splunk> .conf2017

Legacy SIEM to Splunk, how to Conquer Migration and Not Die Trying

Risi Avila | SIEM Migrations Security Consultant, Splunk

Ryan Faircloth | Sr. Security Consultant, Splunk

September 23 – 25, 2017 | Washington, DC

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.

How the Hell Did We Get Here?

I’m done. I’m replacing this SIEM!!!

Most Common Reasons for Replacement!!!

- Splunk’s a great product, why not!!!

- Other worthy reasons ☺ :
  - Limited Security Data Type
  - Inability to Effectively Ingest Data
  - Slow Investigations
  - Instability and Scalability
  - End-of-Life or Uncertain Roadmap
  - Closed Ecosystem
  - Limited to On-Premises

1

Introductions and Agenda

Who are these guys, anyway?

Welcome!

Risi Avila

ravila@splunk.com

Security Consultant, Splunk

- 3 years Splunk
- Former SIEM Consultant / ArcSight Admin, Major Health Insurance Company
- Leads SIEM Migration / Replacement Engagements for Splunk

Ryan Faircloth

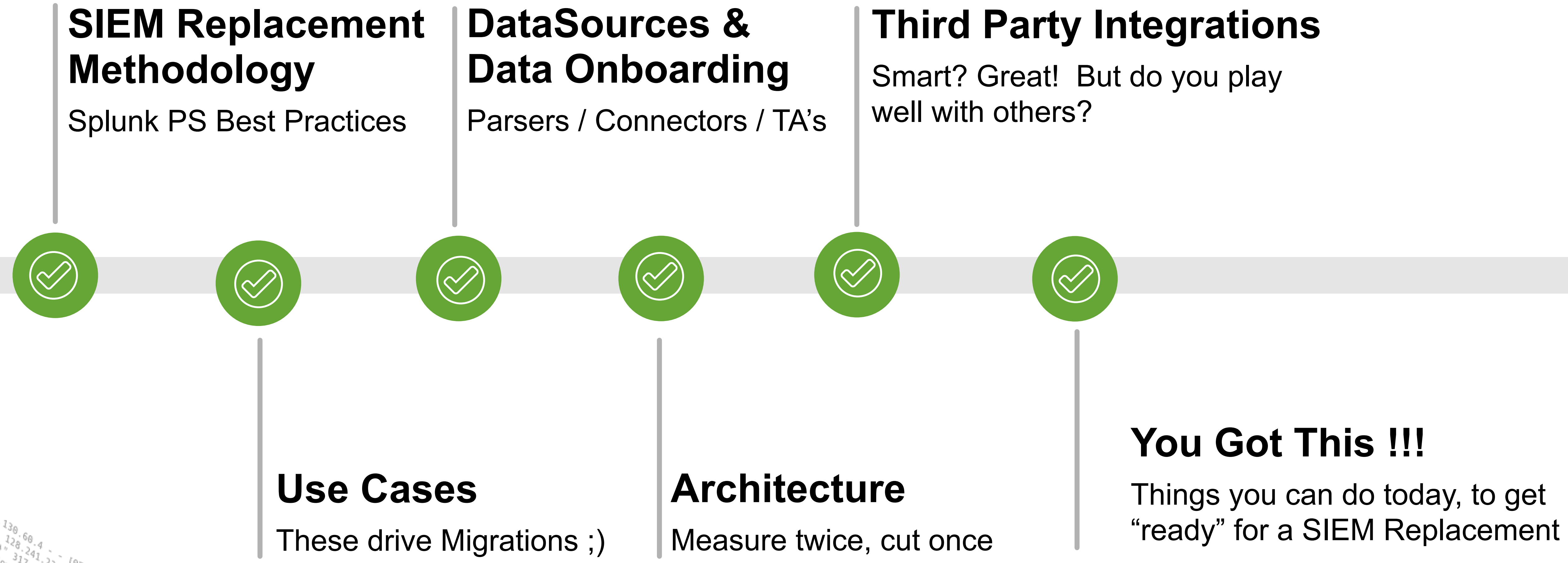
rfaircloth@splunk.com

Sr Security Consultant, Splunk

- 3 Years Splunk
- Security Architect
- Enterprise Architecture
- Leads BHPs (Big Harry Programs)
- Created Use Case Workshop and SIEM Replacement Programs for Splunk

Agenda

What will we be talking about today?



