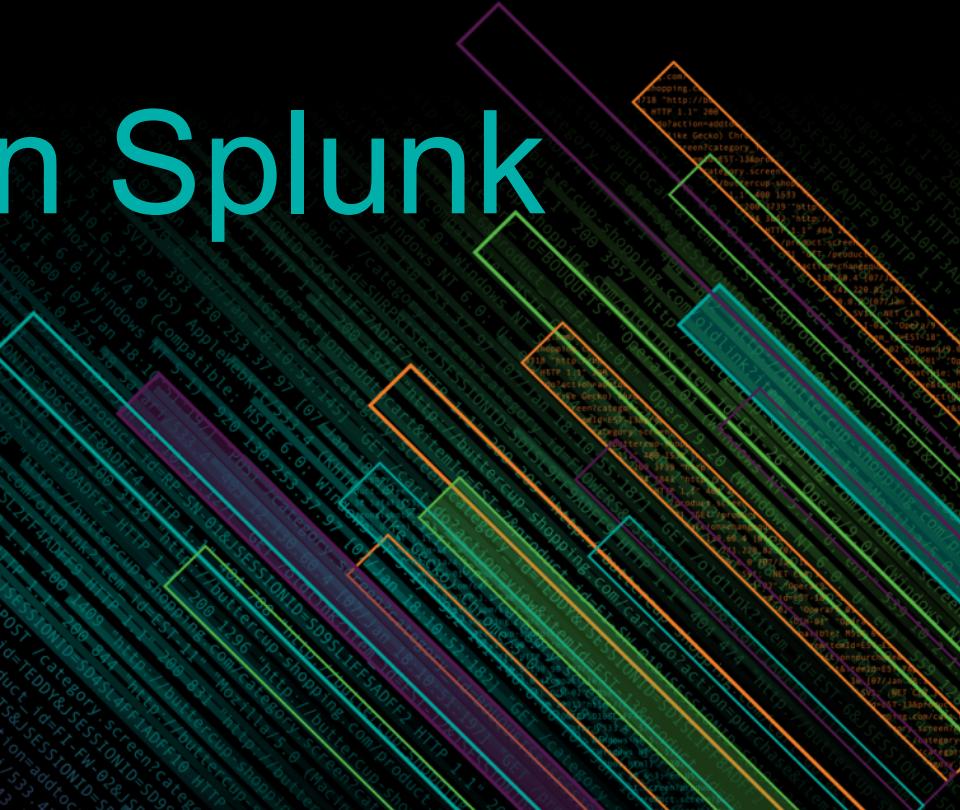




**splunk®**

# 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 the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, 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. © 2018 Splunk Inc. All rights reserved.

