splunk> .conf2017

Splunk at Genesco

How we achieved a rapid ROI using Splunk to monitor application logs

Join the PonyPoll! Go to http://ponypoll.com/Genesco

splunk> .conf2017

Splunk at Genesco

How we achieved a rapid ROI using Splunk to monitor application logs

Jeremy Haggard | Manager Platform Systems & Certified Splunk Admin
Michael Nobles | Senior Sales Engineer & Splunker

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

Speaker Intro

Who are we and why are we here?

Jeremy Haggard

Manager Platform Systems

Genesco, Inc.

Nashville Splunk User Group Leader

Husband to my wife Misty and Dad to my daughter Allison.

Michael Nobles

Senior Sales Engineer

Splunk (based out of Atlanta)

Happily married to my wife Janelle for 26 years.

Four kids, two grown and married, two still at home.

splunk> .conf2017

You will learn..

…new exploration techniques for various areas within your machine data.

Todays Agenda

Forensics
Domain Admins

App Monitoring
Point of Sale

Splunk Apps
Free and Custom

Q & A

splunk> .conf2017

Join the Pony Poll, win some schwag!

ponypoll.com/Genesco

splunk> .conf2017

Who is Genesco?

We are an international, retail company based in Nashville TN

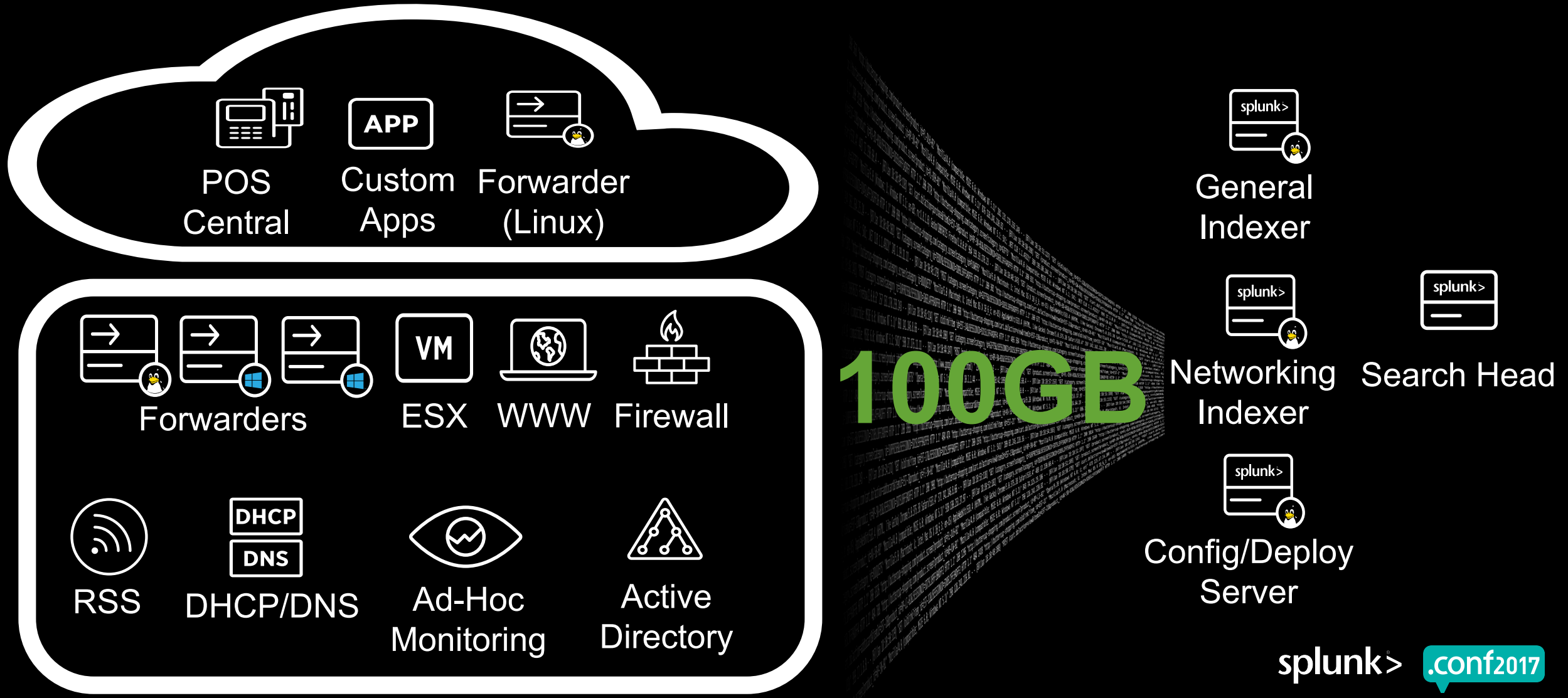
Splunk Environment

What does Splunk machinery look like at Genesco?