SIEM Replacement Methodology

Splunk PS Best Practices

Use Cases

These drive Migrations ;)

DataSources & Data Onboarding

Parsers / Connectors / TA's

Architecture

Measure twice, cut once

Third Party Integrations

Smart? Great! But do you play well with others?

You Got This !!!

Things you can do today, to get "ready" for a SIEM Replacement

2

SIEM Migration Methodology

Splunk PS Best Practices – based on real world experience

Things You Should Know About Legacy SIEM Replacement, and Splunk PS Best Practices

- SIEM Replacements to Splunk Enterprise Security can be complex, but if the following things are taken into account, you won't loose your job | shirt over it:

- Use Cases matter:
  - Audit & Prioritize Use Cases
  - Planned Response ... Do Something!

- Know your data / datasources
  - Identify datasources & owners
  - Audit datasources
  - Identify enrichment requirements

- Current / Future State Integrations

- Research & Preparation is key

- Assets & Identities

- Partner with Splunk + PS

3

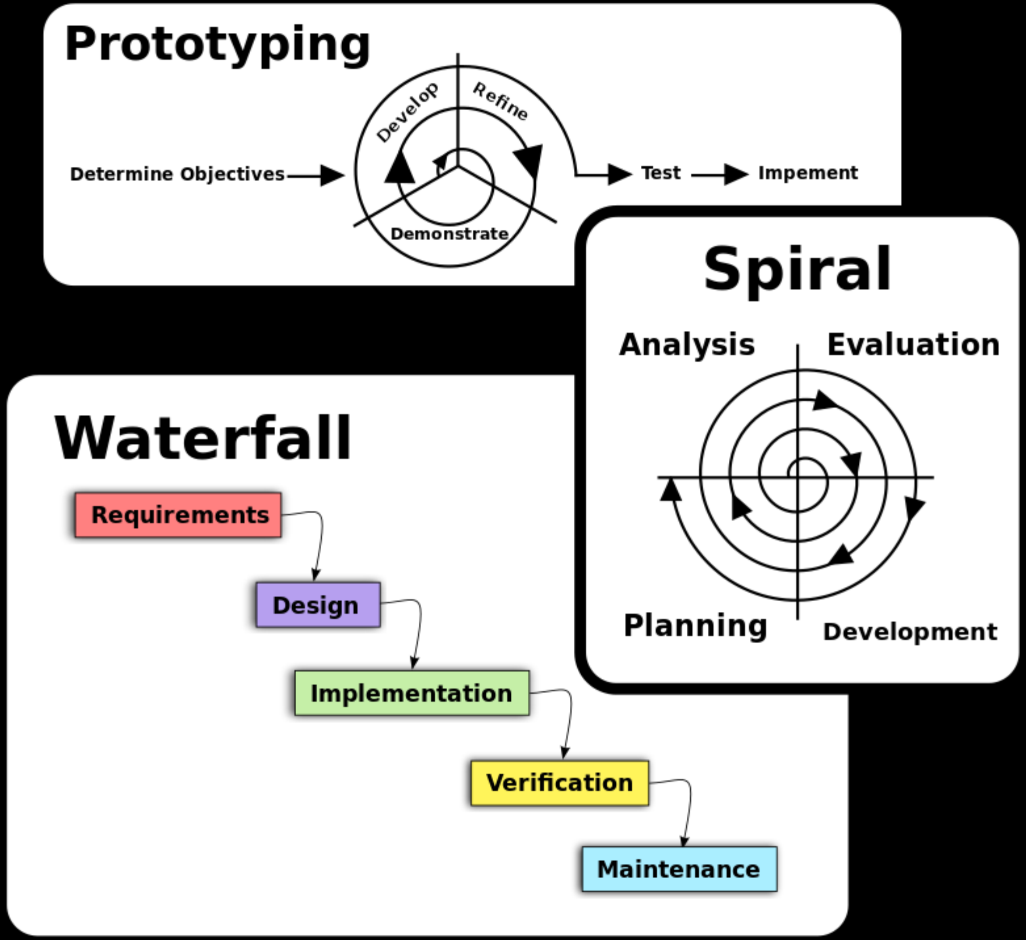
Use Cases

These drive replacements … use cases, Use Cases, USE CASES!!!

What is a Use Case?