# Hello!

## Meet your Splunkers



**Maritza Perez**  
Director, Product Management



**Girish Bhat**  
Director, Product Marketing



**Prasoon Shukla**  
Sr. Product Manager



**Patriz Regalado**  
Sr. Product Marketing Manager



**Rob Truesdell**  
Director, Product Management



**Chris Simmons**  
Sr. Product Marketing Manager

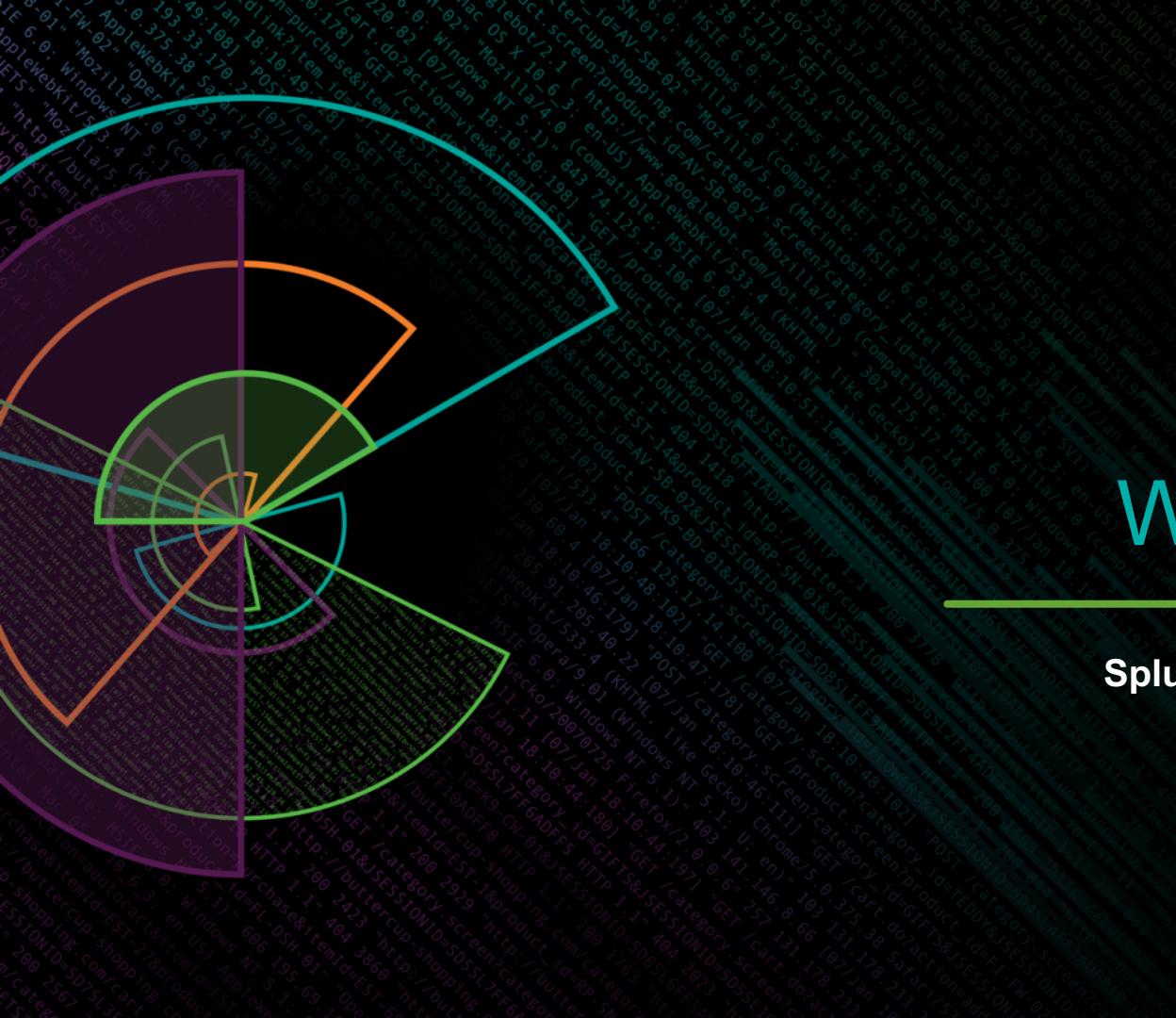
# Splunk for Security Portfolio



splunk> .conf18

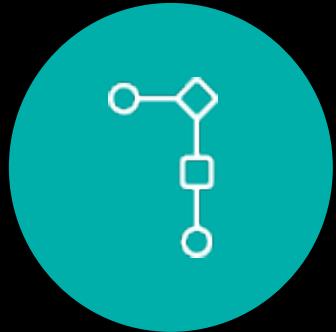
# What's New

## Splunk Enterprise Security

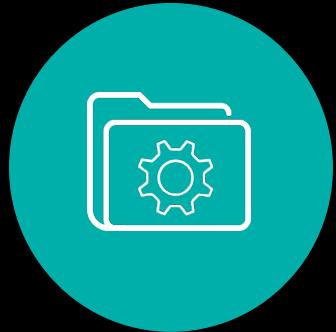


# Splunk Enterprise Security 5.2

ES 5.2



# Event Sequencing



# Use Case Library



# Investigation Workbench

# Event Sequencing

## Optimize Threat Detection and Accelerate Investigation

- ▶ Helps identify actionable threats
- ▶ Improves fidelity of threats detected
- ▶ Sequence correlation searches and risk modifiers
- ▶ Review within *Incident Review* and take investigative or response steps

Sequence Template

Name: Event Sequence #1

Description: Optional

App: Enterprise Security

Defines the app in which the .conf entries will be created.

Start

Correlation Search: Endpoint - Host With Multiple Infections - Rule

Expression:

! Fill in all transition fields.

State:  + Add State

Transitions

Enforce Ordering:  Enforces chronological order of transitions, otherwise just checks for existence. Saving state on transitions is disabled when ordering is disabled.

Aggregate Matches:  Keep accumulating matched events while template is running.

+ Add Transition

# Use Case Library

## Faster Detection and Incident Response

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

**Use Cases**

- Abuse
- Adversary Tactics
- Best Practices
- Cloud Security
- Malware
- Vulnerability

Framework Mapping:	All	(5+)	Data Model:	All	(App:	All	In User:	All	Bookmarked:	All	More...
S-A	Analytic Story	Cloud Security, Best Practices, Vulnerability, Abuse, Adversary Tactics, Malware	Cloud Security								
>	AWS Cross Account Root	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	
>	AWS Cryptomining	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	
>	AWS Network ACL Activity	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	
>	AWS Suspicious Processing Activities	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	
>	AWS User Monitoring	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	Cloud Security	
>	Account Monitoring and Control	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	
>	Apache Struts Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Vulnerability	
>	Asset Testing	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	Best Practices	
>	Brand Monitoring	Abuse	Abuse	Abuse	Abuse	Abuse	Abuse	Abuse	Abuse	Abuse	
>	Collection and Staging	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	
>	Command and Control	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	Adversary Tactics	
>	DHS Report TA00-07A	Malware	Malware	Malware	Malware	Malware	Malware	Malware	Malware	Malware	

Discover new use cases and determine which ones can be used within your environment right away

Create, curate, install, and manage content, Analytic Stories and third-party created content

**Detection Searches**

- **ESCU - AWS Network Access Control List Created with All Open Ports** [edit]
- **ESCU - AWS Network Access Control List Deleted** [edit]
- **ESCU - Detect Spike in blocked Outbound Traffic from your AWS** [edit]
- **ESCU - Detect Spike in Network ACL Activity** [edit]

**Data Sources**

- **awscloudtrail**
- **awsdescription**
- **awsconfig**
- **awscloudwatchlogsgefcpflow**

**Data Models**

- No items found

**Lookups**

- **awscloudwatchlogs\_lookup**
- **governance\_lookup**
- **incident\_review\_comment\_lookup**
- **incident\_review\_lookup**
- **notable\_wrt\_lookup**

**Framework Mapping**

ATTACK Persistence Elevation Command and Control

KILL CHAIN PHASES Actions on Objectives Command and Control

CIS 20 CIS 19 CIS 18 CIS 16

NIST DEMP DEAR DEIC PEAC PRCS

# Investigation Workbench

## Reduce Time to Contain and Remediate

- ▶ Supports new artifacts for use during incident investigation
- ▶ New artifact types (file and URL)
- ▶ Use artifacts when creating a panel or while exploring

