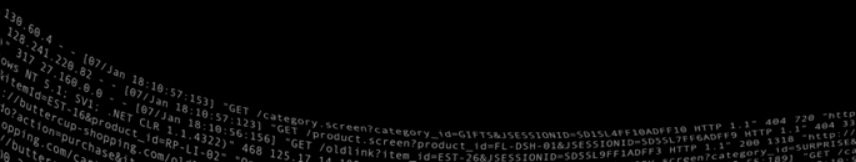
WHAT'S NEW IN
Splunk for Security

EXPRESS EDITION

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.



Hello!

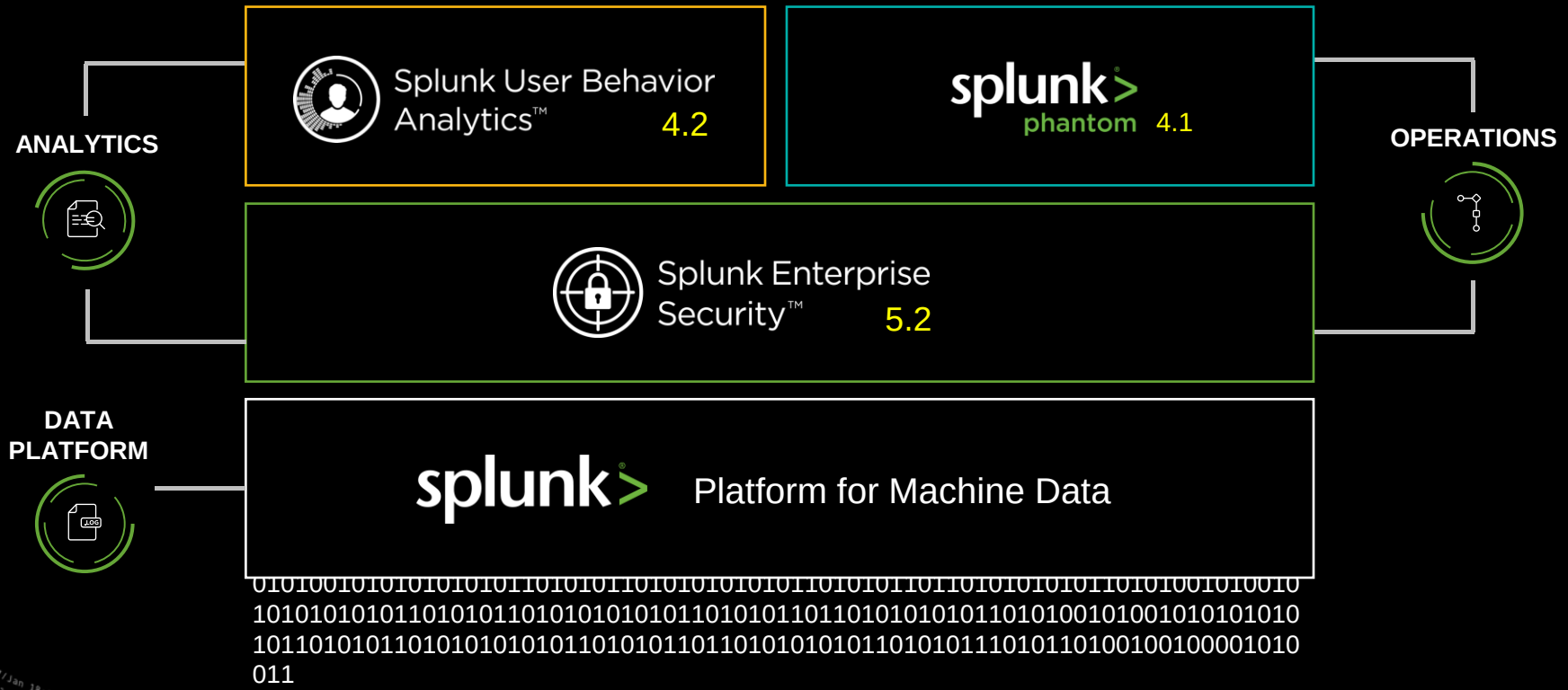
Meet your Splunkers

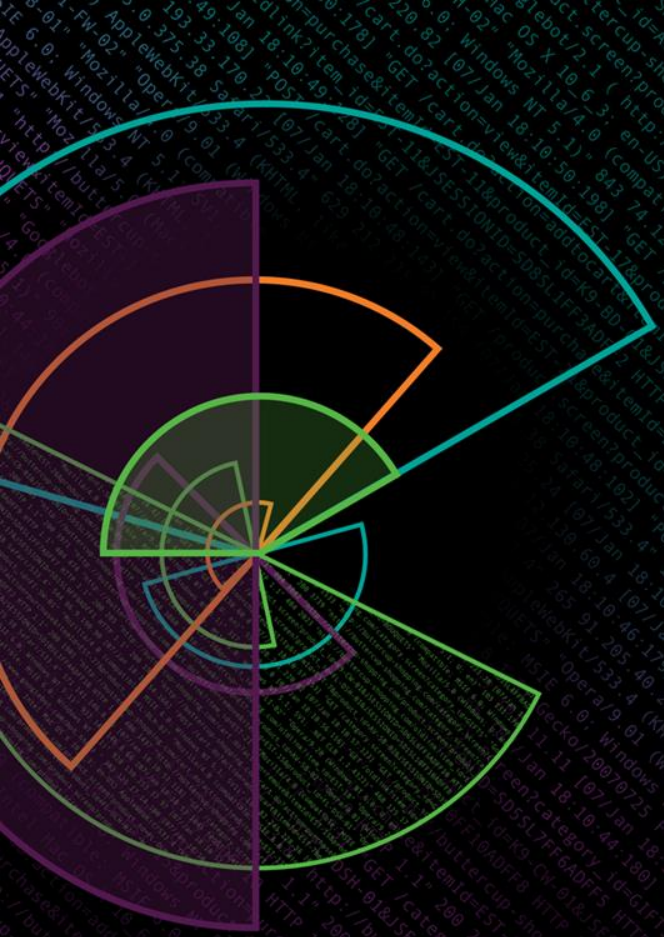
Bob Pratt
Sr. Director,
Product Management - Security

