Splunk User Behavior Analytics (UBA)

Methods and Best Practices to Get Started Now

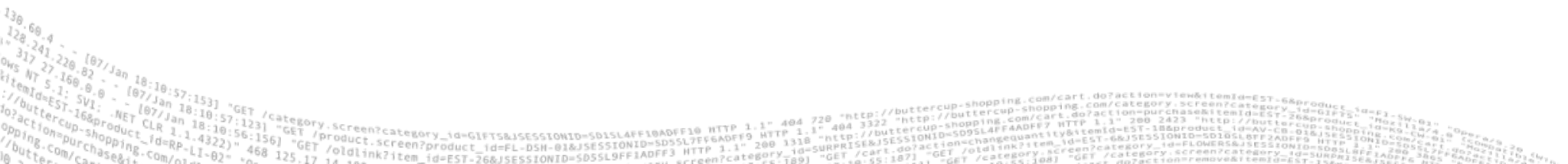
Matt Wilson | Principal Information Security Architect, Asurion
Jeswanth (Jes) Manikonda | Senior Solutions Architect, Splunk
Michael Nobles, CEH | Sr. Sales Engineer, Splunk

Thursday, October 4, 2018 | 12:45 - 1:30 pm ET

Forward-Looking Statements

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 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.



Overall Session Flow

What we will cover...

- Quick Introductions… Matt, Jes, and Michael (5 minutes)
- Set the Stage - Michael (5 minutes)
  - Briefly cover existing Splunk environment
  - Overview of UBA building blocks
- UBA Deployment and Best Practices - Matt and Jes (30 minutes)
  - Preparation & Installation
  - Data Onboarding
  - Workflow Integration

Who We Are

Brief Introductions
Bullet points on Asurion

Matt Wilson

Information Security Principal Architect (Asurion)

- 20 Years in Information Technology
- Splunk Architect
- Splunk Consultant II

- Enjoys fishing and time with family

asurion

Life's Operating System

- Founded in 1994
- Mobile Device Insurance Services
- Based in Nashville, TN
- 317 Million customers in 49 countries

Jeswanth(Jes) Manikonda

Senior Solutions Architect at Splunk

- Based out of San Jose, CA
- Member of the Splunk family for 3 years
- Been part of Splunk UBA since its acquisition and elemental in product and business growth. Worked with UBA solutions for 6+ years/250+ customers

- I am all ears about innovative technologies

Michael Nobles

Sr. Sales Engineer at Splunk

- Based out of Atlanta, GA
- Member of the Splunk family for 3 years
- Fun = 20+ years of Sales Engineering activities

- Enjoys running camera at church and during the Passion Conference every January

Set the Stage

Existing Splunk Environment
Overview of UBA Building Blocks

Existing Splunk

Lay of the Land Before UBA

- 4 TB Splunk Enterprise License
- 4 TB Enterprise Security License
- New Hardware as of late 2017
- Critical Sources
  - Firewall
  - VPN
  - DNS
  - DHCP
  - WinEventSecurity
  - AV / IPS / IDS
  - ...

- Virtualized Environment
- Bare Metal is Cisco UCS
- Indexer Cluster Specs
  - 16 node and 2x6 node
  - 16 core, 24 GB RAM
  - 12,000 IOPS (SSD)
- Search Head Specs
  - 24 core, 96 GB RAM
  - Teams create additional SH as needed

