How to Mitigate Insider Threat With Splunk UBA

SEC1623

Prasanth Sadanala & Annette Fontanilla

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

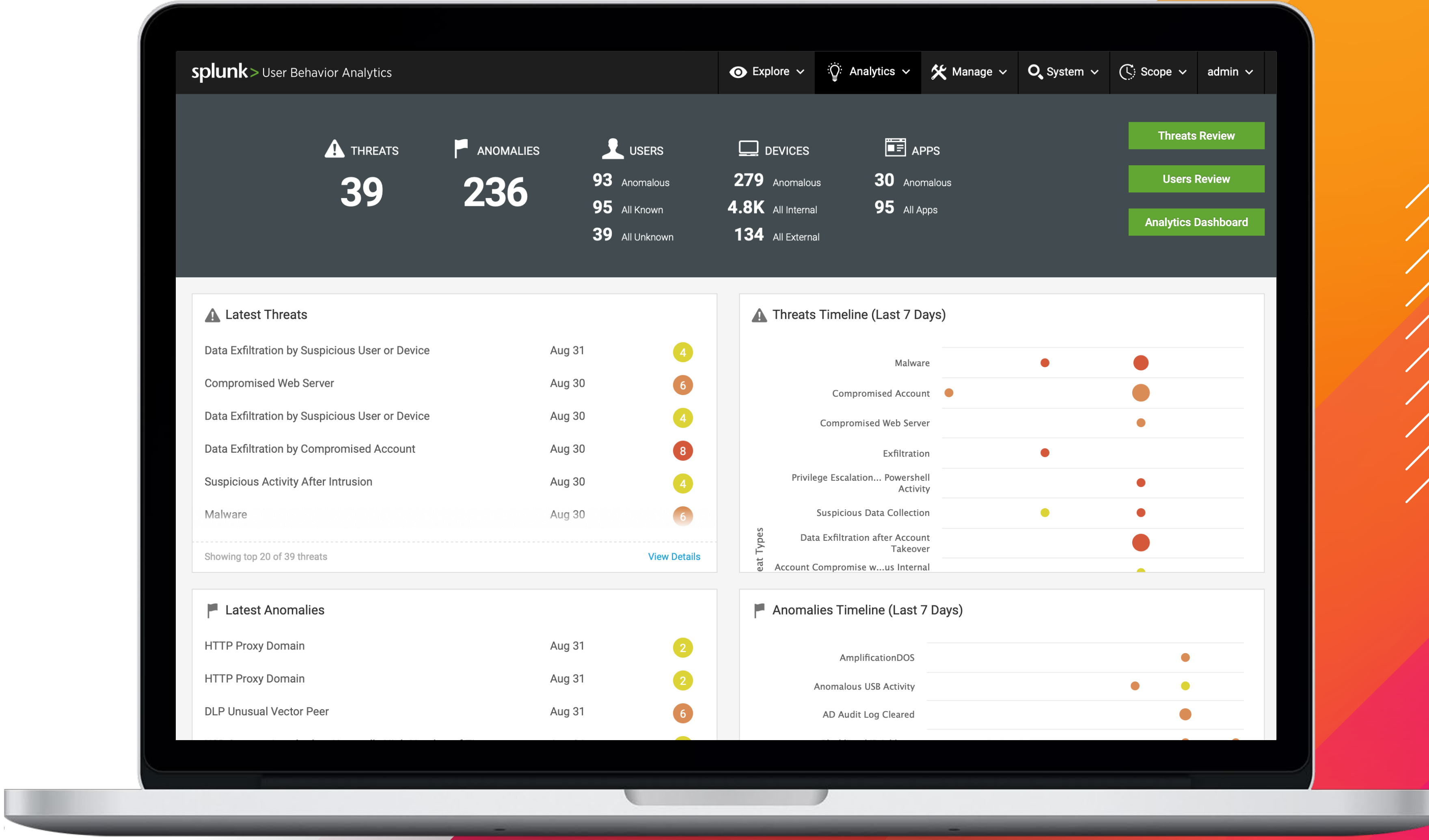
Consultant | Splunk

Prasanth Sadanala

Information Security Specialist | TD Bank

What is Splunk UBA?