Ale Espinosa
Sr. Director,
Product Marketing - Security

Splunk for Security

Portfolio





What's New

Splunk Enterprise Security

splunk> .conf18

Analytics-Driven SIEM

Splunk Enterprise Security

DETECT

Use to detect advanced threats

ENRICH INFORMATION

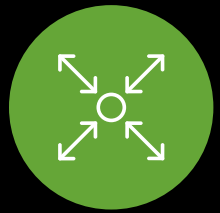
Unlimited context enrichment to qualify incidents fast

INVESTIGATE

Tailored to analyze & investigate incidents

RESPOND

Enterprise-wide coordination & response



Splunk Enterprise Security 5.2

ES 5.2

New and Updated Features

Event Sequencing

Use Case Library

Investigation Workbench

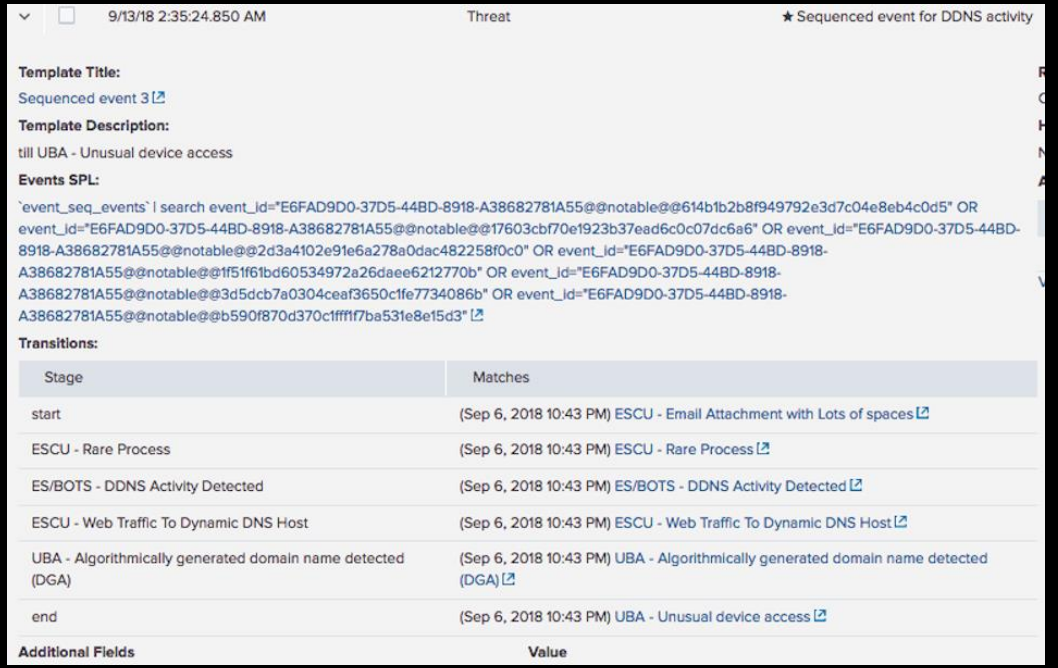
splunk> .conf18

Event Sequencing

ES 5.2

Optimize Threat Detection and Accelerate Investigation

- Helps identify actionable threats
- Improves fidelity of threat detection
- Sequence notable events and risk modifiers
- Use with existing *Incident Review*

