Zero to Enterprise Security In 30 Days

Moving from a traditional SIEM to Splunk and Enterprise Security…

Nabiha Hasan | Senior IT Security Operations Engineer

Michael Richardson | IT Security Operations Engineer

October 2, 2018 | Version 1.0

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

Who We Are

Nabiha Hasan – Senior IT Security Operations Engineer

Nabiha Hasan has a 10-year career in computing and engineering and has contributed the last five years towards IT Security and Operations at George Mason University. She has a BS in Electrical Engineering and a Masters in Computer Science, with several years of experience with various SIEMs and other security monitoring tools. She holds a certification as a GIAC Certified Incident Handler (GCIH).

Michael Richardson – IT Security Operations Engineer

Mike Richardson has 18 years of professional experience in software development, systems engineering, and security operations. For the past three years, he has served as Security Operations Engineer and Forensics Technician for the IT Security Office at George Mason University. Mike has a BS in Information Technology and is currently pursuing a MS in Digital Forensics and Cyber Analysis at GMU. He holds GIAC certifications in Security Essentials (GSEC) and Certified Incident Handler (GCIH).

George Mason University

Demographics

- Largest public University in Virginia
  - 36,000 students, 5,000 faculty and staff
- Founded in 1972, originally branch of the University of Virginia established in 1957
- Classified as R1: Research Universities (Highest research activity) by Carnegie
- Ranked Most Diverse university in Virginia by U.S. News & World Report
  - Students from 130 countries, 50 states
- 82 undergraduate programs, 88 master's, 39 doctoral, law school

George Mason University

IT Security Office (ITSO) within Information Technology Services (ITS)

- Small shop relative to our peers
  - Director of IT Security
  - 3 Security Analysts
    - Day-to-day threat analysis, mitigation
    - Create splunk content
  - 2 Security Operations Engineers
    - Maintain servers and tools (applications) used by ITSO and outside stakeholders
    - Primary splunk administrators
    - Work with sources to bring in new data, create splunk content
  - Student Interns (7)
    - Assist with analyst functions, engineering tasks

The University Environment

- Relatively open access
  - Researchers actively engaging with malware, botnets
- Bring-your-own-device for faculty, staff and students
- Highly segmented network environment
- Mix of managed and unmanaged end devices
  - Difficult to enumerate, no single source of truth
  - End users do “interesting things” from time to time
- Large firewall ruleset with full logging

Why Move to Splunk?

How it all started…

Where Did We Come From?

- Discussions about a new SIEM started early in the year
- License expiration fast approaching (June 2017) , fiscal year ending as well
- Appliance hosts were end-of-life
- CIO requirements
  - Changeover required ZERO loss of visibility in environment
  - Maintenance of all current capabilities (log sources, alerts, etc)
  - Proof-of-Concept environment required before signoff on purchase order

Challenges with Previous SIEM Application

- Resource intensive with limited scalability
- Licensing model was not transparent
- Not as feature-rich as Splunk
- Offered little flexibility for users
- Lack of prompt customer support / community
- Challenges with onboarding log data
  - Some missing data sources could not be easily consumed
- Closed-source application made debugging difficult

What Happened?

The quest begins…

Getting the Ball Rolling

- Reached out to splunk sales for quote, cloud demo
  - Demo of splunk enterprise and Enterprise Security app
- Worked with sales engineer to properly size hardware / licensing volume
  - Estimated GB/day with several months of live data volume on existing environment
  - splunk Storage Sizing app (https://splunk-sizing.appspot.com/) to determine disk capacity
  - Hardware requirement documentation for RAM, CPU requirements
- Built up hardware, software licensing quotes