splunk> .conf2017

Data Flows and Splunk Architecture

High-level Environment Overview



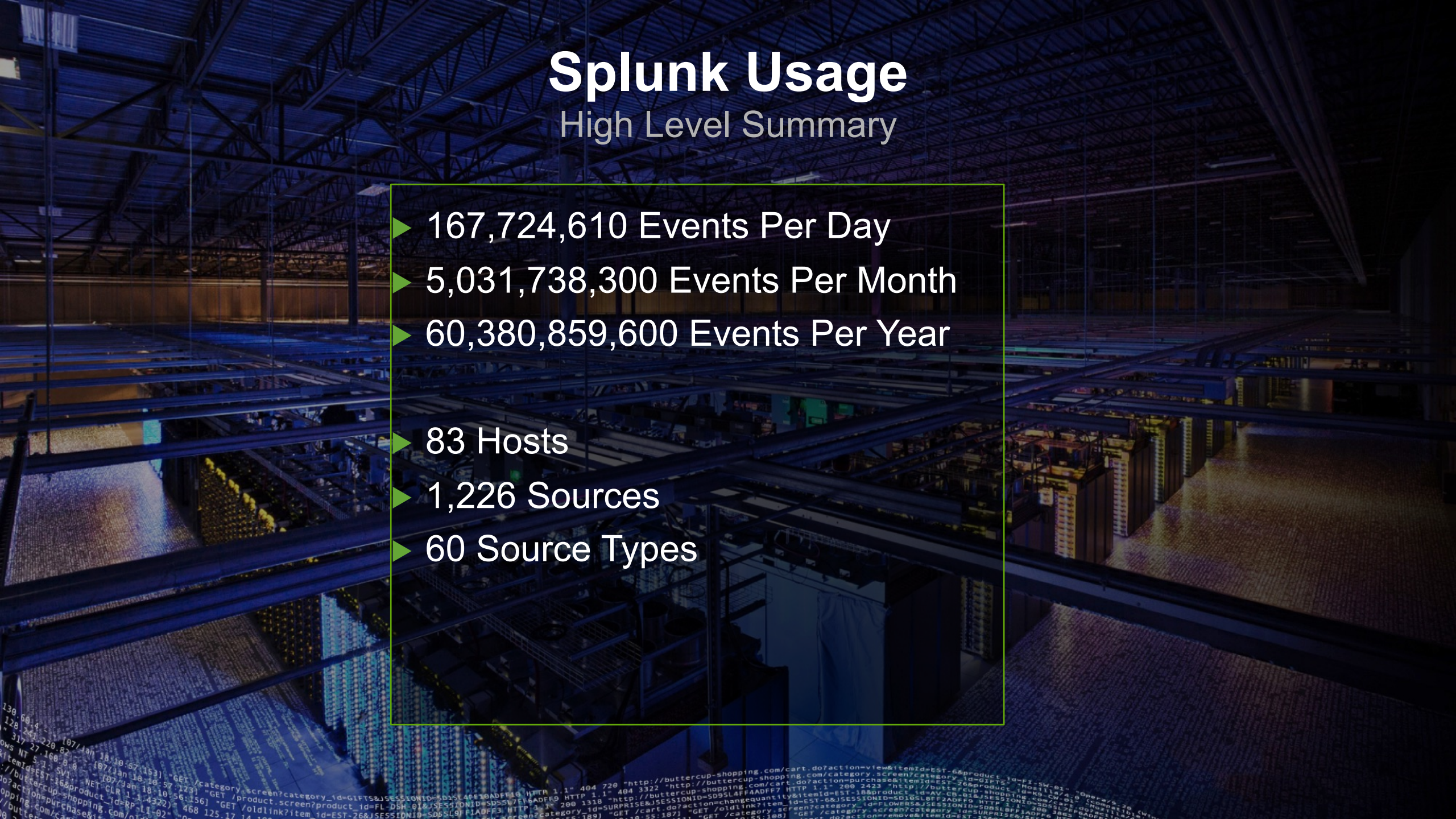
splunk> .conf2017

Splunk Usage

High Level Summary

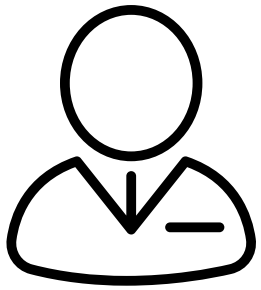
- 167,724,610 Events Per Day
- 5,031,738,300 Events Per Month
- 60,380,859,600 Events Per Year

- 83 Hosts
- 1,226 Sources
- 60 Source Types

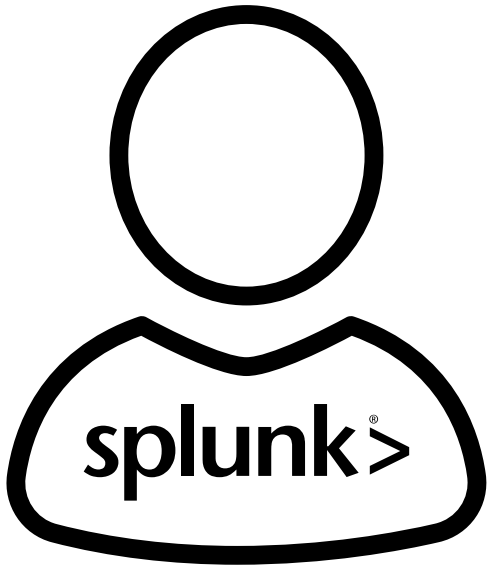


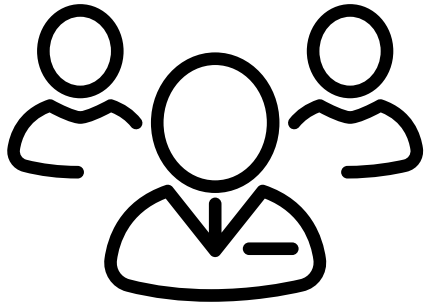
Splunk Team @ Genesco

You don’t need a full time Splunk team to get a ROI

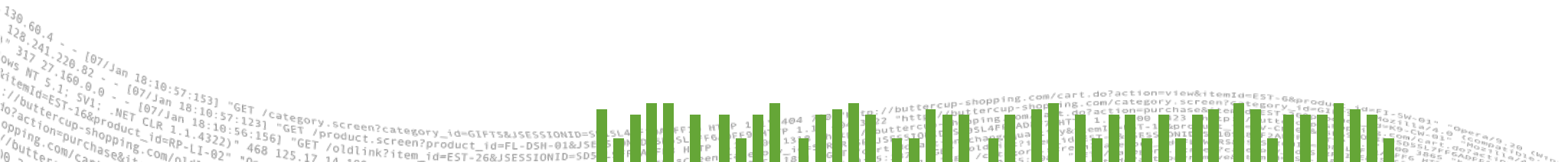


Tools & Automation Administrator





Splunk Userbase



splunk> .conf2017

Genesco's Journey

Forensics, POS (point of sale) and Useful Apps

splunk> .conf2017

FORENSICS

WHO / WHAT / WHERE / WHEN

Monitoring Active Directory

Where's Waldo… And what's he doing?

- The Problem:
  - We had a legacy account enabled on our network.
    - It was used for an old application service years ago, but was never disabled.
    - Last activity time on account was < 2 weeks.
    - Active timestamp would update approx every 2 weeks.
    - No leads when looking at Palo Alto logging.
- The question:
  - What would break if we just disabled this old account?
  - What services/applications were hardcoded to use it that we didn't know?

Splunk Trials – Value in 15 Days

Knowing WHERE to look was the key Splunk provided.

Research started

May 4, 2016
Manual Process for 5 days.

Splunk Trial Installed

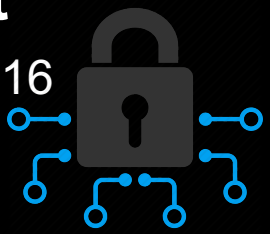
May 9, 2016
Data Ingest Started on Domain Controllers

Splunk Alerts Triggered – Event Analyzed

May 16, 2016 – May 23, 2016
Real-Time searches prove value.
Index=UserActivity “username”