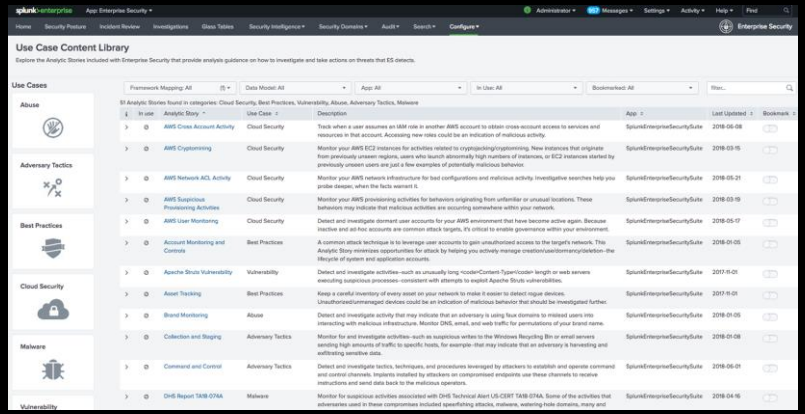


splunk> .conf18

Use Case Library

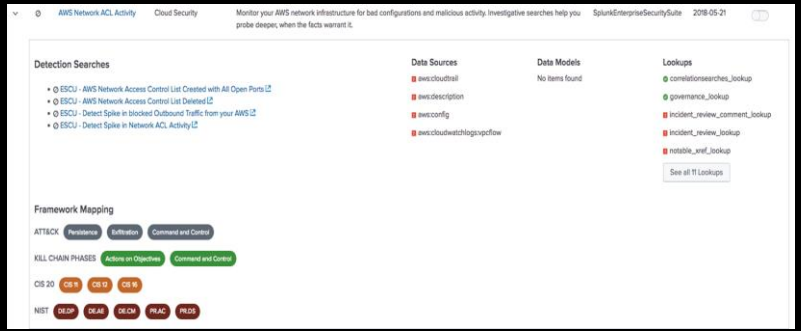
ES 5.2

Faster Detection and Incident Response



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



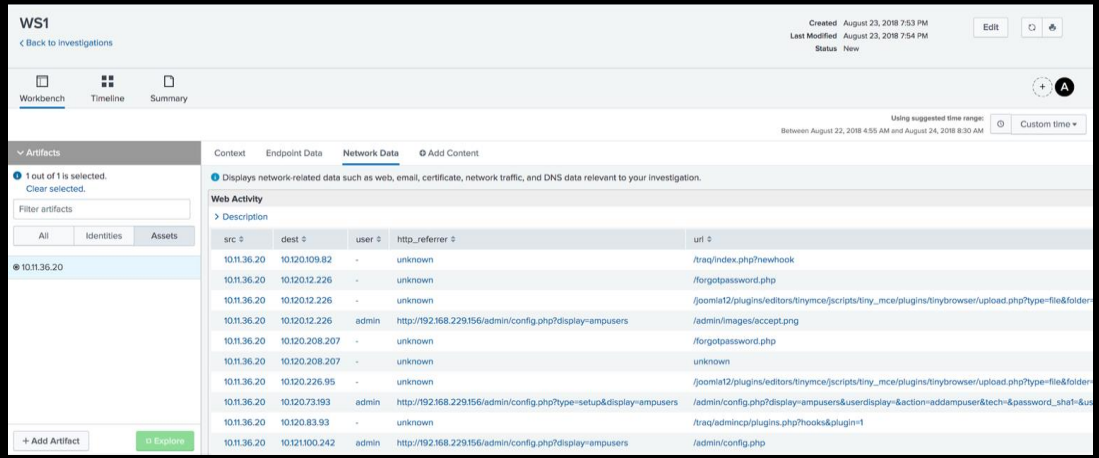
splunk> .conf18

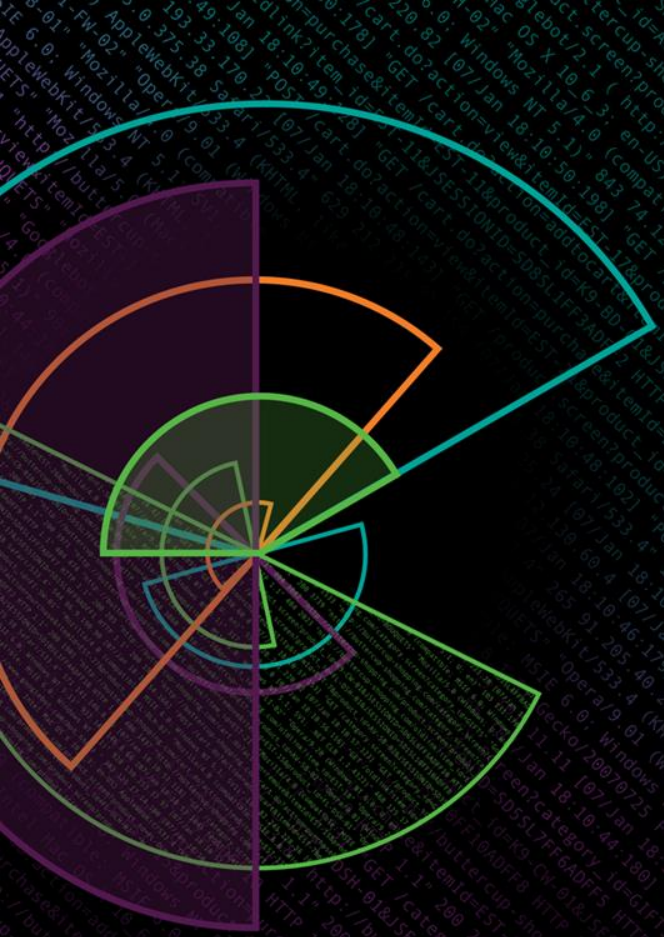
Investigation Workbench

ES 5.2

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





What's New

Splunk User Behavior Analytics

splunk> .conf18

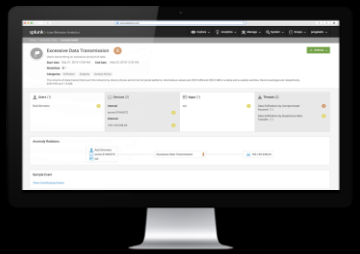
UBA

Splunk User Behavior Analytics (UBA)

Detect Unknown Threats and Anomalous User Behavior using Machine Learning

Container-based Architecture

Advanced Investigation



Data Availability

Enhanced Data Ingestion

User Feedback Learning

UBA 4.1

Greater Scalability for Insider Threat Detection

Container-based Architecture

20
Cluster Nodes

80K
Events per Second

750K
Accounts Monitored

1M
Devices Monitored

kubernetes

docker

splunk> .conf18

Enhanced Investigation with Splunk

Drill Down into Raw Events

UBA 4.1

Drill down into triggering events

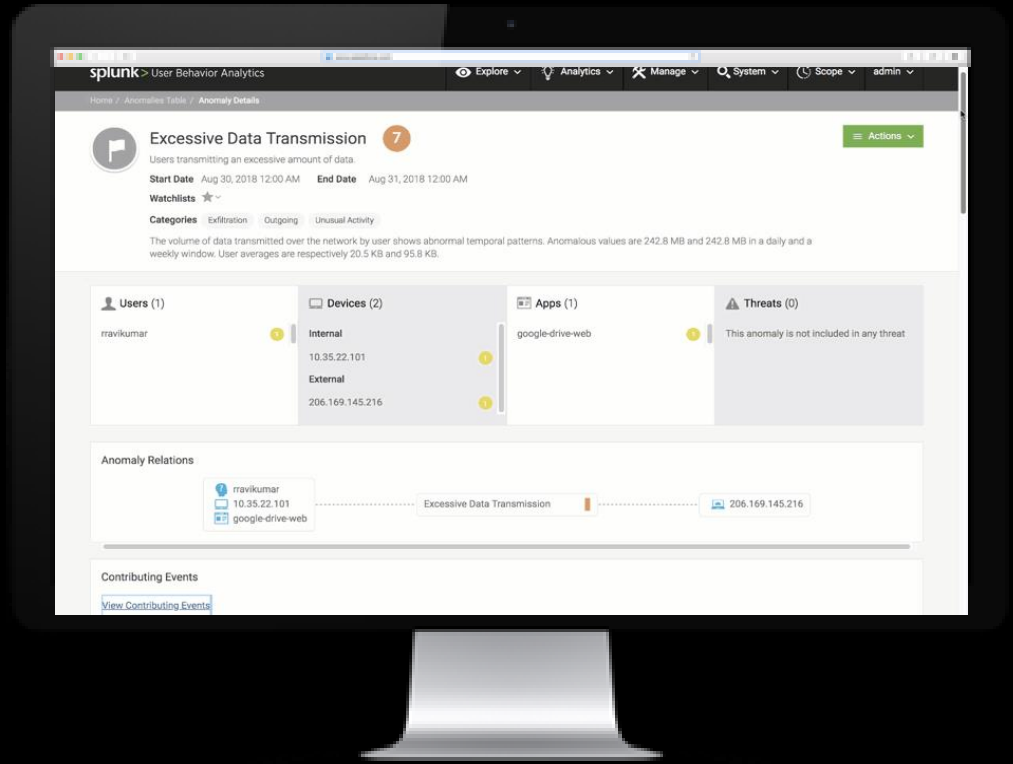
Investigation starts in UBA and continues in core

