



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.

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

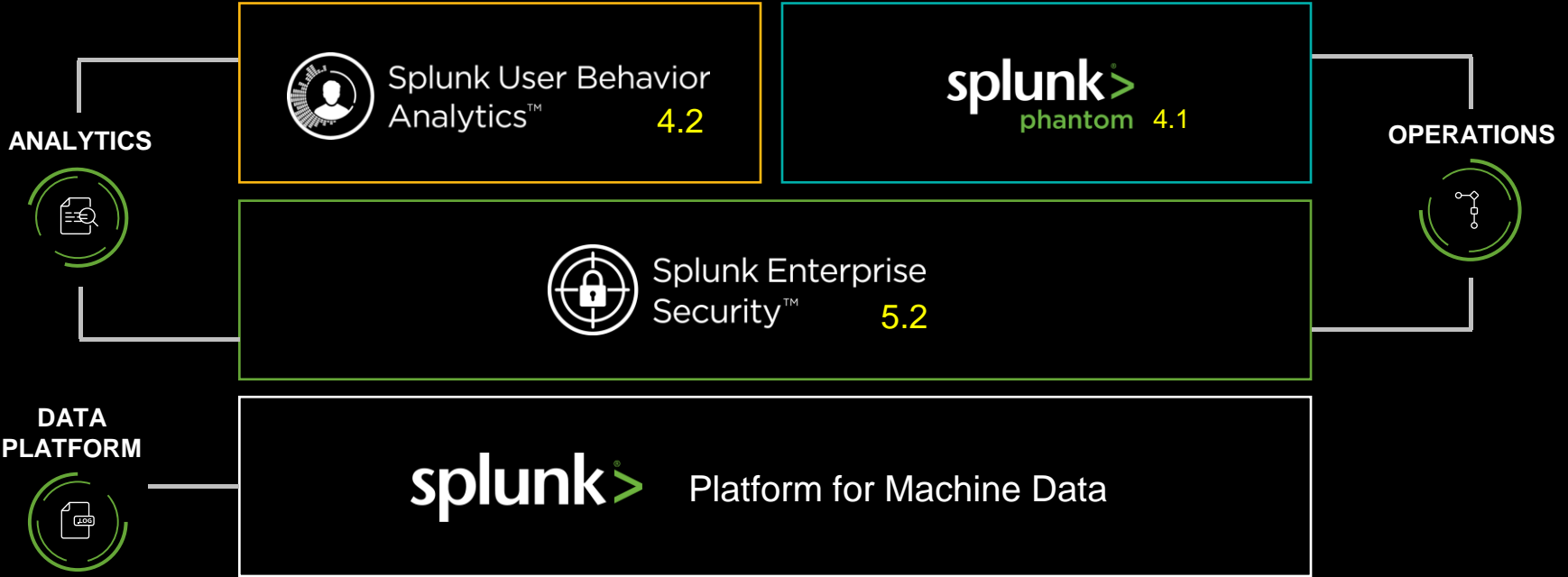


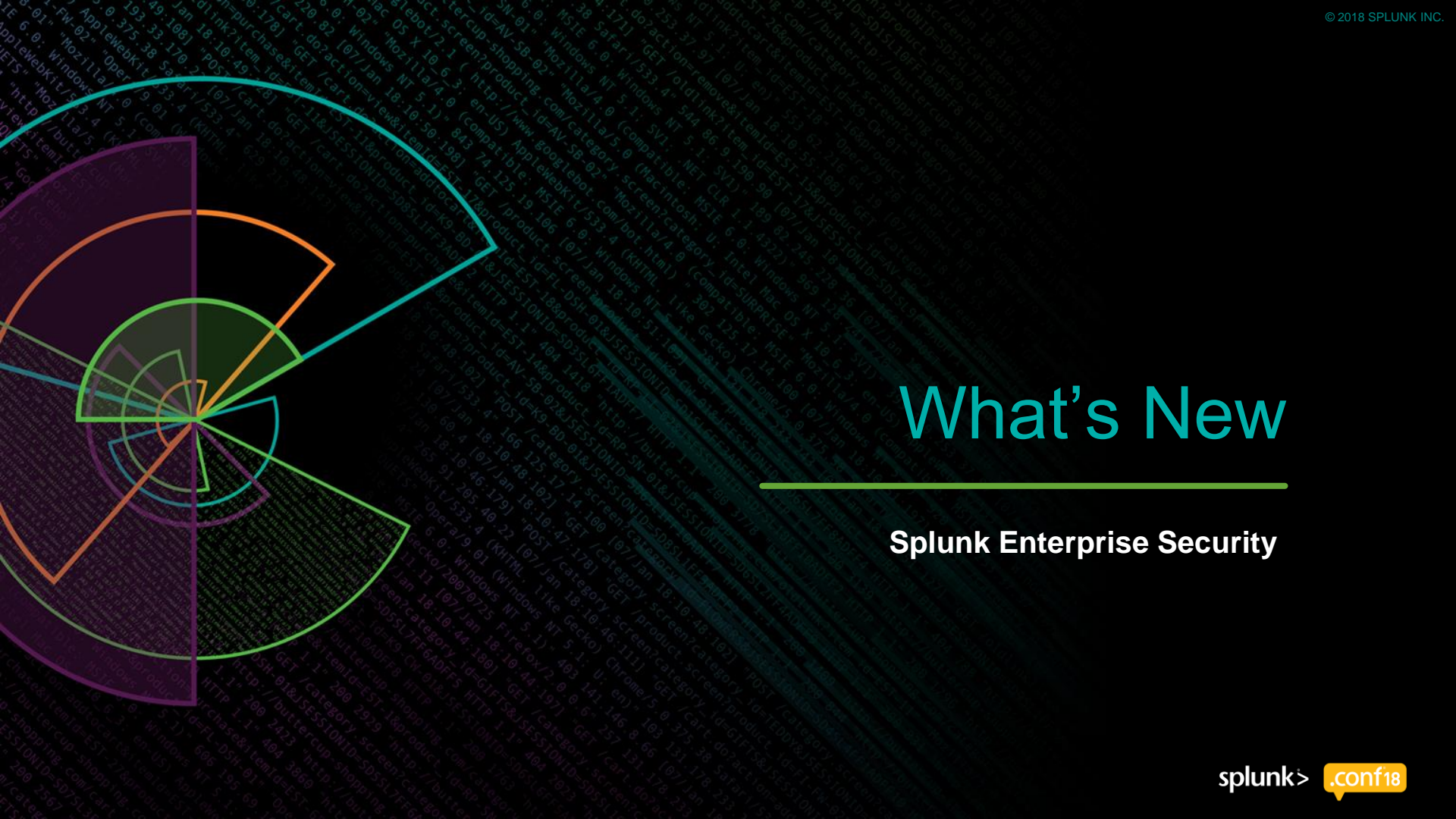
Bob Pratt
Sr. Director,
Product Management - Security



Ale Espinosa
Sr. Director,
Product Marketing - Security

Splunk for Security Portfolio





What's New

Splunk Enterprise Security

Splunk Enterprise Security

Use to detect
advanced threats



Unlimited context enrichment to qualify incidents fast



Tailored to analyze
& investigate
incidents



Enterprise-wide coordination & response



Splunk Enterprise Security 5.2

New and Updated Features



**Event
Sequencing**



**Use Case
Library**



**Investigation
Workbench**

Event Sequencing

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*

9/13/18 2:35:24.850 AM Threat ★ Sequenced event for DDNS activity

Template Title:
Sequenced event 3 [\[Link\]](#)

Template Description:
till UBA - Unusual device access

Events SPL:
`event_seq_events` | search event_id="E6FAD9D0-37D5-44BD-8918-A38682781A55@notable@614b1b2b8f949792e3d7c04e8eb4c0d5" OR event_id="E6FAD9D0-37D5-44BD-8918-A38682781A55@notable@17603cbf70e1923b37ead6c0c07dc6a6" OR event_id="E6FAD9D0-37D5-44BD-8918-A38682781A55@notable@2d3a4102e91e6a278a0dac482258f0c0" OR event_id="E6FAD9D0-37D5-44BD-8918-A38682781A55@notable@1f51f61bd60534972a26dae6212770b" OR event_id="E6FAD9D0-37D5-44BD-8918-A38682781A55@notable@3d5dcb7a0304ceaf3650cfe7734086b" OR event_id="E6FAD9D0-37D5-44BD-8918-A38682781A55@notable@b590f870d370c1fff17ba531e8e15d3" [\[Link\]](#)

Transitions:

