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.

Annette Fontanilla

Sr. Professional Services Consultant | Splunk

splunk> .conf20

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	Reality
No tuning required	Noisy IPS/IDS, DLP alerts
False positives will disappear... eventually	Network changes
Just add data	Data hygiene is key
Data science will solve everything	Known behavior vs. unknown behavior

splunk> .conf20

~~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

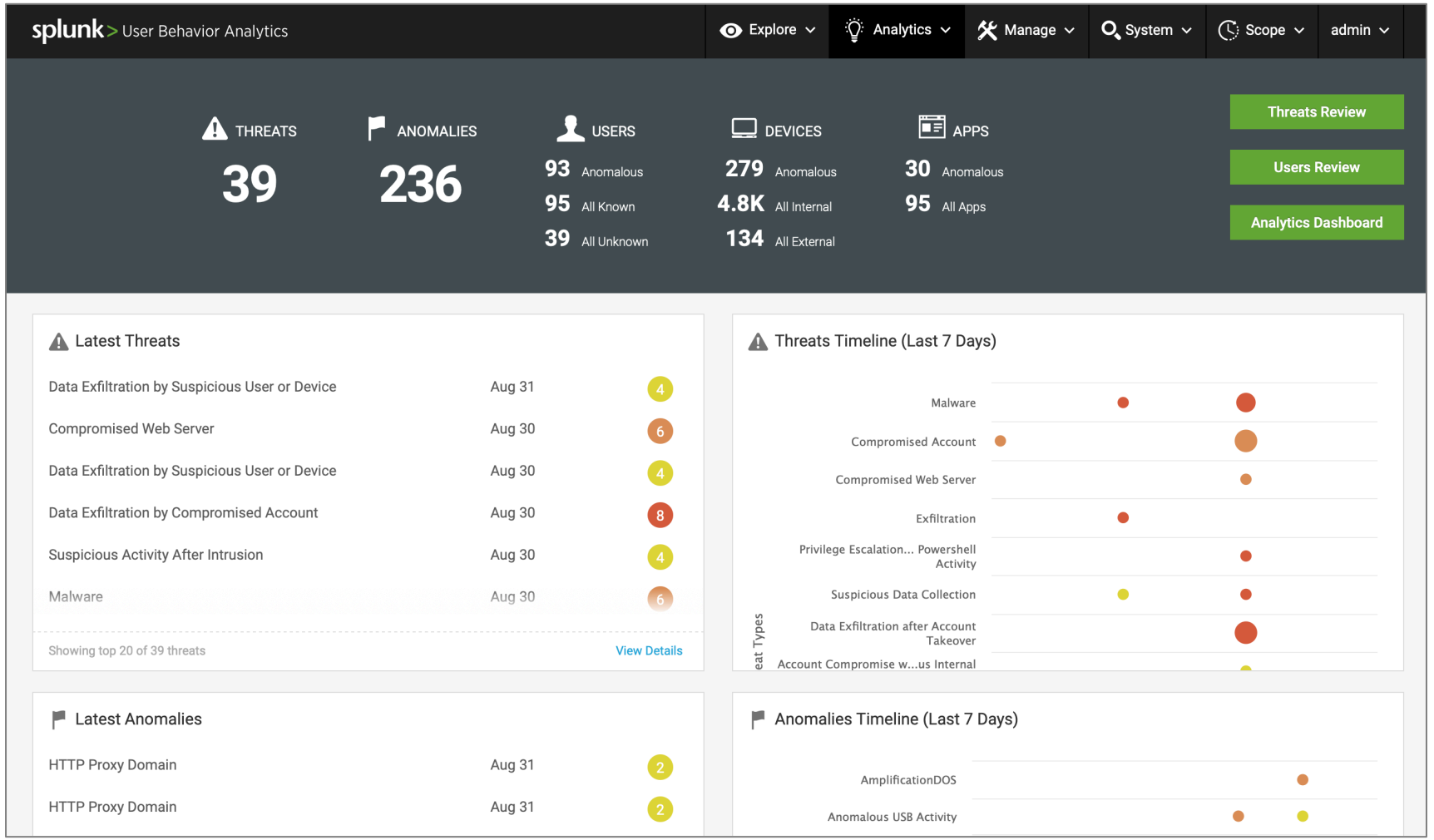
Alerting tools can cause several false positives in UBA due to a misconfiguration or noisy alert

