Splunk Enterprise Security 8: AI Era Defense for Modern SOCs

Marquis Montgomery

Director, Security Products | Splunk

SEC1337

.conf25

splunk>

Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. 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.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. 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 us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about 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. We undertake no 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.

splunk> .conf25

Splunk Enterprise Security 8: AI Era Defense for Modern SOCs

SEC1337

Marquis Montgomery
Director, Security Products | Splunk

.conf25
splunk>

Nice to meet you.

Marquis
Montgomery

Director, Product Management, Security | Splunk

Agenda

The State of Security in the AI Era

How to defend with Enterprise Security 8

AI is reshaping the threat landscape.

90%

of data breaches will include a human element - due to the impact of genAI and the prevalence of communication channels that make social engineering attacks simpler and faster

Forrester

https://www.forrester.com/blogs/predictions-2024-security-and-risk/

#1

AI-Enhanced Malicious Attacks the #1 most commonly cited emerging risk by enterprise risk executives

Gartner

https://www.gartner.com/en/newsroom/press-releases/2024-05-22-gartner-survey-shows-ai-enhanced-malicious-attacks-are-new0

The SOC is overwhelmed.

59%

of Security Operations Centers (SOCs) report being inundated with an unmanageable volume of alerts, leading to analyst fatigue and potential oversight of critical threats.

57%

of Security Operations Centers (SOCs) report having lost valuable investigation time due to data management gaps

49%

of Security Operations Centers (SOCs) say being understaffed and underskilled is the biggest cybersecurity challenge in their organization

Splunk
2025 State of Security Report

The stakes have never been higher.

$25.6M

fraud perpetrated using synthetic media against Arup Engineering, highlighting the sophisticated and costly nature of modern cyber threats.

CNN Business

https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

$4.9M

The global average cost of a data breach reached USD $4.9 million in 2024, marking a 10% increase over the previous year and the highest total ever recorded.

IBM

https://www.ibm.com/reports/data-breach

Do more with less

ES 8 delivers the unified TDIR platform

Better Signal to Noise

- Cut through alert fatigue with Risk-based Alerting
- MITRE-mapped detections from Splunk Threat Research Team
- Native Findings grouping

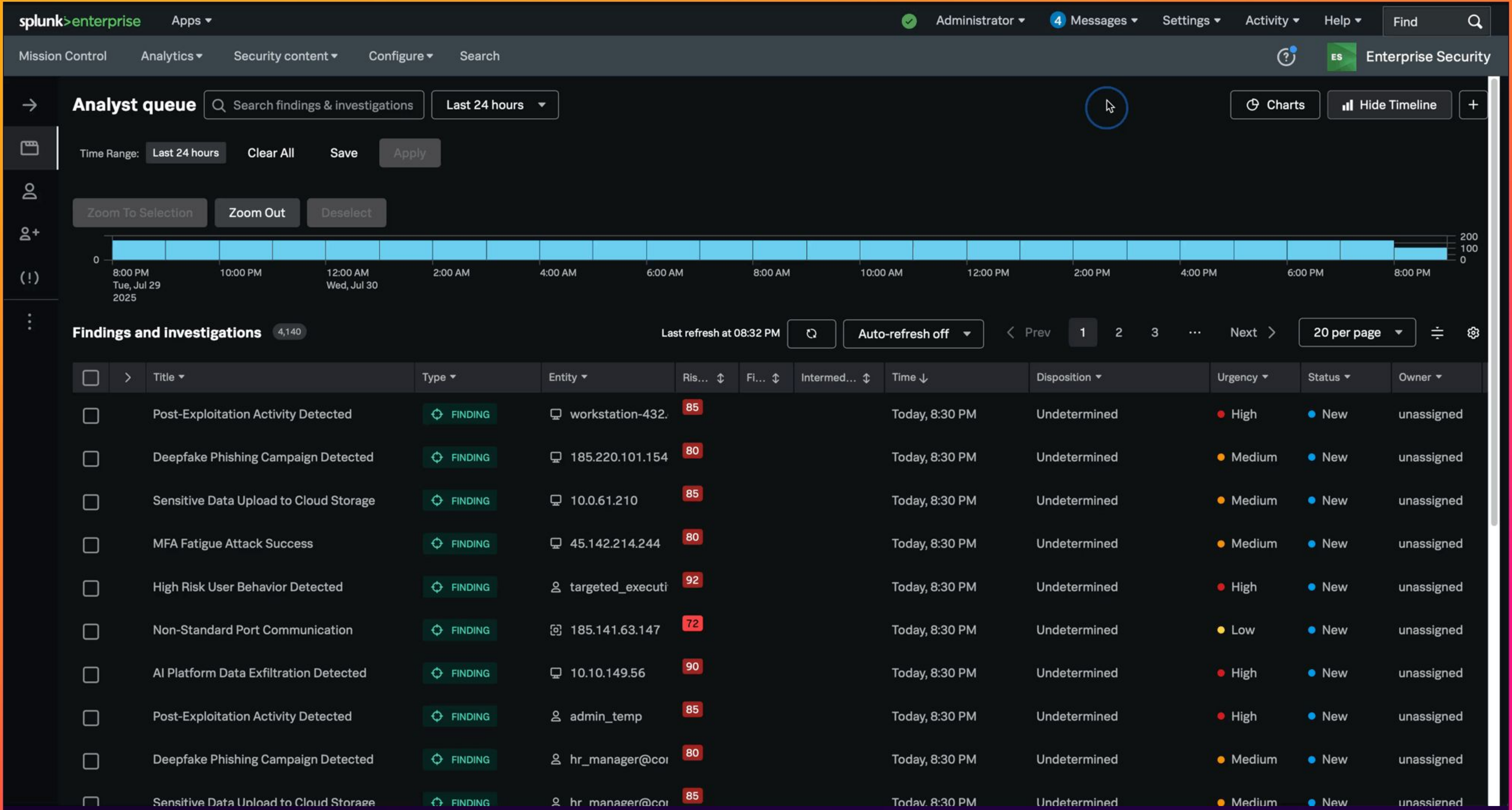
Richer Context

- Real-time threat intelligence alongside alerts “in the moment”
- Tune without breaking production
- AI-powered Finding explanations and Investigation Reports

Faster Decisions

- Built-in Response Plans that streamline investigations and automation
- Unified SOAR for automated enrichment and remediation actions

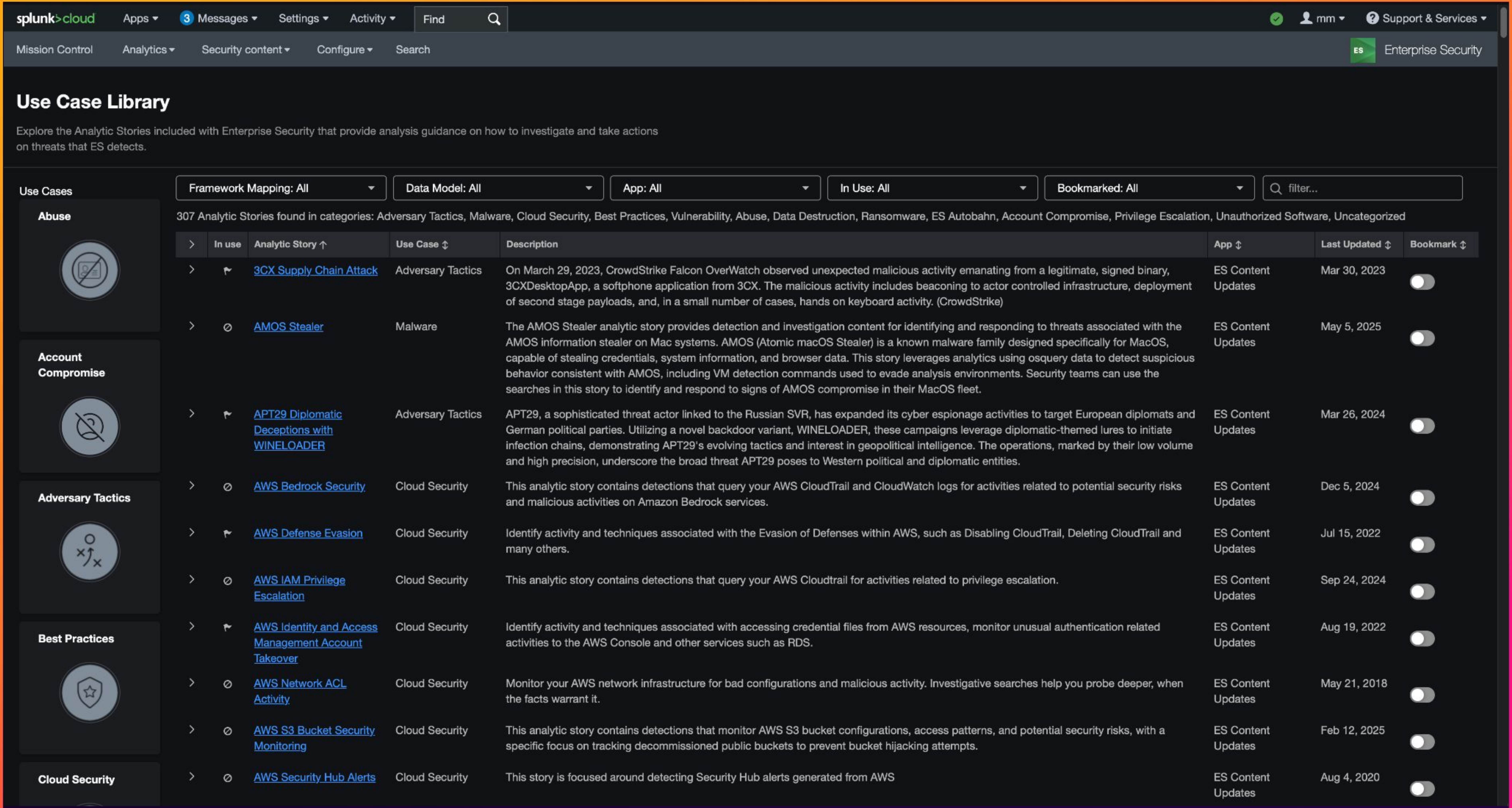
Let’s build the Modern SOC together



□	Title	Type	Entity	Ris...	Fi...	Intermed...	Time	Disposition	Urgency	Status	Owner
□	Post-Exploitation Activity Detected	FINDING	workstation-432.	85			Today, 8:30 PM	Undetermined	High	New	unassigned
□	Deepfake Phishing Campaign Detected	FINDING	185.220.101.154	80			Today, 8:30 PM	Undetermined	Medium	New	unassigned
□	Sensitive Data Upload to Cloud Storage	FINDING	10.0.61.210	85			Today, 8:30 PM	Undetermined	Medium	New	unassigned
□	MFA Fatigue Attack Success	FINDING	45.142.214.244	80			Today, 8:30 PM	Undetermined	Medium	New	unassigned
□	High Risk User Behavior Detected	FINDING	targeted_executi	92			Today, 8:30 PM	Undetermined	High	New	unassigned
□	Non-Standard Port Communication	FINDING	185.141.63.147	72			Today, 8:30 PM	Undetermined	Low	New	unassigned
□	AI Platform Data Exfiltration Detected	FINDING	10.10.149.56	90			Today, 8:30 PM	Undetermined	High	New	unassigned
□	Post-Exploitation Activity Detected	FINDING	admin_temp	85			Today, 8:30 PM	Undetermined	High	New	unassigned
□	Deepfake Phishing Campaign Detected	FINDING	hr_manager@coı	80			Today, 8:30 PM	Undetermined	Medium	New	unassigned
□	Sensitive Data Upload to Cloud Storage	FINDING	hr_manager@coı	85			Today, 8:30 PM	Undetermined	Medium	New	unassigned

