Advanced Threat Hunting

Richard Towle
Enterprise Architect: Security | Splunk

splunk> .conf19

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.

Johnathan Guillotte
Senior Security Engineer | LyondellBasell

Christopher Schuler
Security Masked Superhero | LyondellBasell

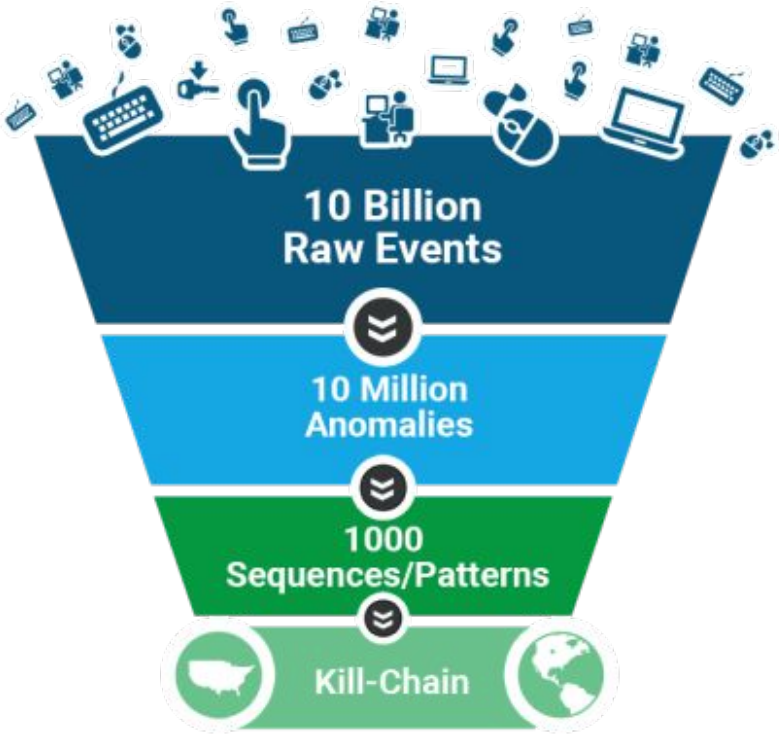
splunk> .conf19

Advanced Threat Hunting with UBA

splunk> .conf19

What is Splunk UBA?

Splunk UBA is an out-of-the-box solution that helps organizations find **unknown threats** and **anomalous behavior** with the use of **machine learning.**



