Cisco and Splunk

Innovation through the Power of Innovation

Douglas Hurd | Cisco Security Technical Alliances PM
Colin Lowenberg | Cisco Meraki Platform Partnerships PM
Karthik Karupasamy | Cisco UCS Technical Marketing Engineer
Robert Novak | Cisco Big Data Technical Solutions Architect

September 28, 2017 | Washington, DC
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.
Eight Years of Integration and Innovation

A brief history of Cisco and Splunk together

With Robert Novak
Why Does Hardware Still Matter?

- Splunk will run on almost anything (even my laptop)
- Standalone servers have lower admin overhead
- Build up your clusters and you have to keep them consistent
- Grow your data sources (and uses) and you have to add servers
- Cluster constipation is bad, mmmkay?
Cisco customer big data pools tend to grow 2-3x/year

Cisco customer IT staff doesn’t grow as fast

The Cisco Unified Computing System (UCS) provides scalable, repeatable, predictable, and manageable deployments across dozens to thousands of servers for any application deployment

Pallet to production in hours, not days or weeks

Deep engineering integration between Cisco and Splunk with tested and proven configurations

More on this later…
Big Data at a Big Customer: Cisco

- 10s of thousands of employees, contractors, devices
- 100s of offices, business apps, audiences
- Lots of data in lots of places
- No one tool (not even Splunk) can do everything for everyone all the time
- High volume, low value, low shelf life
  - Stealthwatch (formerly Lancope), Hadoop feed into Splunk
- Low to moderate volume, high value, (any) shelf life
  - Splunk on its own, sometimes with fronting dashboards
- Additional visualizations with Platfora, Tableau, etc
A closer look at Splunk within Cisco

- Customer for 8+ years, strategic partner for 4+ years
- Geographically disparate data collection and analysis
- Over 70 business applications/use cases across the company
  - Around 20 teams using Splunk including Cisco IT and CSIRT
- Nearly 10x growth in search volume from 2014-2016
Dozens Of Apps And Add-ons At Splunkbase

Always more being added and updated, by Cisco, Splunk, partners, third party developers, and end users!
Splunk and Cisco API-based Integrations
Programmable Operational Analytics at Scale

<table>
<thead>
<tr>
<th>Security</th>
<th>Infrastructure</th>
<th>Collaboration Business Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Services (ISE/pxGrid)</td>
<td>Cisco UCS</td>
<td>Call Manager</td>
</tr>
<tr>
<td>FirePOWER Next Gen Firewall</td>
<td>ACI / APIC</td>
<td>Spark</td>
</tr>
<tr>
<td>Umbrella (DNS)</td>
<td>Nexus 9k</td>
<td></td>
</tr>
<tr>
<td>CloudLock</td>
<td>Meraki Wireless / CMX</td>
<td></td>
</tr>
<tr>
<td>ThreatGrid*</td>
<td>Tetration</td>
<td></td>
</tr>
</tbody>
</table>

and many more here [https://splunkbase.splunk.com/apps/#/search/Cisco/](https://splunkbase.splunk.com/apps/#/search/Cisco/)
Cisco Security Integrations

Making sense of a broad security platform using Cisco and Splunk technologies

With Douglas Hurd

Security Breadth, Customer Reach, Infrastructure for Automation

- Largest security footprint in the industry
- Produces broad range of security telemetry across most security technologies
- Ubiquitous network footprint enables bi-directional integration for executing security automation
- High investment in Splunk apps for serving joint customers

Analytics Efficacy, Ability to Automate, Committed Customers

- Voluminous, context-rich Cisco data sources drive license volumes while enabling improved security & compliance, more effective SIEM use cases and new use cases beyond security
- Automated actions in Cisco network environs
- Proven, supported integrations accelerate time to value
Cisco Splunk Integrations

