.conf2015

Aurizon and Splunk Cloud

Şebnem Kürklü
Information Security Manager

splunk>

Disclaimer

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 the 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.

About Aurizon

- Aurizon (ASX:AZJ) is the largest rail freight operator and a top 50 ASX company.
- Each year, Aurizon transports more than 250 million tonnes of Australian commodities.
- Aurizon also owns and operates one of the world's largest coal rail networks, linking more than 50 mines with three major ports in Queensland.
- Vision is to be a world leading rail-based transport business.
- Safety of ourselves and others is the number one priority. Safety is at the core of everything we do as we commit to ZeroHarm.

About Me

Şebnem Kürklü

- Information Security Manager in Aurizon for the last 12 months.
- Previously held Security and Risk Management roles in the financial sector.

Areas of focus:

- Improve the security posture of Aurizon by improving core competencies in IT and OT.
- Improve vendor and service provider relationships to achieve better security outcomes.
- Improve the risk awareness in the business units.
- Leverage investment in current technologies.

Aurizon IT Environment

Parts of Aurizon IT is outsourced to Fujitsu. They provide majority of corporate IT services.

Networks & Comms

Storage

Server & Desktop

Messaging

Directories

Application Support

Aurizon IT Environment

Aurizon retains some core functions internally and interacts directly with the business.

Architecture & Design

Project Delivery

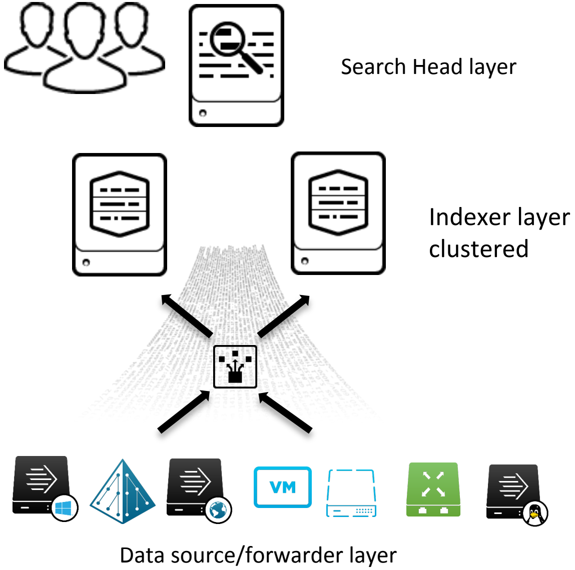
Service Management

Security

Governance

Advisory

Aurizon Using Splunk



Splunk was deployed in house to assist the Security Team in :

- Detection of some malware events – supported by ES
- Performance monitoring of some directory servers
- Investigations relating to privileged access changes
- Investigations relating to Code of Conduct breaches
- Monitoring a number of internal applications errors

Limitations

Licensing – 20 Gig capacity

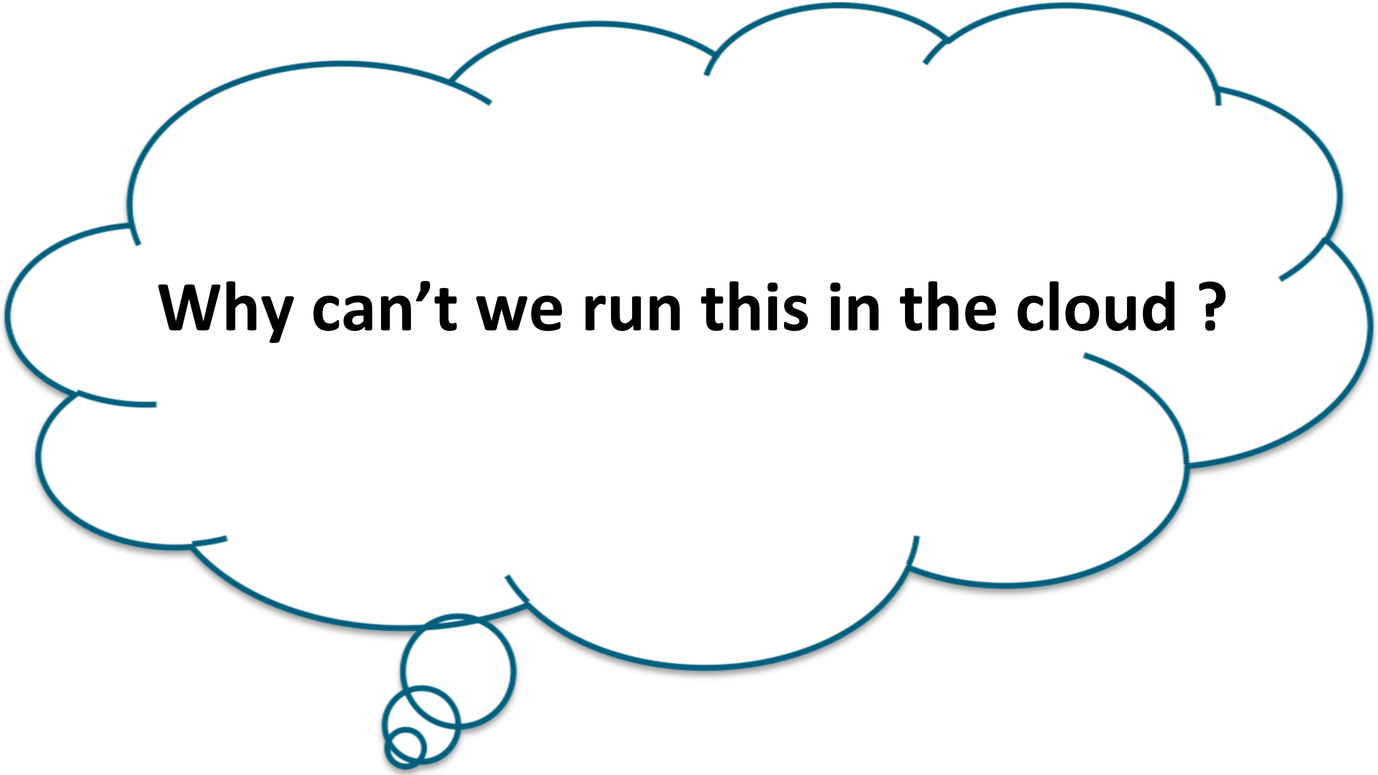
Resourcing – Lack of an internal support team

Aurizon Growing Splunk

Re:platform Costs – Setup & Ongoing

	Physical Servers	Virtual Servers
Additional Servers	💰	
OS Licence	💰	
VM Licence	💰	💰💰
Additional Disk	💰💰	💰💰
Mirror/Backup costs	💰💰	💰💰
Datacentre costs	💰💰	💰💰
Splunk Licence & Maintenance	💰💰💰💰	💰💰💰💰

Aurizon Growing Splunk



Why can’t we run this in the cloud ?

Splunk Cloud Considerations

Costs – Setup & Ongoing

	Physical Servers	Virtual Servers	Splunk Cloud
Additional Servers	💰		
OS Licence	💰		
VM Licence	💰	💰💰	
Additional Disk	💰💰	💰💰	
Mirror/Backup costs	💰💰	💰💰	
Datacentre costs	💰💰	💰💰	
Licence & Maintenance	💰💰💰💰	💰💰💰💰	💰💰💰💰💰💰💰

Splunk Cloud Considerations

Cost Savings & Performance Gains

Reduce the monthly operating costs while improving performance.

Availability

Ensure 100% availability without creating a full DR replica of the system.

Administration

Simplify Splunk to reduce system administration and maintenance tasks.