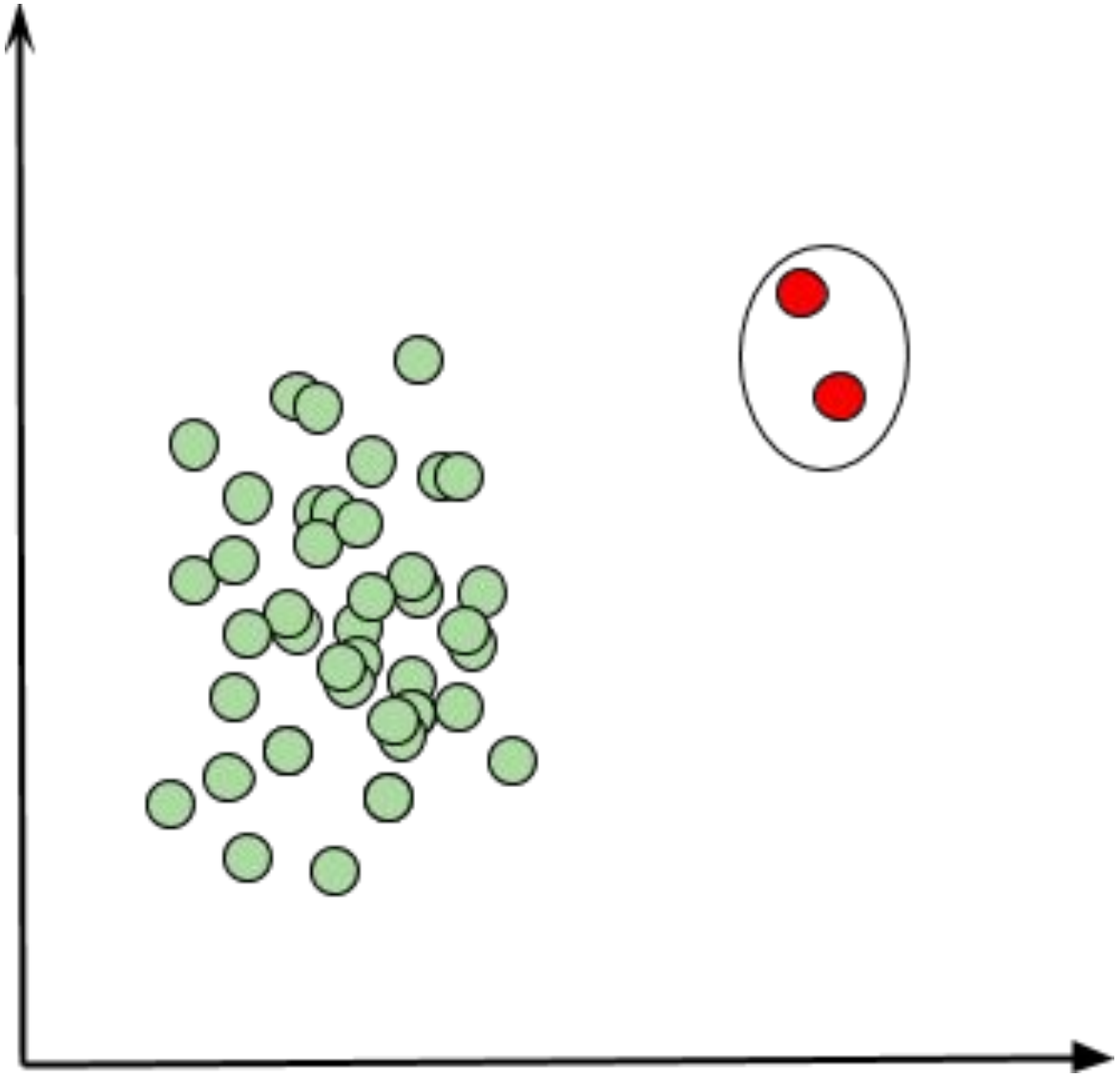
⚠ Top-10

critical and actionable unknown threats

Making machine data accessible, usable, and valuable to everyone.

Anomalies

What are we hunting?