Getting Funded

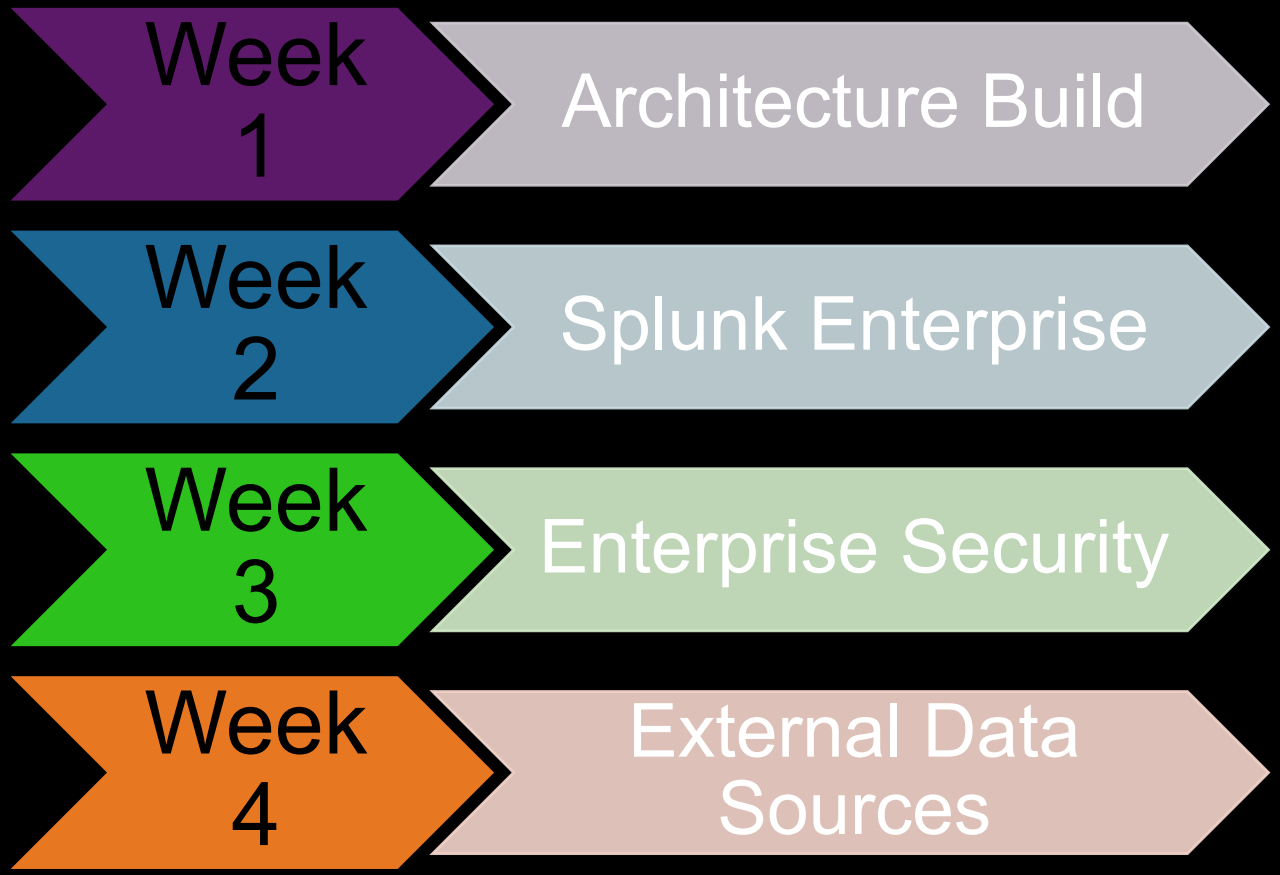
The Proof-of-Concept Environment

- Worked with splunk partner and sales engineers to build proof-of-concept cluster
  - Used existing hardware
    - 1 search head (virtual machine)
    - 2 indexers (2 physical servers)
  - Added splunk forwarder to existing syslog servers to partially redirect live data
  - Customized TAs for initial data consumption
- Demonstration to Senior Leadership for approval

