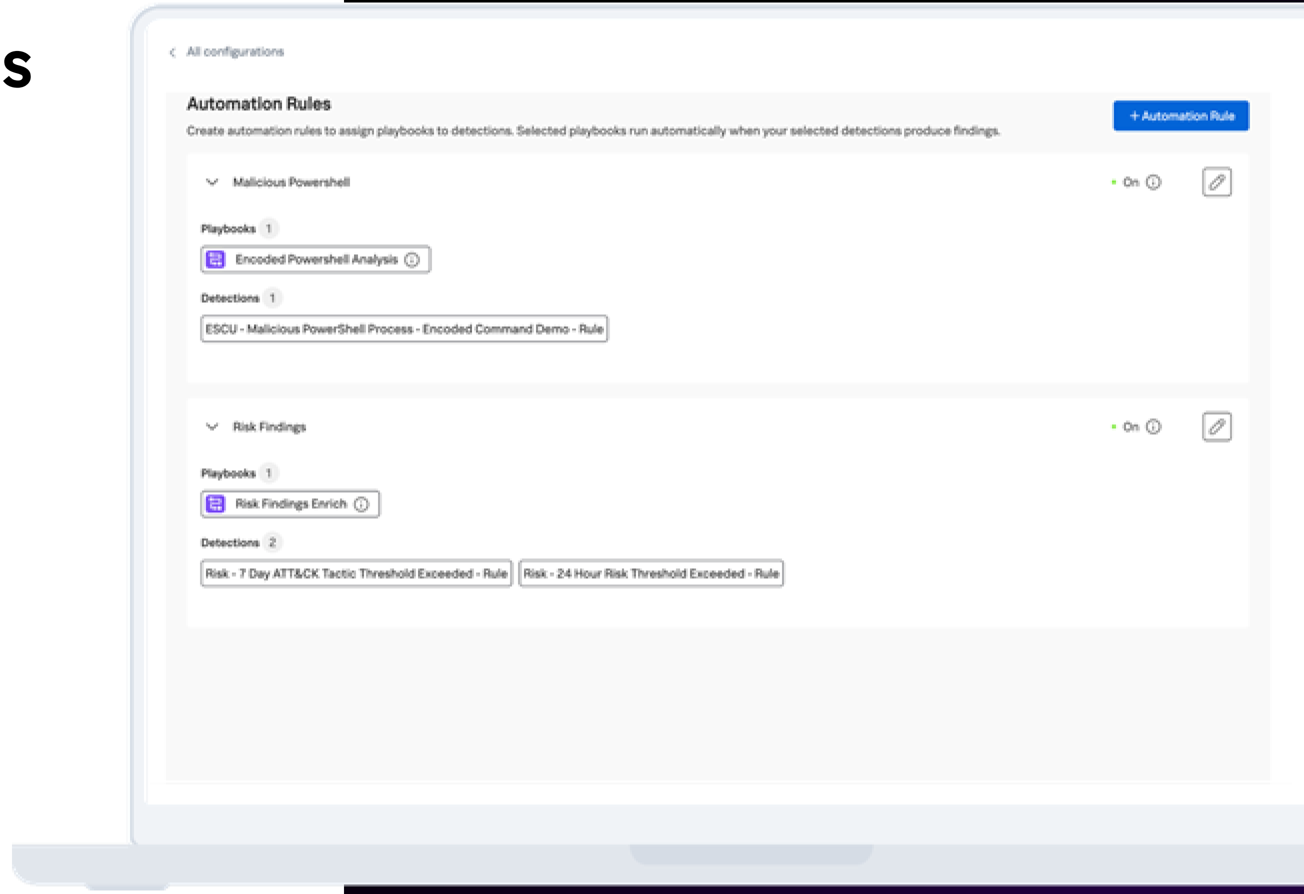
- Special APIs for bi-directional interaction with Splunk SOAR
- Automate anything an analyst can do in the UI
- Augment existing playbooks with ES 8 functionality



add finding or investigation note
add finding to investigation
add investigation file
add response plan
add task file
add task note
add task to current phase
create event
create risk modifier of a risk entity
delete event
delete file attachments
delete finding or investigation note
delete task file
delete task note
get asset
get current phase

Automation Rules Framework

- Easily trigger Playbooks based on ES Detections
- Better visibility and control over what playbooks are being triggered automatically
- Supports both generic enrichment and hyper-specific automation use cases



Automation Rules

Create automation rules to assign playbooks to detections. Selected playbooks run automatically when your selected detections produce findings.