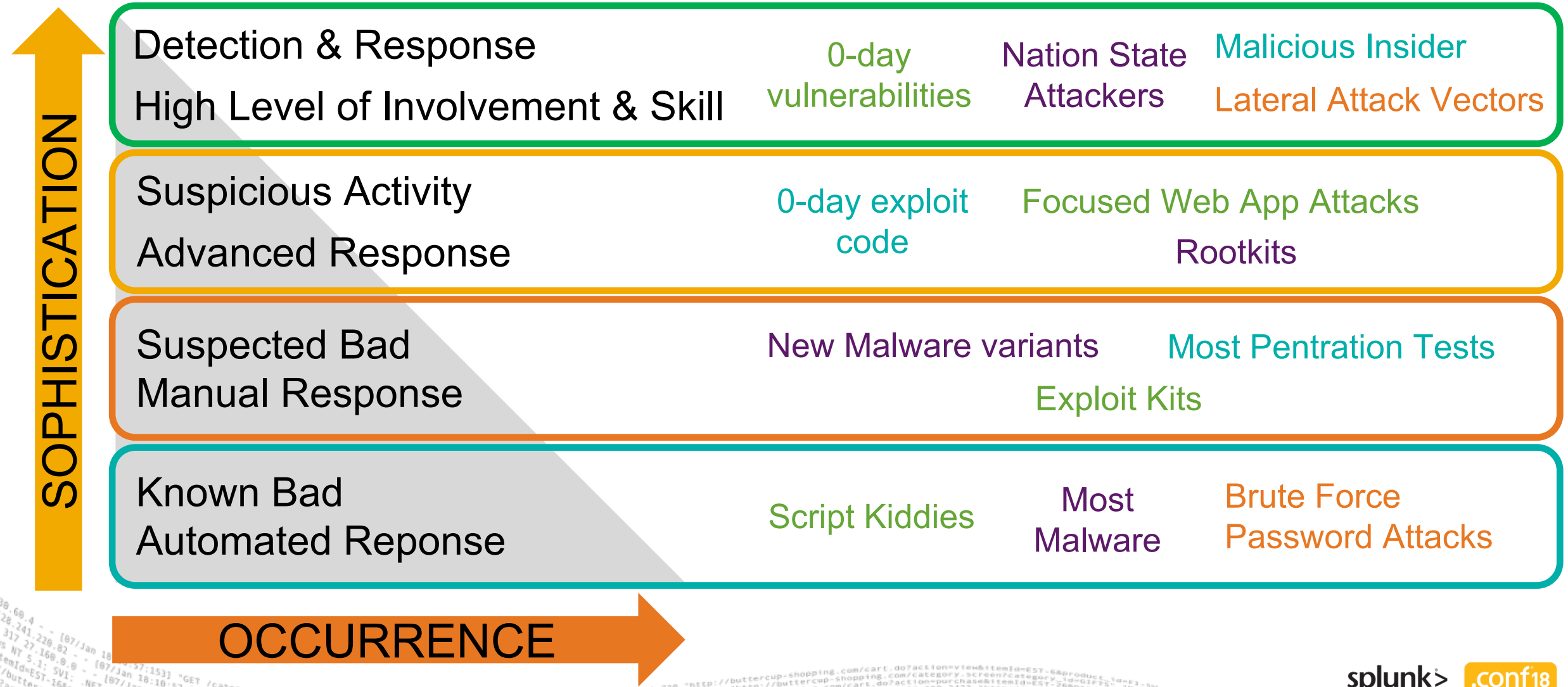
12 Splunk Search Heads

40 Splunk Indexers

1,000s of Splunk Forwarders

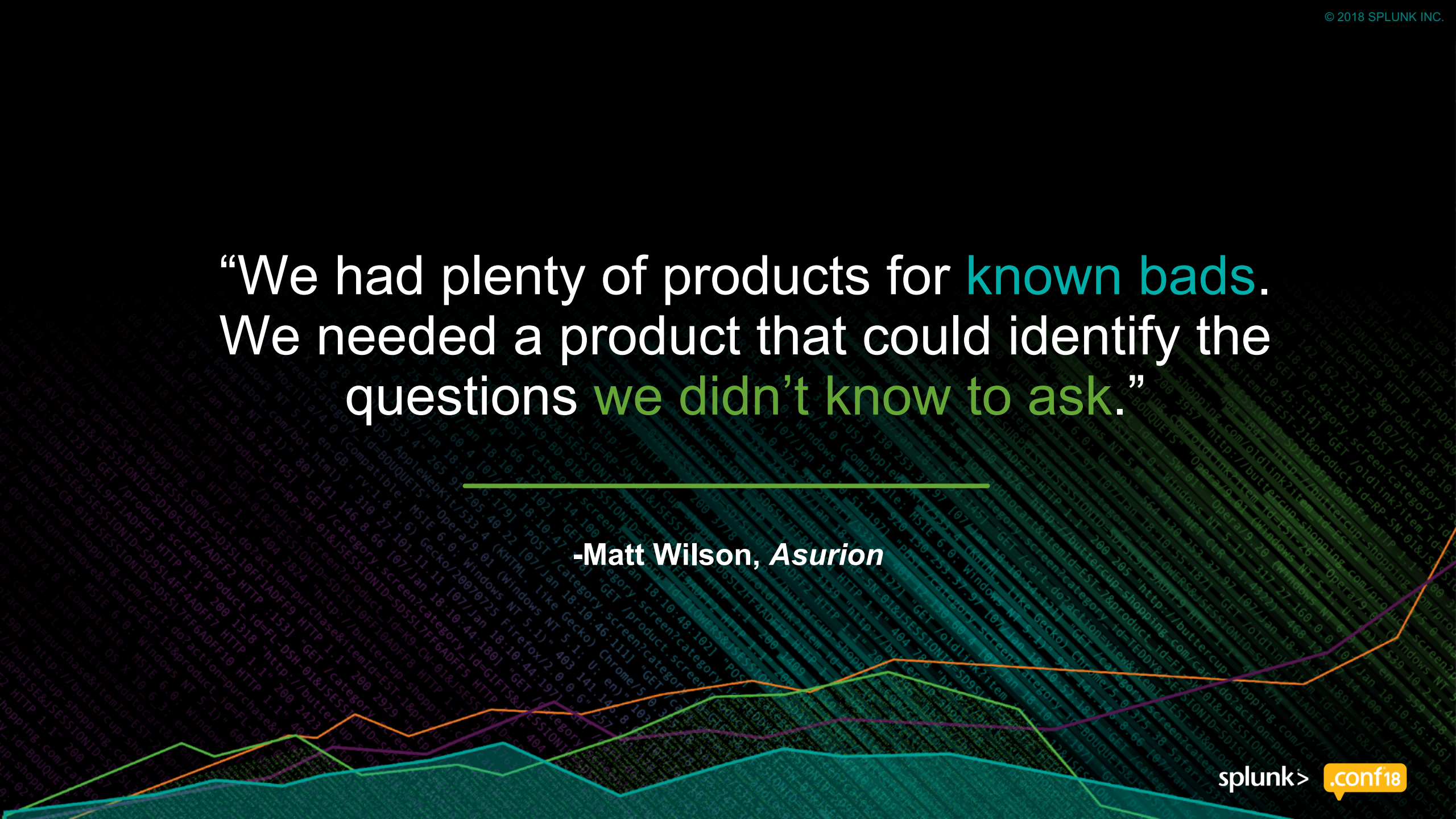
Evolution of Security Controls

The triangle slide



"We had plenty of products for known bads. We needed a product that could identify the questions we didn't know to ask."

-Matt Wilson, *Asurion*



splunk> .conf18

High-level View of UBA Building Blocks

Foundational Concepts for those Just Getting Started

Packaged & Expandable Big-Data Architecture

Identity Correlation

Multi Entity Behavior Profiling

Building Intelligent Security Context

Sophisticated Security Modelling

Known & Unknown Threat Detection

Customize & Build

Machine Learning Driven

Splunk User Behavior Analytics™

splunk> .conf18

Overview for Getting Started Now

Key elements to plug UBA into your environment

- Preparation & Installation
  - Datasource identification & validation
  - Sizing
  - Environment preparation
- Data Onboarding
  - Contextual data
  - Event data
- Workflow Integration
  - Analyst/Hunter Feedback
  - Investigation approach

Disclaimer: The presentation will cover only the best recommended practices and will not cover all the available options

