

Operationalizing UBA to Fullest Potential

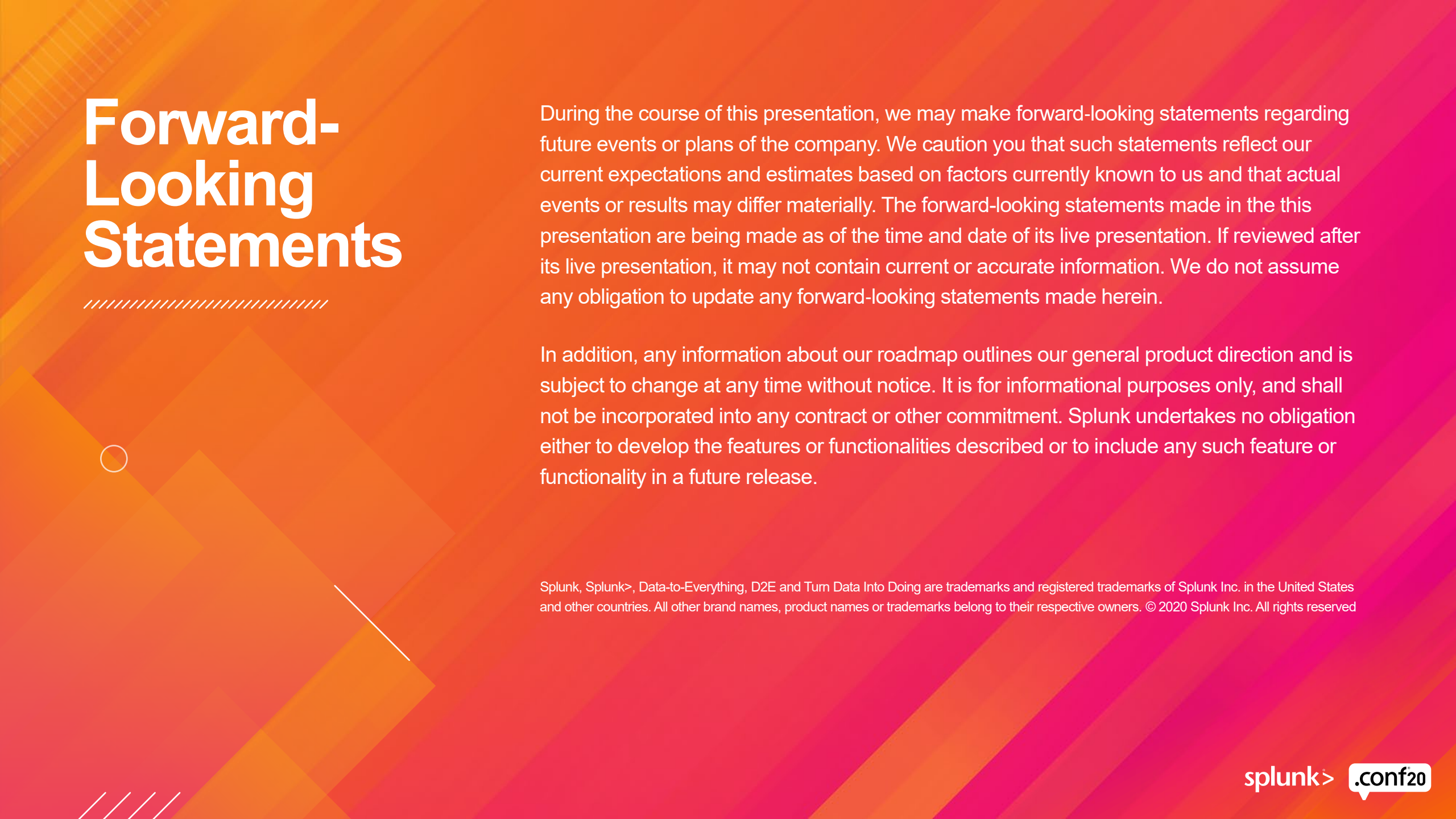
SEC1616

Annette Fontanilla

Sr. Professional Services Consultant | Splunk



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>, Data-to-Everything, D2E and Turn Data Into Doing 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. © 2020 Splunk Inc. All rights reserved

Annette Fontanilla

Sr. Professional Services Consultant | Splunk



Agenda

SEC1616 .conf2020

1) Intro

What is Splunk UBA

2) Important of Operationalizing UBA

Reality vs. Expectations

3) Tuning

Identity Resolution, Anomaly Action Rules, Threat Rules

4) Roles

Analyst vs. Threat Hunter

5) Workflows

Customizations

6) Key Takeaways

What “Operationalizing UBA” looks like

Expectations vs. Reality



Expectations

No tuning required

False positives will disappear... eventually

Just add data

Data science will solve everything



Reality

Noisy IPS/IDS, DLP alerts

Network changes

Data hygiene is key

Known behavior vs. unknown behavior



~~Expectations~~ vs. Reality

Important of Operationalizing UBA

Network Spike

Network changes can
cause a spike in
anomalies and
threats. i.e. Remote,
increase in Zoom

Shadow IT

Noisy Alerts

Discovery

~~Expectations~~ vs. Reality

Important of Operationalizing UBA

Network Spike

Network changes can cause a spike in anomalies and threats. i.e. Remote, increase in Zoom

Shadow IT

Users using unapproved software

Noisy Alerts

Discovery

~~Expectations~~ vs. Reality

Important of Operationalizing UBA

Network Spike

Network changes can cause a spike in anomalies and threats. i.e. Remote, increase in Zoom

Shadow IT

Users using unapproved software

Noisy Alerts

Alerting tools can cause several false positives in UBA due to a misconfiguration or noisy alert

Discovery

Expectations vs. Reality

Important of Operationalizing UBA

Network Spike

Network changes can cause a spike in anomalies and threats. i.e. Remote, increase in Zoom