Splunk UBA uses machine learning capabilities to help organizations find **hidden threats** and **anomalous** behavior across users, devices and applications. Splunk UBA detects insider threats using out-of-the-box use cases that use **unsupervised machine learning algorithms**.



splunk> User Behavior Analytics

THREATS 39

ANOMALIES 236

USERS
93 Anomalous
95 All Known
39 All Unknown

DEVICES
279 Anomalous
4.8K All Internal
134 All External

APPS
30 Anomalous
95 All Apps

Latest Threats

Data Exfiltration by Suspicious User or Device	Aug 31	4
Compromised Web Server	Aug 30	6
Data Exfiltration by Suspicious User or Device	Aug 30	4
Data Exfiltration by Compromised Account	Aug 30	8
Suspicious Activity After Intrusion	Aug 30	4
Malware	Aug 30	6

Showing top 20 of 39 threats

View Details

Threats Timeline (Last 7 Days)

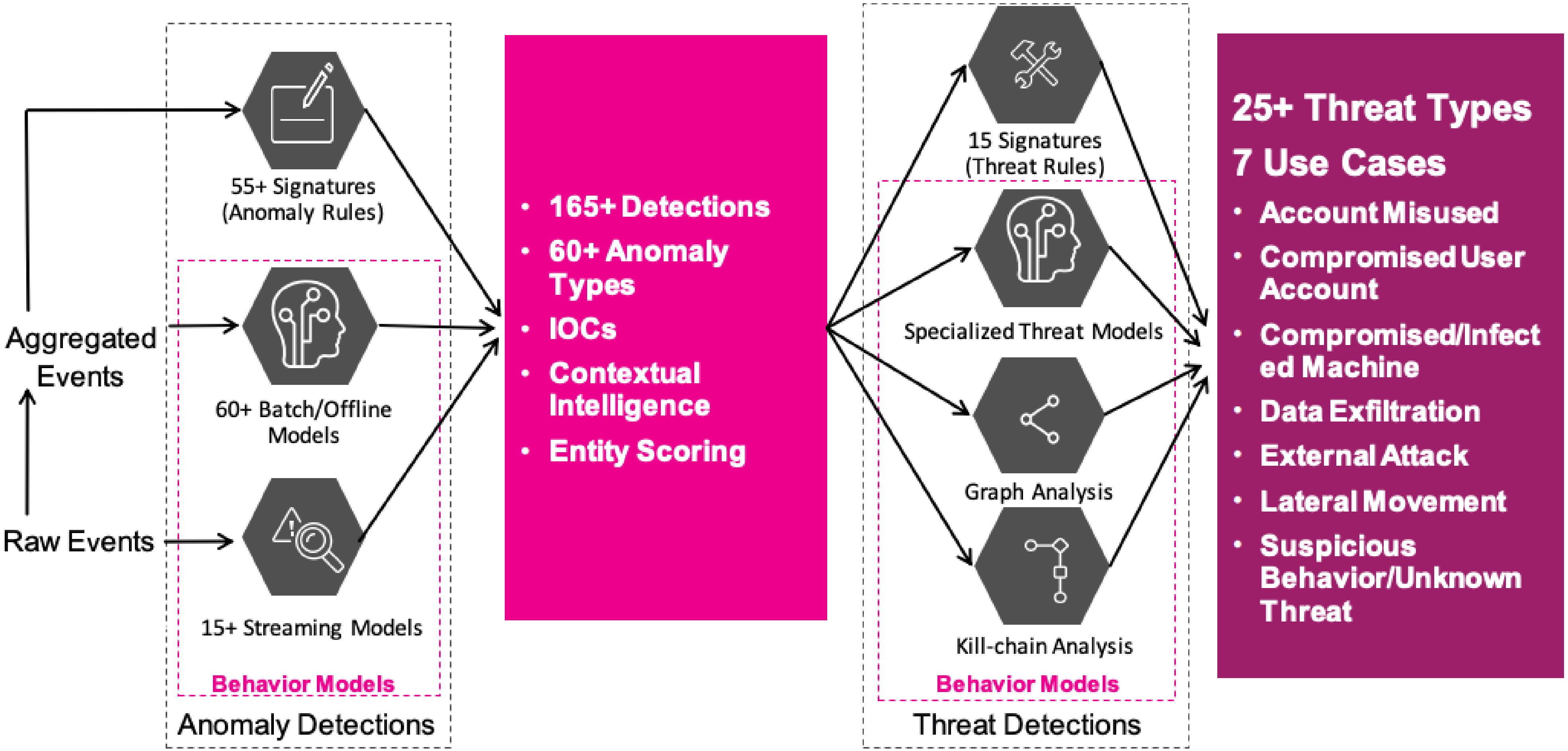
Malware
Compromised Account
Compromised Web Server
Exfiltration
Privilege Escalation... Powershell Activity
Suspicious Data Collection
Data Exfiltration after Account Takeover
Account Compromise w...us Internal
eat Types