**Security**
- IPS
- Identity Services Engine/pxGrid
- FireSIGHT (including AMP)
- ASA/PX/FWSM Firewalls
- Web Security Appliance (WSA)
- Email Security Appliance (ESA)
- Stealthwatch
- Umbrella Investigate
- Cloud Web Security (CWS)
- AnyConnect
- CloudLock
- ThreatGrid

**Data Center / ACI**
- Cisco UCS
- UCS Director Express for Big Data
- Application Centric Infrastructure (ACI - APIC)
- Nexus 9K
- Tetration (planned)

**Enterprise Networking**
- Nexus and Catalyst Switches
- Nexus 1000V
- NGN Routers (CRS, ASR, ISR)
- Meraki Wireless
- Open SDN Network Controller
- OMX Wireless
- Network Data Platform (planned)

**Collaboration**
- Call Manager
- Spark
- AppDynamics

✅ Inaugural SIEM & Threat Defense Partner
✅ Inaugural pxGrid partner
✅ Inaugural member of Cisco Security Tech Alliances program
✅ Inaugural ACI Partner
✅ Inaugural Data Analytics Partner

**Cisco Splunk Integrations**

- **CVD**: Cisco UCS Integrated Infrastructure for Splunk Enterprise (Distributed Deployment, High Capacity) ([link])
- **CVD**: Cisco Application Centric Infrastructure with Splunk ([link])
- Splunk on UCS Reference Architecture ([link])
- Cisco Cloud Security for VMDC 1.0 Design Guide ([link])
Cisco Firepower & Splunk

Douglas Hurd / Cisco Security Technical Alliances
Threat Defense Security

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Unified Threat Management
Meraki Appliances Wired & Wi-Fi
Meraki Cloud Management
Secure Access & Identity
Identity Services Engine (ISE)
TrustSec, AnyConnect VPN

Next Generation Firewall
FirePOWER Services
FirePOWER Appliances

Next Generation IPS
FirePOWER Services
FirePOWER Appliances

Email Security
Email Security Appliance
Cloud Email Security
Web Security
OpenDNS Umbrella
Cloud Web Security, Web Security
Appliance
CloudLock

Advanced Malware Protection
AMP for Endpoints
AMP for Networks

Sandboxing & Threat Analysis
AMP ThreatGRID Cloud & Appliance
OpenDNS Investigate

Network Anomaly Detection
StealthWatch
Cognitive Threat Analytics

Threat Intelligence

Talos

© 2017 SPLUNK INC.
Threat Defense Security

Summary Dashboard (6.2.0)
Provides a summary of activity on the appliance

Top Attackers

Source IP | Count
--- | ---
192.168.199.132 | 20,722
192.168.199.133 | 7,643
220.231.10.124 | 3,965
186.107.10.124 | 1,723
172.149.41.1 | 1,453
172.91.41.1 | 1,441
12.100.10.50 | 1,263
220.231.10.78 | 1,102
220.231.10.21 | 1,088
192.168.199.254 | 1,020

Top Targets

Destination IP | Count
--- | ---
224.0.0.22 | 26,122
192.168.199.133 | 2,312
10.0.10.124 | 2,164
10.0.10.21 | 1,937
10.0.10.75 | 1,741
10.110.10.12 | 1,723
192.38.41.133 | 1,453
192.89.41.133 | 1,441
10.0.10.122 | 1,266
192.168.199.132 | 1,020

Intrusion Events

Total Events by Application Protocol

Application | Total Events
--- | ---
ICMP | 52,114
SNMP | 23,070
ICMP | 12,248
HTTP | 386
ICMP for IPv6 | 204
FTP | 16
SMTP | 16
IMAP | 12
LDAP | 12
SSH | 10