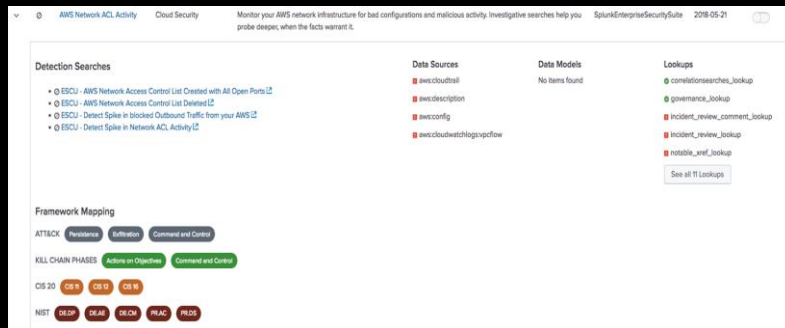
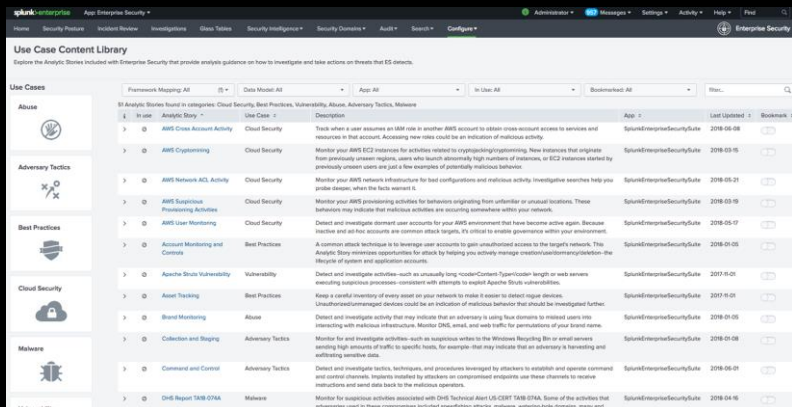
Stage	Matches
start	(Sep 6, 2018 10:43 PM) ESCU - Email Attachment with Lots of spaces [Link]
ESCU - Rare Process	(Sep 6, 2018 10:43 PM) ESCU - Rare Process [Link]
ES/BOTS - DDNS Activity Detected	(Sep 6, 2018 10:43 PM) ES/BOTS - DDNS Activity Detected [Link]
ESCU - Web Traffic To Dynamic DNS Host	(Sep 6, 2018 10:43 PM) ESCU - Web Traffic To Dynamic DNS Host [Link]
UBA - Algorithmically generated domain name detected (DGA)	(Sep 6, 2018 10:43 PM) UBA - Algorithmically generated domain name detected (DGA) [Link]
end	(Sep 6, 2018 10:43 PM) UBA - Unusual device access [Link]

Additional Fields **Value**

Use Case Library

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

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

WS1

Created August 23, 2018 7:53 PM
Last Modified August 23, 2018 7:54 PM
Status New

Workbench Timeline Summary

Using suggested time range: Between August 22, 2018 4:55 AM and August 24, 2018 8:30 AM Custom time

Artifacts

1 out of 1 is selected.
Clear selected.

Filter artifacts

All Identities Assets

@ 10.11.36.20

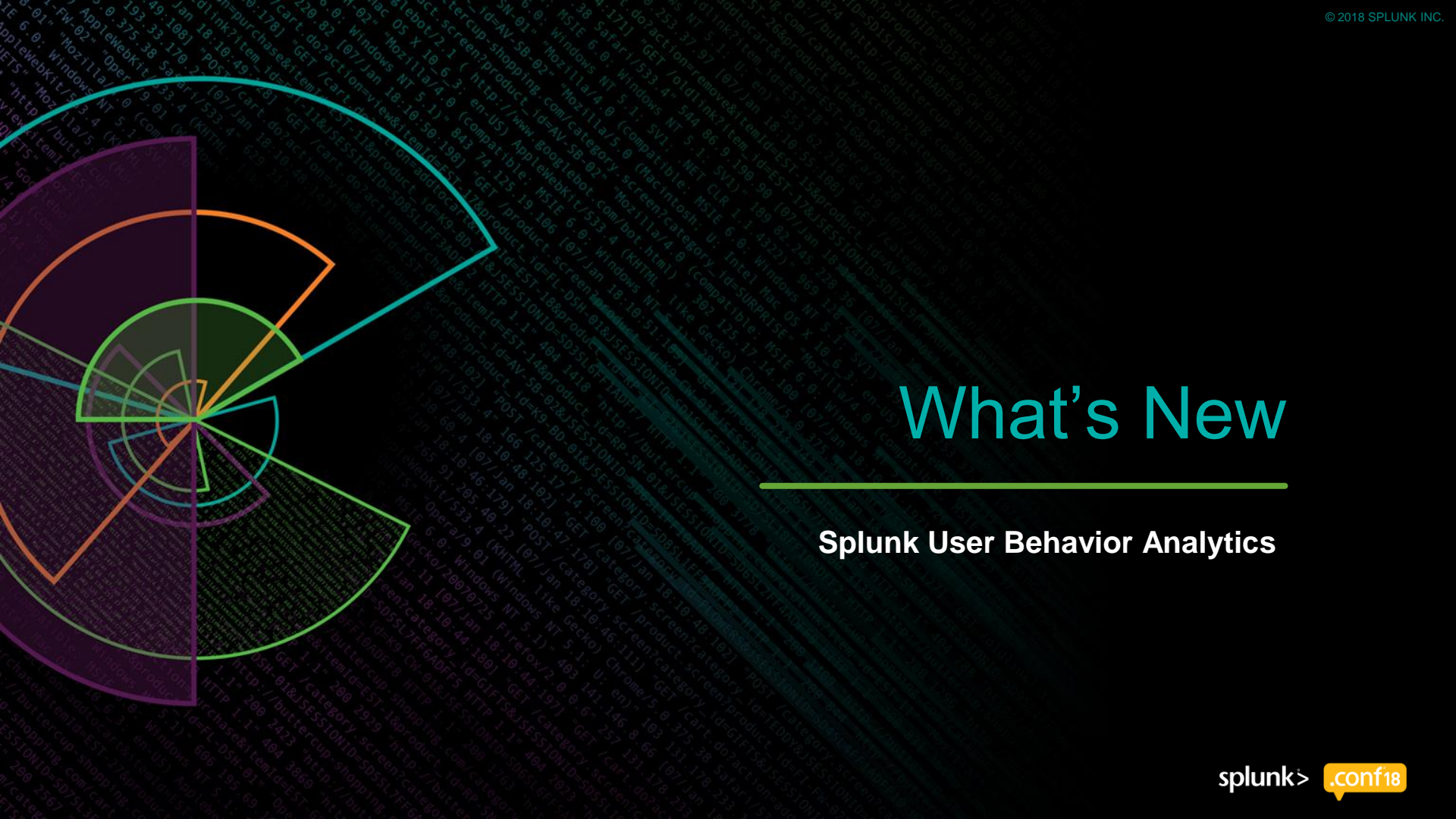
Context Endpoint Data Network Data Add Content