The screenshot shows the Splunk Investigation Workbench interface. At the top, there's a header with 'WS1' and navigation tabs for 'Workbench', 'Timeline', and 'Summary'. Below this is a sidebar titled 'Artifacts' with a message '1 out of 1 is selected.' and a 'Filter artifacts' input field. The main area has tabs for 'Context', 'Endpoint Data', 'Network Data' (which is selected), and 'Add Content'. A sub-section titled 'Web Activity' displays a table of network events. The table columns are 'src', 'dest', 'user', 'http\_referer', and 'url'. The data in the table includes various URLs from 'http://192.168.229.156/admin/config.php' and file paths like '/wp-content/themes/twentyfifteen/'. There are also entries for 'forgotpassword.php' and 'joomla12/plugins/editors/tinymce/scripts/tiny\_mce/plugins/tinybrowser/upload.php?type=folder'. The bottom of the interface has buttons for '+ Add Artifact' and 'Explore'.

# Splunk Enterprise Security

## Quick Demo

The screenshot shows the Splunk Enterprise Security interface running on a laptop. The dashboard is titled "Security Posture" and displays the following key indicators:

- THREAT ACTIVITY**: Total Count **768** (decreasing minimally)
- AUTH. USERS**: Distinct Count **3.7k** (decreasing minimally)
- CLOUD ACTIVITY**: Email Count **2.9k** (increasing +6)
- INFECTED SYSTEMS**: System Count **219** (0)
- UNIQUE DESTINATIONS**: Unique Count **39k** (increasing +59)
- AGGREGATED RISK**: Total Risk **extreme** (increasing minimally, currently 421.7k)

Below these metrics are two charts:

- Overall Notable Event Occurrence By Urgency**: A bar chart showing event counts for critical, high, low, and medium urgency levels. The counts are approximately 100, 150, 1200, and 1500 respectively.
- Overall Notable Events Occurrence Trend**: A line graph showing the count of events over time from April 24 to April 25. The graph tracks four categories: access (blue), audit (orange), endpoint (green), and network (yellow).

The laptop's taskbar at the bottom shows several open windows, including a command prompt and a browser tab for Splunk documentation.

# What's New

# Splunk User Behavior Analytics

# Splunk User Behavior Analytics (UBA)

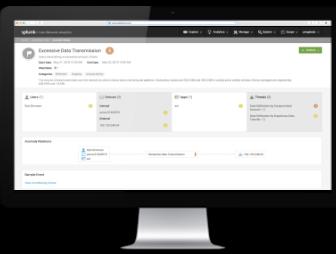
UBA

# Detect Unknown Threats and Anomalous User Behavior using Machine Learning

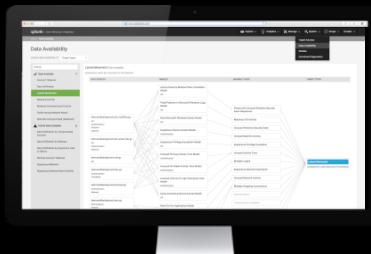
# Container-based Architecture



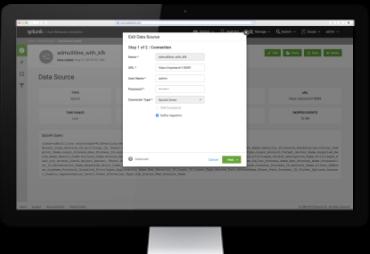
## Advanced Investigation



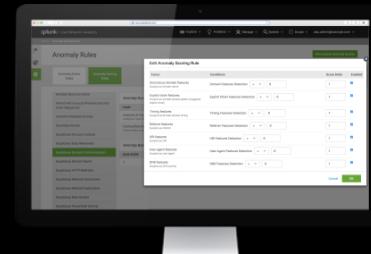
## Data Availability



## Enhanced Data Ingestion



## User Feedback Learning



# Greater Scalability for Insider Threat Detection

## Container-based Architecture

20

## Cluster Nodes

**80K**

## Events per Second

**750K**

## Accounts Monitored

1M

## Devices Monitored



# kubernetes



docker

# Enhanced Investigation with Splunk

## Drill Down into Raw Events

## Drill down into triggering events

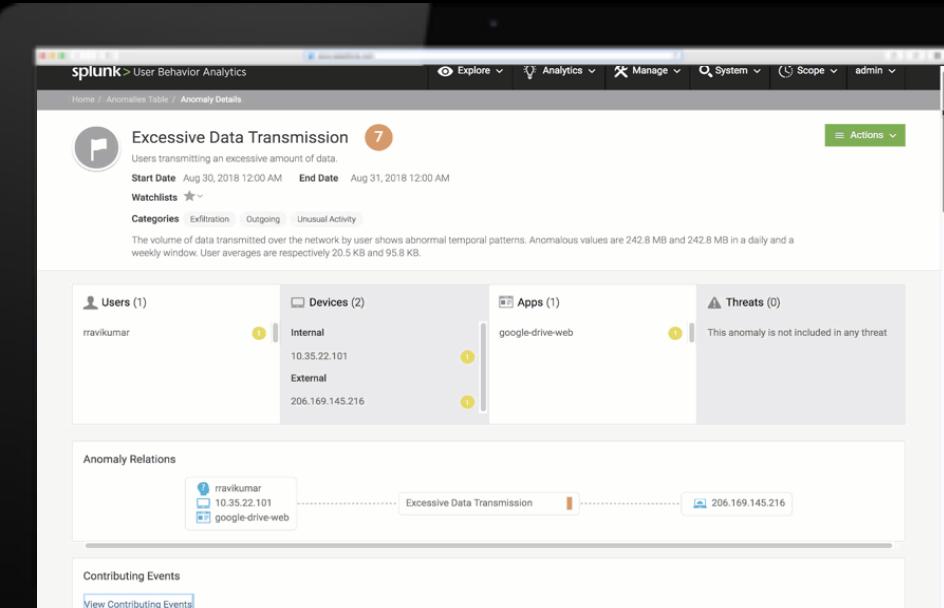
Investigation starts in UBA and continues in core