All Clear to disable the account

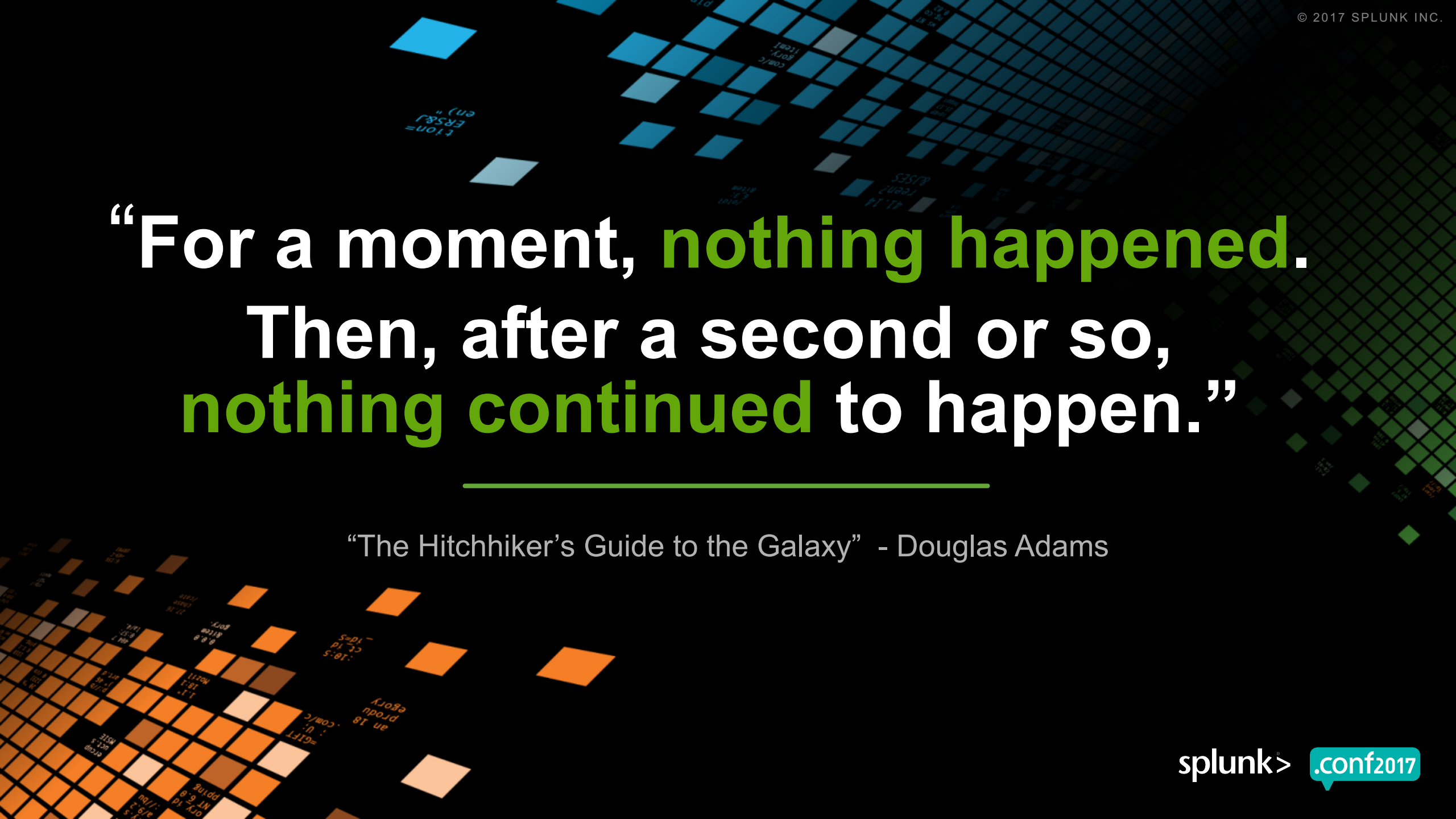
May 25, 2016



Last remnants removed

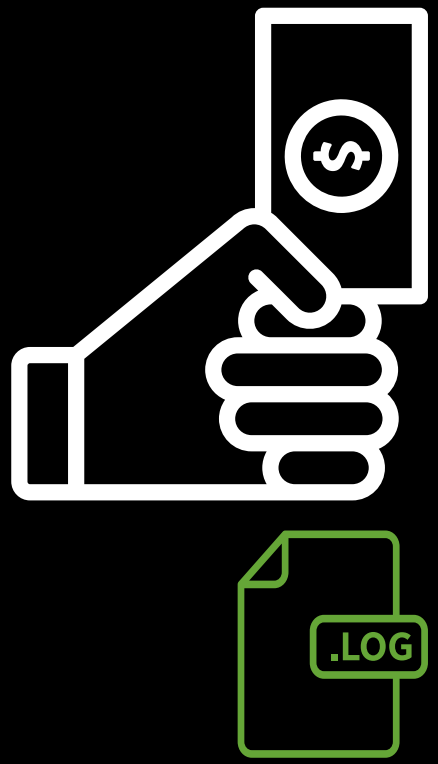
May 24, 2016

splunk> .conf2017



“For a moment, nothing happened. Then, after a second or so, nothing continued to happen.”

“The Hitchhiker’s Guide to the Galaxy” - Douglas Adams



APP MONITORING

POINT OF SALE

“Big things have small beginnings.”

T.E. Lawrence (Lawrence of Arabia) / Michael Fassbender (Prometheus)

splunk> .conf2017

We have many thousands of errors in the logs in dev. Someone needs to look at all of these.
Inside the file “errors.tgz” is where I was just pulling out the word “ERROR” from the logs and ended up getting 63,356 lines worth of data.
The errors themselves are in the log files and need immediate attention.
There is no way to know what is working and what is not with this many errors.

Challenge Accepted

Still growing, now at **133,247 lines of errors**…
I think Joe should be looking at this instead of scanner upgrades.

Still many errors out there getting generated... Logs attached.

I got this.

What the machine data looks like

central.log

2017-08-08 16:27:25,250 ERROR [ReplicationResequencingPublisher_6::0{549}..<1234] [FAILED_PERSISTENCE_LOG] Persistence Failed: dtv.data2.access.exception.PrimaryKeyViolationException: java.sql.SQLIntegrityConstraintViolationException: ORA-00001: unique constraint (DTV.PK_INV_INVCTL_TRANS_DETAIL) violated Caused by --> java.sql.SQLException: ORA-00001: uniq TV.PK_INV_INVCTL_TRANS_DETAIL) violated 2017-08-08 16:27:28,414 ERROR [ReplicationResequencingPublisher_6::0{549}..<1234] [dtv.data2.access.pm.PersistenceManager] Primary Key Violation while persisting object: [dtv.xst.dao.inv.impl.InventoryDocumentDAO@9df1254Object Id: [98765432::SHIPPING::6::5555} DaoState: [UPDATE] Id: 98765432::SHIPPING::6::1234 Values: documentId=5851452 documentTypeCode=SHIPPING organizationId=6 retailLocationI eateDate=2017-08-07 17:58:00.545 createUserId=0 updateDate=2017-08-08 16:32:54.139 updateUserId=989898 createDateTime=2017-08-07 00:00:00.0 originatorId=4444 statusCode=CLOSED documentSubtypeCode=FOUND originatorName=DIVISION NAME lastActivityDate=2017-08-08 12:32:54.139 recordCreationType=HOME_OFFICE originatorAddressId=999999999999 , dtv.xst.dao.inv.impl.InventoryDocumentL AO@5851452Object Id: [642465842::SHIPPING::1::6::5555} DaoState: [UPDATE] Id: 989898::SHIPPING::104::6::5555 Values: documentId=647852 documentTypeCode=SHIPPING inventoryDocumentLineNumber=1 organizationId=6 retailLocationId=5555 createDate=2017-08-07 17:58:00.548 createUserId=0 updateDate=2017-08-08 16:32:54.139 updateUserId=222333 inventoryItemId=9879871 lineItemTypeCode=ITEM statusCode=OPEN unitCount=0 unitCost=21 expectedCount=1 postedCount=0 postedCost=0 recordCreationType=STORE controlNumber=0 , dtv.xst.dao.inv.i entLineItemDAO@af12345Object Id: [6::5555::646652484::SHIPPING eState: [UPDATE] Id: 6::5555::99988887::SHIPPING::1::1 Values: organizationId=6 retailLocationId=5555 documentId=55559999 documentTypeCode=SHIPPING shipmentS 1 lineItemSequence=1 createDate=201 createUserId=0 updateDate=2017-08-08 16:32:54.139 updateUserId=989898 inventoryDocumentLineNumber=1 shipQuantity=0 , dtv.xst.dao.inv.impl.InventoryTransactionDetailDAO@9999999cObject Id: [6::5555::1502150400000::2::4184::1} DaoState: [INSERT] Id: 6::5555::987987900000 1 Values: organizationId=6 retailLocationId=5555 businessDate=2017-08-08 00:00:00.0 workstationId=1 transactionSequence=6543