Operational Intelligence

Focus on driving operational intelligence using Splunk.

Capacity Management

Increase indexing capacity with additional licences without platform changes.

Data Retention

Increase data retention capability without increasing operating costs.

Version

Upgrade and remain up to date with latest advancements.

Missing

Splunk Cloud Considerations

Security

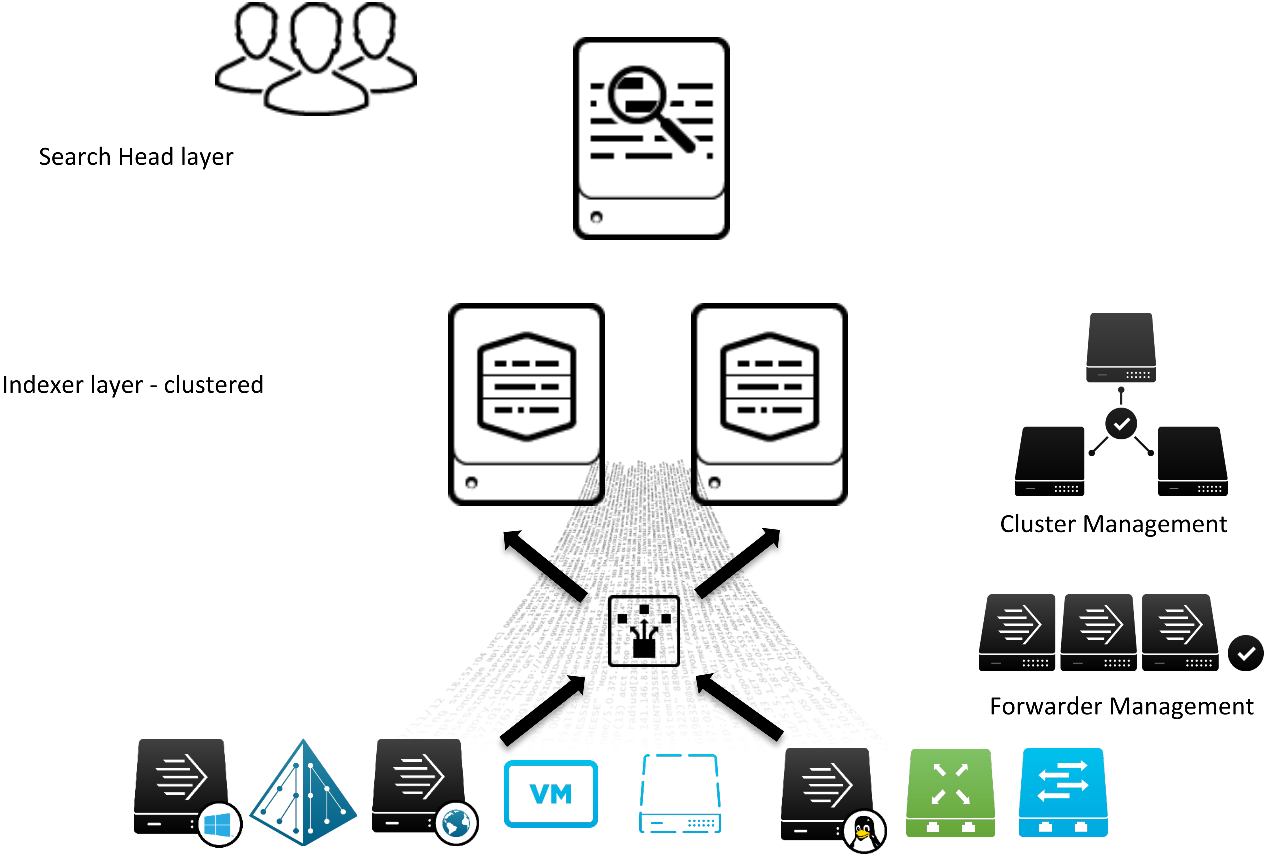
Governance

.conf2015

TECHNICAL DISCUSSION

splunk>

Before Cloud...



Search Head layer

Indexer layer - clustered

Cluster Management

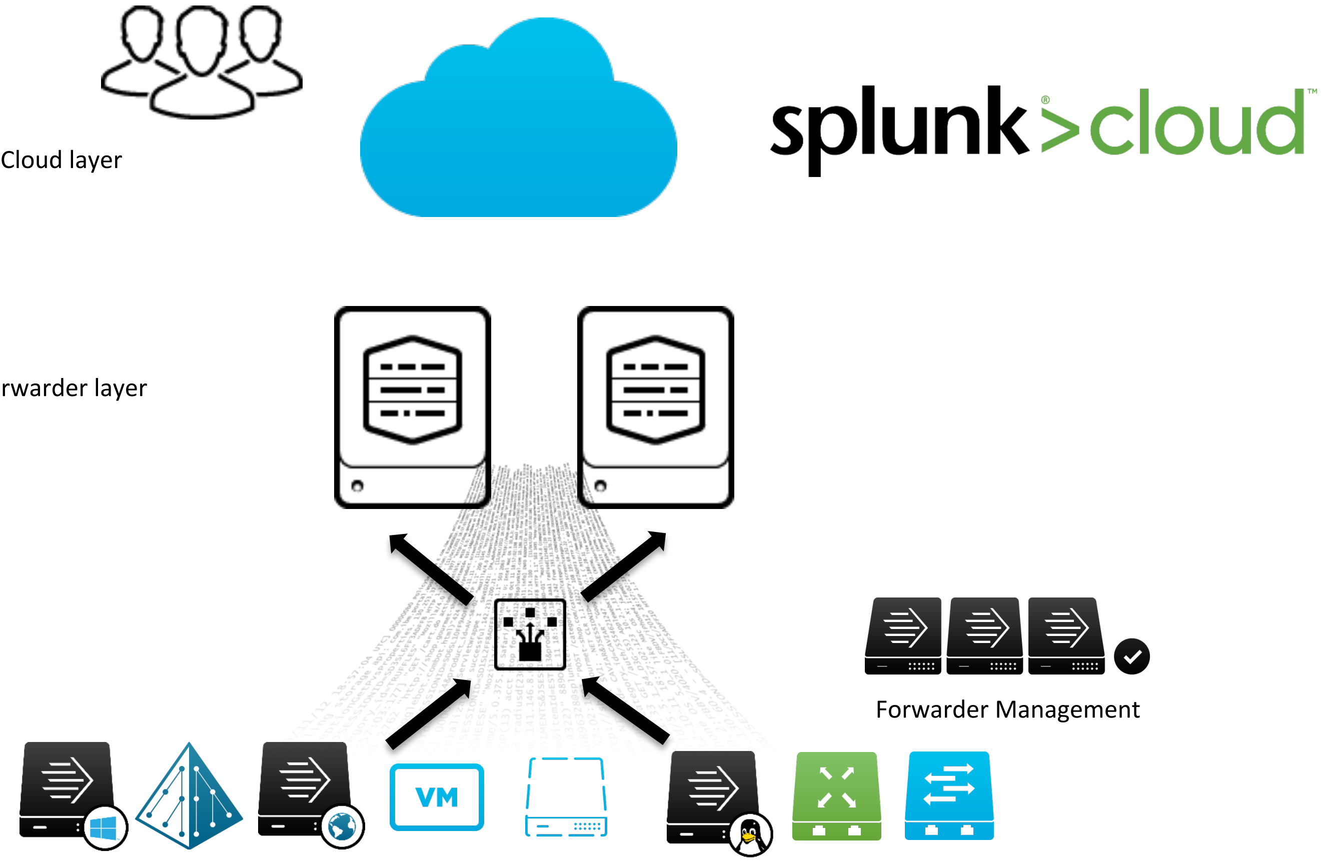
Forwarder Management

Data source/forwarder layer

Easy Migration Strategy

- Existing platform indexing most required data sources
- Leave existing data in current indexers and all new data sent to Cloud

With Cloud...