# Targeted hunting using automated SPL

Leverages anomaly data from users and assets

### **Collect more supporting evidence**

Further your investigation with focused timestamps



# Data Availability Validation

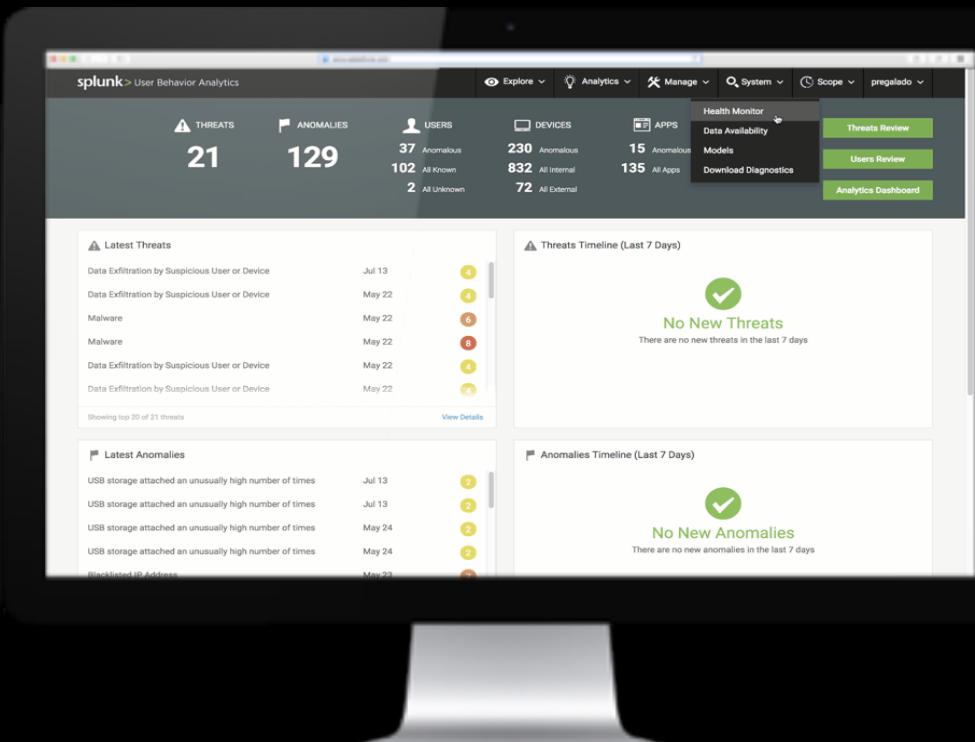
## Quickly Validate Your Data Ingestion

**View relationships across data sources**

Map models and anomalies to generated threat

**Identify missing data sources**

Gain additional scope and context of threats



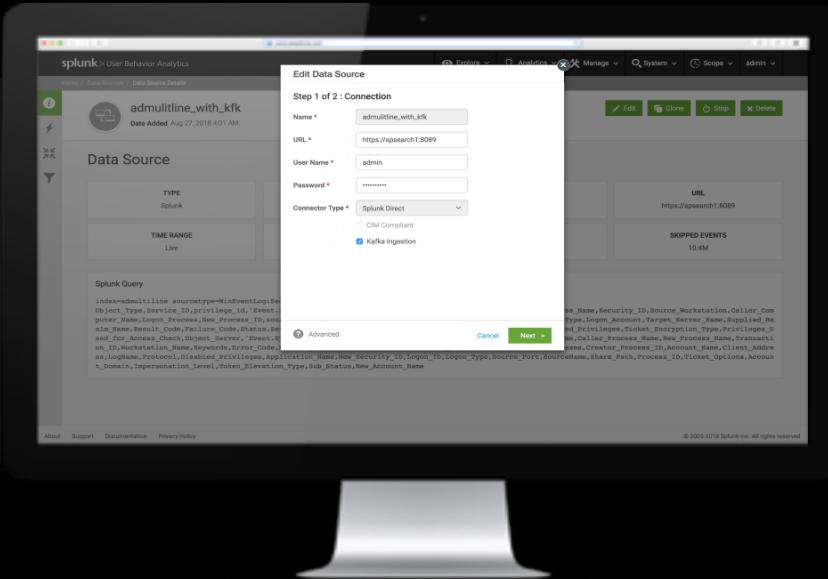
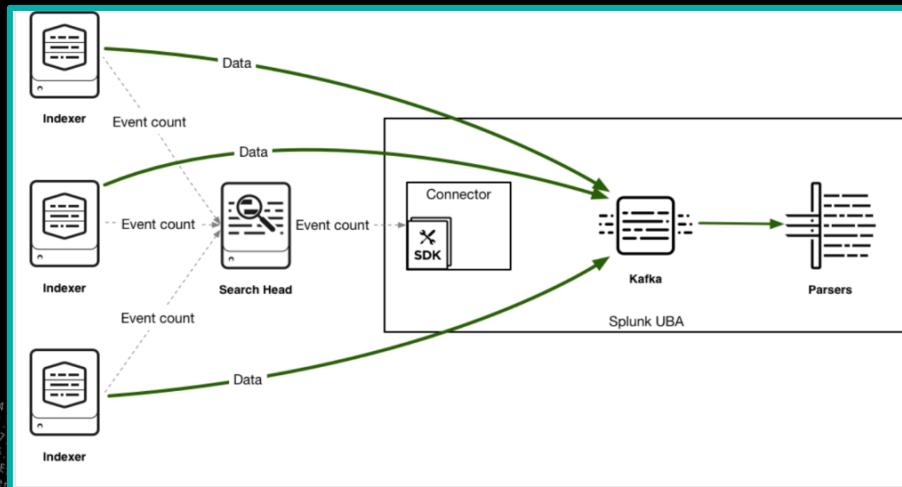
# Splunk-to-UBA Kafka Connector

