splunk> .conf2017

Security Hands-on @ Pavilion

Stream + NetFlow for Security & Insider Threat Detection

Kelly Feagans | Sales Engineering

September 2017 | Washington, DC

Objective

OBJECTIVE

- Learn how to use NetFlow with the Splunk Stream Forwarder for outlier detection

USE CASES

- NetFlow: Endpoint outlier detection (overall) and insider threat
- NetFlow: Anomalous connections by host
- NetFlow: Possible data exfiltration
- NetFlow: Extra-Credit – Adding proxy data in the mix!

BENEFITS

- Identify anomalies and outliers respective to network usage by time of day, port, bytes sent/received, geographic location, or by functional group.

NetFlow for Outlier (Insider Threat) Detection

NetFlow, when used in conjunction with Splunk Stream, is an effective and rather simple solution to capture wire data moving across an environment.

SPLUNK STREAM USED AS A FLOW COLLECTOR

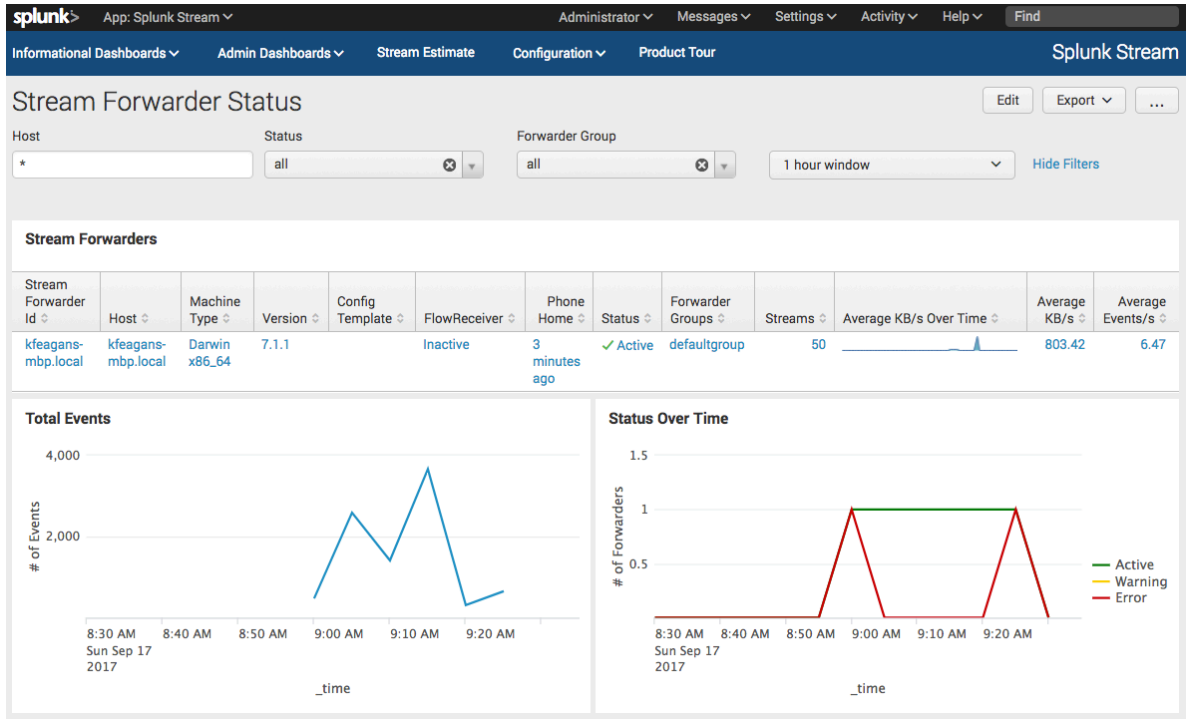
- Use one or many Stream Forwarder(s) as needed

FAST AND SIMPLE SETUP

- Configure flow data ingestion (streamfwd.conf)
- Configure forwarding of flows to Stream Forwarder
- Supported Flow Protocols: NetFlow v5, v9, IPFIX; sFlow v5, jFlow

FIND OUTLIERS, ANOMALOUS CONNECTIONS, DATA EXFIL, ETC

- Start searching!



splunk> .conf2017

splunk> .conf2017

Security Hands-on @ Pavilion

Use Case 1 : Find the Outlier (by bytes & port)