Displays network-related data such as web, email, certificate, network traffic, and DNS data relevant to your investigation.

Web Activity

src ip	dest ip	user	http_referrer	url
10.11.36.20	10.120.109.82	-	unknown	/traq/index.php?newhook
10.11.36.20	10.120.12.226	-	unknown	/forgotpassword.php
10.11.36.20	10.120.12.226	-	unknown	/joomla2/plugins/editors/tiny_mce/plugins/tinybrowser/upload.php?type=file&folder=
10.11.36.20	10.120.12.226	admin	http://192.168.229.156/admin/config.php?display=ampusers	/admin/images/accept.png
10.11.36.20	10.120.208.207	-	unknown	/forgotpassword.php
10.11.36.20	10.120.208.207	-	unknown	unknown
10.11.36.20	10.120.226.95	-	unknown	/joomla2/plugins/editors/tiny_mce/plugins/tinybrowser/upload.php?type=file&folder=
10.11.36.20	10.120.73.193	admin	http://192.168.229.156/admin/config.php?type=setup&display=ampusers	/admin/config.php?display=ampusers&userdisplay=&action=addampuser&tech=&password_sha1=&us
10.11.36.20	10.120.83.93	-	unknown	/traq/admin/plugins.php?hooks&plugin=1
10.11.36.20	10.121.100.242	admin	http://192.168.229.156/admin/config.php?display=ampusers	/admin/config.php

+ Add Artifact Explore



What's New

Splunk User Behavior Analytics

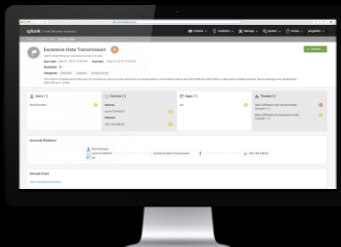
Splunk User Behavior Analytics (UBA)