Latest Anomalies

HTTP Proxy Domain	Aug 31	2
HTTP Proxy Domain	Aug 31	2
DLP Unusual Vector Peer	Aug 31	6

Anomalies Timeline (Last 7 Days)

Splunk UBA Detections



Aggregated Events

Raw Events

55+ Signatures (Anomaly Rules)

60+ Batch/Offline Models

15+ Streaming Models

Behavior Models

Anomaly Detections

- 165+ Detections
- 60+ Anomaly Types
- IOCs
- Contextual Intelligence
- Entity Scoring

15 Signatures (Threat Rules)

Specialized Threat Models

Graph Analysis

Kill-chain Analysis

Behavior Models

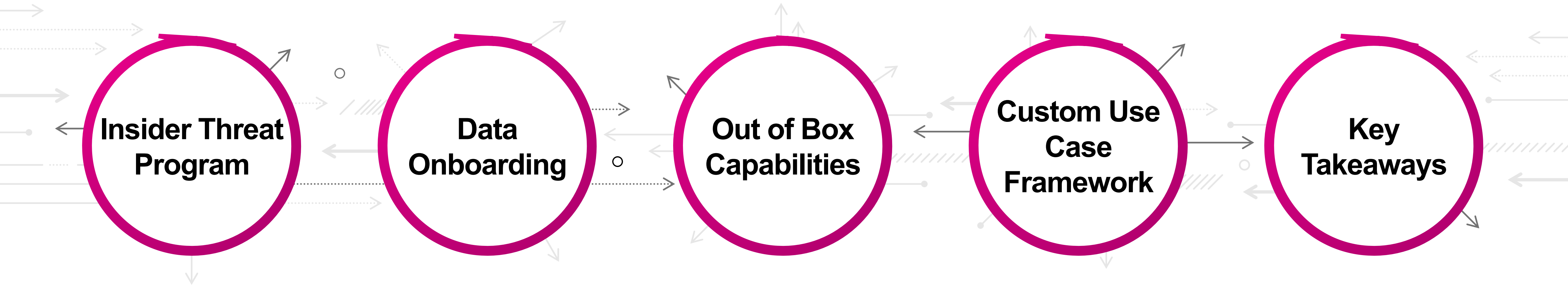
Threat Detections

25+ Threat Types

7 Use Cases

- Account Misused
- Compromised User Account
- Compromised/Infected Machine
- Data Exfiltration
- External Attack
- Lateral Movement
- Suspicious Behavior/Unknown Threat

Agenda



Insider Threat Program

Data Onboarding

Out of Box Capabilities

Custom Use Case Framework

Key Takeaways

Insider Threat Program

What to consider?

