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

Christopher Jonnes | NetCentrics
Jonathan Fair | DIOS 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> .conf18

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

splunk> .conf18

Overview

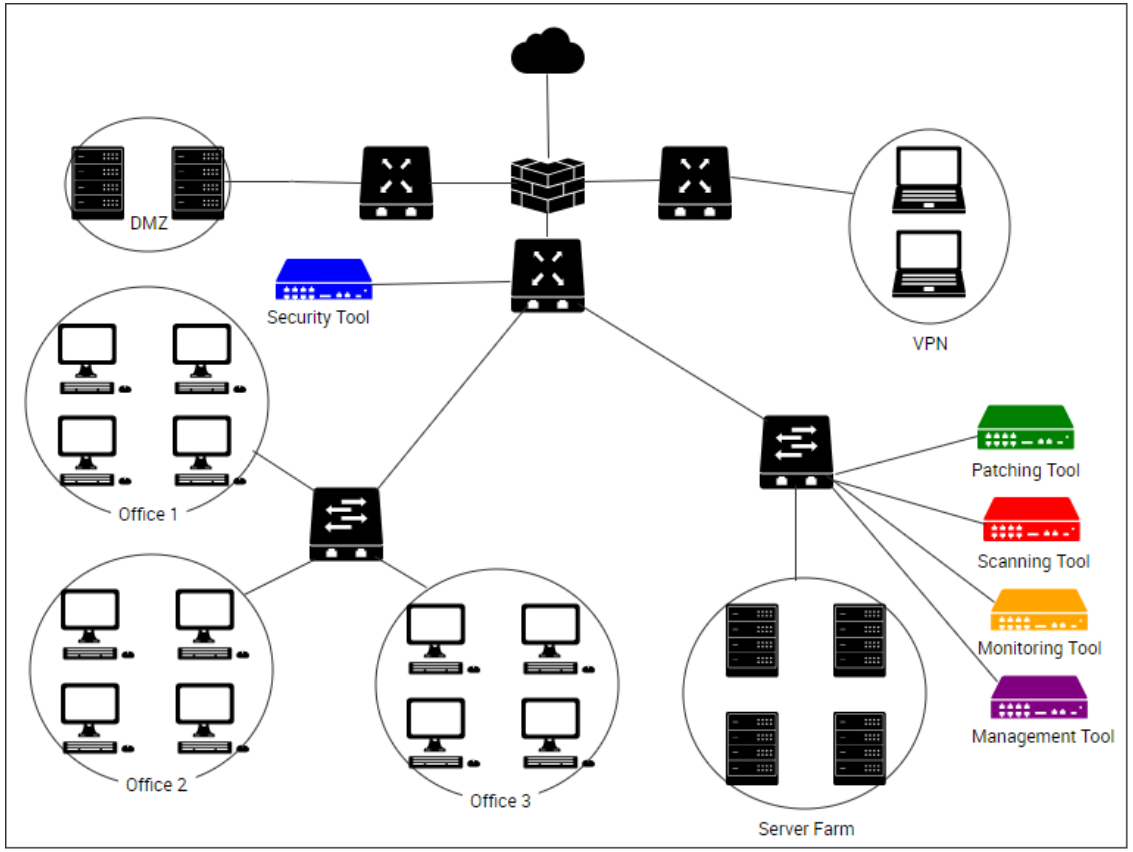
Solve Fundamental IT Issues by Leveraging Your Network Tools' Data Using Splunk