Preparation & Installation

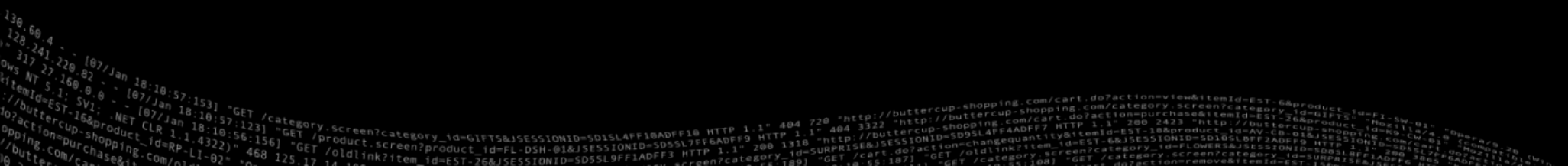
Best Practices to install UBA

splunk> .conf18

Datasource Identification

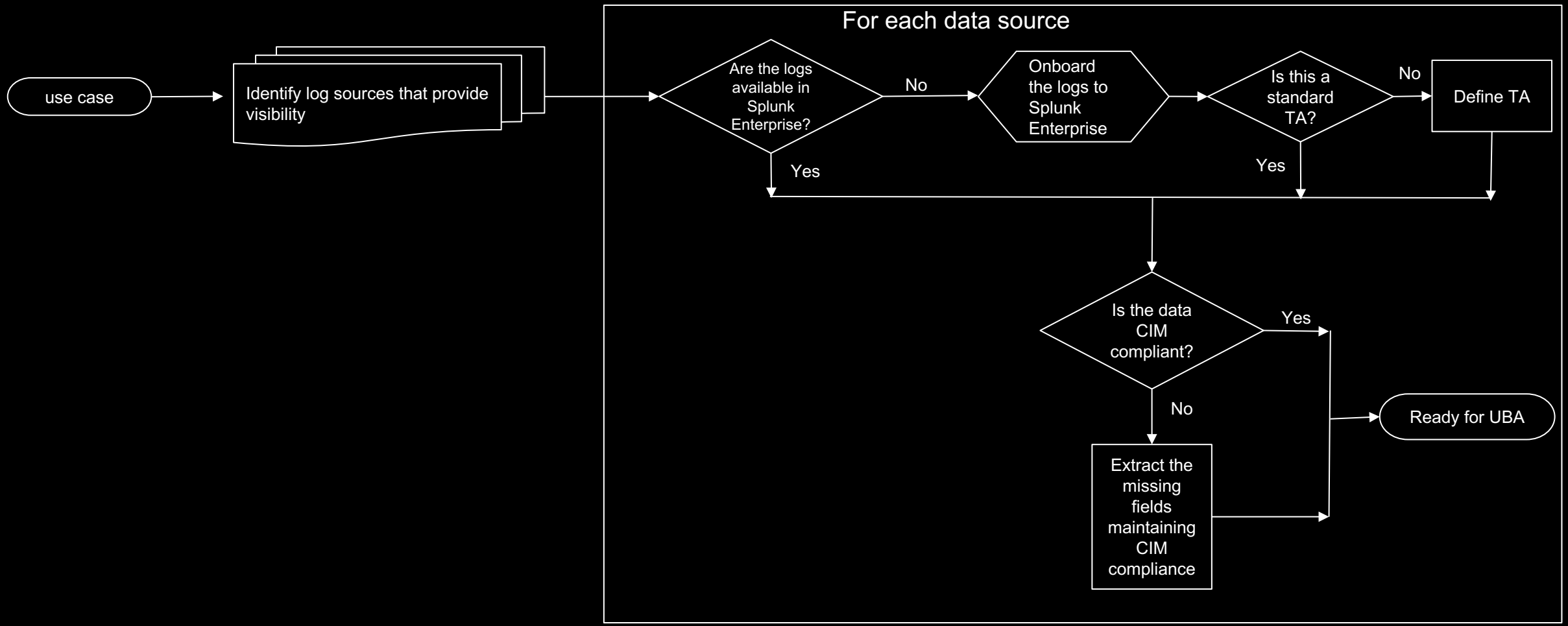
Use-case driven approach

- Event data
  - Always start with specific use cases that you would like to solve with UBA
  - Involve Security Architects/Infosec Engineers/SOC team for inputs
  - Use cases:
    - Data Exfiltration
    - Lateral Movement
    - Account Compromise/Misuse
    - Compromised/Infected Machine
    - Suspicious/Unknown threats
  - Identify the data sources that would provide indicators to detect the use case and verify if they are CIM compliant
  - For example: Data Exfiltration -> Firewall, Web gateway/proxy, Email, Printer, USB etc.