Kelly Feagans | Sales Engineering

September, 2017 | Washington, DC

Use Case 1: Find the Outlier by Port

OBJECTIVE

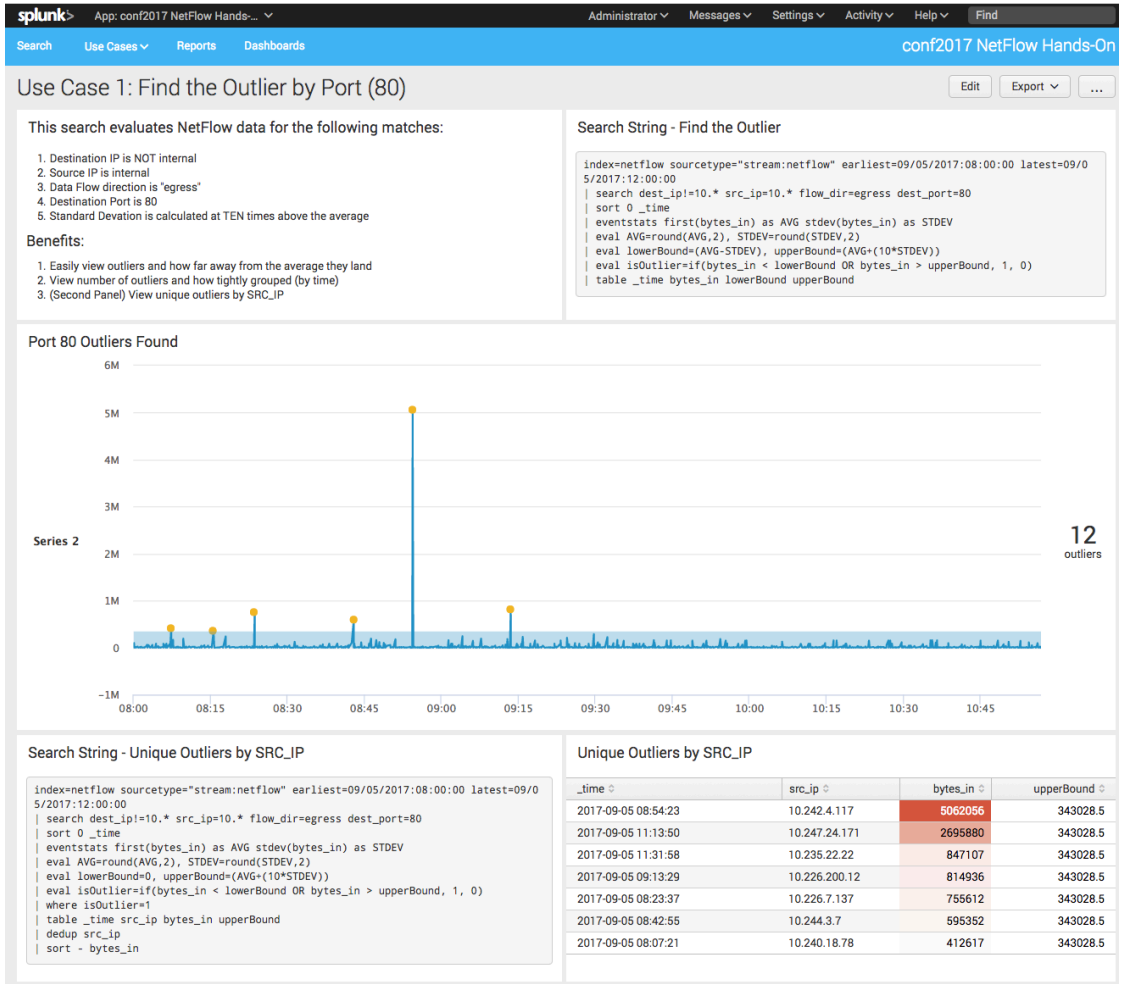
- Use NetFlow data to find the outlier by port

USE CASE

- User activities tracking by port (80)
- Use an extreme number (standard deviation) above the mean (like 10x)