Publisher

Publisher

Store #

User

Store #

Store #

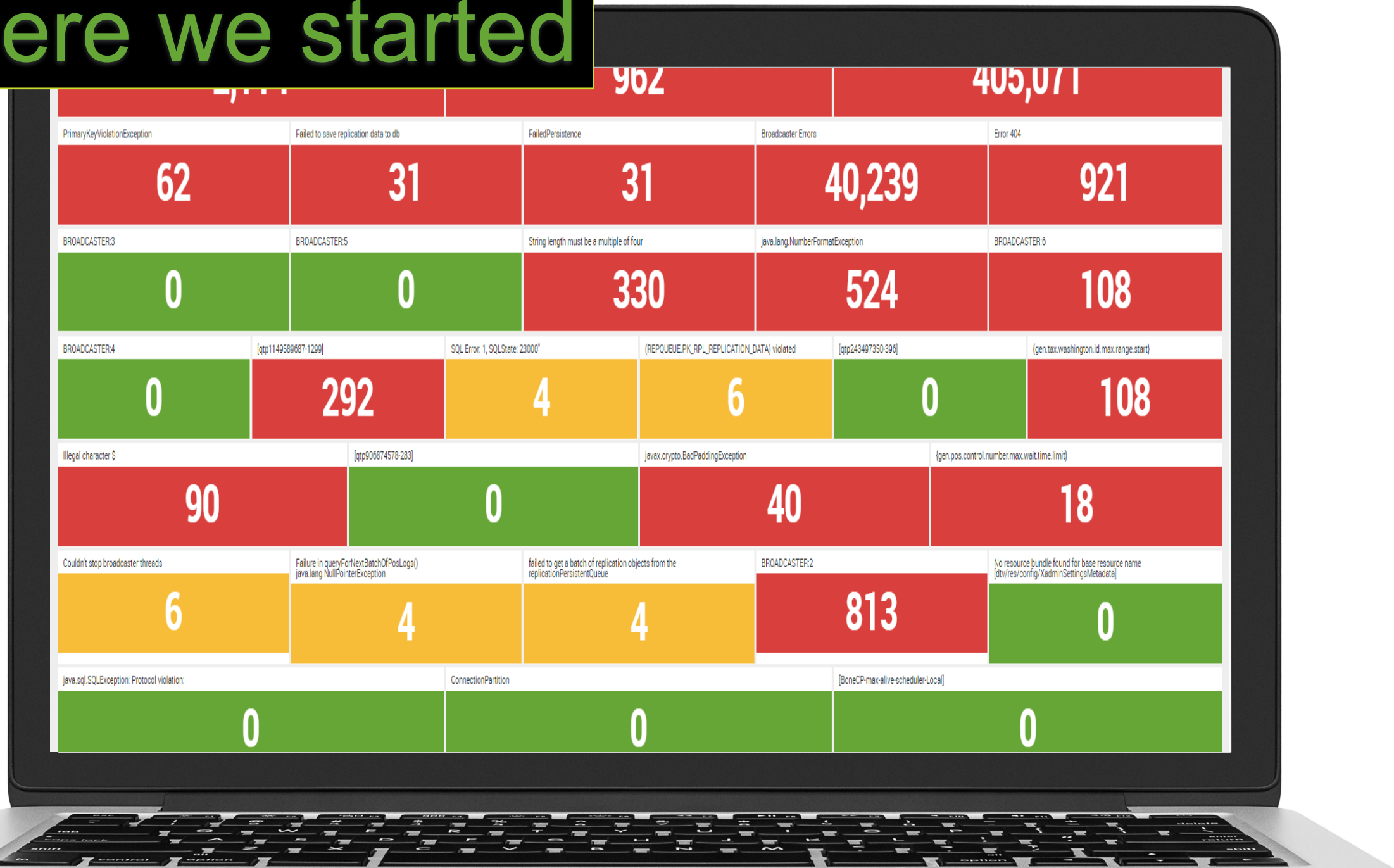
Store #

User

Store #

splunk> .conf2017

Where we started



Where we ended

Building the Dashboard

1. Identify the specific error you want to find
   - look at raw logs, events or Splunk statistics tab.
2. Build the SPL for that error
   - Index=AWSPROD “ERROR” “primarykeyexception”
3. Save the result as a dashboard widget.
4. Repeat.

Tip!

Easily move through your events by adding exclusions.

Build your SPL and each time you make a new widget add the error to a master SPL to help you drill down to quickly get through every error.

