.conf19 splunk>

What’s New in Splunk for Security

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

.conf19

splunk>

Hello!

Meet your Splunkers

Chris Simmons

Product Marketing Director

Robert Truesdell

Sr. Director, Product Management

Patriz Regalado

Sr. Product Marketing Manager

Kyle Champlin

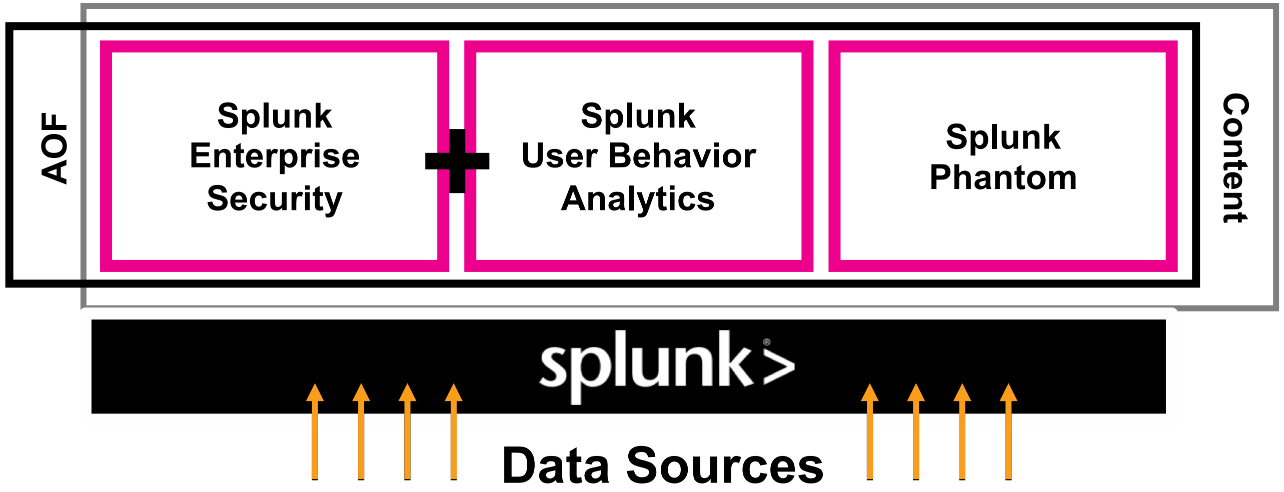
Principal Product Manager

Koulick Ghosh

Product Manager

Splunk Security Operations Suite

Modernize your security operations



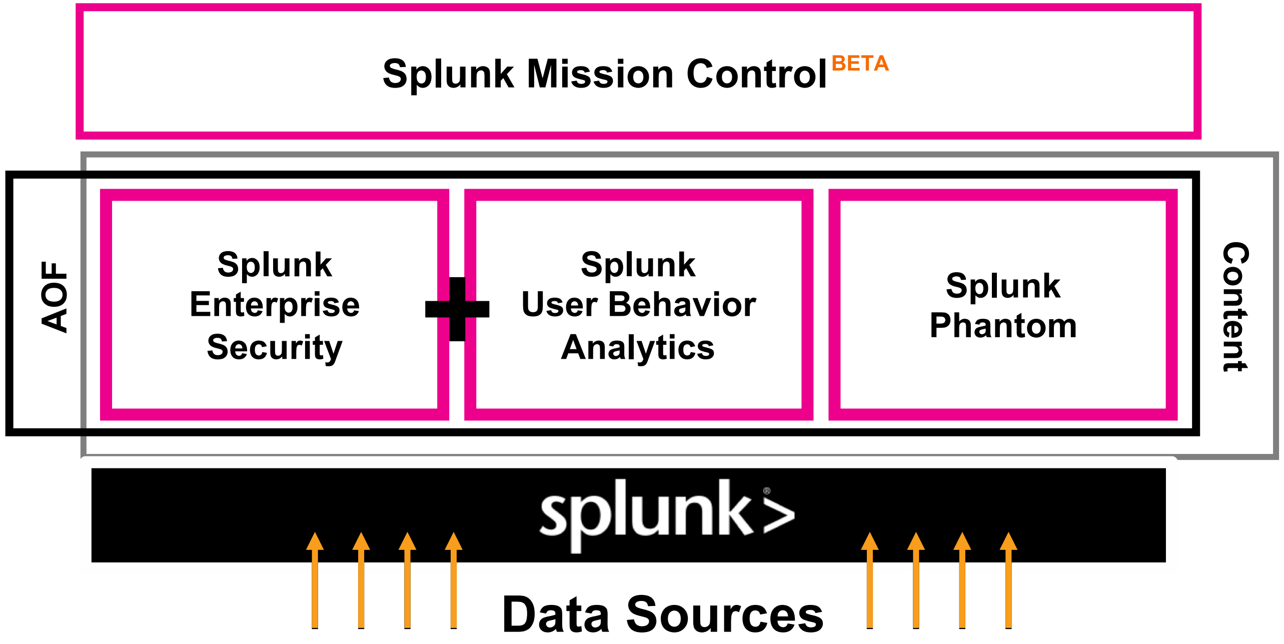
AOF *= Adaptive Operations Framework - our ecosystem of apps and security partner integrations.*

Content *= Pre-packaged security content (searches, detection models, automation playbooks) from the Splunk Research Team. Stay current with latest threat landscape.*

Splunk Security Operations Suite is the only **integrated suite** with industry-leading **SIEM**, **UEBA** and **SOAR** solutions that utilize a market-proven, **scalable big data platform**, continually augmented with actionable use case content.

Splunk Security Operations Suite

Re-imagine security operations


Splunk Mission Control BETA
AOF
Splunk Enterprise Security
+
Splunk User Behavior Analytics
Splunk Phantom
Content
splunk>
Data Sources

AOF *= Adaptive Operations Framework - our ecosystem of apps and security partner integrations.*

Content *= Pre-packaged security content (searches, detection models, automation playbooks) from the Splunk Research Team. Stay current with latest threat landscape.*

Splunk modernizes security operations by acting as their **security nerve center**, turning **data into detections**, and **insights into actions**, across all security use cases, teams, and functions.

Splunk drives the **Data**, **Analytics**, and **Operations** layers for the SOC to enable security teams to function at its highest level of performance.