Spotting Anomalies

Unique behavior

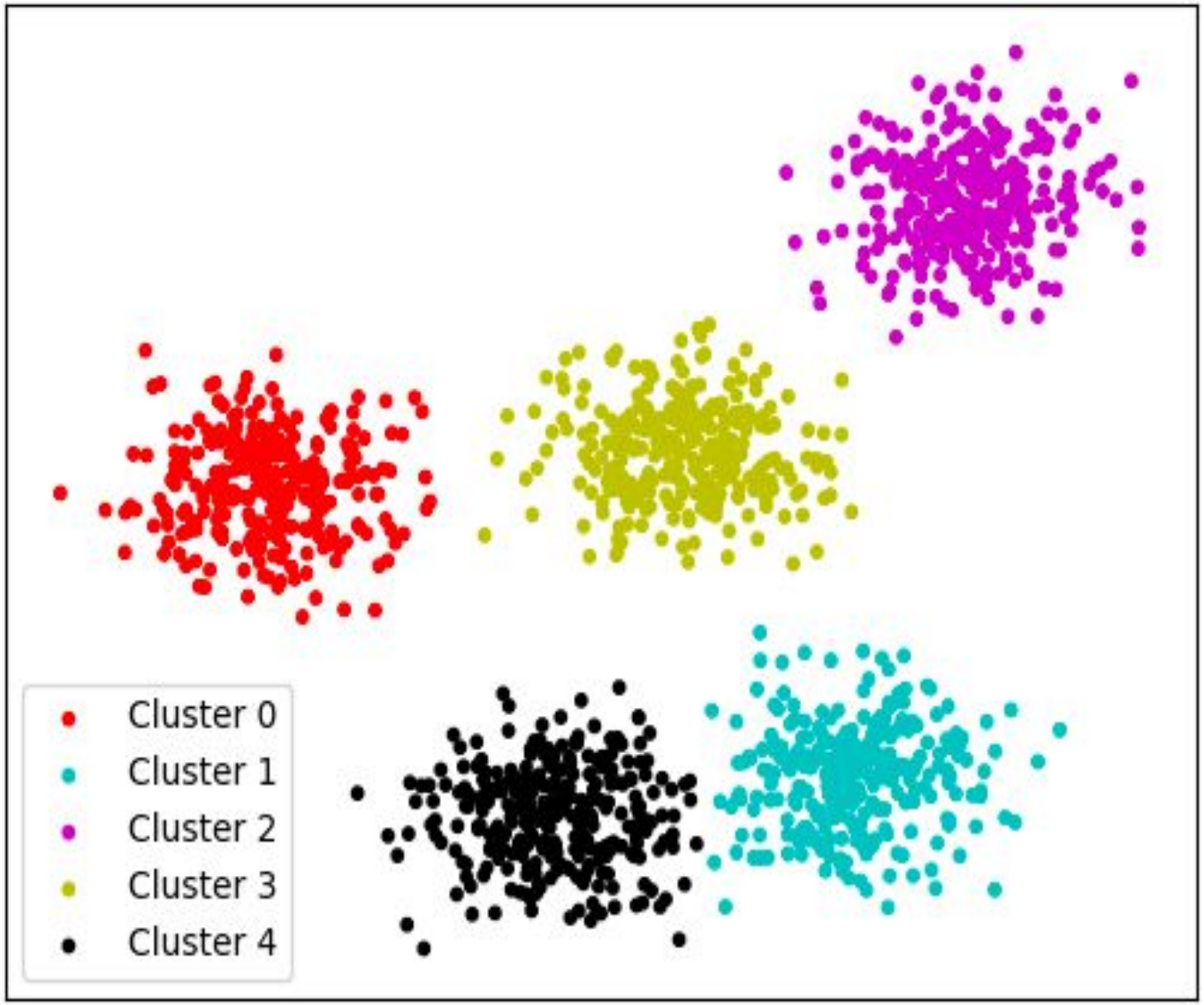
“Access to Crown Jewels”

“Strange Time of Day”

“Exfil of Large file”

Peer Grouping

Behavior grouping



Spotting Deviation From Team

Group behavior

“Peer group never access that Data Store”

“Different location from all peers”

“Different time of day from peers”

What are UBA Customers Detecting?

Account Misuse

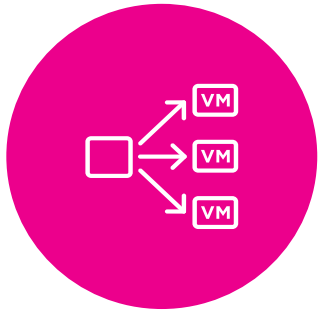
- Privilege Abuse of admin account
- Detection of account sharing
- Detection of Shadow IT Servers
- Privilege operations on self
- Short lived accounts on Box & AD
- Interactive logins by service accounts
- Unauthorized password change attempt
- Critical file access by service accounts
- Unauthorized file access
- Unauthorized application usage

Compromised User Account

- Compromised service accounts that enabled remote access
- Usage of co-worker's machine by user
- Query blank password on admin acct

Compromised/ Infected Machine

- Malware communication where the standard security tools failed to detect (multiple customers)
- Exposed company's sensitive information on public web services
- Compromised mobile phone generating suspicious outbound connection
- Infected machine based on alert correlation & internal detection

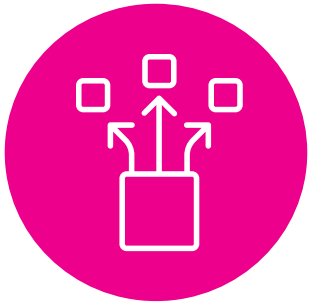


Lateral Movement

- Creation of temporary local accounts across multiple machines
- Unusual process creating sockets across internal machines

splunk> .conf19

What are UBA Customers Detecting?