Malicious Powershell — On

Playbooks 1

Encoded Powershell Analysis

Detections 1

ESCU - Malicious PowerShell Process - Encoded Command Demo - Rule

Risk Findings — On

Playbooks 1

Risk Findings Enrich

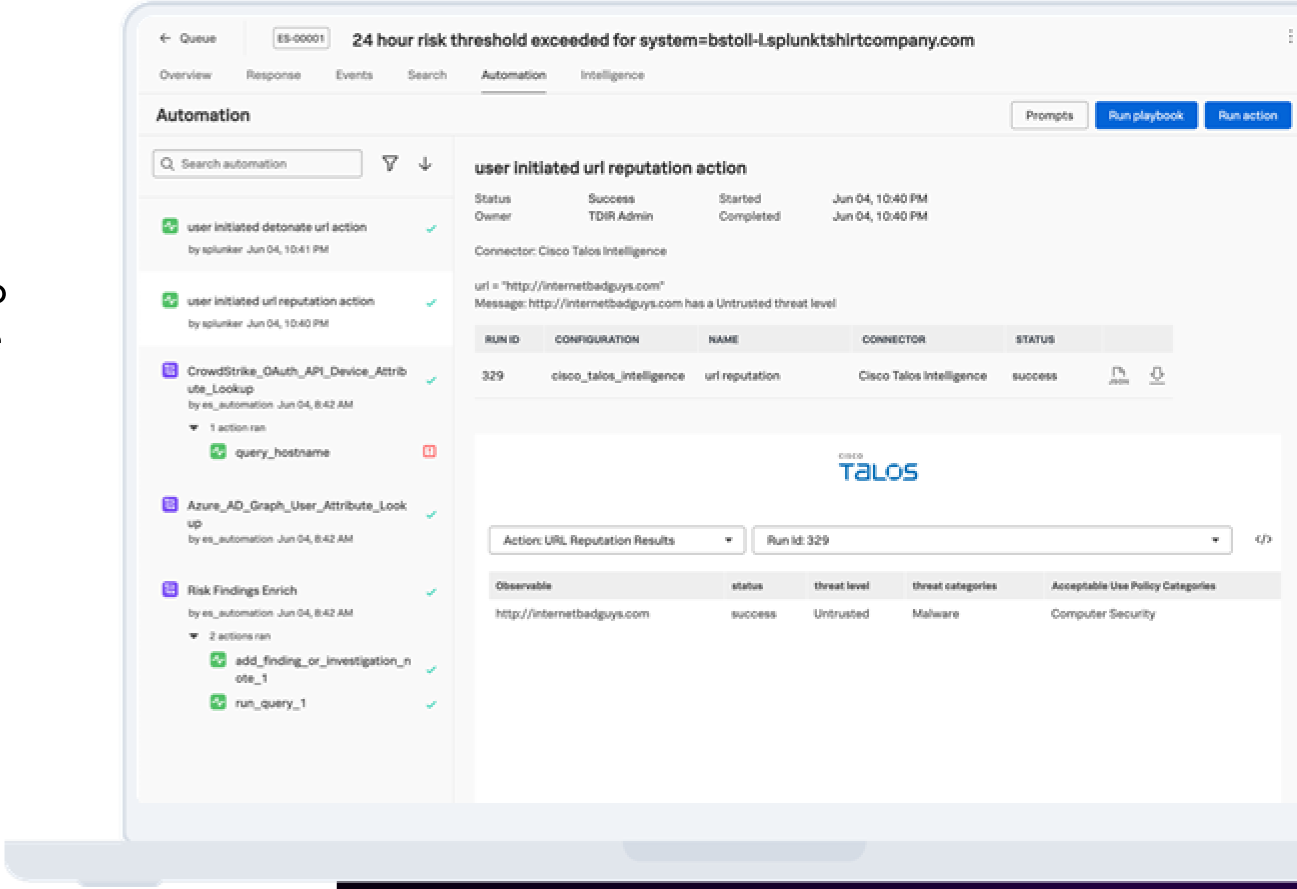
Detections 2

Risk - 7 Day ATT&CK Tactic Threshold Exceeded - Rule

Risk - 24 Hour Risk Threshold Exceeded - Rule

Automation History

- Run actions and/or playbooks and respond to prompts within Enterprise Security
- Review history and detailed results of automation regardless of how it was run
- Open playbooks in one click to paired SOAR instance



