You Replaced IBM QRadar with Splunk Enterprise Security. Now What?

Ross Rutherford
Manager, Information Security | Western Union

Forward-Looking Statements

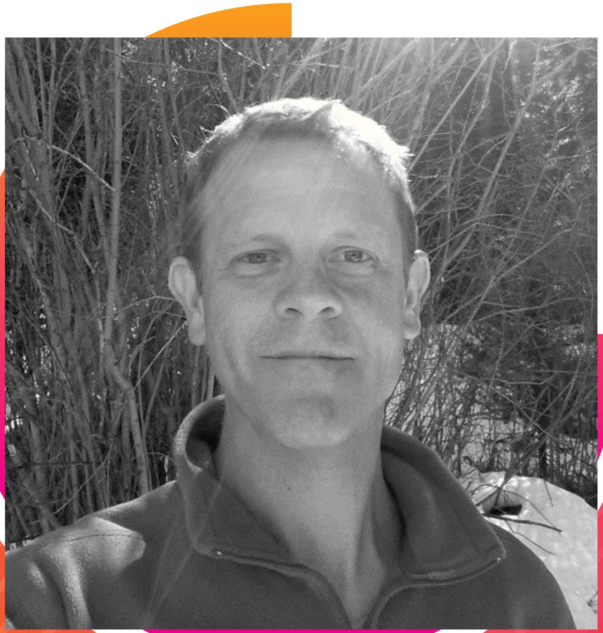
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, 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. © 2019 Splunk Inc. All rights reserved.

splunk> .conf19

You Replaced IBM QRadar with Splunk Enterprise Security. Now What?



Ross Rutherford

Manager, Information Security | Western Union

Nick Ho

Sales Engineer | Splunk

Western Union

About us

Western Union

At a glance

+550K

550,000+ Agent locations around the globe

+200

In over 200 countries and territories

+300bn

We moved more than $300 billion in principal around the world in 2018

130

Transacting in nearly **130 currencies**

Billions

The capability to send money to billions of accounts worldwide

34

Completing an average of 34 transactions each second in 2018

Western Union

At a glance

>12,000 employees worldwide

>50 Large office & Data Center locations

~20,000 servers/network devices/appliances

Terabytes of data per day

What Were We Replacing?

What did QRadar do for us?

- Logging & monitoring – security/compliance (non-application logging)
  - ~20k log sources
- Alerting – SIEM
  - >100 of correlation rules
- Routing relevant data to secondary destination
  - Firewall logs to Algosec
  - Authentication & Proxy logs to CASB

Why Splunk?

Move IT to the Cloud!

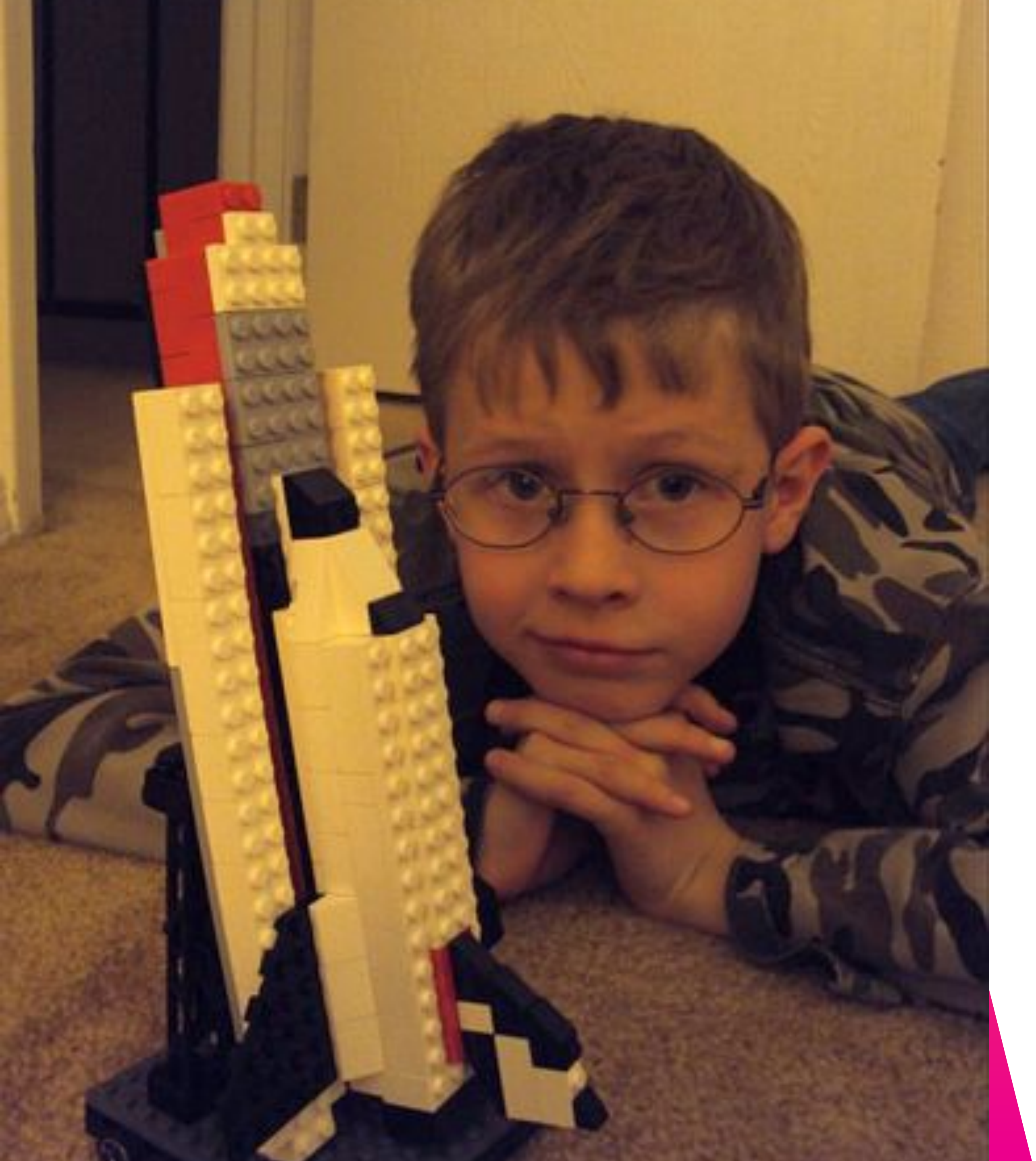
- Reduce physical appliance footprint
  - Maintenance/Support
- Lower storage costs

