



**splunk®**

# Solve Fundamental IT Issues by Leveraging Your Network Tools' Data Using Splunk

Christopher Jonnes | NetCentrics  
Jonathan Fair | DIOS Tech

Jonathan Fair | BIOS Tech

October 4, 2018 | Orlando, FL

# 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, Splunk>, Listen to Your Data, 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. © 2018 Splunk Inc. All rights reserved.

# Introduction

## Solve Fundamental IT Issues by Leveraging Your Network Tools' Data Using Splunk



**Christopher Jonnes - NetCentrics**

- ▶ Started on Service Desk worked way up
- ▶ 10 Years + IT experience
- ▶ 2+ Years Splunk experience
- ▶ Splunk Admin, Sec +, ITIL, MSTA

Avid fantasy baseball player



**Jonathan Fair - DIOS Tech**

- ▶ 5 Years in the Marines, Incident Response, Security Engineering, Operational Engineering
- ▶ 12+ Years IT experience,
- ▶ 4+ Years Splunk experience
- ▶ Splunk Architect, CISSP, ITIL, CEH

Drives a Tesla and an avid Gamer

# Overview

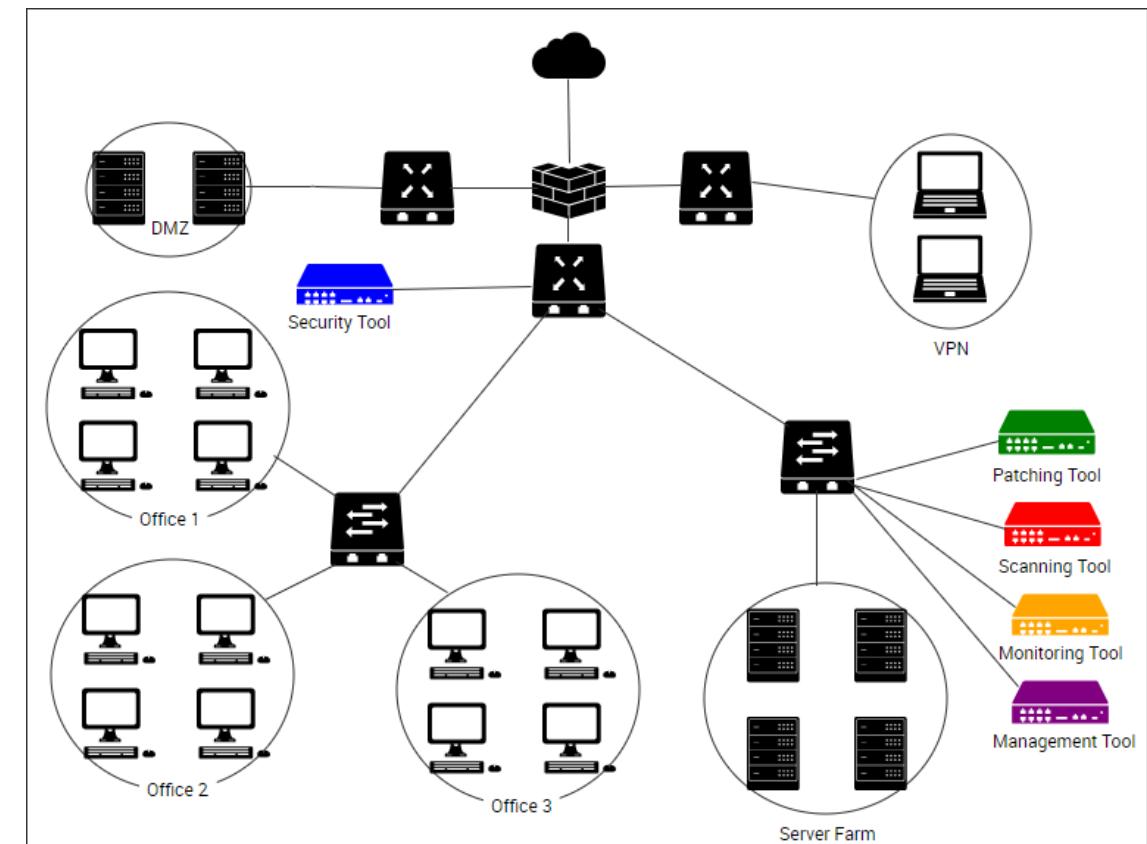
## Solve Fundamental IT Issues by Leveraging Your Network Tools' Data Using Splunk

- ▶ Problems of managing your IT infrastructure today
    - What if you could see a holistic and accurate view of the assets on your network?
  - ▶ Solution: Asset Data Hub
    - Sample dashboards
  - ▶ Process flow of how it was built
    - i.e. Splunk searches along with methodology

# Fundamental Network Issues

## **So many tools, so little time**

- ▶ Managing multiple Tools
  - ▶ Utilizing your Tools Efficiently and Effectively
  - ▶ Tracking devices on your network
  - ▶ What coverage gaps do you have?
  - ▶ How do you determine what your tools don't see?