BENEFITS

- Quickly visualize the outlier(s) (different than all the rest) that are communicating on port 80
- View how tightly the outlier(s) are grouped by time



splunk> .conf2017

Use Case 1: Outlier - SPL


```
index=netflow sourcetype="stream:netflow"
earliest=09/05/2017:08:00:00
latest=09/05/2017:17:00:00 src_ip=10.232.117.*
| bucket _time span=1h@h
| stats dc(dest_ip) as count by src_ip, _time
| eventstats max(_time) as maxtime
| stats count as num_data_samples max(eval(if(_time
>= relative_time(maxtime, "-1h@h"), 'count',null)))
as "count" avg(eval(if(_time<="" or="" 'count'="">
upperBound) AND num_data_samples >=7, "YES", "NO")
| eval vs="current vs last hour”
| eval howFarAway=count/avg
| table src_ip, vs, isOutlier, count, avg,
howFarAway, lowerBound, upperBound
| where isOutlier="YES”
| sort - howFarAway
```

STEP BY STEP GUIDE – Use Case 1

Start with a look at the first search - Find the Outlier:

- Hover over the panel, and click on the magnifying glass icon to launch search
- How many Stats rows do you see? (Statistics Tab)
- Change flow_dir from“egress” to “ingress”
  - How many outliers do you see?

For the second search – Unique Outliers:

- Hover over the panel, and click on the magnifying glass icon to launch search
- Change flow_dir from ”egress” to “ingress”
- What SRC_IP do you see as ”the” outlier?

splunk> .conf2017

Security Hands-on @ Pavilion

Use Case 2 : Anomalous Connections by Host

Kelly Feagans | Sales Engineering

September 2017| Washington, DC

Use Case 2: Anomalous Connections by Host

OBJECTIVE

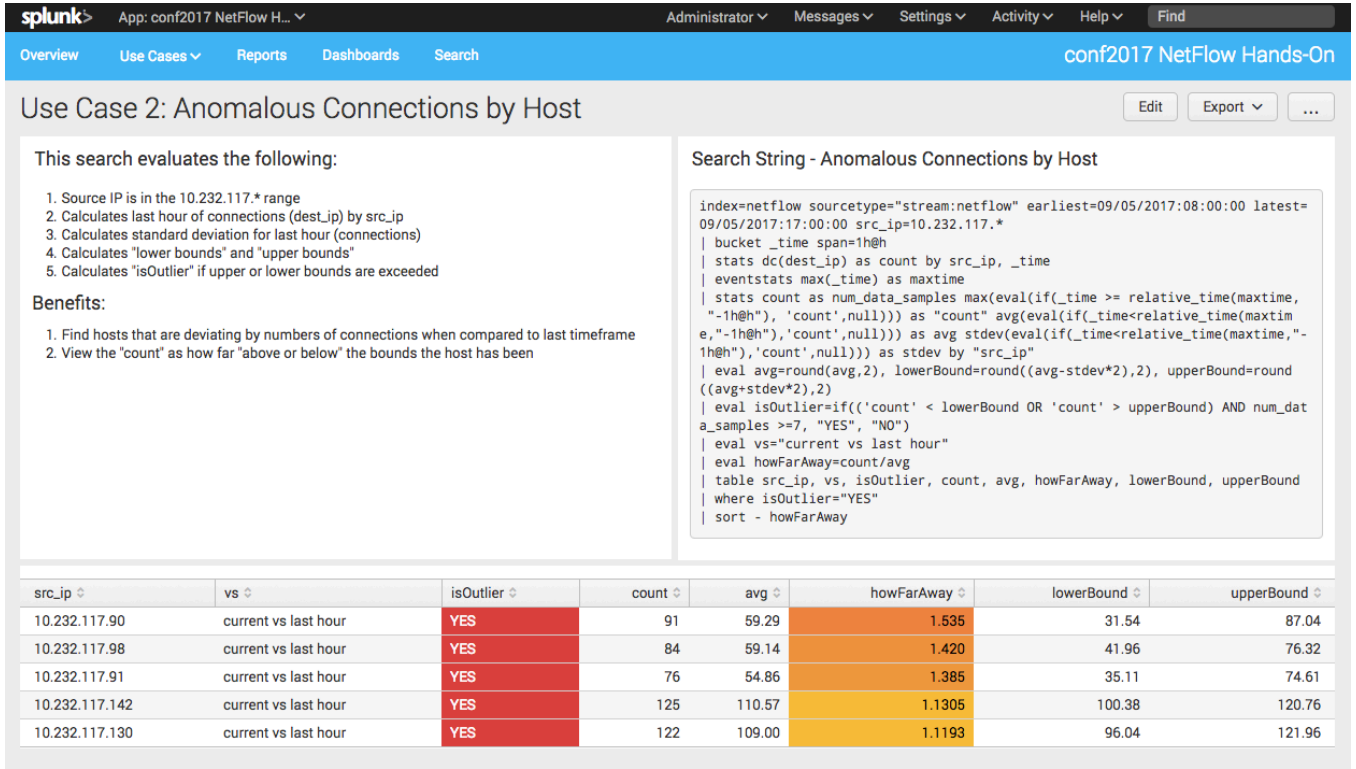
- Learn how to use NetFlow data to evaluate "anomalous connections by host"