Consolidate logging platform

- Application logging
- Security/Compliance logging
- IT infrastructure monitoring

Flexibility

- Out-of-box content
- Customized content



“Splunk is Like a Box of Legos”

You can build almost anything you want

But you can’t build a Space Shuttle if you don’t understand how the pieces fit together

Getting Started

On-prem architecture (IFs, HFs, DSs)

UF installs on ~10K servers

- Across multiple BUs
- Manual & Automated

On-board network logs

On-board security appliance logs

3TB/day data ingestion in 3 months

- All with a One-man Splunk team

The Process

What we did right

PS engagements

- On-site (most valuable)
- Not just data on-boarding assistance, knowledge transfer/training

Staff Augmentation

Education (Admin / ES training)

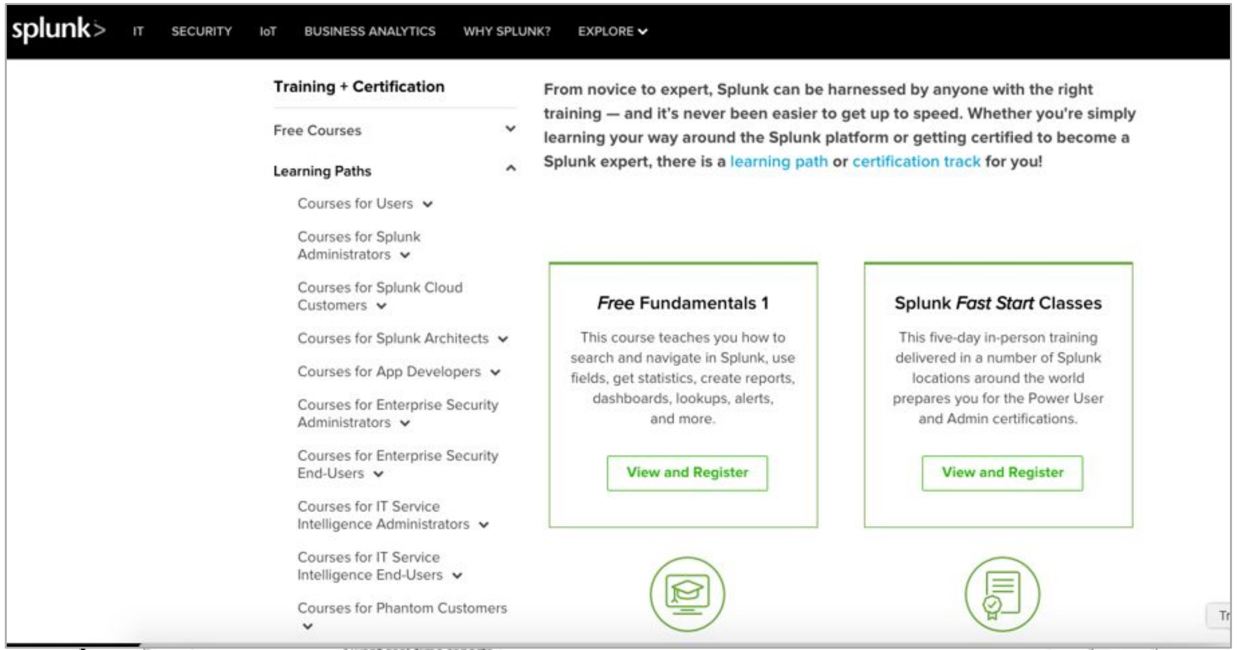
SE lead hands-on workshops

Data on-boarding questionnaire

Exec sponsorship

Splunk evangelization

- People are excited about what Splunk> can do for them



Training + Certification

Free Courses

Learning Paths

- Courses for Users
- Courses for Splunk Administrators
- Courses for Splunk Cloud Customers
- Courses for Splunk Architects
- Courses for App Developers
- Courses for Enterprise Security Administrators
- Courses for Enterprise Security End-Users
- Courses for IT Service Intelligence Administrators
- Courses for IT Service Intelligence End-Users
- Courses for Phantom Customers

From novice to expert, Splunk can be harnessed by anyone with the right training — and it's never been easier to get up to speed. Whether you're simply learning your way around the Splunk platform or getting certified to become a Splunk expert, there is a learning path or certification track for you!

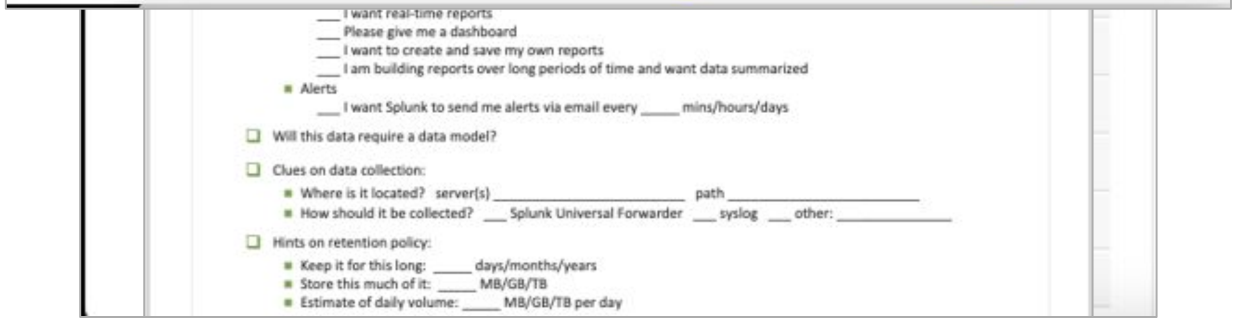
Free Fundamentals 1

This course teaches you how to search and navigate in Splunk, use fields, get statistics, create reports, dashboards, lookups, alerts, and more.

Splunk Fast Start Classes

This five-day in-person training delivered in a number of Splunk locations around the world prepares you for the Power User and Admin certifications.

View and Register