Targeted hunting using automated SPL

Leverages anomaly data from users and assets

Collect more supporting evidence

Further your investigation with focused timestamps



splunk> .conf18

Data Availability Validation

Quickly Validate Your Data Ingestion

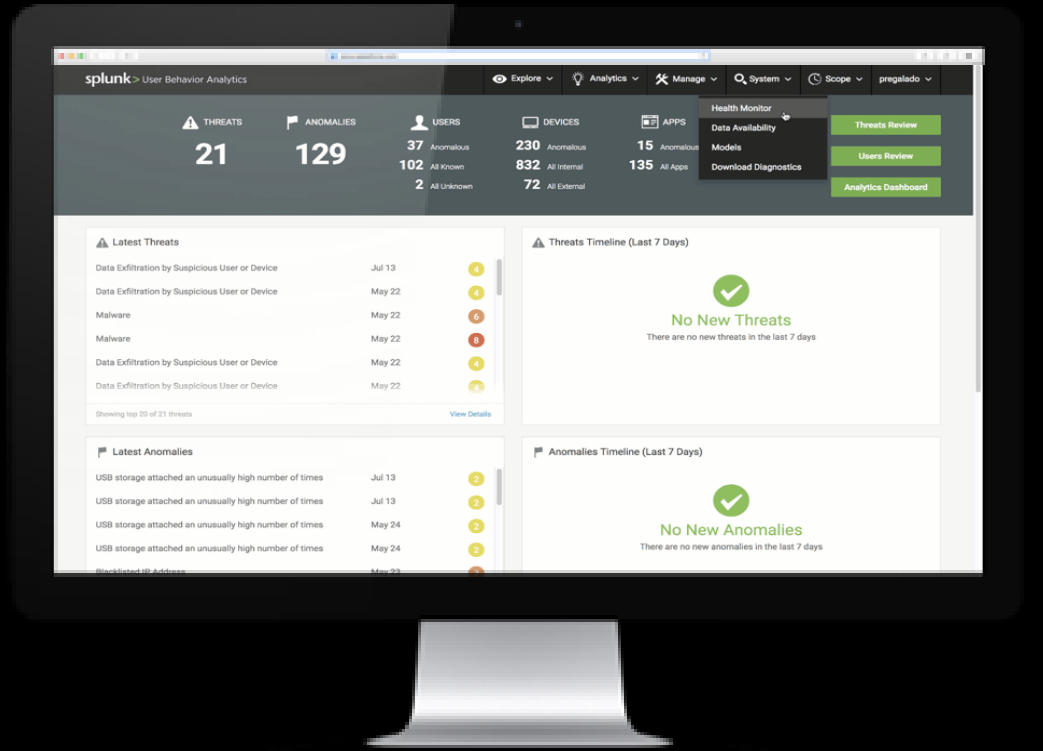
UBA 4.1

View relationships across data sources

Map models and anomalies to generated threat

Identify missing data sources

Gain additional scope and context of threats



splunk> .conf18

Splunk-to-UBA Kafka Connector

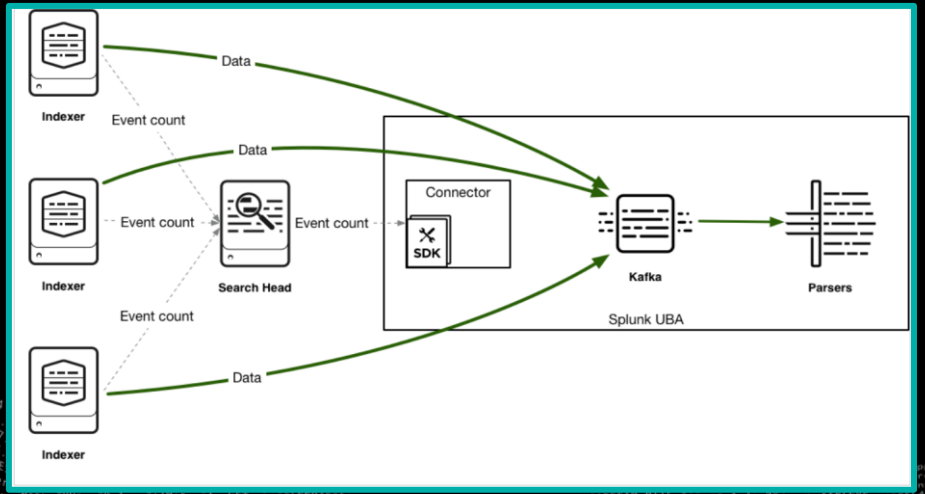
Data Ingestion Performance Doubled