Splunk Cloud layer

Heavy forwarder layer

Forwarder Management

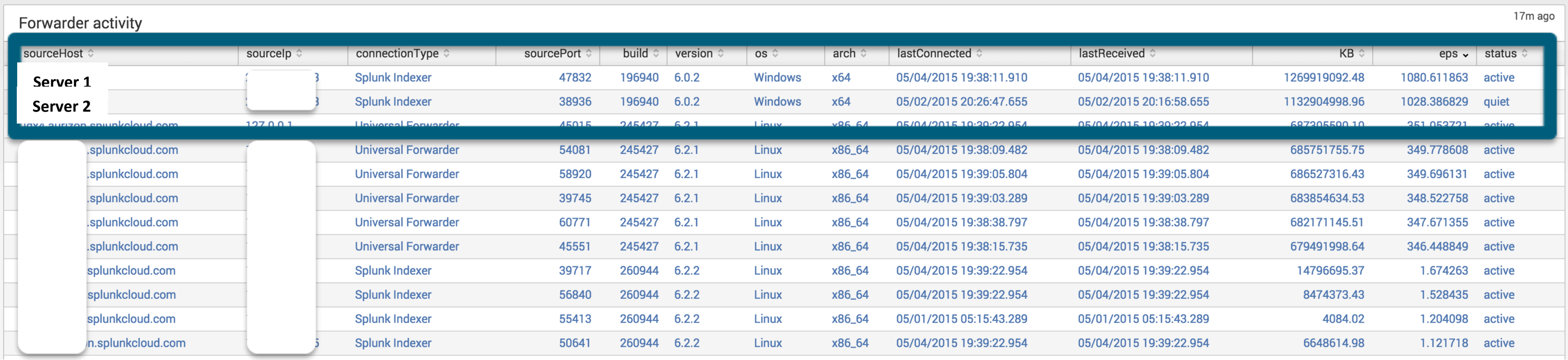
Data source/forwarder layer

A Word On Forwarders…

- Splunk Cloud Ops provision Forwarder App
  - Default Encrypted
  - Easy to install on forwarders
  - Splunk generated keyset
  - Auto load balancing across IDX

```
OUTPUTS.CONF

[tcpout]

defaultGroup = splunkcloud


[tcpout:splunkcloud]

server = inputs1.aurizon.splunkcloud.com:9996,
inputs2.aurizon.splunkcloud.com:9996, inputs3.aurizon.splunkcloud.com:9996,
inputs4.aurizon.splunkcloud.com:9996, inputs5.aurizon.splunkcloud.com:9996

compressed = false

sslCertPath = $SPLUNK_HOME/etc/auth/aurizon_server.pem

sslCommonNameToCheck = *.aurizon.splunkcloud.com

sslPassword = Not_Telling

sslRootCAPath = $SPLUNK_HOME/etc/auth/aurizon_cacert.pem

sslVerifyServerCert = true

useClientSSLCompression = true
```