24 hour risk threshold exceeded for system=bstoll-l.splunktshirtcompany.com

Automation

user initiated detonate url action ✓
by splunker Jun 04, 10:41 PM

user initiated url reputation action ✓
by splunker Jun 04, 10:40 PM

CrowdStrike_OAuth_API_Device_Attribute_Lookup ✓
by es_automation Jun 04, 8:42 AM
1 action ran
- query_hostname

Azure_AD_Graph_User_Attribute_Lookup ✓
by es_automation Jun 04, 8:42 AM

Risk Findings Enrich ✓
by es_automation Jun 04, 8:42 AM
2 actions ran
- add_finding_or_investigation_note_1 ✓
- run_query_1 ✓

user initiated url reputation action

Status	Success	Started	Jun 04, 10:40 PM
Owner	TDIR Admin	Completed	Jun 04, 10:40 PM

Connector: Cisco Talos Intelligence

url = "http://internetbadguys.com"
Message: http://internetbadguys.com has a Untrusted threat level

RUN ID	CONFIGURATION	NAME	CONNECTOR	STATUS
329	cisco_talos_intelligence	url reputation	Cisco Talos Intelligence	success

Observable	status	threat level	threat categories	Acceptable Use Policy Categories
http://internetbadguys.com	success	Untrusted	Malware	Computer Security

User Entity Behavior Analytics

A Note on UBA (formerly Caspida) versus UEBA Feature in ES Premier

UEBA ≠ UBA

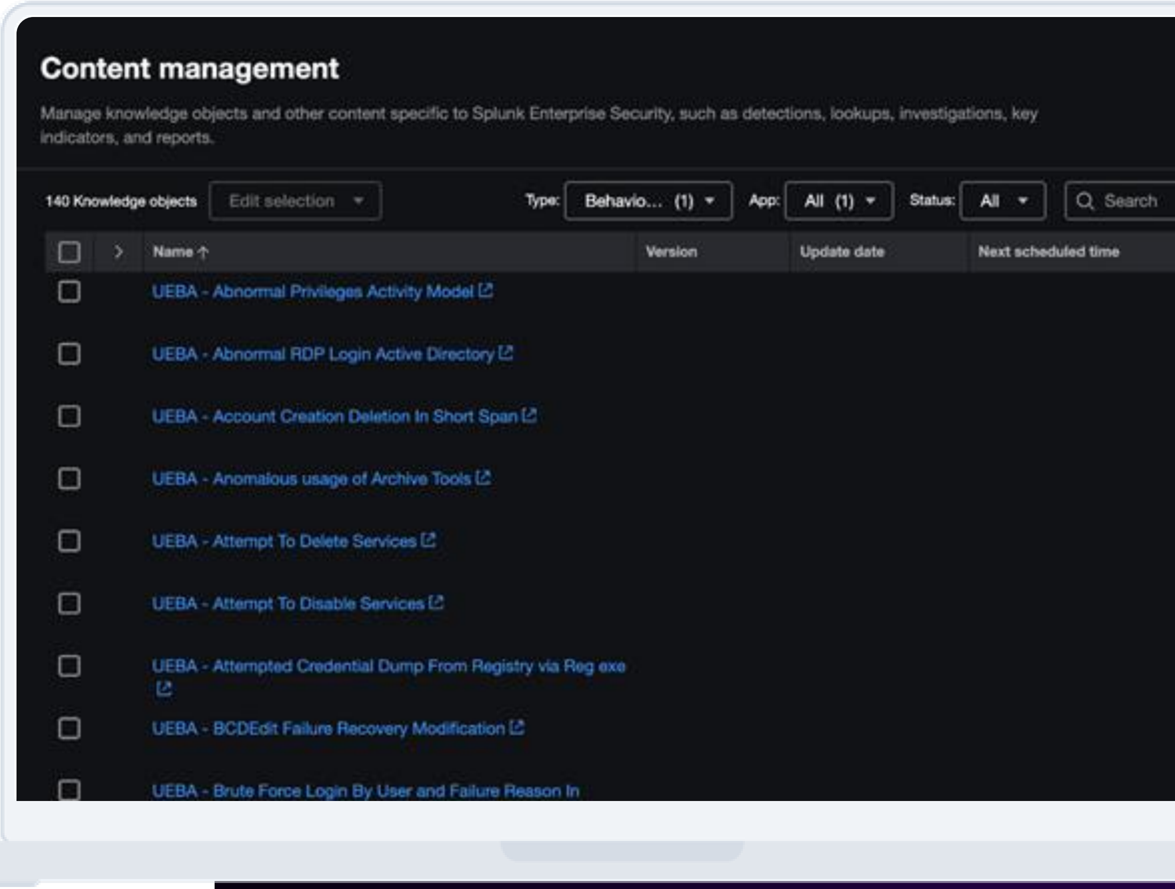
UEBA **is not a standalone product.** It is a new feature/capability that will be launched as part of the **ES Premier only.**

There will be **no capability to migrate configuration or data** from the existing UBA product to the new UEBA feature in Premier.