- 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

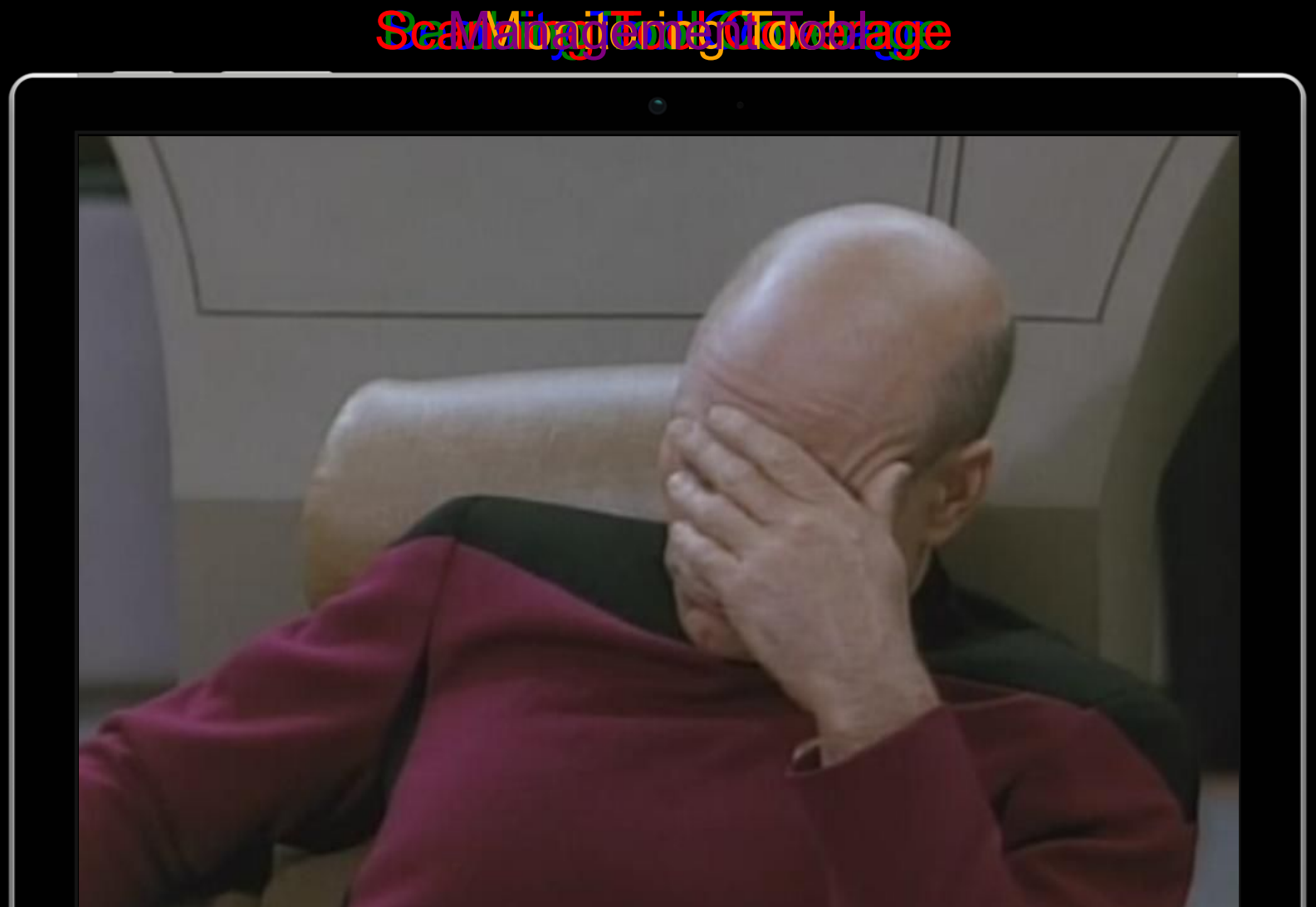
- Managing multiple Tools
- Utilizing your Tools Efficiently and Effectively
- Tracking devices on your network
- What coverage gaps do you have?
- How do you determine what your tools don't see?



How do you know what you don't know?

Tool Coverage and Network Visibility

Tell me about my network, Bob



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

Other Challenges

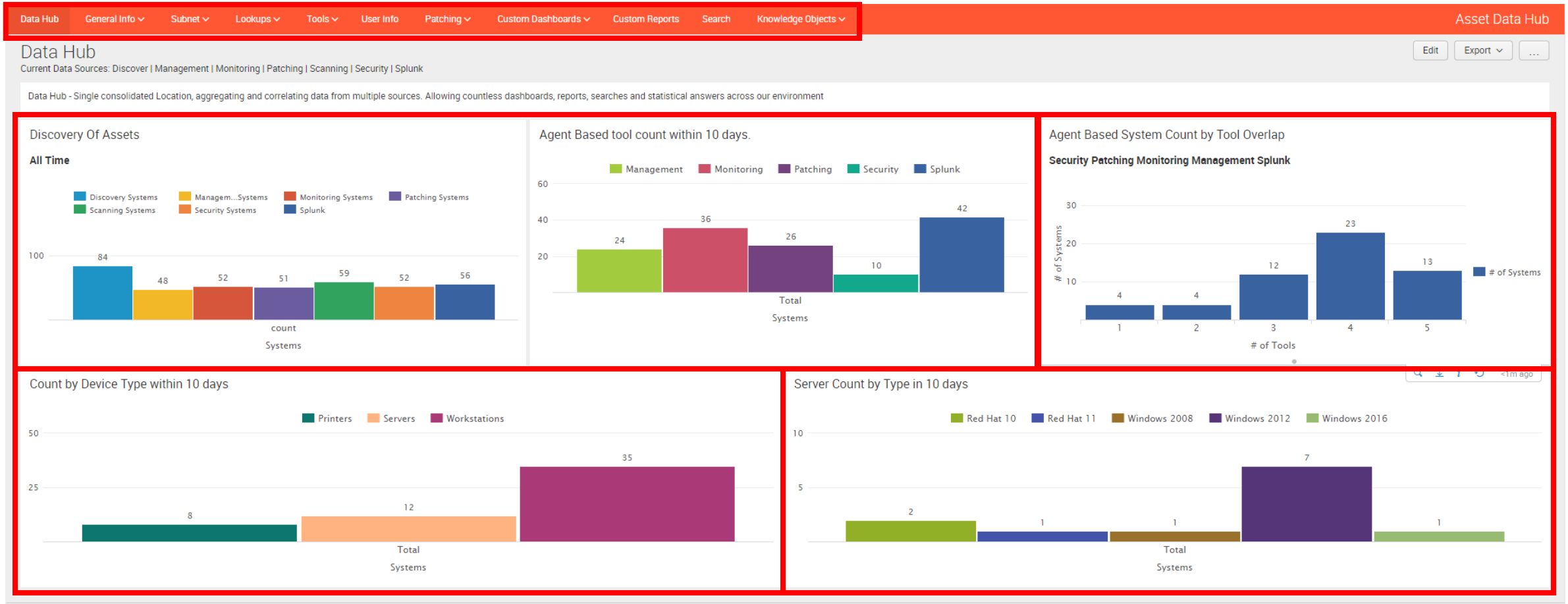
Why can't this just be easier!