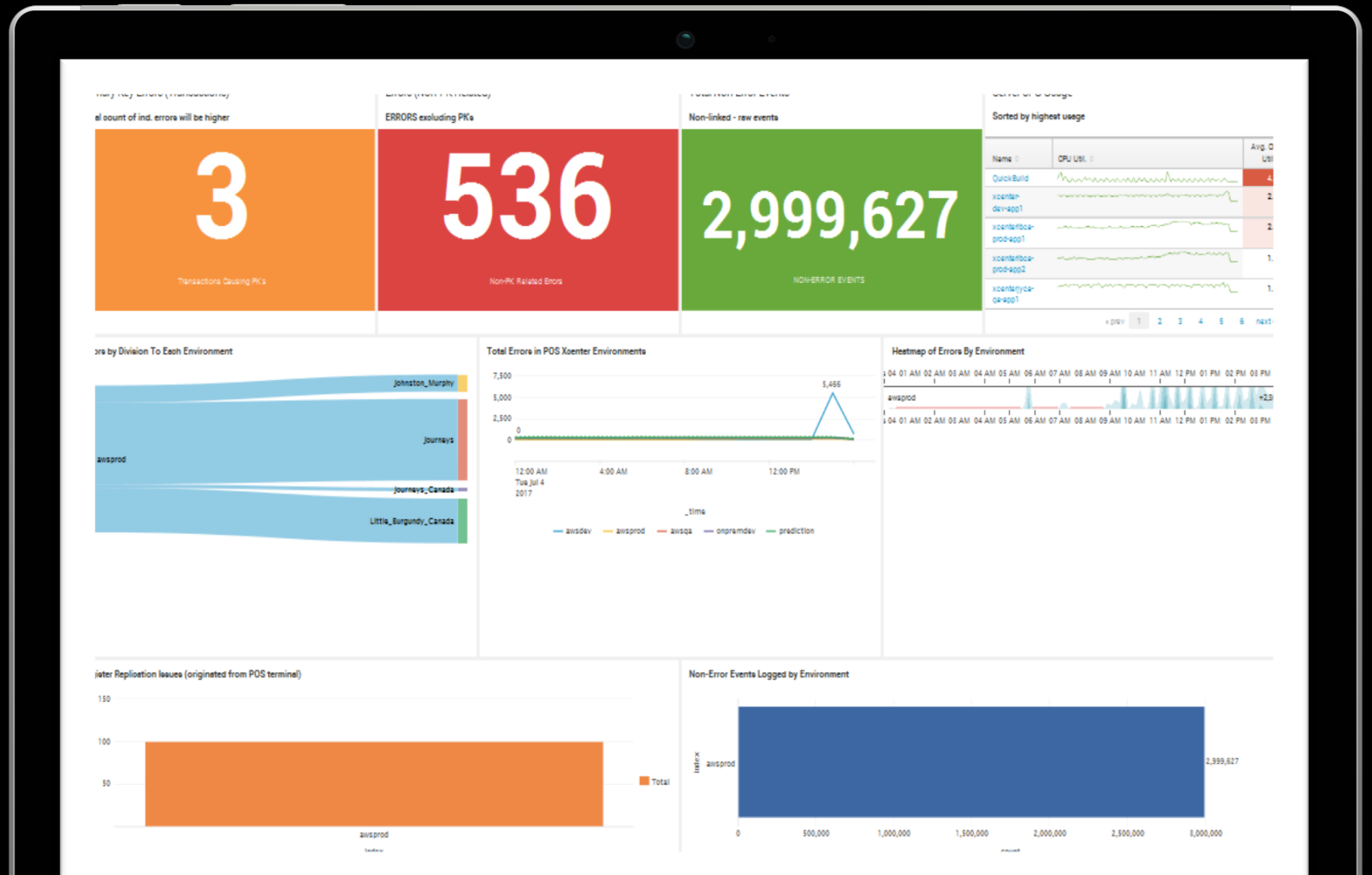
Example:

index=AWSPROD "ERROR"

- NOT "The server sent HTTP status code 404“
- NOT "Failed to save replication data to db"
- NOT "FailedPersistence"
- NOT "PrimaryKeyViolationException"
- NOT "{gen.tax.washington.id"
- NOT "${gen.pos.control.number.max.wait.time.limit}"
- NOT "[qtp243497350-396]"
- NOT "String length must be a multiple of four"
- NOT "(REPQUEUE.PK_RPL_REPLICATION_DATA) violated“
- Etc……

Pinpointing Error Origination

"This always happens" – Every end user ever



- TRUTHS:
  - Sometimes we don't get the whole truth.
  - Emotions get in the way when going across teams/depts.
  - With data in hand
    - Quickly gets you to the issue.
    - Allows you to focus on the problem and not the perception.
    - It's hard to argue FACTUAL DATA.

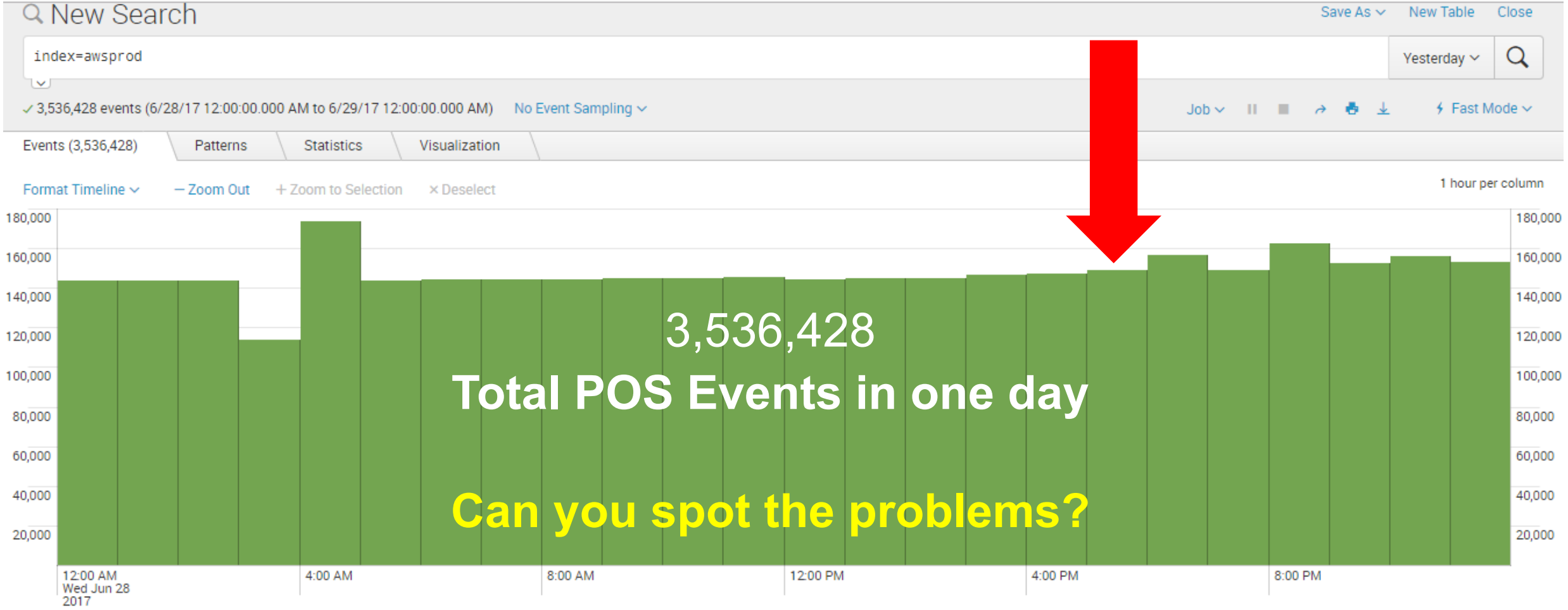
splunk> .conf2017

“The system never works.”

