Building a Cyber Security Program

With Splunk App for Enterprise Security

Jeff Campbell

CISSP+ISSAP, Splunk Certified Architect

Cyber Security | Splunk Architect

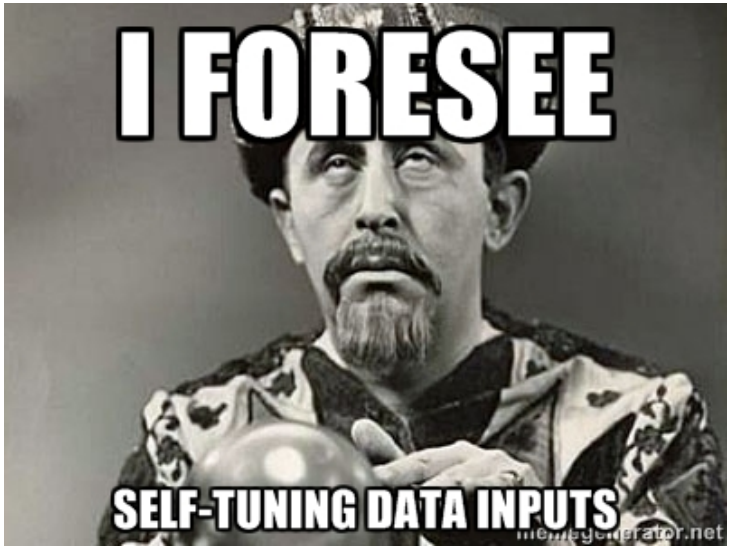
Penn State Hershey Medical Center

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.

