.conf2015

So What Is This UBA Thing Anyway?

Bob Pratt

Director, UBA Product Management

splunk>

Disclaimer

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 the 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.

ENTERPRISE **CHALLENGES**

THREATS

Cyber Attacks, Insider Threats, Hidden, Or Unknown

PEOPLE

Availability of Security Expertise

EFFICIENCY

Too Many Alerts And False Positives

Majority of the
Threat Detection Solutions
focus on the **KNOWNS**.

What about the

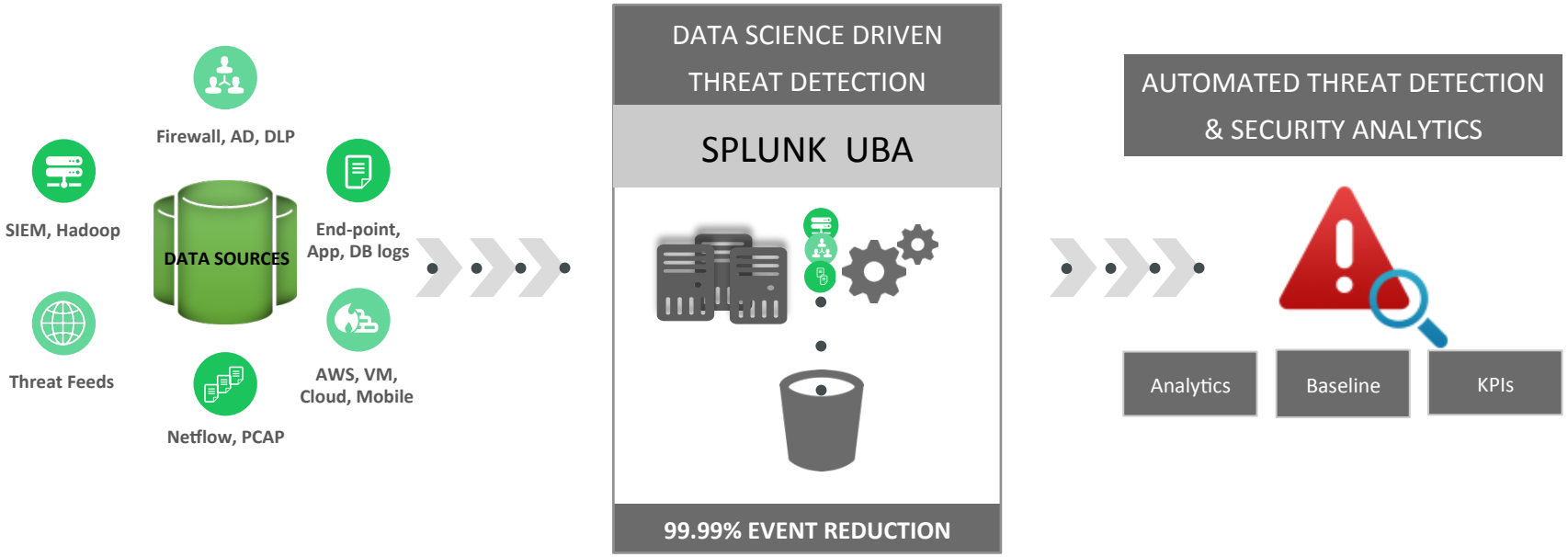
UNKNOWNS?