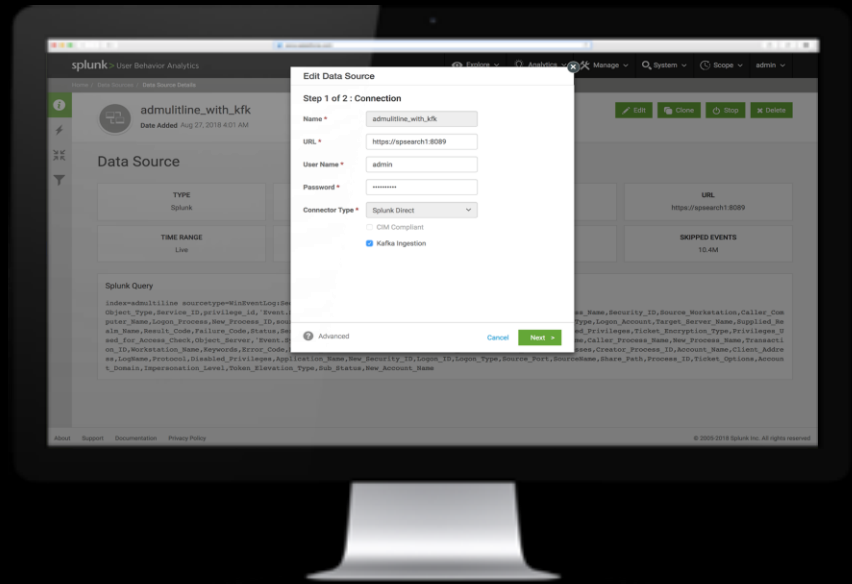
UBA 4.2

Ingest data directly from Splunk indexers to Kafka messaging queue

Strengthen data quality and efficacy

For all machine learning and rule-based detection models





splunk> .conf18

UBA 4.2

User Feedback Learning

Increase Threat Detection Accuracy and Anomaly Customization

Provide granular feedback to anomaly models

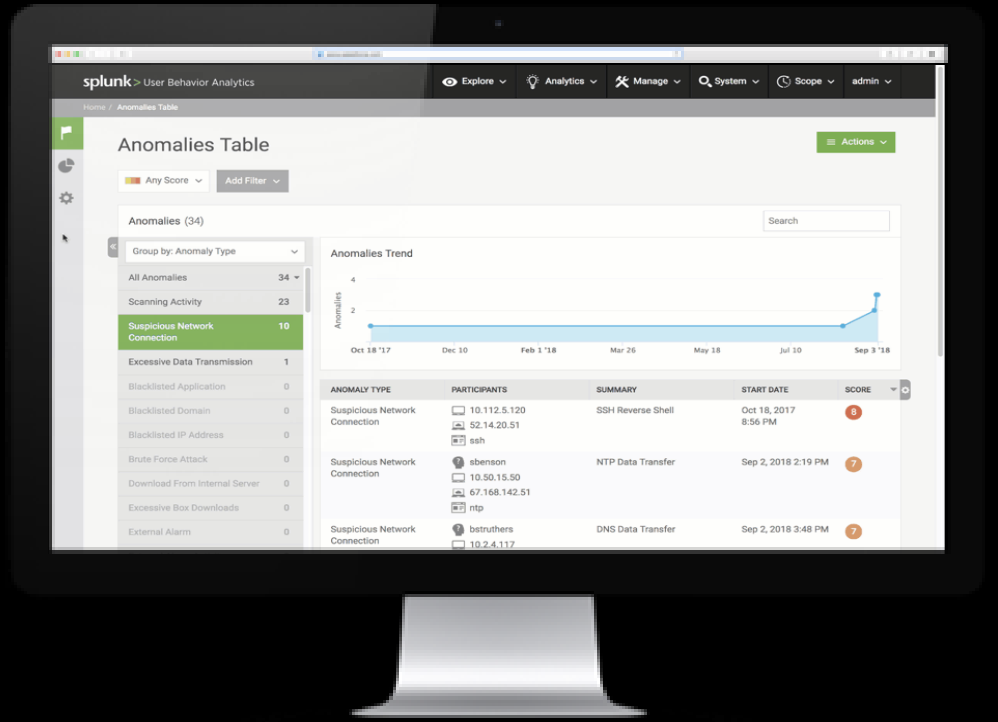
Anomaly scoring rules per anomaly type

Control overall threat detection severity and confidence

Tune scoring weights up/down for each model feature

Customize anomaly models