Forwarders Details



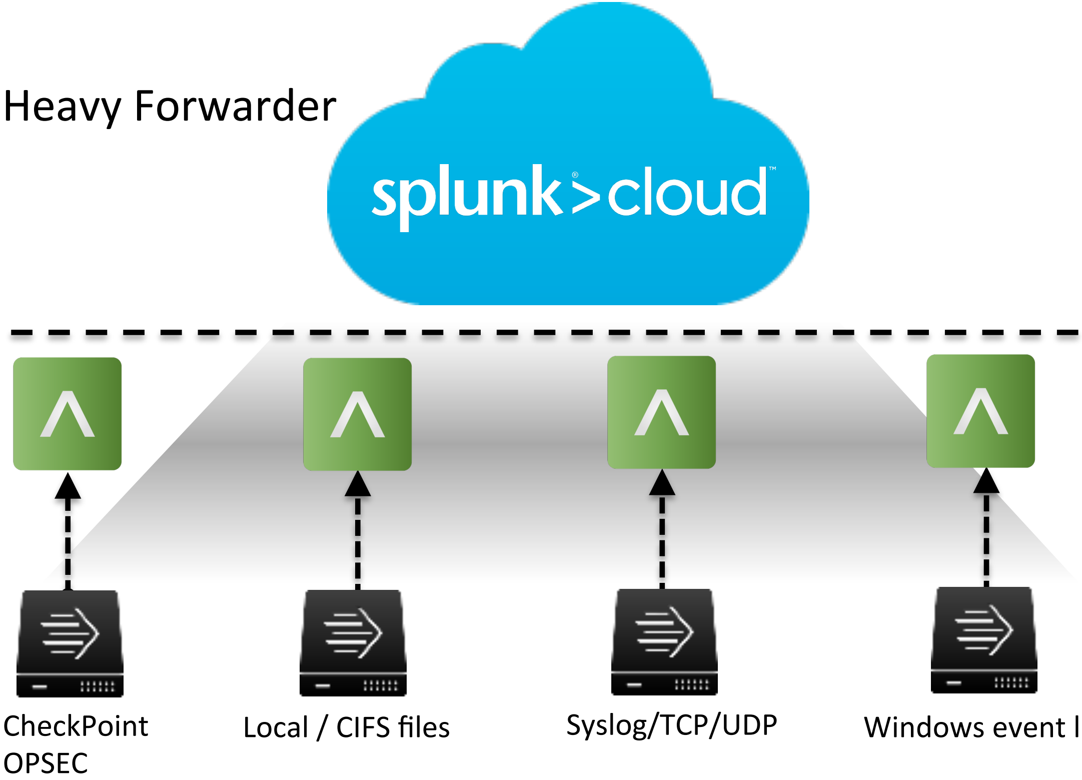
Forwarder activity

17m ago

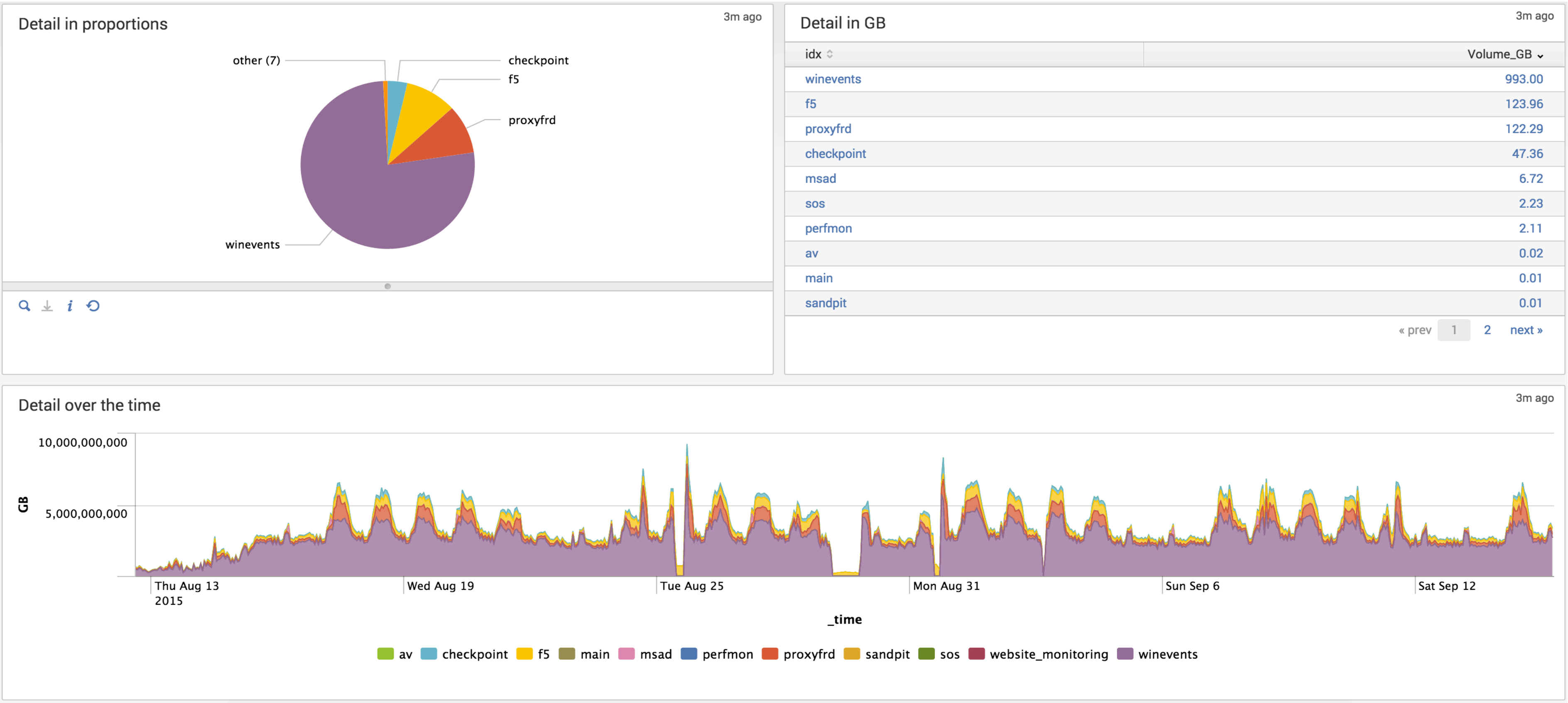
sourceHost	sourceIp	connectionType	sourcePort	build	version	os	arch	lastConnected	lastReceived	KB	eps	status
Server 1	[redacted]	Splunk Indexer	47832	196940	6.0.2	Windows	x64	05/04/2015 19:38:11.910	05/04/2015 19:38:11.910	1269919092.48	1080.611863	active
Server 2	[redacted]	Splunk Indexer	38936	196940	6.0.2	Windows	x64	05/02/2015 20:26:47.655	05/02/2015 20:16:58.655	1132904998.96	1028.386829	quiet
ugxq-aurizon.splunkcloud.com	127.0.0.1	Universal Forwarder	45015	245427	6.2.1	Linux	x86_64	05/04/2015 19:39:22.954	05/04/2015 19:39:22.954	687305590.10	351.053721	active
[redacted].splunkcloud.com	[redacted]	Universal Forwarder	54081	245427	6.2.1	Linux	x86_64	05/04/2015 19:38:09.482	05/04/2015 19:38:09.482	685751755.75	349.778608	active
[redacted].splunkcloud.com	[redacted]	Universal Forwarder	58920	245427	6.2.1	Linux	x86_64	05/04/2015 19:39:05.804	05/04/2015 19:39:05.804	686527316.43	349.696131	active
[redacted].splunkcloud.com	[redacted]	Universal Forwarder	39745	245427	6.2.1	Linux	x86_64	05/04/2015 19:39:03.289	05/04/2015 19:39:03.289	683854634.53	348.522758	active