- 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!

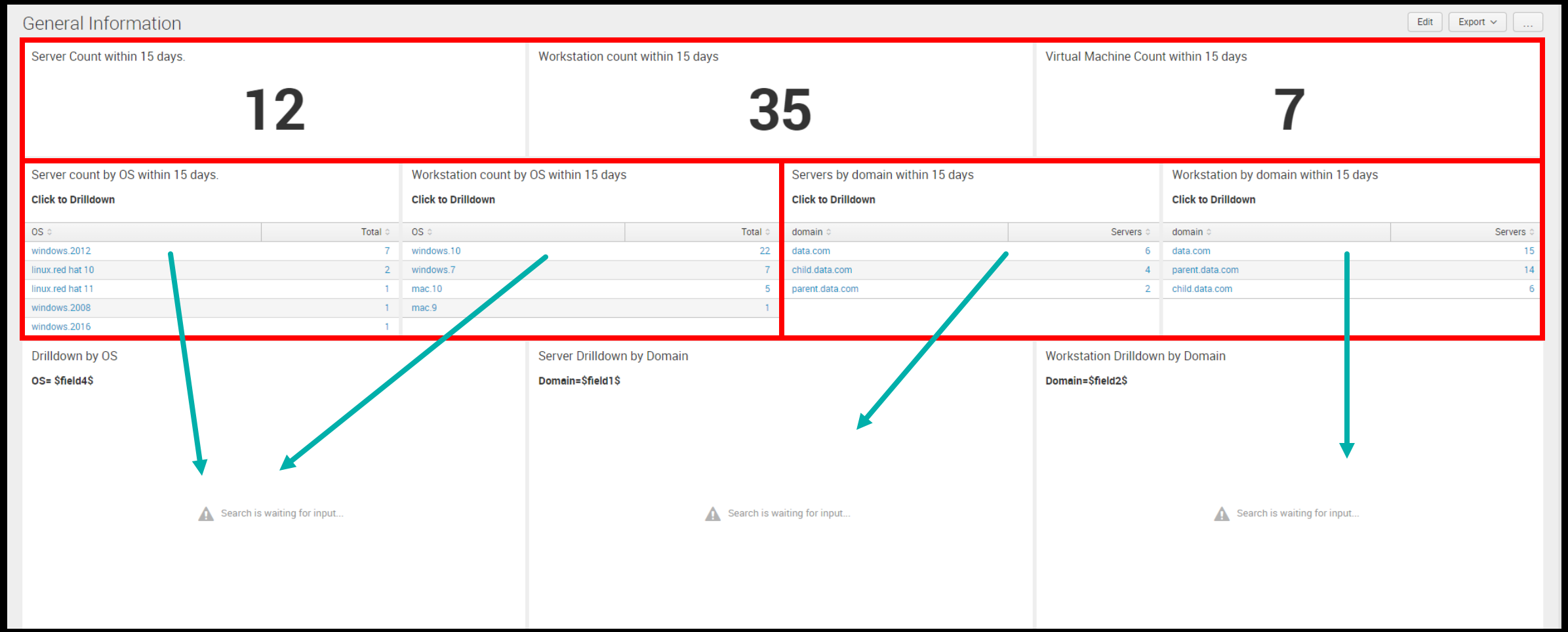
Asset Data Hub



splunk> .conf18

Asset Data Hub

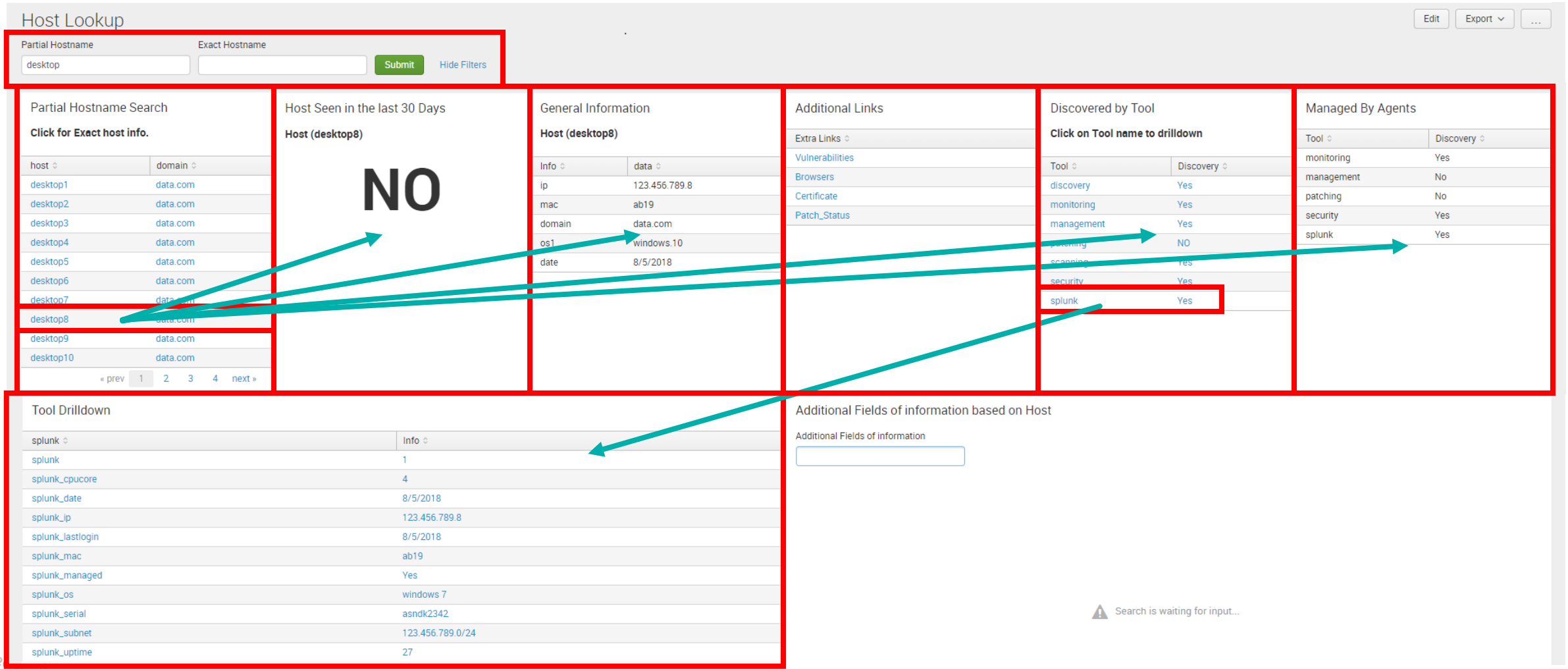
General Information