Detection Engineering and Content Tuning

The fastest way to defend against modern threats is to start with curated, intelligence-led content — and customize it safely for your environment.



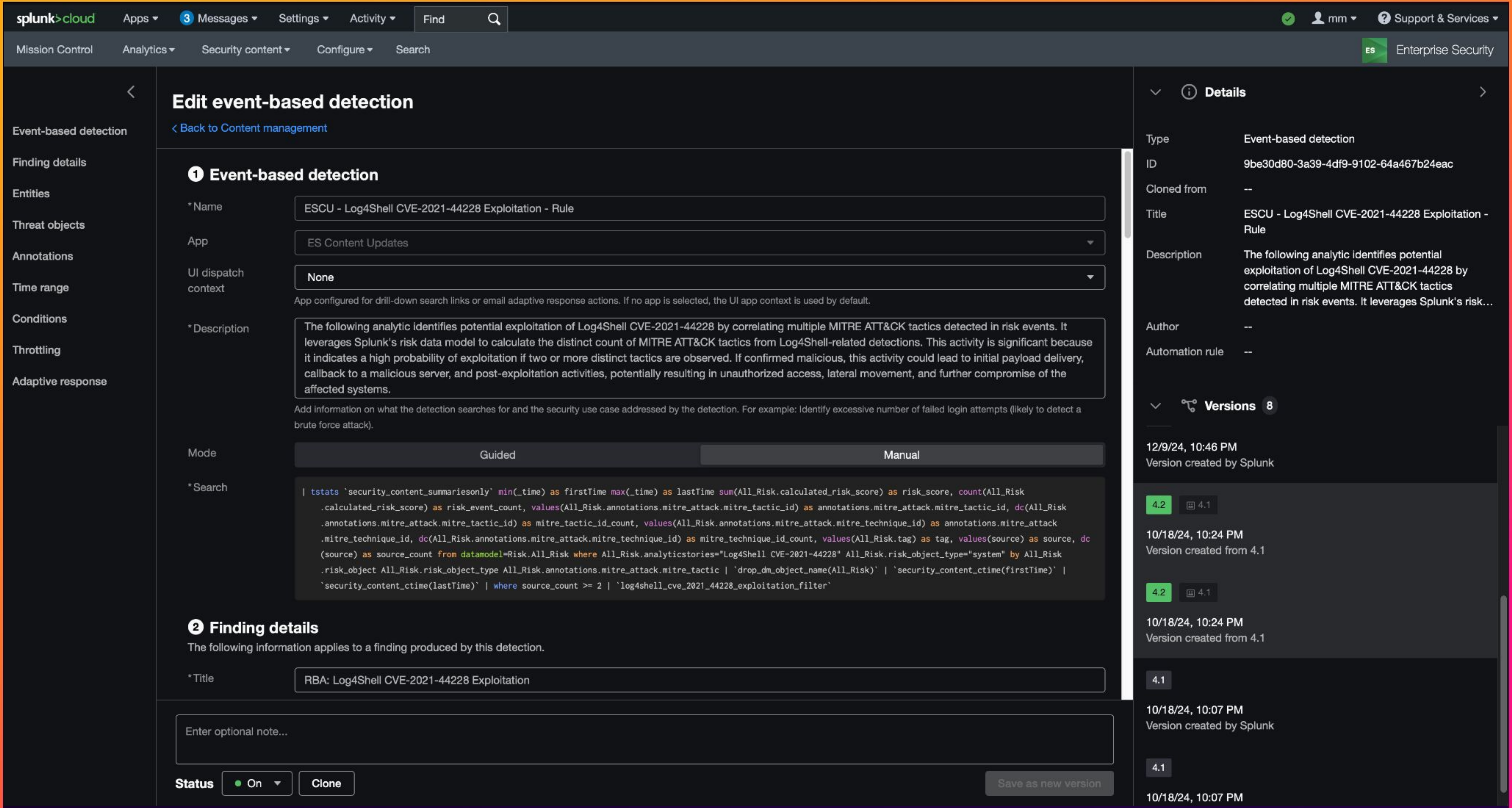
Use Case Library

Explore the Analytic Stories included with Enterprise Security that provide analysis guidance on how to investigate and take actions on threats that ES detects.

Framework Mapping: All | Data Model: All | App: All | In Use: All | Bookmarked: All | filter...

307 Analytic Stories found in categories: Adversary Tactics, Malware, Cloud Security, Best Practices, Vulnerability, Abuse, Data Destruction, Ransomware, ES Autobahn, Account Compromise, Privilege Escalation, Unauthorized Software, Uncategorized

>	In use	Analytic Story ↑	Use Case ↕	Description	App ↕	Last Updated ↕	Bookmark ↕
>	⚑	3CX Supply Chain Attack	Adversary Tactics	On March 29, 2023, CrowdStrike Falcon OverWatch observed unexpected malicious activity emanating from a legitimate, signed binary, 3CXDesktopApp, a softphone application from 3CX. The malicious activity includes beaconing to actor controlled infrastructure, deployment of second stage payloads, and, in a small number of cases, hands on keyboard activity. (CrowdStrike)	ES Content Updates	Mar 30, 2023	○
>	⊘	AMOS Stealer	Malware	The AMOS Stealer analytic story provides detection and investigation content for identifying and responding to threats associated with the AMOS information stealer on Mac systems. AMOS (Atomic macOS Stealer) is a known malware family designed specifically for MacOS, capable of stealing credentials, system information, and browser data. This story leverages analytics using osquery data to detect suspicious behavior consistent with AMOS, including VM detection commands used to evade analysis environments. Security teams can use the searches in this story to identify and respond to signs of AMOS compromise in their MacOS fleet.	ES Content Updates	May 5, 2025	○
>	⚑	APT29 Diplomatic Deceptions with WINELOADER	Adversary Tactics	APT29, a sophisticated threat actor linked to the Russian SVR, has expanded its cyber espionage activities to target European diplomats and German political parties. Utilizing a novel backdoor variant, WINELOADER, these campaigns leverage diplomatic-themed lures to initiate infection chains, demonstrating APT29's evolving tactics and interest in geopolitical intelligence. The operations, marked by their low volume and high precision, underscore the broad threat APT29 poses to Western political and diplomatic entities.	ES Content Updates	Mar 26, 2024	○
>	⊘	AWS Bedrock Security	Cloud Security	This analytic story contains detections that query your AWS CloudTrail and CloudWatch logs for activities related to potential security risks and malicious activities on Amazon Bedrock services.	ES Content Updates	Dec 5, 2024	○
>	⚑	AWS Defense Evasion	Cloud Security	Identify activity and techniques associated with the Evasion of Defenses within AWS, such as Disabling CloudTrail, Deleting CloudTrail and many others.	ES Content Updates	Jul 15, 2022	○
>	⊘	AWS IAM Privilege Escalation	Cloud Security	This analytic story contains detections that query your AWS Cloudtrail for activities related to privilege escalation.	ES Content Updates	Sep 24, 2024	○
>	⚑	AWS Identity and Access Management Account Takeover	Cloud Security	Identify activity and techniques associated with accessing credential files from AWS resources, monitor unusual authentication related activities to the AWS Console and other services such as RDS.	ES Content Updates	Aug 19, 2022	○
>	⊘	AWS Network ACL Activity	Cloud Security	Monitor your AWS network infrastructure for bad configurations and malicious activity. Investigative searches help you probe deeper, when the facts warrant it.	ES Content Updates	May 21, 2018	○
>	⊘	AWS S3 Bucket Security Monitoring	Cloud Security	This analytic story contains detections that monitor AWS S3 bucket configurations, access patterns, and potential security risks, with a specific focus on tracking decommissioned public buckets to prevent bucket hijacking attempts.	ES Content Updates	Feb 12, 2025	○
>	⊘	AWS Security Hub Alerts	Cloud Security	This story is focused around detecting Security Hub alerts generated from AWS	ES Content Updates	Aug 4, 2020	○



Edit event-based detection

< Back to Content management

1 Event-based detection

*Name: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule

App: ES Content Updates

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 default.

*Description: The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228 by correlating multiple MITRE ATT&CK tactics detected in risk events. It leverages Splunk's risk data model to calculate the distinct count of MITRE ATT&CK tactics from Log4Shell-related detections. This activity is significant because it indicates a high probability of exploitation if two or more distinct tactics are observed. If confirmed malicious, this activity could lead to initial payload delivery, callback to a malicious server, and post-exploitation activities, potentially resulting in unauthorized access, lateral movement, and further compromise of the affected systems.

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).