Impact 1 Events by Application Protocol

Application | Impact 1 Events
--- | ---
SNMP | 2,346
ICMP | 10

Last updated 4 minutes ago
Threat Defense Security

Unified Threat Management
FirePOWER Services
FirePOWER Appliances
Secure Access & Identity
Next Generation Firewall
Next Generation IPS
Email Security
Web Security
Advanced Malware Protection
Sandboxing & Threat Analysis
Network Anomaly Detection
FirePOWER Services
FirePOWER Appliances
AMP for Endpoints
AMP for Networks
Meraki Appliances Wired & Wi-Fi
Meraki Cloud Management
Email Security Appliance
Cloud Email Security
AMP ThreatGRID Cloud & Appliance
OpenDNS Investigate
Identity Services Engine (ISE)
TrustSec, AnyConnect VPN
OpenDNS
Umbrella
Cloud Web Security, Web Security Appliance
CloudLock
StealthWatch
Cognitive Threat Analytics
Threat Intelligence
Background on Firepower and Splunk

- Firepower-Splunk mutual customer base expanding
  - ASA to Firepower Threat Defense – More FMCs
- Add-Ons for Firepower available on Splunkbase
- Cisco’s Firepower TA & App built in 2014, based on v.5.4
  - Over 6000 downloads
  - Not recommended with FMC V6.x
- ‘Community Supported’ model facing challenges
- Focused on new business model for this critical integration
- Resources directed at Firepower 6.x customers
Background on Firepower and Splunk

- Firepower-Splunk mutual customer base expanding
  - ASA to Firepower Threat Defense – More FMCs
- Add-Ons for Firepower available on Splunkbase
- Cisco’s Firepower TA & App built in 2014, based on v.5.4
  - Over 6000 downloads
  - *Not recommended with FMC V6.x*
- ‘Community Supported’ model facing challenges
- Focused on new business model for this critical integration
- Resources directed at Firepower 6.x customers
Data Consumption – Eat In or Delivery?

Expectations and User Roles are Changing
Data Parity

Some customers want all data to be replicated on their SIEM
New Cisco eStreamer ‘eNcore’ for Splunk

- Scalable app with major improvements
- TAC Support option will be offered
  - Free for customers that do not want TAC support
  - Chargeable for customers that want TAC support
- Official GA Release: End of June
- Beta II underway during May thru June 2017
- PID: FP-SPLUNK-SW-K9
- Description: “Cisco eStreamer eNcore for Splunk
  - Software downloads: software.cisco.com

<table>
<thead>
<tr>
<th>Feature</th>
<th>Free Version</th>
<th>Pay Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Cost</td>
<td>Free</td>
<td>$$$</td>
</tr>
<tr>
<td>Community Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TAC Support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>App Updates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Improvements and Enhancements

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built from scratch in Python</td>
<td>• No Perl dependencies&lt;br&gt;• Python very popular&lt;br&gt;• Completely up to date with entire 6.2 API schema</td>
</tr>
<tr>
<td>Multi-process</td>
<td>• Highly scalable</td>
</tr>
<tr>
<td>Multi-FMC Support</td>
<td>• Connect multiple FMCs to one instance&lt;br&gt;• Reduce complexity</td>
</tr>
<tr>
<td>Fully Qualified Event Output</td>
<td>• Encoded event info is written out in text</td>
</tr>
<tr>
<td>Event de-duplication (Future)</td>
<td>• Avoid paying Splunk for redundant event data&lt;br&gt;• Gives Firepower HA configurations more flexibility</td>
</tr>
<tr>
<td>TAC Supported option available</td>
<td>• End to End support for Firepower Splunk customers</td>
</tr>
<tr>
<td>Forward Compatible</td>
<td>• Ongoing maintenance to support new eStreamer API versions</td>
</tr>
</tbody>
</table>
PXGrid?
Cisco Cloud Security and Splunk
Cisco Cloud Security

Umbrella

Cloudlock

Investigate
Splunk Add-on for Cisco Umbrella Investigate

Automatically enrich security alerts inside Splunk, allowing analysts to discover the connections between the domains, IPs, and file hashes in an attacker’s infrastructure.
Splunk App for Cisco Cloudlock