splunk> .conf18

Asset Data Hub

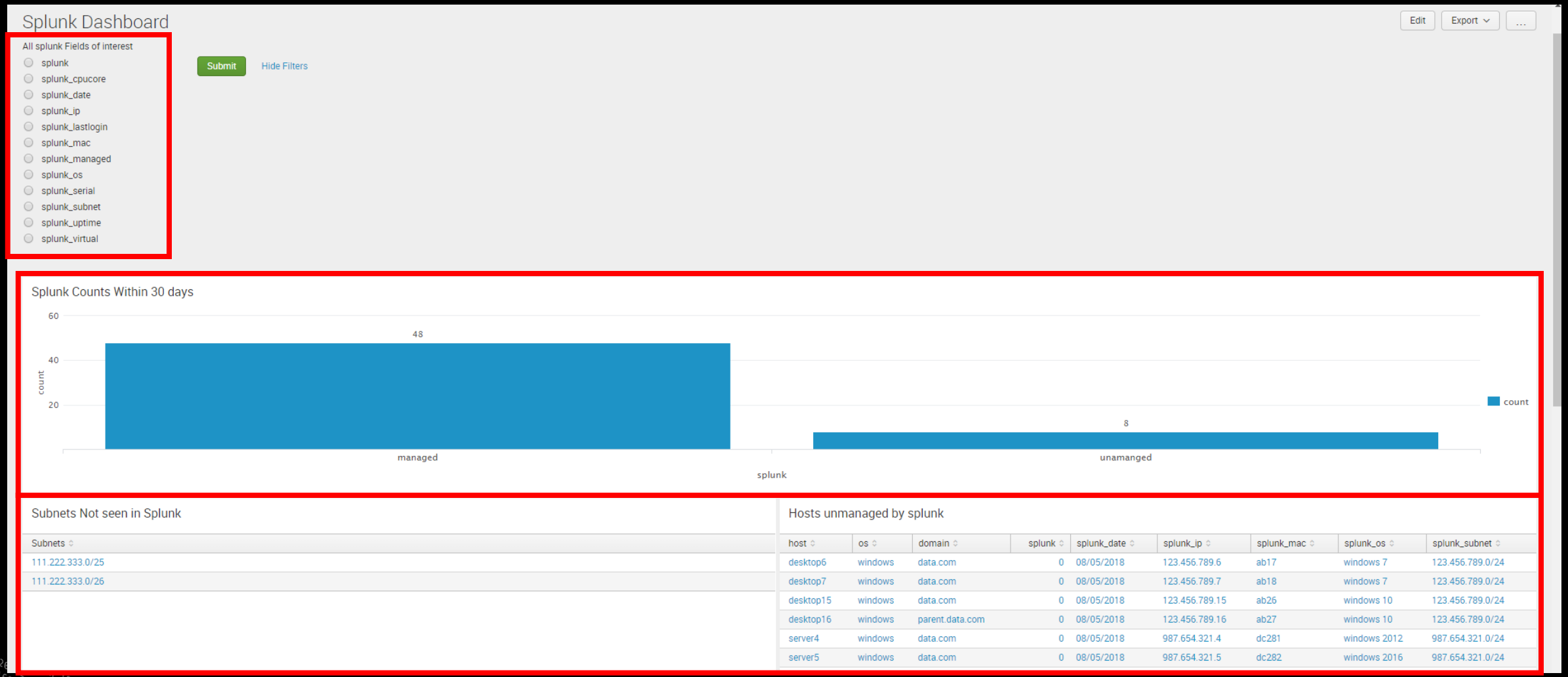
Lookup



splunk> .conf18

Asset Data Hub

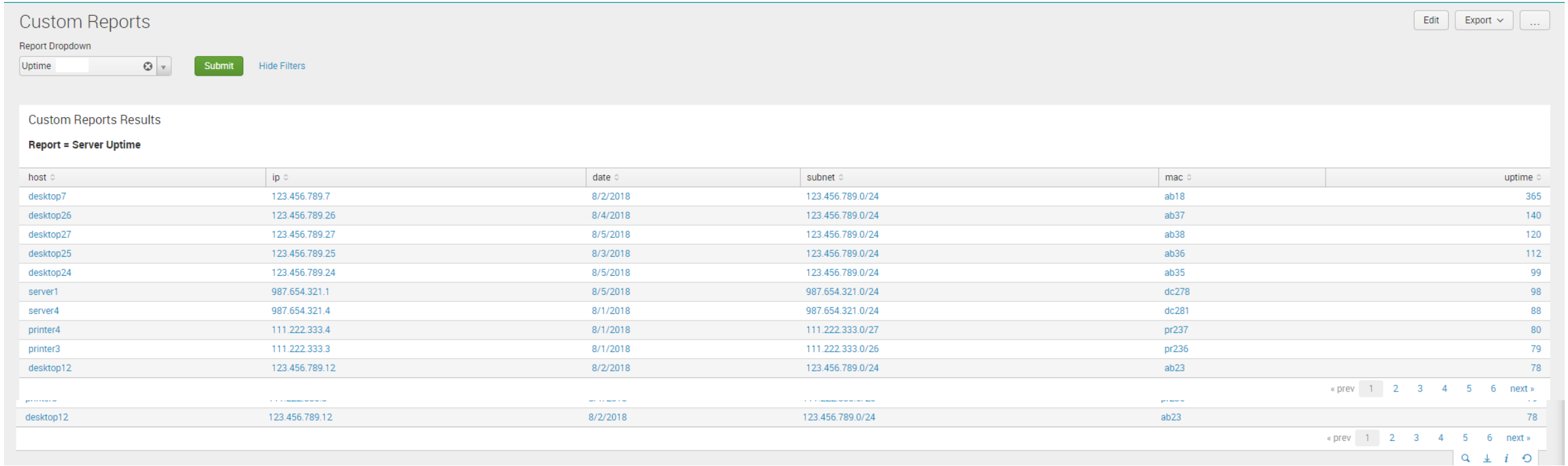
Tool Dashboards – All Data is Correlated