SPLUNK UBA detects

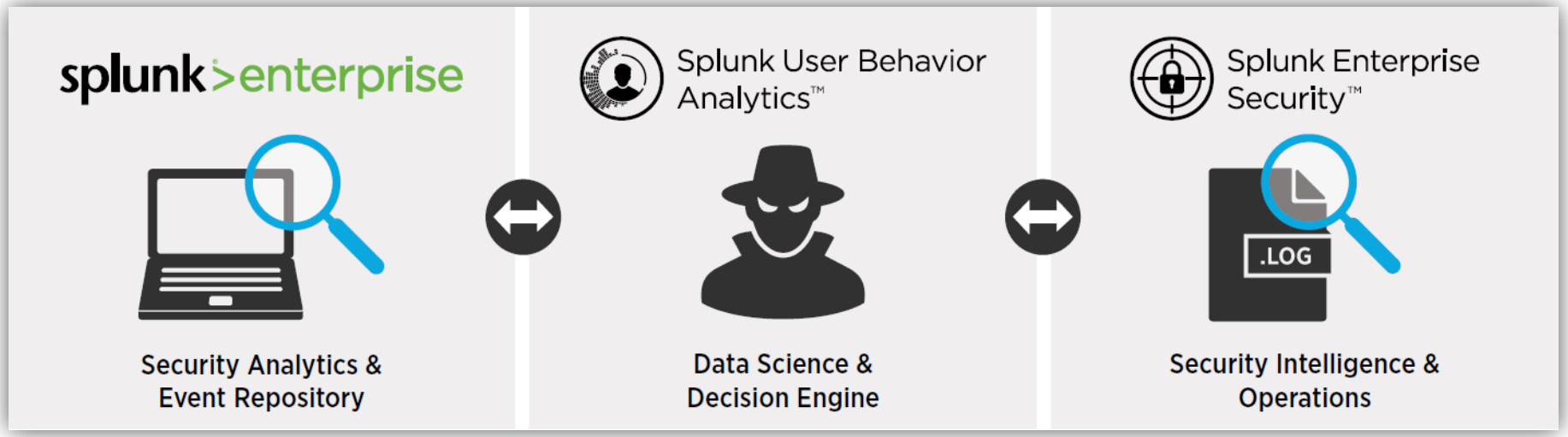
ADVANCED CYBER ATTACKS & INSIDER THREATS

with BEHAVIORAL THREAT DETECTION

WHAT DOES **SPLUNK UBA** DO?



THE OVERALL **SOLUTION**



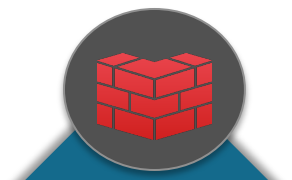
What Data Does UBA Need to Work?

Identity/Auth

- Active Directory/ Domain Controller
- Single Sign-on
- HRMS
- VPN
- DNS, DHCP

Activity (N-S, E-W)

- Web Gateway
- Proxy Server
- Firewall
- Netflow, PCAP
- DLP, File Server/Host Logs



Security Products

- Malware
- End-point
- IDS, IPS, AV

SaaS/Mobile

- AWS CloudTrail
- Box, SF.com, Dropbox, other SaaS apps
- Mobile Devices

External Threat Feeds

- Norse, Threat Stream, FS-ISAC or other blacklists for IPs/domains

OPTIONAL

HUNTER WORKFLOW

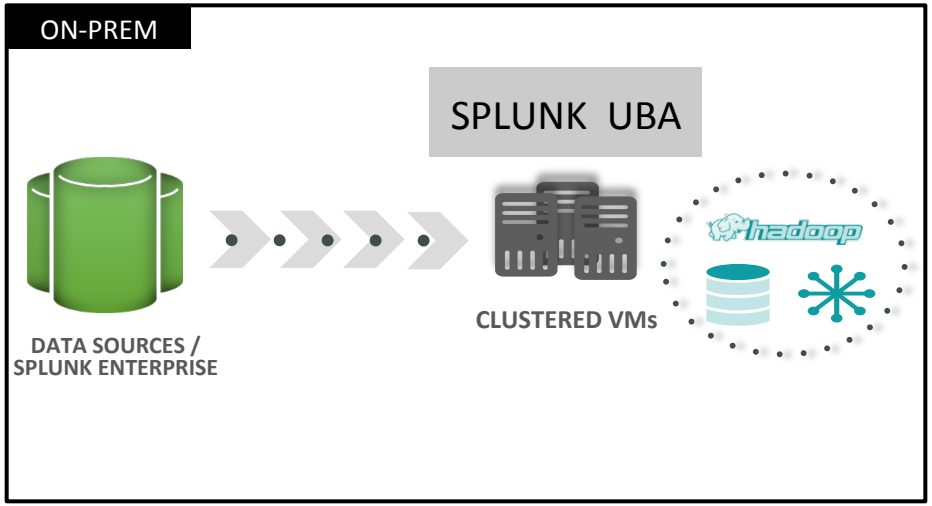
HUNTER

- Investigate suspicious users, devices, and applications
- Dig deeper into identified anomalies and threat indicators
- Look for policy violations

SOC ANALYST WORKFLOW

- Quickly spot threats within your network
- Leverage **Threat Detection** workflow to investigate insider threats and cyber attacks
- Act on forensic details – deactivate accounts, unplug network devices, etc.

DEPLOYMENT MODELS



THANK YOU

splunk>