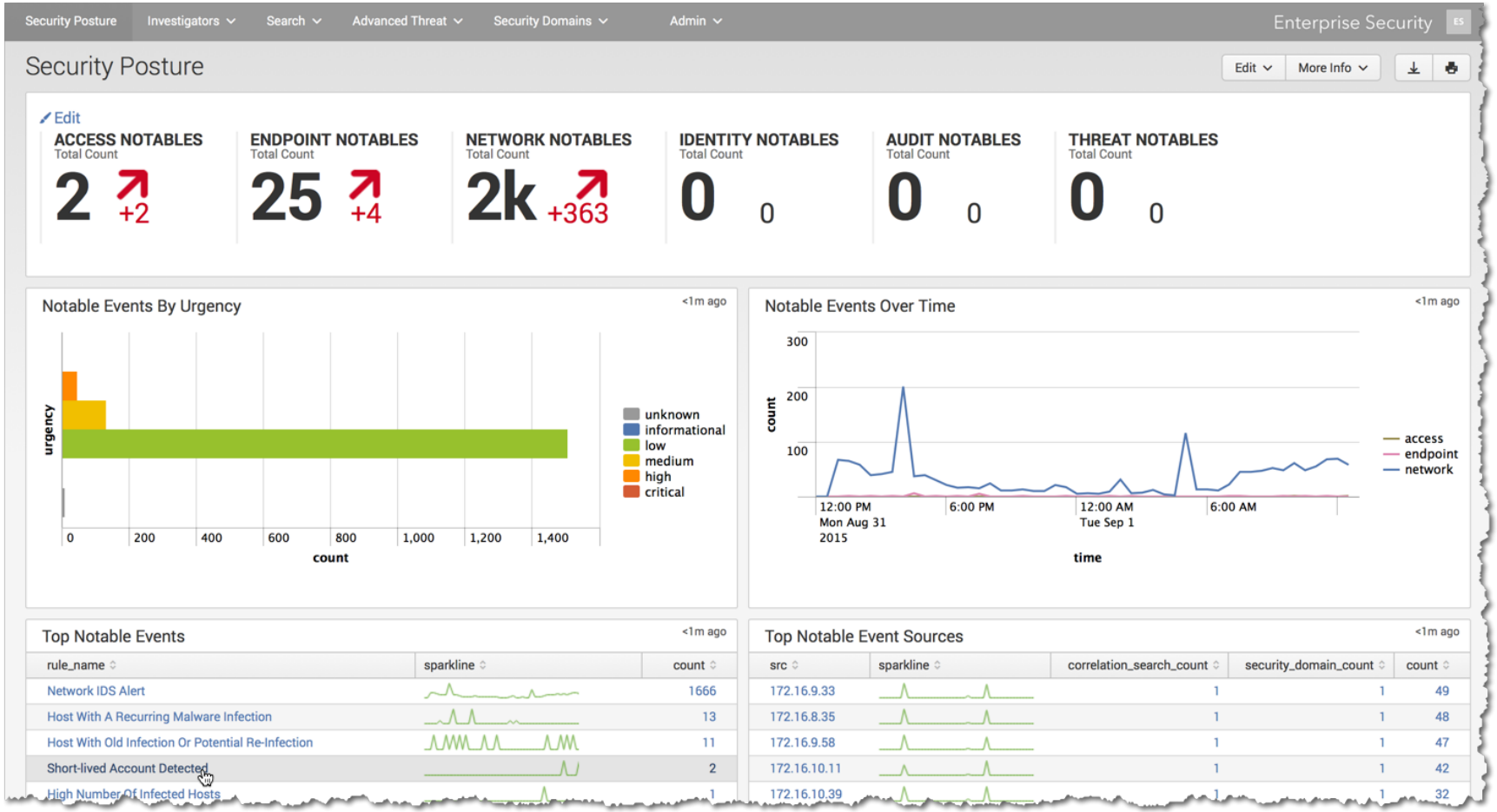


Jeff Campbell

- Focus shift towards Cyber
- More people w/specialization
- New tech

- More data!

http://bit.ly/psh-jobs
keyword: cyber


Security Posture
Investigators
Search
Advanced Threat
Security Domains
Admin
Enterprise Security
Security Posture
Edit
More Info
Edit
ACCESS NOTABLES
Total Count
2
+2
ENDPOINT NOTABLES
Total Count
25
+4
NETWORK NOTABLES
Total Count
2k
+363
IDENTITY NOTABLES
Total Count
0
0
AUDIT NOTABLES
Total Count
0
0
THREAT NOTABLES
Total Count
0
0
Notable Events By Urgency
<1m ago
urgency
0
200
400
600
800
1,000
1,200
1,400
count
unknown
informational
low
medium
high
critical
Notable Events Over Time
<1m ago
300
200
100
count
12:00 PM
Mon Aug 31
2015
6:00 PM
12:00 AM
Tue Sep 1
6:00 AM
time
access
endpoint
network
Top Notable Events
<1m ago
rule_name
sparkline
count
Network IDS Alert
1666
Host With A Recurring Malware Infection
13
Host With Old Infection Or Potential Re-Infection
11
Short-lived Account Detected
2
High Number Of Infected Hosts
1
Top Notable Event Sources
<1m ago
src
sparkline
correlation_search_count
security_domain_count
count
172.16.9.33
1
1
49
172.16.8.35
1
1
48
172.16.9.58
1
1
47
172.16.10.11
1
1
42
172.16.10.39
1
1
32