USE CASE

- Find hosts that have deviated in the count of connections, as compared to last hour

BENEFITS

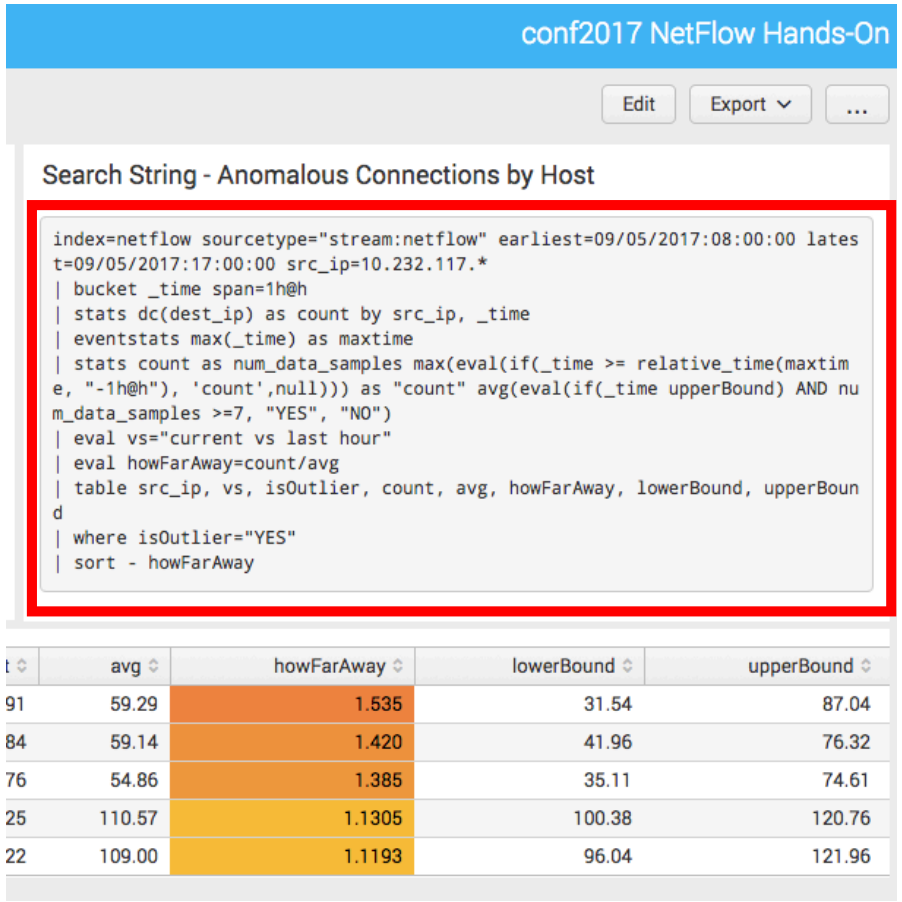
- Identify hosts that could be abnormally affected by Malware, etc.



Note: "Anomalous Connections by Host" is borrowed from a search in the Splunk Security Essentials App. Thank you David Veuve!!!

splunk> .conf2017

Use Case 2: Anomalous Connections - SPL




```
index=netflow sourcetype="stream:netflow"
earliest=09/05/2017:08:00:00 latest=09/05/2017:17:00:00
src_ip=10.232.117.*
| bucket _time span=1h@h
| stats dc(dest_ip) as count by src_ip, _time
| eventstats max(_time) as maxtime
| stats count as num_data_samples max(eval(if(_time >=
relative_time(maxtime, "-1h@h"), 'count',null))) as "count"
avg(eval(if(_time<relative_time(maxtime,"-
1h@h"),'count',null))) as avg
stdev(eval(if(_time<relative_time(maxtime,"-
1h@h"),'count',null))) as stdev by "src_ip"
| eval avg=round(avg,2), lowerBound=round((avg-stdev*2),2),
upperBound=round((avg+stdev*2),2)
| eval isOutlier=if(('count' < lowerBound OR 'count' >
upperBound) AND num_data_samples >=7, "YES", "NO")
| eval vs="current vs last hour"
| eval howFarAway=count/avg
| table src_ip, vs, isOutlier, count, avg, howFarAway,
lowerBound, upperBound
| where isOutlier="YES"
| sort - howFarAway
```

splunk> .conf2017

STEP BY STEP GUIDE – Use Case 2

Start with a look at the search “Anomalous Connections by Host”:

- Hover over the panel, and click on the magnifying glass icon to launch search
- How many Stats rows do you see out of how many events returned?
- Try changing the bounds (avg+/stdev*2) …. to a 4 ….
  - How many outliers do you see now?
- What do you think this could tell you about hosts in your environment?

splunk> .conf2017

splunk> .conf2017

Security Hands-on @ Pavilion

Use Case 3 : Possible Data Exfiltration

Kelly Feagans | Sales Engineering

September, 2017 | Washington, DC

Use Case 3: Possible Data Exfiltration

OBJECTIVE

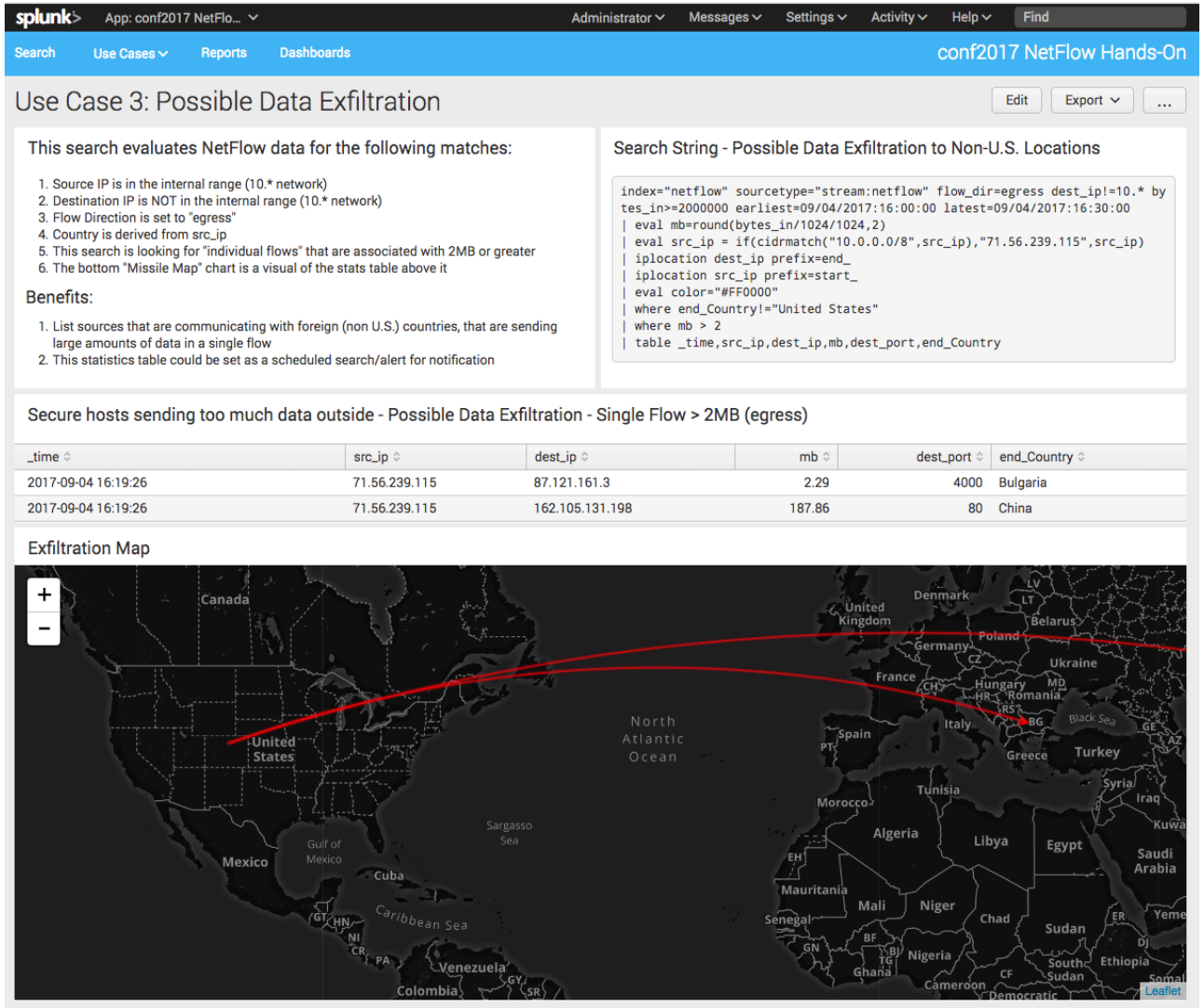
- Gain an understanding of which hosts internal to an environment are sending a large amount of data outbound in “single” flows.