## Data Ingestion Performance Doubled

Ingest data directly from Splunk indexers to Kafka messaging queue

Strengthen data quality and efficacy

For all machine learning and rule-based detection models



# User Feedback Learning

## Increase Threat Detection Accuracy and Anomaly Customization

### Provide granular feedback to anomaly models

Anomaly scoring rules per anomaly type

### Control overall threat detection severity and confidence

Tune scoring weights up/down for each model feature

### Customize anomaly models

Based on your enterprise policies

The screenshot displays the Splunk User Behavior Analytics (UBA) interface. At the top, there's a navigation bar with links for Explore, Analytics, Manage, System, Scope, and a user account (admin). Below the navigation is a search bar labeled "Search". The main area is titled "Anomalies Table" and shows a list of anomalies grouped by type. The list includes:

- All Anomalies (34)
- Scanning Activity (23)
- Suspicious Network Connection (10)**
- Excessive Data Transmission (1)
- Blacklisted Application (0)
- Blacklisted Domain (0)
- Blacklisted IP Address (0)
- Brute Force Attack (0)
- Download From Internal Server (0)
- Excessive Box Downloads (0)
- External Alarm (0)

Below the table is a "Anomalies Trend" chart showing the number of anomalies over time from October 2017 to September 2018. The chart shows a steady increase in anomalies, particularly towards the end of the period.

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE
Suspicious Network Connection	10.112.5.120 52.14.20.51 ssh	SSH Reverse Shell	Oct 18, 2017 8:56 PM	8
Suspicious Network Connection	sbenson 10.50.15.50 67.168.142.51 ntp	NTP Data Transfer	Sep 2, 2018 2:19 PM	7
Suspicious Network Connection	bstruthers 10.2.4.117	DNS Data Transfer	Sep 2, 2018 3:48 PM	7

# Splunk UBA Content Updates

Stay Ahead of Advanced and Insider Threats



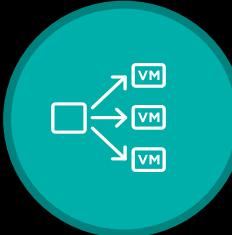
## Account Takeover

Disabled account activity  
Terminated user activity  
Interactive logins by svc accounts  
VPN logins by svc accounts



## Suspicious Behavior

Suspicious badge activity  
Account recovery detection



## Lateral Movement

Suspicious account lockout  
Privilege escalation after PowerShell activity  
Local account creation  
Password policy circumvention  
Multiple auths and failures



## Cloud Security

High downloads  
High deletions  
Unusual file access



## External Alarm

Aggregation of external alarms with security analytics



## Security Context

Behavior-based fingerprinting of user roles and assets

## Data Exfiltration

Unusual USB device  
High USB attachments

File relay  
Data destruction  
Data collection  
Watering hole  
Suspicious new access

# Splunk User Behavior Analytics

## Quick Demo

The screenshot displays the Splunk User Behavior Analytics interface on a laptop screen. The top navigation bar includes links for Explore, Analytics, Manage, System, Scope, and admin. Below the header is a summary dashboard with counts for Threats (23), Anomalies (122), Users (35 Anomalous, 102 All Known, 2 All Unknown), Devices (225 Anomalous, 833 All Internal, 61 All External), and Apps (14 Anomalous, 135 All Apps). Three green buttons on the right provide links to Threats Review, Users Review, and the Analytics Dashboard.

**Latest Threats:**

Threat Type	Date	Count
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 Type	Timeline
Malware	May 29
Compromised Account	May 28
Data Exfiltration after Account Takeover	May 28
Exfiltration	May 28
Privilege Escalation... Powershell Activity	May 28
Data Exfiltration by Compromised Account	May 28
Data Exfiltration by...icious Data Transfer	May 28

**Latest Anomalies:**

Anomaly Type	Date	Count
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):**