[redacted].splunkcloud.com	[redacted]	Universal Forwarder	60771	245427	6.2.1	Linux	x86_64	05/04/2015 19:38:38.797	05/04/2015 19:38:38.797	682171145.51	347.671355	active
[redacted].splunkcloud.com	[redacted]	Universal Forwarder	45551	245427	6.2.1	Linux	x86_64	05/04/2015 19:38:15.735	05/04/2015 19:38:15.735	679491998.64	346.448849	active
[redacted]splunkcloud.com	[redacted]	Splunk Indexer	39717	260944	6.2.2	Linux	x86_64	05/04/2015 19:39:22.954	05/04/2015 19:39:22.954	14796695.37	1.674263	active
[redacted]splunkcloud.com	[redacted]	Splunk Indexer	56840	260944	6.2.2	Linux	x86_64	05/04/2015 19:39:22.954	05/04/2015 19:39:22.954	8474373.43	1.528435	active
[redacted]splunkcloud.com	[redacted]	Splunk Indexer	55413	260944	6.2.2	Linux	x86_64	05/01/2015 05:15:43.289	05/01/2015 05:15:43.289	4084.02	1.204098	active
[redacted]n.splunkcloud.com	[redacted]	Splunk Indexer	50641	260944	6.2.2	Linux	x86_64	05/04/2015 19:39:22.954	05/04/2015 19:39:22.954	6648614.98	1.121718	active

Aurizon – Data Inputs

- Universal or Heavy Forwarder



Data Sources Within Aurizon



Detail in proportions

3m ago

Detail in GB

3m ago

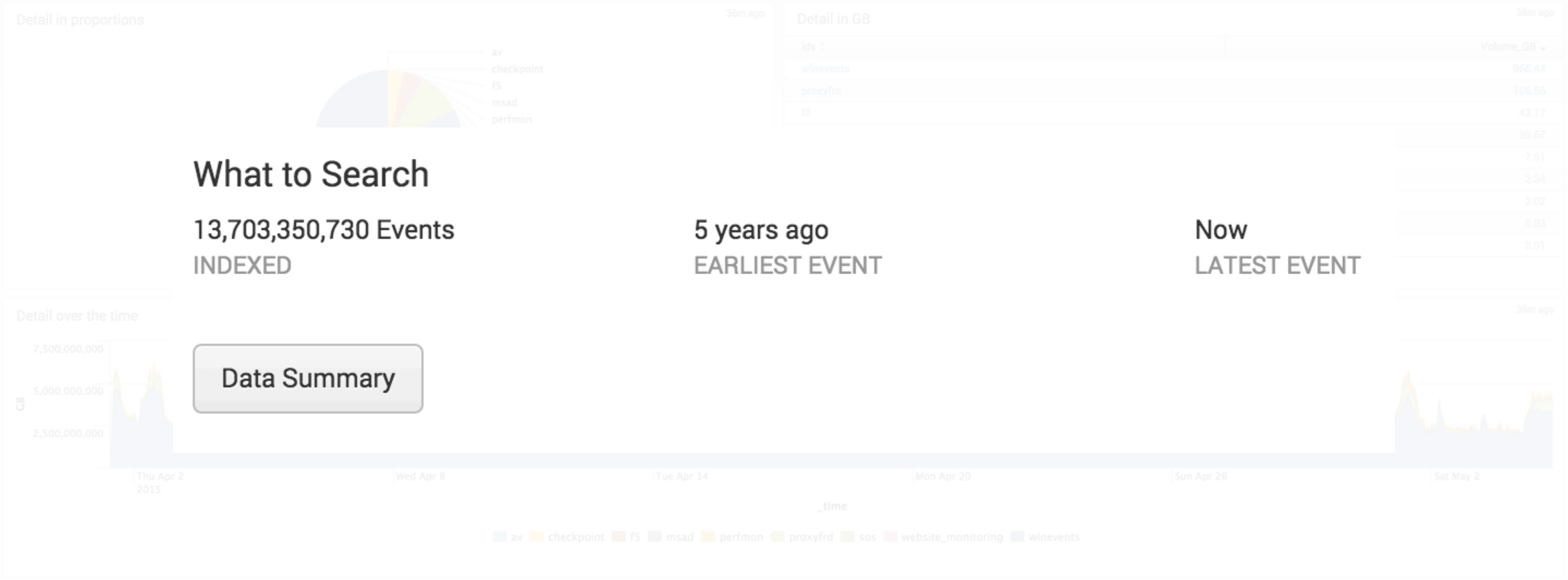
idx ⇕	Volume_GB ⌄
winevents	993.00
f5	123.96
proxyfrd	122.29
checkpoint	47.36
msad	6.72
sos	2.23
perfmon	2.11
av	0.02
main	0.01
sandpit	0.01