Mode: Guided | Manual

*Search:

```
| tstats `security_content_summariesonly` min(_time) as firstTime max(_time) as lastTime sum(All_Risk.calculated_risk_score) as risk_score, count(All_Risk
    .calculated_risk_score) as risk_event_count, values(All_Risk.annotations.mitre_attack.mitre_tactic_id) as annotations.mitre_attack.mitre_tactic_id, dc(All_Risk
    .annotations.mitre_attack.mitre_tactic_id) as mitre_tactic_id_count, values(All_Risk.annotations.mitre_attack.mitre_technique_id) as annotations.mitre_attack
    .mitre_technique_id, dc(All_Risk.annotations.mitre_attack.mitre_technique_id) as mitre_technique_id_count, values(All_Risk.tag) as tag, values(source) as source, dc
    (source) as source_count from datamodel=Risk.All_Risk where All_Risk.analyticstories="Log4Shell CVE-2021-44228" All_Risk.risk_object_type="system" by All_Risk
    .risk_object All_Risk.risk_object_type All_Risk.annotations.mitre_attack.mitre_tactic | `drop_dm_object_name(All_Risk)` | `security_content_ctime(firstTime)` |
    `security_content_ctime(lastTime)` | where source_count >= 2 | `log4shell_cve_2021_44228_exploitation_filter`
```

2 Finding details

The following information applies to a finding produced by this detection.

*Title: RBA: Log4Shell CVE-2021-44228 Exploitation

Enter optional note...

Status: ● On | Clone | Save as new version

Details

Type	Event-based detection
ID	9be30d80-3a39-4df9-9102-64a467b24eac
Cloned from	--
Title	ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
Description	The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228 by correlating multiple MITRE ATT&CK tactics detected in risk events. It leverages Splunk's risk...
Author	--
Automation rule	--

Versions 8

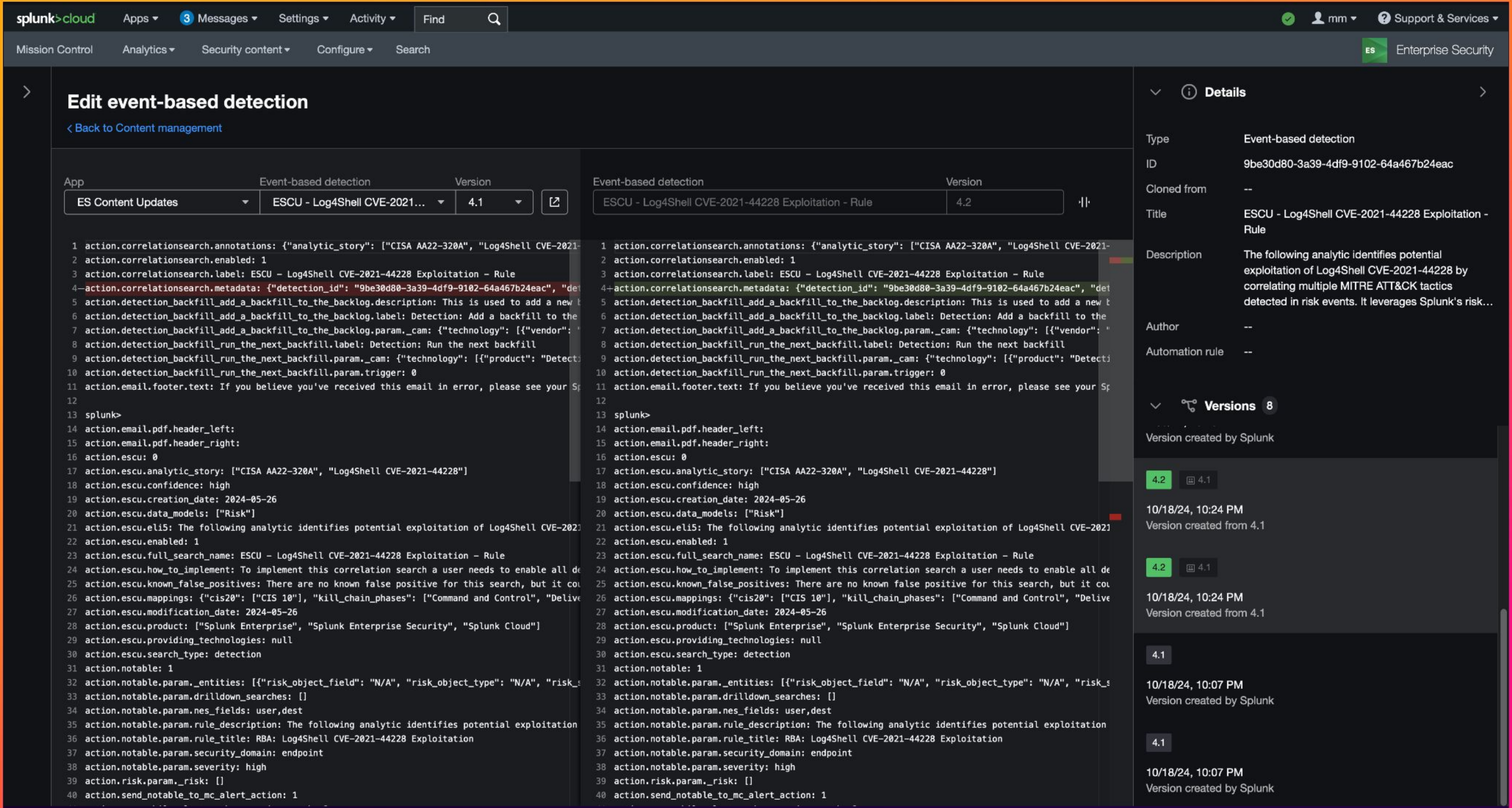
12/9/24, 10:46 PM
Version created by Splunk

4.2 4.1
10/18/24, 10:24 PM
Version created from 4.1

4.2 4.1
10/18/24, 10:24 PM
Version created from 4.1

4.1
10/18/24, 10:07 PM
Version created by Splunk

4.1
10/18/24, 10:07 PM



Edit event-based detection

< Back to Content management

App: ES Content Updates
Event-based detection: ESCU - Log4Shell CVE-2021...
Version: 4.1

Event-based detection: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
Version: 4.2

```
action.correlationsearch.annotations: {"analytic_story": ["CISA AA22-320A", "Log4Shell CVE-2021-
action.correlationsearch.enabled: 1
action.correlationsearch.label: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
-action.correlationsearch.metadata: {"detection_id": "9be30d80-3a39-4df9-9102-64a467b24eac", "de
action.detection_backfill_add_a_backfill_to_the_backlog.description: This is used to add a new
action.detection_backfill_add_a_backfill_to_the_backlog.label: Detection: Add a backfill to the
action.detection_backfill_add_a_backfill_to_the_backlog.param._cam: {"technology": [{"vendor":
action.detection_backfill_run_the_next_backfill.label: Detection: Run the next backfill
action.detection_backfill_run_the_next_backfill.param._cam: {"technology": [{"product": "Detect
action.detection_backfill_run_the_next_backfill.param.trigger: 0
action.email.footer.text: If you believe you've received this email in error, please see your Sp

splunk>
action.email.pdf.header_left:
action.email.pdf.header_right:
action.escu: 0
action.escu.analytic_story: ["CISA AA22-320A", "Log4Shell CVE-2021-44228"]
action.escu.confidence: high
action.escu.creation_date: 2024-05-26
action.escu.data_models: ["Risk"]
action.escu.eli5: The following analytic identifies potential exploitation of Log4Shell CVE-202
action.escu.enabled: 1
action.escu.full_search_name: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
action.escu.how_to_implement: To implement this correlation search a user needs to enable all de
action.escu.known_false_positives: There are no known false positive for this search, but it cou
action.escu.mappings: {"cis20": ["CIS 10"], "kill_chain_phases": ["Command and Control", "Delive
action.escu.modification_date: 2024-05-26
action.escu.product: ["Splunk Enterprise", "Splunk Enterprise Security", "Splunk Cloud"]
action.escu.providing_technologies: null
action.escu.search_type: detection
action.notable: 1
action.notable.param._entities: [{"risk_object_field": "N/A", "risk_object_type": "N/A", "risk_s
action.notable.param.drilldown_searches: []
action.notable.param.nes_fields: user,dest
action.notable.param.rule_description: The following analytic identifies potential exploitation
action.notable.param.rule_title: RBA: Log4Shell CVE-2021-44228 Exploitation
action.notable.param.security_domain: endpoint
action.notable.param.severity: high
action.risk.param._risk: []
action.send_notable_to_mc_alert_action: 1
```

```
action.correlationsearch.annotations: {"analytic_story": ["CISA AA22-320A", "Log4Shell CVE-2021-
action.correlationsearch.enabled: 1
action.correlationsearch.label: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
+action.correlationsearch.metadata: {"detection_id": "9be30d80-3a39-4df9-9102-64a467b24eac", "det
action.detection_backfill_add_a_backfill_to_the_backlog.description: This is used to add a new b
action.detection_backfill_add_a_backfill_to_the_backlog.label: Detection: Add a backfill to the
action.detection_backfill_add_a_backfill_to_the_backlog.param._cam: {"technology": [{"vendor": "
action.detection_backfill_run_the_next_backfill.label: Detection: Run the next backfill
action.detection_backfill_run_the_next_backfill.param._cam: {"technology": [{"product": "Detecti
action.detection_backfill_run_the_next_backfill.param.trigger: 0
action.email.footer.text: If you believe you've received this email in error, please see your Sp

splunk>
action.email.pdf.header_left:
action.email.pdf.header_right:
action.escu: 0
action.escu.analytic_story: ["CISA AA22-320A", "Log4Shell CVE-2021-44228"]
action.escu.confidence: high
action.escu.creation_date: 2024-05-26
action.escu.data_models: ["Risk"]
action.escu.eli5: The following analytic identifies potential exploitation of Log4Shell CVE-2021
action.escu.enabled: 1
action.escu.full_search_name: ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
action.escu.how_to_implement: To implement this correlation search a user needs to enable all de
action.escu.known_false_positives: There are no known false positive for this search, but it cou
action.escu.mappings: {"cis20": ["CIS 10"], "kill_chain_phases": ["Command and Control", "Delive
action.escu.modification_date: 2024-05-26
action.escu.product: ["Splunk Enterprise", "Splunk Enterprise Security", "Splunk Cloud"]
action.escu.providing_technologies: null
action.escu.search_type: detection
action.notable: 1
action.notable.param._entities: [{"risk_object_field": "N/A", "risk_object_type": "N/A", "risk_s
action.notable.param.drilldown_searches: []
action.notable.param.nes_fields: user,dest
action.notable.param.rule_description: The following analytic identifies potential exploitation
action.notable.param.rule_title: RBA: Log4Shell CVE-2021-44228 Exploitation
action.notable.param.security_domain: endpoint
action.notable.param.severity: high
action.risk.param._risk: []
action.send_notable_to_mc_alert_action: 1
```

