splunk> .conf2017

Reducing Time to Data

Define millions of inbound web requests

Robert Jue | fb Engineering

September 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.

splunk> .conf2017

Define Millions Of Inbound Web Requests

Harness power of splunk to reduce the time to data

- Millions of inbound web requests
  - What are the requests?
  - Where are the requests coming from?
  - Data visualization?
  - Pattern?
  - Automated reporting?

Turn data points into action items

Define Millions Of Inbound Web Requests

Example: Usage profile, legacy certificate hash versus current

2+

In millions for OCSP requests in 24 hours

1.7

In millions, legacy cert hash issuance

141

Certificate types

splunk> .conf2017

Define Millions Of Inbound Web Requests

How would one data compare without splunk?

- Excel
  - Create a workbook with worksheets of the data to compare
    - Vlookups
    - Scripted compare logic
    - Attempt to throw more resources at it
    - Attempt to reduce time frame to actually come back with data

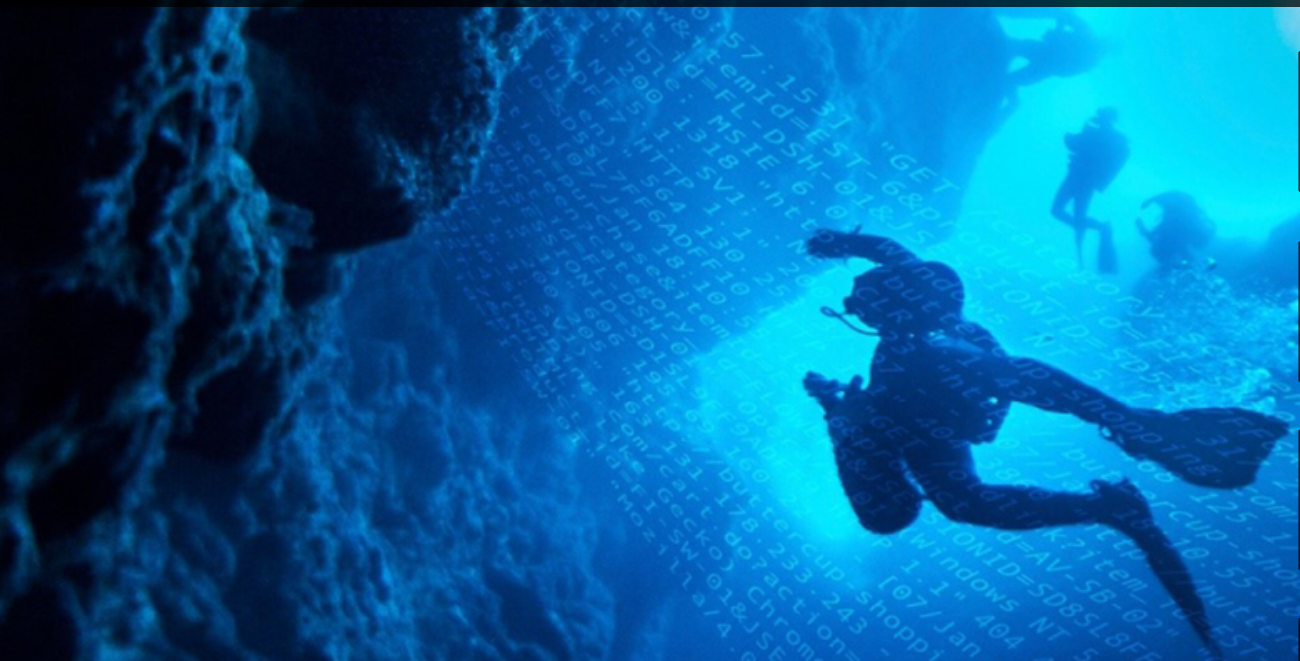
Result: nothing and/or reduced information set

- Custom code
  - Data compare (any/all methods)
    - Index the millions of events in a given time period
    - Attempt to perform data correlation
    - Attempt to throw more resources at it
    - Attempt to reduce time frame to actually come back with data

Result: nothing and/or reduced information set

Define Millions Of Inbound Web Requests

Deep diving the data with splunk



- Import a custom own data set
- Real time data compare
- Minutes away from the data
- Automated reporting / visualization

How Easy It Is?