Based on your enterprise policies



splunk> .conf18

UBACU

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

Data Exfiltration

Unusual USB device
High USB attachments

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

box

File relay
Data destruction
Data collection
Watering hole
Suspicious new access

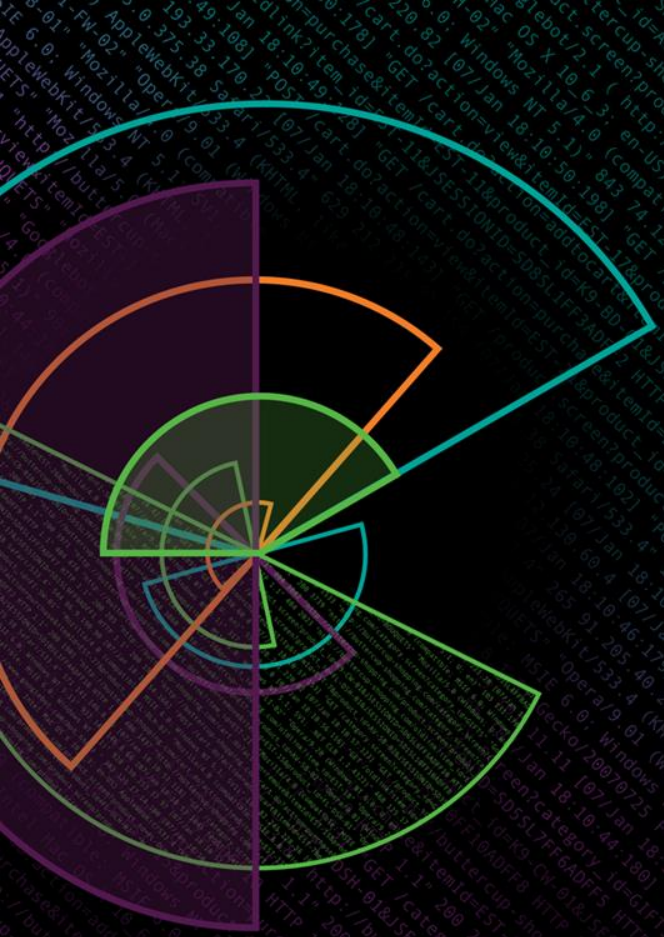
External Alarm

Aggregation of external alarms with security analytics

Security Context

Behavior-based fingerprinting of user roles and assets

splunk> .conf18

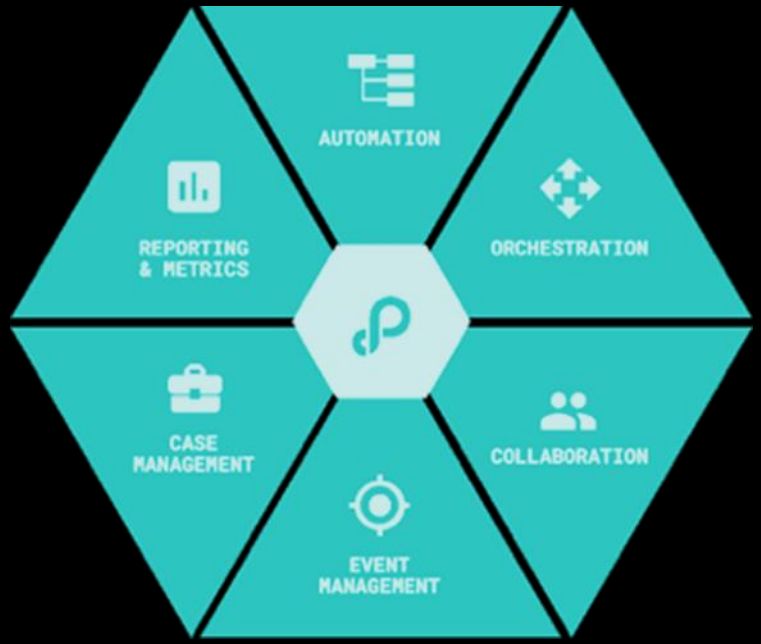


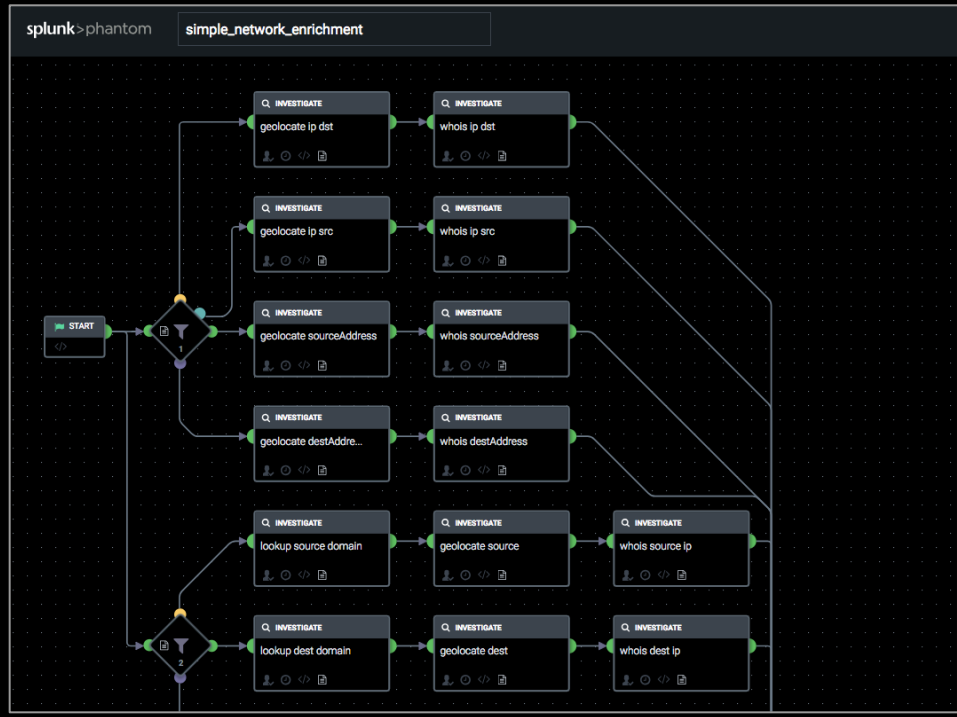
What's New