Details

Type	Event-based detection
ID	9be30d80-3a39-4df9-9102-64a467b24eac
Cloned from	--
Title	ESCU - Log4Shell CVE-2021-44228 Exploitation - Rule
Description	The following analytic identifies potential exploitation of Log4Shell CVE-2021-44228 by correlating multiple MITRE ATT&CK tactics detected in risk events. It leverages Splunk's risk...
Author	--
Automation rule	--

Versions 8

Version created by Splunk

4.2 4.1
10/18/24, 10:24 PM
Version created from 4.1

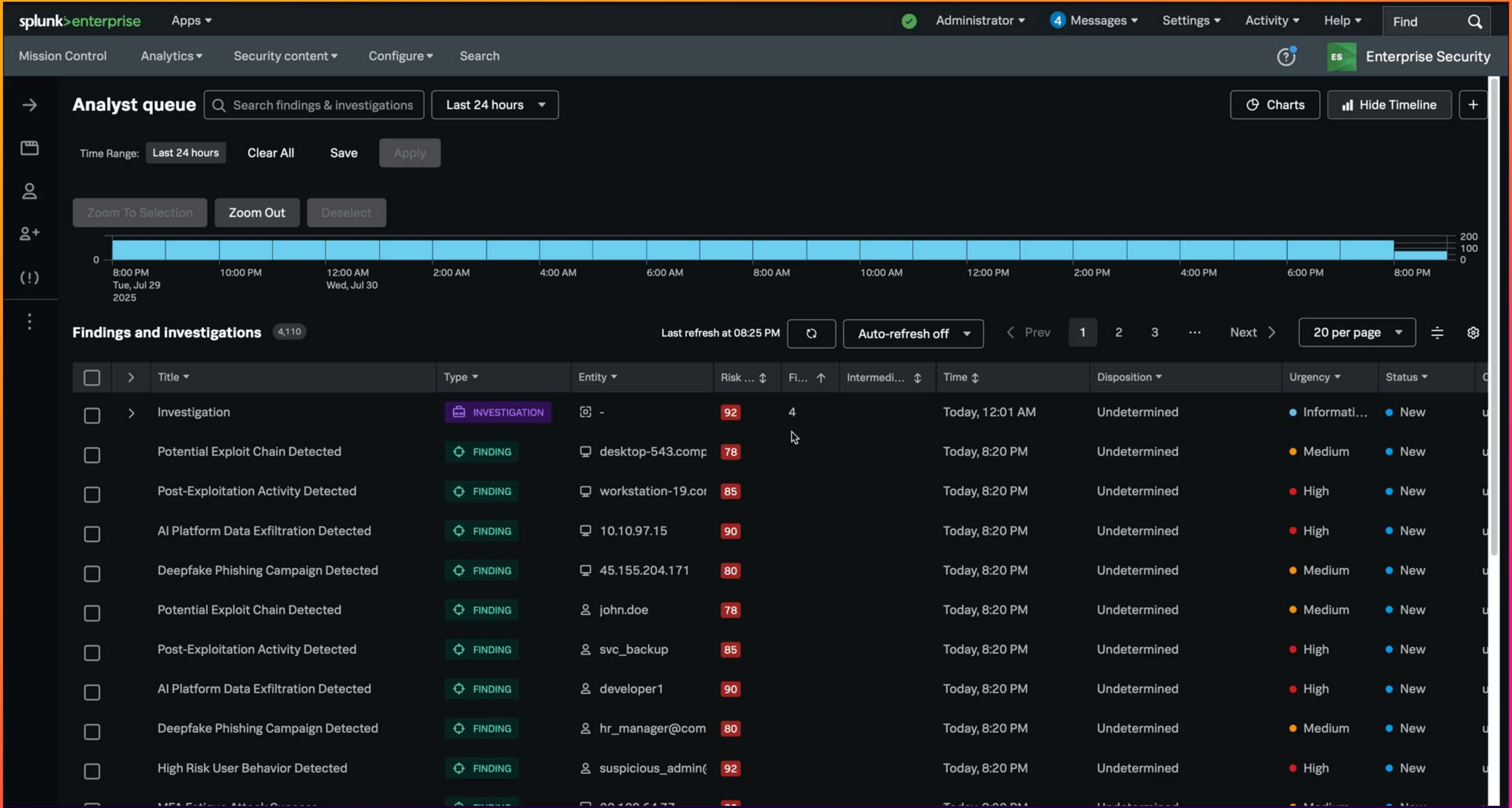
4.2 4.1
10/18/24, 10:24 PM
Version created from 4.1

4.1
10/18/24, 10:07 PM
Version created by Splunk

4.1
10/18/24, 10:07 PM
Version created by Splunk

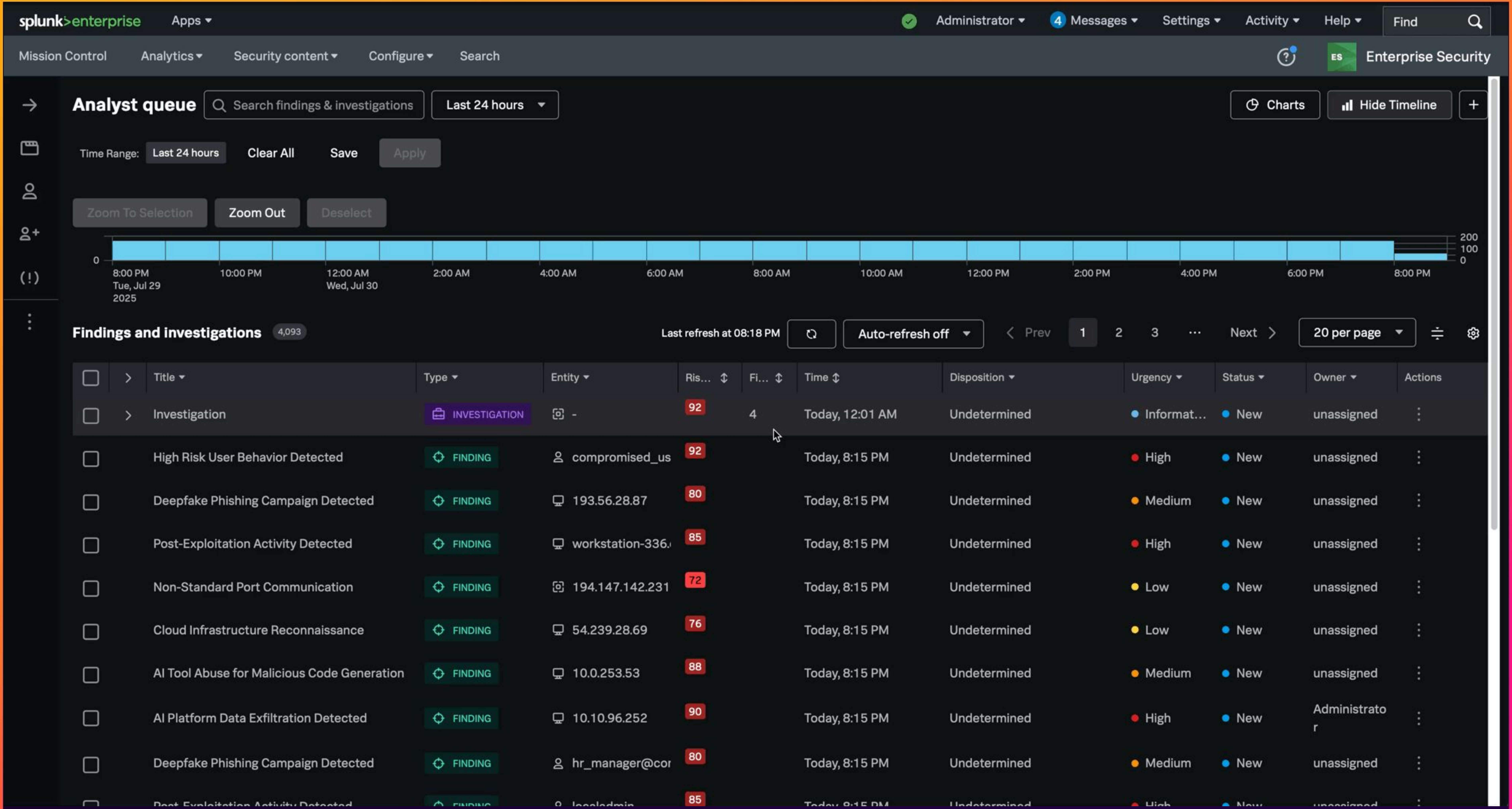
Prioritized Findings in the Analyst Queue

Splunk ES 8's redesigned triage workflow helps analysts focus on high-priority findings with the context they need — all from a clean, intuitive queue interface.