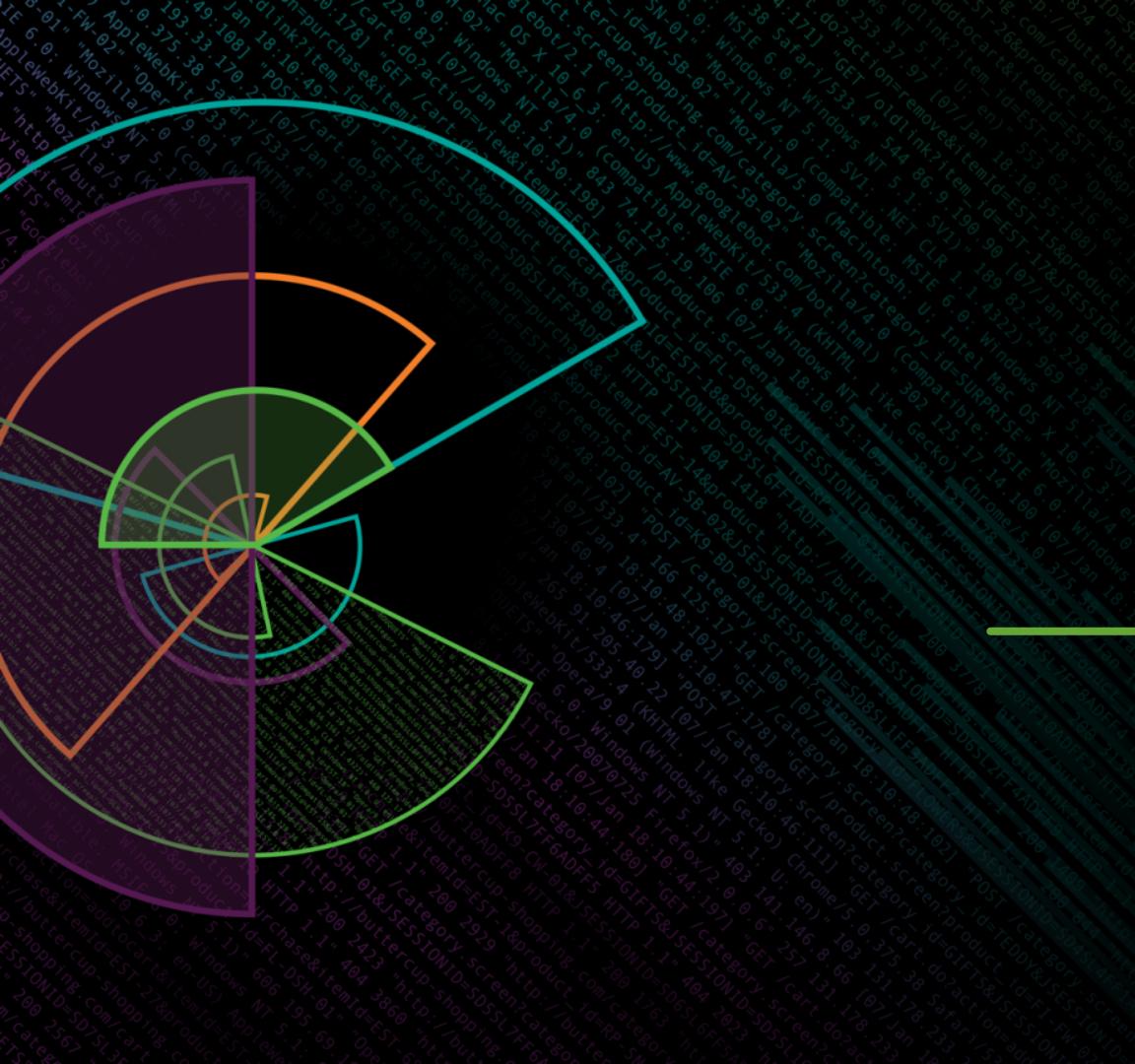
Anomaly Type	Timeline
Unusual Printer Usage	May 29
Blacklisted IP Address	May 28
Blacklisted IP Address	May 27

**Bottom Left:** A snippet of log data from a file named `putter.log` shows various user interactions and system events.

**Bottom Right:** The Splunk logo with the text ".conf18" in a speech bubble.

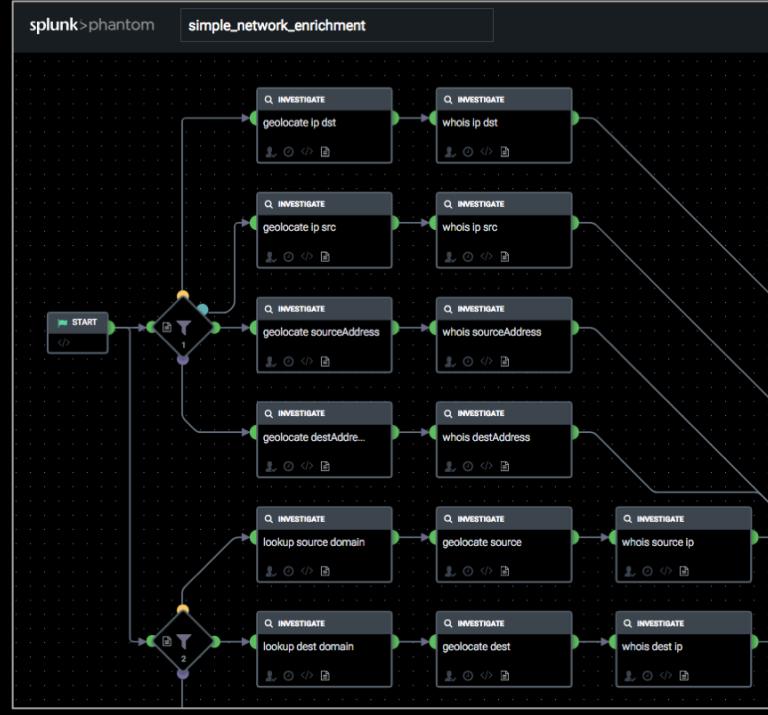
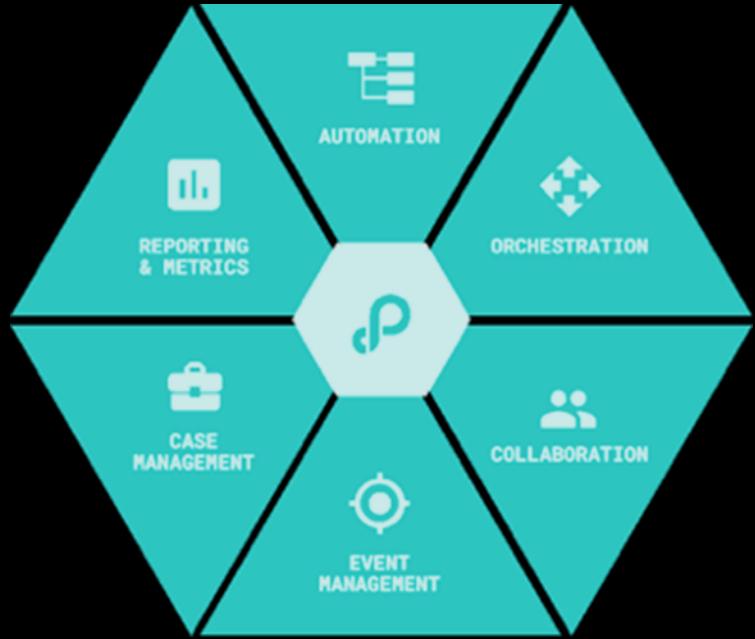
# What's New