An example scenario

POS Server Data Captured

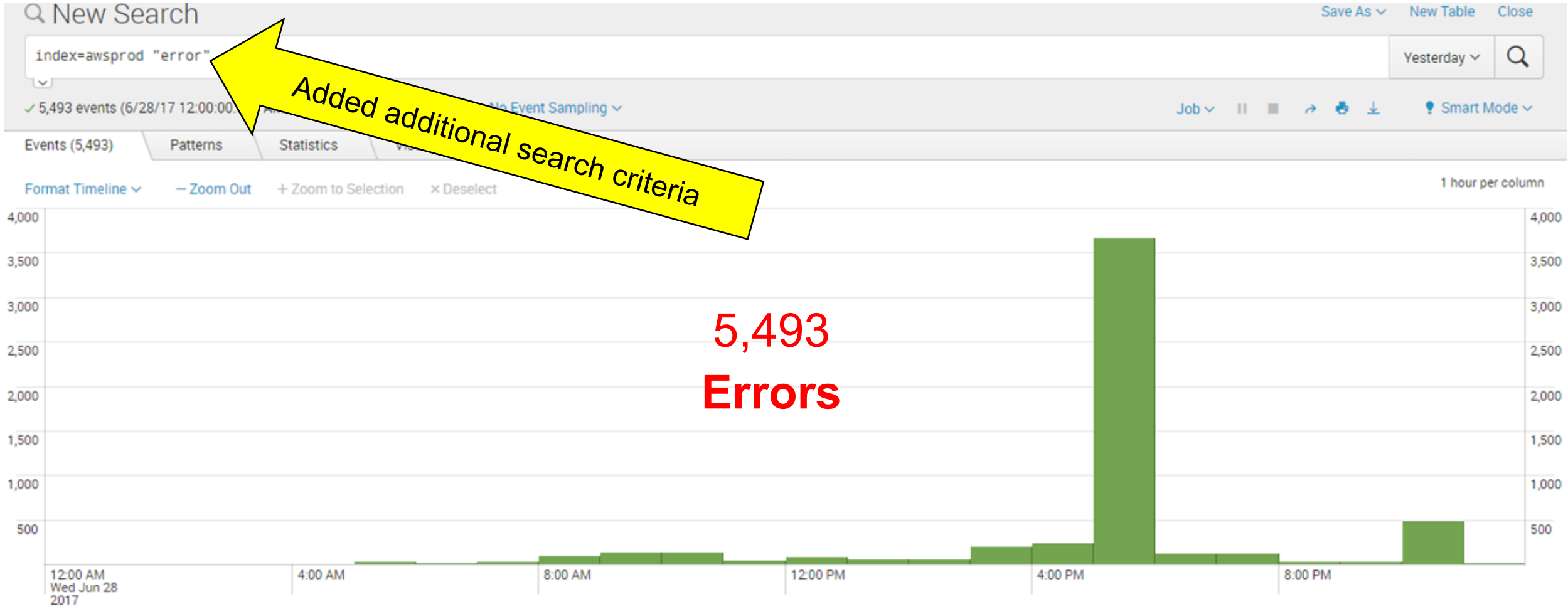
Straight from application log files.



splunk> .conf2017

POS Server Data Captured

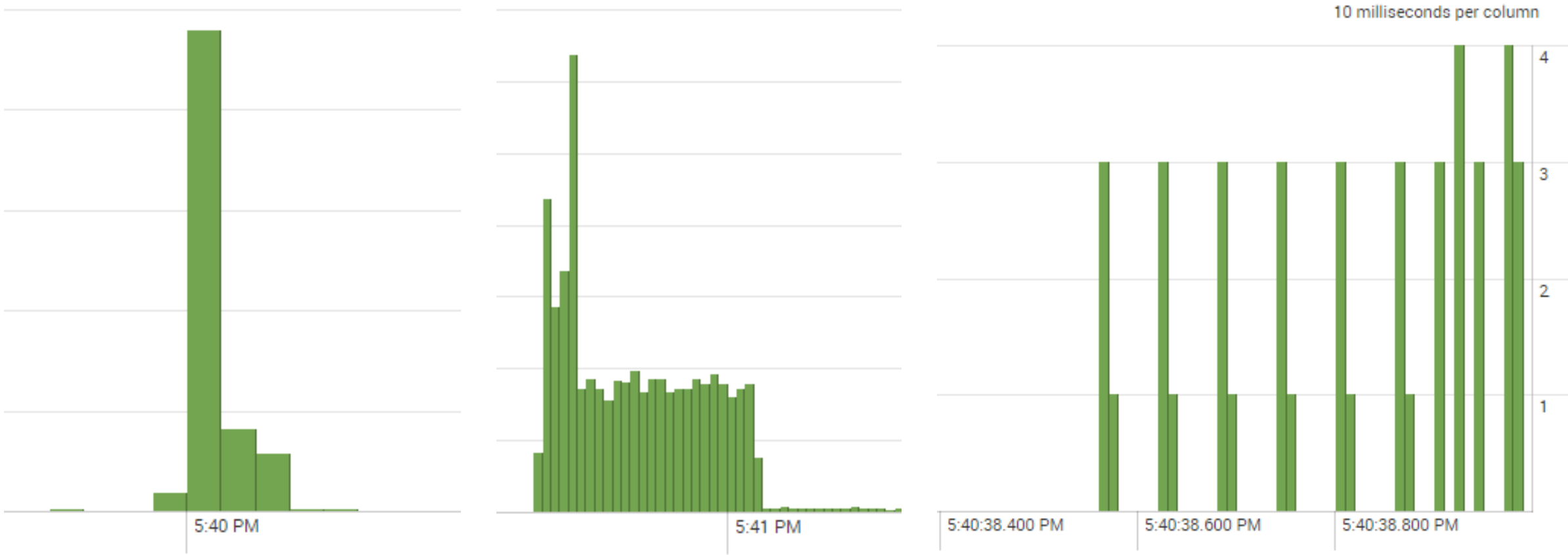
The timeline tells a story and reduces time to resolve



splunk> .conf2017

POS Server Data Captured

Drill down further to capture the minute and second in time this started.



“Factual data is actionable data.”