Introducing

Splunk Mission Control

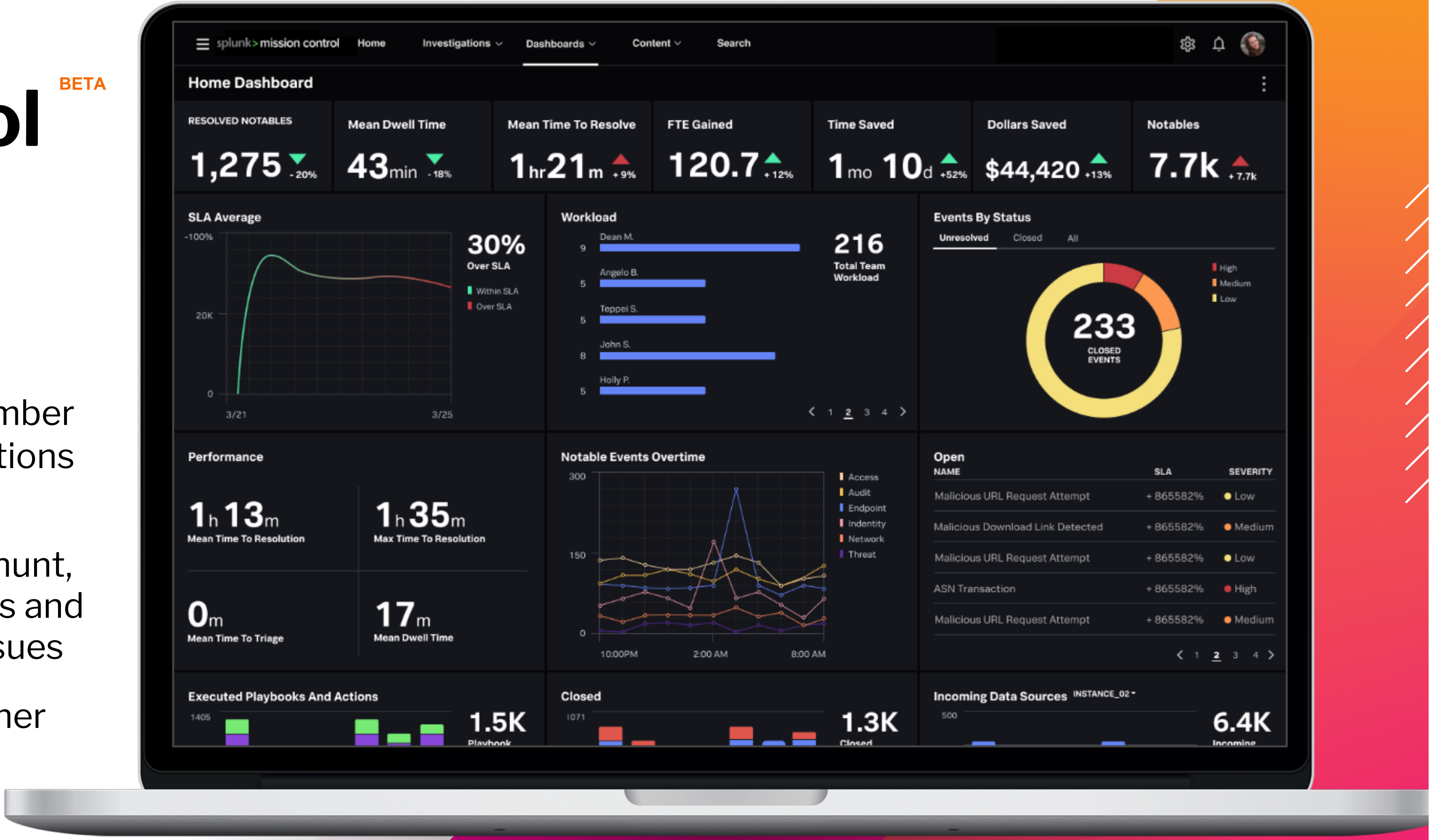
.conf19
splunk>

Splunk Mission Control

BETA

A Modern, Cloud-Based, and Unified Security Operations Experience

- One place for every team member to manage the security operations event lifecycle, start to finish
- Detect, manage, investigate, hunt, contain, and remediate threats and other high-priority security issues
- Integrate Splunk tools and other cloud, on-premise, and hybrid tools/services together



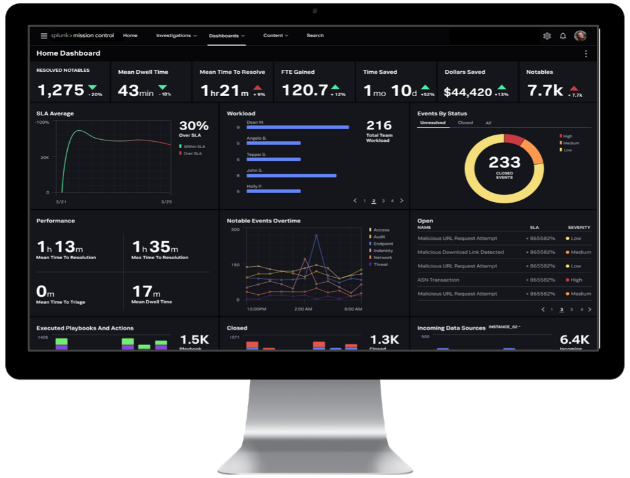
Open

NAME	SLA	SEVERITY
Malicious URL Request Attempt	+ 865582%	● Low
Malicious Download Link Detected	+ 865582%	● Medium
Malicious URL Request Attempt	+ 865582%	● Low
ASN Transaction	+ 865582%	● High
Malicious URL Request Attempt	+ 865582%	● Medium

Splunk Mission Control

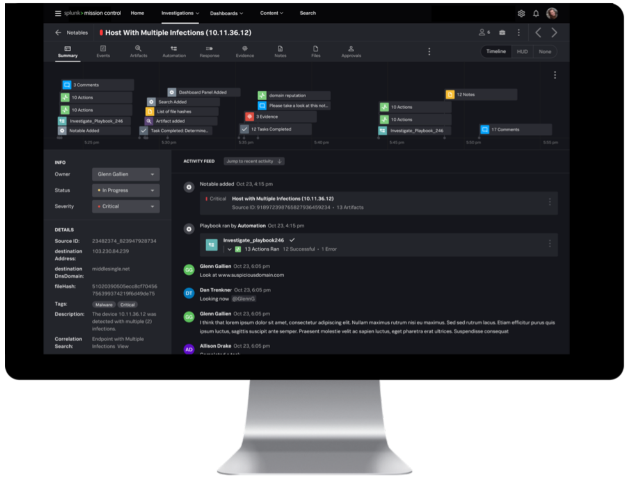
Key Features

Customizable Operations Dashboards



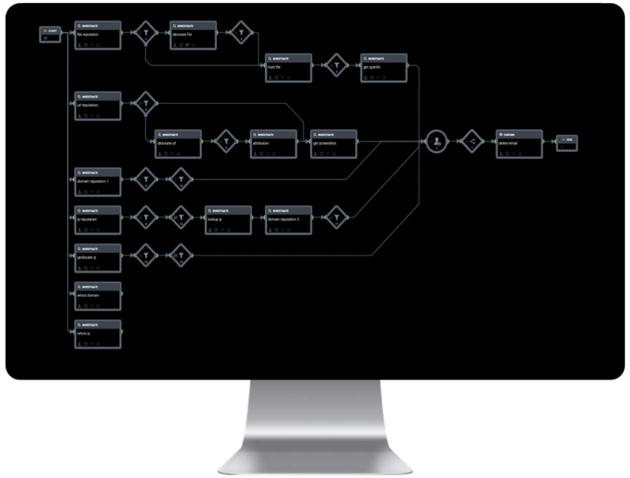
- Every user/role can have a dashboard of metrics that is customized to their needs
- Supports Splunk SPL for the ultimate in customization

Investigations and Case Management



- Analytics extension taps into new/existing Splunk instances
- Case management improves the precision of response workflows