splunk> .conf18

Asset Data Hub

Custom Reports / Dashboards



splunk> .conf18

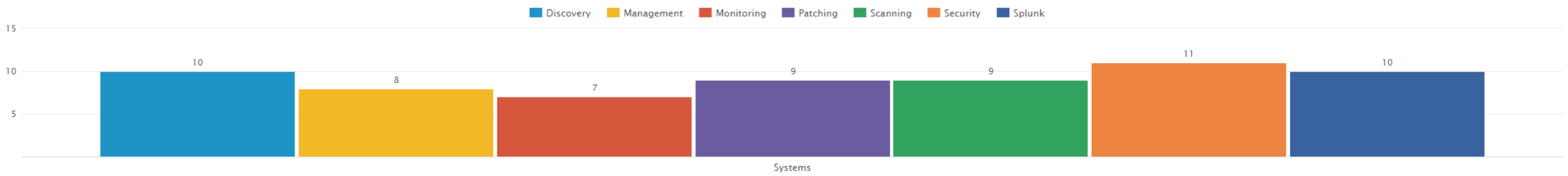
Asset Data Hub

Subnet Analysis

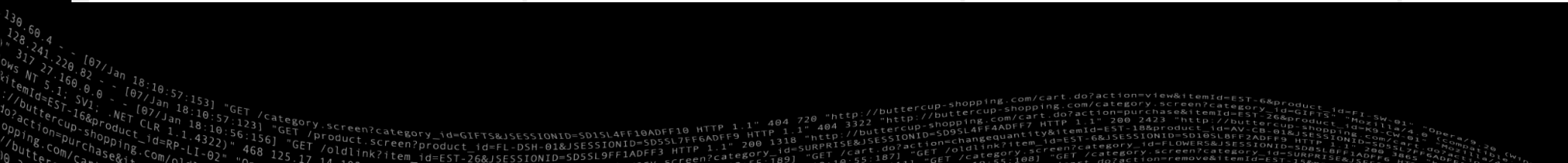
Subnet Info

Edit | Export | ...