Discovery

Understanding devices and user/service account or device roles

Ultimate Goal

Important of operationalizing UBA

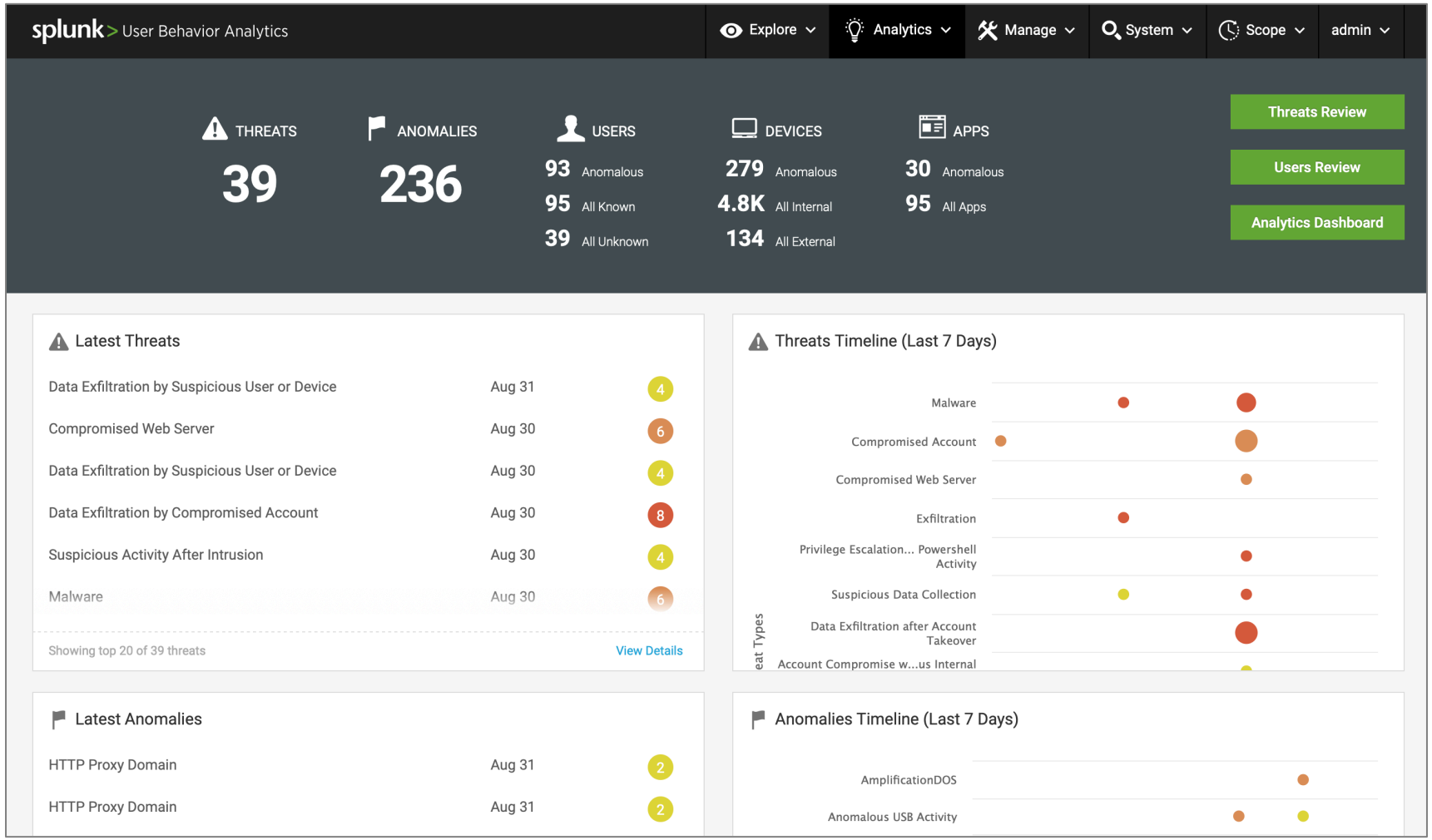


splunk> .conf20

Ultimate Goal

Important of operationalizing UBA

Reduce False Positives