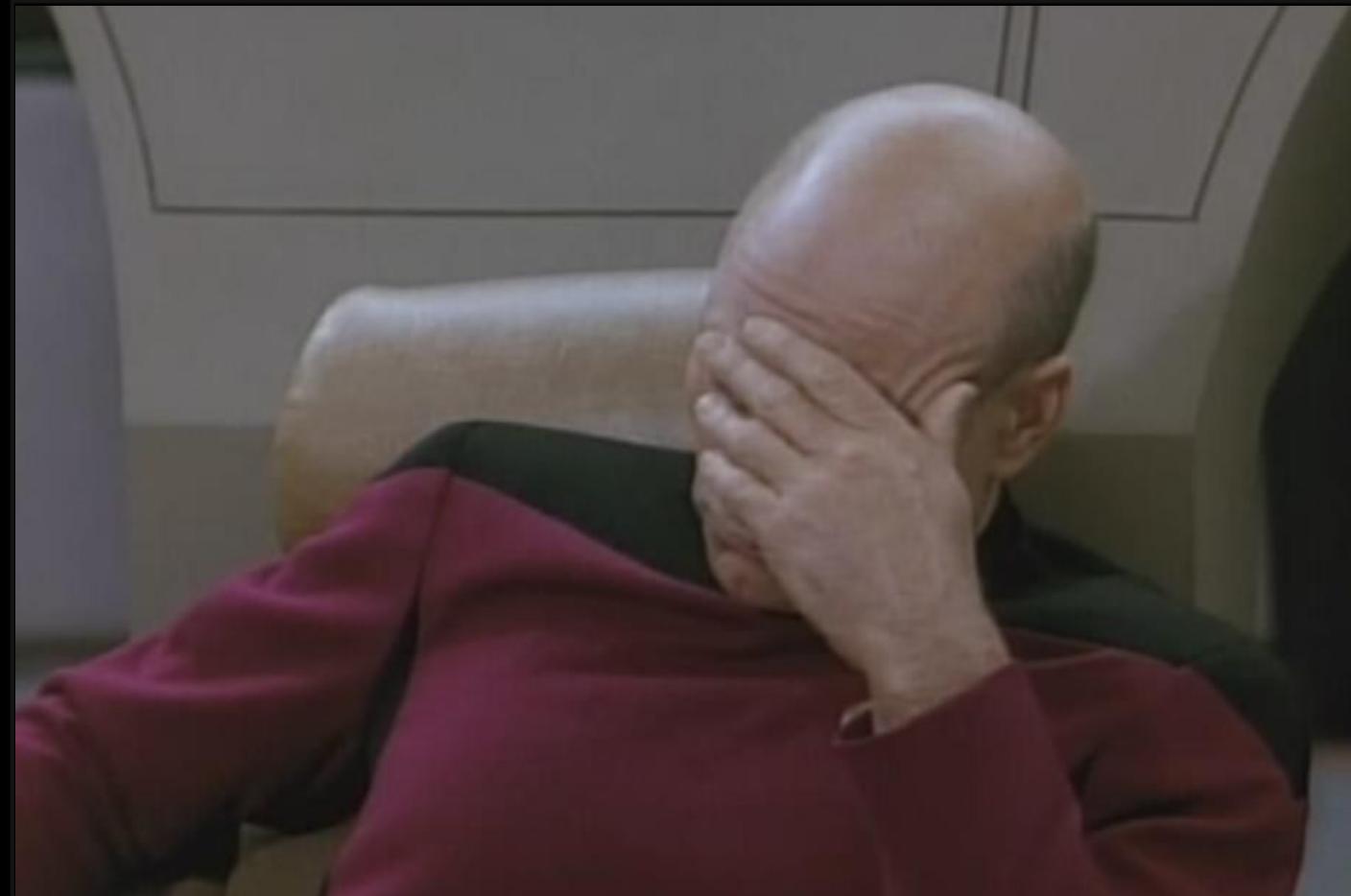


# How do you know what you don't know?

# Tool Coverage and Network Visibility

Tell me about my network, Bob

Scanning Management Coverage



- ▶ Different tools see the world differently
- ▶ Agents vs Agentless
- ▶ Proper configuration can be difficult to determine

# Other Challenges

# Why can't this just be easier!

- ▶ Many moving parts
  - ▶ Inefficient Communication
  - ▶ Miscommunication
  - ▶ Causing wasted resources, wasted time and wasted money.
  - ▶ Problem exists EVERYWHERE!

## So, how do we fix this??

# Don't Worry We Got You!



# Asset Data Hub

Data Hub General Info Subnet Lookups Tools User Info Patching Custom Dashboards Custom Reports Search Knowledge Objects Asset Data Hub

Data Hub Current Data Sources: Discover | Management | Monitoring | Patching | Scanning | Security | Splunk Edit Export ...

Data Hub - Single consolidated Location, aggregating and correlating data from multiple sources. Allowing countless dashboards, reports, searches and statistical answers across our environment.