Subnet count by Tool

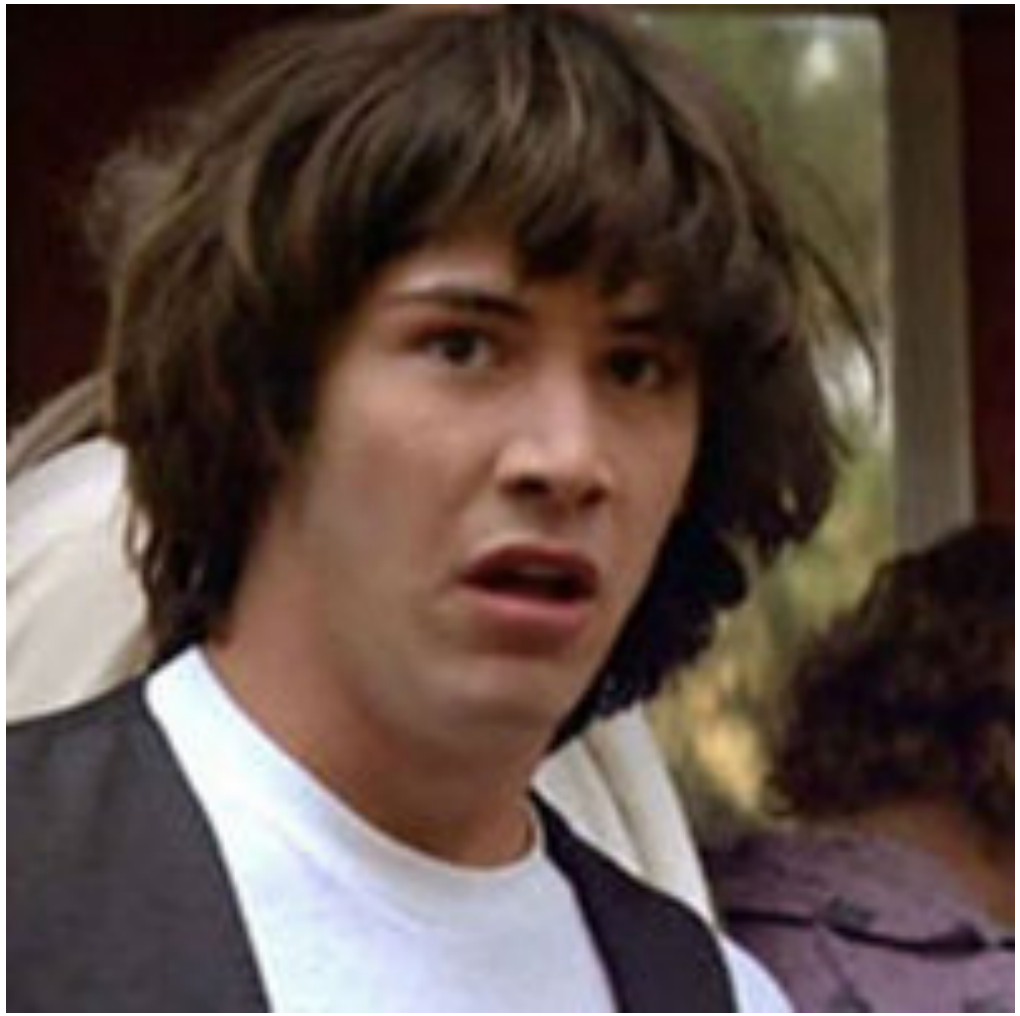


Discovery Seen Subnets	Management Seen Subnets	Monitong Seen Subnets	Patching Seen Subnets	Scanning Seen Subnets	Security Subnets	Splunk Seen Subnets
Subnets	Subnets	Subnets	Subnets	Subnets	Subnets	Subnets
11.22.33.0/24	11.22.33.0/24	11.22.33.0/24	11.22.33.0/24	11.22.33.0/24	11.22.33.0/24	11.22.33.0/24
111.222.33.0/24	123.789.456.0/24	111.222.33.0/24	111.222.33.0/24	111.222.33.0/24	111.222.33.0/24	123.456.789.0/24
123.456.789.0/24	15.45.87.0/24	123.789.456.0/24	123.456.789.0/24	123.456.789.0/24	123.456.789.0/24	15.45.87.0/24
123.789.456.0/24	24.5.7.0/24	15.45.87.0/24	123.789.456.0/24	123.789.456.0/24	123.789.456.0/24	18.55.62.0/24
15.45.87.0/24	77.19.22.0/24	88.80.41.0/24	15.45.87.0/24	15.45.87.0/24	15.45.87.0/24	456.789.123.0/24
24.5.7.0/24	88.80.41.0/24	99.14.5.0/24	18.55.62.0/24	77.19.22.0/24	18.55.62.0/24	77.19.22.0/24
77.19.22.0/24	97.45.123.0/24	**Unseen Subnets**	88.80.41.0/24	97.45.123.0/24	456.789.123.0/24	88.80.41.0/24