Splunk Phantom



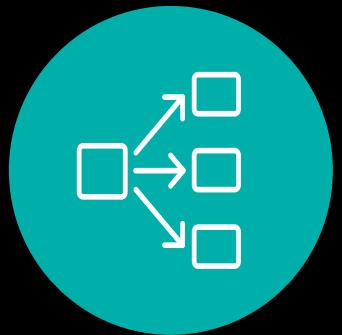
# Splunk Phantom

## Security Orchestration, Automation, and Response



# Splunk Phantom 4.0

**PHANTOM  
4.0**



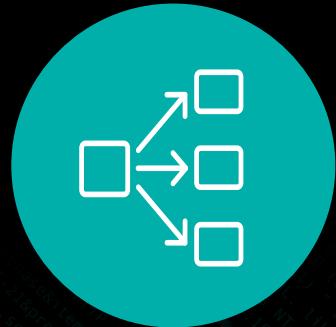
# Clustering Support



# Indicator View



# Splunk Search & Storage



# Clustering

▶ Scale performance as needs grow  
▶ Add redundancy for greater availability

splunk>phantom

Administration Company Settings Product Settings User Management System Health

## Clustering

### Nodes (3)

Online	Active since 0 minutes ago	Enabled:
10.209.34.45	Active since 0 minutes ago	ON <input checked="" type="button"/>
<a href="#">System health</a> <a href="#">View</a>		

Online	Active since 0 minutes ago	Enabled:
10.209.34.32	Active since 0 minutes ago	ON <input checked="" type="button"/>
<a href="#">System health</a> <a href="#">View</a>		



# Indicator View

Gain deeper insights into your data

Approach incidents from an indicator perspective

Drill Down to see indicator details

**splunk>phantom**

Indicators Last 30 days

Events Indicators Cases

Search indicator values

Indicator Count

159 Unique Indicators    4.04K Total Indicators

Top Indicators

80	507
4286	504
120	490

Top Types

port (blue), ip (green), hash (purple)

INDICATOR	TYPE	TOTAL EVENTS	OPEN EVENTS	SEVERITY	TAGS
test artifact label		2	2	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	
test artifact data		2	2	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	
www.badurl.com	host name	3	2	<div style="width: 66.66%; height: 10px; background-color: #ccc;"></div>	
144.21.34.155	ip	3	2	<div style="width: 66.66%; height: 10px; background-color: #ccc;"></div>	
10.10.1.201	ip	3	2	<div style="width: 66.66%; height: 10px; background-color: #ccc;"></div>	
http://gxtuookbjnyo.co.uk/home/	url	3	2	<div style="width: 66.66%; height: 10px; background-color: #ccc;"></div>	
854abcc4ea75ae38fe2765fd3e205af3	hash	3	2	<div style="width: 66.66%; height: 10px; background-color: #ccc;"></div>	



# Splunk Search and Storage

Only SOAR platform  
with integrated Splunk  
search support

Supports existing  
Splunk datastores for  
single source of truth

splunk>phantom

Q zeus

Home ▾

Containers  Artifacts  Actions  Assets  Apps  Docs  Other

11 or more results found containing "zeus"

[EVENTS] Zeus Infection on 10.17.1.201  
16 minutes ago Status: Open, Severity: **High** Sensitivity: **TLP: Green**, Description: Zeus infection has been detected on our system running at 10.17.1.201 running on ESXi server 10.1.16.157

[EVENTS] Zeus Infection on 10.17.1.201  
17 minutes ago Status: Open, Severity: **High** Sensitivity: **TLP: Amber**, Description: Zeus infection has been detected on our system running at 10.17.1.201 running on ESXi server 10.1.16.157

[EVENTS] Zeus Infection on 10.17.1.201  
18 minutes ago Status: Open, Severity: **High** Sensitivity: **TLP: Green**, Description: Zeus infection has been detected on our system running at 10.17.1.201 running on ESXi server 10.1.16.157