UEBA capabilities will be delivered to ES Premier **Cloud & CMP.**

UEBA Detection Types

- ML models
  - Example: Rare VPN Login Location
- Anomaly rules
  - Example: Unauthorized Activity Time
- Streaming rules
  - Example: DNS Lookup using Nslookup App



Content management

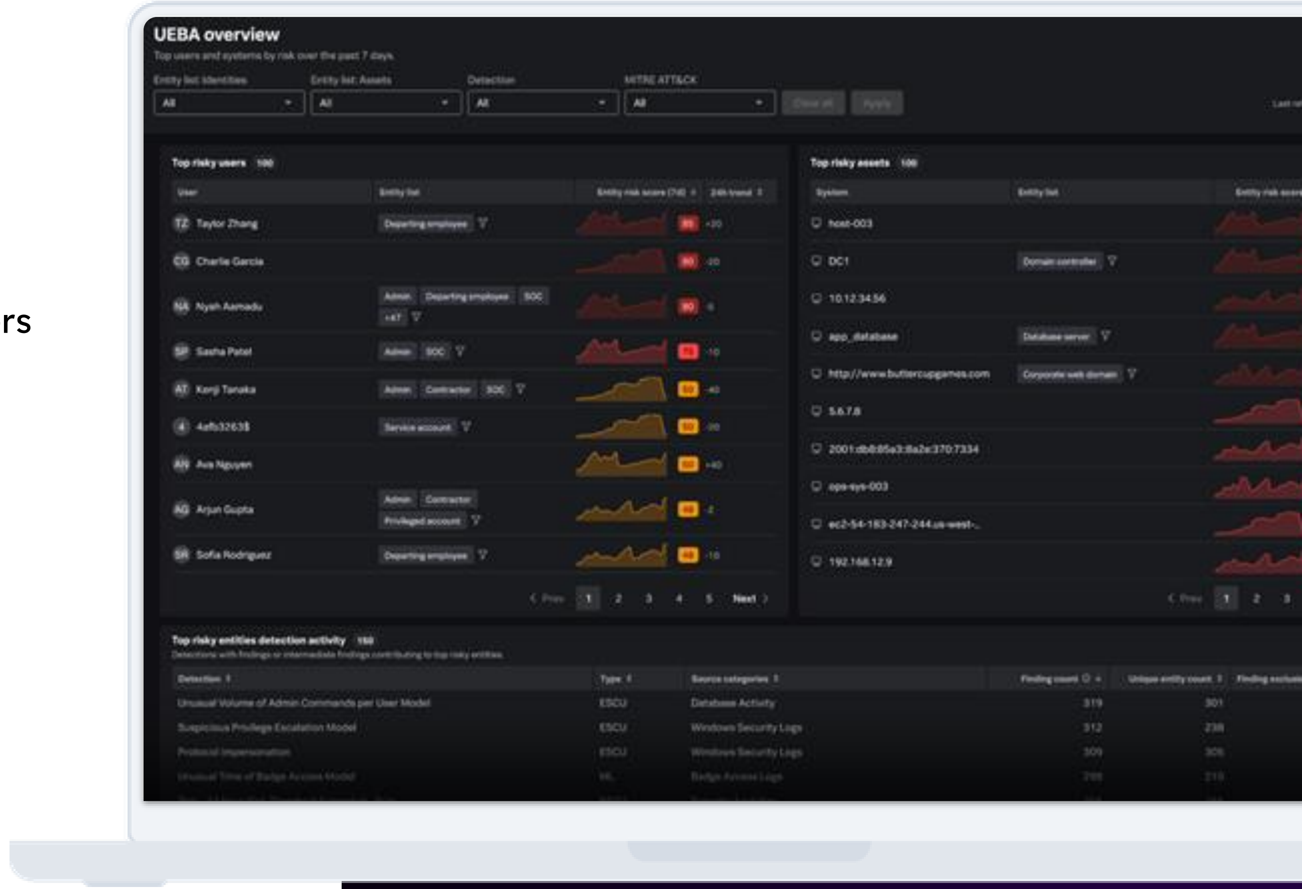
Manage knowledge objects and other content specific to Splunk Enterprise Security, such as detections, lookups, investigations, key indicators, and reports.