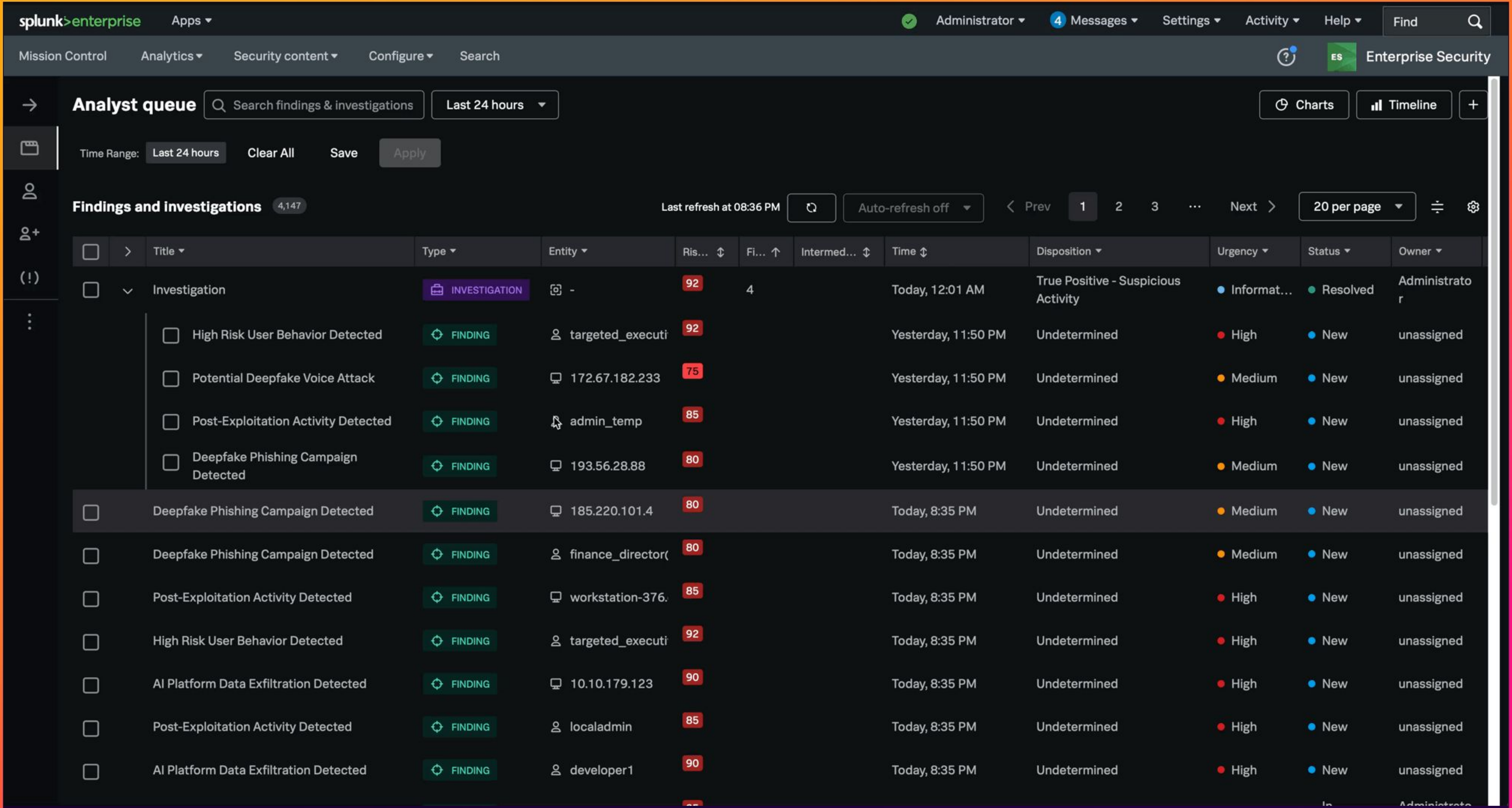


Findings and investigations 4,110

□		Title	Type	Entity	Risk ...	Fi...	Intermedi...	Time	Disposition	Urgency	Status
□	>	Investigation	INVESTIGATION	-	92	4		Today, 12:01 AM	Undetermined	● Informati...	● New
□		Potential Exploit Chain Detected	FINDING	desktop-543.comp	78			Today, 8:20 PM	Undetermined	● Medium	● New
□		Post-Exploitation Activity Detected	FINDING	workstation-19.coı	85			Today, 8:20 PM	Undetermined	● High	● New
□		AI Platform Data Exfiltration Detected	FINDING	10.10.97.15	90			Today, 8:20 PM	Undetermined	● High	● New
□		Deepfake Phishing Campaign Detected	FINDING	45.155.204.171	80			Today, 8:20 PM	Undetermined	● Medium	● New
□		Potential Exploit Chain Detected	FINDING	john.doe	78			Today, 8:20 PM	Undetermined	● Medium	● New
□		Post-Exploitation Activity Detected	FINDING	svc_backup	85			Today, 8:20 PM	Undetermined	● High	● New
□		AI Platform Data Exfiltration Detected	FINDING	developer1	90			Today, 8:20 PM	Undetermined	● High	● New
□		Deepfake Phishing Campaign Detected	FINDING	hr_manager@com	80			Today, 8:20 PM	Undetermined	● Medium	● New
□		High Risk User Behavior Detected	FINDING	suspicious_admin(	92			Today, 8:20 PM	Undetermined	● High	● New



□		Title	Type	Entity	Ris...	Fi...	Time	Disposition	Urgency	Status	Owner	Actions
□	>	Investigation	INVESTIGATION	-	92	4	Today, 12:01 AM	Undetermined	● Informat...	● New	unassigned	⋮
□		High Risk User Behavior Detected	FINDING	compromised_us	92		Today, 8:15 PM	Undetermined	● High	● New	unassigned	⋮
□		Deepfake Phishing Campaign Detected	FINDING	193.56.28.87	80		Today, 8:15 PM	Undetermined	● Medium	● New	unassigned	⋮
□		Post-Exploitation Activity Detected	FINDING	workstation-336.	85		Today, 8:15 PM	Undetermined	● High	● New	unassigned	⋮
□		Non-Standard Port Communication	FINDING	194.147.142.231	72		Today, 8:15 PM	Undetermined	● Low	● New	unassigned	⋮
□		Cloud Infrastructure Reconnaissance	FINDING	54.239.28.69	76		Today, 8:15 PM	Undetermined	● Low	● New	unassigned	⋮
□		AI Tool Abuse for Malicious Code Generation	FINDING	10.0.253.53	88		Today, 8:15 PM	Undetermined	● Medium	● New	unassigned	⋮
□		AI Platform Data Exfiltration Detected	FINDING	10.10.96.252	90		Today, 8:15 PM	Undetermined	● High	● New	Administrato r	⋮
□		Deepfake Phishing Campaign Detected	FINDING	hr_manager@cor	80		Today, 8:15 PM	Undetermined	● Medium	● New	unassigned	⋮
□		Post-Exploitation Activity Detected	FINDING	localadmin	85		Today, 8:15 PM	Undetermined	● High	● New	unassigned	⋮



Analyst queue

Search findings & investigations | Last 24 hours

Time Range: Last 24 hours | Clear All | Save | Apply

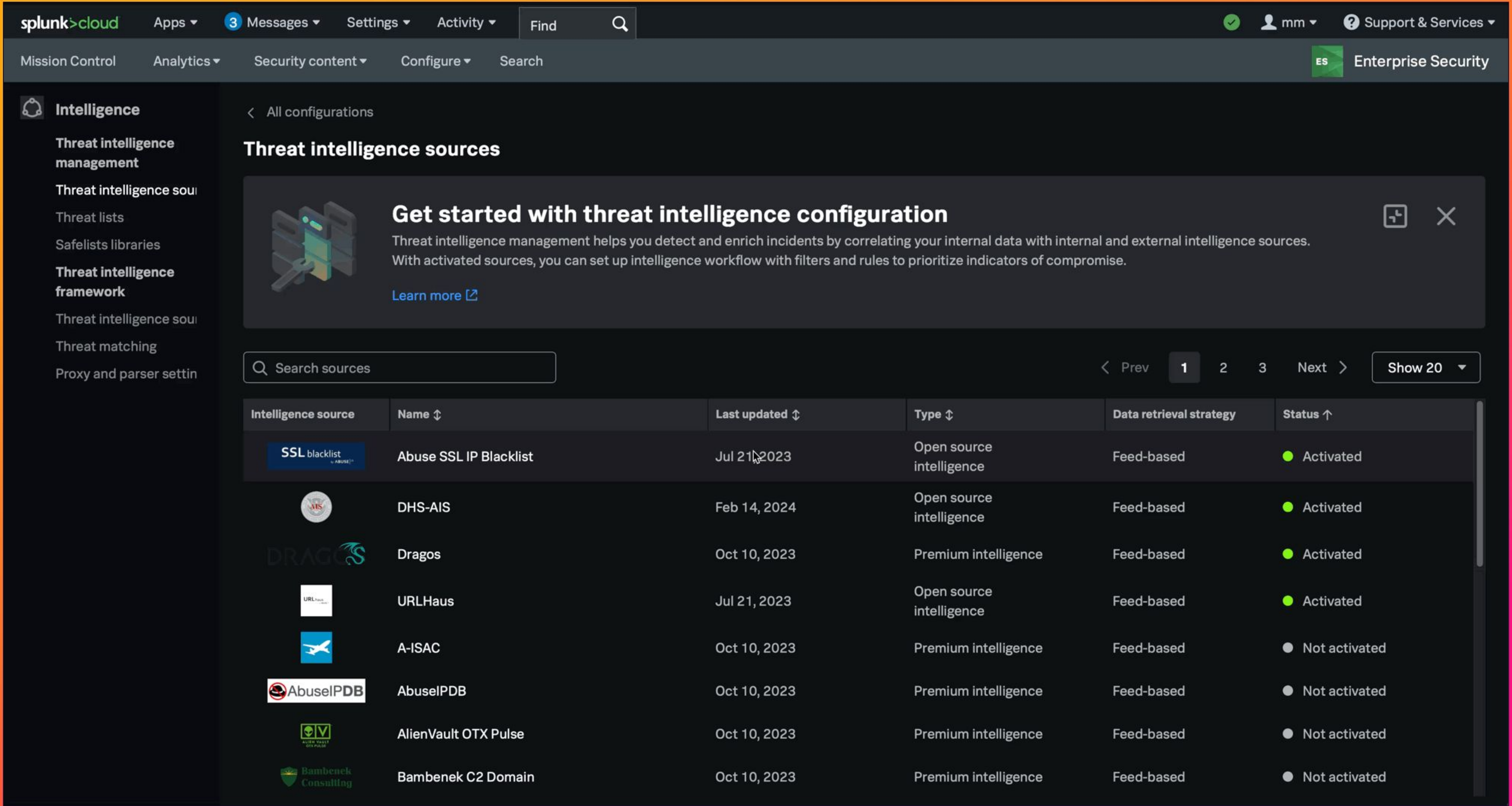
Findings and investigations 4,147

Last refresh at 08:36 PM | Auto-refresh off | Prev 1 2 3 … Next | 20 per page

Title	Type	Entity	Ris...	Fi...	Intermed...	Time	Disposition	Urgency	Status	Owner
Investigation	INVESTIGATION	-	92	4		Today, 12:01 AM	True Positive - Suspicious Activity	● Informat...	● Resolved	Administrator
High Risk User Behavior Detected	FINDING	targeted_executi	92			Yesterday, 11:50 PM	Undetermined	● High	● New	unassigned
Potential Deepfake Voice Attack	FINDING	172.67.182.233	75			Yesterday, 11:50 PM	Undetermined	● Medium	● New	unassigned
Post-Exploitation Activity Detected	FINDING	admin_temp	85			Yesterday, 11:50 PM	Undetermined	● High	● New	unassigned
Deepfake Phishing Campaign Detected	FINDING	193.56.28.88	80			Yesterday, 11:50 PM	Undetermined	● Medium	● New	unassigned
Deepfake Phishing Campaign Detected	FINDING	185.220.101.4	80			Today, 8:35 PM	Undetermined	● Medium	● New	unassigned
Deepfake Phishing Campaign Detected	FINDING	finance_director(	80			Today, 8:35 PM	Undetermined	● Medium	● New	unassigned
Post-Exploitation Activity Detected	FINDING	workstation-376.	85			Today, 8:35 PM	Undetermined	● High	● New	unassigned
High Risk User Behavior Detected	FINDING	targeted_executi	92			Today, 8:35 PM	Undetermined	● High	● New	unassigned
AI Platform Data Exfiltration Detected	FINDING	10.10.179.123	90			Today, 8:35 PM	Undetermined	● High	● New	unassigned
Post-Exploitation Activity Detected	FINDING	localadmin	85			Today, 8:35 PM	Undetermined	● High	● New	unassigned
AI Platform Data Exfiltration Detected	FINDING	developer1	90			Today, 8:35 PM	Undetermined	● High	● New	unassigned

Enrichment with Threat Intelligence & SOAR Automation

Splunk ES 8 integrates threat intel and SOAR automation directly into triage — helping analysts make faster, more confident decisions.