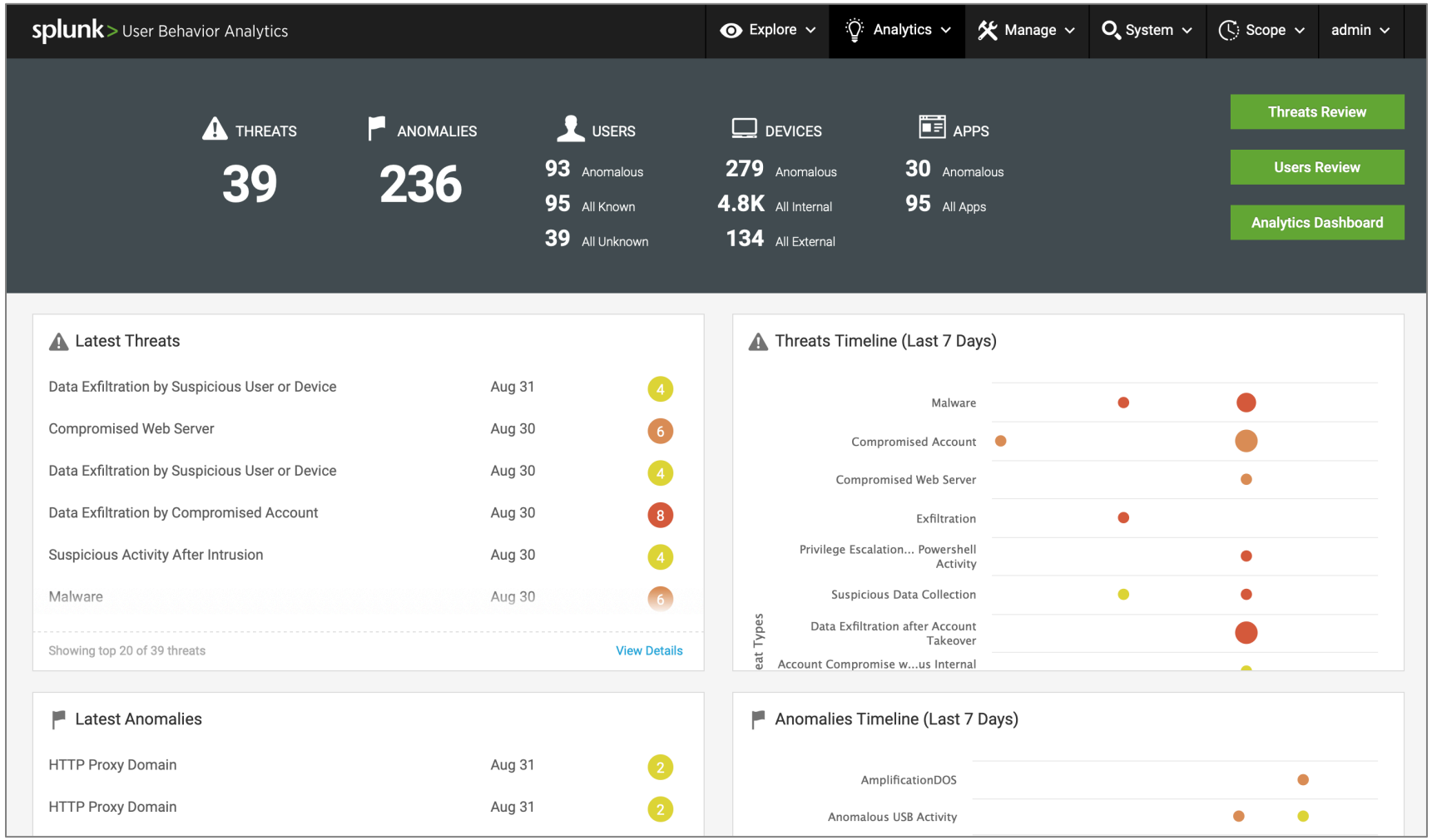


splunk> .conf20

Ultimate Goal

Important of operationalizing UBA

Reduce False Positives



Finalize Use Cases

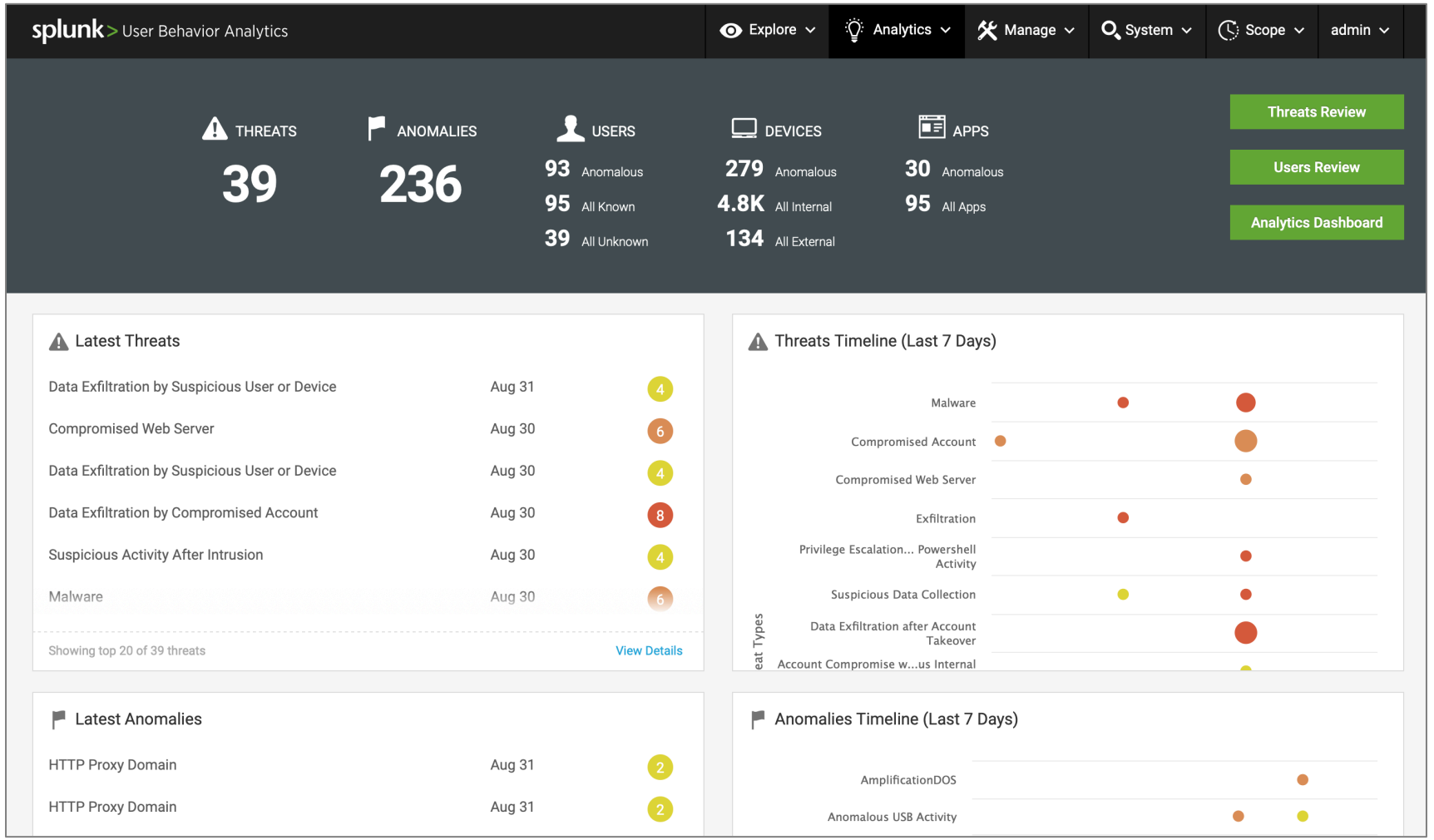
splunk> .conf20

Ultimate Goal