- Manage Cloud Security incidents within Splunk
- Seamless extend Security Operations to cloud environments while maintaining existing workflows
- Leverage Splunk’s rich data visualization, alerting and reporting functionality
- Two leaders - Partnership Strength
ShadowIT for Cisco FP and Splunk Customers

DESIGNED TO SUPPORT ANY DATA SOURCE
Correlating Network And Infrastructure Data Around The World

Using open APIs monitor and manage connectivity and security for the largest Latin American country

Colin Lowenberg
Collecting Meraki Data Into Splunk

Syslog

TCP Input

Add-on

HTTP Event Collector

API

XML CMX

Cisco Meraki
Cisco Meraki + Splunk

México Conectado connects all Mexican government buildings using Meraki

- Managed WiFi in all Mexican Gov’t buildings: libraries, health centers, community buildings, etc.
- Indoor and outdoor APs for gov’t and public use
- 22K+ sites across Mexico
### Smart Cities & Government Analytics

The Mexico Conectado Project

Country Digitization Analytics Platform

CDAP (powered by Splunk)

---

### 3,841,279 Usuarios Únicos

El número representa la suma de los dispositivos únicos en el periodo de tiempo especificado. Se realiza el supuesto de que un dispositivo es igual a un usuario.

<table>
<thead>
<tr>
<th>Cuánto Ancho de Banda se Consumió de Internet:</th>
<th>Cuánto Ancho de Banda se Generó hacia Internet:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>172.8 TeraBytes</strong></td>
<td><strong>20.2 TeraBytes</strong></td>
</tr>
</tbody>
</table>

**Suma del Tráfico Recibido en el periodo de tiempo.**

**Suma del Tráfico Enviado en el periodo de tiempo.**

### Cuánto Tráfico se Recibe por Tipo de Aplicación:

- other (129)
- microsoft.com
- YouTube
- UDP
- Software updates
- SOCSS proxy
- Non-web TCP
- CDNs
- Facebook
- Google HTTPS
- Miscellaneous audio
- Miscellaneous secure web
- Miscellaneous video
- Miscellaneous web

### Cuánto Tráfico se Envía por Tipo de Aplicación:

- other (128)
- microsoft.com
- apple.com
- YouTube
- UDP
- Non-web TCP
- Miscellaneous web
- Miscellaneous secure web
- Miscellaneous audio
- Miscellaneous video
- Miscellaneous web
Your Splunk Environment: Better on Cisco UCS

Automate deployment, correlate with your entire datacenter, and optimize for management and scalability

With Karthik Karupasamy
Cisco UCS Add-On for Splunk Enterprise
Splunk Add-On for Cisco UCS

- Splunk-built rewrite of original UCS add-on
- Aggregates, monitors, trends and analyzes all relevant data from Cisco UCS Manager instances
- Enables proactive capacity and performance monitoring/management, fault trending, power and cooling, and more
- Works with other Splunk add-ons and data sources (including Enterprise Security and PCI Compliance add-ons) to aggregate and correlate data across your enterprise
Accelerated Troubleshooting with Splunk & UCS

See demo on Youtube at bit.ly/splunk-ucs-mtti
Cisco Unified Computing System

A differentiated, revolutionary approach

**Simplified Architecture**
- Networking with fewer components
- Lower cost and easier scaling
- Fewer management touch points
- Stateless: any resource, any time
- Better TCO/ROI

**Unified Management**
- Faster deploy/provision
- Unification leads to reduced complexity
- Management via a single interface

**Higher Performance**
- Brings out the best of x86 architecture
- Optimized resource utilization for compute, networking, and management

**Scale**
- Ultimate Scalability Enhanced design capability
- Designed for the future, today
Cisco UCS Integrated Infrastructure for Big Data Topology