Threat intelligence sources

Get started with threat intelligence configuration

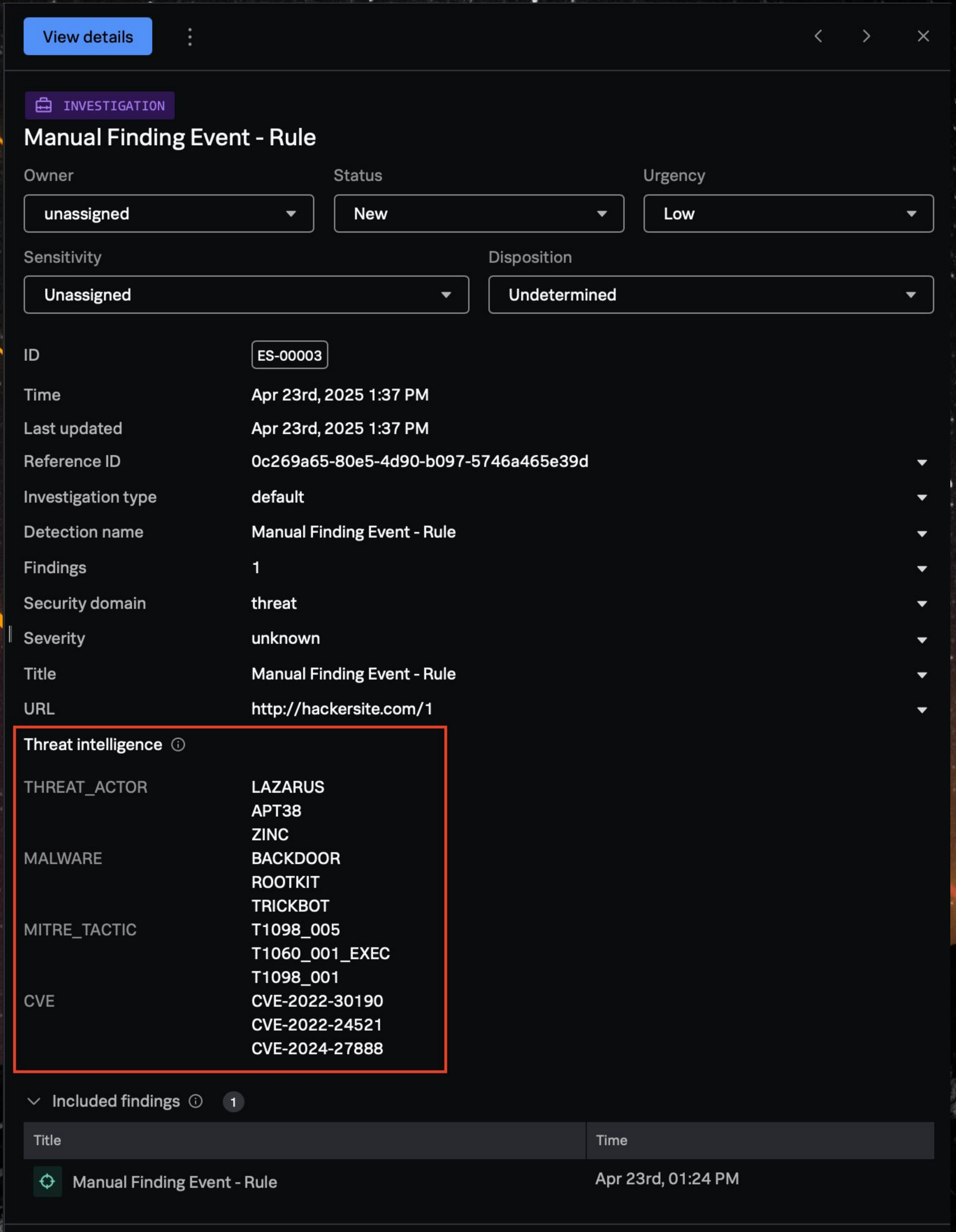
Threat intelligence management helps you detect and enrich incidents by correlating your internal data with internal and external intelligence sources. With activated sources, you can set up intelligence workflow with filters and rules to prioritize indicators of compromise.

Learn more

Intelligence source	Name	Last updated	Type	Data retrieval strategy	Status
SSL blacklist	Abuse SSL IP Blacklist	Jul 21, 2023	Open source intelligence	Feed-based	● Activated
AIS	DHS-AIS	Feb 14, 2024	Open source intelligence	Feed-based	● Activated
DRAGOS	Dragos	Oct 10, 2023	Premium intelligence	Feed-based	● Activated
URLhaus	URLHaus	Jul 21, 2023	Open source intelligence	Feed-based	● Activated
	A-ISAC	Oct 10, 2023	Premium intelligence	Feed-based	● Not activated
AbuseIPDB	AbuseIPDB	Oct 10, 2023	Premium intelligence	Feed-based	● Not activated
AV	AlienVault OTX Pulse	Oct 10, 2023	Premium intelligence	Feed-based	● Not activated
Bambenek Consulting	Bambenek C2 Domain	Oct 10, 2023	Premium intelligence	Feed-based	● Not activated

Threat Intelligence

Embedded in the TDIR workflow



Manual Finding Event - Rule

Owner	unassigned
Status	New
Urgency	Low
Sensitivity	Unassigned
Disposition	Undetermined

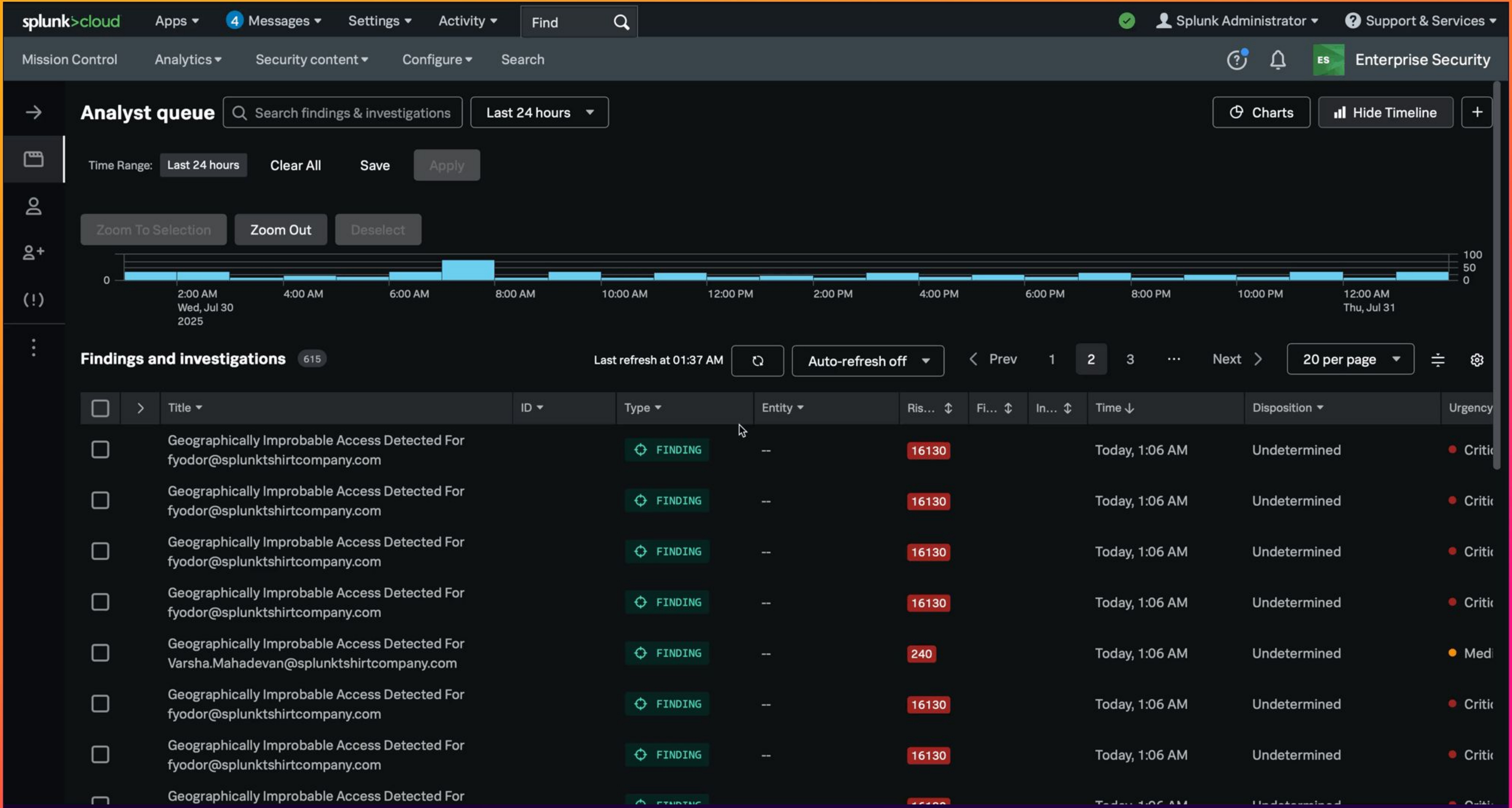
ID	ES-00003
Time	Apr 23rd, 2025 1:37 PM
Last updated	Apr 23rd, 2025 1:37 PM
Reference ID	0c269a65-80e5-4d90-b097-5746a465e39d
Investigation type	default
Detection name	Manual Finding Event - Rule
Findings	1
Security domain	threat
Severity	unknown
Title	Manual Finding Event - Rule
URL	http://hackersite.com/1