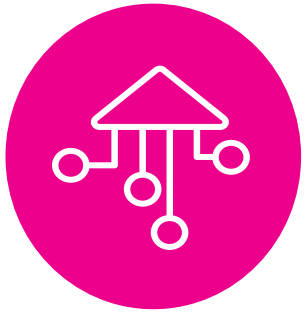


Data Exfiltration

- User forwarding all corporate emails to personal email address
- User copying few years older email archive data from central repository
- High volume of data downloads from box and previews indicating data gathering/snooping
- Users exfiltrating data out of organization - detected by deviations from user's and peer group's profiles

Suspicious Behavior/ Unknown Threat

- Users with web proxy disabled
- Users logging in from unusual/unauthorized geo locations
- Suspicious call home activity
- Users encountering malvertising
- Suspicious account lockout
- Misconfigured services using expired credentials
- Accounts impersonating user logins
- Misconfigured/corrupted VDI profile
- Unauthorized use of P2P software
- Unauthorized corporate resource usage for BitCoin mining
- DNS abuse activity



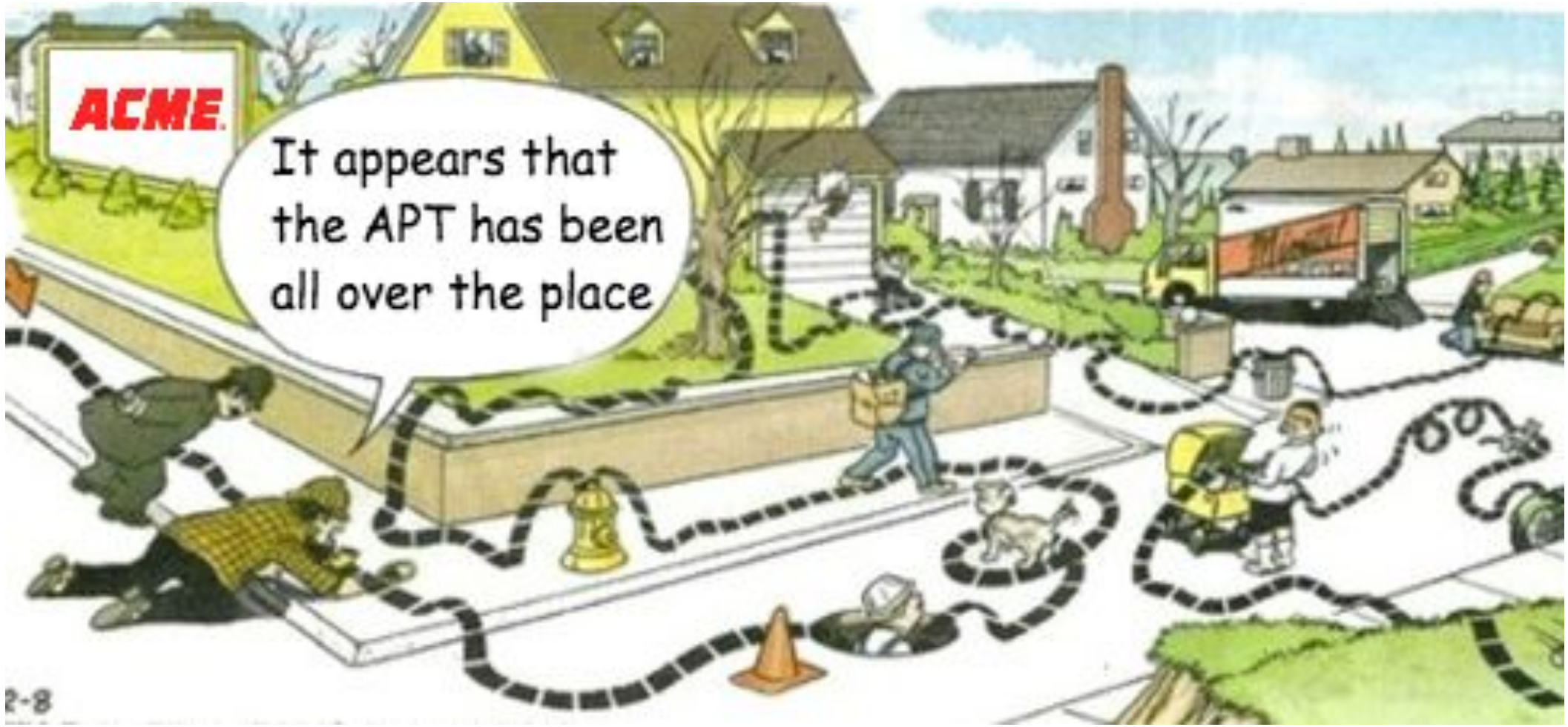
Contextual Intelligence

- Automatic detection of user/account related details
  - Account types - domain administrators, service accounts
  - User risk scoring – internal & external risk
- Automatic detection of device types in environment
  - DCs, exchange servers, email servers, DNS servers, personal laptops, web servers, NTP servers
- Popularity of external domains & IPs