« prev 1 2 next »

Detail over the time

3m ago

Data Sources Within Aurizon



What to Search

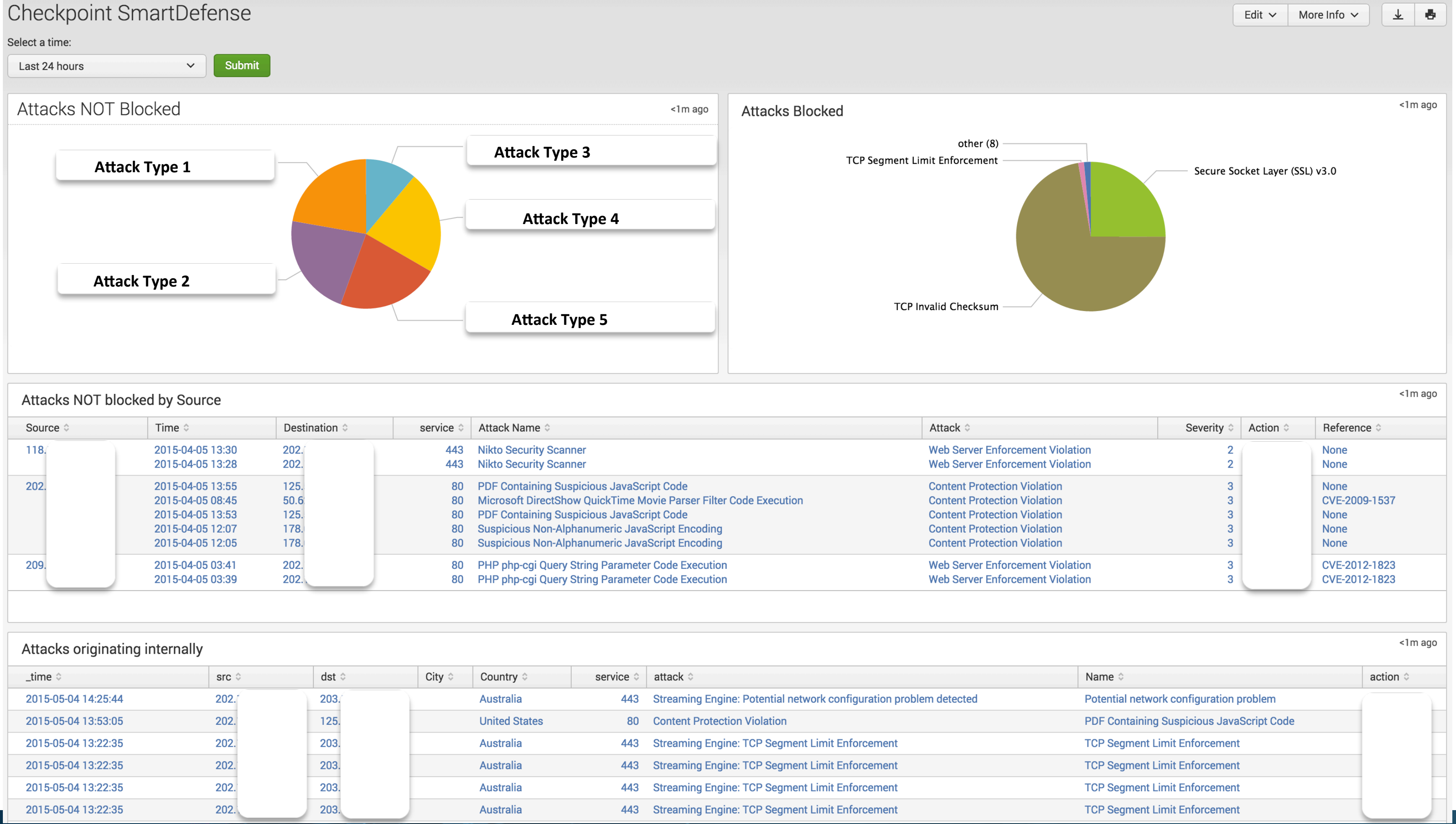
13,703,350,730 Events
INDEXED

5 years ago
EARLIEST EVENT

Now
LATEST EVENT

Data Summary

Example Dashboards



Checkpoint SmartDefense

Attacks NOT Blocked

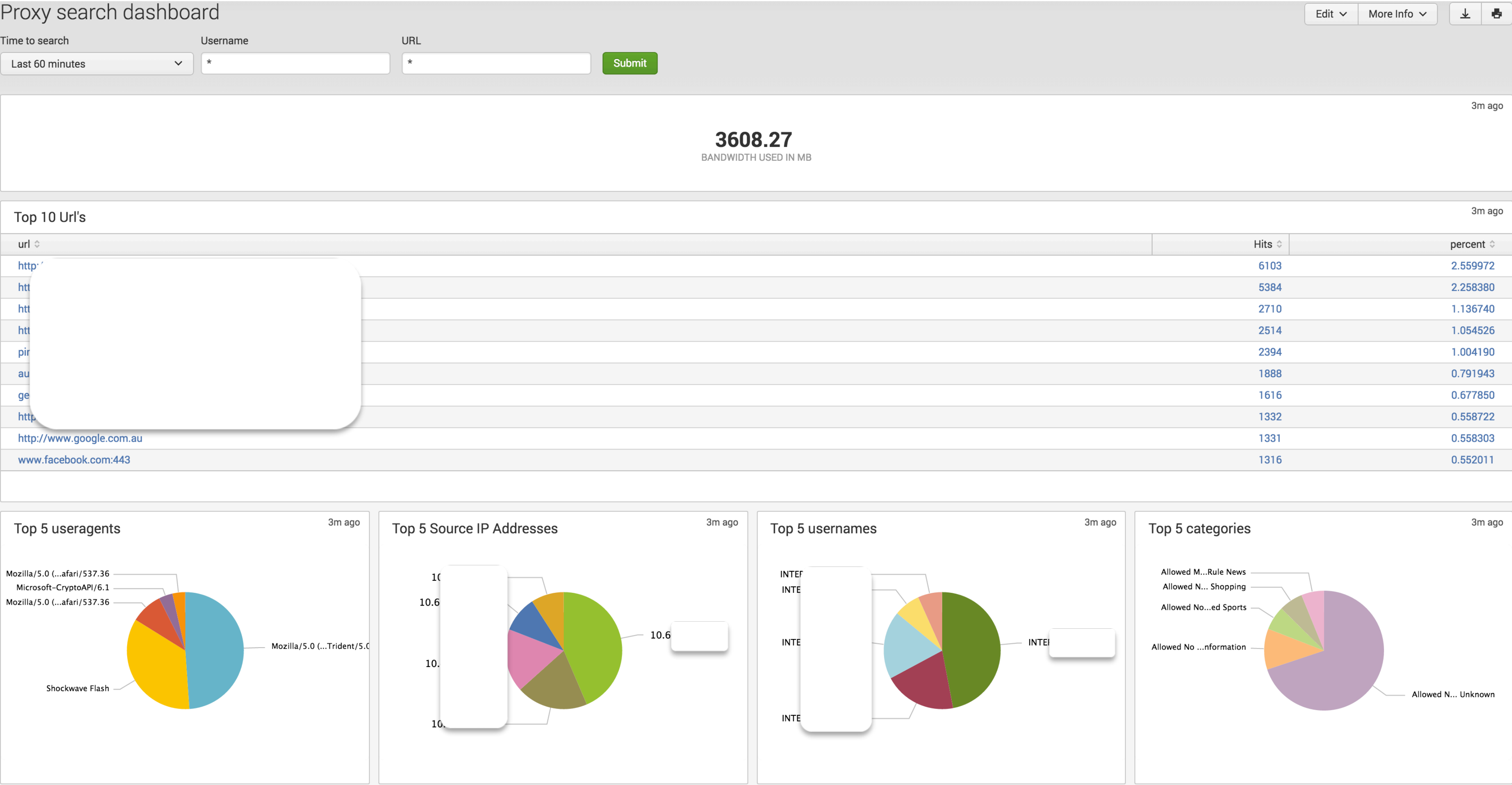
Attacks Blocked

Attacks NOT blocked by Source

Source	Time	Destination	service	Attack Name	Attack	Severity	Action	Reference
118.[redacted]	2015-04-05 13:30 2015-04-05 13:28	202.[redacted] 202.[redacted]	443 443	Nikto Security Scanner Nikto Security Scanner	Web Server Enforcement Violation Web Server Enforcement Violation	2 2	[redacted]	None None
202.[redacted]	2015-04-05 13:55 2015-04-05 08:45 2015-04-05 13:53 2015-04-05 12:07 2015-04-05 12:05	125.[redacted] 50.6[redacted] 125.[redacted] 178.[redacted] 178.[redacted]	80 80 80 80 80	PDF Containing Suspicious JavaScript Code Microsoft DirectShow QuickTime Movie Parser Filter Code Execution PDF Containing Suspicious JavaScript Code Suspicious Non-Alphanumeric JavaScript Encoding Suspicious Non-Alphanumeric JavaScript Encoding	Content Protection Violation Content Protection Violation Content Protection Violation Content Protection Violation Content Protection Violation	3 3 3 3 3	[redacted]	None CVE-2009-1537 None None None
209.[redacted]	2015-04-05 03:41 2015-04-05 03:39	202.[redacted] 202.[redacted]	80 80	PHP php-cgi Query String Parameter Code Execution PHP php-cgi Query String Parameter Code Execution	Web Server Enforcement Violation Web Server Enforcement Violation	3 3	[redacted]	CVE-2012-1823 CVE-2012-1823

Attacks originating internally

_time	src	dst	City	Country	service	attack	Name	action
2015-05-04 14:25:44	202.[redacted]	203.[redacted]		Australia	443	Streaming Engine: Potential network configuration problem detected	Potential network configuration problem	[redacted]
2015-05-04 13:53:05	202.[redacted]	125.[redacted]		United States	80	Content Protection Violation	PDF Containing Suspicious JavaScript Code	[redacted]
2015-05-04 13:22:35	202.[redacted]	203.[redacted]		Australia	443	Streaming Engine: TCP Segment Limit Enforcement	TCP Segment Limit Enforcement	[redacted]
2015-05-04 13:22:35	202.[redacted]	203.[redacted]		Australia	443	Streaming Engine: TCP Segment Limit Enforcement	TCP Segment Limit Enforcement	[redacted]
2015-05-04 13:22:35	202.[redacted]	203.[redacted]		Australia	443	Streaming Engine: TCP Segment Limit Enforcement	TCP Segment Limit Enforcement	[redacted]
2015-05-04 13:22:35	202.[redacted]	203.[redacted]		Australia	443	Streaming Engine: TCP Segment Limit Enforcement	TCP Segment Limit Enforcement	[redacted]



Proxy search dashboard

Edit More Info

Time to search: Last 60 minutes

Username: *

URL: *

Submit

3m ago

3608.27
BANDWIDTH USED IN MB

Top 10 Url's

3m ago

url	Hits	percent
[redacted]	6103	2.559972
[redacted]	5384	2.258380
[redacted]	2710	1.136740
[redacted]	2514	1.054526
[redacted]	2394	1.004190
[redacted]	1888	0.791943
[redacted]	1616	0.677850
[redacted]	1332	0.558722
http://www.google.com.au	1331	0.558303
www.facebook.com:443	1316	0.552011

Top 5 useragents

3m ago

Mozilla/5.0 (...afari/537.36
Microsoft-CryptoAPI/6.1
Mozilla/5.0 (...afari/537.36
Mozilla/5.0 (...Trident/5.0
Shockwave Flash