140 Knowledge objects | Edit selection | Type: Behavio... (1) | App: All (1) | Status: All | Search

□	Name ↑	Version	Update date	Next scheduled time
□	UEBA - Abnormal Privileges Activity Model			
□	UEBA - Abnormal RDP Login Active Directory			
□	UEBA - Account Creation Deletion In Short Span			
□	UEBA - Anomalous usage of Archive Tools			
□	UEBA - Attempt To Delete Services			
□	UEBA - Attempt To Disable Services			
□	UEBA - Attempted Credential Dump From Registry via Reg exe			
□	UEBA - BCDEdit Failure Recovery Modification			
□	UEBA - Brute Force Login By User and Failure Reason In			

UEBA Overview

- Holistic view of the riskiest users and assets
- Drill down into specific users or assets
- Helps with prioritization based on the ERS



UEBA overview

Top users and systems by risk over the past 7 days.

Entity list: Identities: All | Entity list: Assets: All | Detection: All | MITRE ATT&CK: All | Clear all | Apply

Top risky users 100

User	Entity list	Entity risk score (7d)	24h trend
TZ Taylor Zhang	Departing employee	85	+20
CG Charlie Garcia		80	-20
NA Nyah Aamadu	Admin Departing employee SOC +47	80	0
SP Sasha Patel	Admin SOC	75	-10
AT Kenji Tanaka	Admin Contractor SOC	50	-40
4 4afb3263$	Service account	50	-20
AN Ava Nguyen		50	+40
AG Arjun Gupta	Admin Contractor Privileged account	48	2
SR Sofia Rodriguez	Departing employee	48	-10

‹ Prev 1 2 3 4 5 Next ›

Top risky assets 100

System	Entity list
host-003	
DC1	Domain controller
10.12.34.56	
app_database	Database server
http://www.buttercupgames.com	Corporate web domain
5.6.7.8	
2001:db8:85a3:8a2e:370:7334	
ops-sys-003	
ec2-54-183-247-244.us-west-...	
192.168.12.9	

‹ Prev 1 2 3

Top risky entities detection activity 150

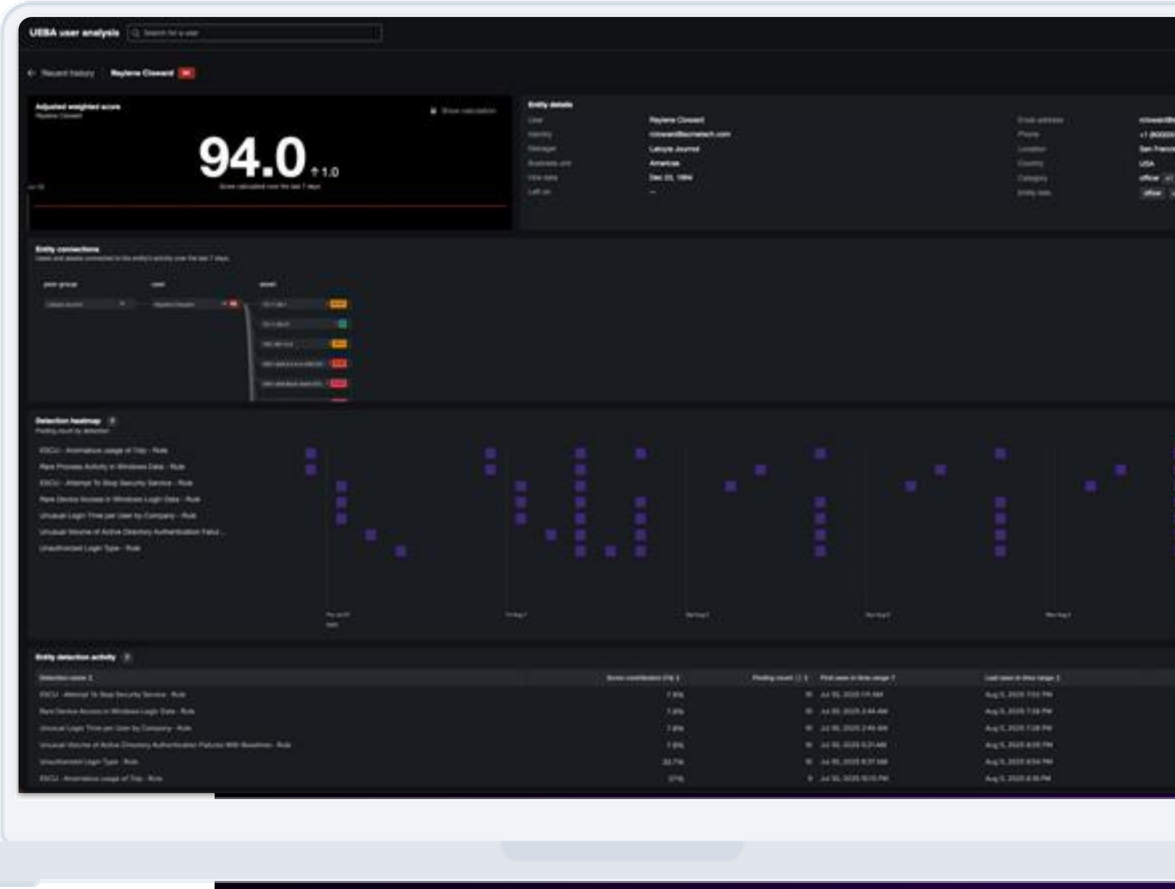
Detections with findings or intermediate findings contributing to top risky entities.