### Discovery Of Assets

All Time

System Type	Count
Discovery Systems	84
Management Systems	48
Monitoring Systems	52
Patching Systems	51
Scanning Systems	59
Security Systems	52
Splunk	56

Count Systems

### Agent Based tool count within 10 days.

Tool	Count
Management	24
Monitoring	36
Patching	26
Security	10
Splunk	42

Total Systems

### Agent Based System Count by Tool Overlap

#### Security Patching Monitoring Management Splunk

# of Tools	# of Systems
1	4
2	4
3	12
4	23
5	13

# of Systems

# of Tools

### Count by Device Type within 10 days

Device Type	Count
Printers	8
Servers	12
Workstations	35

Total Systems

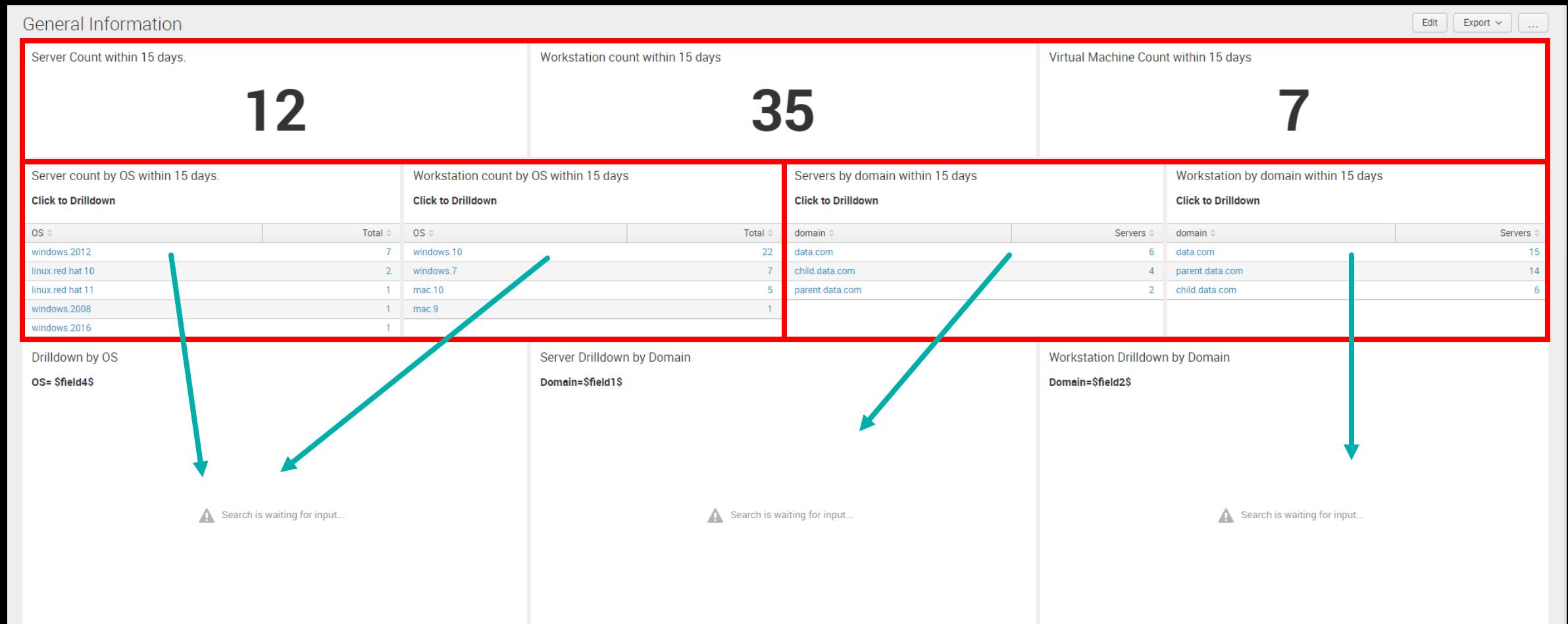
### Server Count by Type in 10 days

Server Type	Count
Red Hat 10	2
Red Hat 11	1
Windows 2008	1
Windows 2012	7
Windows 2016	1

Total Systems

# Asset Data Hub

## General Information



# Asset Data Hub

## Lookup

**Host Lookup**

Partial Hostname      Exact Hostname

desktop       **Submit** **Hide Filters**

Partial Hostname Search		Host Seen in the last 30 Days	General Information	Additional Links	Discovered by Tool	Managed By Agents
<b>Click for Exact host info.</b>		<b>Host (desktop8)</b>	<b>Host (desktop8)</b>	<b>Info</b>	<b>Tool</b>	<b>Tool</b>
host	domain			ip mac domain os date	discovery monitoring management patching security splunk	monitoring management patching security splunk
desktop1	data.com			123.456.789.8 ab19 data.com windows.10	NO Yes Yes Yes Yes	Yes No No Yes Yes
desktop2	data.com					
desktop3	data.com					
desktop4	data.com					
desktop5	data.com					
desktop6	data.com					
desktop7	data.com					
desktop8	data.com					
desktop9	data.com					
desktop10	data.com					
« prev 1 2 3 4 next »						

**Tool Drilldown**

splunk	Info
splunk	1
splunk_cputcore	4
splunk_date	8/5/2018
splunk_ip	123.456.789.8
splunk_lastlogin	8/5/2018
splunk_mac	ab19
splunk_managed	Yes
splunk_os	windows 7
splunk_serial	asndk2342
splunk_subnet	123.456.789.0/24
splunk_uptime	27

**Additional Fields of information based on Host**

Additional Fields of information

Search is waiting for input...