SOURCES

Verify custom data

| inputlookup <custom data set name>

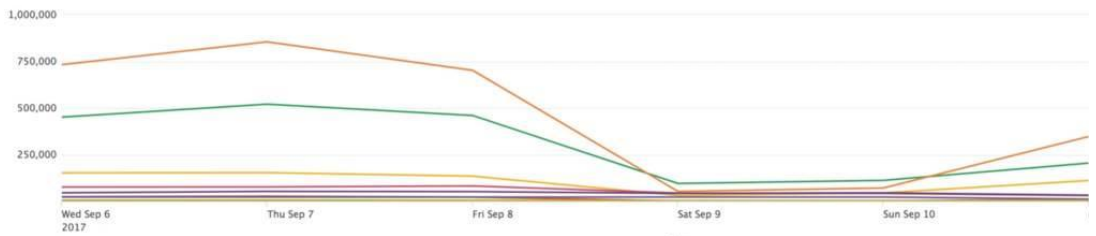
Verify target data

EventCode=5125 "*<Legacy CA name match>*" | dedup Certificate_Serial_Number

Data compare

| lookup cert_serial_num Serial_Number as Certificate_Serial_Number OUTPUT Requester_Name as LegacyUser | search LegacyUser ="*" | table LegacyUser,Certificate_Serial_Number