Shadow IT

Users using unapproved software

Noisy Alerts

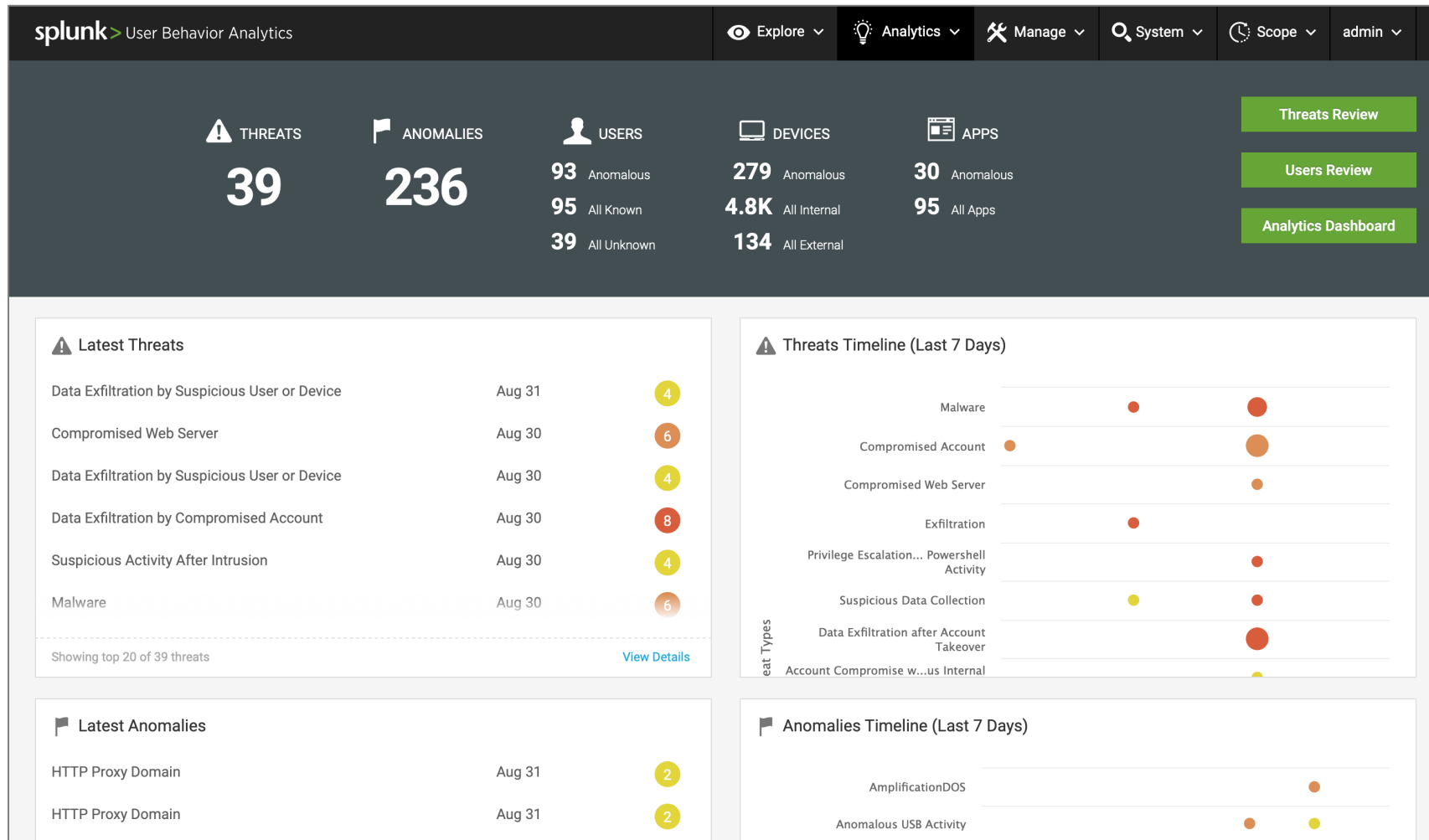
Alerting tools can cause several false positives in UBA due to a misconfiguration or noisy alert