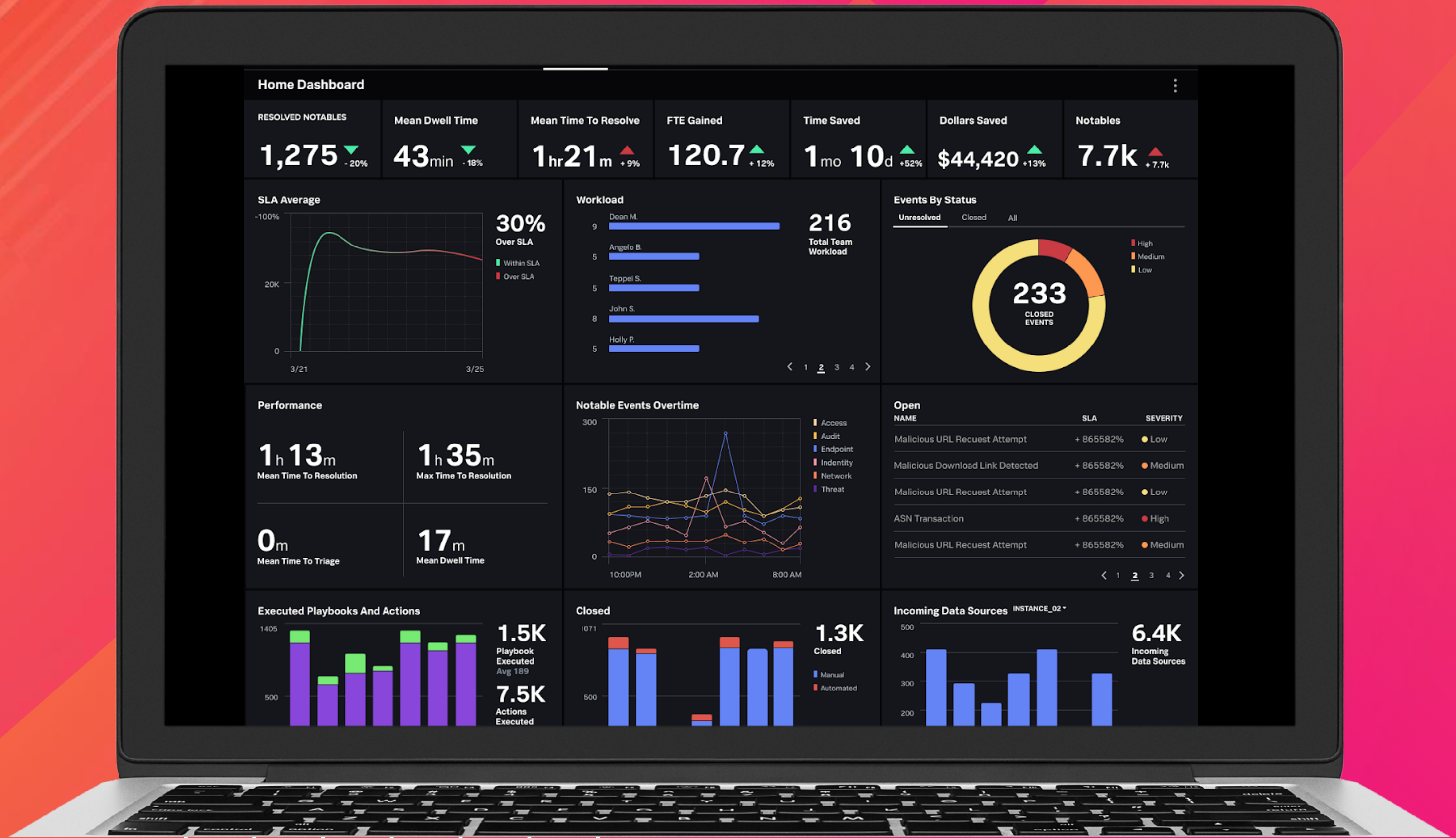
Orchestration & Automation



- Orchestration & Automation extension recovers lost time performing time-consuming and often repetitive actions

Splunk Mission Control

Quick Demo



Home Dashboard

RESOLVED NOTABLES	Mean Dwell Time	Mean Time To Resolve	FTE Gained	Time Saved	Dollars Saved	Notables
1,275 - 20%	43min - 18%	1hr21m + 9%	120.7 + 12%	1mo 10d +52%	$44,420 +13%	7.7k + 7.7k

SLA Average

30% Over SLA

Workload

216 Total Team Workload

Events By Status

233 CLOSED EVENTS

Performance

1h 13m Mean Time To Resolution

1h 35m Max Time To Resolution

0m Mean Time To Triage

17m Mean Dwell Time

Notable Events Overtime

Open

NAME	SLA	SEVERITY
Malicious URL Request Attempt	+ 865582%	● Low
Malicious Download Link Detected	+ 865582%	● Medium
Malicious URL Request Attempt	+ 865582%	● Low
ASN Transaction	+ 865582%	● High
Malicious URL Request Attempt	+ 865582%	● Medium

Executed Playbooks And Actions

1.5K Playbook Executed Avg 189

7.5K Actions Executed

Closed

1.3K Closed

Incoming Data Sources INSTANCE_02

6.4K Incoming Data Sources

What's New

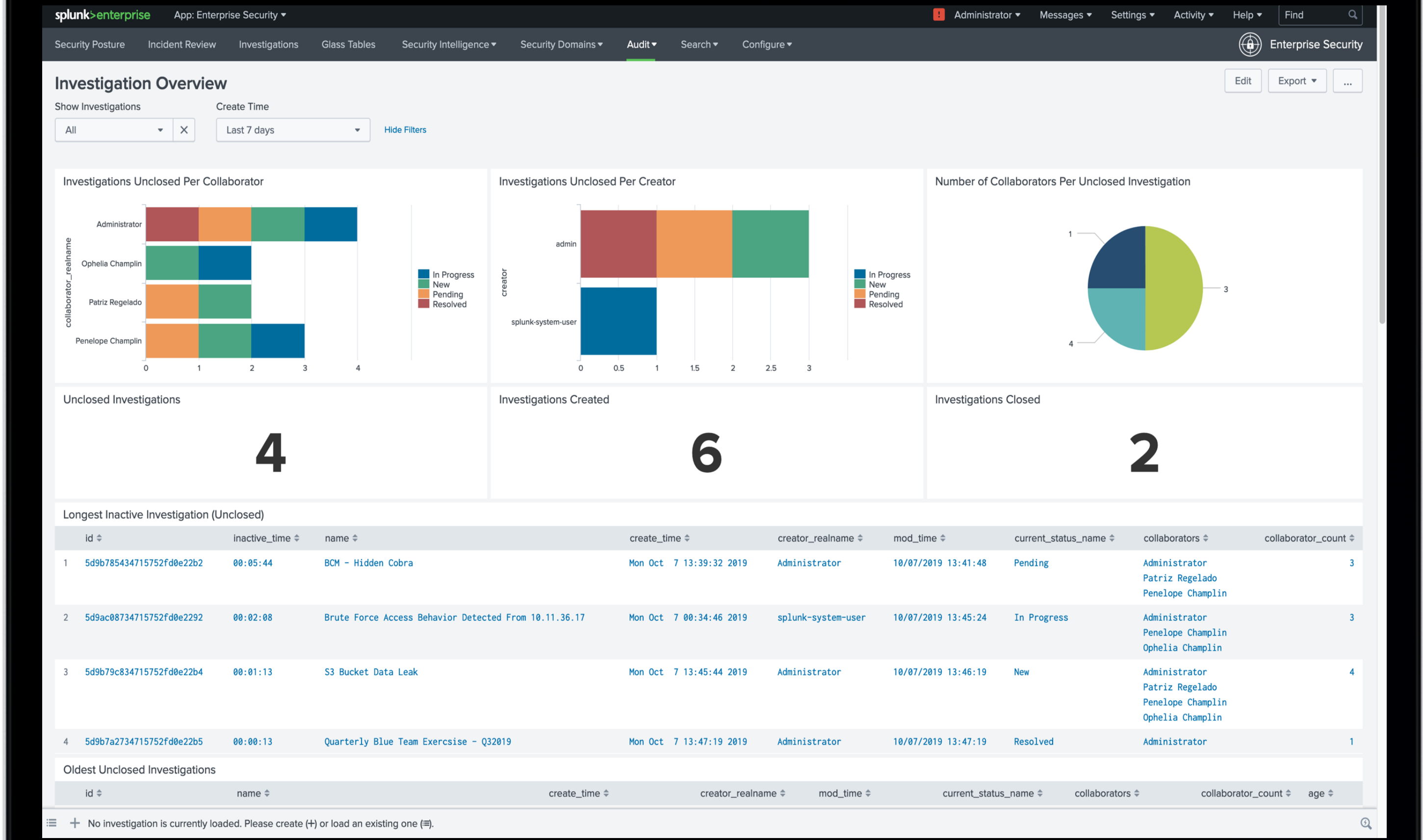
Splunk Enterprise Security

.conf19
splunk>

Splunk Enterprise Security 6.0

Analytics-driven Security Information Event Management (SIEM)

- Quickly gain visibility into a SOC team's investigations with key security metric reports
- Greater performance and ease of use for massive lookups
- Improved anomaly and threat detection with enhanced ML algorithms



Investigation Overview

Show Investigations: All

Create Time: Last 7 days

Unclosed Investigations: 4

Investigations Created: 6

Investigations Closed: 2

Longest Inactive Investigation (Unclosed)

	id	inactive_time	name	create_time	creator_realname	mod_time	current_status_name	collaborators	collaborator_count
1	5d9b785434715752fd0e22b2	00:05:44	BCM - Hidden Cobra	Mon Oct 7 13:39:32 2019	Administrator	10/07/2019 13:41:48	Pending	Administrator Patriz Regelado Penelope Champlin	3
2	5d9ac08734715752fd0e2292	00:02:08	Brute Force Access Behavior Detected From 10.11.36.17	Mon Oct 7 00:34:46 2019	splunk-system-user	10/07/2019 13:45:24	In Progress	Administrator Penelope Champlin Ophelia Champlin	3
3	5d9b79c834715752fd0e22b4	00:01:13	S3 Bucket Data Leak	Mon Oct 7 13:45:44 2019	Administrator	10/07/2019 13:46:19	New	Administrator Patriz Regelado Penelope Champlin Ophelia Champlin	4
4	5d9b7a2734715752fd0e22b5	00:00:13	Quarterly Blue Team Exercsise - Q32019	Mon Oct 7 13:47:19 2019	Administrator	10/07/2019 13:47:19	Resolved	Administrator	1

Oldest Unclosed Investigations

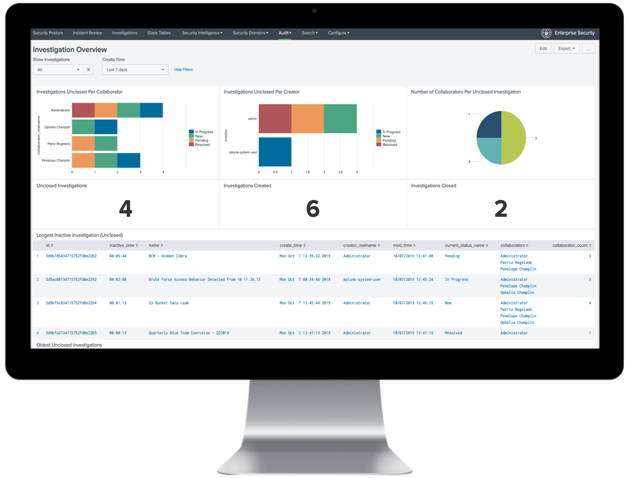
id	name	create_time	creator_realname	mod_time	current_status_name	collaborators	collaborator_count	age

No investigation is currently loaded. Please create (+) or load an existing one (☰).