Production Deployment Begins

splunk> .conf18

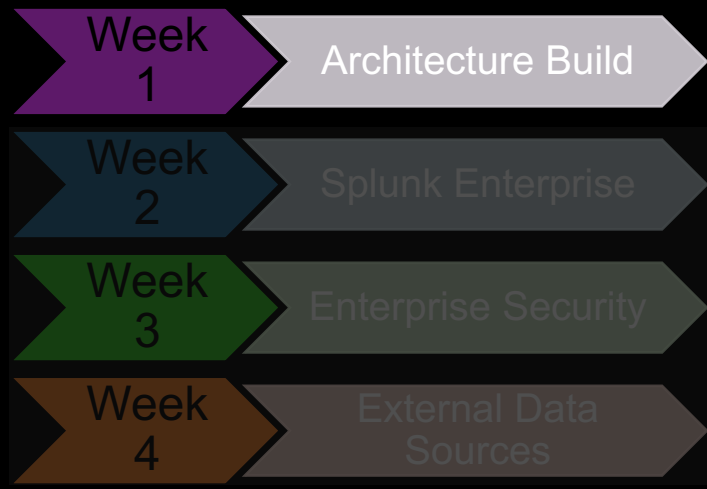
4 Week Roadmap



Week 1 – Architecture Buildout

Physical buildout

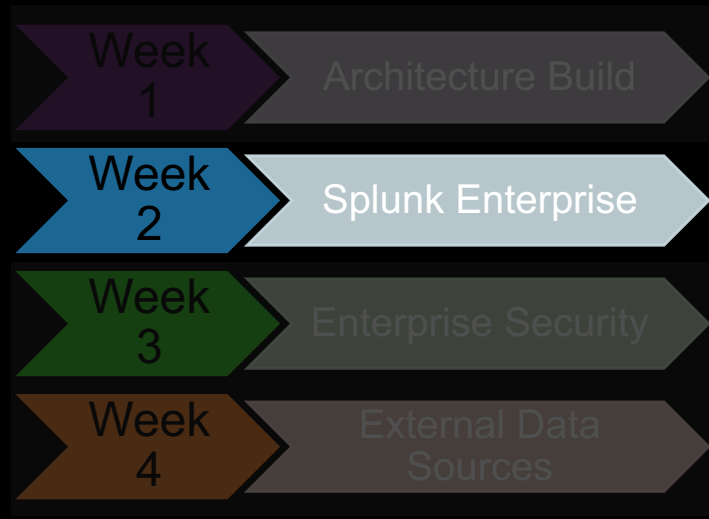
- Receiving, installation of server hardware
  - 6 indexers (clustered)
  - 2 search heads
  - 1 license master, cluster master
- Establish network connections, create and deploy firewall rules
  - New, partitioned network block dedicated to splunk
- OS installation, patching, and hardening
- Installed splunk RPMs
- Requested splunk service accounts for log sources



Week 2 – Splunk Professional Services

Splunk Enterprise

- Configuration of splunk cluster
  - Licensing, cluster master
  - Bringing indexers online into cluster
  - Replaced VM cluster master with physical machine
- First data sources (from proof-of-concept requirements)
  - Firewall data
  - Windows logging (non-production Windows servers for testing)
  - Unix logging (forwarded from a non-ITSO syslog server)
  - Network devices (Cisco ASA, ESA, ISE, WLC)
  - Authentication logs (Active Directory, Unix, VPN, Wireless Authentication)
- Established indexing standards
  - Most log sources have their own indexes = robust access control