Discovery

Understanding devices and user/service account or device roles

Ultimate Goal

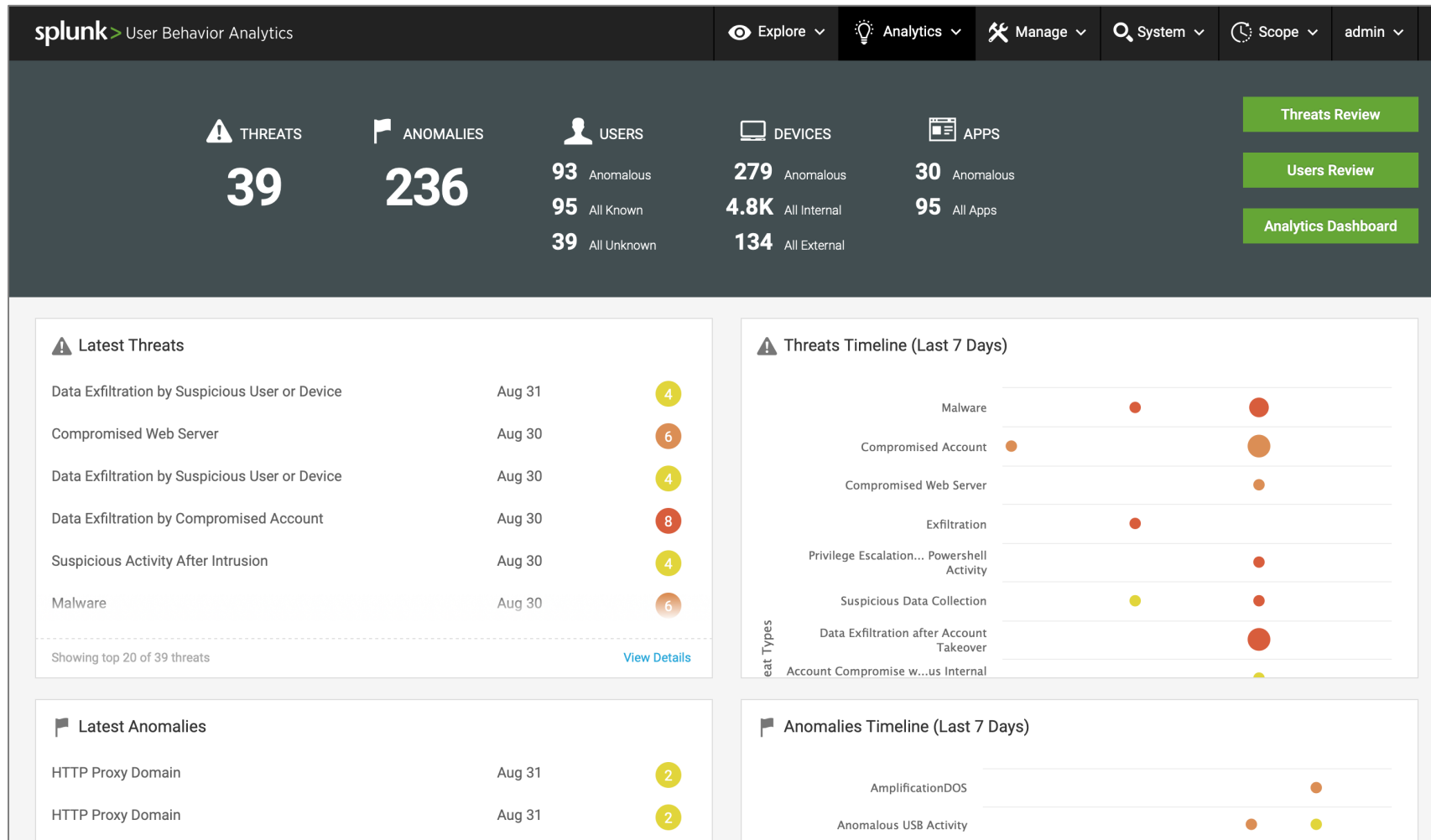
Important of operationalizing UBA



Ultimate Goal

Important of operationalizing UBA