Data Identification & Validation

Use case driven approach



Sizing

Sizing & deployment

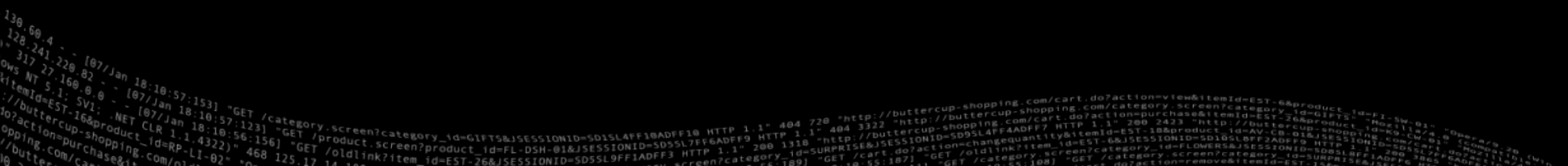
- Sizing
  - Scope for near future growth (minimum 2 - 3 years)
    - User population, additional logging/sources
  - Factor in EPS (perc90) + user population + device count (workstations, servers, any other devices on network)

- Hardware
  - Specs - Use the recommended specs to avoid additional configuration
  - Deployment - OVA/AMI preferred
  - OS - Use supported OS version. If requirements do not comply, work with Splunk before the installation

Environment Preparation

Preparing for UBA installation

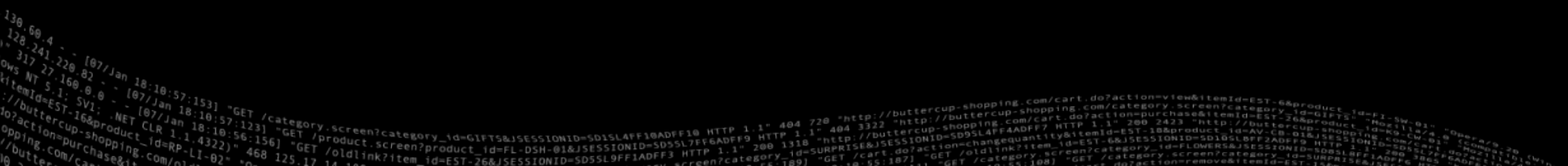
- Network
  - Get static IP(s) & register on DNS
  - Ensure firewall policies/restrictions between UBA nodes and to search-head(s)
- Splunk Enterprise/ES preparation
  - Set up a UBA service account and assign appropriate privileges on the search-heads
  - Install sa-ldapsearch add-on and create a service account to login to Active Directory from sa-ldapsearch (on-prem customers only) and test the connectivity
  - Enable SA-UEBA and go through the UBA setup process (may require restart)
  - Identify the list of sources that do not have non-CIM compliant TA's and fix them
  - If switching to Kafka based ingestion, install Splunk UBA Kafka ingestion app



Environment Preparation

Preparing for UBA installation

- UBA Internal
  - System Access - If you have tight policies,verify sudoers and ensure it complies to your requirements
- Other information
  - Gather internal & publicly owned IP ranges across all your office locations
  - Identify SMTP server configuration for admin & analyst alerts