- Document describing a single detection activity.
  - What is the condition to detect?
  - What is the event data required?
  - What enrichment is required to scope down events?
  - What enrichment will reduce noise (false positives)?
  - Point to the response plan

  - What are your Current Use Cases?
    - Which ones provide value?
    - Which ones don’t?



Prototyping

Determine Objectives → Develop → Refine → Demonstrate → Test → Impement

Spiral

Analysis

Evaluation

Planning

Development

Waterfall

Requirements → Design → Implementation → Verification → Maintenance

What is a Response Plan?

- Document describing a single response activity
  - For a response what event data is required to triage
  - What actions should be taken
  - Escalation communication and do we need to order pizza
  - Can we reduce the cost of pizza by providing better data for response decisions?

Putting the Horse Before the Cart …

- The first step in embarking on a SIEM Replacement initiative is
  - first identifying and prioritizing high value use cases, response plans and compliancy reports:
    - Splunk PS has a 1-to-2 week SIEM replacement workshop where we come in and help customers:
      - Identify / develop high-fidelity use cases slated for migration / development
      - Datasources, and enrichment identified via use-case prioritization process
      - Plan the solution architecture
    - We typically see a 30% - 60% reduction in use-cases selected for migration

      Generally due to:
      - Old and/or Stale Rules
      - House-Keeping Rules no longer needed
      - Rule consolidation due to advanced Splunk Query Language

So no, You don't have to migrate ALL your old funky rules !!!

How Use Cases Affect SIEM Replacements?

- Next step in embarking on a SIEM Replacement initiative is
  - Quantifying the # of use case / compliancy reports to be migrated and developed in the new Splunk ES environment - 1yr, 3yrs, 5yrs planning:
    - 1 Search/Report = compute resource utilized
  - Quantifying the # of concurrent users will be using the SIEM on a daily basis:

    Generally based on SIEM usage:
    - Security Operations Center (SOC)
    - Security Engineering Team
    - Security Officer(s)
    - Audit Team
  - Assets & Identities – Can't do without it how will you collect from your environment

4

Datasources & Data Onboarding

Parsers / Connectors / TA’s (Technology Addon’)

splunk> .conf2017

How do You Migrate Datasources to Splunk?

- Use Case Analysis determines in-scope datasources
- Why you don’t need to migrate your historical data from Legacy SIEM

- Data Source Onboarding via:
  - Splunk Log Forwarding:
    - Universal Forwarder (UF) Deployed along side existing Parsers /Connectors
  - Syslog Aggregation
    - UF deployed on syslog aggregator to read and ship logs into Splunk
  - Modern HTTP Event Collection
  - Database Tables (DBX)
  - Much more.
  - Never forget Splunk Stream
  - TA’s (Technology Addon)
    - Fields from raw data
    - Data Normalization
    - Splunkbase
      - splunkbase.splunk.com
      - Easy Button: Custom TA's via “Splunk Add-on Builder” App