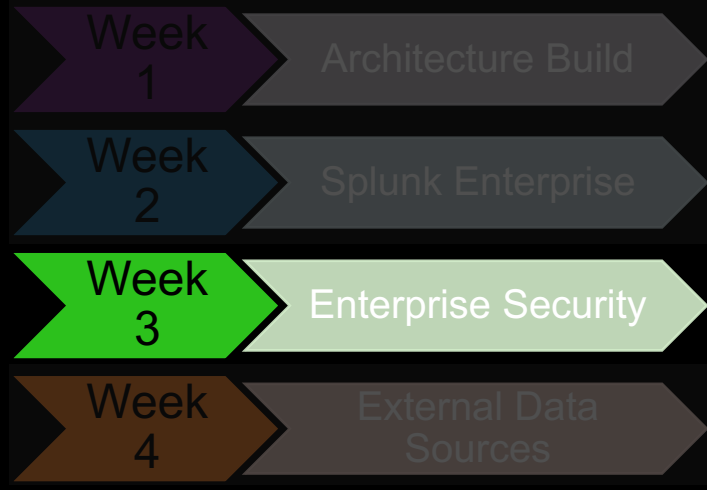


splunk> .conf18

Week 3 – Splunk Professional Services

Splunk Enterprise Security

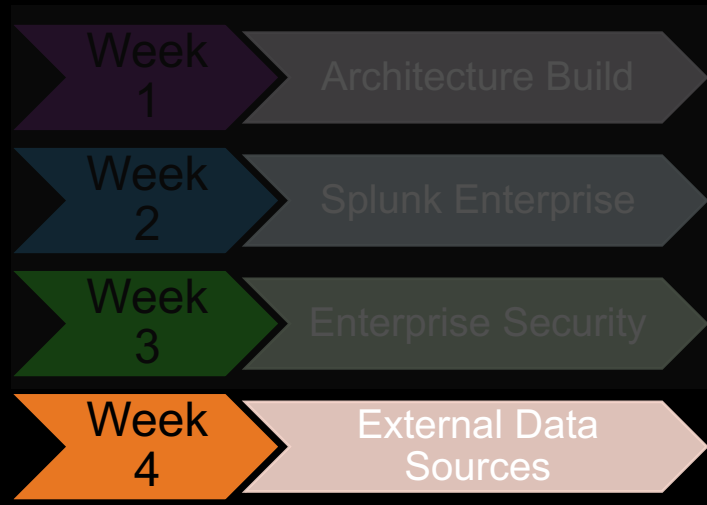
- Installed Splunk Enterprise Security app
  - Modifying correlation searches in ES
  - Adding our specific indexes / source types to the appropriate search queries
- Identify Common Information Model-compliant data sources and Add-ons
  - For non-CIM compliant data, created road map to become CIM compliant
- Windows Authentication use cases
  - Tracking Administrator authentication / notification alerts
- Began working on defining Notables



Week 4 – Splunk Professional Services

External Data Sources / Threat Feeds

- Data Model accelerations
- Proxy servers added and instantiated
  - external threat feeds / intel sources (Threat lists, Two-Factor Log API)
  - Internal feeds as queries (Active Directory authentication, assets, and identities)
- Buildup of Assets and Identities lists for ES
- Brought up resource monitoring alerts
- Building out equivalent alerts from our prior SIEM
  - Privileged account access
  - Improbable VPN authentications
  - Blacklisted external IP communications inbound
- Worked on Notable Items



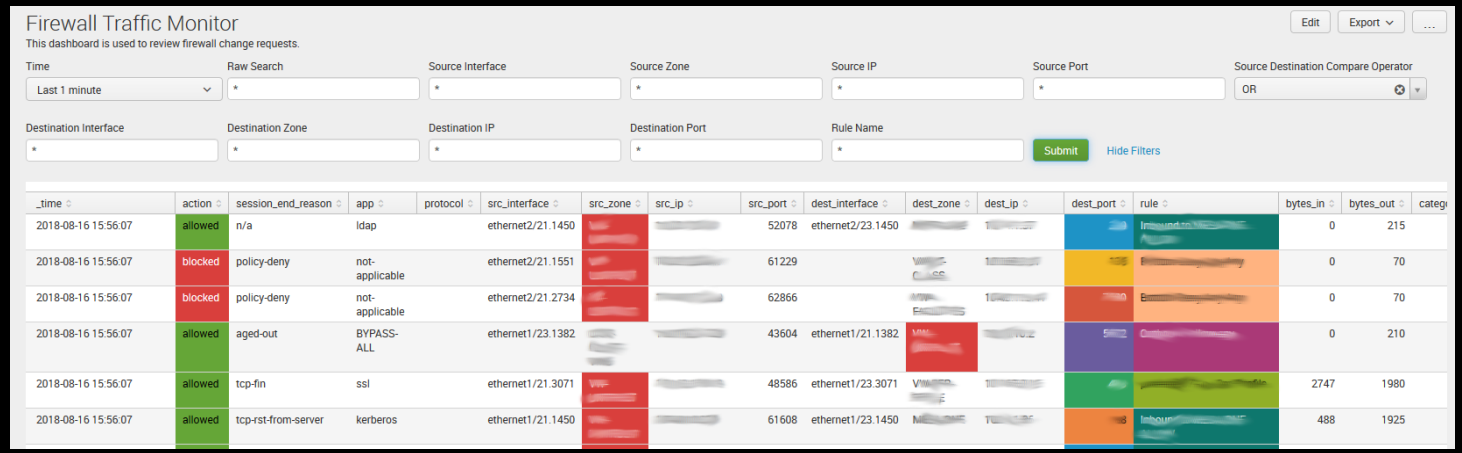
Lessons Learned

Where do we go from here?