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



Analyst queue

Last 24 hours

Time Range: Last 24 hours

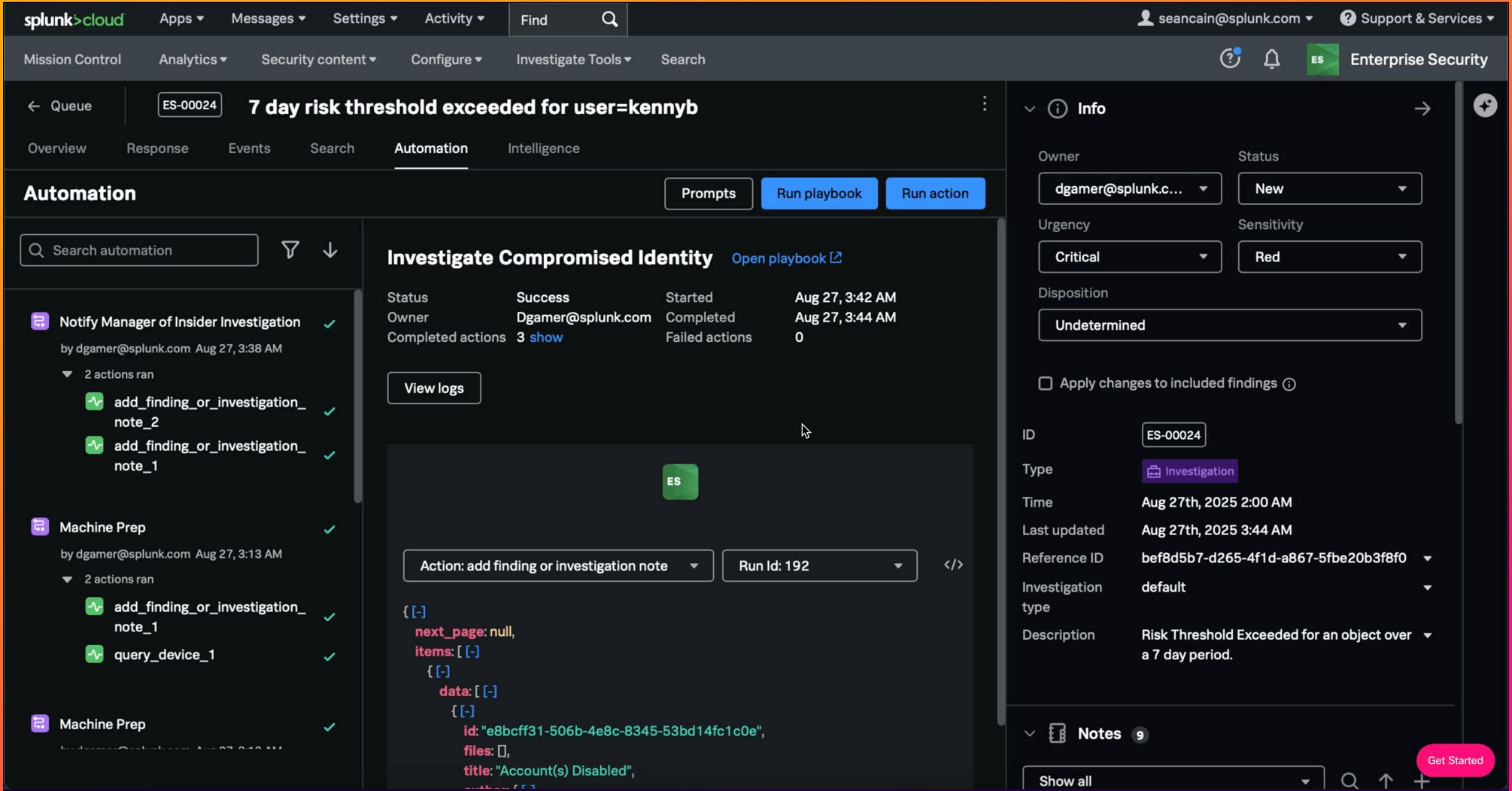
Findings and investigations 615

Last refresh at 01:37 AM

Auto-refresh off

20 per page

☐	Title	ID	Type	Entity	Ris...	Fi...	In...	Time	Disposition	Urgency
☐	Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	16130			Today, 1:06 AM	Undetermined	● Critic
☐	Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	16130			Today, 1:06 AM	Undetermined	● Critic
☐	Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	16130			Today, 1:06 AM	Undetermined	● Critic
☐	Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	16130			Today, 1:06 AM	Undetermined	● Critic
☐	Geographically Improbable Access Detected For Varsha.Mahadevan@splunktshirtcompany.com		FINDING	--	240			Today, 1:06 AM	Undetermined	● Medi
☐	Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	16130			Today, 1:06 AM	Undetermined	● Critic
☐	Geographically Improbable Access Detected For fyodor@splunktshirtcompany.com		FINDING	--	16130			Today, 1:06 AM	Undetermined	● Critic
☐	Geographically Improbable Access Detected For		FINDING		16130			Today, 1:06 AM	Undetermined	● Critic



ES-00024 **7 day risk threshold exceeded for user=kennyb**

Automation

Notify Manager of Insider Investigation ✓
by dgamer@splunk.com Aug 27, 3:38 AM
▾ 2 actions ran
- add_finding_or_investigation_note_2 ✓
- add_finding_or_investigation_note_1 ✓

Machine Prep ✓
by dgamer@splunk.com Aug 27, 3:13 AM
▾ 2 actions ran
- add_finding_or_investigation_note_1 ✓
- query_device_1 ✓

Machine Prep ✓

Investigate Compromised Identity Open playbook

Status	Success	Started	Aug 27, 3:42 AM
Owner	Dgamer@splunk.com	Completed	Aug 27, 3:44 AM
Completed actions	3 show	Failed actions	0

Action: add finding or investigation note ▾ Run Id: 192 ▾

```
{ [-]
  next_page: null,
  items: [ [-]
    { [-]
      data: [ [-]
        { [-]
          id: "e8bcff31-506b-4e8c-8345-53bd14fc1c0e",
          files: [],
          title: "Account(s) Disabled",
```

Info

Owner	dgamer@splunk.c... ▾
Status	New ▾
Urgency	Critical ▾
Sensitivity	Red ▾
Disposition	Undetermined ▾

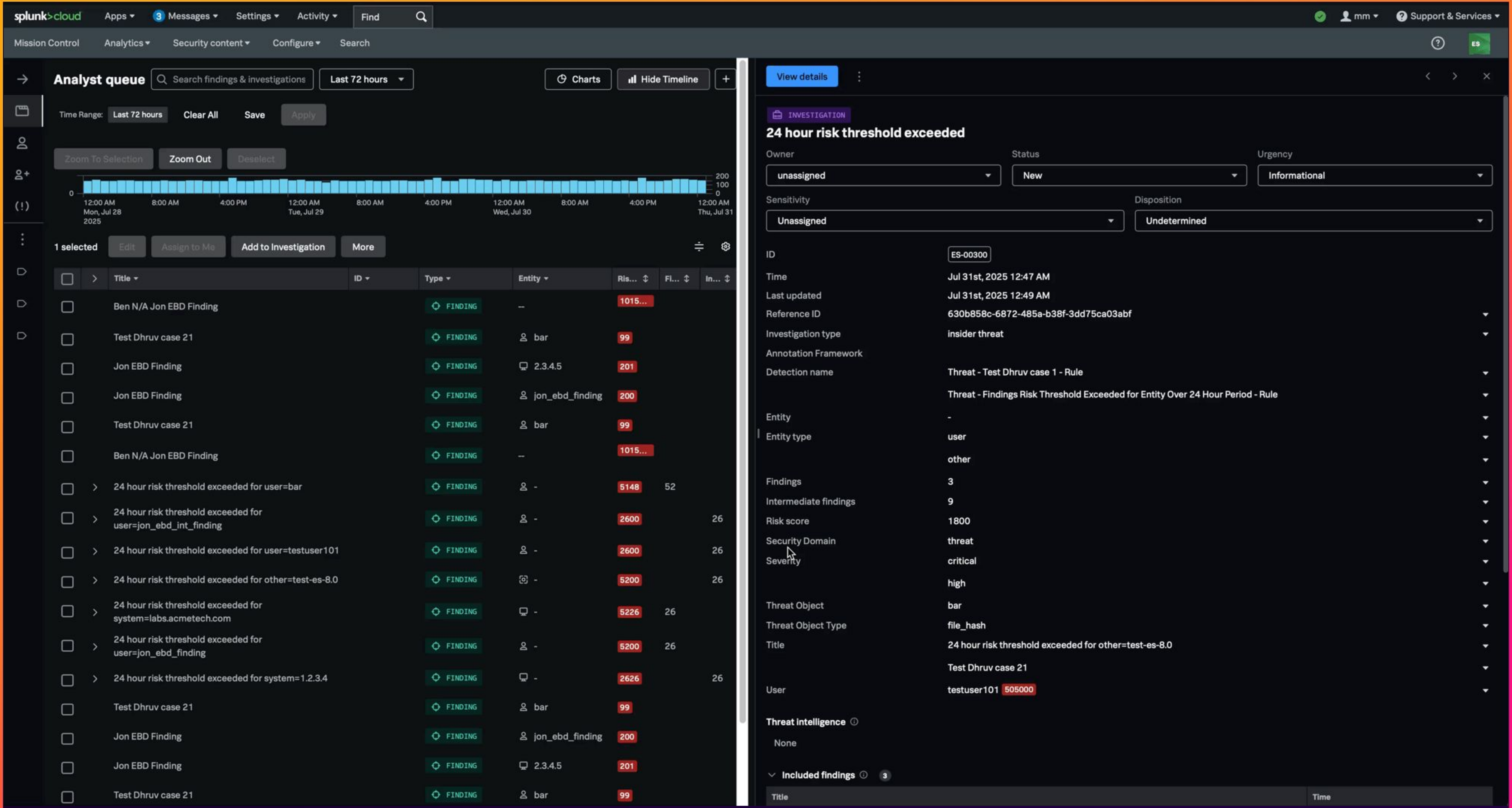
☐ Apply changes to included findings

ID	ES-00024
Type	Investigation
Time	Aug 27th, 2025 2:00 AM
Last updated	Aug 27th, 2025 3:44 AM
Reference ID	bef8d5b7-d265-4f1d-a867-5fbe20b3f8f0
Investigation type	default
Description	Risk Threshold Exceeded for an object over a 7 day period.