splunk> .conf2017

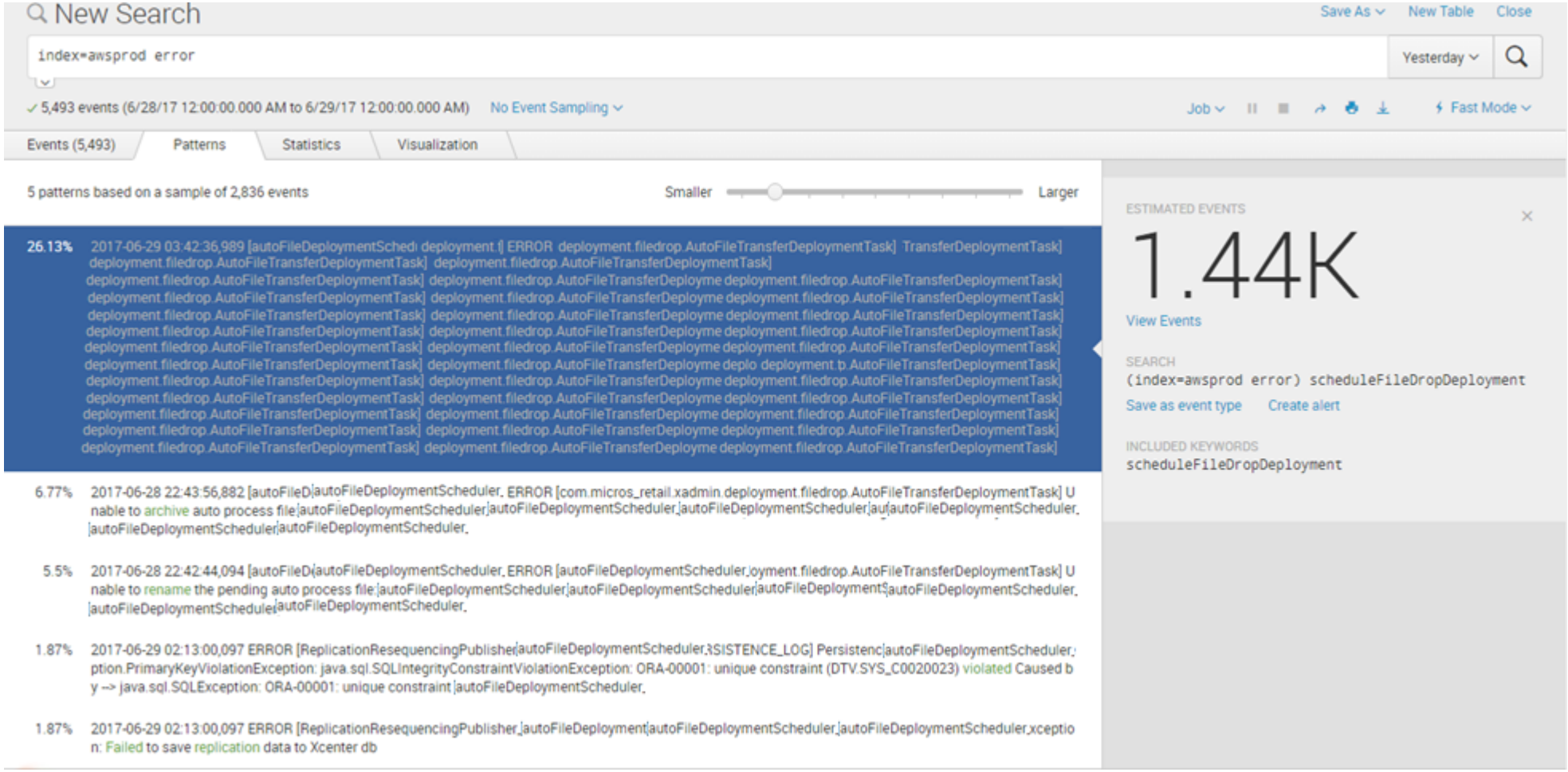
POS Server Data Captured

Easily pin-point the source of the errors

26%

< 13%

< 4%

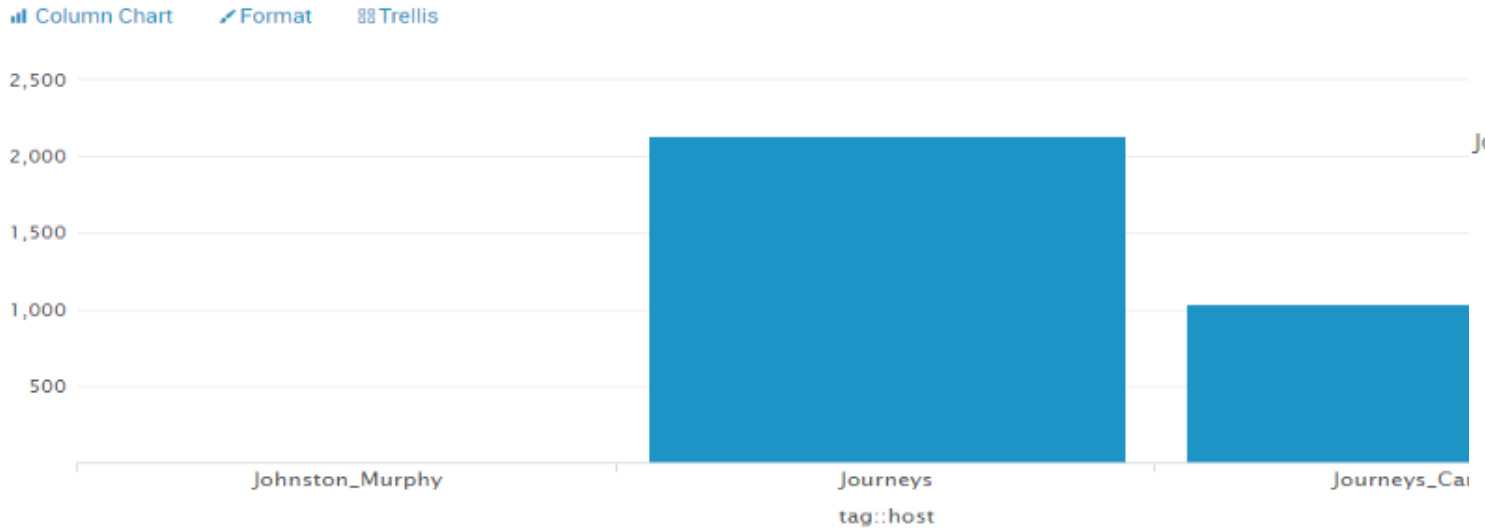


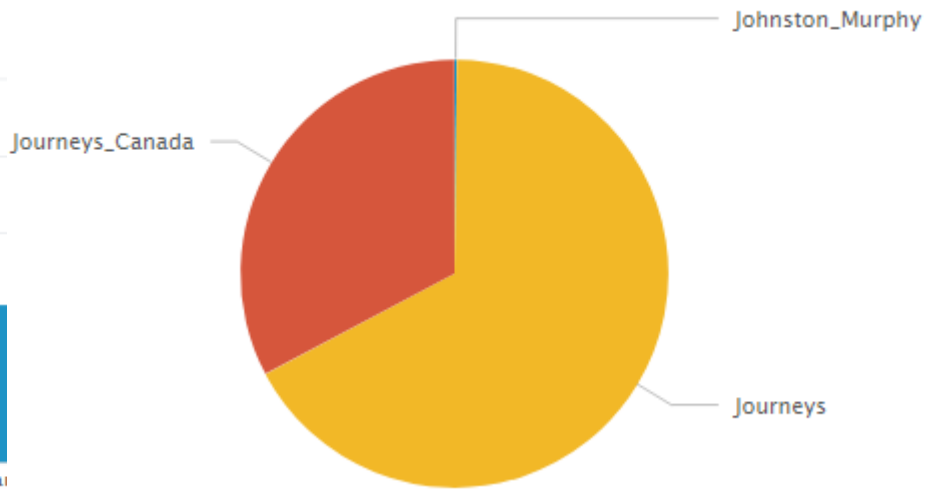
splunk> .conf2017

POS Server Data Captured

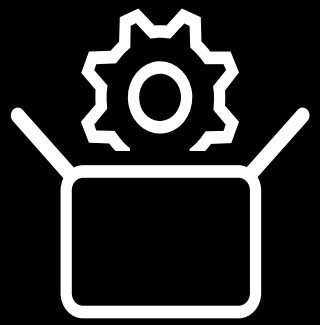
And see who is impacted using a number of views

Example SPL: index=awsprod error| stats count by tag::host





splunk> .conf2017



APPS

SPLUNKBASE & CUSTOM

Splunkbase Apps = Time Saver

Secret sauce to a fast ROI

SplunkBase:

- Splunk App for AWS
- NMON Performance by Octamis
- Splunk App for Windows Infrastructure
- Website Monitoring
- Template for Citrix XenApp
- Template for Citrix XenDesktop 7
- Palo Alto
- Detailed License Monitoring and Alerting for Splunk

Tip!