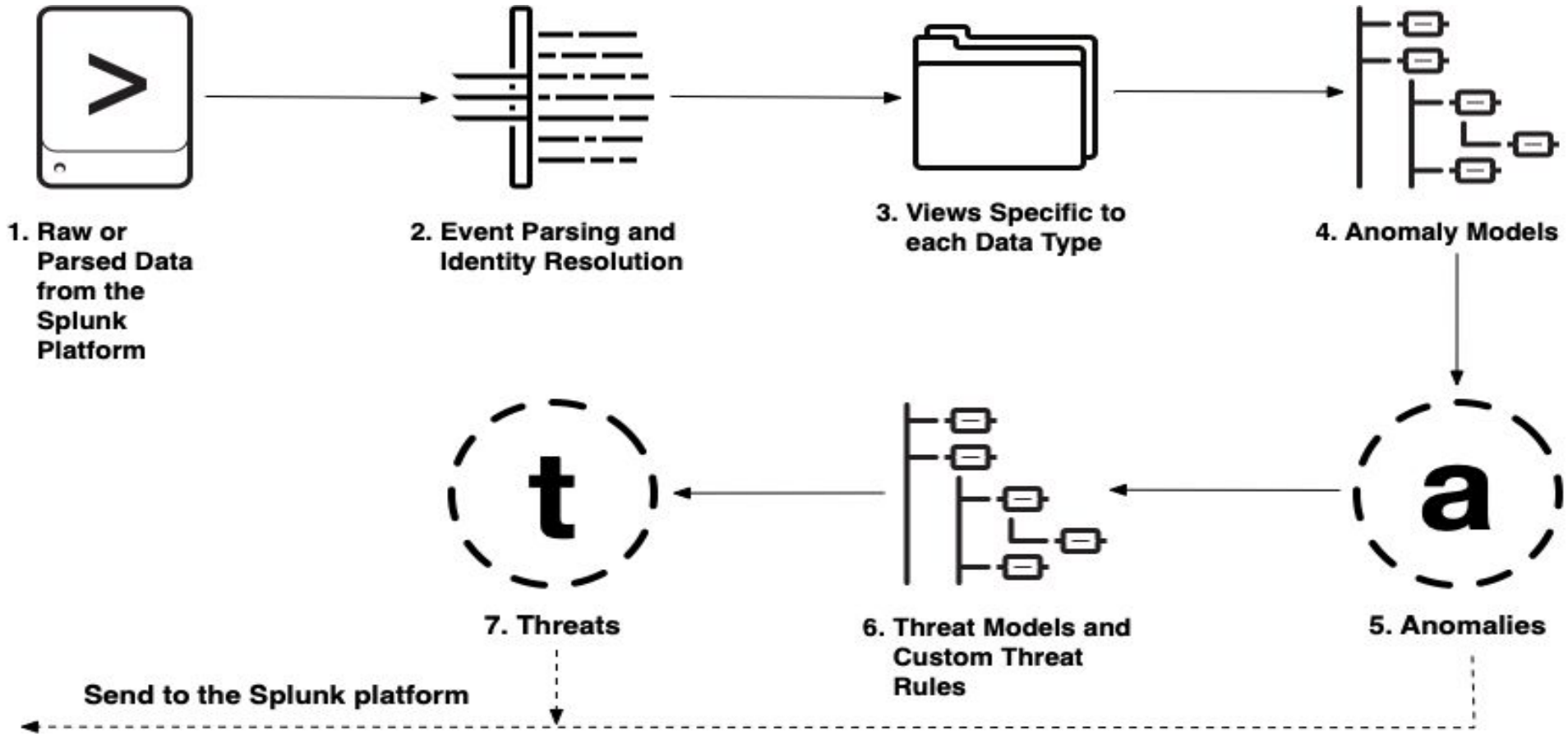
External Attack

- Detection of directory traversal attacks based on malicious strings in Web URL requests to web servers
- RDP traffic from suspicious sources