Notes 9

Investigation, Collaboration, and AI Assistance

ES 8 provides a modern investigation workspace where teams can group findings, collaborate seamlessly, and leverage AI to accelerate resolution.



Title	ID	Type	Entity	Ris...	Fi...	In...
Ben N/A Jon EBD Finding		FINDING	--	1015...		
Test Dhruv case 21		FINDING	bar	99		
Jon EBD Finding		FINDING	2.3.4.5	201		
Jon EBD Finding		FINDING	jon_ebd_finding	200		
Test Dhruv case 21		FINDING	bar	99		
Ben N/A Jon EBD Finding		FINDING	--	1015...		
24 hour risk threshold exceeded for user=bar		FINDING	-	5148	52	
24 hour risk threshold exceeded for user=jon_ebd_int_finding		FINDING	-	2600		26
24 hour risk threshold exceeded for user=testuser101		FINDING	-	2600		26
24 hour risk threshold exceeded for other=test-es-8.0		FINDING	-	5200		26
24 hour risk threshold exceeded for system=labs.acmetech.com		FINDING	-	5226	26	
24 hour risk threshold exceeded for user=jon_ebd_finding		FINDING	-	5200	26	
24 hour risk threshold exceeded for system=1.2.3.4		FINDING	-	2626		26
Test Dhruv case 21		FINDING	bar	99		
Jon EBD Finding		FINDING	jon_ebd_finding	200		
Jon EBD Finding		FINDING	2.3.4.5	201		
Test Dhruv case 21		FINDING	bar	99		

24 hour risk threshold exceeded

Owner	Status	Urgency
unassigned	New	Informational

Sensitivity	Disposition
Unassigned	Undetermined

ID	ES-00300
Time	Jul 31st, 2025 12:47 AM
Last updated	Jul 31st, 2025 12:49 AM
Reference ID	630b858c-6872-485a-b38f-3dd75ca03abf
Investigation type	insider threat
Annotation Framework	
Detection name	Threat - Test Dhruv case 1 - Rule Threat - Findings Risk Threshold Exceeded for Entity Over 24 Hour Period - Rule
Entity	-
Entity type	user other
Findings	3
Intermediate findings	9
Risk score	1800
Security Domain	threat
Severity	critical high
Threat Object	bar
Threat Object Type	file_hash
Title	24 hour risk threshold exceeded for other=test-es-8.0 Test Dhruv case 21
User	testuser101 505000

Threat intelligence

None

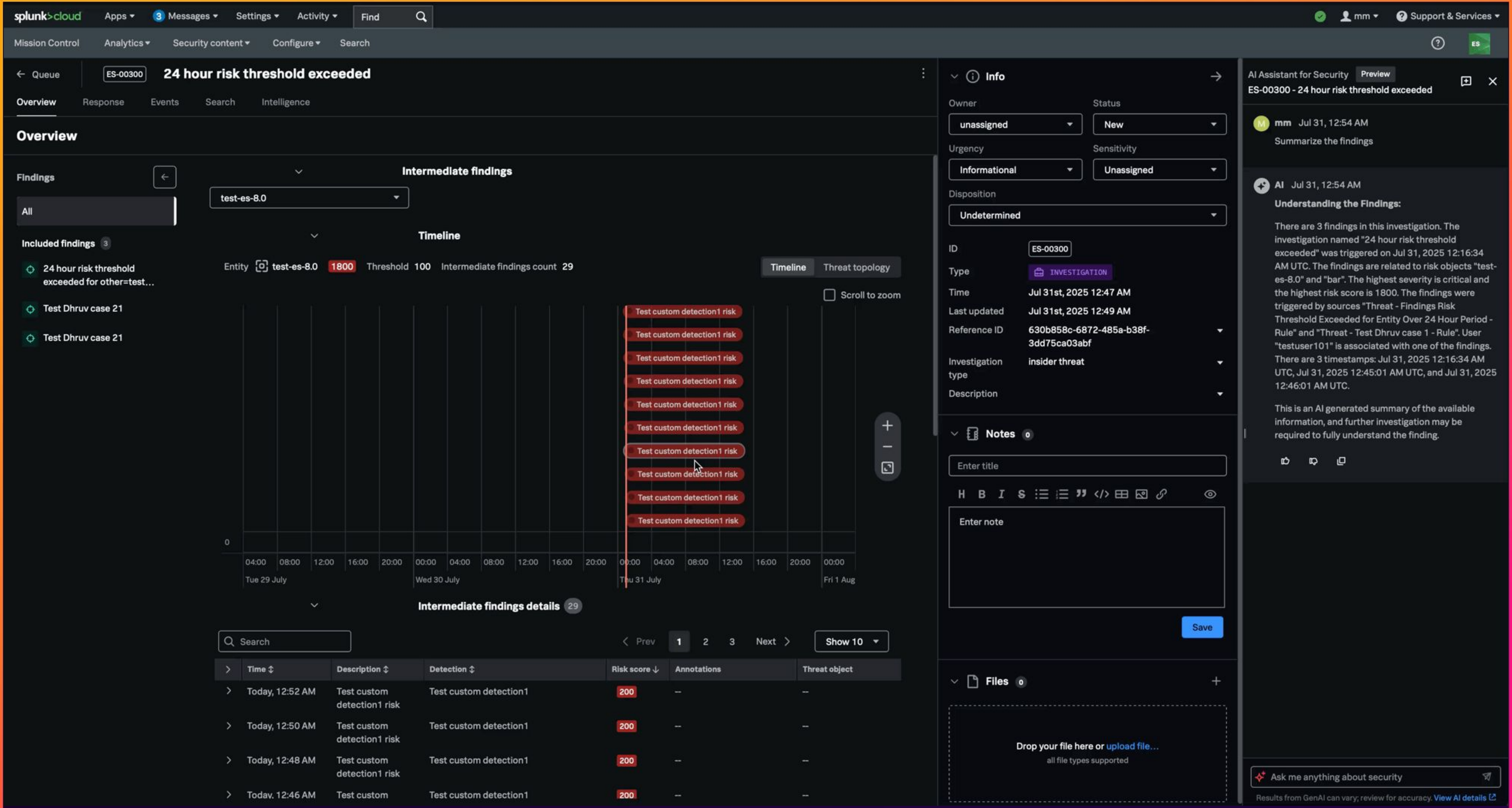
Included findings 3

Title	Time

© 2025 SPLUNK LLC

Detection → Triage → Decision → Investigation

Splunk ES 8 reimagines every step of the TDIR workflow for speed, context, and confidence.



ES-00300 **24 hour risk threshold exceeded**

Overview

Findings

All

Included findings 3

- 24 hour risk threshold exceeded for other=test...
- Test Dhruv case 21
- Test Dhruv case 21

Intermediate findings

test-es-8.0

Timeline

Entity test-es-8.0 1800 Threshold 100 Intermediate findings count 29

Test custom detection1 risk
Test custom detection1 risk
Test custom detection1 risk
Test custom detection1 risk
Test custom detection1 risk
Test custom detection1 risk
Test custom detection1 risk
Test custom detection1 risk
Test custom detection1 risk
Test custom detection1 risk
0
04:00
08:00
12:00
16:00
20:00
00:00
04:00
08:00
12:00
16:00
20:00
00:00
04:00
08:00
12:00
16:00
20:00
00:00
Tue 29 July
Wed 30 July
Thu 31 July
Fri 1 Aug

Intermediate findings details 29

Search

	Time	Description	Detection	Risk score	Annotations	Threat object
>	Today, 12:52 AM	Test custom detection1 risk	Test custom detection1	200	--	--
>	Today, 12:50 AM	Test custom detection1 risk	Test custom detection1	200	--	--
>	Today, 12:48 AM	Test custom detection1 risk	Test custom detection1	200	--	--
>	Today, 12:46 AM	Test custom	Test custom detection1	200	--	--

Info

Owner	Status
unassigned	New

Urgency	Sensitivity
Informational	Unassigned

Disposition: Undetermined

ID	ES-00300
Type	INVESTIGATION
Time	Jul 31st, 2025 12:47 AM
Last updated	Jul 31st, 2025 12:49 AM
Reference ID	630b858c-6872-485a-b38f-3dd75ca03abf
Investigation type	insider threat
Description	

Notes 0

Enter title

Enter note

Files 0

Drop your file here or upload file...
all file types supported

AI Assistant for Security Preview
ES-00300 - 24 hour risk threshold exceeded

mm Jul 31, 12:54 AM
Summarize the findings

AI Jul 31, 12:54 AM
Understanding the Findings:

There are 3 findings in this investigation. The investigation named "24 hour risk threshold exceeded" was triggered on Jul 31, 2025 12:16:34 AM UTC. The findings are related to risk objects "test-es-8.0" and "bar". The highest severity is critical and the highest risk score is 1800. The findings were triggered by sources "Threat - Findings Risk Threshold Exceeded for Entity Over 24 Hour Period - Rule" and "Threat - Test Dhruv case 1 - Rule". User "testuser101" is associated with one of the findings. There are 3 timestamps: Jul 31, 2025 12:16:34 AM UTC, Jul 31, 2025 12:45:01 AM UTC, and Jul 31, 2025 12:46:01 AM UTC.

This is an AI generated summary of the available information, and further investigation may be required to fully understand the finding.

Ask me anything about security

Results from GenAI can vary; review for accuracy. View AI details

The SOC Has Changed. Has Yours?

The traditional SOC model no longer works. ES 8 helps you evolve, not rebuild.

How to get started with ES 8

- Talk to your friendly Splunker
  - Free Workshops
  - Splunk University
  - https://lantern.splunk.com/Security/Getting_Started/Getting_started_with_ES
  - Splunking for outcomes: Kicking off your RBA journey

Thank you

.conf25
splunk>