Important of operationalizing UBA

Reduce False Positives

Roles



Finalize Use Cases

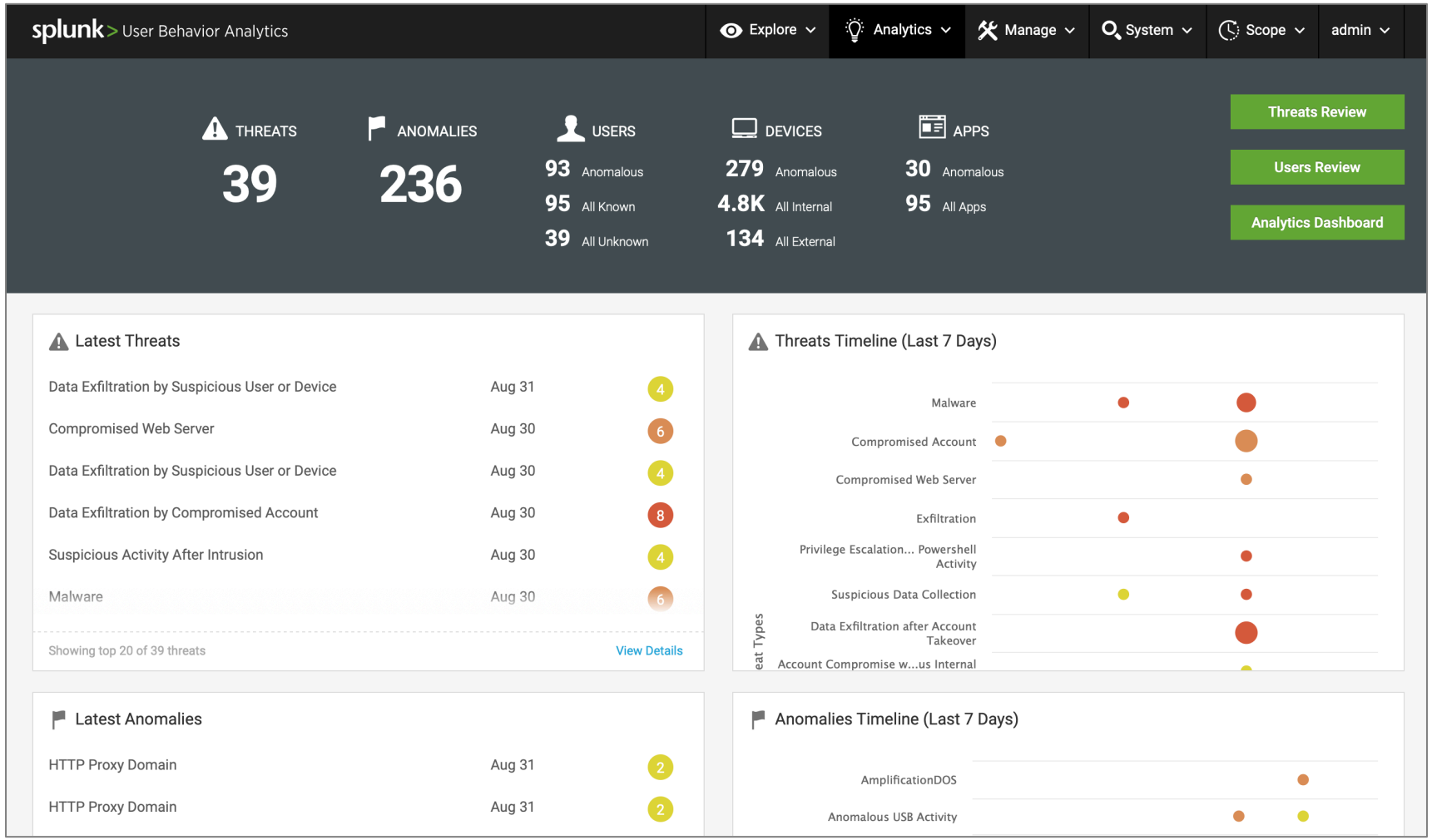
splunk> .conf20

Ultimate Goal

Important of operationalizing UBA

Reduce False Positives

Roles



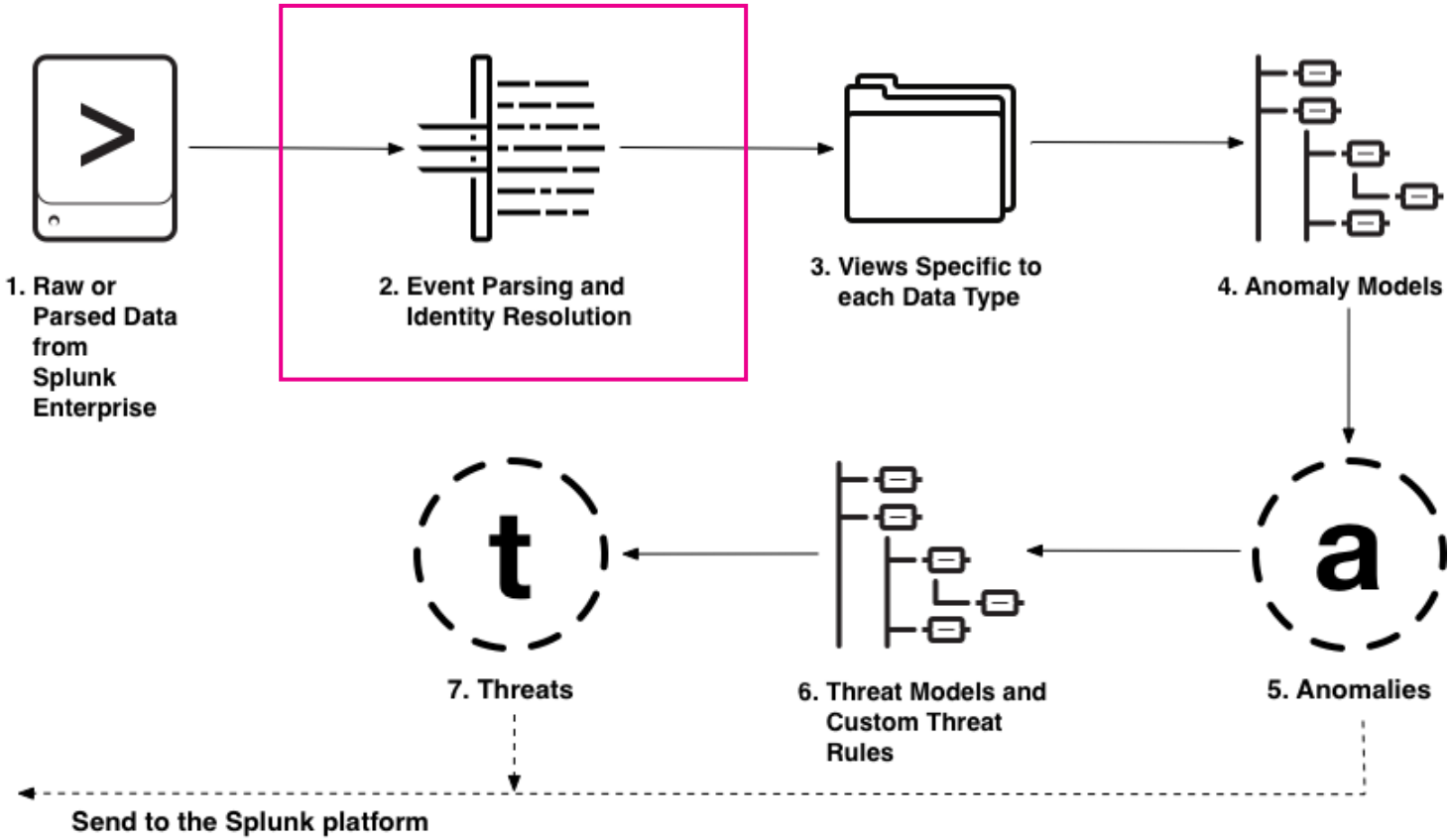