Top 5 Source IP Addresses

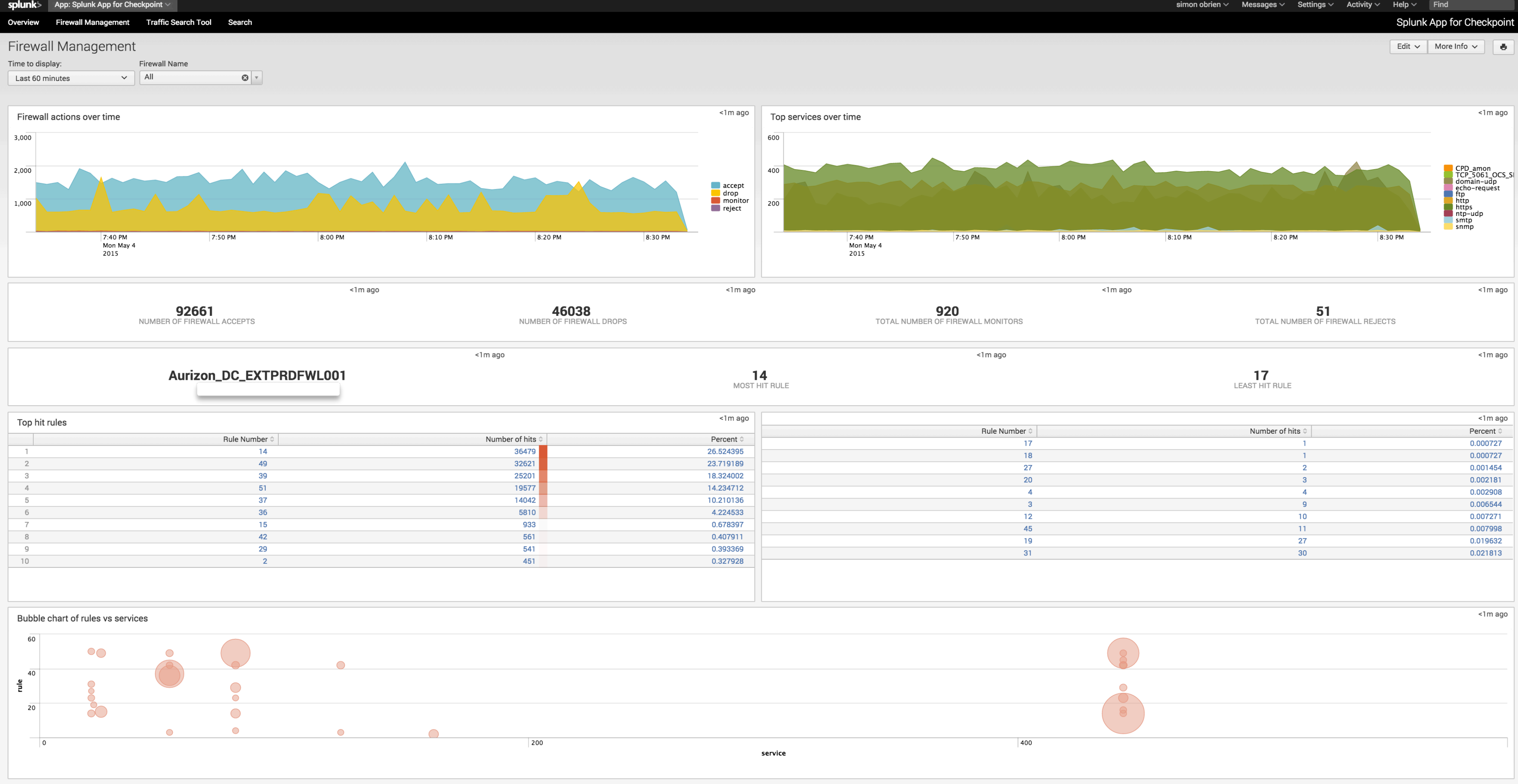
3m ago

Top 5 usernames

3m ago

Top 5 categories

3m ago



Firewall Management

Time to display: Last 60 minutes

Firewall Name: All

Firewall actions over time

Top services over time

92661 NUMBER OF FIREWALL ACCEPTS

46038 NUMBER OF FIREWALL DROPS

920 TOTAL NUMBER OF FIREWALL MONITORS

51 TOTAL NUMBER OF FIREWALL REJECTS

Aurizon_DC_EXTPRDFWL001

14 MOST HIT RULE

17 LEAST HIT RULE

Top hit rules

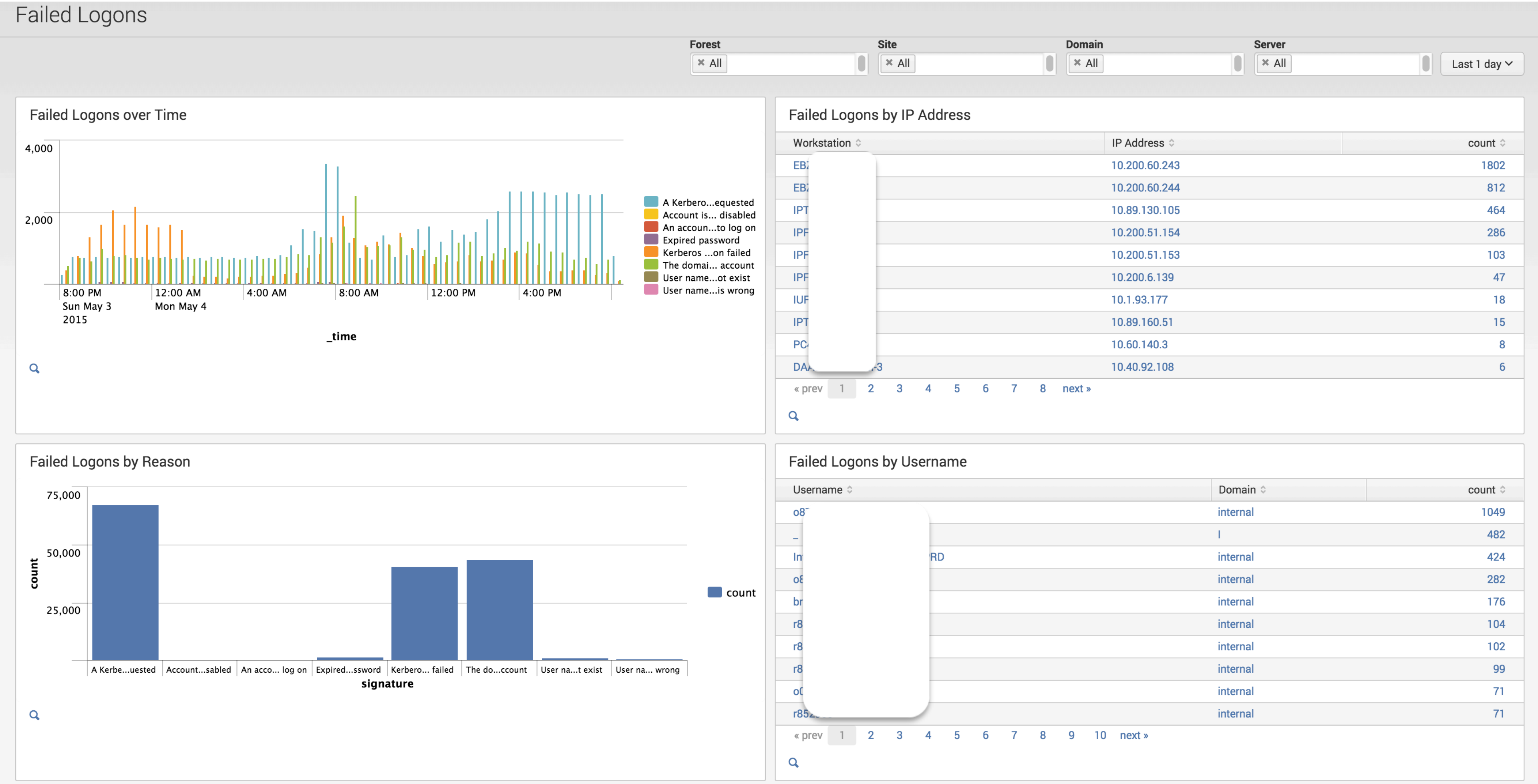
	Rule Number	Number of hits	Percent
1	14	36479	26.524395
2	49	32621	23.719189
3	39	25201	18.324002
4	51	19577	14.234712
5	37	14042	10.210136
6	36	5810	4.224533
7	15	933	0.678397
8	42	561	0.407911
9	29	541	0.393369
10	2	451	0.327928

Rule Number	Number of hits	Percent
17	1	0.000727
18	1	0.000727
27	2	0.001454
20	3	0.002181
4	4	0.002908
3	9	0.006544
12	10	0.007271
45	11	0.007998
19	27	0.019632
31	30	0.021813

Bubble chart of rules vs services

.conf2015

splunk>



Failed Logons

Failed Logons over Time

Failed Logons by IP Address

Workstation	IP Address	count
[redacted]	10.200.60.243	1802
[redacted]	10.200.60.244	812
[redacted]	10.89.130.105	464
[redacted]	10.200.51.154	286
[redacted]	10.200.51.153	103
[redacted]	10.200.6.139	47
[redacted]	10.1.93.177	18
[redacted]	10.89.160.51	15
[redacted]	10.60.140.3	8
[redacted]	10.40.92.108	6