5

ES Architecture

Measure twice, cut once

Plan the Architecture

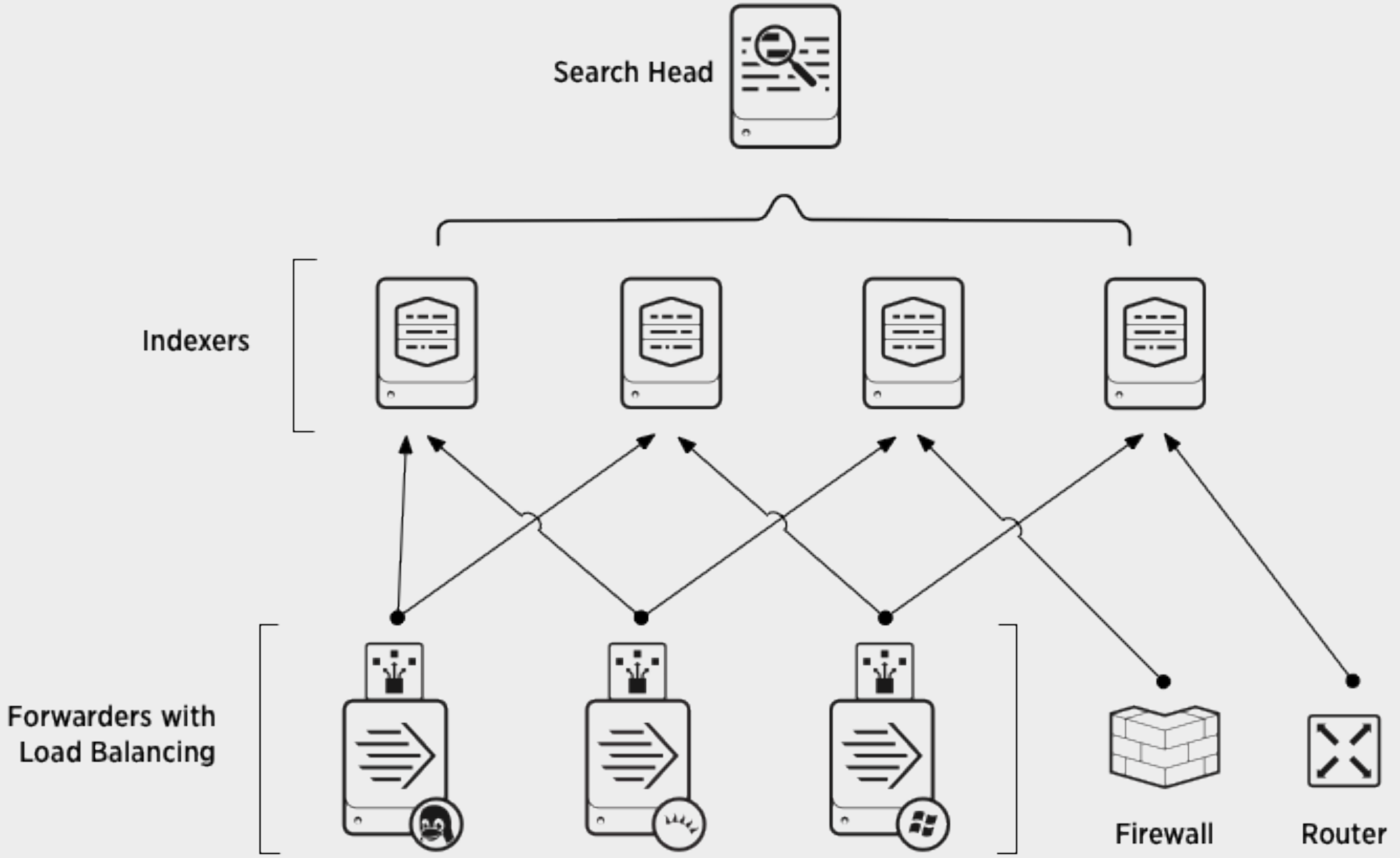
- Now we know what we want to do, how will we do it?
- Plan for modern data collection, deprecate legacy log collection infrastructure, stop accepting log loss today.
- Plan for Disaster Recovery and Availability
- Plan to remediate logging policies, and source configuration