___ I want real-time reports
___ Please give me a dashboard
___ I want to create and save my own reports
___ I am building reports over long periods of time and want data summarized

- Alerts
  ___ I want Splunk to send me alerts via email every _____ mins/hours/days

□ Will this data require a data model?

□ Clues on data collection:
- Where is it located? server(s) _______________________ path _______________________
- How should it be collected? ___ Splunk Universal Forwarder ___ syslog ___ other: _______________

□ Hints on retention policy:
- Keep it for this long: _____ days/months/years
- Store this much of it: _____ MB/GB/TB
- Estimate of daily volume: _____ MB/GB/TB per day

The Process

What we learned

Move too quickly

- IF/HF builds across multiple BUs
- UF Installs
- Users/Roles/Permissions

Competing directions

- SIEM migration
- Application logging
- System performance monitoring

Splunk evangelization

- People are excited about what Splunk can do for them…and they want it NOW!

Not having adequate resources to meet expectations

Splunk Western Union Education Journey

Crawl

Perform simple searches

Walk

Education, know the basics

Run

Education + PS + experience

Ninja

Education + PS + experience + conf + workshops

TAs, CIM, and Data Models…Oh, My!

How to make ES work

Choosing the right TAs/Apps

- Know your data and sources!
- What do you want to see?
- What has the most value?
- What are your use cases?
- Does it align to priority/business need?

CIM

- Make custom sources CIM compliant
- Ensure CIM compliance of TAs installed from Splunkbase

Data models

- Understand what DMs your data applies to
- Assets and identities

Maturing Beyond Legos

Taking Splunk to the next level

Today we are still building with Legos but we're on our way to becoming robot-building Splunk ninjas

Key Takeaways

1. Requirements
2. Requirements
3. Requirements
4. Know your data
5. Invest in expertise/training
6. Set reasonable, attainable expectations

Q&A

Ross Rutherford | Information Security Manager
Nick Ho | Splunk Sales Engineer

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION