The Great SIEM Migration

Nathan Adams | PNC Bank
nathan.adams@pnc.com

October 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

The Great SIEM Migration

How to start from nowhere

splunk> .conf18

NATHAN ADAMS

Security Engineer

splunk> .conf18

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

splunk> .conf18

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

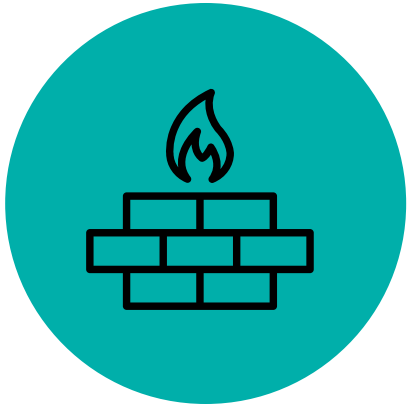
Data Volume

Architecture

Log Sources

What are the crown jewels?

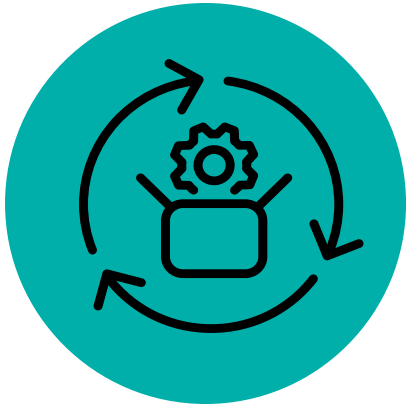
VPN



Network

Endpoint

IDS or IPS



Application Servers

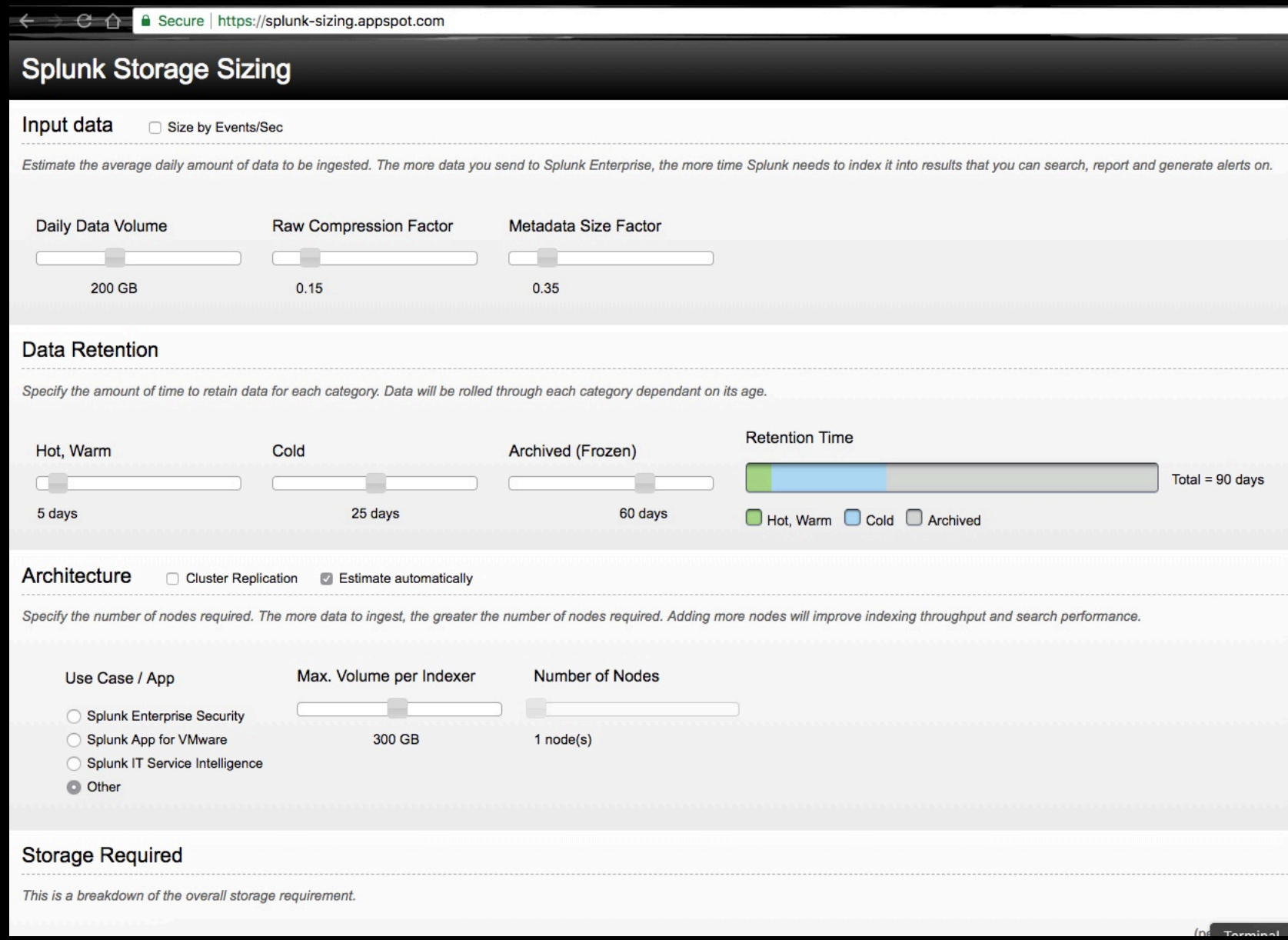
Data Volume

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



Storage and Retention

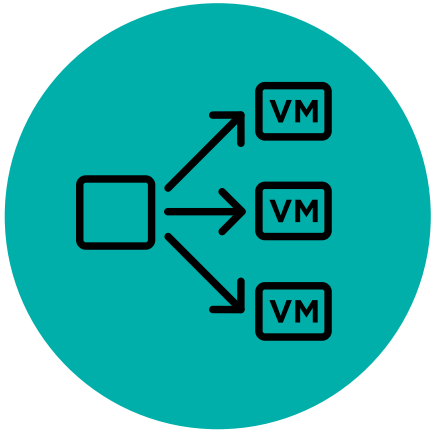
How much does speed matter?

> "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.

- **Dedicated Virtual**
  - Splunk best practices
  - Performance varies with configuration
  - Scalability

A gated community with only one resident

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

Sharing a gated community

The Finish Line

Progress is progress

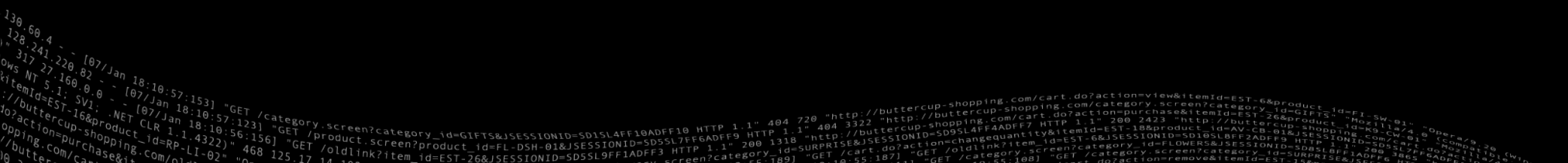
1
SIEM

10,000+
Endpoints

40
Standard Operating Procedures

20
Security Rules and Reports

4 Billion
Daily Events



splunk> .conf18

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

splunk> .conf18

Thank You

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