Splunk Enterprise Security 6.0

Key Enhancements

Analytics Reporting on Investigations



Investigation Overview

Show Investigations: All

Create Time: Last 7 days

Unclosed Investigations: 4

Investigations Created: 6

Investigations Closed: 2

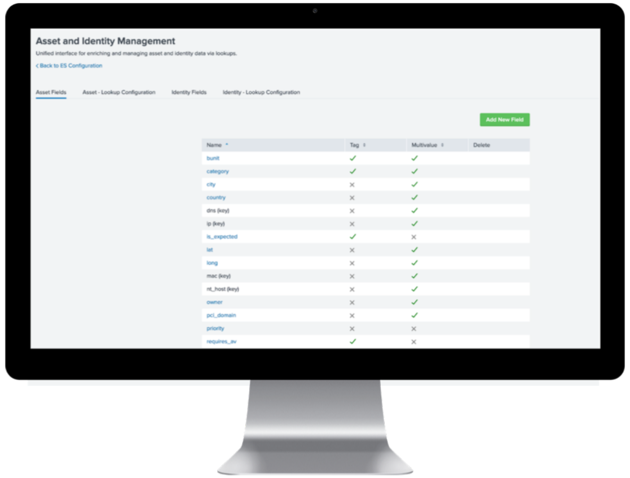
Longest Inactive Investigation (Unclosed)

	id	inactive_time	name	create_time	creator_realname	mod_time	current_status_name	collaborators	collaborator_count
1	5d9b785434715752fd0e22b2	00:05:44	BCM - Hidden Cobra	Mon Oct 7 13:39:32 2019	Administrator	10/07/2019 13:41:48	Pending	Administrator Patriz Regelado Penelope Champlin	3
2	5d9ac08734715752fd0e2292	00:02:08	Brute Force Access Behavior Detected From 10.11.36.17	Mon Oct 7 00:34:46 2019	splunk-system-user	10/07/2019 13:45:24	In Progress	Administrator Penelope Champlin Ophelia Champlin	3
3	5d9b79c834715752fd0e22b4	00:01:13	S3 Bucket Data Leak	Mon Oct 7 13:45:44 2019	Administrator	10/07/2019 13:46:19	New	Administrator Patriz Regelado Penelope Champlin Ophelia Champlin	4
4	5d9b7a2734715752fd0e22b5	00:00:13	Quarterly Blue Team Exercsise - Q32019	Mon Oct 7 13:47:19 2019	Administrator	10/07/2019 13:47:19	Resolved	Administrator	1

Oldest Unclosed Investigations

- Report on the number of investigations created/closed, oldest unclosed investigations, total time spent on investigations and more
- Exposed to SPL allowing you to tailor reports based on your SOC requirements
- Visibility into SOC team performance and efficiency

Asset and Identity Framework Enhancements


‹ Back to ES Configuration
Asset Fields
Asset - Lookup Configuration
Identity Fields
Identity - Lookup Configuration
Add New Field

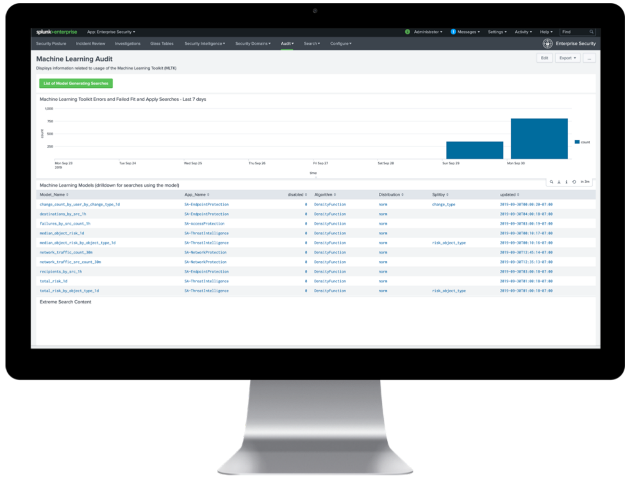
Asset and Identity Management

Unified interface for enriching and managing asset and identity data via lookups.

Name	Tag	Multivalue	Delete
bunit	✓	✓	
category	✓	✓	
city	✗	✓	
country	✗	✓	
dns (key)	✗	✓	
ip (key)	✗	✓	
is_expected	✓	✗	
lat	✗	✓	
long	✗	✓	
mac (key)	✗	✓	
nt_host (key)	✗	✓	
owner	✗	✓	
pci_domain	✗	✓	
priority	✗	✗	
requires_av	✓	✗	

- 2x performance improvements;
- 3x scale ; supports up to 2M entities
- Extensible fields for richer context enabling faster and more accurate investigations
- 5TB to 15TB ES Cloud, 30TB to 50TB on-prem ES 3x overall performance improvement in the last year

Splunk Machine Learning Tool Kit (MLTK) Integration



Machine Learning Audit

Displays information related to usage of the Machine Learning Toolkit (MLTK)

Machine Learning Models (drilldown for searches using the model)

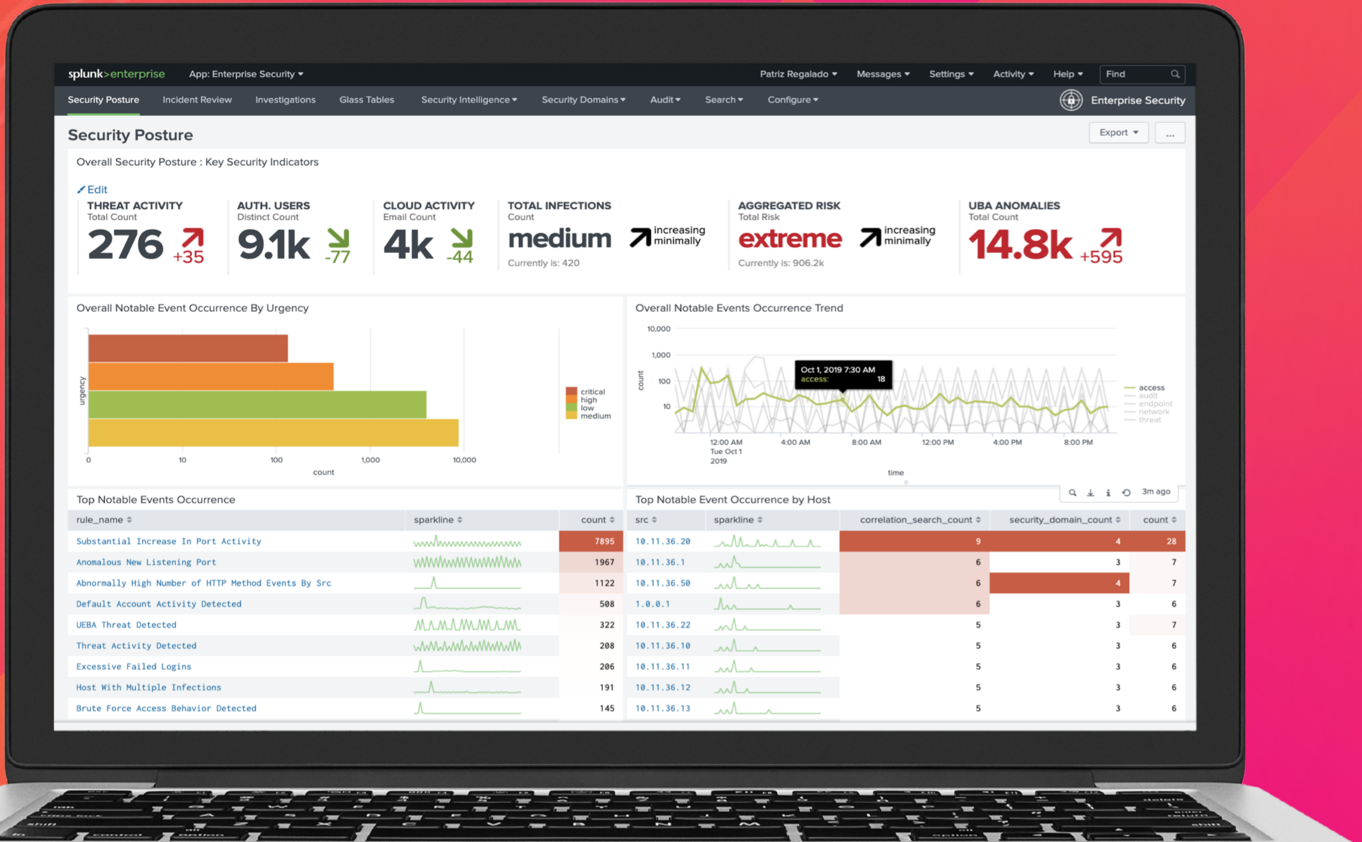
Model_Name	App_Name	disabled	Algorithm	Distribution	Splitby	updated
change_count_by_user_by_change_type_1d	SA-EndpointProtection	0	DensityFunction	norm	change_type	2019-09-30T00:00:20-07:00
destinations_by_src_1h	SA-EndpointProtection	0	DensityFunction	norm		2019-09-30T04:00:18-07:00
failures_by_src_count_1h	SA-AccessProtection	0	DensityFunction	norm		2019-09-30T03:00:19-07:00
median_object_risk_1d	SA-ThreatIntelligence	0	DensityFunction	norm		2019-09-30T00:10:17-07:00
median_object_risk_by_object_type_1d	SA-ThreatIntelligence	0	DensityFunction	norm	risk_object_type	2019-09-30T00:10:16-07:00
network_traffic_count_30m	SA-NetworkProtection	0	DensityFunction	norm		2019-09-30T12:45:14-07:00
network_traffic_src_count_30m	SA-NetworkProtection	0	DensityFunction	norm		2019-09-30T12:35:13-07:00
recipients_by_src_1h	SA-EndpointProtection	0	DensityFunction	norm		2019-09-30T03:00:18-07:00
total_risk_1d	SA-ThreatIntelligence	0	DensityFunction	norm		2019-09-30T01:00:18-07:00
total_risk_by_object_type_1d	SA-ThreatIntelligence	0	DensityFunction	norm	risk_object_type	2019-09-30T01:00:18-07:00