tag=network
tag=communicate

Dedicated Search Head

16 CPU cores

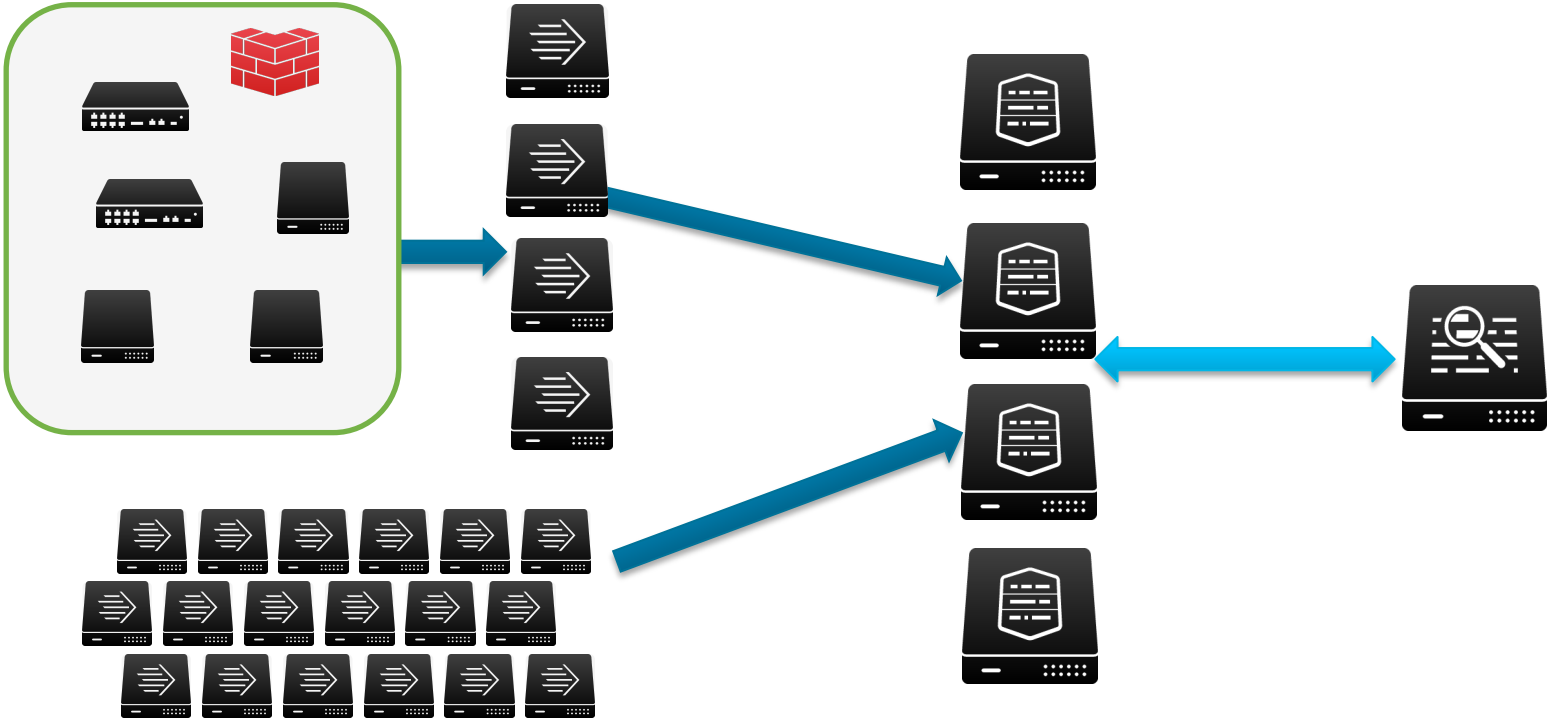
16 GB RAM

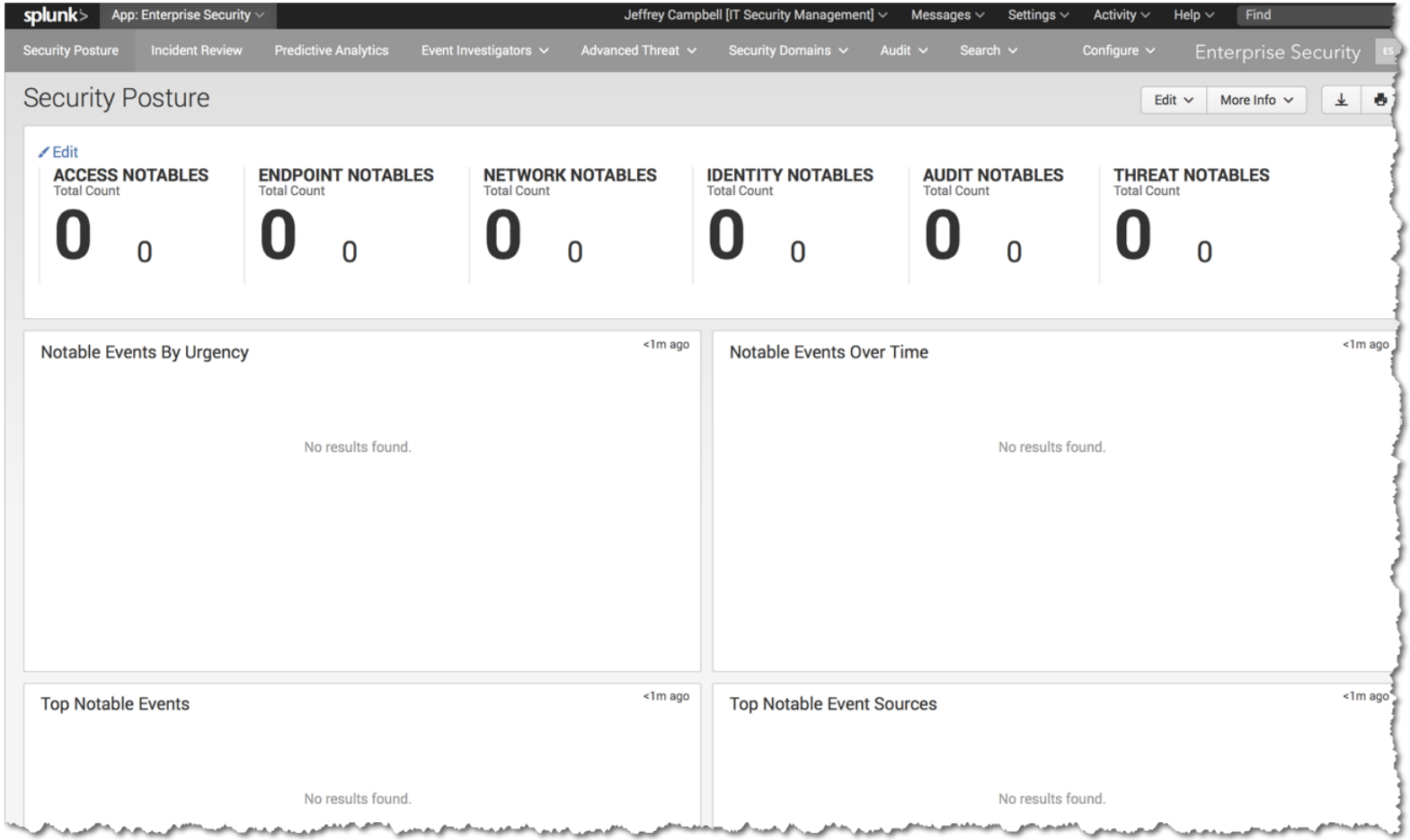
Indexers

1 per 100 GB indexed

review the online documentation
@ docs.splunk.com

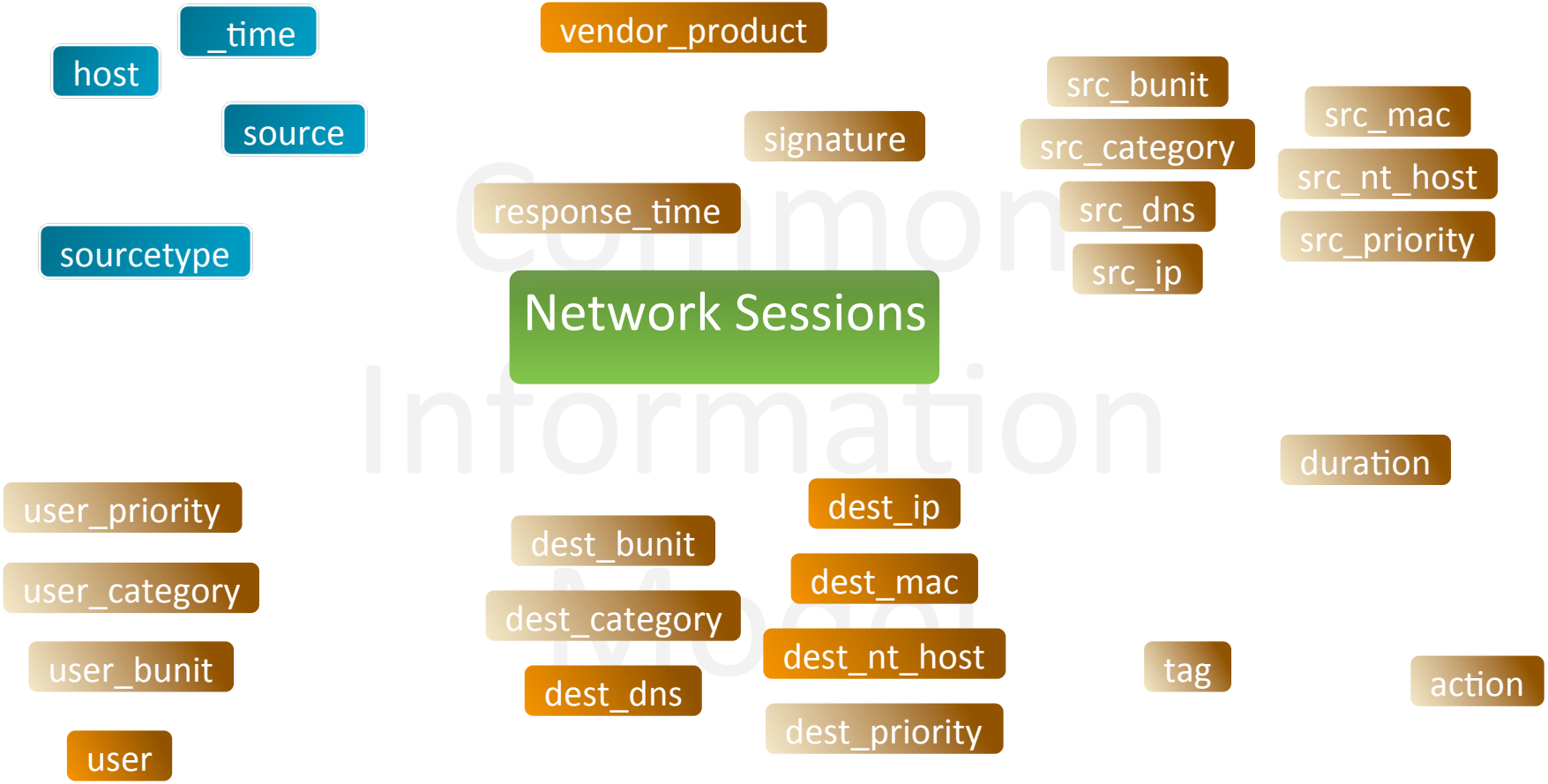
Documentation > Splunk App for Enterprise Security >
Installation and Configuration Manual >
Splunk Enterprise deployment planning




splunk> App: Enterprise Security
Jeffrey Campbell [IT Security Management]
Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Predictive Analytics
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Security Posture
Edit
More Info
Edit
ACCESS NOTABLES
Total Count
0 0
ENDPOINT NOTABLES
Total Count
0 0
NETWORK NOTABLES
Total Count
0 0
IDENTITY NOTABLES
Total Count
0 0
AUDIT NOTABLES
Total Count
0 0
THREAT NOTABLES
Total Count
0 0
Notable Events By Urgency
<1m ago
No results found.
Notable Events Over Time
<1m ago
No results found.
Top Notable Events
<1m ago
No results found.
Top Notable Event Sources
<1m ago
No results found.