Finalize Use Cases

Establish Workflows

splunk> .conf20

Identity Resolution

Tuning



Time Series

UBA/ UEBA

Detection

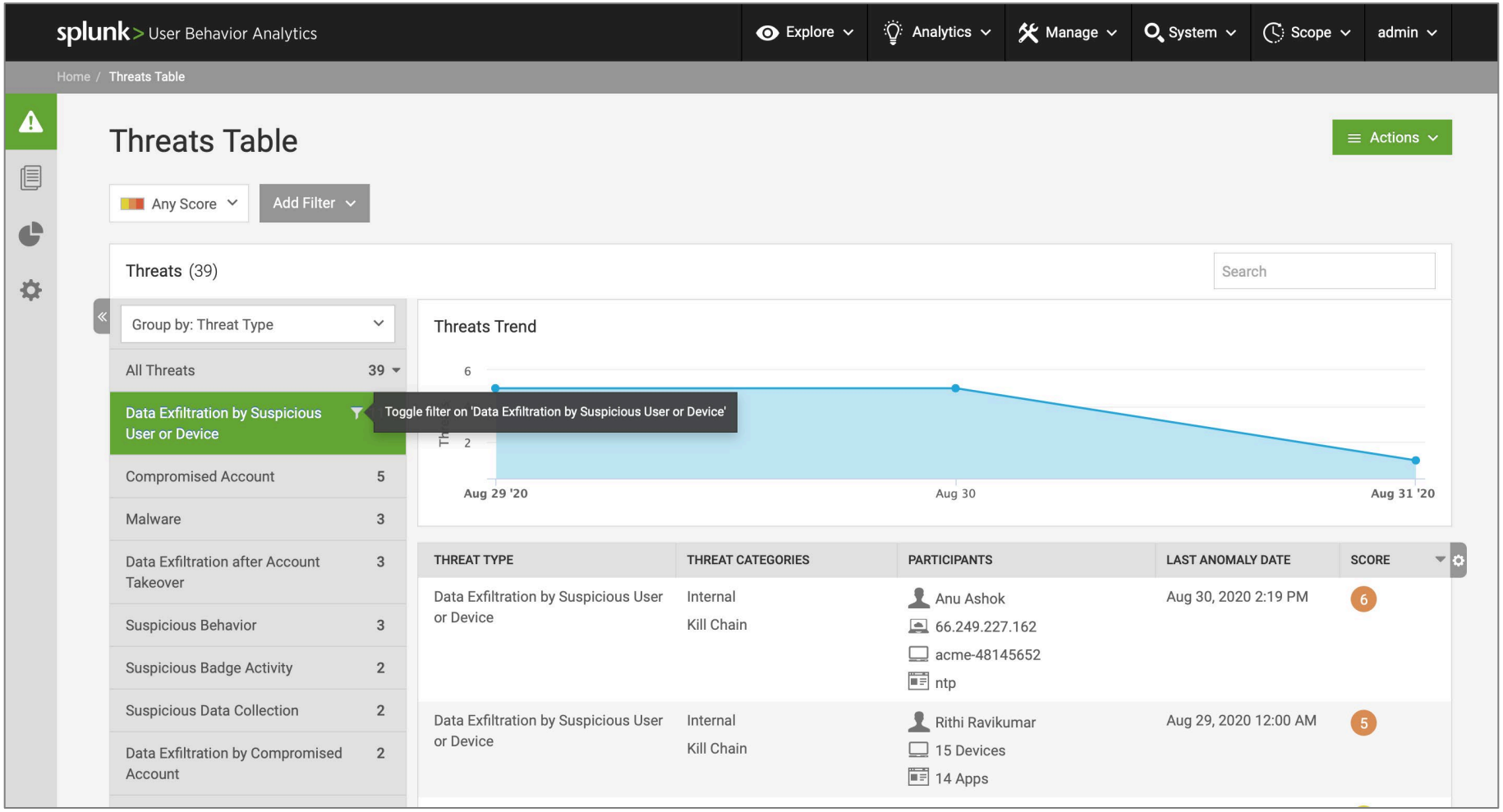
- Risk behavior detection
- Entity profiling, scoring
- Kil chain, graph analysis