Data Onboarding

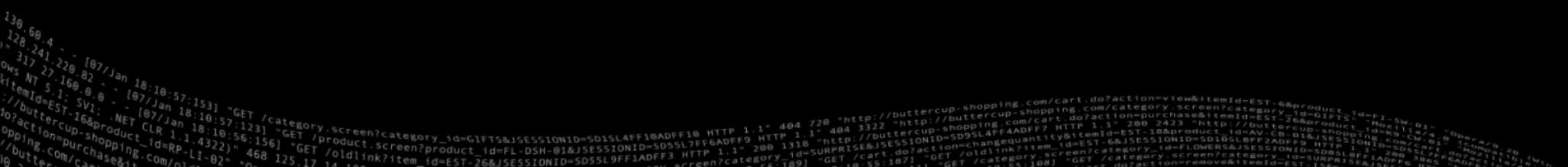
Getting data in

splunk> .conf18

Contextual Data

HR & assets data

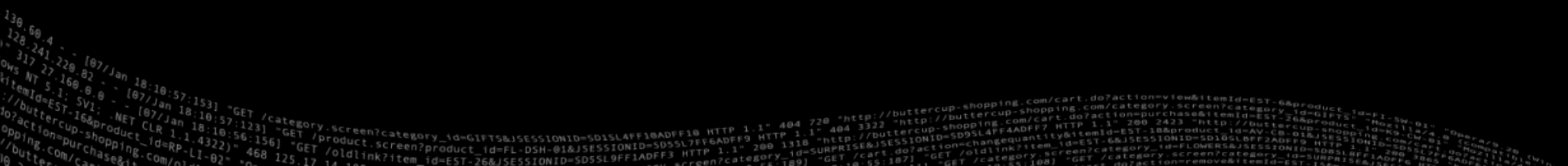
- HR data
  - Why: Account Metadata Enrichment + Account Correlation + User Metadata Enrichment
  - Source: HR application/Active Directory
  - Field identification: Information that would assist in investigation
  - Data flow: Raw data -> lookup (report) -> UBA
  - Ingest -> Validate -> Reiterate till it is correct
- Assets data
  - Why: Device Metadata Enrichment
  - Source: CMDB/ES Assets/Active Directory
  - Data flow: Raw data -> lookup (report) -> UBA



Event & Alert Data

Data sources that support use cases

- Data onboarding & validation
  - Test mode -> Validate -> Turn live
  - Types of logs
    - DHCP + DNS + WinEventLog:Security (DCs + workstations; powershell logging)
    - Network (internal-to-internal + internal-to-external; Netflow/NGFW/packet information)
    - HTTP traffic
    - Email/USB/Print/Cloud repositories
    - External Alerts (DLP/EPO/IDS/Malware/Phishing/SIEM)



Workflow Integration

UBA Post-Installation Best Practices

splunk> .conf18

Environmental Feedback

Hunter workflow

- Scoring
  - Provide input on key assets or key users/departments to increase the risk score.
    - ex: a user in ‘Research Lab’ may carry more risk with data exfiltration than other departments
  - UBA points out misconfigurations. If not correctable in near future, reduce the risk to avoid white noise.
    - ex: service accounts are used for interactive logins
  - UBA exposes the scoring logic. If a specific scoring logic is not applicable to your environment, adjust it upfront.
    - ex: For excessive data exfiltration, UBA increases the score if it deviates from peer group profile. If peer group deviation is not applicable, adjust it accordingly.
- Suppression
  - Whitelist activity that may be behaviorally suspicious but may not be a concern
    - ex: desktop support team logging onto unusual machines
  - Whitelist known external entities for specific behavior
    - ex: data transmission to an external organization(CIDR) that one of your teams is working with

Approach to Investigation

Analyst workflow

- Adjust your investigative lens
  - Alerts are not generic across the environment. They are per entity.
  - Anomalies tend to be noisy. Focus on threats.
    - ex: a user logging in over the weekend
  - Verify anomaly relations and identify the common entity(ies) if multiple entities were involved to start your investigation
- Avoid bias
  - Mask PII data
    - authorized-to-do vs why