- Identity Data
  - Active Directory
  - Exchange
  - Identity Management

- Asset Data
  - Asset & Inventory Management
  - Configuration Management
  - Data Center Management System


_time
host
source
sourcetype
vendor_product
signature
response_time
src_bunit
src_category
src_dns
src_ip
src_mac
src_nt_host
src_priority
Network Sessions
duration
user_priority
user_category
user_bunit
user
dest_bunit
dest_category
dest_dns
dest_ip
dest_mac
dest_nt_host
dest_priority
tag
action

Alerts
tag=alert

JVM
tag=jvm

Certificates
tag=certificate

Performance
tag=performance

Web
tag=web

Application State
(tag=listening tag=port) OR (tag=process tag=report) OR (tag=service tag=report)

Change Analysis
tag=change

Network Resolution (DNS)
tag=network tag=resolution tag=dns

Network Sessions
tag=network tag=session

Malware
tag=malware tag=attack

Interprocess Messaging
tag=messaging

Intrusion Detection
tag=ids tag=attack

Updates
tag=update tag=status

Vulnerabilities
tag=vulnerability tag=report

Network Traffic
tag=network tag=communicate

Inventory
tag=inventory

Email
tag=email

Ticket Management
tag=ticketing

Database
tag=database

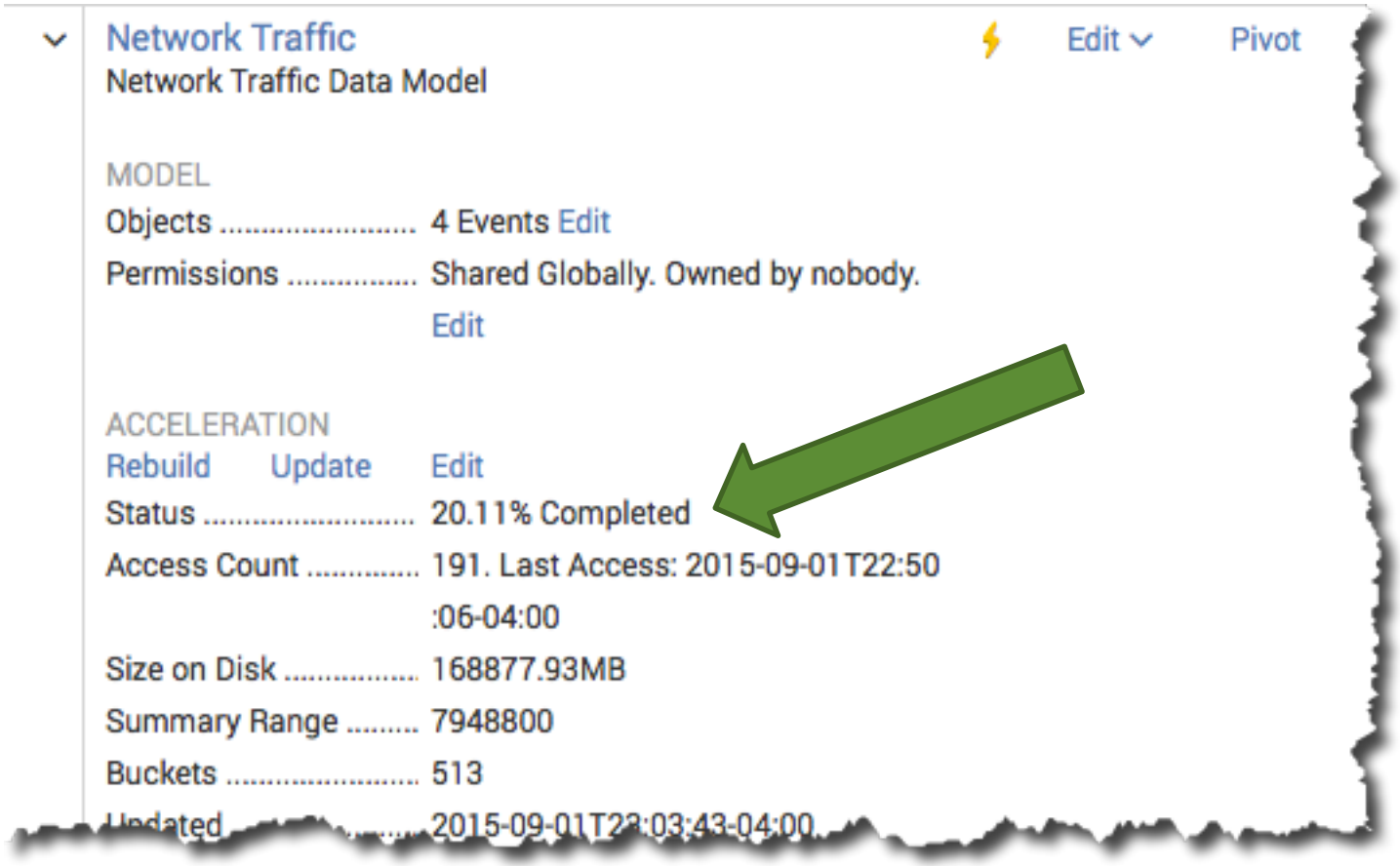
Authentication
tag=authentication NOT (action=success user=*$)