1. **Include the proper stakeholders**
   Human Resources, Legal, Privacy, Risk Management, Information Technology and Security
2. **Identify the company’s most valuable assets**
   People, Information, Intellectual Property, Technology
3. **Intentional vs. Unintentional insiders**
   Negligence vs. Malicious/Financial Gain/Disgruntled Employees
4. **Security Policies**
   Data Use Policy
5. **Build Insider Threat Use Cases**
   Aside from Data Loss Prevention
6. **Apply Lessons Learned**
   Identify Gaps, Use Case Development

Common Types of Malicious Insiders

Types

- Espionage/Inside Agents
- Disgruntled Employees
- Negligent Employees
- Compromised/Vulnerable Employees

Insider Threat Patterns

- Abuse of Privilege
- Human Error
- Policy Violators
- Data Exfiltration

Common Types of Malicious Insiders

Types

- Espionage/Inside Agents
- **Disgruntled Employees**
- Negligent Employees
- **Compromised/Vulnerable Employees**

Insider Threat Patterns

- Abuse of Privilege
- Human Error
- **Policy Violators**
- Data Exfiltration

Common Types of Malicious Insiders

Types

- **Espionage/Inside Agents**
- Disgruntled Employees
- **Negligent Employees**
- Compromised/Vulnerable Employees

Insider Threat Patterns

- **Abuse of Privilege**
- **Human Error**
- Policy Violators
- **Data Exfiltration**

Data Onboarding

Required

- Assets
- Identities
- Windows Security (AD)
- Firewall
- VPN
- Proxy
- DNS
- DHCP

Data Onboarding

Required

- Assets
- Identities
- Windows Security (AD)
- Firewall
- VPN
- Proxy
- DNS
- DHCP

Nice to Have

- Authentication
- Badge
- Cloud Data
- DLP
- Endpoint
- Email
- External Alarm
- Network IDS/IPS
- Printer