Extreme Search Content

- 20% performance improvement
- 10% improvement in accuracy and fewer notable events
- 10% improvement in correlation search performance

Splunk Enterprise Security

Quick Demo



Security Posture

Overall Security Posture : Key Security Indicators

THREAT ACTIVITY
Total Count
276 +35

AUTH. USERS
Distinct Count
9.1k -77

CLOUD ACTIVITY
Email Count
4k -44

TOTAL INFECTIONS
Count
medium increasing minimally
Currently is: 420

AGGREGATED RISK
Total Risk
extreme increasing minimally
Currently is: 906.2k

UBA ANOMALIES
Total Count
14.8k +595

Overall Notable Event Occurrence By Urgency

Overall Notable Events Occurrence Trend

Top Notable Events Occurrence

rule_name	sparkline	count
Substantial Increase In Port Activity		7895
Anomalous New Listening Port		1967
Abnormally High Number of HTTP Method Events By Src		1122
Default Account Activity Detected		508
UEBA Threat Detected		322
Threat Activity Detected		208
Excessive Failed Logins		206
Host With Multiple Infections		191
Brute Force Access Behavior Detected		145

Top Notable Event Occurrence by Host

src	sparkline	correlation_search_count	security_domain_count	count
10.11.36.20		9	4	28
10.11.36.1		6	3	7
10.11.36.50		6	4	7
1.0.0.1		6	3	6
10.11.36.22		5	3	7
10.11.36.10		5	3	6
10.11.36.11		5	3	6
10.11.36.12		5	3	6
10.11.36.13		5	3	6

What’s New

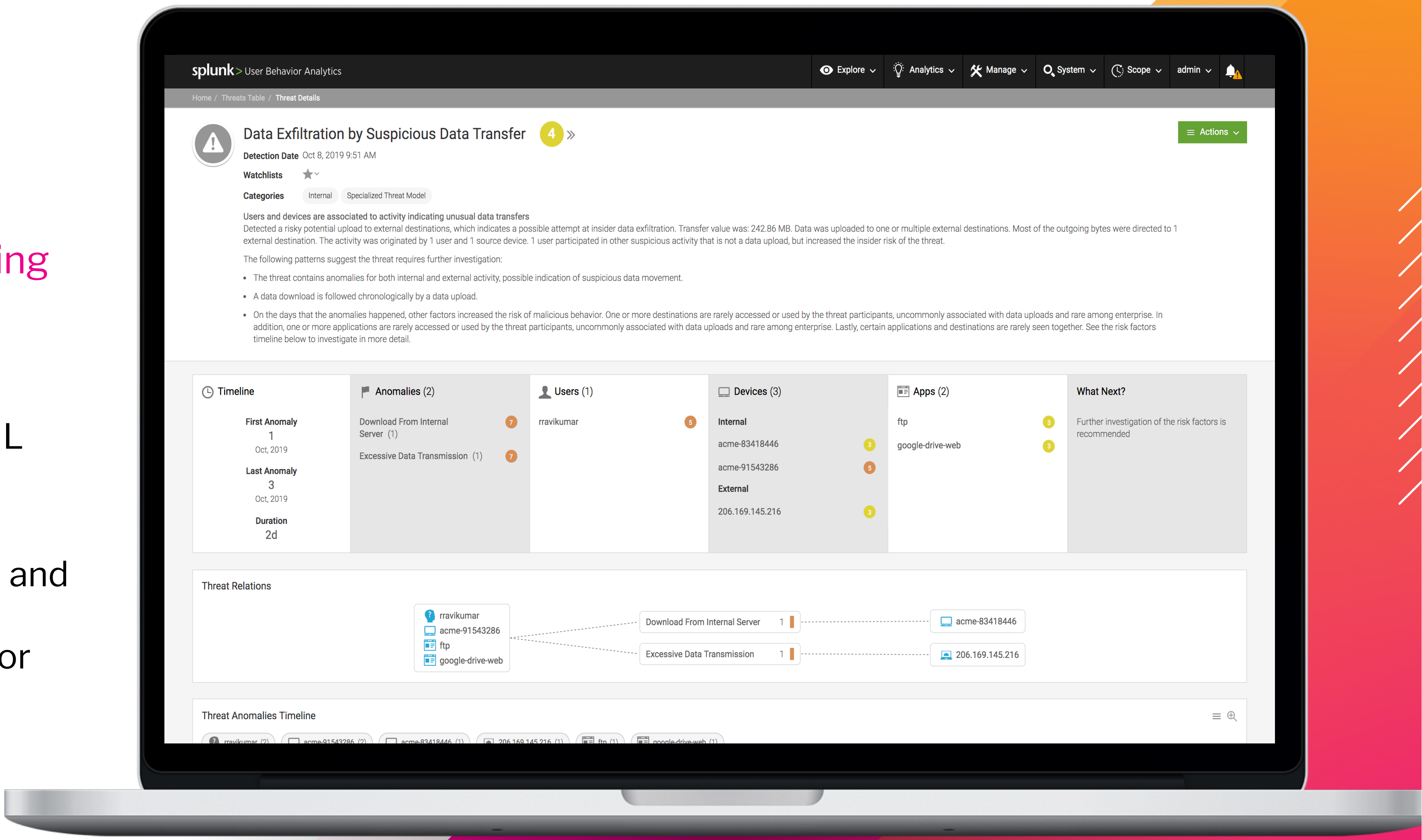
Splunk User Behavior Analytics

.conf19
splunk>

Splunk User Behavior Analytics 5.0

Detect Unknown Threats and Anomalous User Behavior Using Machine Learning

- Advanced customization of ML models for custom use case development
- Easily manage known devices and unknown assets resulting in performance improvements for large scale deployments
- Minimize data loss and SOC operational disruptions in the event of an outage


splunk> User Behavior Analytics
Explore
Analytics
Manage
System
Scope
admin
Home / Threats Table / Threat Details
Actions

Data Exfiltration by Suspicious Data Transfer 4

Detection Date Oct 8, 2019 9:51 AM

Watchlists

Categories Internal Specialized Threat Model

Users and devices are associated to activity indicating unusual data transfers
Detected a risky potential upload to external destinations, which indicates a possible attempt at insider data exfiltration. Transfer value was: 242.86 MB. Data was uploaded to one or multiple external destinations. Most of the outgoing bytes were directed to 1 external destination. The activity was originated by 1 user and 1 source device. 1 user participated in other suspicious activity that is not a data upload, but increased the insider risk of the threat.

