IT Services Modernization at Cisco

How Cisco Monitors 3 Million Devices Daily with Splunk

Chris Williamson | Cisco Systems, Consulting Engineer

October 2018

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.

splunk> .conf18

Eating the Network Elephant

Tracking and improving customer networks

splunk> .conf18

Analytics

- Infrastructure analytics
- Application profiling

Using Cisco intellectual capital from over 2.7 million connected devices, 3000 syslog rules and hundreds of industry-standard best practices.

Make informed decisions, faster:

- Gain insight and foresight through proactive monitoring
- Achieve business continuity
- Increase performance

splunk> .conf18

Ongoing Value Through Analytics

- Custom KPIs/metrics
- Innovative analytics use cases
- Multi-architectures, Big Data platforms, and 3rd party solutions integration
- Custom software and apps

- Device configurations
- SW Platform information
- HW Platform information
- Syslogs
- Cisco proprietary data correlation

- Configuration conformance
- Security vulnerabilities
- Software conformance
- Hardware lifecycle status
- SW/HW known published issues
- Device/network performance

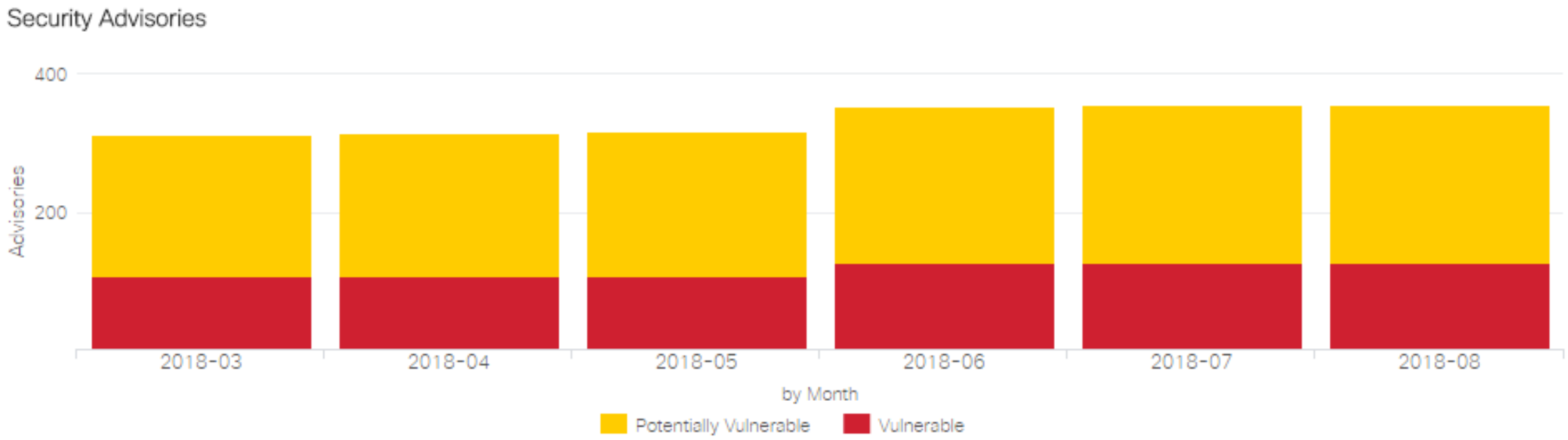
- SME recommendations to prioritize actionable insights
- Insights and analytics consulting and support against industry-standard best practices and intellectual capital

- Improved risk and compliance tracking
- Improved overall network performance
- Improved anomaly detection
- Improved remediation tracking
- Minimized operational gaps through trending and proactive insights

splunk> .conf18

Dive Into the Demo

- BCI demo



How Do We Do it?

The Behind-the-Scenes

What's Under The Hood

- "The Collector"
  - Cisco custom application that manages information collection
  - Functionally similar to a Splunk forwarder or heavy forwarder
  - Handles requirements of data collection against different Cisco OS types
  - Manages different protocol data requirements (SNMP, Syslog, CLI)
  - Completely customizable data collection timeframe & scope
  - Customizable data redaction

An Important Note on Security

- Security & Data Protection is #1 priority
- All data is encrypted
- Data redaction for any information is possible (passwords, username, IPs, etc.)
- Data offloads are not remotely initiated.

How Do We Do It?

The Middle layer of intelligence

Explanation of Middle Processors

- Intellectual Capital
  - Best Practices to Recommended Syslog Actions
  - Each process against their own data type
  - Continuously updated
  - New initiatives on how to mine and increase validity of Intellectual Capital faster
- Automation
  - Matching pieces against Cisco announcements (EOL & PSIRT)
- Making data machine readable

Explanation of Middle Processors

router#show interface

GigabitEthernet0/0/0 is administratively down, line protocol is down
  Hardware is A900-IMA8S, address is c8f9.f98d.1500 (bia c8f9.f98d.1500)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  <snip>

Explanation of Middle Processors

```
bandwidth: 10000000000
bia: c8f9.f98d.1500
cacheTime: 2018-07-14T04:13:36
duplex: full-duplex
input_underruns: 0
input_unicast_packets: 125717290020
input_watchdogs: 0
interface: gigabitEthernet0/0/0
last_clear_counters: never
mac: c8f9.f98d.1500
media_type: null
mtu: 1500 bytes
operStatus: up
order: 99
output_unicast_packets: 124675842256
reliability: 255/255
resets: 2
rxload: 1/255
speed: 1Gb/s
switchport_mode: trunk
timeStamp: 2018-07-13T21:05:48
<snip>
```

How Do We Do It?

Splunk as the Engine

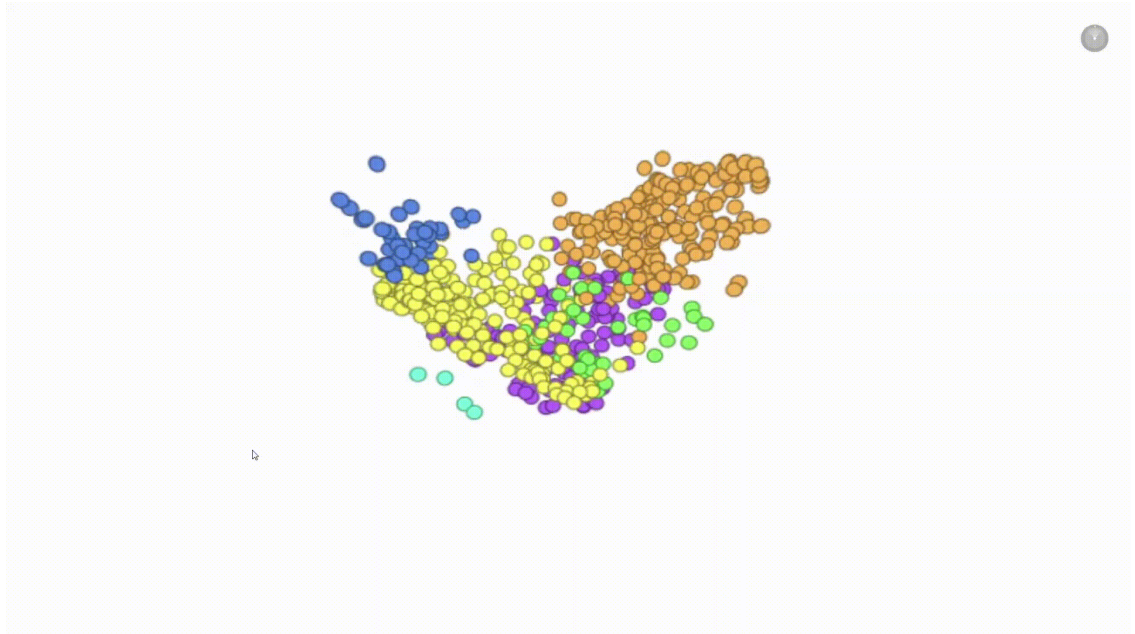
Splunk as an Engine

- Splunk provides:
  - Consulting engineers entry point for data examination
  - Data Scientists an entry point for data mining for recommendations back to Consultants
  - A valuable display tool for Consultants to share information with Customers

How Do We Do It?

The Engineer's Playground

Engineer's Playground – Machine Learning



- Data Scope Consistently increasing
- New use cases consistently in development
- Availability & Ease of access to data is..
  - Driving innovation
  - Reducing time to resolution

Key Take-aways

1. Services provides near-real time analysis of network devices.
2. New subscription access to Cisco intellectual capital as never before offered.
3. Continuous improvements based around data about you and your peers' network.

Questions?

Thank You

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