Splunk Phantom

Splunk Phantom

Security Orchestration, Automation, and Response



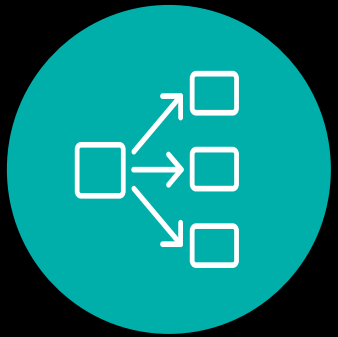


splunk> .conf18

PHANTOM 4.0

Splunk Phantom 4.0

New and Updated Features



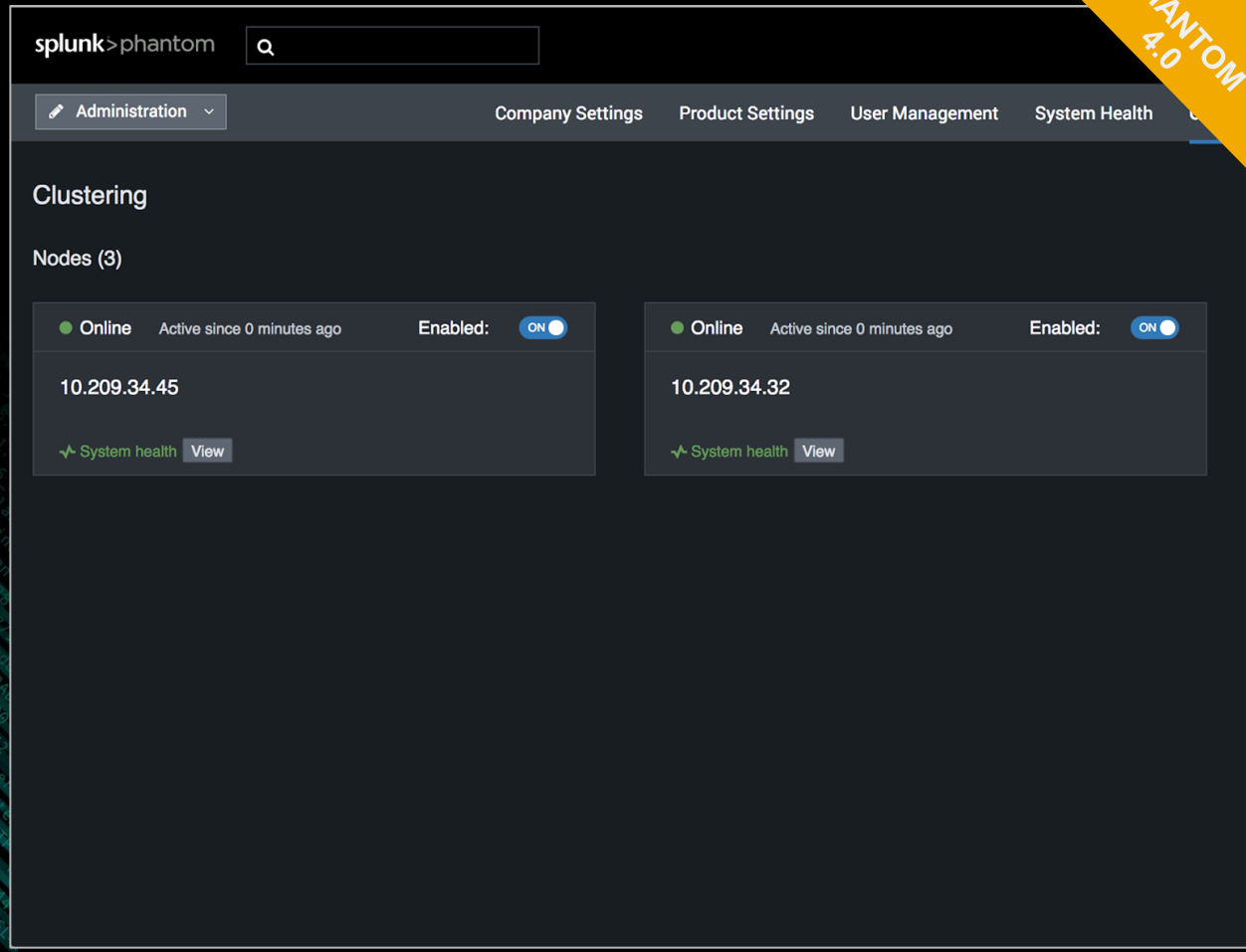
Clustering Support

Indicator View

Splunk Search & Storage

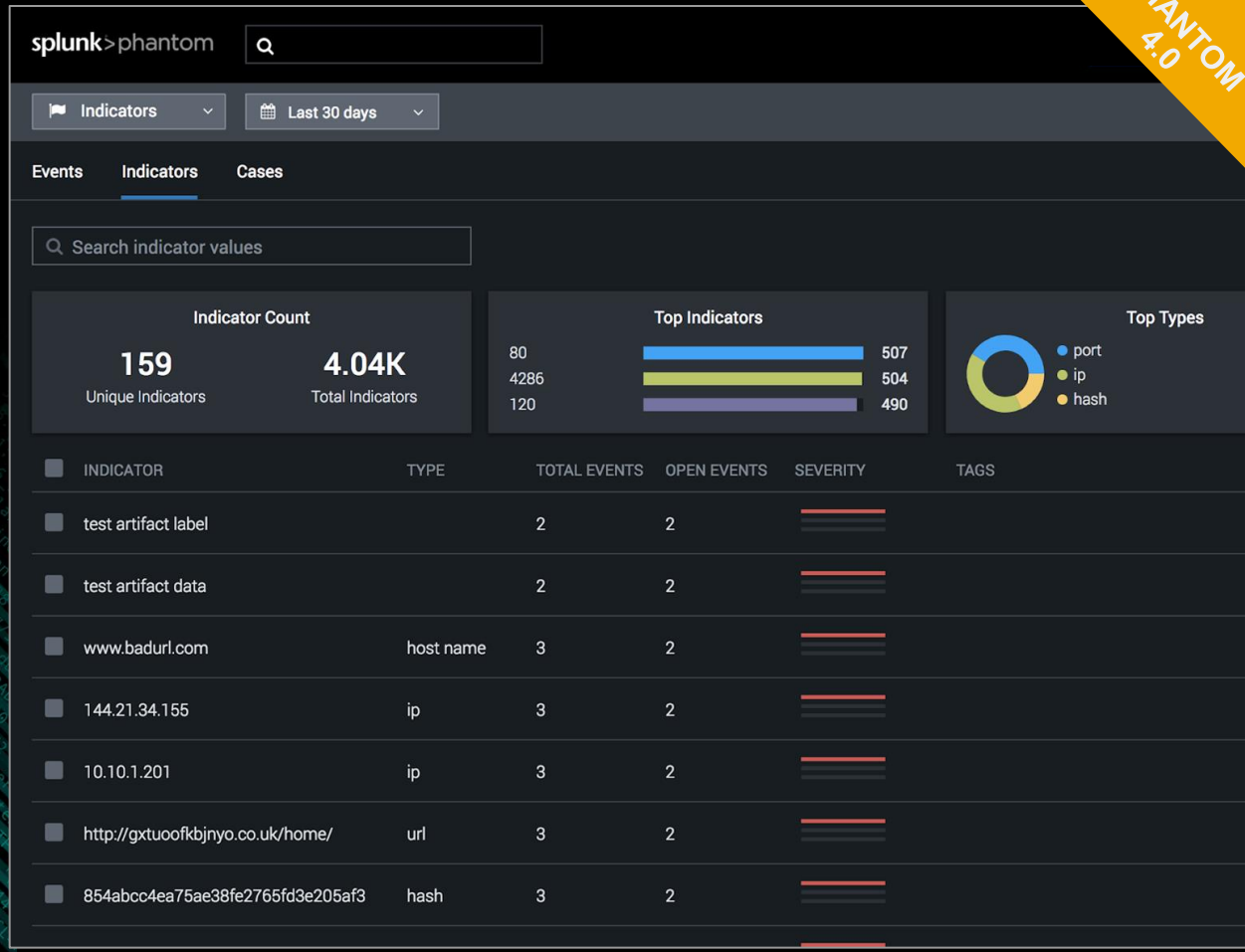
Clustering

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



Indicator View

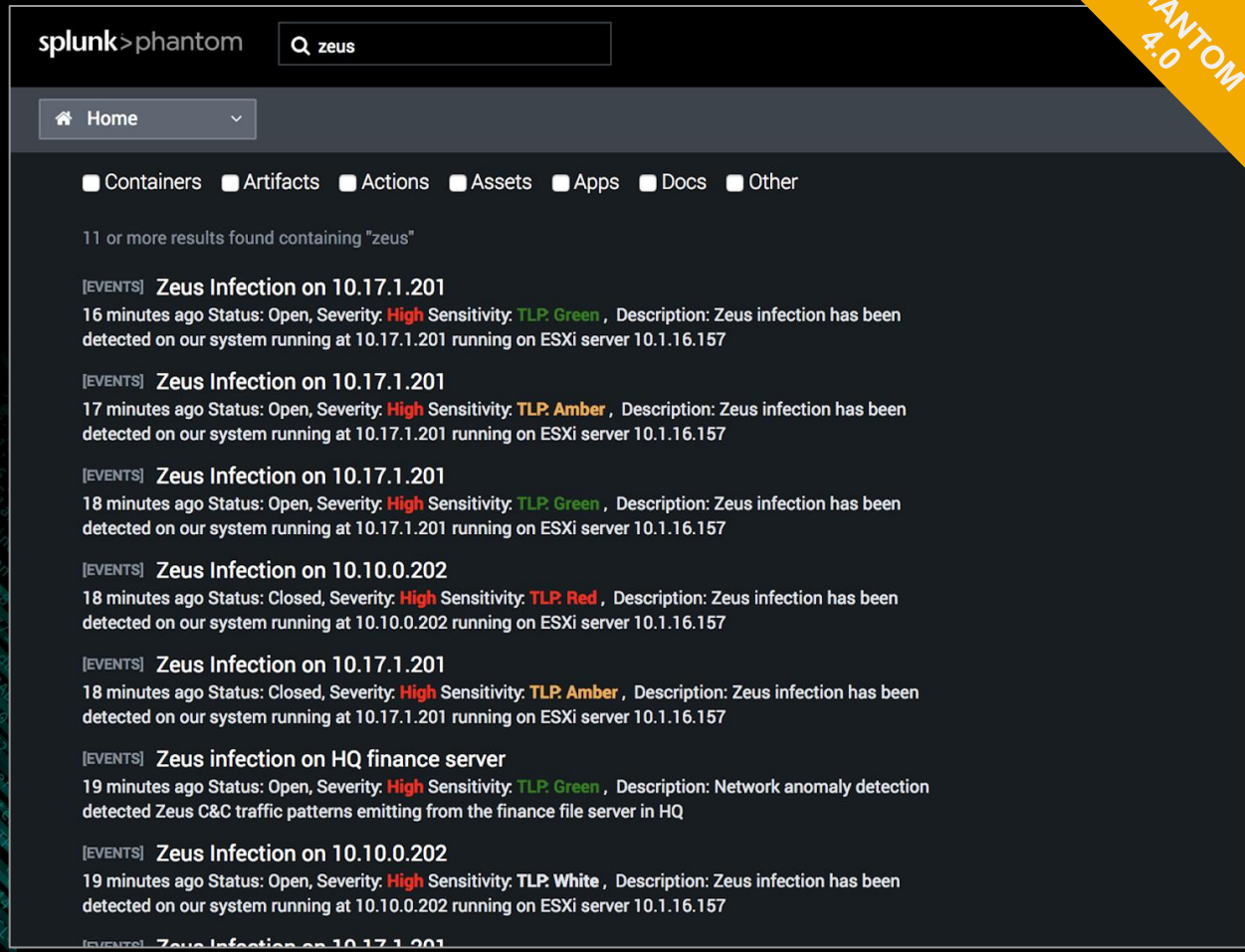
- Gain deeper insights into your data
- Approach incidents from an indicator perspective
- Drill Down to see indicator details