# Asset Data Hub

# Tool Dashboards – All Data is Correlated

# Splunk Dashboard

All splunk Fields of interest

- splunk
- splunk\_cpucore
- splunk\_date
- splunk\_ip
- splunk\_lastlogin
- splunk\_mac
- splunk\_managed
- splunk\_os
- splunk\_serial
- splunk\_subnet
- splunk\_uptime
- splunk\_virtual

**Submit** [Hide Filters](#)

**Splunk Counts Within 30 days**

A horizontal bar chart titled "Splunk Counts Within 30 days". The y-axis is labeled "count" and ranges from 0 to 60. There are two bars: one for "managed" hosts with a count of 48, and one for "unmanaged" hosts with a count of 8. A legend indicates the blue color represents the "count".

Host Type	Count
managed	48
unmanaged	8

**Subnets Not seen in Splunk**

Subnets
111.222.333.0/25
111.222.333.0/26

**Hosts unmanaged by splunk**

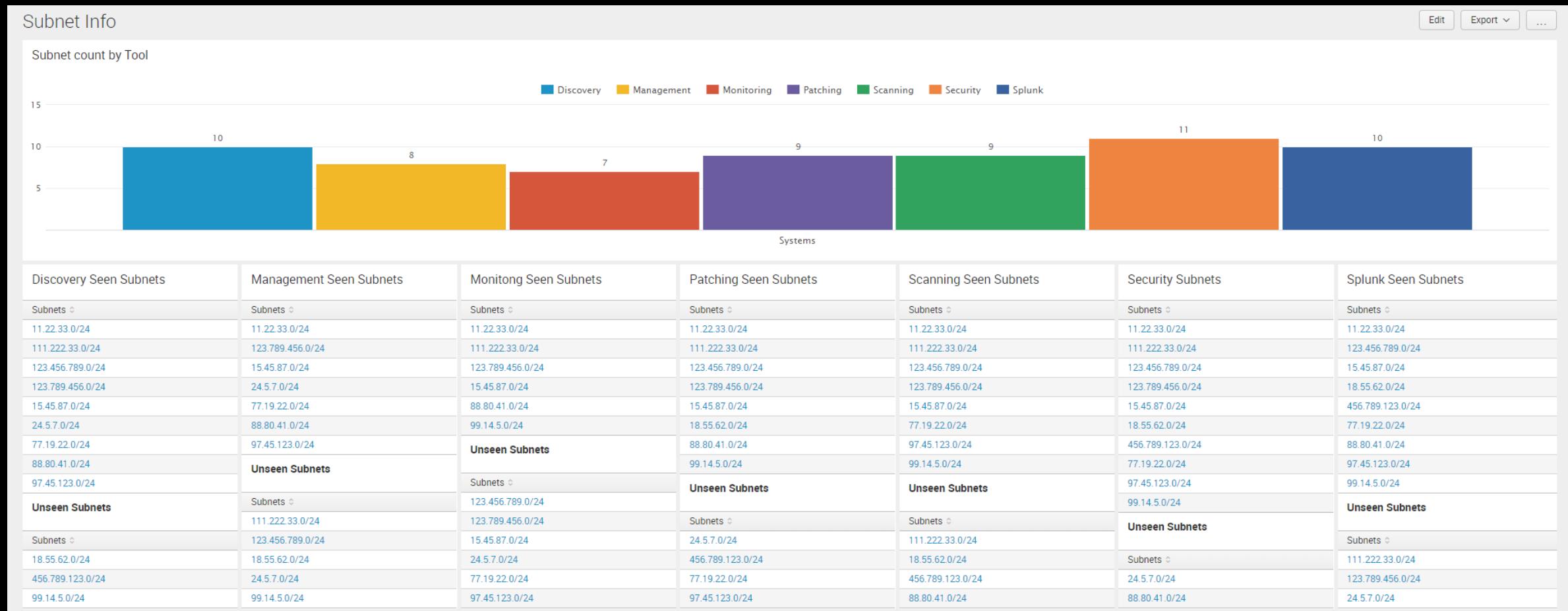
host	os	domain	splunk	splunk_date	splunk_ip	splunk_mac	splunk_os	splunk_subnet
desktop6	windows	data.com	0	08/05/2018	123.456.789.6	ab17	windows 7	123.456.789.0/24
desktop7	windows	data.com	0	08/05/2018	123.456.789.7	ab18	windows 7	123.456.789.0/24
desktop15	windows	data.com	0	08/05/2018	123.456.789.15	ab26	windows 10	123.456.789.0/24
desktop16	windows	parent.data.com	0	08/05/2018	123.456.789.16	ab27	windows 10	123.456.789.0/24
server4	windows	data.com	0	08/05/2018	987.654.321.4	dc281	windows 2012	987.654.321.0/24
server5	windows	data.com	0	08/05/2018	987.654.321.5	dc282	windows 2016	987.654.321.0/24