The following patterns suggest the threat requires further investigation:

- The threat contains anomalies for both internal and external activity, possible indication of suspicious data movement.
- A data download is followed chronologically by a data upload.
- On the days that the anomalies happened, other factors increased the risk of malicious behavior. One or more destinations are rarely accessed or used by the threat participants, uncommonly associated with data uploads and rare among enterprise. In addition, one or more applications are rarely accessed or used by the threat participants, uncommonly associated with data uploads and rare among enterprise. Lastly, certain applications and destinations are rarely seen together. See the risk factors timeline below to investigate in more detail.

Timeline	Anomalies (2)	Users (1)	Devices (3)	Apps (2)	What Next?
First Anomaly 1 Oct, 2019 **Last Anomaly** 3 Oct, 2019 **Duration** 2d	Download From Internal Server (1) 7 Excessive Data Transmission (1) 7	rravikumar 5	**Internal** acme-83418446 3 acme-91543286 5 **External** 206.169.145.216 3	ftp 3 google-drive-web 3	Further investigation of the risk factors is recommended

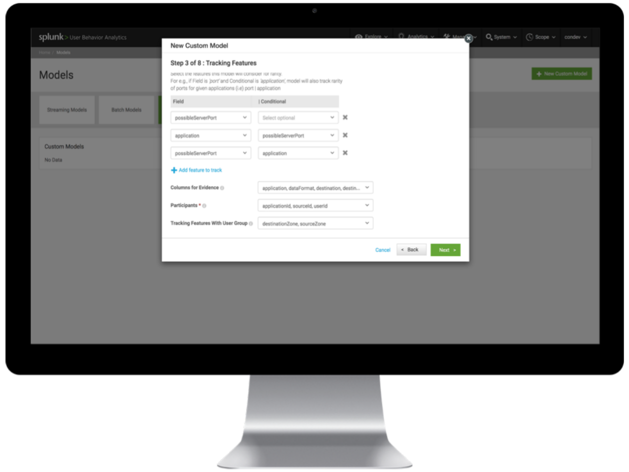
Threat Relations

Threat Anomalies Timeline

Splunk User Behavior Analytics 5.0

Key Enhancements

Custom Use Case Framework



New Custom Model

Step 3 of 8 : Tracking Features

Select the features this model will consider for rarity.
For e.g., if Field is 'port' and Conditional is 'application', model will also track rarity of ports for given applications (i.e) port | application

Field	Conditional
possibleServerPort	Select optional
application	possibleServerPort
possibleServerPort	application

+ Add feature to track

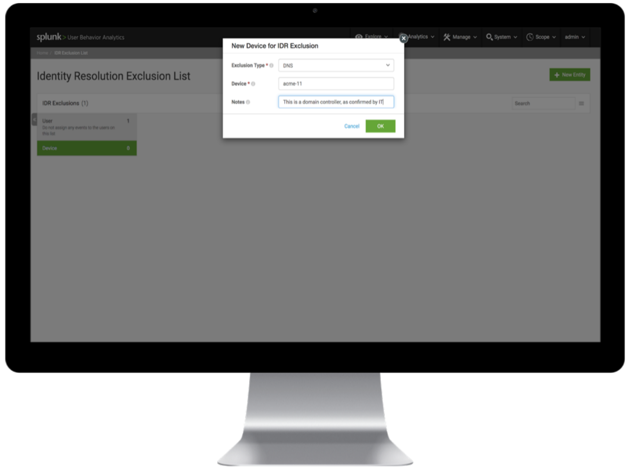
Columns for Evidence: application, dataFormat, destination, destin...

Participants *: applicationId, sourceId, userId

Tracking Features With User Group: destinationZone, sourceZone

- Develop your own machine learning models to generate custom content and create your own use cases
- Enables content developers to build a custom use case declaratively and without the need to define algorithms

Device Management



Identity Resolution Exclusion List

IDR Exclusions (1)

User 1 – Do not assign any events to the users on this list

Device 0

New Device for IDR Exclusion

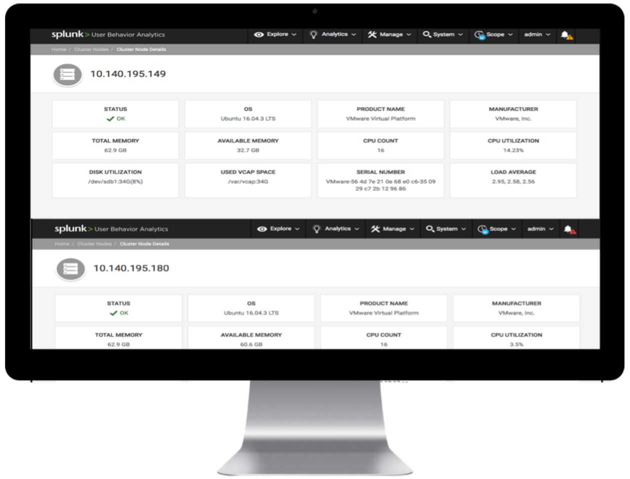
Exclusion Type *: DNS

Device *: acme-11

Notes: This is a domain controller, as confirmed by IT

- Easily manage unresolved devices assets discovered by UBA
- Seamlessly manage Identity Resolution exclusion lists maintaining quality of user and device associations
- Up to 4x performance improvements at large scale (1M+ devices)

High Availability and Disaster Recovery


splunk> User Behavior Analytics
Explore
Analytics
Manage
System
Scope
admin
Home / Cluster Nodes / Cluster Node Details

10.140.195.149

STATUS	OS	PRODUCT NAME	MANUFACTURER
✓ OK	Ubuntu 16.04.3 LTS	VMware Virtual Platform	VMware, Inc.

TOTAL MEMORY	AVAILABLE MEMORY	CPU COUNT	CPU UTILIZATION
62.9 GB	32.7 GB	16	14.23%

DISK UTILIZATION	USED VCAP SPACE	SERIAL NUMBER	LOAD AVERAGE
/dev/sdb1:34G(8%)	/var/vcap:34G	VMware-56 4d 7e 21 0e 68 e0 c6-35 09 29 c7 2b 12 96 86	2.95, 2.58, 2.56

10.140.195.180

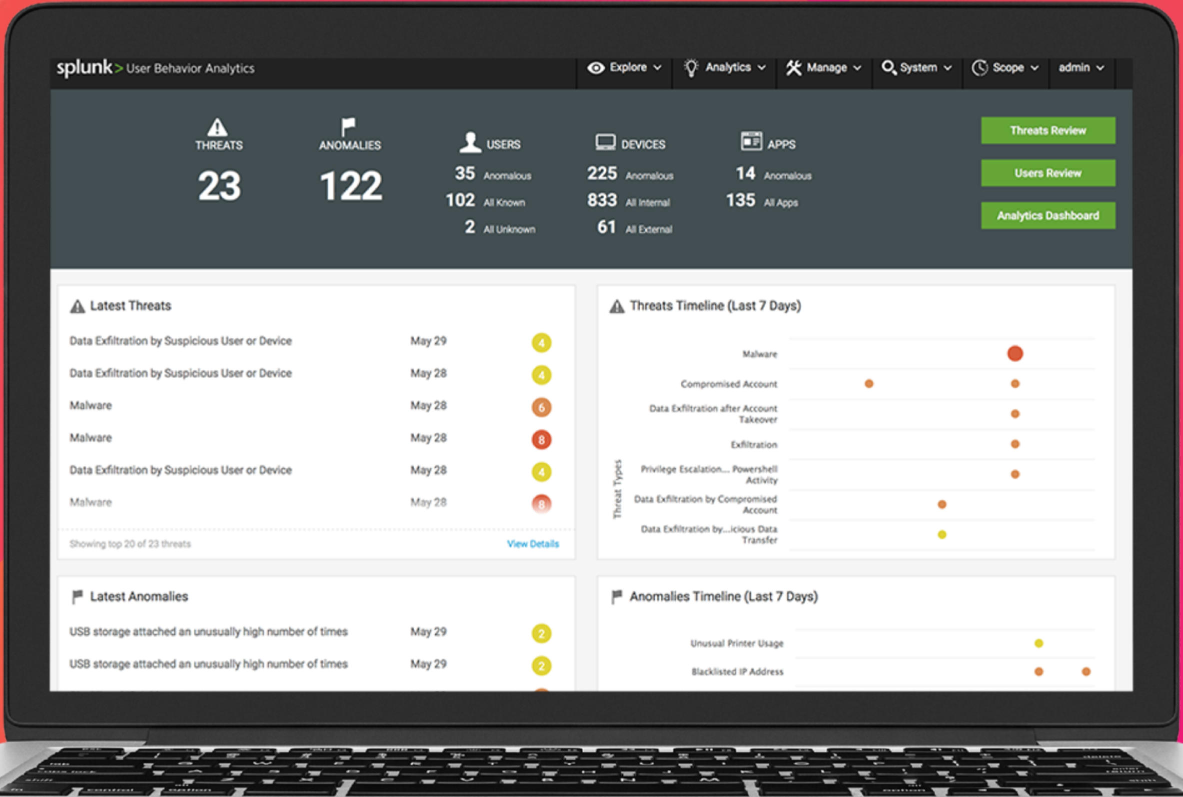
STATUS	OS	PRODUCT NAME	MANUFACTURER
✓ OK	Ubuntu 16.04.3 LTS	VMware Virtual Platform	VMware, Inc.