Detect Unknown Threats and Anomalous User Behavior using Machine Learning

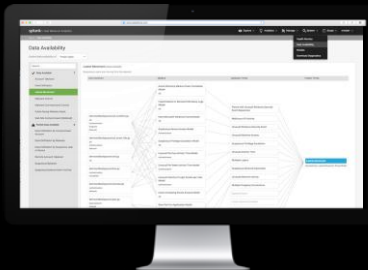
Container-based Architecture



Advanced Investigation



Data Availability



Enhanced Data Ingestion



User Feedback Learning



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

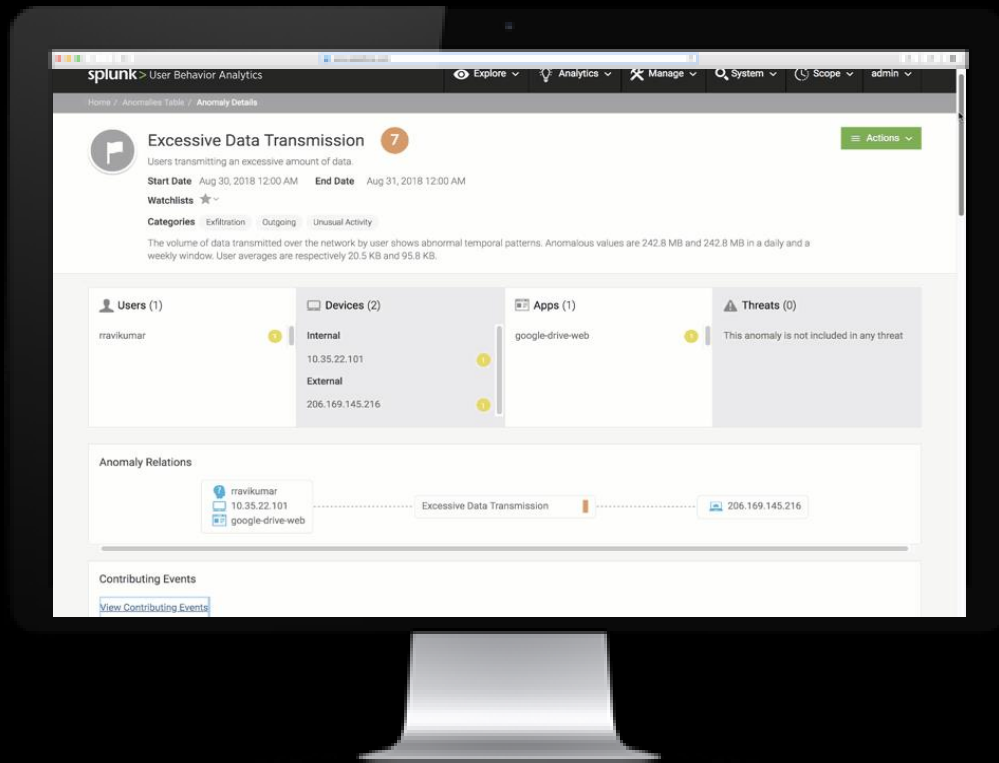
Investigation starts in UBA and continues in core