Realm of unknown

Rare Series

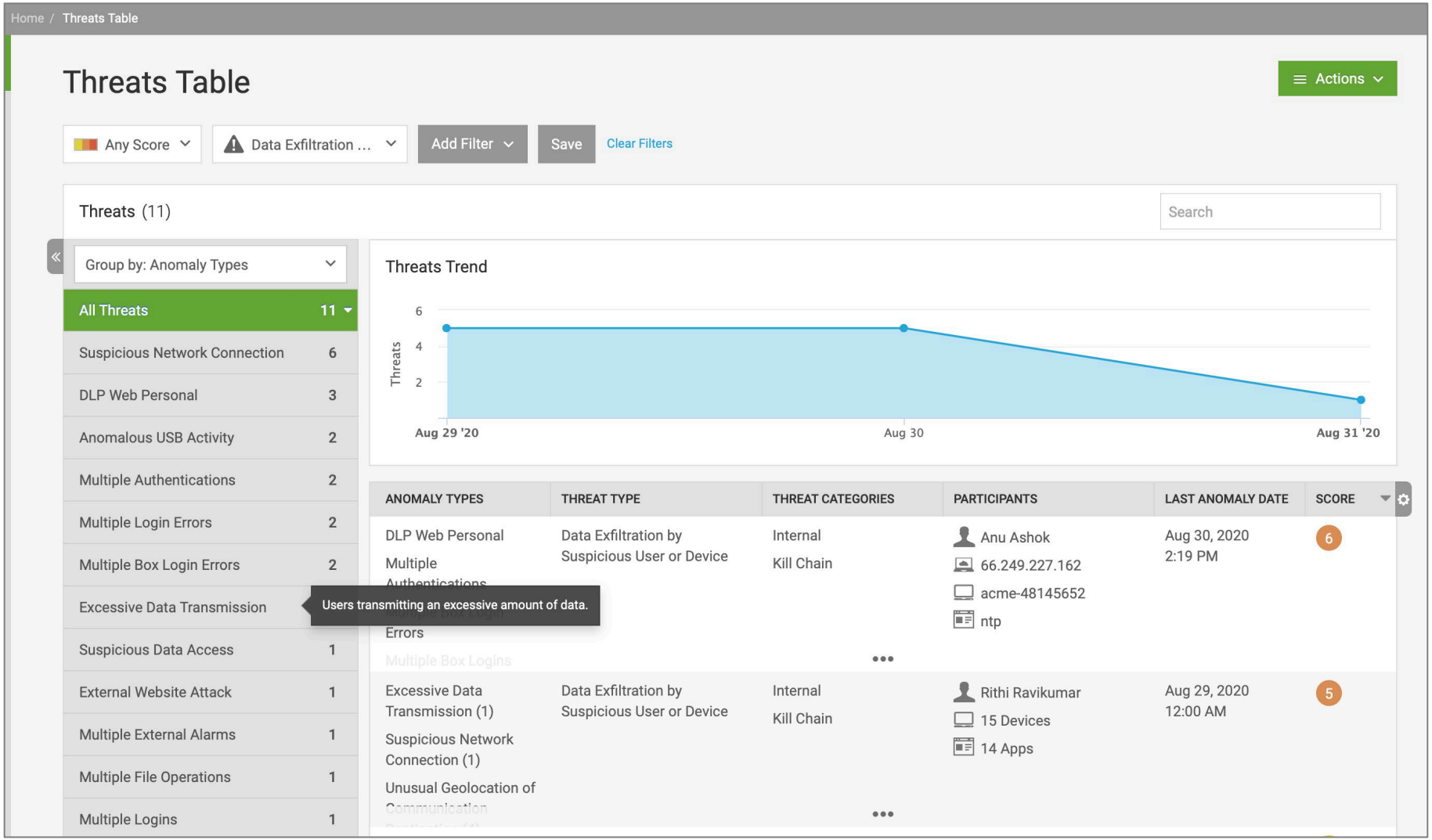
Anomaly Action Rules

Tuning



Anomaly Action Rules

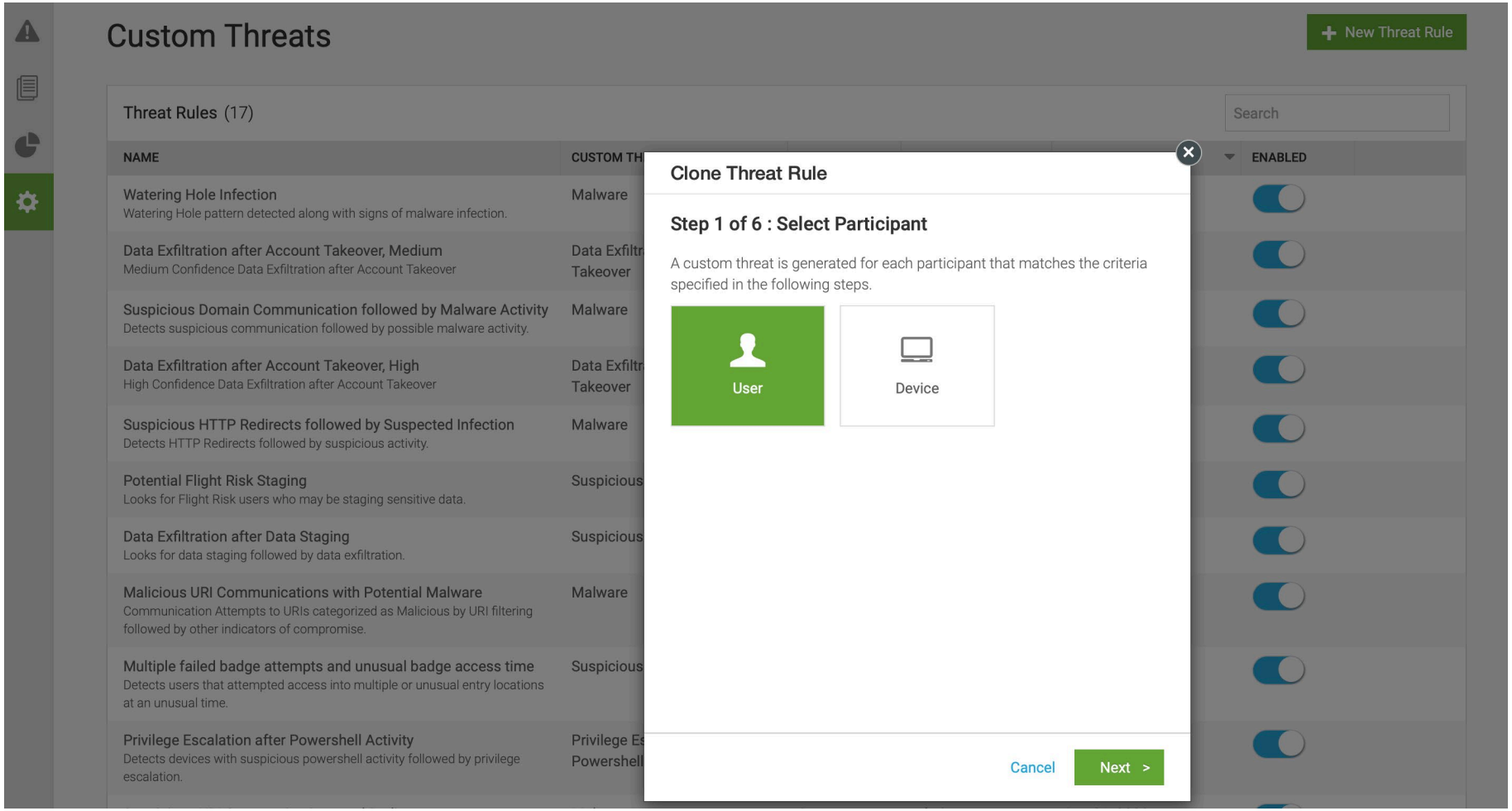
Tuning



splunk> .conf20

Customize Threat Rules

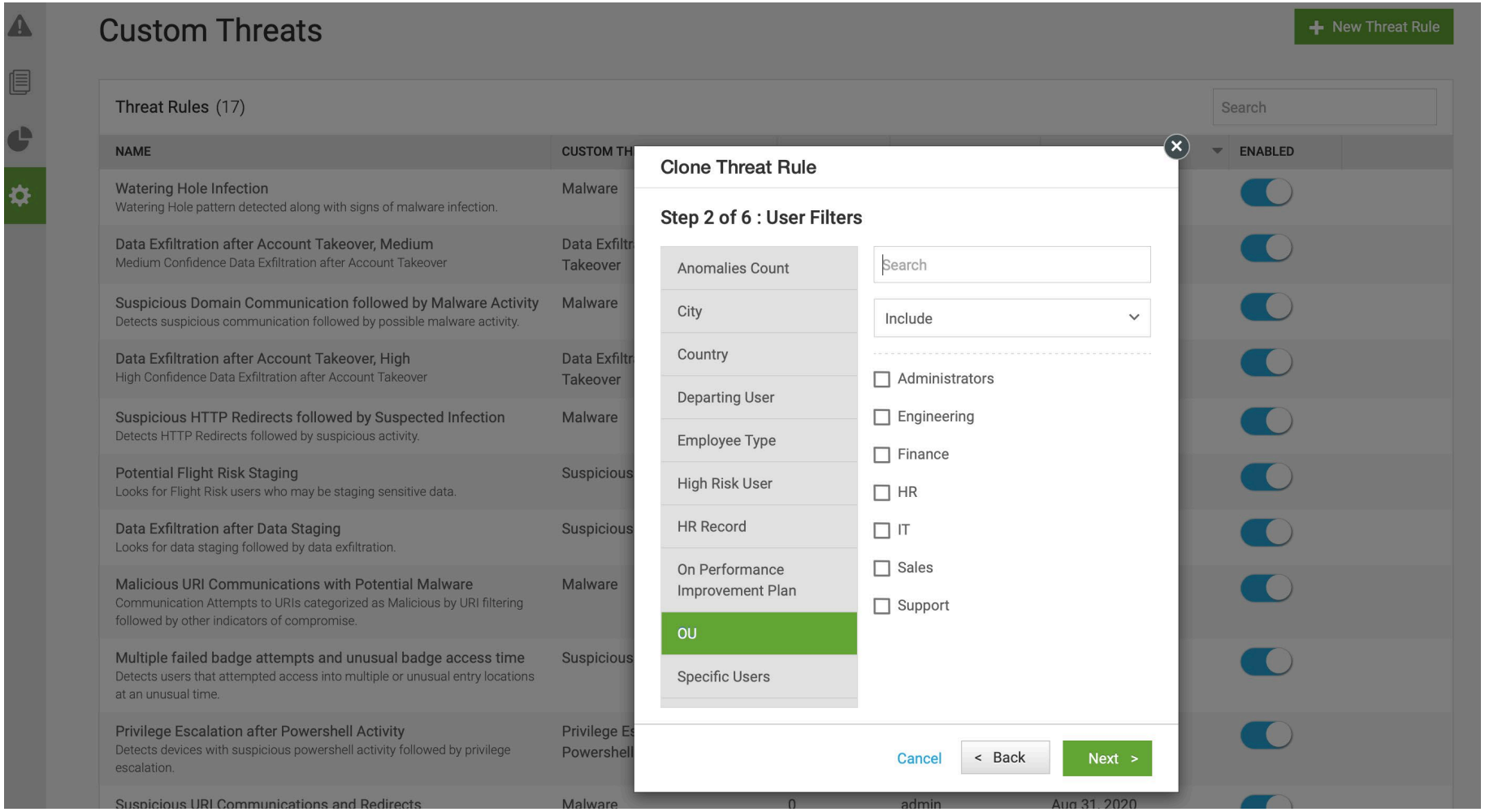
Tuning