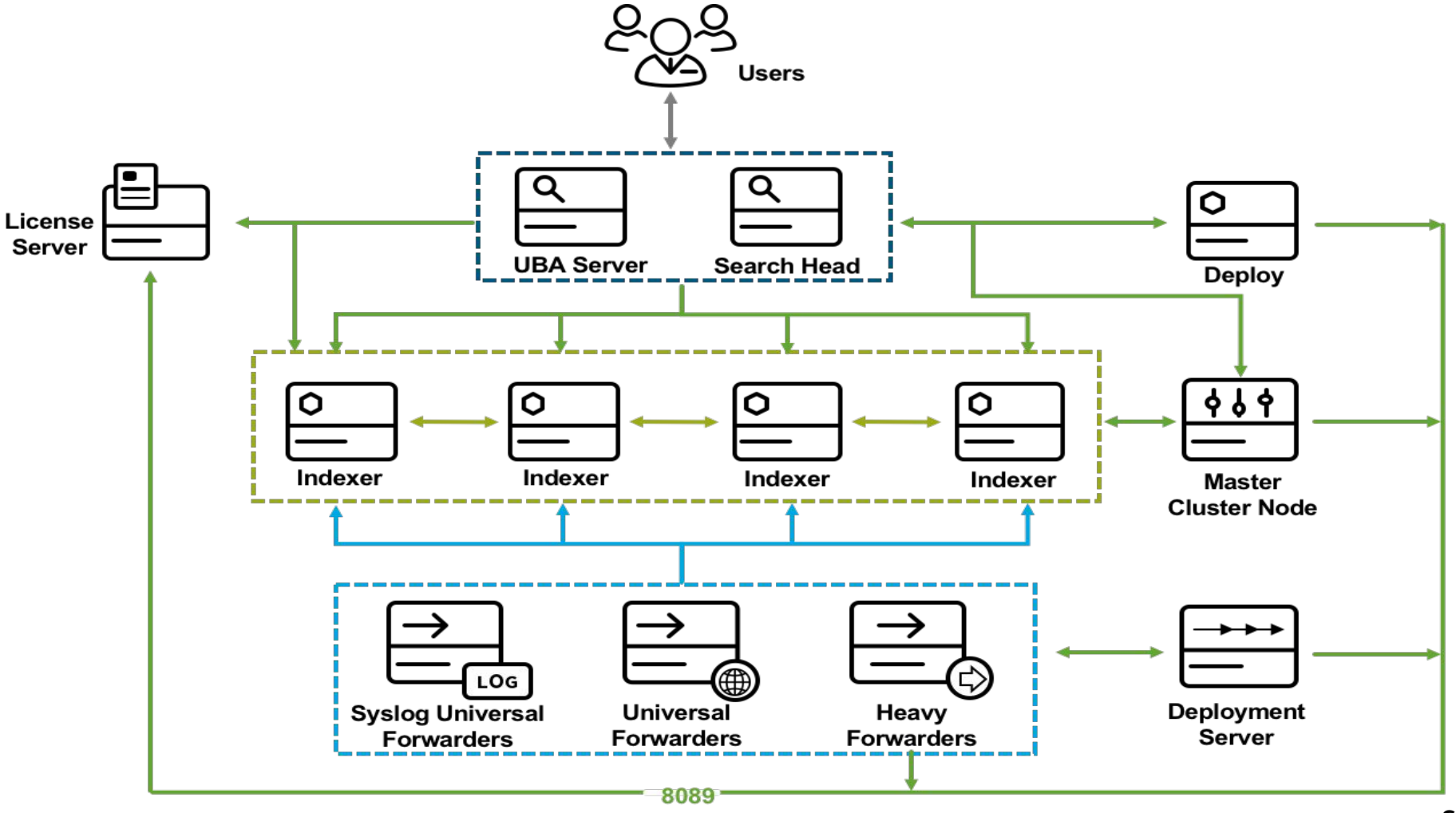
splunk> .conf19



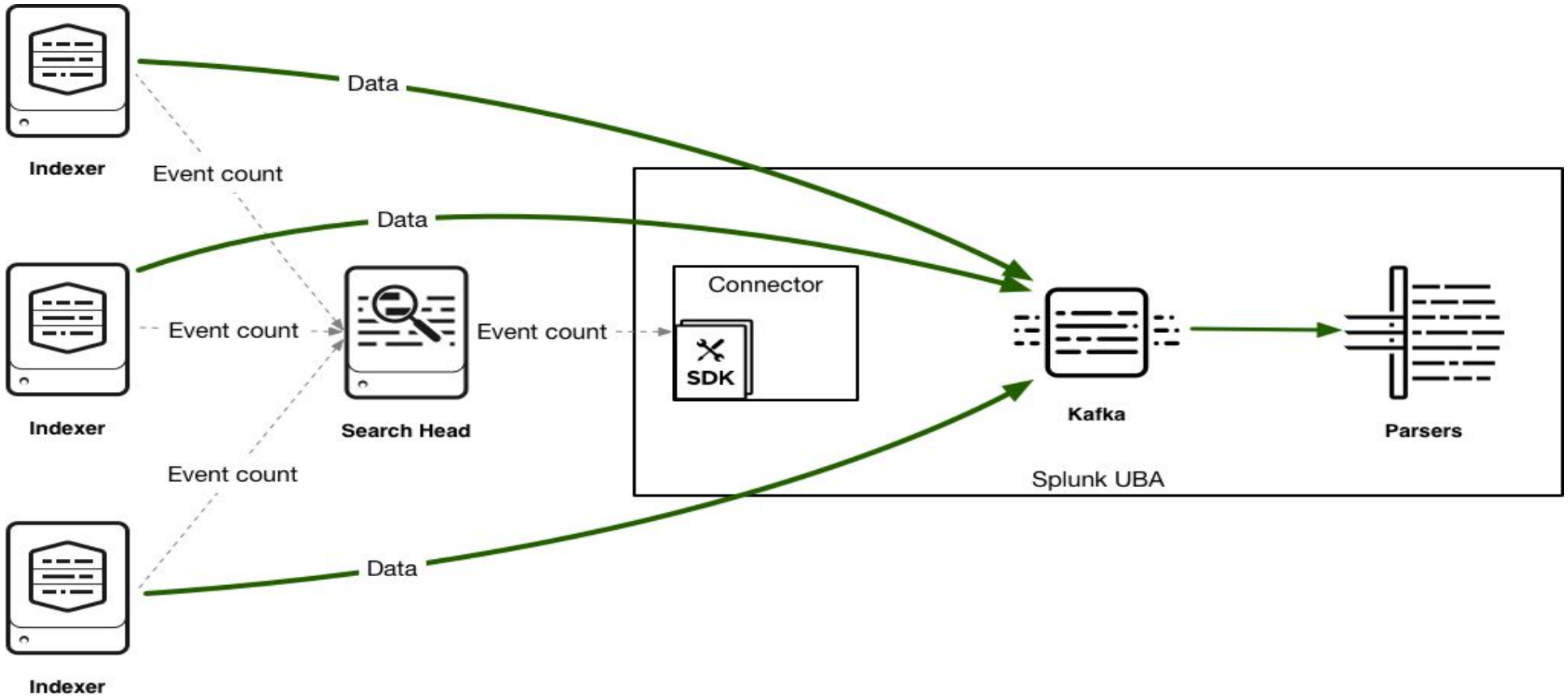
UBA Data Ingestion from Splunk Core-ES



Where Does UBA Fit?



Adding Data Direct From Kafka Direct From Indexer to UBA



Demo

UBA in Security

Machine Learning is cool

1. Accelerate investigation of advanced threats through automated early attack detection

2. Increase SOC efficiency and work smarter by leveraging the power of machine learning to augment SIEM

3. Optimize insider threat detection and uncover unknown threats by combining threat intel from SIEM and UBA

4. A proven, analytics-driven SIEM supercharged with machine learning and behavior analytics

Q&A

Thank You !

Richard Towle
rtowle@splunk.com

Go to the .conf19 mobile app to

RATE THIS SESSION