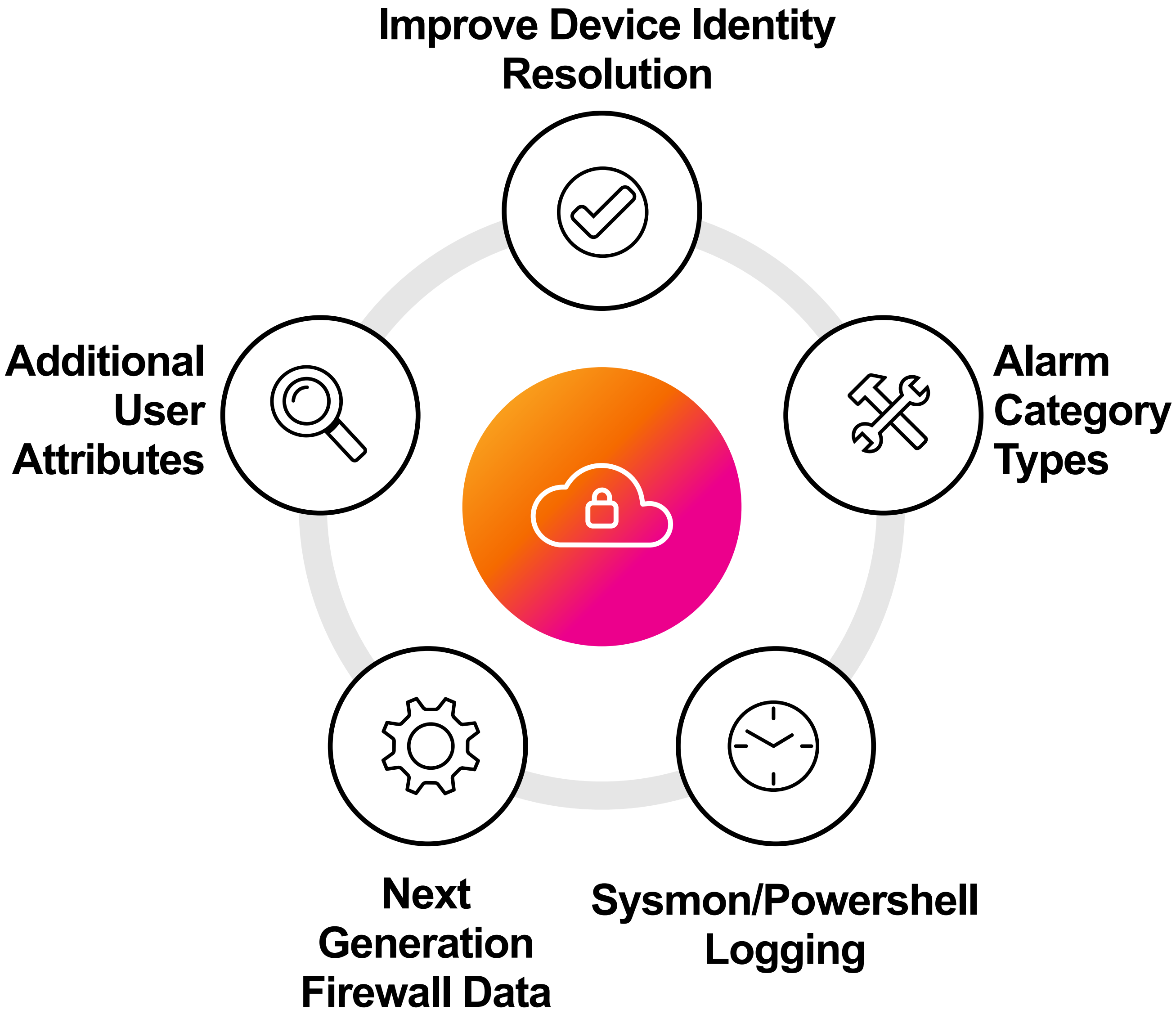
Data Onboarding

Enrichment

- Assets
- Identities
- Windows Security (AD)
- Firewall
- VPN
- Proxy
- DNS
- DHCP
- Authentication
- Badge
- Cloud Data
- DLP
- Endpoint
- Email
- External Alarm
- Network IDS/IPS
- Printer