# Asset Data Hub

## Custom Reports / Dashboards

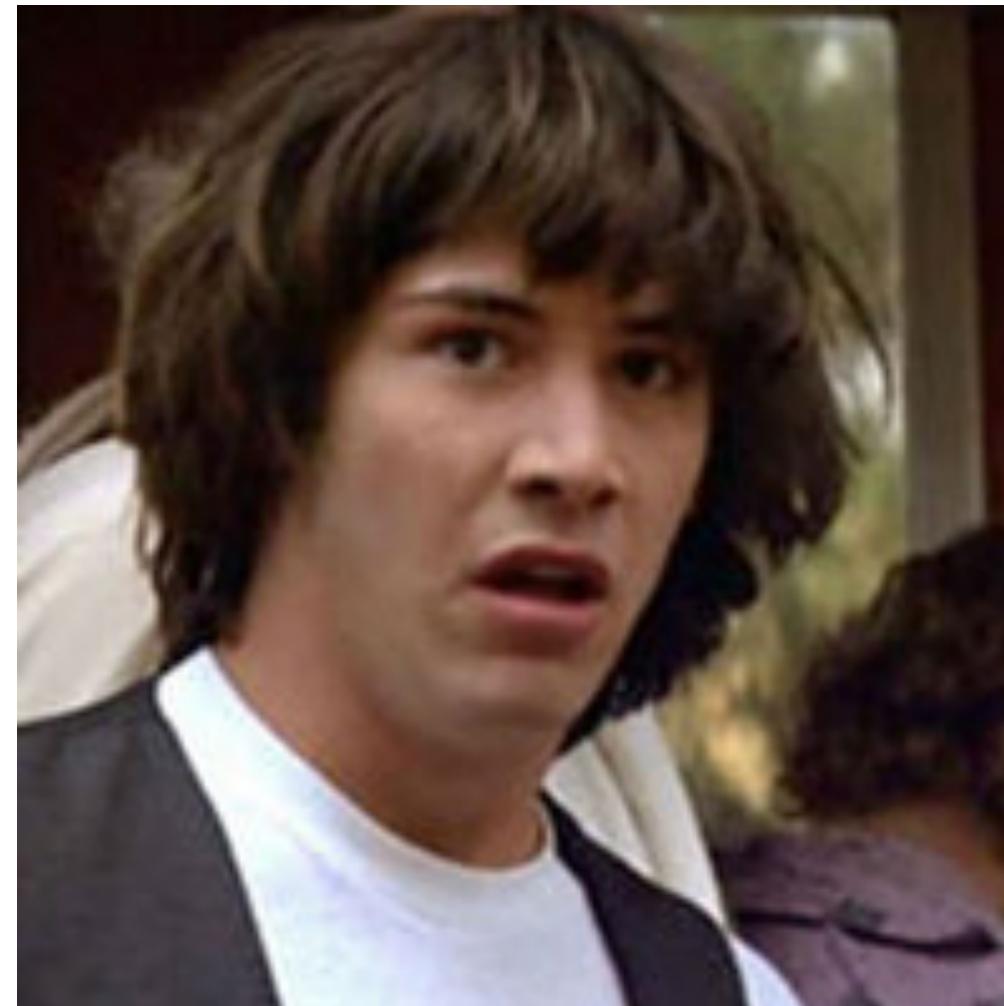
# Asset Data Hub

## Subnet Analysis



[{ "id": 1, "name": "Gifts", "parent\_id": null, "category\_id": 1, "order": 1, "image": "gifts.png", "description": "A collection of various gift items such as wrapped boxes, balloons, and decorative ornaments." }, { "id": 2, "name": "Clothing", "parent\_id": null, "category\_id": 2, "order": 2, "image": "clothing.png", "description": "A collection of clothing items including shirts, pants, dresses, and accessories." }, { "id": 3, "name": "Electronics", "parent\_id": null, "category\_id": 3, "order": 3, "image": "electronics.png", "description": "A collection of electronic devices and accessories like phones, tablets, and headphones." }, { "id": 4, "name": "Home Goods", "parent\_id": null, "category\_id": 4, "order": 4, "image": "home-goods.png", "description": "A collection of home goods including kitchenware, bedding, and decor." }, { "id": 5, "name": "Sports & Outdoors", "parent\_id": null, "category\_id": 5, "order": 5, "image": "sports-outdoors.png", "description": "A collection of sports equipment and outdoor gear for various activities." }, { "id": 6, "name": "Books & Media", "parent\_id": null, "category\_id": 6, "order": 6, "image": "books-media.png", "description": "A collection of books, movies, and other media items." }, { "id": 7, "name": "Pet Supplies", "parent\_id": null, "category\_id": 7, "order": 7, "image": "pet-supplies.png", "description": "A collection of pet supplies and accessories for pets like dogs and cats." }, { "id": 8, "name": "Personal Care", "parent\_id": null, "category\_id": 8, "order": 8, "image": "personal-care.png", "description": "A collection of personal care products like skincare, makeup, and hygiene items." }, { "id": 9, "name": "Groceries", "parent\_id": null, "category\_id": 9, "order": 9, "image": "groceries.png", "description": "A collection of grocery items including food, drink, and household supplies." }, { "id": 10, "name": "Tools & Hardware", "parent\_id": null, "category\_id": 10, "order": 10, "image": "tools-hardware.png", "description": "A collection of tools and hardware items for home improvement and maintenance." }, { "id": 11, "name": "Leisure & Hobbies", "parent\_id": null, "category\_id": 11, "order": 11, "image": "leisure-hobbies.png", "description": "A collection of leisure and hobby items like games, puzzles, and craft supplies." }, { "id": 12, "name": "Automotive", "parent\_id": null, "category\_id": 12, "order": 12, "image": "automotive.png", "description": "A collection of automotive parts and accessories for vehicles." }, { "id": 13, "name": "Furniture", "parent\_id": null, "category\_id": 13, "order": 13, "image": "furniture.png", "description": "A collection of furniture items including tables, chairs, and sofas." }, { "id": 14, "name": "Gadgets", "parent\_id": null, "category\_id": 14, "order": 14, "image": "gadgets.png", "description": "A collection of small electronic gadgets like smartwatches, portable speakers, and drones." }, { "id": 15, "name": "Pet Products", "parent\_id": null, "category\_id": 