88.80.41.0/24	**Unseen Subnets**	Subnets	99.14.5.0/24	99.14.5.0/24	77.19.22.0/24	97.45.123.0/24
97.45.123.0/24	Subnets	123.456.789.0/24	**Unseen Subnets**	**Unseen Subnets**	97.45.123.0/24	99.14.5.0/24
Unseen Subnets	111.222.33.0/24	123.789.456.0/24	Subnets	Subnets	99.14.5.0/24	**Unseen Subnets**
Subnets	123.456.789.0/24	15.45.87.0/24	24.5.7.0/24	111.222.33.0/24	**Unseen Subnets**	Subnets
18.55.62.0/24	18.55.62.0/24	24.5.7.0/24	456.789.123.0/24	18.55.62.0/24	Subnets	111.222.33.0/24
456.789.123.0/24	24.5.7.0/24	77.19.22.0/24	77.19.22.0/24	456.789.123.0/24	24.5.7.0/24	123.789.456.0/24
99.14.5.0/24	99.14.5.0/24	97.45.123.0/24	97.45.123.0/24	88.80.41.0/24	88.80.41.0/24	24.5.7.0/24



splunk> .conf18

We can use Splunk for all of this?



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 endless 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

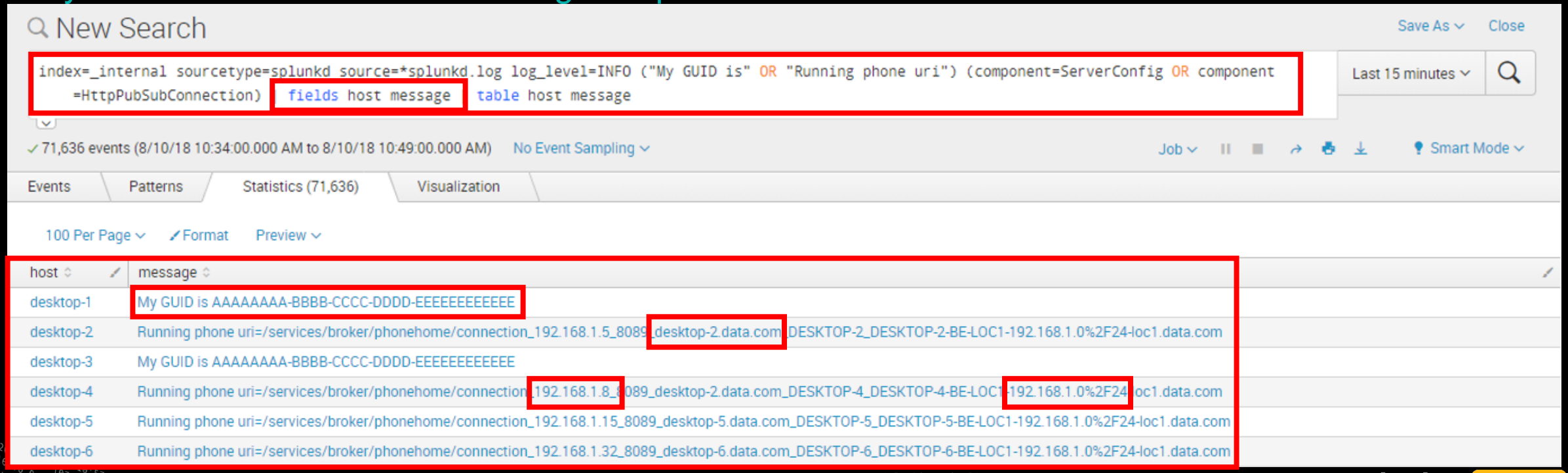
We are going to use Splunk as our example to walk through