Detection	Type	Source categories	Finding count	Unique entity count
Unusual Volume of Admin Commands per User Model	ESCU	Database Activity	319	301
Suspicious Privilege Escalation Model	ESCU	Windows Security Logs	312	238
Protocol Impersonation	ESCU	Windows Security Logs	309	306
Unusual Time of Badge Access Model	ML	Badge Access Logs	298	215

© 2025 SPLUNK LLC

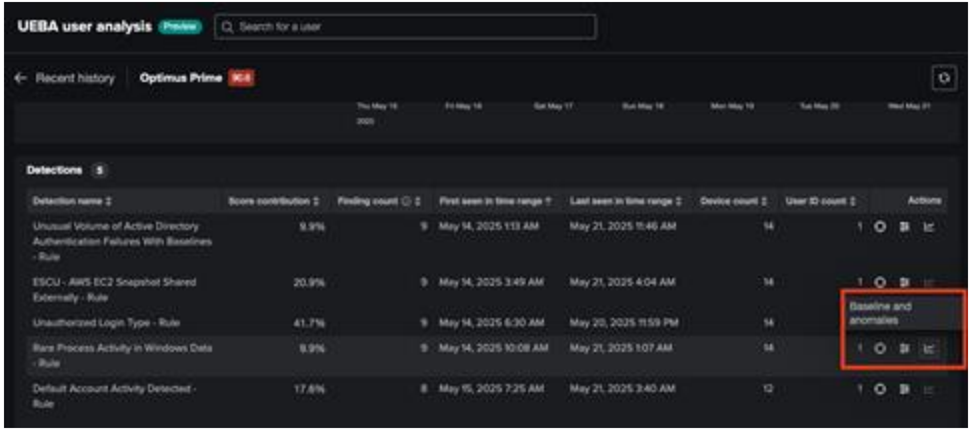
User & Asset Centric Analysis

- Dashboards focused on users or assets, providing a consolidated view of behavior, detections and risk
- Introduces ERS (Entity Risk Scoring) based on behaviors and detections
- Includes user details, related assets, relevant detections, and a MITRE ATT&CK heatmap



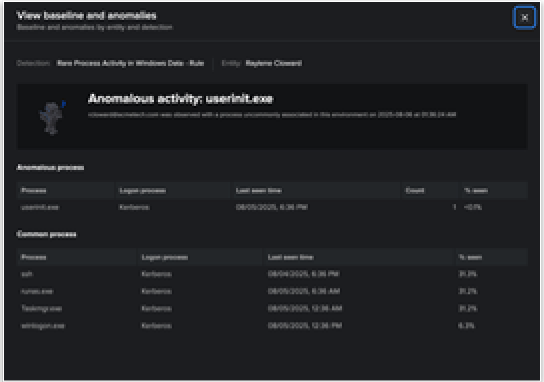
Baselines & Anomalies

- Clear visualization of behavior deviation from baseline to highlight unusual activity
- Drill into each anomaly to understand what triggered it and why UEBA flagged it as an suspicious behavior
- Helps analysts visualize suspicious activity and make informed investigation decisions