15, "order": 15, "image": "pet-products.png", "description": "A collection of pet products specifically designed for pets like birds and reptiles." }, { "id": 16, "name": "Sports Equipment", "parent\_id": null, "category\_id": 16, "order": 16, "image": "sports-equipment.png", "description": "A collection of sports equipment for specific sports like soccer, basketball, and tennis." }, { "id": 17, "name": "Pet Toys", "parent\_id": null, "category\_id": 17, "order": 17, "image": "pet-toys.png", "description": "A collection of toys and accessories for pets like dogs and cats." }, { "id": 18, "name": "Pet Health", "parent\_id": null, "category\_id": 18, "order": 18, "image": "pet-health.png", "description": "A collection of health and wellness products for pets." }, { "id": 19, "name": "Pet Training", "parent\_id": null, "category\_id": 19, "order": 19, "image": "pet-training.png", "description": "A collection of training products and accessories for pets." }, { "id": 20, "name": "Pet Grooming", "parent\_id": null, "category\_id": 20, "order": 20, "image": "pet-grooming.png", "description": "A collection of grooming products and accessories for pets." }, { "id": 21, "name": "Pet Safety", "parent\_id": null, "category\_id": 21, "order": 21, "image": "pet-safety.png", "description": "A collection of safety products for pets like collars and leashes." }, { "id": 22, "name": "Pet Accessories", "parent\_id": null, "category\_id": 22, "order": 22, "image": "pet-accessories.png", "description": "A collection of accessories for pets like beds and bowls." }, { "id": 23, "name": "Pet Supplies", "parent\_id": null, "category\_id": 23, "order": 23, "image": "pet-supplies.png", "description": "A collection of general pet supplies." }]

# We can use Splunk for all of this?



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD55L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=GIFT-5W-01" "Opera/9.20 (Windows NT 5.1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?category\_id=FL-DSH-01&JSESSIONID=SD55L7FFGADFF9 HTTP 1.1" 404 332 "http://buttercup-shopping.com/cart.do?action=purchase&item\_id=EST-26&product\_id=AV-CB-01" "Mozilla/5.0 (Windows NT 5.1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&item\_id=EST-26&product\_id=AV-CB-01" "Mozilla/5.0 (Windows NT 5.1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:55:187] "GET /cart.do?action=changequantity&item\_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=changequantity&item\_id=EST-26&product\_id=AV-CB-01" "Mozilla/5.0 (Windows NT 5.1; .NET CLR 1.1.4322)" 128.241.220.82 - - [07/Jan 18:10:55:189] "GET /cart.do?action=remove&itemId=EST-11&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-11&JSESSIONID=SD55L9FF1ADFF3" "Opera/9.20 (Windows NT 5.1; .NET CLR 1.1.4322)"

# How Is This Done?

# Steps to success

- ▶ Gather raw data from relevant sources  
(Get data into Splunk)
  - ▶ Determine important and relevant fields and features that each tool can provide
  - ▶ Correlate and normalize the data
  - ▶ Summarize the information for ease of understanding and use
  - ▶ Create a endles and scalable solution