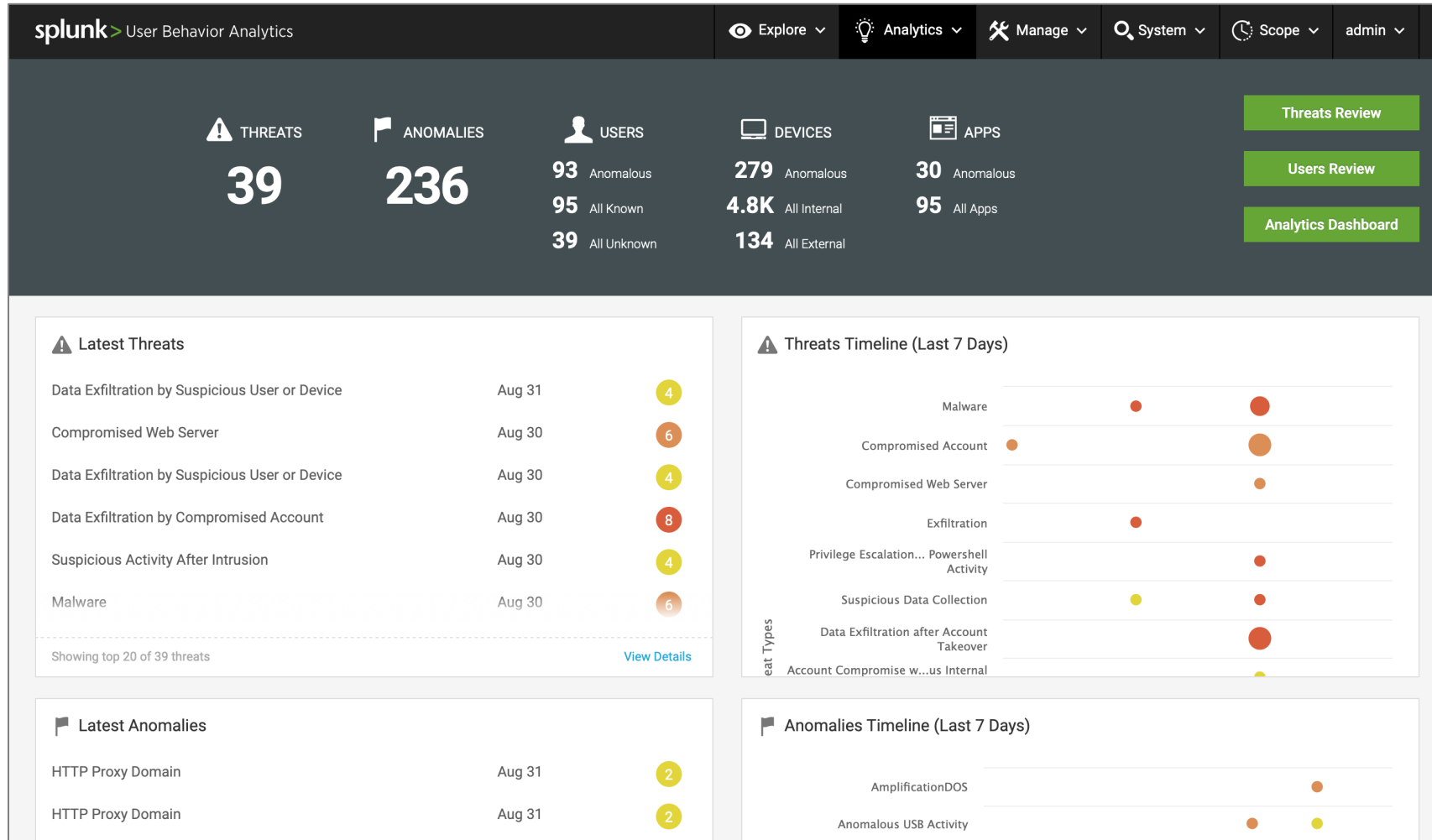
Reduce False
Positives



Ultimate Goal

Important of operationalizing UBA

Reduce False
Positives



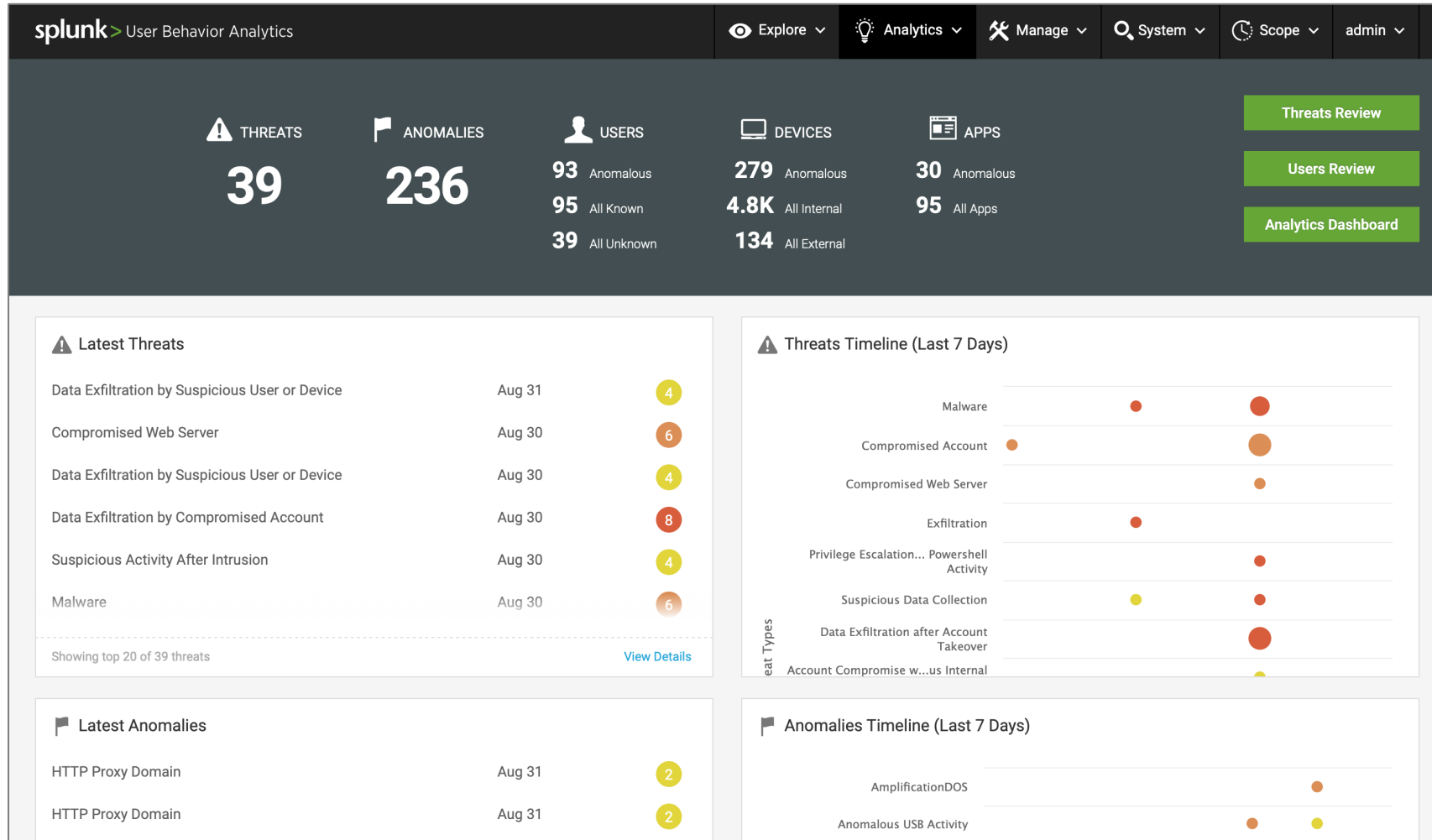
Finalize Use
Cases

Ultimate Goal

Important of operationalizing UBA