Key Takeaways

To get best out of UBA

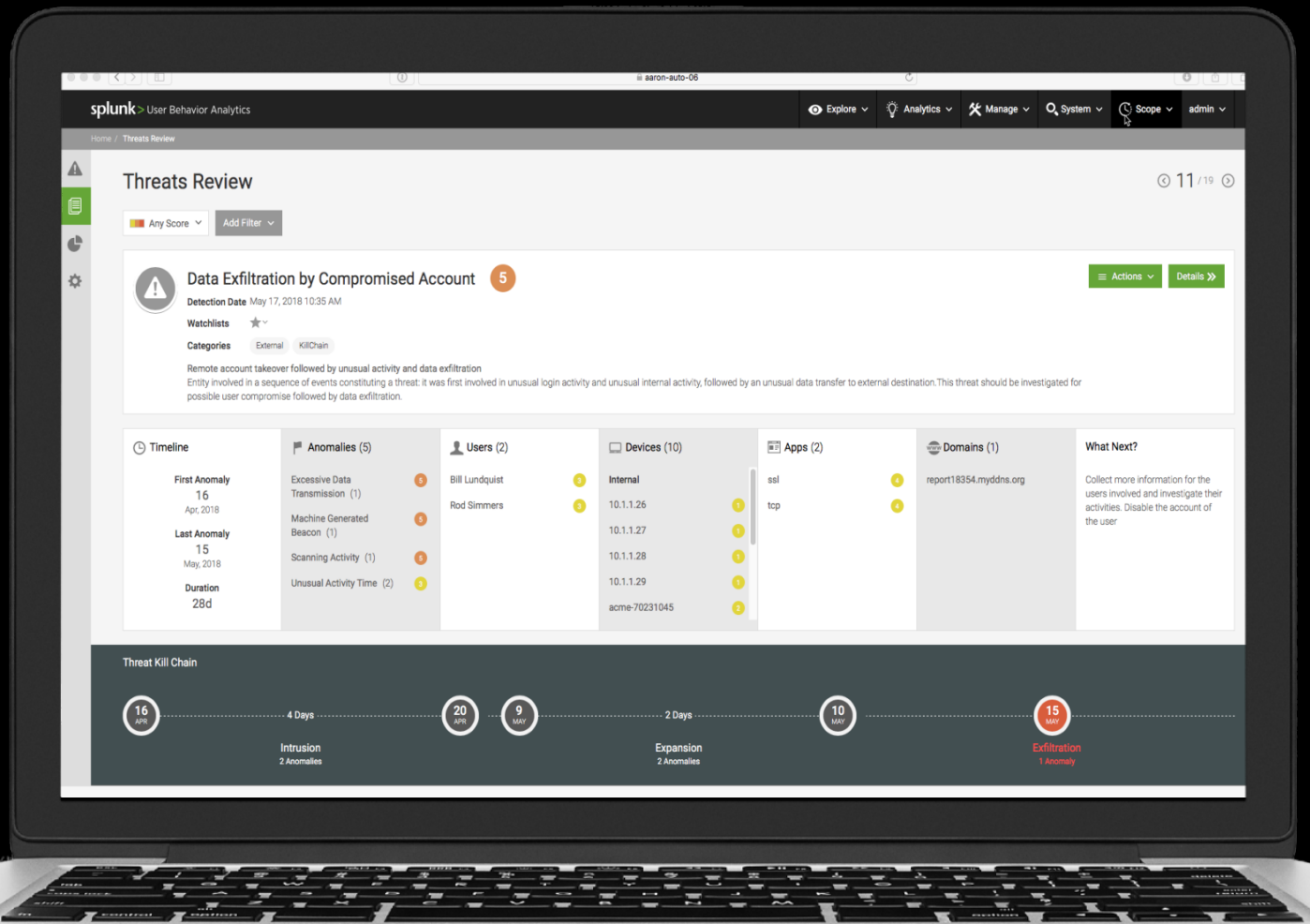
Feed in appropriate and accurate data

Provide feedback

Wear hunter lens - Lookout for possibilities

Get started with Splunk UBA today

- Free cloud-based sandbox trial*
- Available as an add-on to Splunk ES starting at 500 GB/day



* Contact your Splunk sales representative

Appreciate Your Time Today

Matt Wilson | Asurion (Matt.Wilson@Asurion.com)
Jeswanth Manikonda | Splunk (jmanikonda@splunk.com)
Michael Nobles | Splunk (coolness@splunk.com)

splunk> .conf18

Thank You

Don't forget to rate this session in the .conf18 mobile app