- SingleConnect: LAN, SAN and Management
- Support for direct connectivity to Fabric Interconnects
- UCS 6200 and 6300 Series Fabric Interconnects, Installed in pairs, active-active. UCS Manager is embedded

Pre-tested and pre-validated configuration

Fabric-based infrastructure integrates computing, networking, and storage resources

Designed for high performance and availability
Cisco UCS Director Express for Big Data
UCS Director Express for Big Data

Deploy your Splunk Enterprise Cluster in hours – not in days or weeks

Features:

▶ Complete automation of industry-leading validated solution for Splunk Enterprise
▶ Indexer clustering – customizable Replication and Search Factors
▶ Search Head clustering
▶ Shared License Master, Deployer for SHC
▶ Ability to grow the Search head, Indexer clusters.
▶ Monitoring console
UCSD Express For Big Data – Two Ways to Create
Unified Management Platform for Highly Available Distributed Splunk Clusters

Use Bundled Templates (Instant)

Create your Custom Template

Select Size

Splunk Version

OS

IP Address Binding

Ready-to-Use Splunk Cluster
Instant Splunk Cluster Under One Management

- Marketing LOB
- Supply Chain LOB
- Sales LOB
- IT Team

- Shadow IT for Big Data
- Insights
- Decisions

- Marketing Splunk Cluster
- Supply Chain Splunk Cluster
- Sales Splunk Cluster

- Faster Turnaround Time
- No Shadow IT team
- No Growing Pains
- Scalable performance and Enterprise Grade system

- Unified Data Center Management
- Optimal Resource Utilization
- Simplified Compliance and Governance

© 2017 SPLUNK INC.
Unified Management with UCS Director Express for Big Data
Programmability, Scalability and Automation

UCS 6200/6300 Series Fabric Interconnect
UCS C220/C240 M4/M5 Series Rack Servers
UCS S3260 Storage Server

Cisco UCS Service Profile
- NIC MACs
- HBA WWNs
- Server UUID
- VLAN Assignments
- VLAN Tagging
- FC Fabrics
- Assignments
- FC Boot Parameters
- Number of vNICs
- Boot order
- PXE settings
- IPMI Settings
- Number of vHBAs
- QoS
- Call Home
- Template Association

Org & Sub Org Assoc.
- Server Pool Association
- Statistic Thresholds
- BIOS scrub actions
- Disk scrub actions
- BIOS firmware
- Adapter firmware
- BMC firmware
- RAID settings
- Advanced NIC settings
- Serial over LAN settings
- BIOS Settings

Splunk Enterprise
UCSD Express
Cisco UCS Manager
Service Template
Service Profiles
UCS Manager
Splunk Enterprise
## Programmable Infrastructure

### Policy based Management

Abstraction of all configuration and identity information into a service profile speeds deployment, reduces errors, lowers costs.

<table>
<thead>
<tr>
<th>UCS Management Software provides:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provisioning</strong></td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
</tr>
<tr>
<td><strong>Growth</strong></td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>UCS Manager</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Industry leading tool to provision, manage and monitor all software and hardware components</td>
</tr>
<tr>
<td>• Policy and model-based management, with service profiles, that improves agility and reduces risk</td>
</tr>
<tr>
<td>• Utilizes auto-discovery to detect, inventory, manage, and provision system components</td>
</tr>
<tr>
<td>• Offers a comprehensive open XML API, which facilitates integration with third-party management tools</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>UCS Central</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Manages multiple, globally distributed Cisco UCS domains with thousands of servers from a single pane</td>
</tr>
<tr>
<td>• Provides global configuration capabilities for pools, policies, and firmware</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>UCS Director</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Delivers a unified converged infrastructure management solution</td>
</tr>
<tr>
<td>• Provides programmable application containers across computing, networking, and storage resources and extend automation benefits to the entire infrastructure stack</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>UCS Director Express for Big Data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Delivers scalable and reliable Hadoop deployment on UCS Big Data clusters</td>
</tr>
<tr>
<td>• Offers centralized visibility across Hadoop and physical infrastructure</td>
</tr>
<tr>
<td>• Provides greater IT agility resulting in increased IT impact on business</td>
</tr>
</tbody>
</table>
UCS Director Express for Big Data
End-to-end provisioning, deployment and management