splunk> .conf20

Customize Threat Rules

Tuning



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

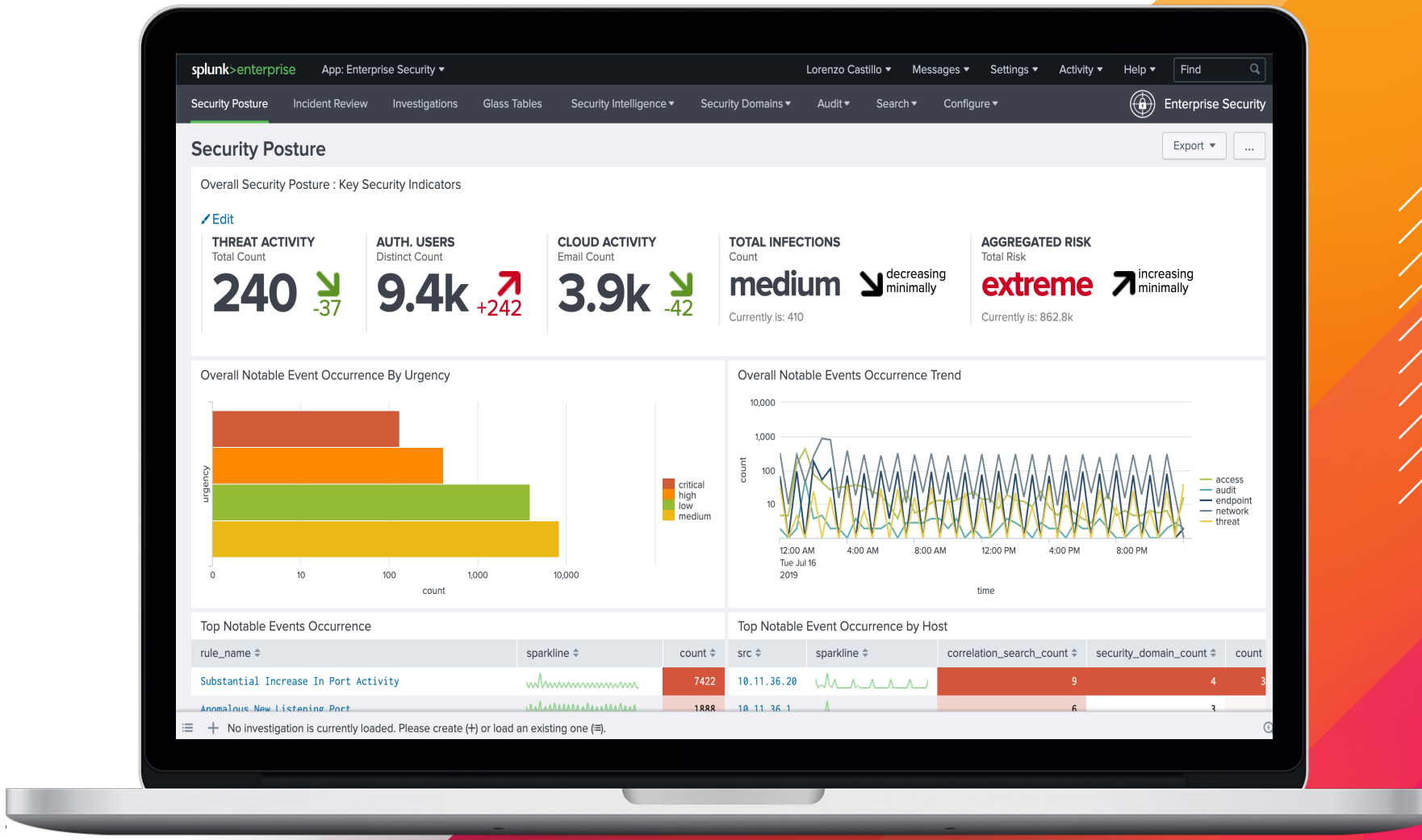
- Focused on Use Cases
- Fine Tuning Use Cases
- Use Case Framework
- Onboarding New Data Sources
- Adding Blacklisted IP's or Domains