[EVENTS] Zeus Infection on 10.10.0.202  
18 minutes ago Status: Closed, Severity: **High** Sensitivity: **TLP: Red**, Description: Zeus infection has been detected on our system running at 10.10.0.202 running on ESXi server 10.1.16.157

[EVENTS] Zeus Infection on 10.17.1.201  
18 minutes ago Status: Closed, Severity: **High** Sensitivity: **TLP: Amber**, Description: Zeus infection has been detected on our system running at 10.17.1.201 running on ESXi server 10.1.16.157

[EVENTS] Zeus infection on HQ finance server  
19 minutes ago Status: Open, Severity: **High** Sensitivity: **TLP: Green**, Description: Network anomaly detection detected Zeus C&C traffic patterns emitting from the finance file server in HQ

[EVENTS] Zeus Infection on 10.10.0.202  
19 minutes ago Status: Open, Severity: **High** Sensitivity: **TLP: White**, Description: Zeus infection has been detected on our system running at 10.10.0.202 running on ESXi server 10.1.16.157

[EVENTS] Zeus Infection on 10.17.1.201

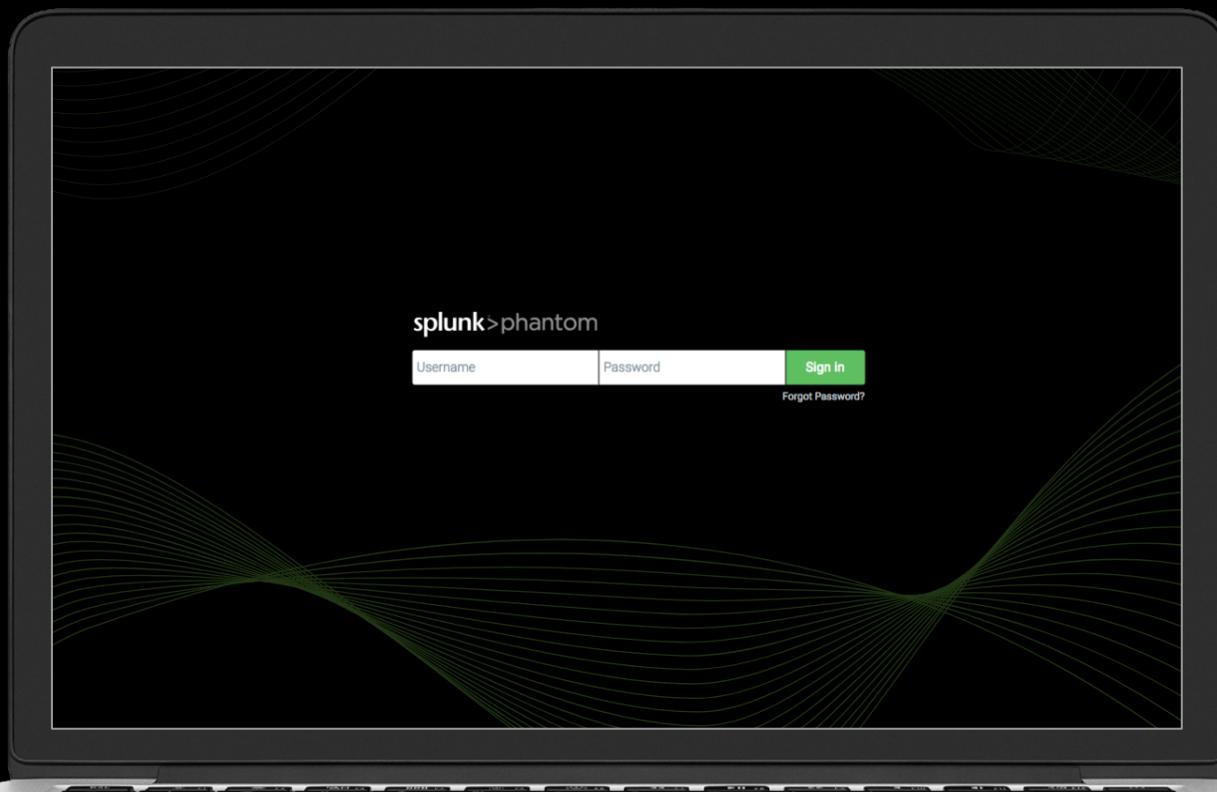
# Additional Features

visit the Phantom Community to learn more about the Splunk Phantom 4.0 release

- ▶ User Management UI
- ▶ New Onboarding Tour
- ▶ Concurrent Viewing of Multiple Artifacts
- ▶ Revamped Notifications View
- ▶ Filtering of Custom Fields in Analyst Queue
- ▶ Playbook Import Wizard
- ▶ Artifact Search in Mission Control
- ▶ Requiring Notes on Task Completion
- ▶ ROI Summary Changes
- ▶ Support for Thycotic Secret Server
- ▶ Debug log for entry and exit out of Python
- ▶ Dashboard Permissions
- ▶ Case Template Descriptions
- ▶ Indicator Info in Contextual Menu
- ▶ Searchable Notes

# Splunk Phantom

## Quick Demo



# Get More with Splunk

Splunk for Security



# Advancing Your Security Journey

Download  
Upgrades

splunk®  
essentials  
for Security

splunk®  
content  
updates

splunkbase™  
+ Phantom  
Community

# Questions?

# Thank You!

Don't forget to **rate** this session  
in the .conf18 mobile app

.conf18  
splunk>