1. Subject Matter Expert
   Define Policies

2. Policies Used to Create Hadoop and Infrastructure
   Service Profile Templates

3. Service Profile Templates
   Create Service Profiles

4. Associate Hadoop and Infrastructure Profiles to
   create Hadoop Clusters

Create Infrastructure Profile
Create Hadoop Profile
Create Hadoop Application Profile

- Namnode, data node configuration
  - Configure Hadoop services
  - Setup heap size and memory buffers
  - HDFS, MapReduce configuration
  - Setup other Hadoop services

- Uplink and server port configuration
  - Network interface card (NIC) configuration: MAC address, VLAN, and QoS settings; worldwide names (WWNs), and bandwidth constraints; and firmware revisions

- Unique user ID (UUID), firmware revisions, and RAID controller settings
  - Service profile assigned to server, chassis slot, or pool

- Server SME
- Storage SME
- Hadoop SME
- Network SME

Create Hadoop Profile

Create Hadoop Application Profile

- Server SME
- Storage SME
- Hadoop SME
Creating and Managing Splunk clusters
Splunk Cluster customizations

Select physical infrastructure options

Optionally add another NIC for Replication Traffic

Select custom RAID policy for each Role

Customize Storage Tiers
Creating a Splunk cluster

- Cluster Name
- OS (RHEL)
- Splunk version
- UCS Manager
- Organization
Creating a Splunk Cluster

- Server-pools (per role)
- Map vNIC to IP-Pools.
  - Mgmt, (and ingest)
  - Data1 for Replication (optional)

Replication Factor, Search Factor

Click Submit

Server Pools

Networking

PXE VLAN

Replication Factor, Search Factor
Creating a Splunk Cluster -- Server Pool Selection

- **Server Count**
- **Hostname Prefix**
- **Server Pools**
Creating a Splunk Cluster -- VNIC configuration

- Map vNIC to IP-Pools.
  - NOTE: eth0 → MGMT pool binding shown.
- Click Submit
Splunk Cluster is powered by Underlying UCS HW Template

Splunk’s UCS HW Template comes with Flexible RAID Policy

RAID Policies Supported:

- RAID1, RAID0
- RAID5, RAID6
- RAID10 (default)
- Future (RAID50, RAID60)

Separate RAID policies for HOT/WARM, COLD and Frozen
Splunk UCS HW Template – RAID Policy

Custom Partitions

RAID Policy
Splunk UCS HW Template – Inside the RAID Policy

RAID10 for HOT/WARM

Cold data on the same RAID group
Splunk UCS HW Template – Inside the RAID Policy

RAID10 for HOT/WARM

RAID5 for COLD
Typical Big Data Deployment Challenges

- Paralysis by HW analysis
- Inconsistent configurations
- Repeatable results
- Justifiable costs/TCO/footprint
- Scalability and sustainability

Cisco UCS Delivers

- Accelerated Sales cycle/time to production
- Reduced architectural planning and calculation for the customer
- Consistent, repeatable results
- Comprehensive automated deployment
- Facilitates Splunk expansion at a reduced footprint
ACI and Tetration
Aci-splunk: What Is New?
Cisco ACI App & Add-on for Splunk Enterprise version 4.0 – Splunk Certified

- Multi-Pod visibility
- Micro-Segmentation support
- Enhanced user interface with drill down capabilities
- ACI App Center integration

Supported on APIC 1.3 and higher
Compatible with Splunk 6.4 & above
Tetration Analytics App for Splunk
Cisco Tetration App & Add-on for Splunk Enterprise version 1.0
Use Tetration APIs to receive ADM, Endpoints, Inventory data
Send Configuration data, health & performance metrics, syslog and fault information
Enforce policies using Tetration sensors