Reduce False
Positives

Roles



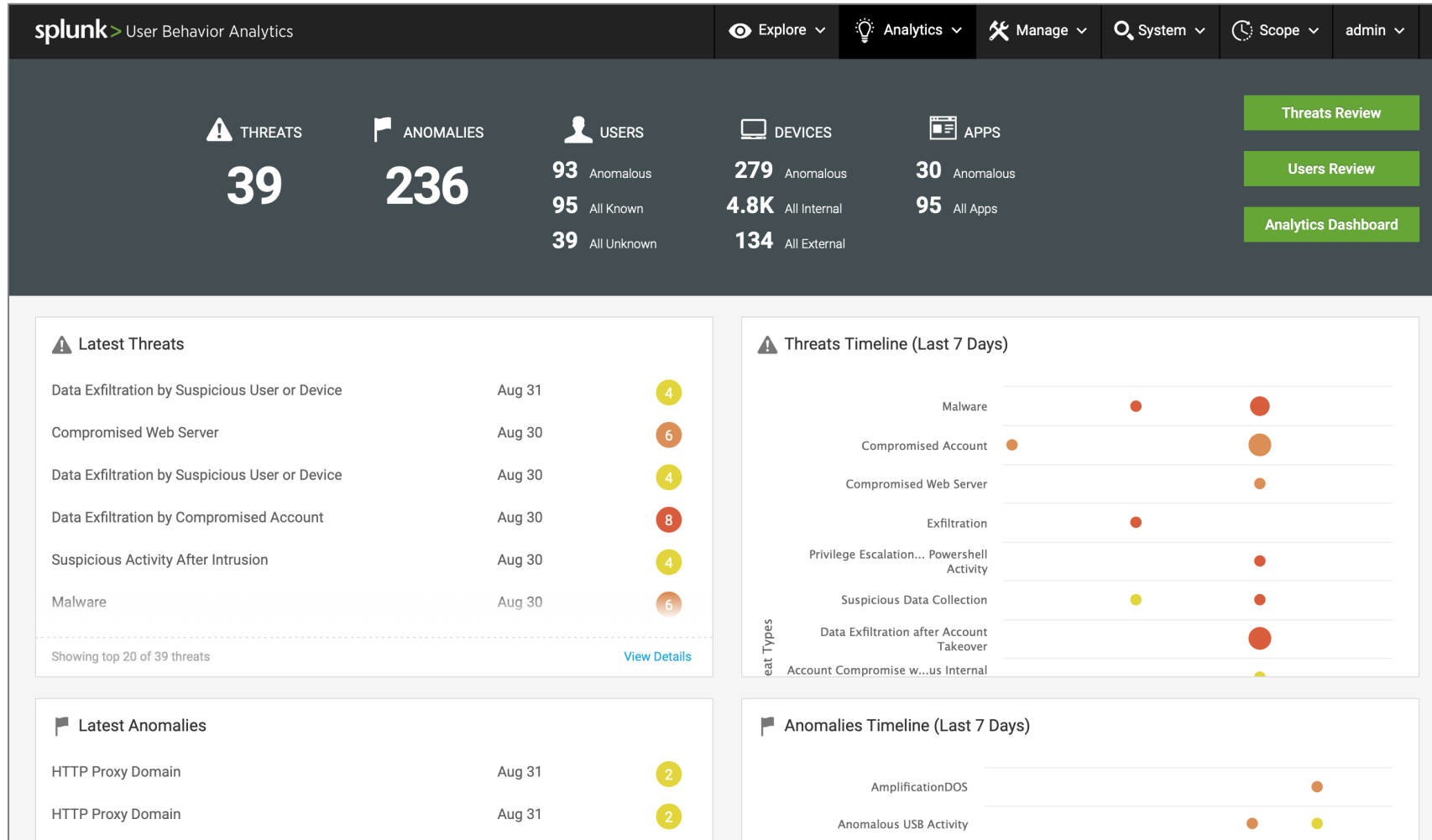
Finalize Use
Cases

Ultimate Goal

Important of operationalizing UBA

Reduce False
Positives

Roles

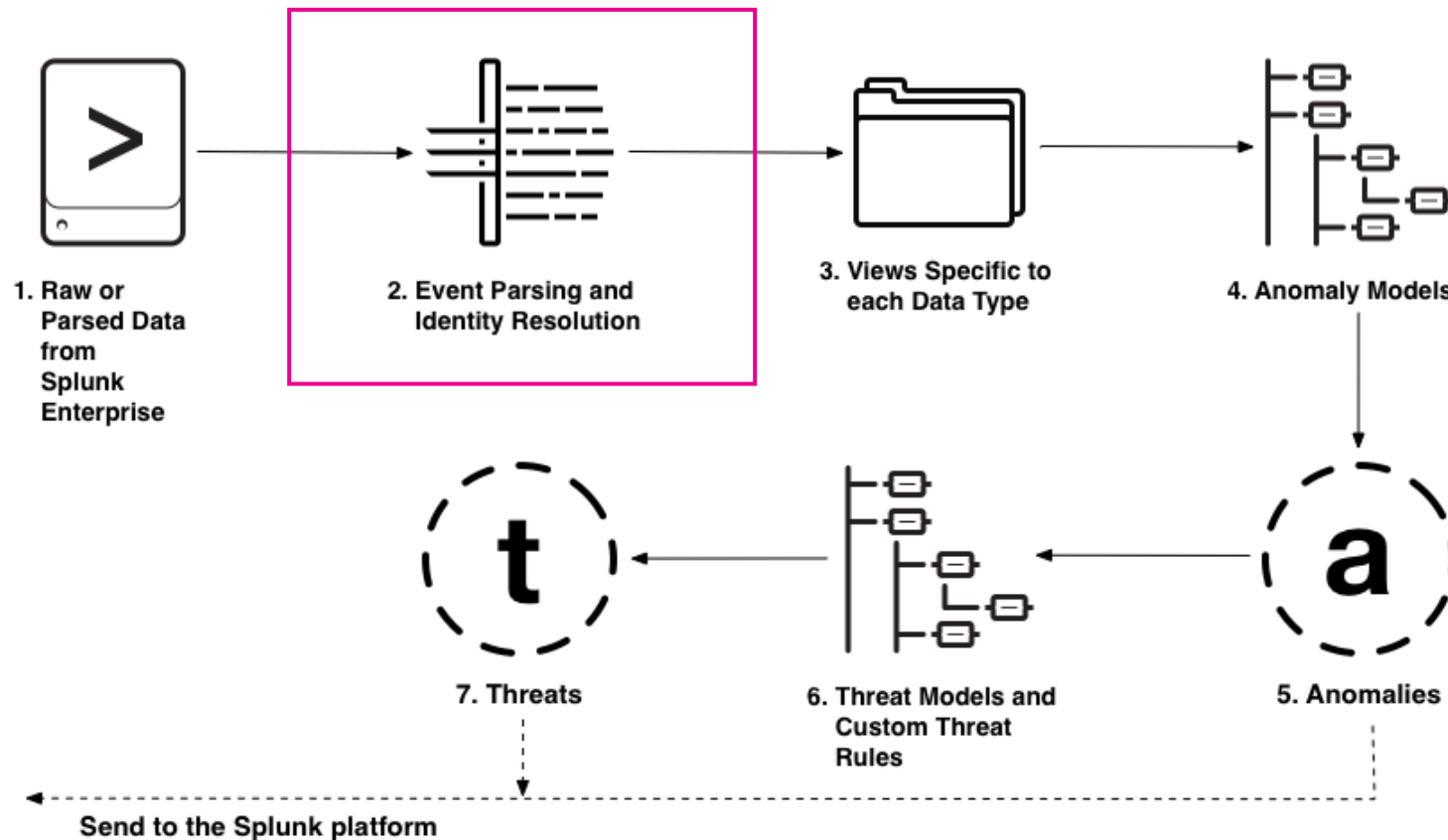