# Let's look at an example!

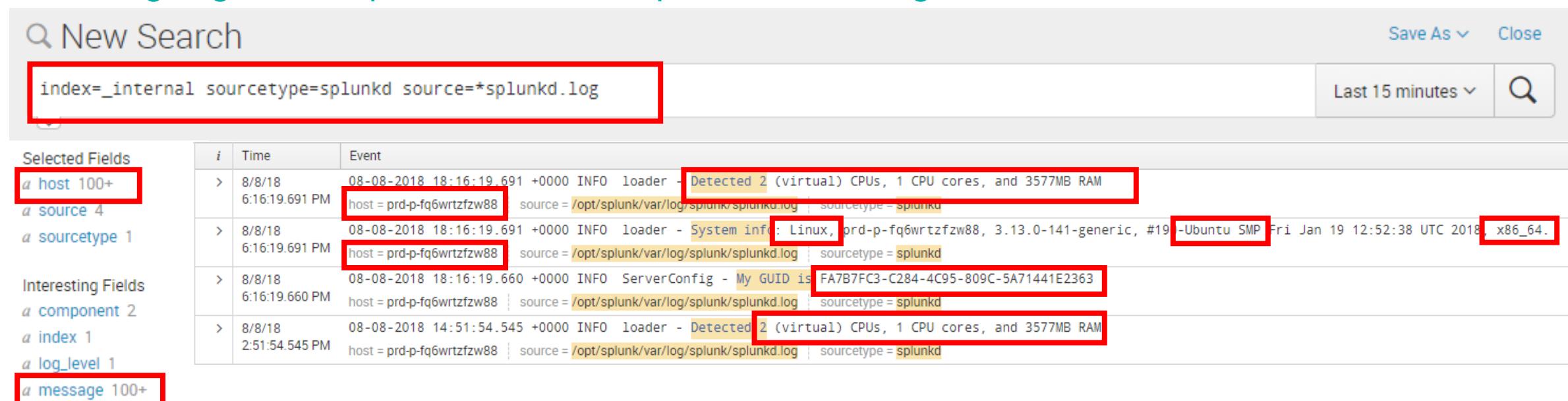


# Gather Raw Data

Leverage any indexed data to populate our Dataset

- ▶ Get indexed data for each tool / data source in your environment
  - Patching, monitoring, security, management, scanning, discovery tools
  - Includes non-obvious sources such as DHCP and Windows Security Logs

We are going to use Splunk as our example to walk through

A screenshot of the Splunk search interface. The search bar contains the query: "index=\_internal sourcetype=splunkd source=\*splunkd.log". The results table shows four log entries. The first entry is highlighted with a red box around the entire row. The second entry is also highlighted with a red box around the entire row. The third entry is highlighted with a red box around the entire row. The fourth entry is highlighted with a red box around the entire row. The left sidebar shows selected fields: host (100+), source (4), and sourcetype (1). The interesting fields sidebar shows component (2), index (1), log\_level (1), and message (100+).

i	Time	Event
>	8/8/18 6:16:19.691 PM	08-08-2018 18:16:19.691 +0000 INFO loader - Detected 2 (virtual) CPUs, 1 CPU cores, and 3577MB RAM host = prd-p-fq6wrtzfw88 source = /opt/splunk/var/log/splunk/splunkd.log   sourcetype = splunkd
>	8/8/18 6:16:19.691 PM	08-08-2018 18:16:19.691 +0000 INFO loader - System info: Linux, prd-p-fq6wrtzfw88, 3.13.0-141-generic, #19-Ubuntu SMP Fri Jan 19 12:52:38 UTC 2018, x86_64. host = prd-p-fq6wrtzfw88 source = /opt/splunk/var/log/splunk/splunkd.log   sourcetype = splunkd
>	8/8/18 6:16:19.660 PM	08-08-2018 18:16:19.660 +0000 INFO ServerConfig - My GUID is F47B7FC3-C284-4C95-809C-5A71441E2363 host = prd-p-fq6wrtzfw88 source = /opt/splunk/var/log/splunk/splunkd.log   sourcetype = splunkd
>	8/8/18 2:51:54.545 PM	08-08-2018 14:51:54.545 +0000 INFO loader - Detected 2 (virtual) CPUs, 1 CPU cores, and 3577MB RAM host = prd-p-fq6wrtzfw88 source = /opt/splunk/var/log/splunk/splunkd.log   sourcetype = splunkd

# Determine Relevant Information

# Useful data != data

- ▶ How do you know what you don't know?
  - ▶ What was the initial question that lead to this solution?
  - ▶ Begin to understand what data is useful and relevant

**Key to success is not overwhelming with pointless data**

# Normalize and Baseline

Making all the data look the same

- ▶ Understanding the differences between each data source
- ▶ Multiple data sources, formats, field names
- ▶ Create a standard baseline for these “common” fields
- ▶ Retain Latest information by chosen baseline unique field (e.g. hostname)