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

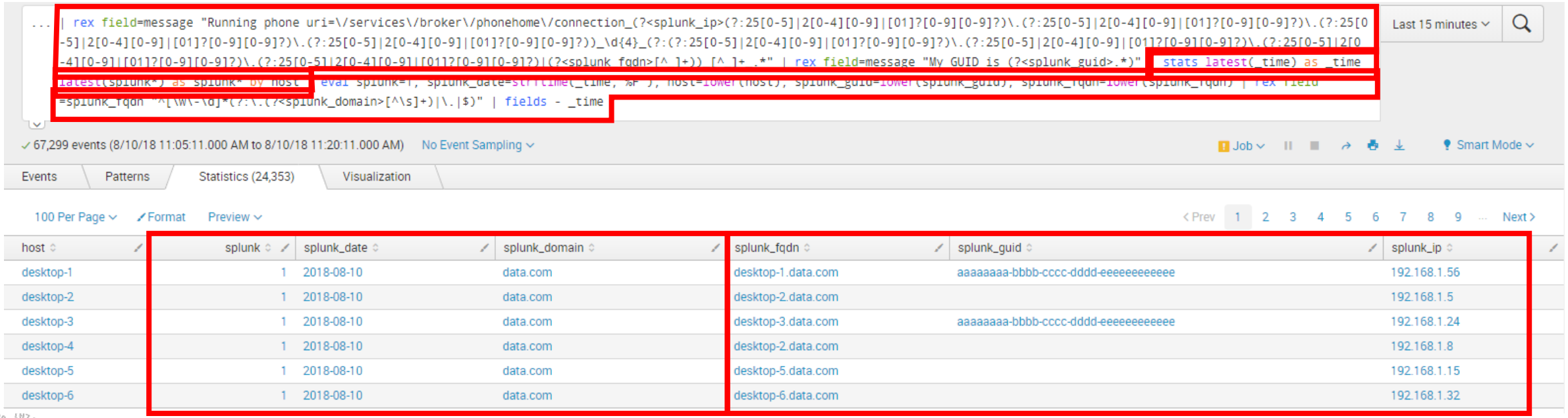


splunk> .conf18

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)



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.

```
... | inputlookup append=true asset_data_hub | stats first(splunk*) as splunk* first(discovery*) as discovery* first(management*) as management* first(monitoring*) as monitoring* first
(patching*) as patching* first(scanning*) as scanning* first(security*) as security* by host | eval ip=case(isnotnull(discovery_ip) AND strptime(discovery_date,"%F")>=now()-(60*60*24*3
),discovery_ip,isnotnull(splunk_ip) AND strptime(splunk_date,"%F")>=now()-(60*60*24*3),splunk_ip, isnotnull(scanning_ip) AND strptime(scanning_date,"%F")>=now()-(60*60*24*3),scanning_ip,
isnotnull(security_ip) AND strptime(security_date,"%F")>=now()-(60*60*24*3),security_ip, isnotnull(management_ip) AND strptime(management_date,"%F")>=now()-(60*60*24*3),management_ip,
isnotnull(security_ip) AND strptime(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(security_ip),security_ip, isnotnull(management_ip),management_ip) ... | outputlookup asset_data_hub
```

Last 15 minutes

✓ 54 results (8/10/18 11:54:52.000 AM to 8/10/18 12:09:52.000 PM) No Event Sampling

Job Smart Mode

Events Patterns Statistics (54) Visualization

100 Per Page Format Preview

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_da
192.168.1.56	1	2018-08-10	data.com	desktop1.data.com	aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee	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-	192.168.1.24	1	2018-08-05	123.456.789.3	2018-08-05	ab14	windows 7	desktop3	1	2018-08-01

splunk> .conf18

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