



splunk®

The Great SIEM Migration

Nathan Adams | PNC Bank

nathan.adams@pnc.com

⑧ 11:00 AM 12

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, 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. © 2018 Splunk Inc. All rights reserved.

The Great SIEM Migration

How to start from nowhere

NATHAN ADAMS

Security Engineer



Ice Breaker

My life in a slide ;)

- ▶ PNC Bank in Pittsburgh, PA
- ▶ Using Splunk for 2+ years
- ▶ Bicycling
- ▶ Hiking
- ▶ Volleyball
- ▶ Golfing

Penny



The Starting Line

Every team needs to start somewhere

2

SIEMS

10,000+

Endpoints

60+

Standard Operating Procedures

90+

Security Rules and Reports

4 Billion

Daily Events

Challenges

What are we trying to solve for?

- ▶ Volume of security events
 - ▶ Manual alert processing
 - ▶ Multiple security tools
 - ▶ Hundreds of daily abuse emails
 - ▶ Manual threat intelligence processing
 - ▶ Multiple SIEM applications



Key Objectives

Things to remember



Log Sources



Data Volume



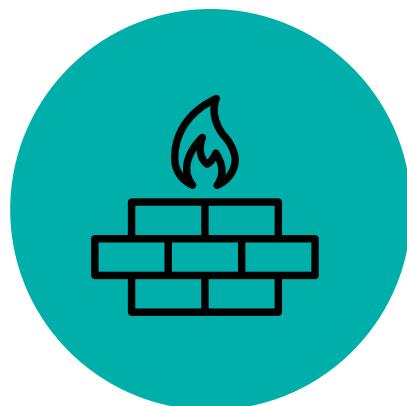
Architecture

Log Sources

What are the crown jewels?



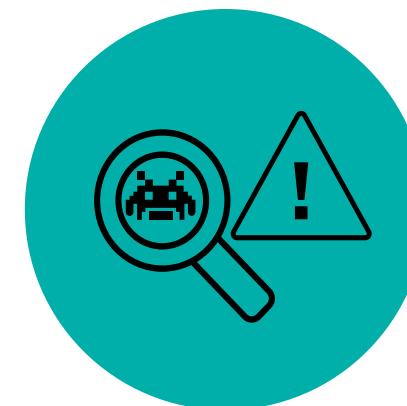
VPN



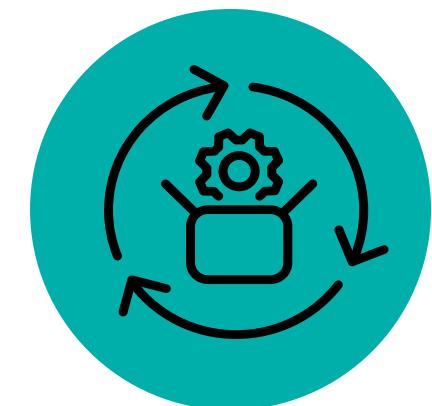
Network



Endpoint



IDS or IPS



Application Servers

Data Volume

What? How much? Where? How long?

- ▶ What are my data sources?
 - ▶ How much data will each source generate per day?
 - ▶ Where is that data being sent?
 - ▶ How long must the data be stored?



Splunk Storage Sizing Tool

<https://splunk-sizing.appspot.com>

Secure | <https://splunk-sizing.appspot.com>

Splunk Storage Sizing

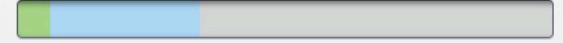
Input data Size by Events/Sec

Estimate the average daily amount of data to be ingested. The more data you send to Splunk Enterprise, the more time Splunk needs to index it into results that you can search, report and generate alerts on.

Daily Data Volume	Raw Compression Factor	Metadata Size Factor
<input type="range" value="200"/> 200 GB	<input type="range" value="0.15"/> 0.15	<input type="range" value="0.35"/> 0.35

Data Retention

Specify the amount of time to retain data for each category. Data will be rolled through each category dependant on its age.

Hot, Warm	Cold	Archived (Frozen)	Retention Time
<input type="range" value="5"/> 5 days	<input type="range" value="25"/> 25 days	<input type="range" value="60"/> 60 days	 Total = 90 days
<input type="checkbox"/> Hot, Warm	<input type="checkbox"/> Cold	<input type="checkbox"/> Archived	

Architecture Cluster Replication Estimate automatically

Specify the number of nodes required. The more data to ingest, the greater the number of nodes required. Adding more nodes will improve indexing throughput and search performance.

Use Case / App	Max. Volume per Indexer	Number of Nodes
<input type="radio"/> Splunk Enterprise Security <input type="radio"/> Splunk App for VMware <input type="radio"/> Splunk IT Service Intelligence <input checked="" type="radio"/> Other	<input type="range" value="300"/> 300 GB	<input type="range" value="1"/> 1 node(s)

Storage Required

This is a breakdown of the overall storage requirement.

Storage and Retention

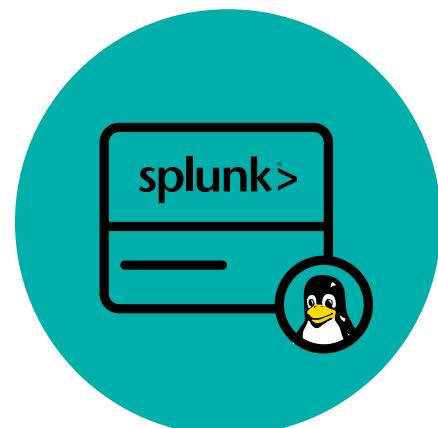
How much does speed matter?

“Splunk will be as slow as it’s slowest device.”

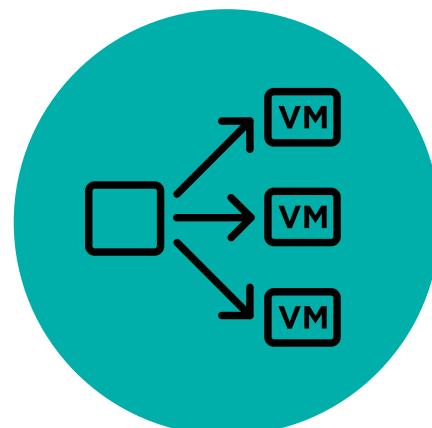
– *Anonymous Splunk Sales Engineer*

- ▶ Disk Input/Output (I/O)
 - 800 I/O Minimum
 - ▶ Key Points:
 - More disks. Better index performance
 - Knowing total throughput is important
 - Understand network latency
 - High latency, slower searches

Splunk Architecture



Bare Metal



Dedicated VMs



Shared VMs

Splunk Architecture

What will be the Splunk foundation?

► Bare Metal

- Best overall performance
 - Latency control
 - Security
 - Alleviates “noisy neighbor” problem

One house. One resident.

A gated community with only one resident

Sharing a gated community

► Dedicated Virtual

- Splunk best practices
 - Performance varies with configuration
 - Scalability

► Shared Virtual

- Lowest performance
 - Shared resources leading to “noisy neighbor”

The Finish Line

Progress is progress

1

SIEM

10,000+

Endpoints

40

Standard Operating Procedures

20

Security Rules and Reports

4 Billion

Daily Events

Key Takeaways

If you don't remember anything else, remember this.

1. What are the critical log sources?
2. How much data will Splunk consume per day?
3. What infrastructure is best for your deployment?

Q&A

Nathan Adams | Presenter

Thank You

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