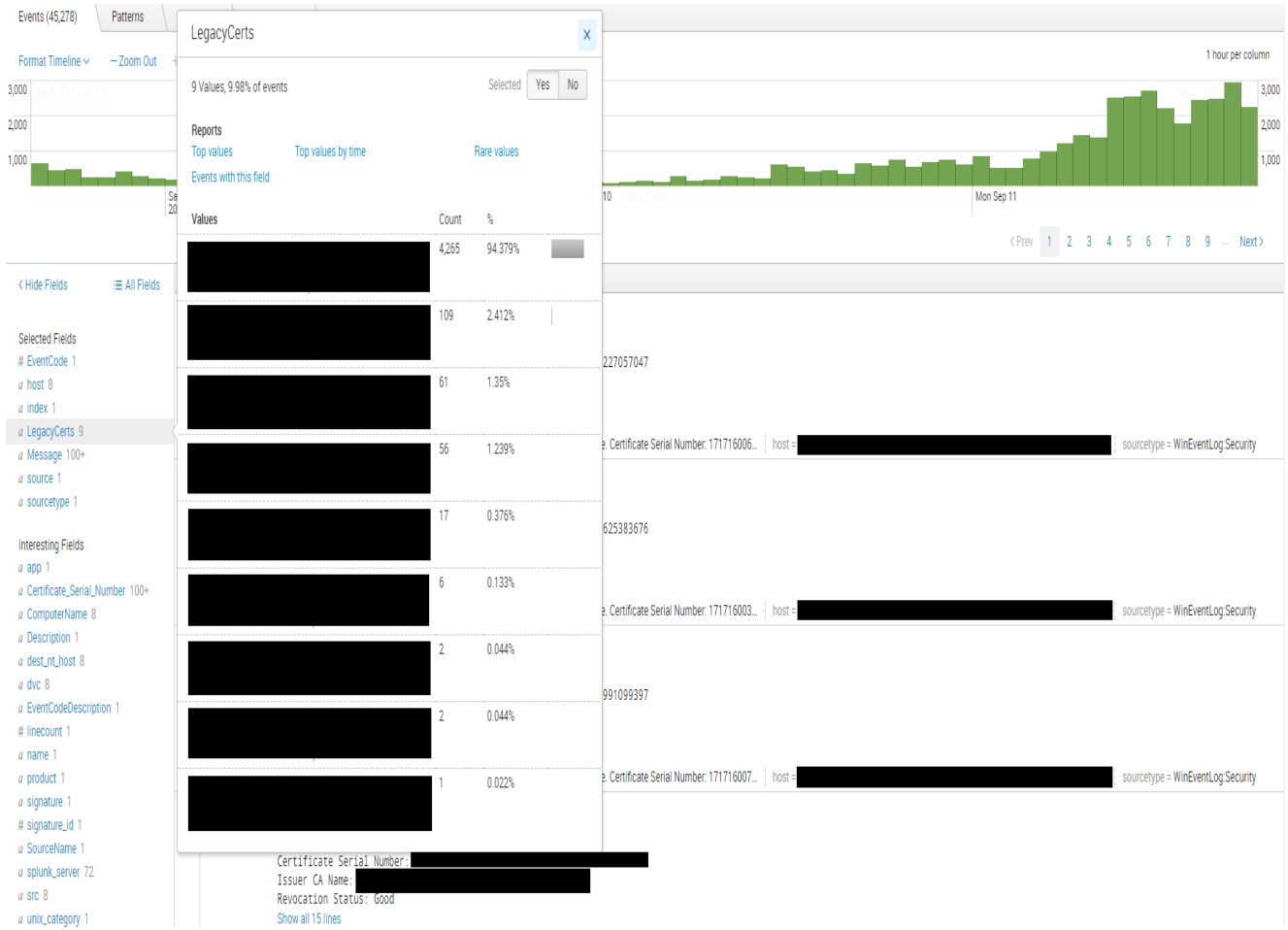
Profit



splunk> .conf2017

Define Millions Of Inbound Web Requests

- Retrieving real time data
- Data visualization
- Default parsing
  - Host breakdown
  - Source
  - Custom lookup

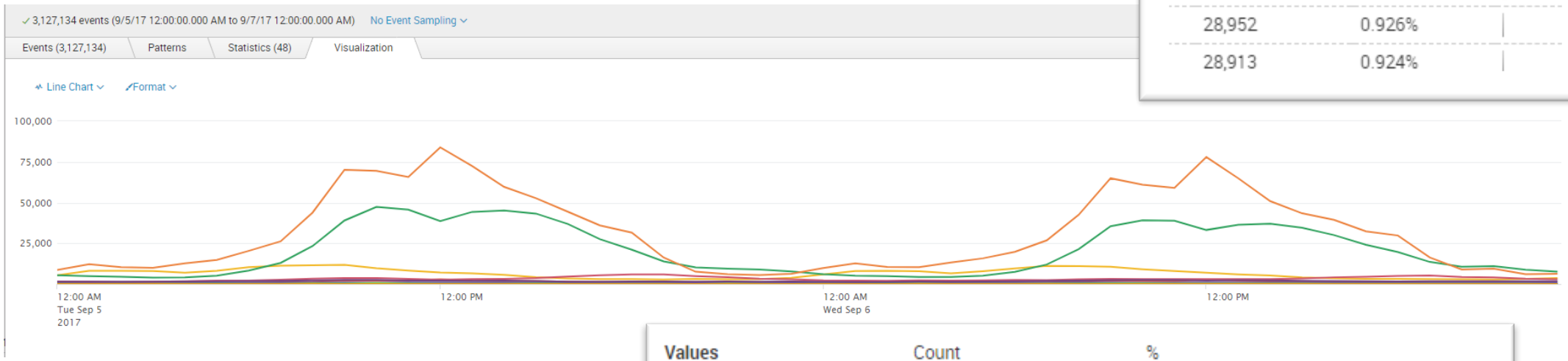


splunk> .conf2017

Define Millions Of Inbound Web Requests

- Simple data visualization overlay
- Simple dashboard creation

Count	%
1,155,962	36.966%
1,155,806	36.96%
196,085	6.27%
196,082	6.27%
182,701	5.842%
182,633	5.84%
28,952	0.926%
28,913	0.924%



Values	Count	%
Good	3,044,971	97.374%
Revoked	82,111	2.626%

splunk> .conf2017

Key Takeaways

Reducing time to data

1. Customize the splunk experience
2. Reduce time to data using splunk
3. Leverage the power of splunk cloud

Thank You

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