One Year In – Maturing the Environment

What else have we come up with?

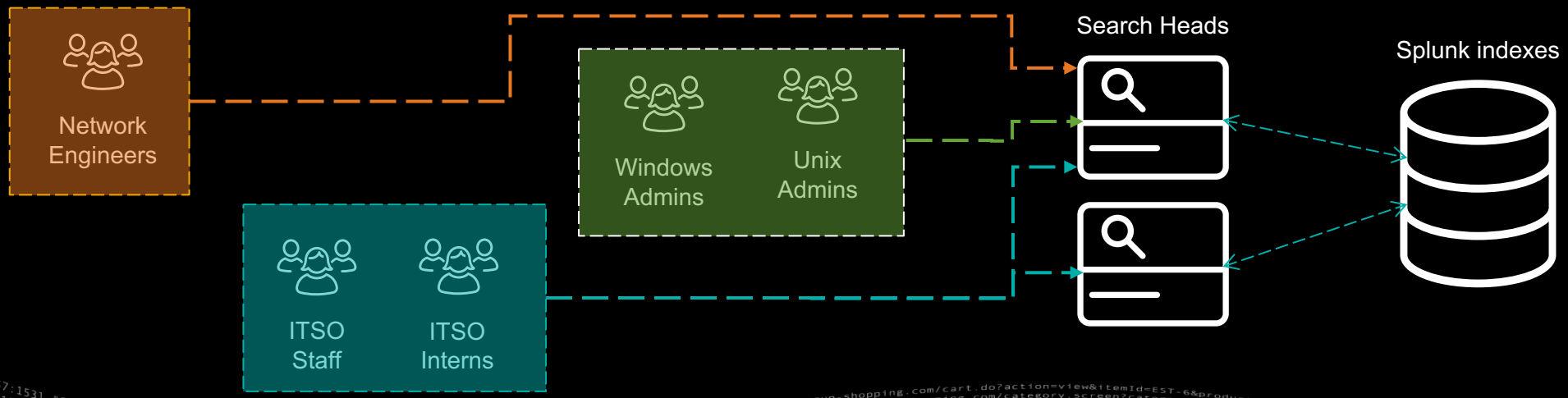
- Use cases that were not on our radar
  - HR – unauthorized payroll deposit changes
  - Asset and Identity correlation across multiple sources
  - Auditing 2-Factor policy enforcement
  - Filesystem forensics (timelining)
  - Firewall rule auditing / verification



One Year In – Maturing the Environment

What else have we come up with?

- Rollout search capability to other departments
  - Create separate app to contain their searches, alerts, dashboards, etc
  - ACLs grant each group access to only the indexes they need to see
  - Separate AD group for splunk users
  - App customizable to remove features (time picker, restrict search windows)
  - Remove default content / dashboards
  - Mandatory training before access is permitted