Admin

Managing Platform Infrastructure

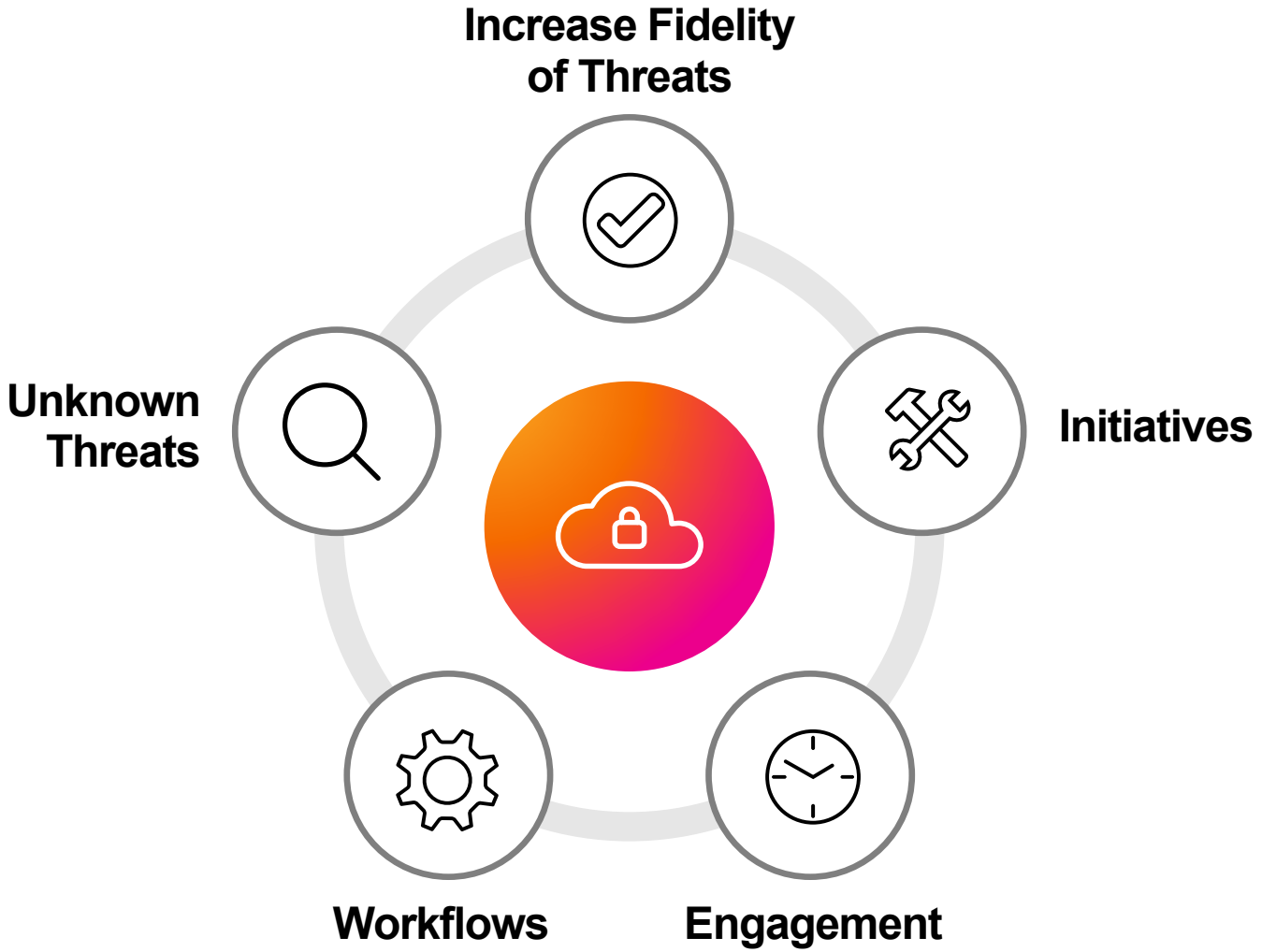
Workflow

Understand how to integrate Splunk UBA into your Security Operations



Key Takeaways

Lessons Learned



Thank You

Please provide feedback via the

SESSION SURVEY