USE CASE

- Find internal hosts that are not permitted to send data outside their network, and/or to prohibited sites.

BENEFITS

- List sources that are communicating (large byte counts, single flow) with non-U.S. endpoints.



splunk> .conf2017

Use Case 3: Possible Data Exfiltration - SPL

```
index="netflow" sourcetype="stream:netflow" flow_dir=egress dest_ip!=10.*
bytes_in>=2000000 earliest=09/04/2017:16:00:00 latest=09/04/2017:16:30:00
| eval mb=round(bytes_in/1024/1024,2)
| eval src_ip = if(cidrmatch("10.0.0.0/8",src_ip),"71.56.239.115",src_ip)
| iplocation dest_ip prefix=end_
| iplocation src_ip prefix=start_
| eval color="#FF0000”
| where end_Country!="United States”
| where mb > 2
| table _time,src_ip,dest_ip,mb,dest_port,end_Country
```

splunk> .conf2017

STEP BY STEP GUIDE – Use Case 3

Start with a look at the search “Possible Data Exfiltration”:

- Hover over the panel, and click on the magnifying glass icon to launch search
- How many Stats rows do you see returned?
- Try remove the ’where’ command “end_Country!=United States”
  - What do you see now?

Take a look at the second panel … “Missile Map”:

- Hover over the panel, and click on the magnifying glass icon to launch search
- Try remove the ’where’ command “end_Country!=United States”
  - What do you see now when clicking on the “Visualization Tab”?

splunk> .conf2017

splunk> .conf2017

Security Hands-on @ Pavilion

Extra Credit: NetFlow + Proxy

Kelly Feagans | Sales Engineering

September, 2017 | Washington, DC

Extra Credit: Proxy + NetFlow

OBJECTIVE

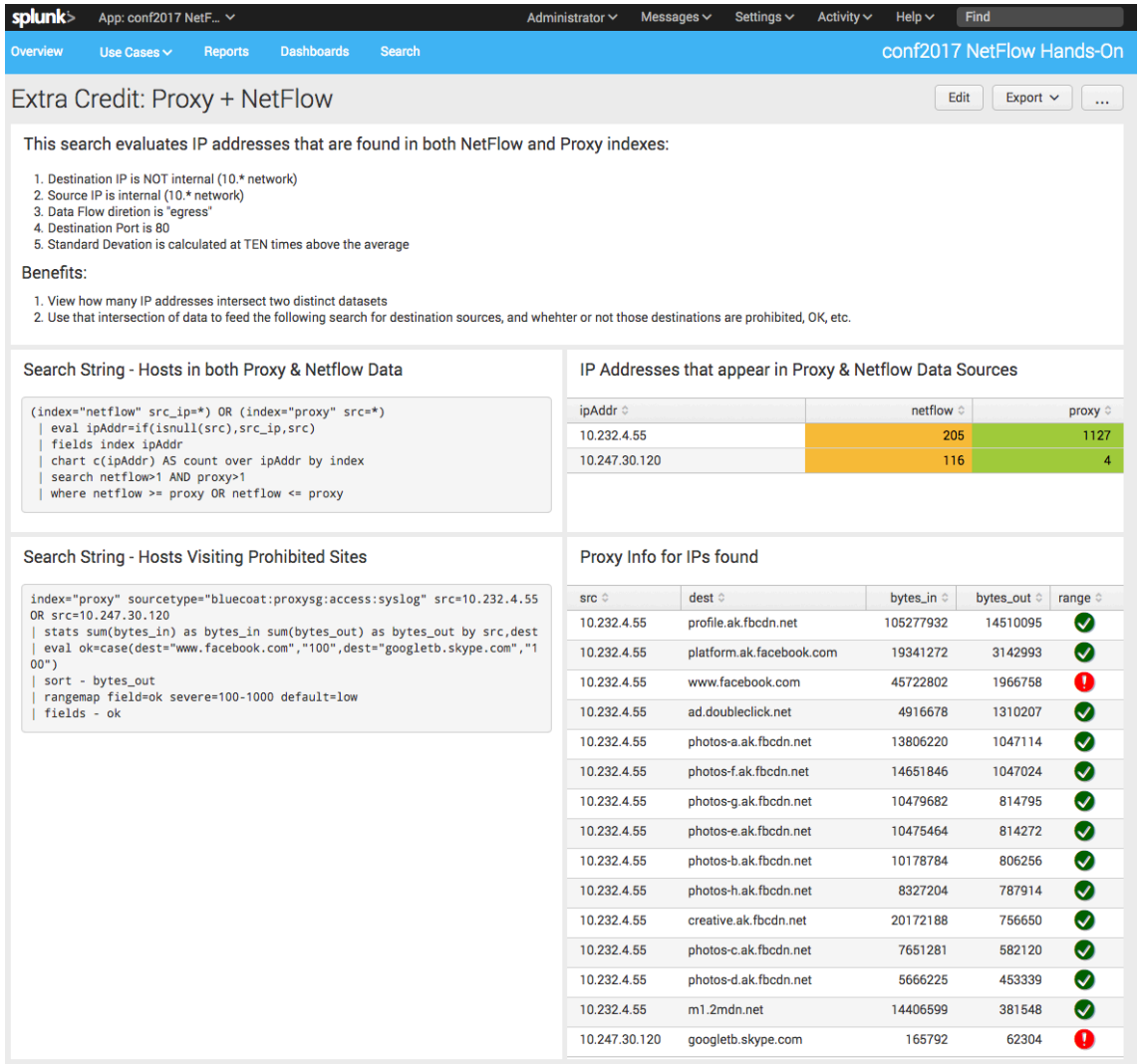
- Gain an understanding of hosts that are seen in both NetFlow and Proxy data (cross-reference)