Be sure to research best practices

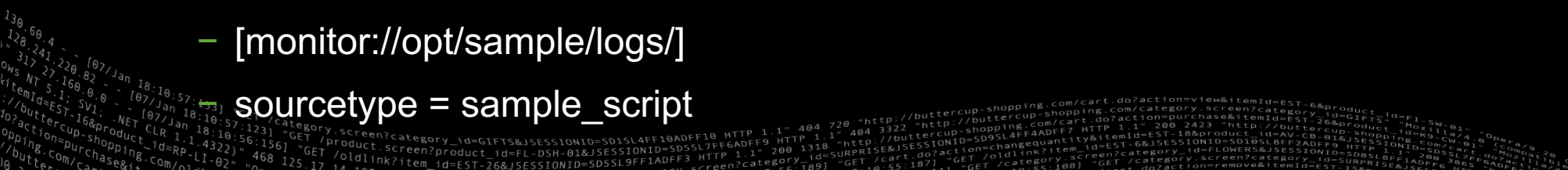
1. Setup and maintain a “sandbox”/Splunk Development area (obtain your own free, 50 GB/day Personal Developer license)
2. Feel free to run Splunk on your own machine to quickly explore new data and new Apps from the Splunkbase app ”store”
3. Sign up for Splunk “Answers” and become part of the community
4. Google is your friend
5. Run Splunk (free version) at home to get even more value and more comfort

Custom Apps

Easier than you think to get your data.

We currently use 10 custom apps to monitor our POS environment.

- These custom apps mostly run scripts on our linux environment to pull specific data.
  - count of files, file permissions, md5sum, etc…
- App/bin directory
  - sample_script.sh
- App/local directory
  - Inputs.conf
    - [script://opt/splunkforwarder/etc/apps/sample_scripts/bin/sample_script.sh]
    - interval = 900
    - [monitor://opt/sample/logs/]
    - sourcetype = sample_script



splunk> .conf2017

Summary

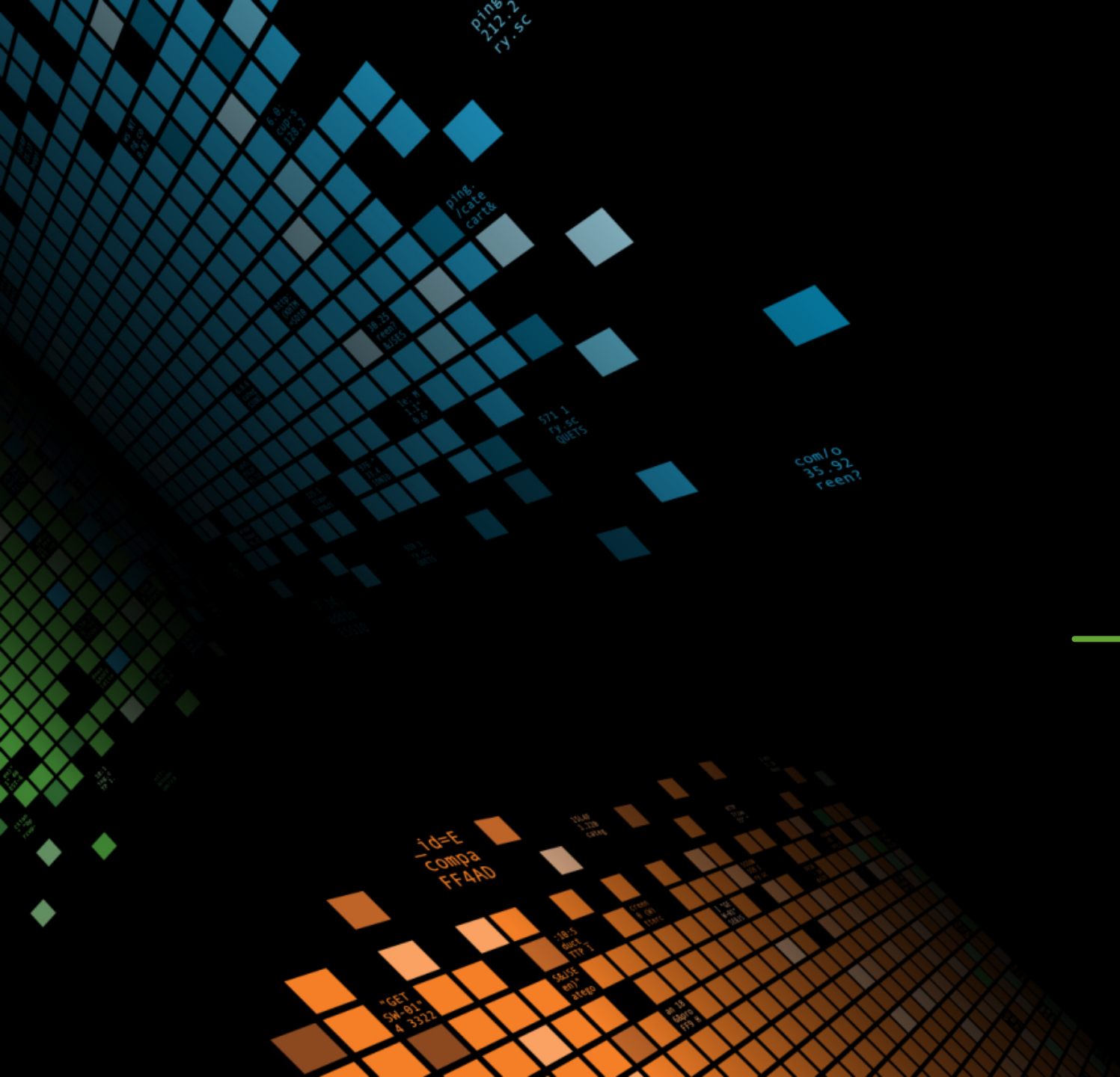
Forensics
Domain Admins

App Monitoring
Point of Sale

Splunk Apps
Free and Custom

Q & A

splunk> .conf2017



Q&A

Jeremy Haggard | Genesco
Mike Nobles | Splunk

splunk> .conf2017

Explore

Explore your data without fear of the great unknown!

splunk> .conf2017

Thank You

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

Jeremy@SplunkNashville.com

splunk> .conf2017