The screenshot shows a Splunk search interface with the following search command:

```
... | rex field=message "Running phone uri=\\services\\broker\\phonehome\\connection_(?<splunk_ip>(?:25[0-5]|2[0-4][0-9])[01]?[0-9][0-9]?)\\.(?:25[0-5]|2[0-4][0-9])[01]?[0-9][0-9]?)\\.(?:25[0-5]|2[0-4][0-9])[01]?[0-9][0-9]?" | rex field=message "My GUID is (?<splunk_guid>.*)" stats latest(_time) as _time | latest(splunk) by host eval splunk=_time, splunk_date=strftime(_time, %F), host=lower(host), splunk_guid=lower(splunk_guid), splunk_rqdn=lower(splunk_rqdn) | rex field=splunk_rqdn~":"[\\W-\\d]*?(?:\\.(?<splunk_domain>[^\\s]+)|\\.|$)" | fields -_time
```

The search results table displays the following data:

host	splunk	splunk_date	splunk_domain	splunk_fqdn	splunk_guid	splunk_ip
desktop-1	1	2018-08-10	data.com	desktop-1.data.com	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee	192.168.1.56
desktop-2	1	2018-08-10	data.com	desktop-2.data.com	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee	192.168.1.5
desktop-3	1	2018-08-10	data.com	desktop-3.data.com	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee	192.168.1.24
desktop-4	1	2018-08-10	data.com	desktop-2.data.com	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee	192.168.1.8
desktop-5	1	2018-08-10	data.com	desktop-5.data.com	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee	192.168.1.15
desktop-6	1	2018-08-10	data.com	desktop-6.data.com	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee	192.168.1.32

# Summarize and Prioritize

## Tool Trustworthiness is Key

- ▶ Multiple large, scheduled searches merging the data together into the existing list
- ▶ Keeping the information updated, relevant, and current
- ▶ Automation of list maintenance ensures that once this is functional, it won't require outside influence.
- ▶ Prioritize authoritative field output by trustworthiness and accuracy of data source.

The screenshot shows a Splunk search interface with the following details:

- Search Command:**

```
... | inputlookup append=true asset_data_hub | stats first(splunk*) as splunk* first(discovery*) as discovery* first(management*) as management* first(monitored*) as monitored* first(patching*) as patching* first(scanning*) as scanning* first(security*) as security* by host | eval ip=case(isnotnull(discovery_ip) AND strftime(discovery_date,"%F")>=now()-(60*60*24*3),discovery_ip,isnotnull(splunk_ip) AND strftime(splunk_date,"%F")>=now()-(60*60*24*3),splunk_ip, isnotnull(scanning_ip) AND strftime(scanning_date,"%F")>=now()-(60*60*24*3),scanning_ip, isnotnull(security_ip) AND strftime(security_date,"%F")>=now()-(60*60*24*3),security_ip, isnotnull(management_ip) AND strftime(management_date,"%F")>=now()-(60*60*24*3),management_ip, isnotnull(security_ip) AND strftime(security_date,"%F")>=now()-(60*60*24*3),security_ip, isnotnull(discovery_ip),discovery_ip, isnotnull(splunk_ip),splunk_ip, isnotnull(scanning_ip),scanning_ip, isnotnull(security_ip),security_ip, isnotnull(management_ip),management_ip) ... | outputlookup asset_data_hub
```
- Results:** 54 results (8/10/18 11:54:52.000 AM to 8/10/18 12:09:52.000 PM) No Event Sampling
- Visualizations:** Job, Smart Mode
- Table View:** Shows a grid of data with columns including ip, splunk, splunk\_date, splunk\_domain, splunk\_fqdn, splunk\_guid, splunk\_ip, discovery, discovery\_date, discovery\_ip, discovery\_lastlogin, discovery\_mac, discovery\_os, host, management, and management\_date. The first three rows are highlighted with a red border.

ip	splunk	splunk_date	splunk_domain	splunk_fqdn	splunk_guid	splunk_ip	discovery	discovery_date	discovery_ip	discovery_lastlogin	discovery_mac	discovery_os	host	management	management_date
192.168.1.56	1	2018-08-10	data.com	desktop1.data.com	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeee	192.168.1.56	1	2018-08-05	123.456.789.1	2018-08-05	ab12	windows 7	desktop1	1	2018-08-04
192.168.1.5	1	2018-08-10	data.com	desktop2.data.com		192.168.1.5	1	2018-08-05	123.456.789.2	2018-08-05	ab13	windows 7	desktop2	1	2018-08-04
192.168.1.24	1	2018-08-10	data.com	desktop3.data.com	aaaaaaaa-bbbb-cccc-dddd	192.168.1.24	1	2018-08-05	123.456.789.3	2018-08-05	ab14	windows 7	desktop3	1	2018-08-01

# Summary

1. Any data source can tell you a lot about your network
2. Merging all sources together is a solvable problem
3. Many different possibilities by merging together different sources to tell a story
  - Patching
  - Users
  - Serial Numbers to specific locations
  - Software Purchased vs Installed vs Usage
  - So many possibilities, so little time...

# Questions

# Thank You

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