PHANTOM 4.0

Splunk Search and Storage

- Only SOAR platform with integrated Splunk search support
- Supports existing Splunk datastores for single source of truth

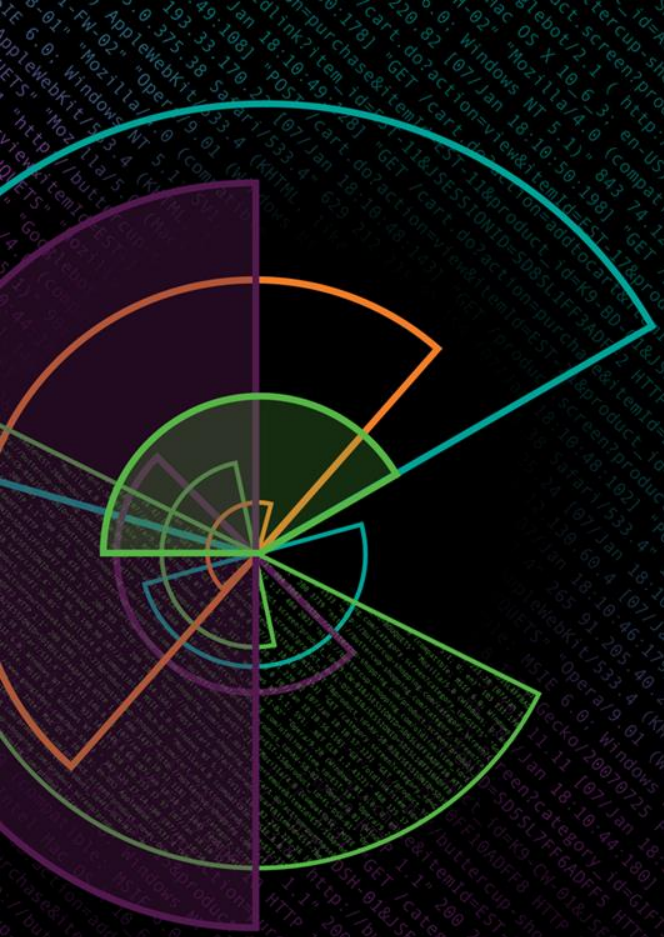


PHANTOM 4.0

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

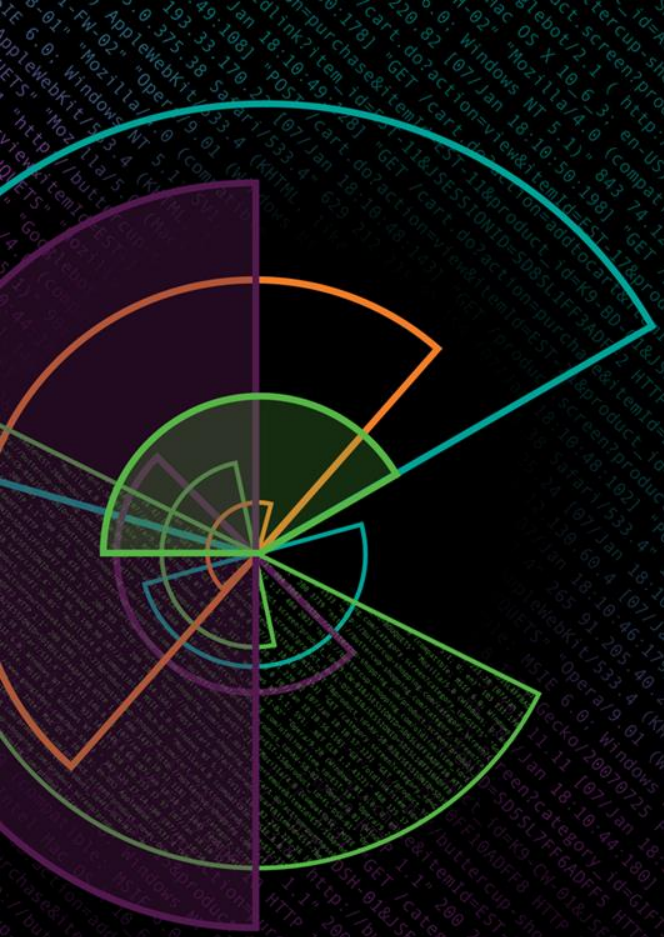


Get More with Splunk

Splunk for Security

splunk> .conf18

Advancing Your Security Journey



Questions?

splunk> .conf18

Thank You!

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