Lessons Learned

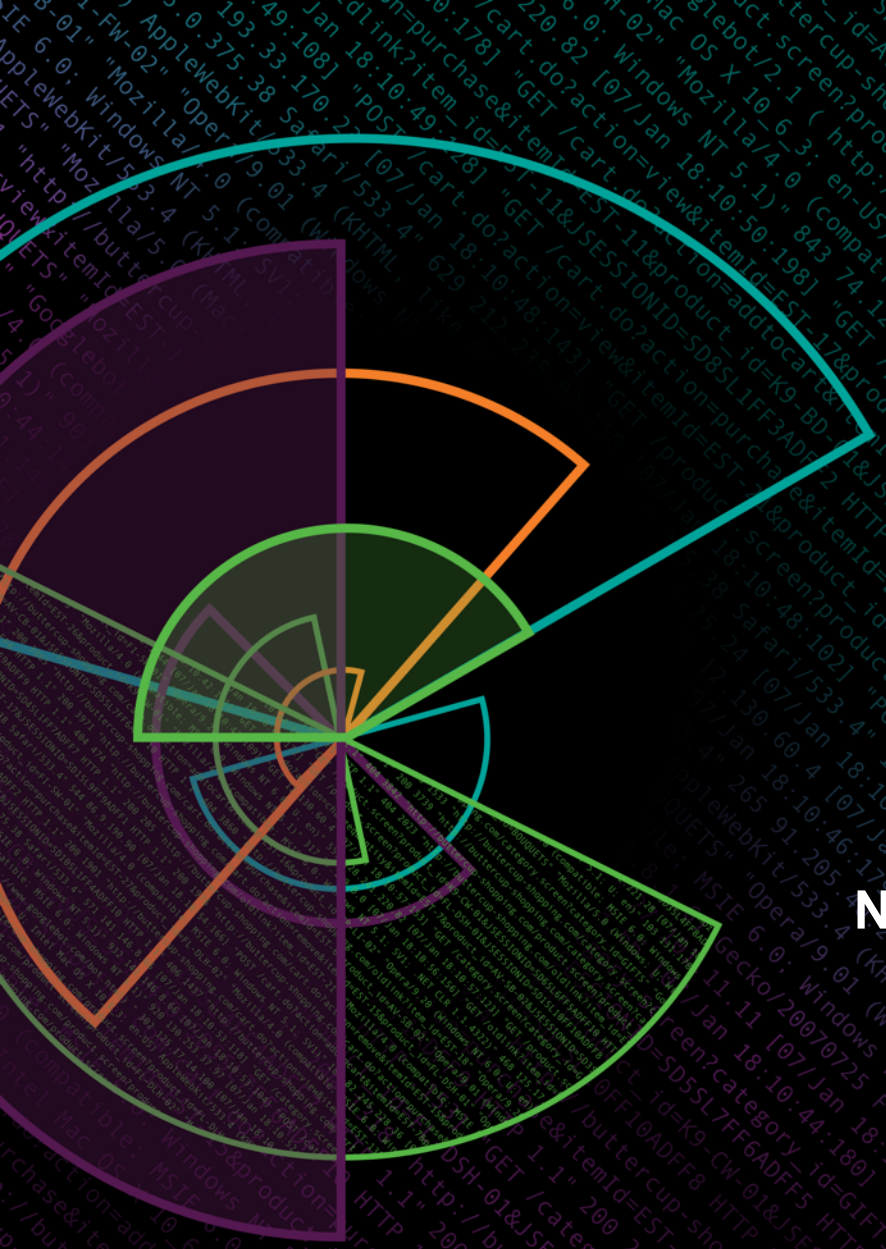
- Professional Services / Partners are valuable assets
  - Three different consultants (pre-engagement, week 1, and remainder)
  - Some initial setups needed to be changed by the next consultant for their tasks
- Estimating Log Volume can be an inexact science
  - Additional log sources required upgrade to our initial licensing volume within 6 months
  - It will be difficult to estimate log sources you are not already consuming
    - Even harder when stakeholders add additional ones you never thought about!
- Trash indexes are your friend
  - Forward to trash for testing, reconfigure to proper index once log receipt and parsing works
  - Flushing trash (using data expiration) much less intrusive than changing production indexes

More Lessons Learned

- Proper network segmentation from the start
  - Challenges with having search heads and indexers in same network once outside users requested access
  - Concerns with high-sensitivity log sources and protecting index data
- Engaging with log source administrators
  - Provide ample time to work within their schedules / workloads
  - Socialize the idea of universal forwarders ahead of time
  - Forwarders much better than chaining rsyslog servers (reduce failure points)
  - Forwarder installation in test environment
    - Especially if using Puppet / Ansible for deployment en masse
  - Nurture buy-in from management / demonstrate value for splunk in their environment
- Existing working relationships helped (especially with Networking and Firewall)

Future Plans

- Search Head Clustering
- Additional indexers
- Further segmentation of indexers from search heads, other application servers
  - Especially as we venture into regulated log sources (PCI, Controlled Unclassified Information)
- Consuming atypical log types
  - Application logs vs. system logs
- Protected data masking
- External cold storage
- OS-level configuration management and orchestration
- Load balancing syslog servers (from devices not Forwarder capable)



Q&A

Nabiha Hasan | Senior IT Security Operations Engineer
Michael Richardson | IT Security Operations Engineer

splunk> .conf18

Thank You

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