Detections 5

Detection name	Score contribution	Finding count	First seen in time range	Last seen in time range	Device count	User ID count	Actions
Unusual Volume of Active Directory Authentication Failures With Baselines - Rule	9.9%	9	May 14, 2025 1:13 AM	May 21, 2025 11:46 AM	14	1	
ESCU - AWS EC2 Snapshot Shared Externally - Rule	20.9%	9	May 14, 2025 3:49 AM	May 21, 2025 4:04 AM	14	1	
Unauthorized Login Type - Rule	41.7%	9	May 14, 2025 6:30 AM	May 20, 2025 11:59 PM	14		
Rare Process Activity in Windows Data - Rule	9.9%	9	May 14, 2025 10:08 AM	May 21, 2025 1:07 AM	14	1	
Default Account Activity Detected - Rule	17.6%	8	May 15, 2025 7:25 AM	May 21, 2025 3:40 AM	12	1	



View baseline and anomalies

Baseline and anomalies by entity and detection

Detection: Rare Process Activity in Windows Data - Rule | Entity: Raylene Clowerd

Anomalous activity: userinit.exe

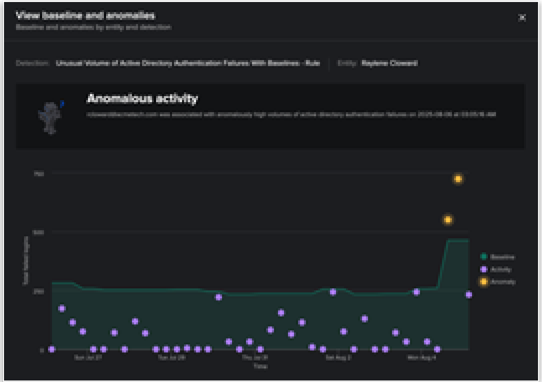
rclowerd@acmetech.com was observed with a process uncommonly associated in this environment on 2025-08-06 at 01:36:24 AM

Anomalous process

Process	Logon process	Last seen time	Count	% seen
userinit.exe	Kerberos	08/05/2025, 6:36 PM	1	<0.1%

Common process

Process	Logon process	Last seen time	% seen
ssh	Kerberos	08/04/2025, 6:36 PM	31.2%
runas.exe	Kerberos	08/05/2025, 6:36 AM	31.2%
Taskmgr.exe	Kerberos	08/05/2025, 12:36 AM	31.2%
winlogon.exe	Kerberos	08/05/2025, 12:36 PM	6.2%



View baseline and anomalies

Baseline and anomalies by entity and detection

Detection: Unusual Volume of Active Directory Authentication Failures With Baselines - Rule | Entity: Raylene Clowerd

Anomalous activity

rclowerd@acmetech.com was associated with anomalously high volumes of active directory authentication failures on 2025-08-06 at 03:05:16 AM

© 2025 SPLUNK LLC

Important Considerations

Before you upgrade....

- Cloud customers should ensure we have the **correct Operational Contact(s)** listed to receive maintenance window notifications.
- On-Prem or BYOL License customers are advised to **make a backup** and also **test the latest version in a development environment** to validate all the changes. Please review the latest release notes for details
- Back up any custom navigation content before you upgrade so that you can restore custom configurations after migration.
- Customers actively using the Investigations features in 7.3 and older are advised to update to 8.3* or higher to access the limited-time legacy feature for closing and archival purposes.
- Some new features might not work for on-prem deployments 8.x and higher, unless you upgrade the `Splunk_TA_ForIndexers` add-on for every release. See Splunk docs.
- Existing SOAR playbooks will need to leverage the new **Enterprise Security block** to have interoperability.
  - Automation Rules (configured within ES) can only be used with playbooks of type “Enterprise Security”, not regular SOAR or input playbooks.

Deprecated or Removed Features & Limitations

Deprecated or Removed Features

https://help.splunk.com/en/splunk-enterprise-security-8/release-notes-and-resources/8.2/splunk-enterprise-security-release-notes/limitations

Feature	Details
Incident Review row expansion	Use the side panel view to review information on findings and investigations.
Enhanced workflows	Replaced by settings available in Analyst queue.
Investigation bar, dashboard, and workbench	Replaced by the Mission Control UI. **NOTE**: MC *incident* data will be migrated to findings, but not *investigation* data. See Migrating Splunk Mission Control incident data to Splunk Enterprise Security 8.0
Sequence templates	Read-only with documentation available for transition to RBA.
Standalone Mission Control app: SLAs, role-based incident type filtering	Not available in ES 8.x.

