Welcome
Data Wars: A New Hope for IT & Security Insights

Jade Catalano | Senior Product Marketing, Security
Robert Christian | Senior Sales Engineer
Sept. 25-28, 2017 | Washington, DC
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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
How we see ourselves

Security Operations

IT Operations

© 2017 SPLUNK INC.
How we see each other

Security Operations

IT Operations
Objectives

1. How to use Splunk for security investigations & IT troubleshooting
2. How to leverage the same data for different use cases
3. How to share IT & security insights with Splunk as a single pane of glass
Data Sources

- Networks
- Web Services/Global
- Security/Lock
- Telecoms
- Web Clickstreams
- Online Services
- Storage
- On-Premise
- Public Cloud
- Private Cloud
- Internet of Things
- Active Directory
- IT Infrastructure
- Databases
- GPS Location
- RFID
- Cell Phones and Devices
- Call Detail Records
- Servers
- Networks Alt
- Networks
- Advanced Search
- Analyze
- Attacker Insider
- Attacker Nation/State
- Log Files
- Security Server
- Custom Applications
- Attacker General
- Malware
- Server
- Virtual Server
- Firewall
- OS
- VM
- APP OS
- Applications
- Energy Meters
- DHCP/DNS
- Desktop
- Laptop
- Online Shopping Cart
- Energy Meters
- Log Files
- Security Server
- Custom Applications
- Attacker General
- Malware
- Server
- Virtual Server
Security
Using Splunk to look at Firewall Data

Palo Alto Networks App for Splunk

- Demo
  - Traffic Data
    - Host
    - External
    - Internal
Using Splunk to Monitor Windows Infrastructure

Splunk App for Windows Infrastructure

- Demo
  - Updates
  - Perfmon
  - Service availability
Joining Forces
Data Types Light Up Use Cases

IT Operations
- Operating System Metric, Status and Diagnostic Commands
- Configuration Files
- Syslog

Security, Compliance and Fraud
- Packet/Flow Data
- Web Access Logs
- Wire Data

IT Ops Analyst

SOC Manager
Data Types Light Up Use Cases

IT Operations
- Filesysterm Audit Logs
- Configuration Files
- Operating System Metric, Status and Diagnostic Commands

Security, Compliance and Fraud
- Syslog
- Packet/Flow Data
- Wire Data
- Web Access Logs

Application Delivery
- Application Logs
- Call Detail Records

Business Analytics
- SCADA Data
- Sensor Data

Internet of Things

IT Ops Analyst
SOC Manager
Site Reliability Engineer
Ecommerce Business Analyst
Manufacturing Engineer
End-to-End Visibility
Thank you!