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

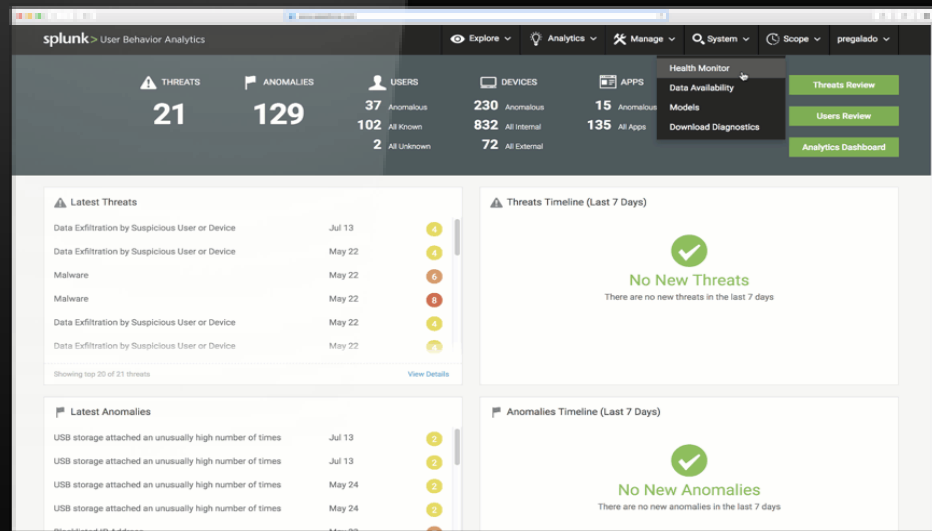
Quickly Validate Your Data Ingestion

View relationships across data sources

Map models and anomalies to generated threat

Identify missing data sources

Gain additional scope and context of threats



User Feedback Learning

Increase Threat Detection Accuracy and Anomaly Customization

Provide granular feedback to anomaly models

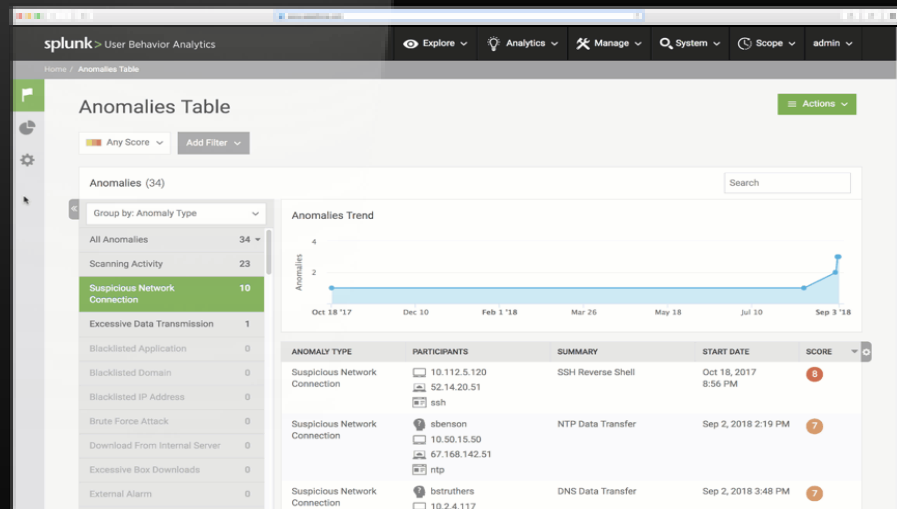
Anomaly scoring rules per anomaly type