USE CASE

- Find internal hosts that are outside of security policy (communicating with forbidden hosts or sites)

BENEFITS

- Search through hundreds to millions of records to find hosts that fall out of policy



splunk> .conf2017

Extra Credit: Proxy + NetFlow

```
(index="netflow" src_ip=*) OR (index="proxy" src=*)
| eval ipAddr=if(isnull(src),src_ip,src)
| fields index ipAddr
| chart c(ipAddr) AS count over ipAddr by index
| search netflow>1 AND proxy>1
| where netflow >= proxy OR netflow <= proxy
```

IP Addresses that appear in Proxy & Netflow Data Sources

ipAddr	netflow	proxy
10.232.4.55	205	1127
10.247.30.120	116	4

```
index="proxy"
sourcetype="bluecoat:proxysg:access:syslog"
src=10.232.4.55 OR src=10.247.30.120
| stats sum(bytes_in) as bytes_in sum(bytes_out) as
bytes_out by src,dest
| eval
ok=case(dest="www.facebook.com","100",dest="googletb
.skype.com","100")
| sort - bytes_out
| rangemap field=ok severe=100-1000 default=low
| fields - ok
```

Proxy Info for IPs found

src	dest	bytes_in	bytes_out	range
10.232.4.55	profile.ak.fbcdn.net	105277932	14510095	✓
10.232.4.55	platform.ak.facebook.com	19341272	3142993	✓
10.232.4.55	www.facebook.com	45722802	1966758	!
10.232.4.55	ad.doubleclick.net	4916678	1310207	✓
10.232.4.55	photos-a.ak.fbcdn.net	13806220	1047114	✓
10.232.4.55	photos-f.ak.fbcdn.net	14651846	1047024	✓
10.232.4.55	photos-g.ak.fbcdn.net	10479682	814795	✓

splunk> .conf2017

STEP BY STEP GUIDE – Extra Credit

Start with a look at the search “Possible Data Exfiltration”:

- Hover over the panel, and click on the magnifying glass icon to launch search
- How many Stats rows do you see returned out of how many events?
- Which is the most interesting row?
  - Click on “10.232.4.55”, then “View Events”
  - What does that data tell you?

- Take a look at the second panel … “Proxy Info for IPs Found”:
  - Hover over the panel, and click on the magnifying glass icon to launch search
  - What are the apps most in use by these hosts?

splunk> .conf2017

splunk> .conf2017

Security Hands-on @ Pavilion

Thank you!

Kelly Feagans | Sales Engineering

September, 2017 | Washington, DC