TOTAL MEMORY	AVAILABLE MEMORY	CPU COUNT	CPU UTILIZATION
62.9 GB	60.6 GB	16	3.5%

- Quick recovery in the event of an outage, minimizing data loss and SOC disruption

Splunk User Behavior Analytics

Quick Demo



splunk> User Behavior Analytics

Explore | Analytics | Manage | System | Scope | admin

THREATS 23

ANOMALIES 122

USERS
35 Anomalous
102 All Known
2 All Unknown

DEVICES
225 Anomalous
833 All Internal
61 All External

APPS
14 Anomalous
135 All Apps

Threats Review

Users Review

Analytics Dashboard

Latest Threats

Data Exfiltration by Suspicious User or Device	May 29	4
Data Exfiltration by Suspicious User or Device	May 28	4
Malware	May 28	6
Malware	May 28	8
Data Exfiltration by Suspicious User or Device	May 28	4
Malware	May 28	8

Showing top 20 of 23 threats

View Details

Threats Timeline (Last 7 Days)

Threat Types
Malware
Compromised Account
Data Exfiltration after Account Takeover
Exfiltration
Privilege Escalation... Powershell Activity
Data Exfiltration by Compromised Account
Data Exfiltration by...icious Data Transfer

Latest Anomalies

USB storage attached an unusually high number of times	May 29	2
USB storage attached an unusually high number of times	May 29	2

Anomalies Timeline (Last 7 Days)

What’s New

Splunk Phantom

.conf19
splunk>

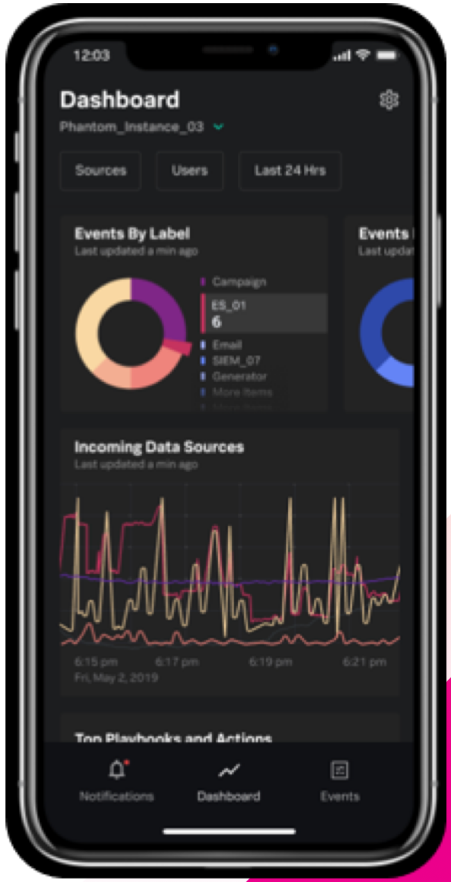
Splunk Phantom 4.6

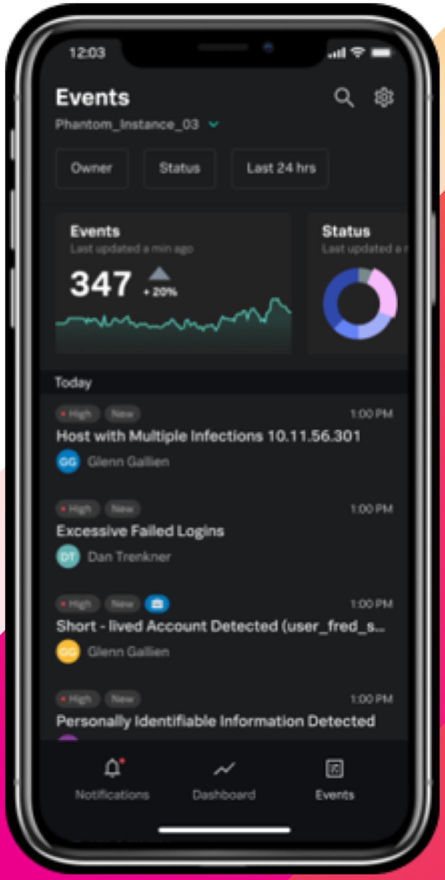
Work Smarter, Respond Faster, and Strengthen Your Defenses, Now From Anywhere at Anytime

- Phantom on Splunk Mobile brings the power of Phantom security orchestration, automation, and response (SOAR) capabilities to your mobile device
- Work smarter, respond faster, and strengthen your defenses, now from anywhere at anytime

Also:

- New User-Seat Pricing
- AWS Cloud Elasticity Support
- ITSI Monitoring of Phantom
- Support for Search Head Clustering for external search



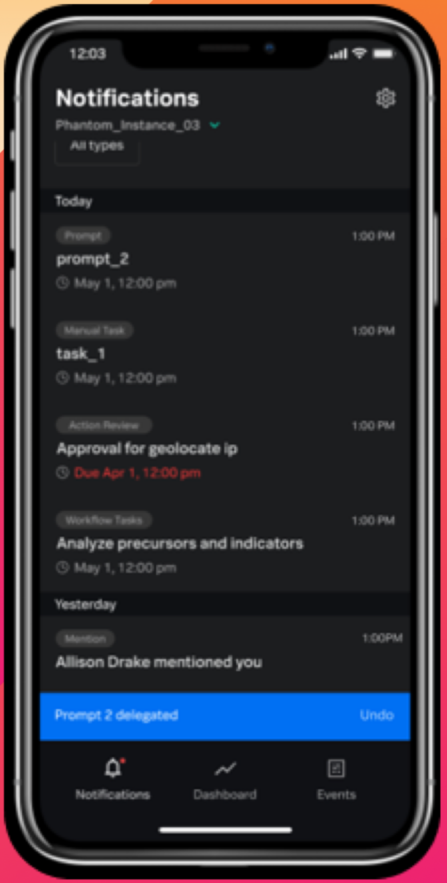


Host with Multiple Infections 10.11.56.301
Glenn Gallien

Excessive Failed Logins
Dan Trenkner

Short - lived Account Detected (user_fred_s...
Glenn Gallien

Personally Identifiable Information Detected



prompt_2
May 1, 12:00 pm

task_1
May 1, 12:00 pm

Approval for geolocate ip
Due Apr 1, 12:00 pm

Analyze precursors and indicators
May 1, 12:00 pm

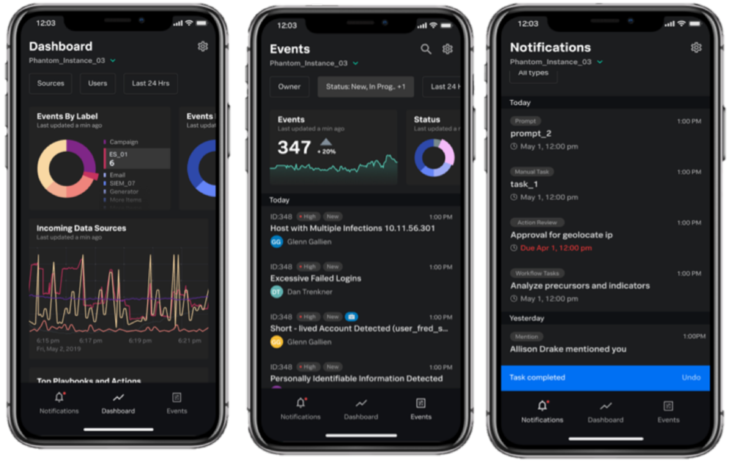
Allison Drake mentioned you

Prompt 2 delegated

Splunk Phantom 4.6

Key Enhancements

Phantom on Splunk Mobile



ID:348 High New 1:00 PM
Host with Multiple Infections 10.11.56.301
GG Glenn Gallien