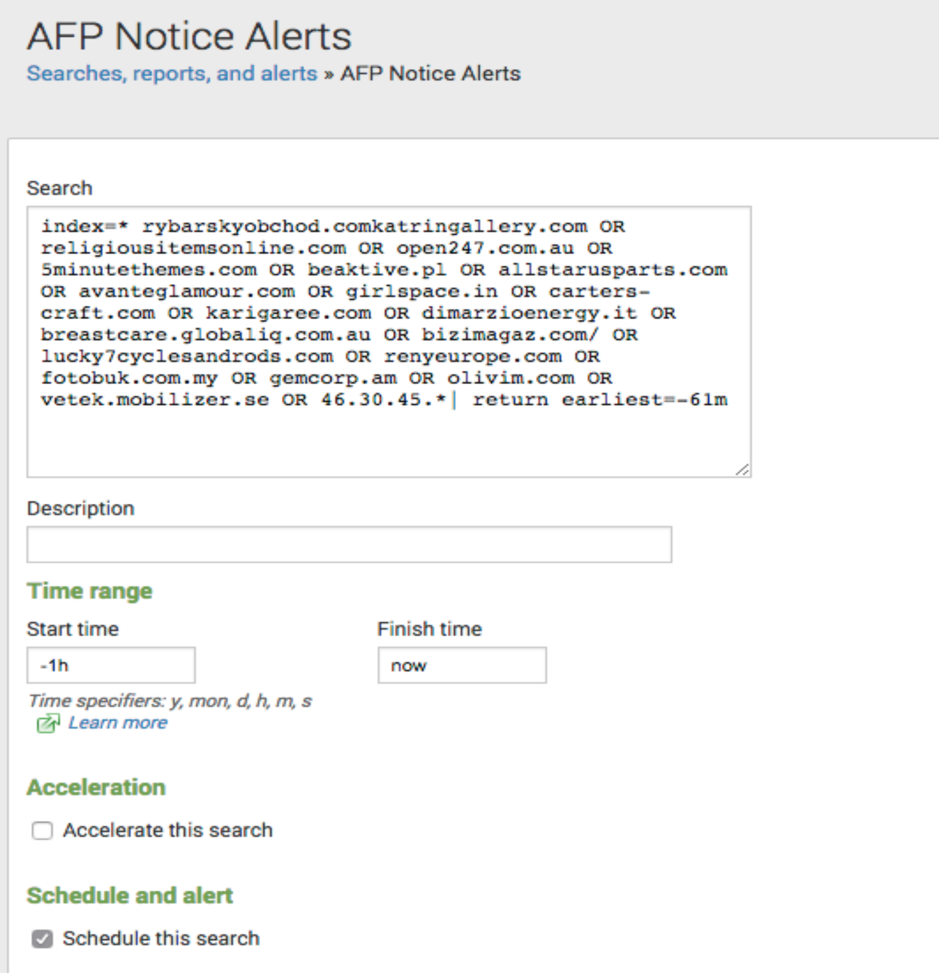
« prev 1 2 3 4 5 6 7 8 next »

Failed Logons by Reason

Failed Logons by Username

Username	Domain	count
[redacted]	internal	1049
[redacted]	l	482
[redacted]	internal	424
[redacted]	internal	282
[redacted]	internal	176
[redacted]	internal	104
[redacted]	internal	102
[redacted]	internal	99
[redacted]	internal	71
[redacted]	internal	71

« prev 1 2 3 4 5 6 7 8 9 10 next »



AFP Notice Alerts

Searches, reports, and alerts » AFP Notice Alerts

Search

```
index=* rybarskyobchod.comkatringallery.com OR
religiousitemsonline.com OR open247.com.au OR
5minutethemes.com OR beaktive.pl OR allstarusparts.com
OR avanteglamour.com OR girlspace.in OR carters-
craft.com OR karigaree.com OR dimarzioenergy.it OR
breastcare.globaliq.com.au OR bizimagaz.com/ OR
lucky7cyclesandrods.com OR renyeurope.com OR
fotobuk.com.my OR gemcorp.am OR olivim.com OR
vetek.mobilizer.se OR 46.30.45.*| return earliest=-61m
```

Description

Time range

Start time: -1h

Finish time: now

Time specifiers: y, mon, d, h, m, s

Learn more

Acceleration

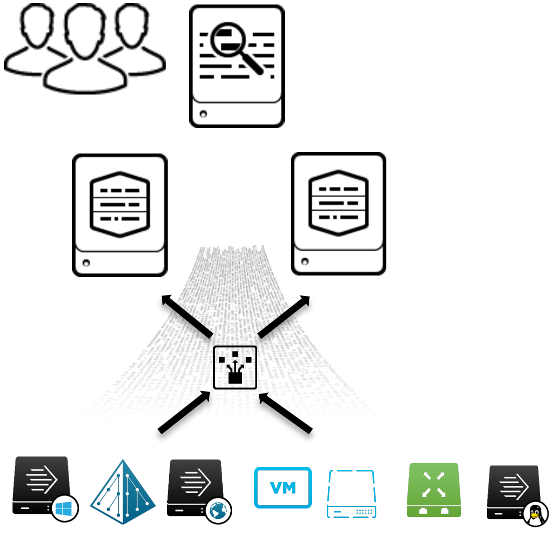
□ Accelerate this search

Schedule and alert

☑ Schedule this search

- Scheduled alerts in place
  - Based on IOC data coming from external sources, such as the Australian Federal Police
  - Mostly manual at this stage
  - Effective in mitigating and responding to a large range of attacks, particularly ransomware, cryptolocker

Where Is The Old Splunk?



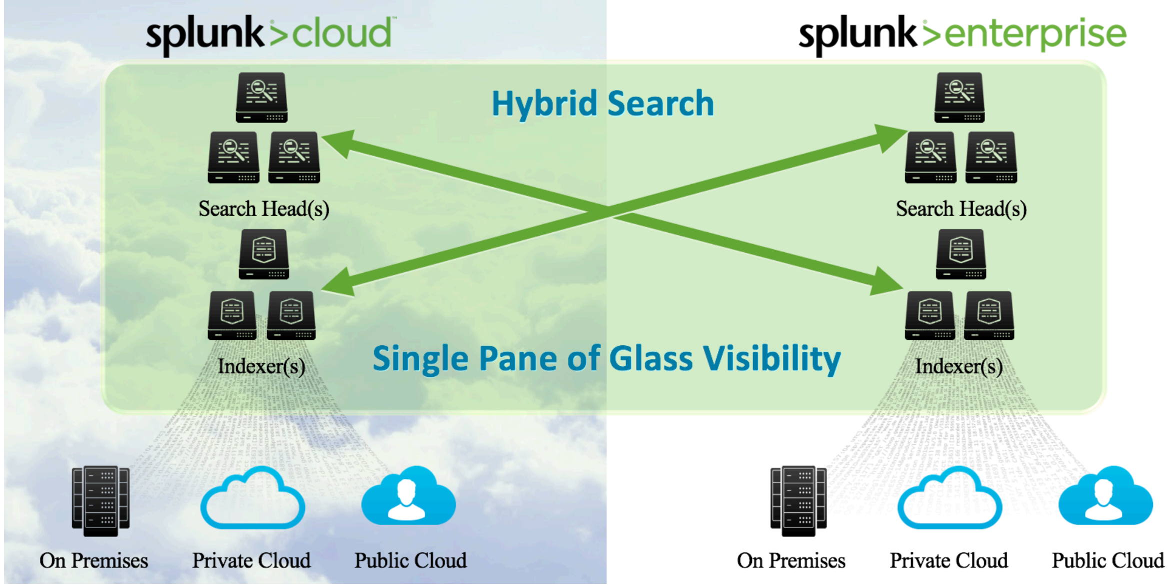
Data source/forwarder layer

A number of new data sources and protocols are available from the OT/SCADA environment.

Sensors
RFID
Telemetry data
Non standard Protocols

Since these data types are generated in a closed network with additional controls, we are utilising the on premise solution to capture and correlate logs.

Where Do I Search?



Hybrid search enables the analyst to conduct searches over the on premise and cloud solution. They can conduct their daily activity from one console seamlessly.

Setup straightforward and seamless, with a simple job to the Splunk support team.

What's Next At Aurizon?

- Improve the visibility into non-standard traffic
- Correlate events to see user & system activity end-to-end
- Augment existing monitoring technologies with Splunk
- Provide OT/SCADA engineers a new platform where they can visualize events in IT & OT networks
- Provide the Security Team real time alert correlation across IT & OT

.conf2015

THANK YOU

splunk>®