Finalize Use
Cases

Establish
Workflows

Identity Resolution

Tuning



Time Series



UBA/ UEBA Detection

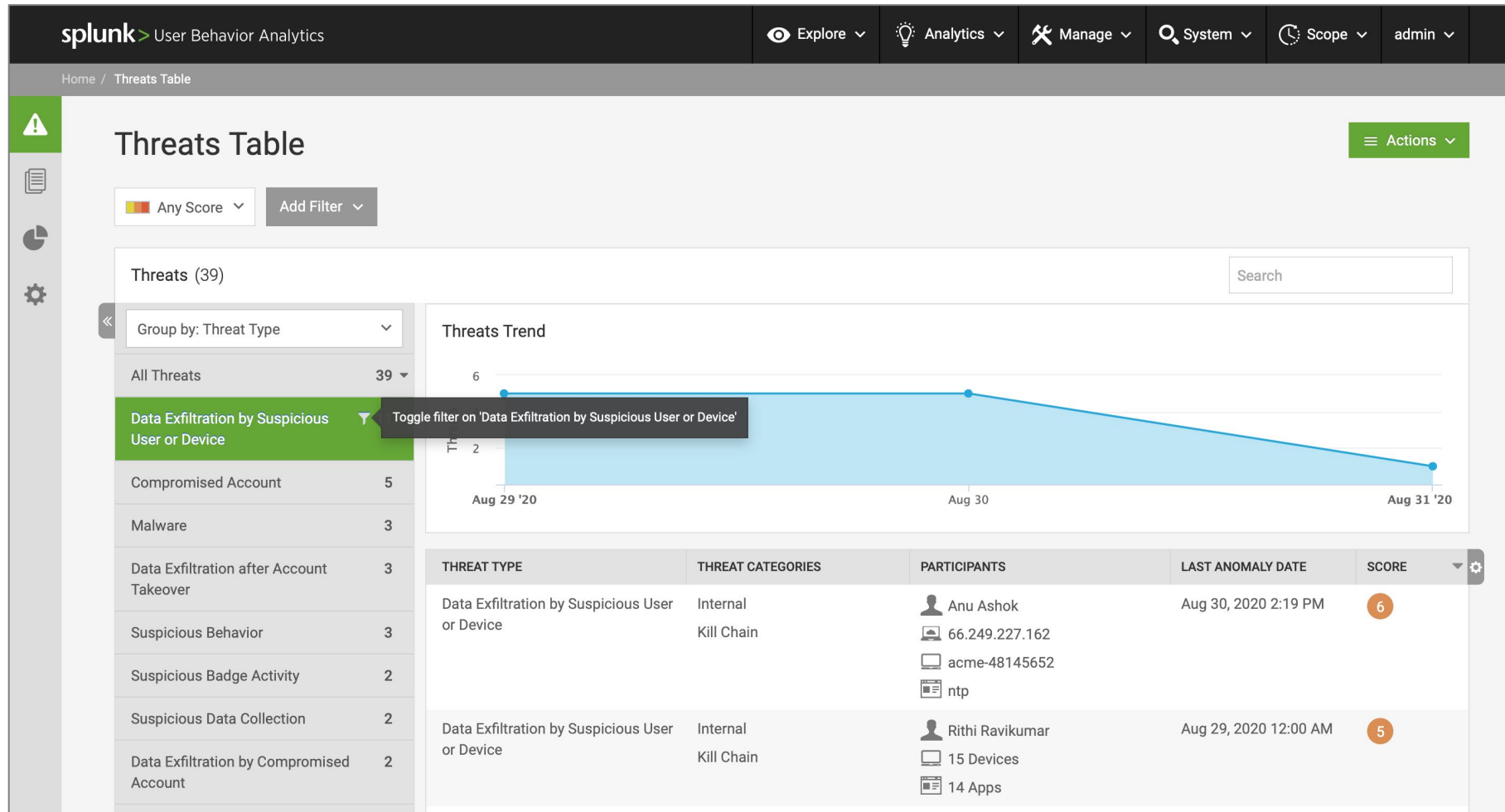
- Risk behavior detection
- Entity profiling, scoring
- Kill chain, graph analysis