Real-time Application Monitoring | Accelerated RCA & deeper visibility | Policy Enforcement
Why You Never See Tacos Mounted On Drones In The Real World

Wrapping up the Cisco and Splunk innovation story
With Robert Novak
Thank You

Don't forget to rate this session in the .conf2017 mobile app
Supplemental Information
<table>
<thead>
<tr>
<th>Cisco Technology</th>
<th>Description</th>
<th>SplunkBase URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Firepower™ Management Center</td>
<td>Splunk Add-on for Cisco FirePower Management Center leverages data collected via Cisco eStreamer to allow a Splunk Admin to analyze and correlate reports from Cisco through the Splunk Common Information Model.</td>
<td><a href="https://splunkbase.splunk.com/app/1808">https://splunkbase.splunk.com/app/1808</a></td>
</tr>
<tr>
<td>Cisco eNcore for Splunk</td>
<td>Comprehensive eStreamer ‘Client’ or Splunk ‘TA’ that collects all ten event types in their entirety from Firepower Management Center 6.x</td>
<td><a href="https://splunkbase.splunk.com/app/3662/">https://splunkbase.splunk.com/app/3662/</a></td>
</tr>
<tr>
<td>Cisco Umbrella</td>
<td>Automatically enrich security alerts inside Splunk, allowing analysts to discover the connections between the domains, IPs, and file hashes in an attacker’s infrastructure</td>
<td><a href="https://splunkbase.splunk.com/app/3324/">https://splunkbase.splunk.com/app/3324/</a></td>
</tr>
<tr>
<td>Cisco eStreamer</td>
<td>eStreamer log collection and comprehensive selection of dashboards optimized for Sourcefire System 5.2+ and Splunk 6.</td>
<td><a href="https://splunkbase.splunk.com/app/1629/">https://splunkbase.splunk.com/app/1629/</a></td>
</tr>
<tr>
<td>Cisco IPS</td>
<td>The Splunk Add-on for Cisco IPS allows a Splunk software administrator to consume, analyze, and report on Cisco IPS data that conforms to the Security Device Event Exchange (SDEE) standard.</td>
<td><a href="https://splunkbase.splunk.com/app/1903">https://splunkbase.splunk.com/app/1903</a></td>
</tr>
<tr>
<td>Cisco CWS</td>
<td>The Cisco Cloud Web Security (CWS) Add-on for Splunk allows a Splunk administrator to analyze and correlate Cisco Cloud Web Security (CWS) log data through the Common Information Model in Splunk Enterprise</td>
<td><a href="https://splunkbase.splunk.com/app/2791">https://splunkbase.splunk.com/app/2791</a></td>
</tr>
<tr>
<td>Cisco ESA</td>
<td>The Splunk Add-on for Cisco ESA allows a the Splunk software administrator to leverage Textmail, HTTP, and Authentication logs of Cisco ESA.</td>
<td><a href="https://splunkbase.splunk.com/app/1761">https://splunkbase.splunk.com/app/1761</a></td>
</tr>
<tr>
<td>Cisco AnyConnect</td>
<td>The Cisco AnyConnect Network Visibility (NVM) App for Splunk allows IT administrators to analyze and correlate user and endpoint behavior in Splunk Enterprise.</td>
<td><a href="https://splunkbase.splunk.com/app/2992/">https://splunkbase.splunk.com/app/2992/</a></td>
</tr>
<tr>
<td>Cisco ASA</td>
<td>The Splunk Add-on for Cisco ASA allows a Splunk software administrator to map Cisco ASA devices, Cisco PIX, and Cisco FWSM events to the Splunk CIM.</td>
<td><a href="https://splunkbase.splunk.com/app/1620">https://splunkbase.splunk.com/app/1620</a></td>
</tr>
</tbody>
</table>