Deprecated or Removed Features

https://help.splunk.com/en/splunk-enterprise-security-8/release-notes-and-resources/8.2/splunk-enterprise-security-release-notes/limitations

Feature	Details
BRSOAR not supported on ES8	BRSOAR stack (legacy MC standalone app) requires migration to a new ES8 compatible SOAR stack.
Comments	Replaced by capability to add notes to a finding or an investigation.

Limitations

https://help.splunk.com/en/splunk-enterprise-security-8/release-notes-and-resources/8.2/splunk-enterprise-security-release-notes/limitations

Feature	Details
Adaptive Response Actions (ARA) – limitation	Not available for investigations, but can be run on a finding by accessing menu using ⋮ next to Start investigation button
Finding-based detections (FBD)	FBD’s are a **Beta** feature
SOAR (on-prem) multi-tenancy	SOAR (on-prem) and ES pairing does not support multi-tenancy at this time

Known Issues

Open/Known Issues

https://help.splunk.com/en/splunk-enterprise-security-8/release-notes-and-resources/8.2/splunk-enterprise-security-release-notes/known-issues

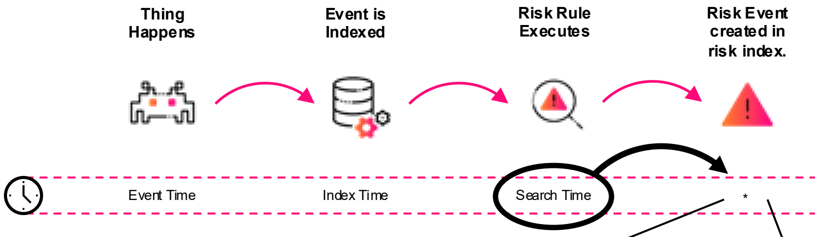
- Diff comparison for detections is not populating information for restricted environment
- Similar Findings type FBD Does not Create All Finding Groups
- URLs linked to ES documentation need to be updated
- Existing detections will run without issue, but may introduce new required fields (e.g., description, risk message) upon first edit of the detection post upgrade

For more information on the known issues, see the latest Release Notes and Resources.

Risk Event _time changes

8.X Introduces material changes to _time assignment for Risk Events.

ES 7.3.x Risk Events



_time: is set to the **search time**.
orig_time: is set to the **_time** value in the **search results** if it exists.

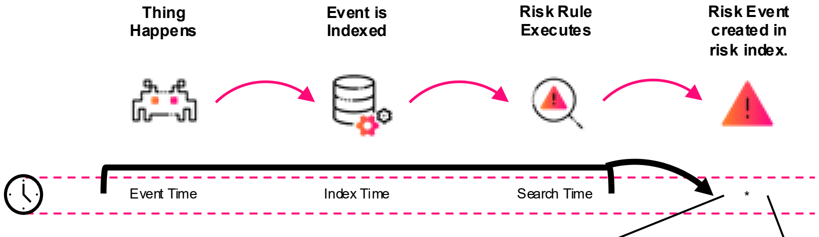
Pros

- **Much more intuitive approach to assigning _time**
- **More accurate risk timeline**

Cons

- **Material change in detection behavior**
- **May impact customer created detections**

ES 8.x Risk Events



_time: is set to the **_time** value in the **search results** if it exists. If there is **no _time** in the **search results**, it is set as the **current time** when the risk event is **written** to the risk index.
orig_time: is set to the _time value in the search results if it exists. If there is no _time in the search results, it is null.

REST API Support

Splunk Enterprise Security API Reference

https://help.splunk.com/en/splunk-enterprise-security-8/api-reference/8.2/splunk-enterprise-security-api-reference

*Supported SPL |rest function

Supported Functions in ES 8.1	New Functions in ES 8.2
Retrieve a list of findings*	Create a finding
Retrieve a list of investigations*	Associate a finding with an investigation
Retrieve a single finding*	Create/Read/Update/Delete a Note / Note Title*
Create an investigation	Respect note title enforcement setting via API
Update an existing investigation	Support pagination and filtering (limit, offset, filter)
Delete an investigation	Role-based authorization on each endpoint
Retrieve a list of risk scores by Entity*	Standardized error handling
Retrieve an asset by ID*	API request/response logging to audit index
Retrieve an identity by ID*	Rate limiting (IP and API key-based)
Add risk modifier to entity	

***NOTE**: API calls will respect the user-configured preference on whether to have a note title. Must be the note creator to update or delete a Note/Note Title.

Thank you!