Realm of unknown

Rare Series

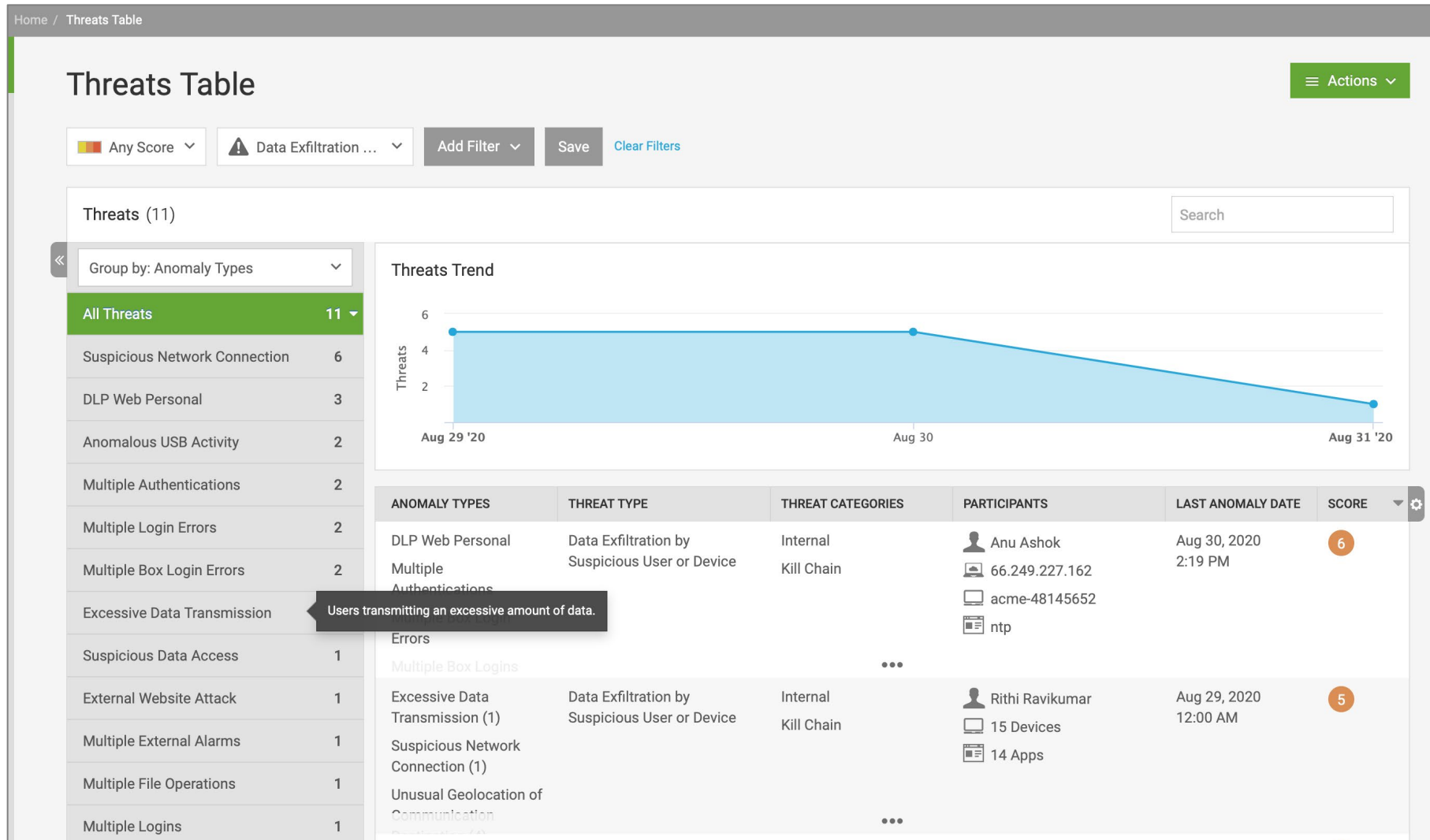
Anomaly Action Rules

Tuning



Anomaly Action Rules

Tuning



Customize Threat Rules

Tuning

The screenshot displays the 'Custom Threats' configuration page in Splunk. A modal dialog titled 'Clone Threat Rule' is open, showing 'Step 1 of 6 : Select Participant'. The dialog explains that a custom threat is generated for each participant matching the criteria and offers two options: 'User' (represented by a green icon) and 'Device' (represented by a laptop icon). The 'User' option is currently selected. The background shows a table of 17 threat rules, including 'Watering Hole Infection', 'Data Exfiltration after Account Takeover, Medium', 'Suspicious Domain Communication followed by Malware Activity', 'Data Exfiltration after Account Takeover, High', 'Suspicious HTTP Redirects followed by Suspected Infection', 'Potential Flight Risk Staging', 'Data Exfiltration after Data Staging', 'Malicious URI Communications with Potential Malware', 'Multiple failed badge attempts and unusual badge access time', and 'Privilege Escalation after Powershell Activity'. Each rule has a description and a category (e.g., Malware, Suspicious, Privilege Escalation). A '+ New Threat Rule' button is visible in the top right corner of the interface.

NAME	CUSTOM TH
Watering Hole Infection Watering Hole pattern detected along with signs of malware infection.	Malware
Data Exfiltration after Account Takeover, Medium Medium Confidence Data Exfiltration after Account Takeover	Data Exfiltration
Suspicious Domain Communication followed by Malware Activity Detects suspicious communication followed by possible malware activity.	Malware
Data Exfiltration after Account Takeover, High High Confidence Data Exfiltration after Account Takeover	Data Exfiltration
Suspicious HTTP Redirects followed by Suspected Infection Detects HTTP Redirects followed by suspicious activity.	Malware
Potential Flight Risk Staging Looks for Flight Risk users who may be staging sensitive data.	Suspicious
Data Exfiltration after Data Staging Looks for data staging followed by data exfiltration.	Suspicious
Malicious URI Communications with Potential Malware Communication Attempts to URIs categorized as Malicious by URI filtering followed by other indicators of compromise.	Malware
Multiple failed badge attempts and unusual badge access time Detects users that attempted access into multiple or unusual entry locations at an unusual time.	Suspicious
Privilege Escalation after Powershell Activity Detects devices with suspicious powershell activity followed by privilege escalation.	Privilege Escalation

Customize Threat Rules

Tuning

The screenshot displays the 'Custom Threats' interface in Splunk. A modal dialog titled 'Clone Threat Rule' is open, showing 'Step 2 of 6 : User Filters'. The dialog includes a search bar for 'Anomalies Count' and a dropdown menu for 'City' set to 'Include'. Below these, there are checkboxes for various user roles: Administrators, Engineering, Finance, HR, IT, Sales, and Support. The 'OU' option is currently selected and highlighted in green. At the bottom of the dialog, there are 'Cancel', '< Back', and 'Next >' buttons.

Custom Threats

Threat Rules (17)

NAME	CUSTOM TH
Watering Hole Infection Watering Hole pattern detected along with signs of malware infection.	Malware
Data Exfiltration after Account Takeover, Medium Medium Confidence Data Exfiltration after Account Takeover	Data Exfiltration
Suspicious Domain Communication followed by Malware Activity Detects suspicious communication followed by possible malware activity.	Malware
Data Exfiltration after Account Takeover, High High Confidence Data Exfiltration after Account Takeover	Data Exfiltration
Suspicious HTTP Redirects followed by Suspected Infection Detects HTTP Redirects followed by suspicious activity.	Malware
Potential Flight Risk Staging Looks for Flight Risk users who may be staging sensitive data.	Suspicious
Data Exfiltration after Data Staging Looks for data staging followed by data exfiltration.	Suspicious
Malicious URI Communications with Potential Malware Communication Attempts to URIs categorized as Malicious by URI filtering followed by other indicators of compromise.	Malware
Multiple failed badge attempts and unusual badge access time Detects users that attempted access into multiple or unusual entry locations at an unusual time.	Suspicious
Privilege Escalation after Powershell Activity Detects devices with suspicious powershell activity followed by privilege escalation.	Privilege Escalation
Suspicious URI Communications and Redirects	Malware

Clone Threat Rule

Step 2 of 6 : User Filters

Anomalies Count: Search

City: Include

Country:

Departing User:

Employee Type:

High Risk User:

HR Record:

On Performance Improvement Plan:

OU

Specific Users

☐ Administrators

☐ Engineering

☐ Finance

☐ HR

☐ IT

☐ Sales

☐ Support

Cancel < Back Next >

Threat Hunter vs. Analyst

Roles

Analyst

Investigating UBA
Threats in Threats
Table

Hunter

**Content
Developer**

Admin

Threat Hunter vs. Analyst

Roles

Analyst

Investigating UBA
Threats in Threats
Table

Hunter

Investigating UBA
Anomalies/ Unknown
Threats in Splunk
UBA Platform

Content Developer

Admin

Threat Hunter vs. Analyst

Roles

Analyst

Investigating UBA
Threats in Threats
Table

Hunter

Investigating UBA
Anomalies/ Unknown
Threats in Splunk
UBA Platform

Content Developer

- Focused on Use Cases
- Fine Tuning Use Cases
- Use Case Framework
- Onboarding New Data Sources
- Adding Blacklisted IP's or Domains

Admin

Threat Hunter vs. Analyst

Roles

Analyst

Investigating UBA
Threats in Threats
Table

Hunter

Investigating UBA
Anomalies/ Unknown
Threats in Splunk
UBA Platform

Content Developer

- Focused on Use Cases
- Fine Tuning Use Cases
- Use Case Framework
- Onboarding New Data Sources
- Adding Blacklisted IP's or Domains

Admin

Managing Platform
Infrastructure

Threat Hunter vs. Analyst

Roles

Who Will?

Reduce False Positives | Creating Custom Anomaly Action Rules | Create Custom Threat Rules

Analyst

Investigating UBA
Threats in Threats
Table

Hunter

Investigating UBA
Anomalies/ Unknown
Threats in Splunk
UBA Platform

Content Developer

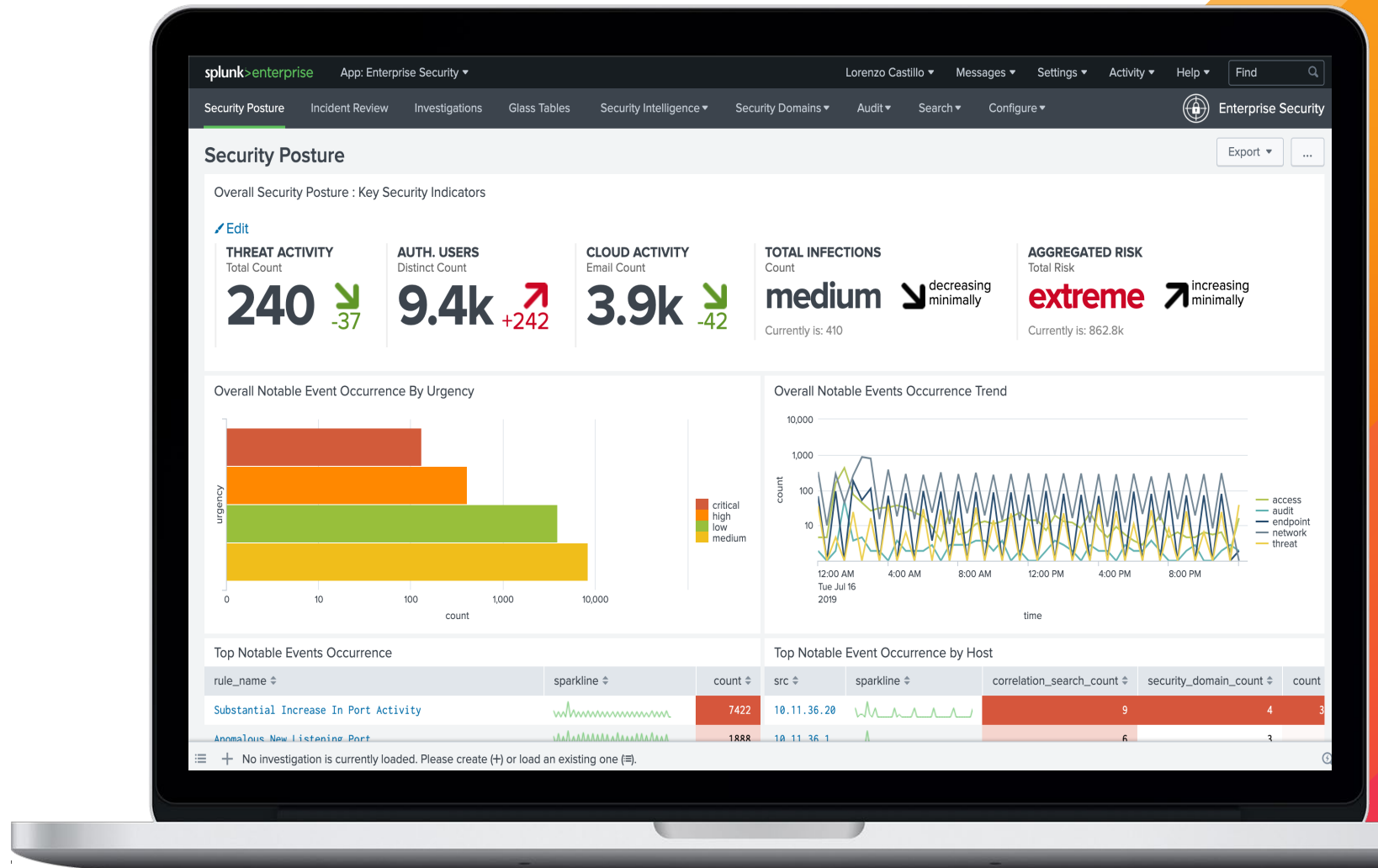
- Focused on Use Cases
- Fine Tuning Use Cases
- Use Case Framework
- Onboarding New Data Sources
- Adding Blacklisted IP's or Domains

Admin

Managing Platform
Infrastructure

Workflow

Understand how to
integrate Splunk UBA into
your Security Operations



Key Takeaways

Lessons Learned