ID:348 High New 1:00 PM
Excessive Failed Logins
DT Dan Trenkner

ID:348 High New 1:00 PM
Short - lived Account Detected (user_fred_s...
GG Glenn Gallien

ID:348 High New 1:00 PM
Personally Identifiable Information Detected

Prompt 1:00 PM
prompt_2
May 1, 12:00 pm

Manual Task 1:00 PM
task_1
May 1, 12:00 pm

Action Review 1:00 PM
Approval for geolocate ip
Due Apr 1, 12:00 pm

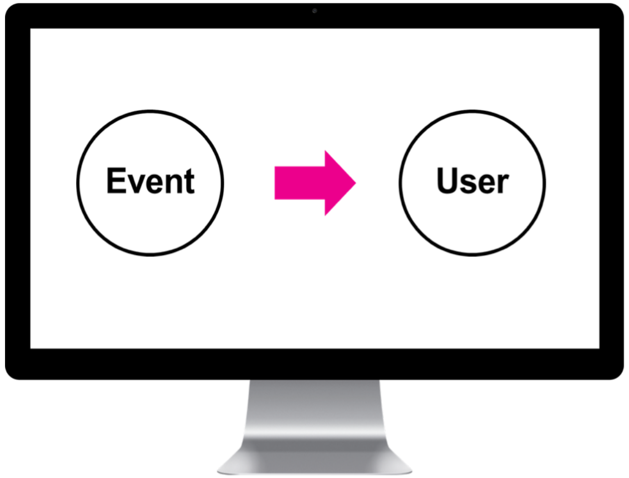
Workflow Tasks 1:00 PM
Analyze precursors and indicators
May 1, 12:00 pm

Mention 1:00PM
Allison Drake mentioned you

Task completed Undo

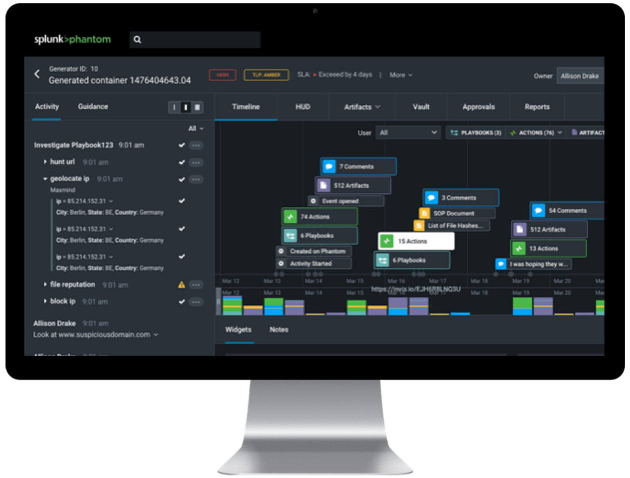
- Reduce mean time to response by addressing security notifications from anywhere at anytime
- Triage events; run and view playbooks on-the-go
- Collaborate with colleagues in real-time from the app

New User-Seat Pricing



- Annual subscription price determined by number of user accounts

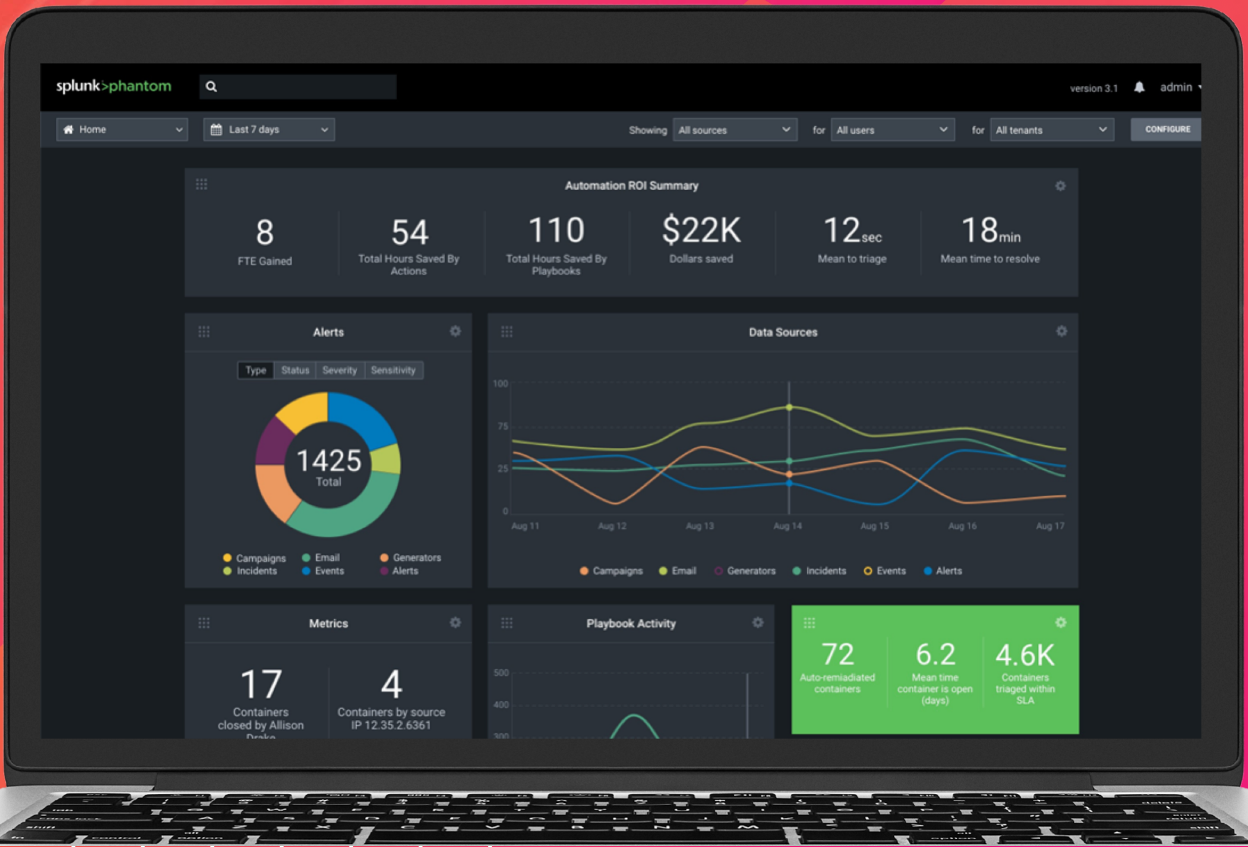
AWS Cloud Elasticity
ITSI Monitoring of Phantom
Support for SHC



- Supports cluster autoscaling and elasticity for AWS
- ITSI can monitor the health of Phantom environment
- Support for search head clustering for external search

Splunk Phantom

Quick Demo



Last 7 days

Showing All sources for All users for All tenants

Automation ROI Summary

8 FTE Gained

54 Total Hours Saved By Actions

110 Total Hours Saved By Playbooks

$22K Dollars saved

12sec Mean to triage

18min Mean time to resolve

1425 Total

Metrics

17 Containers closed by Allison Drake

4 Containers by source IP 12.35.2.6361

72 Auto-remiadiated containers

6.2 Mean time container is open (days)

4.6K Containers triaged within SLA

Advancing Your Security Journey

Get Hands-on

Mission Control Deep Dive
Wed @ 2:15pm

Download Upgrades

Available on Splunkbase

Get Started for Free

splunk> essentials for Security

350+ security use cases available on Splunkbase

Stay Current

splunk> content updates

Pre-packaged security content from the Splunk Research Team

Extend the Power of Splunk

splunkbase™ + Phantom Community

1000+ apps and add-ons from Splunk, our partners, and our community

Q&A

.conf19
splunk>

.conf19®

splunk>®

Thank You!