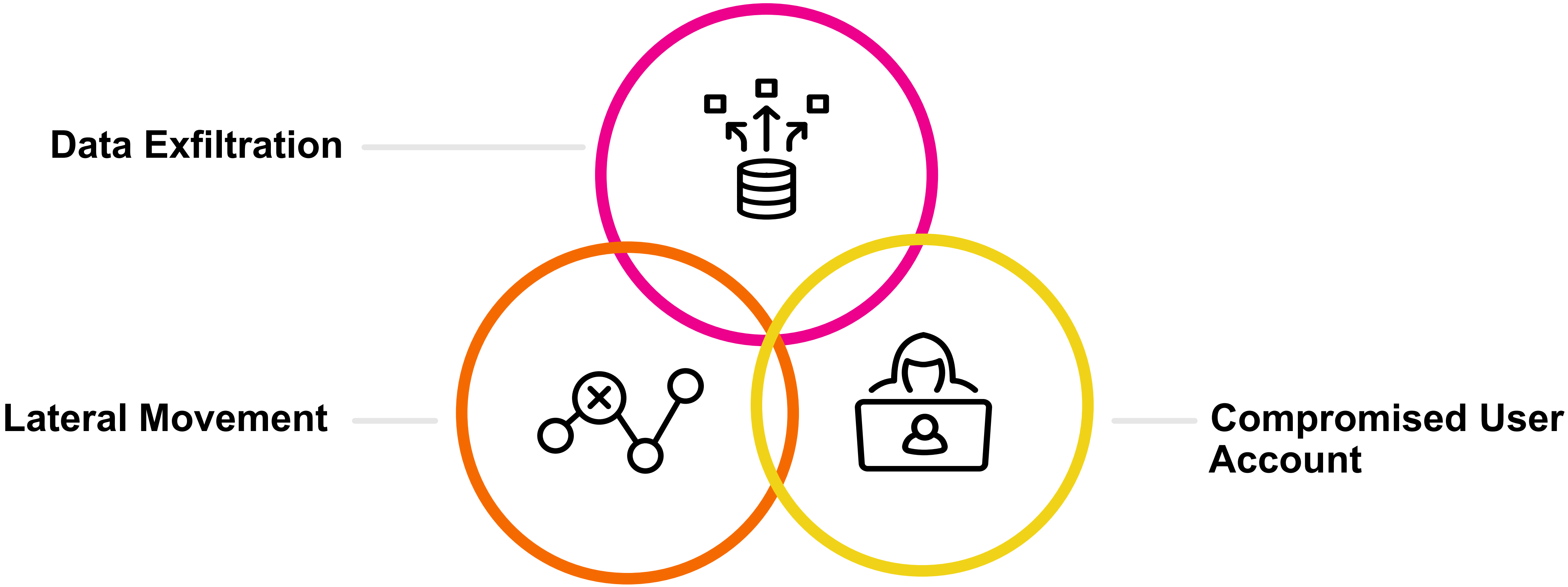
Data Enrichment

Take advantage of out of box capabilities


Improve Device Identity Resolution
Alarm Category Types
Sysmon/Powershell Logging
Next Generation Firewall Data
Additional User Attributes

Out of Box Capabilities

Insider Threat Detection in UBA



Out of Box Capabilities

Data Exfiltration

Anomaly Types

- Suspicious Data movement
- Suspicious Network Connection
- Flight Risk User
- Unusual Printer Usage
- Downloads from Internal Server
- Excessive Data Transmission
- Unusual USB Activity
- Unusual File Extension
- Suspicious New Access

Data Sources

- Firewall
- DLP
- VPN
- Cloud/Box Data
- HTTP

Mitre Framework

Tactic: TA0010 Exfiltration

Techniques:

- T1020 Automated Exfiltration
- T1030 Data Transfer Size Limits
- T1048 Exfiltration Over Alternative protocol
- T1537 Transfer Data to Cloud Account
- T1029 Scheduled Transfer
- T1567 Exfiltration Over Web Service
- T1052 Exfiltration Over USB

Out of Box Capabilities

Compromised User Account

Anomaly Types

- Period with unusual Windows Security Event sequence
- External Alarm
- Blacklisted Application
- Suspicious Network Exploration
- Suspicious AD activity
- Malicious AD activity
- Multiple AD login errors
- Multiple Authentication errors

Data Sources

- AD/Windows Security Events
- External Alarms
- VPN
- Cloud Data
- Authentication

Mitre Framework

Tactic: TA0006 Credential Access

Techniques:

- T1110 Brute Force
- T1555 Credentials from password stores
- T1552 Unsecured Credentials
- T1078 Valid Accounts

Out of Box Capabilities

Lateral Movement

Anomaly Types

- Multiple External Alarms
- Brute Force Attack
- Suspicious Network Exploration
- Local Account Creation
- External Alarm Activity
- Suspicious Powershell Activity
- Scanning Activity
- Unusual External Alarm

Data Sources

- AD/Windows Security Events
- External Alarms
- Network
- Endpoint

Mitre Framework

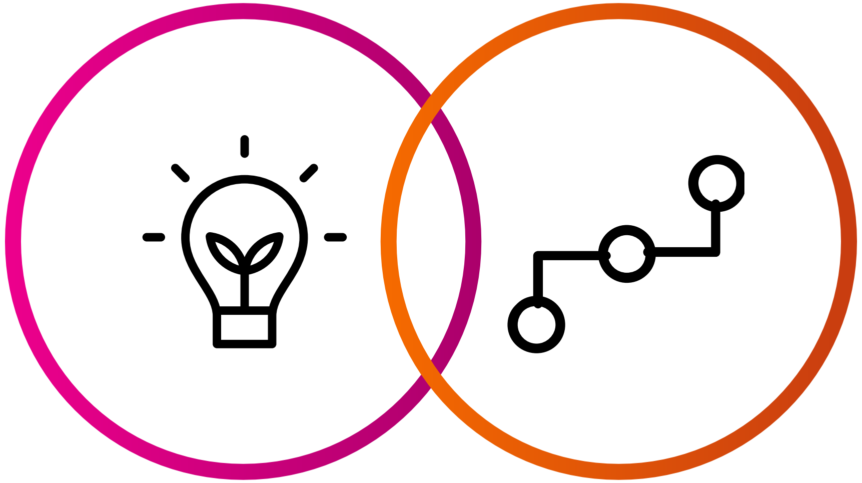
Tactic: TA0008 Lateral Movement

Techniques:

- T1210 Exploitation of Remote Services
- T1570 Lateral Tool Transfer
- T1563 Remote Service Session Hijacking
- T1550 Use Alternate Authentication Material
- T1078 Valid Accounts

Custom Use Case Framework

Rare Events vs. Time Series Models



Rare Events

Unusual Activity

Time Series

Tracks Activity Over

a Period of Time

Custom Use Case Framework

How do I know if my use case can be applied to the custom use case framework?

Out of Box

Data does not correspond to Splunk UBA categories

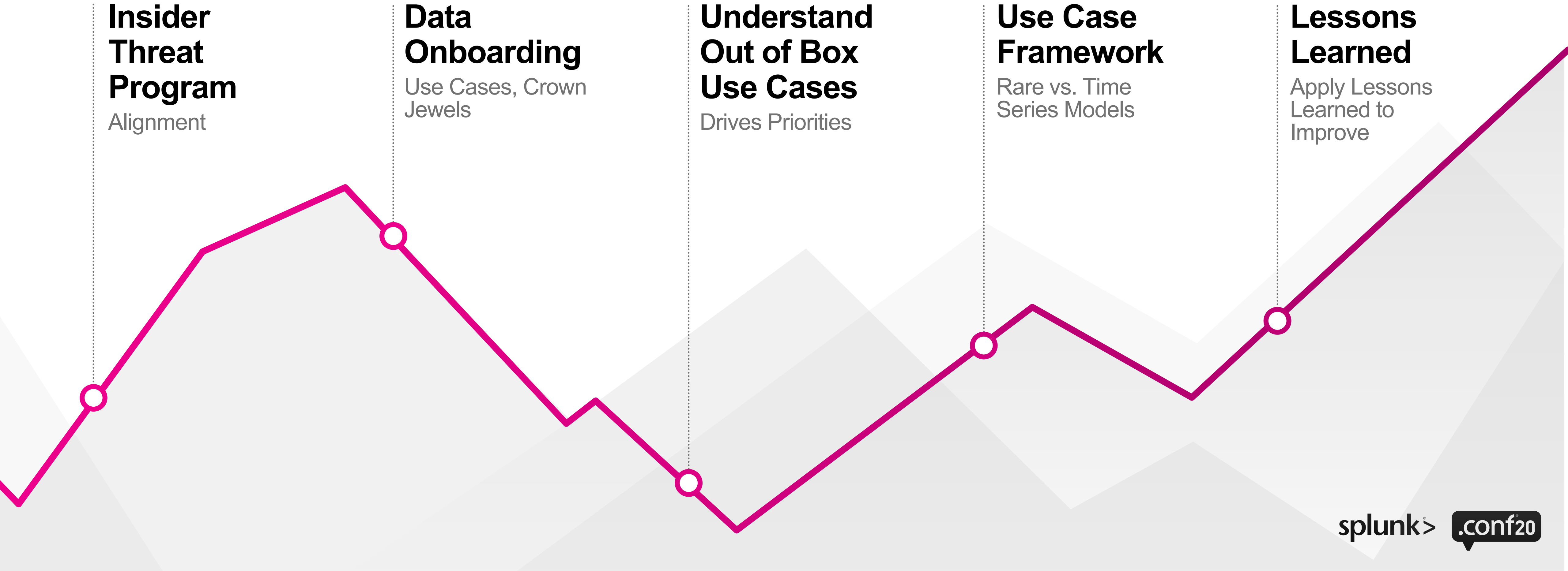
Models

Use case fits into rare events or time series model

Data Cubes

Customize dimensions or measures

Key Takeaways



Insider Threat Program
Alignment

Data Onboarding
Use Cases, Crown Jewels

Understand Out of Box Use Cases
Drives Priorities

Use Case Framework
Rare vs. Time Series Models

Lessons Learned
Apply Lessons Learned to Improve

Thank You!

splunk> .conf20