Splunk Architecture

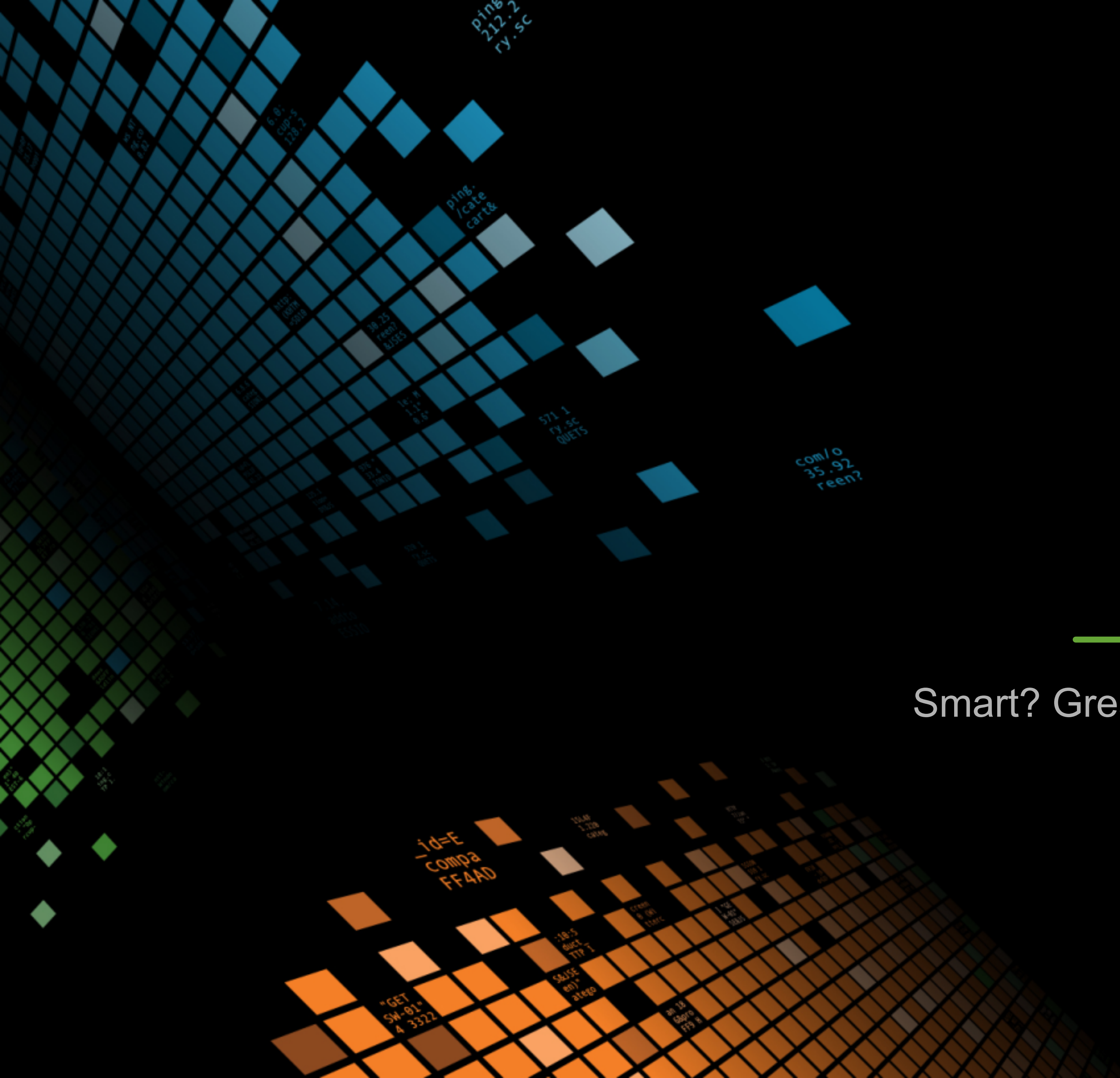
Components >

- Collection Layer (Connectors / parsers Vs. UF's / HF's)
- Parsing Layer (Technology Addon's)
- Storage Layer (Indexers)
- Presentation Layer (Search Head + Enterprise Security App)
- Security Analytics (Enterprise Security App)
- Management Layer (Deployment Server, Cluster Master, License Server, Deployer)

Data source will determine what components are needed. Your network determines where they should be



splunk> listen to your data



5

Third Party Integrations

Smart? Great! But do you play well with others?

Smart? Great! But Do You Play Well With Others?

"At this point in the interview, Johnson, we would like to see how well you play with others."

Richard Stevens, Penfield, N.Y.

Third-Party Integrations

Identify current / future state third-party integration points

We Support Integration with most third-party systems:

- Case Management / Ticketing Systems
  - (ServiceNow, Remedy, etc)
- Threat Intelligence Feeds
  - (STIX, TAXII, Internal, etc)
- Database Integration
  - (Oracle, MySQL, etc)
- Microsoft Active Directory
- REST API support
- Custom Code
- Others

5

You got this!!!

Things you can do today, to get prepared for your SIEM Replacement

Replacement Checklist:

- Identify / Audit & prioritize use cases for migrations
- Identify / Audit and prioritize datasources for Migration
- Identify datasource owners
- Research Splunk Technology Addon's for datasource: splunkbase.splunk.com
- Assets & Identities: Identify CMDB Sources
- Third-party Integrations
- Develop logging standards

What Do “You” Do Next ?

- We've successfully completed countless hair-pulling SIEM replacements before, you're in good hands – partner with us!!!
- Get on the fast track, contact your Splunk Sales Rep. “today” to learn more about PS' SIEM & Use Case Development Programs
- You're in luck, we're here to help you today: We have a break-out room X dedicated for you to talk to us about your SIEM Replacement

splunk> .conf2017

Making Machine Data Accessible, Usable And Valuable To Everyone.

Thank You

Don't forget to **rate this session** in the .conf2017 mobile app

splunk> .conf2017