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 UBA Content Updates

Stay Ahead of Advanced and Insider Threats



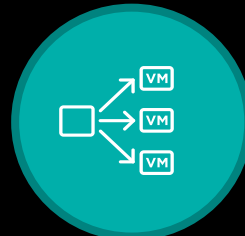
Account Takeover

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

Data Exfiltration

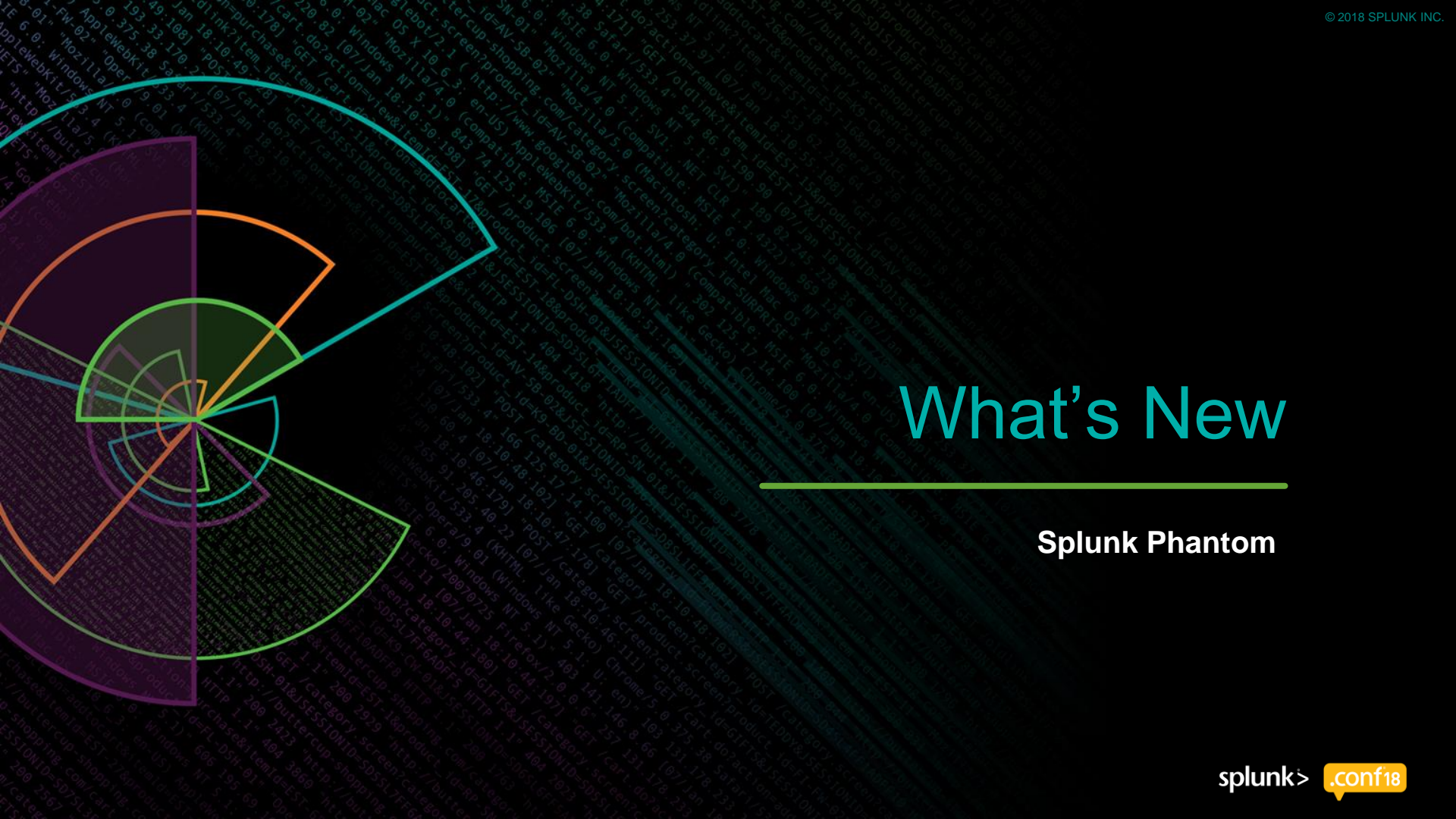
Unusual USB device
High USB attachments



File relay
Data destruction
Data collection
Watering hole
Suspicious new access

Security Context

Behavior-based fingerprinting of user roles and assets

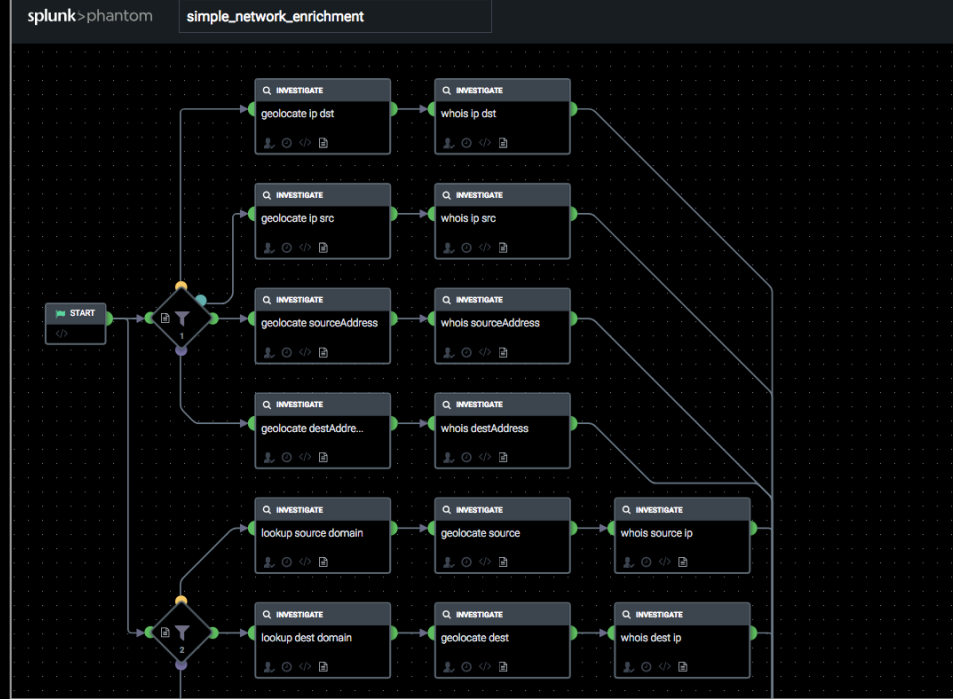
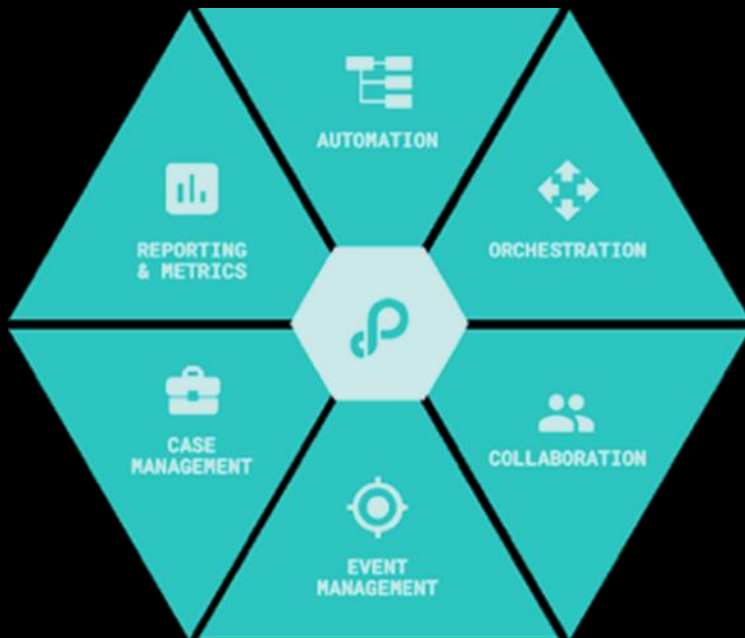


What's New

Splunk Phantom

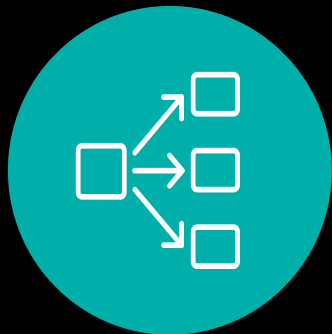
Splunk Phantom

Security Orchestration, Automation, and Response



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

PHANTOM 4.0

splunk>phantom

Administration Company Settings Product Settings User Management System Health

Clustering

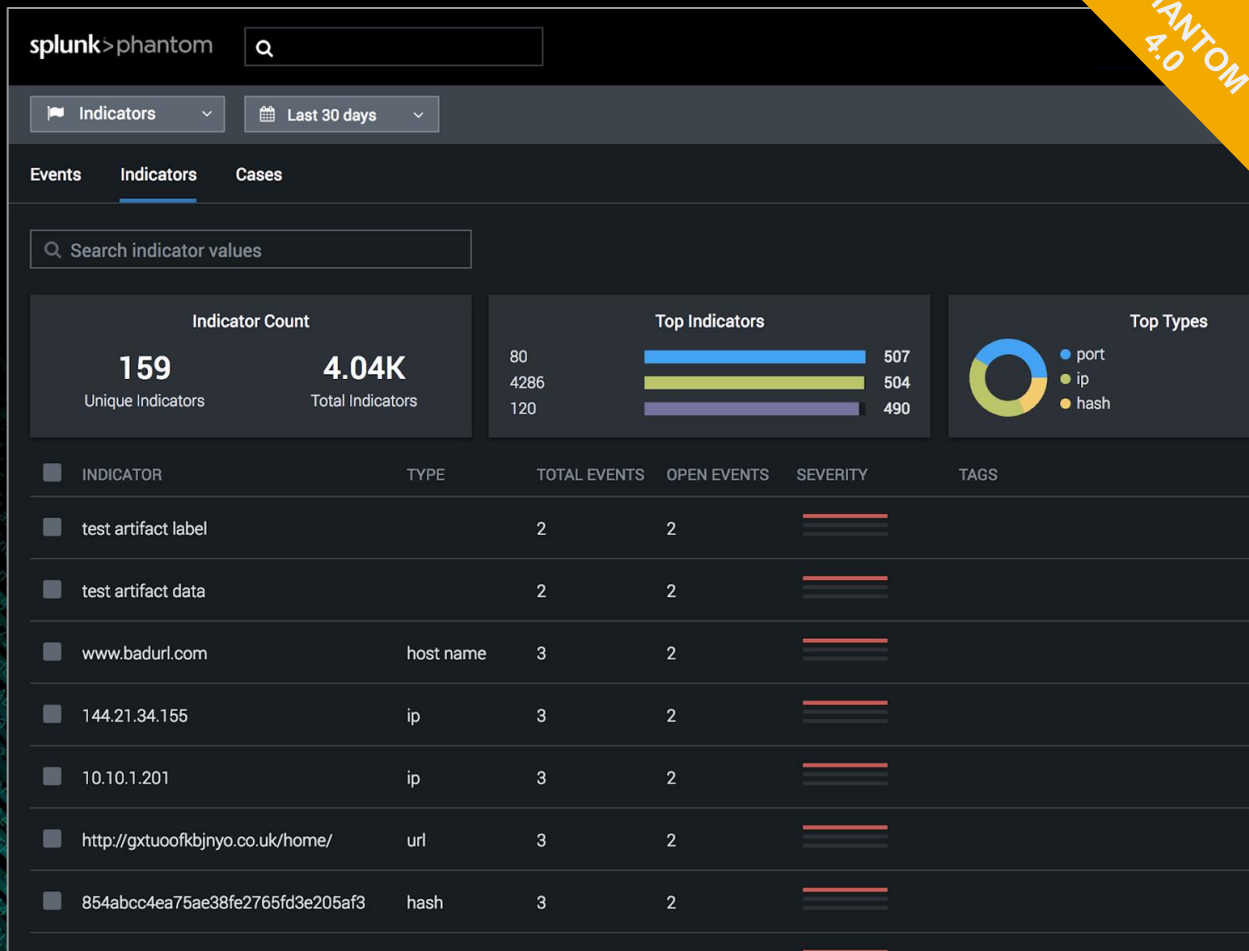
Nodes (3)

<div><div>● Online</div><div>Active since 0 minutes ago</div><div>Enabled: <input checked="" type="checkbox"/></div></div> <div>10.209.34.45</div> <div><div>↗ System health</div><div>View</div></div>	<div><div>● Online</div><div>Active since 0 minutes ago</div><div>Enabled: <input checked="" type="checkbox"/></div></div> <div>10.209.34.32</div> <div><div>↗ System health</div><div>View</div></div>
---	---



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

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

19 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

splunk>

conf18

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



Questions?

Thank You!

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

.conf18

splunk>