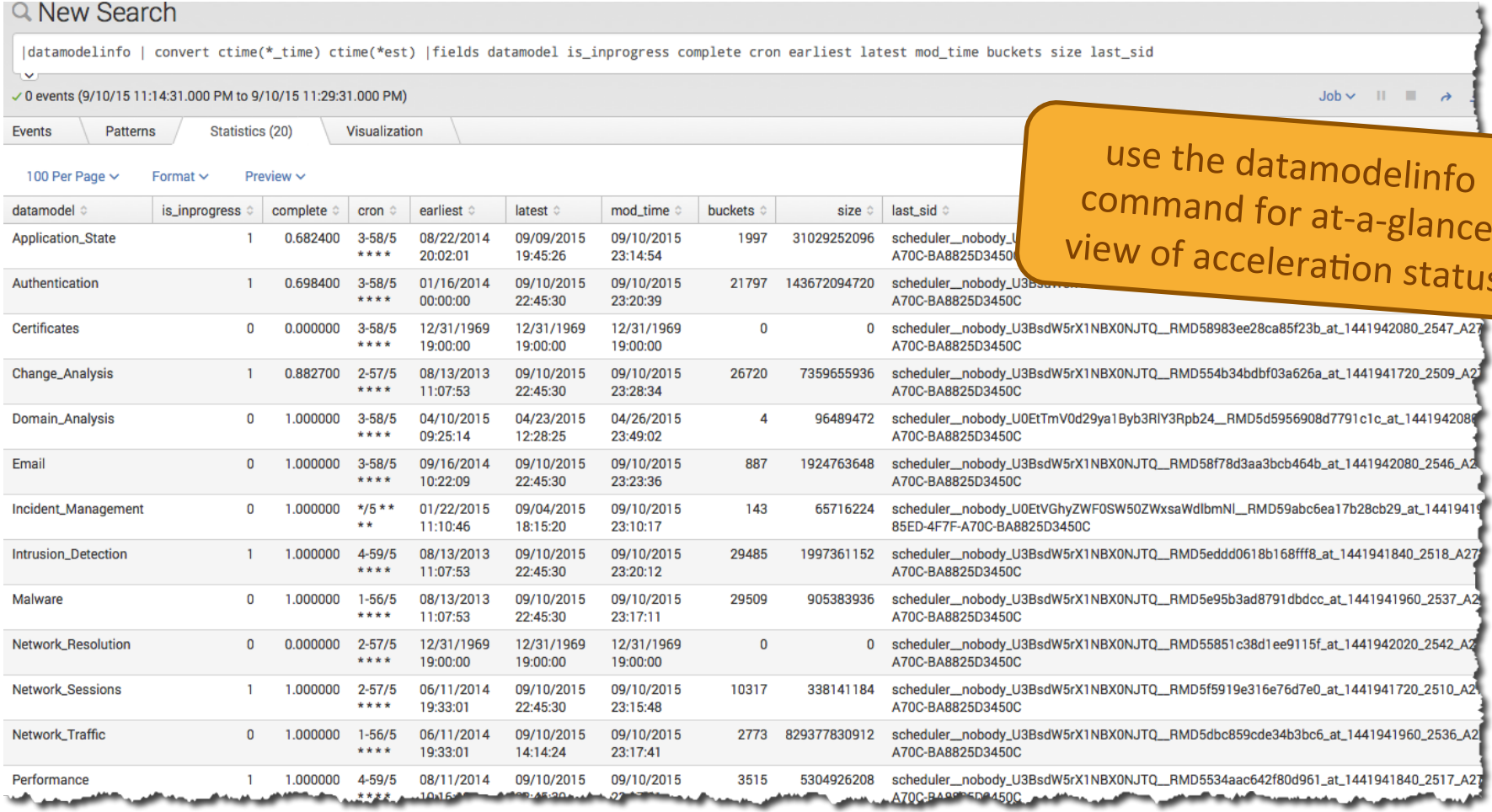
tag=network tag=communicate

modifiedTime	2015-09-01T14:22:04.503-04:00
normalizedSearch	litsearch ((((sourcetype=DhcpSrvLog)) OR ((index=firewall sourcetype="cisco:*" ((((sourcetype="cisco:asa") AND ((((((sourcetype="cisco:wsa") AND ((sc_result_code=built))) OR ((sourcetype="cisco:wsa:squid") AND ((txn_result_code=built))) OR ((sourcetype="cisco:wsa:w3c") AND ((sc_result_code=built))) OR ((sourcetype=fs_notification) AND ((action=built))) OR ((sourcetype=pan_config) AND ((command=built))) OR ((sourcetype=pan_threat) AND ((action=built))) OR ((sourcetype=pan_traffic) AND ((action=built)))) OR (vendor_action=built))) OR (((((sourcetype="cisco:wsa") AND ((sc_result_code=Built))) OR ((sourcetype="cisco:wsa:squid") AND ((txn_result_code=Built))) OR ((sourcetype="cisco:wsa:w3c") AND ((sc_result_code=Built))) OR ((sourcetype=fs_notification) AND ((action=Built))) OR ((sourcetype=pan_config) AND ((command=Built))) OR ((sourcetype=pan_threat) AND ((action=Built))) OR ((sourcetype=pan_traffic) AND ((action=Built)))) OR (vendor_action=Built))) OR (((((sourcetype="cisco:wsa") AND ((sc_result_code=Permitted))) OR ((sourcetype="cisco:wsa:squid") AND ((txn_result_code=Permitted))) OR ((sourcetype="cisco:wsa:w3c") AND ((sc_result_code=Permitted))) OR ((sourcetype=fs_notification) AND ((action=Permitted))

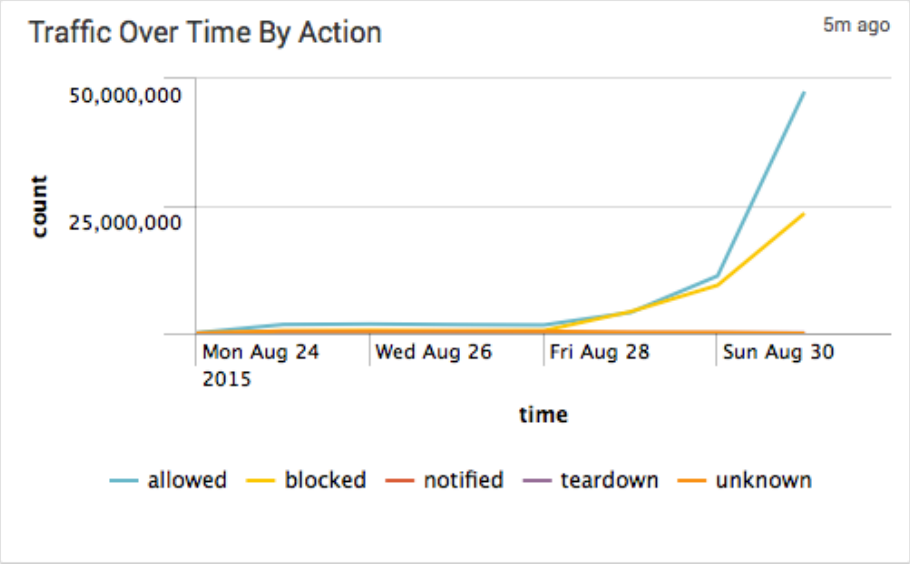
- - - 3000 lines later - - -

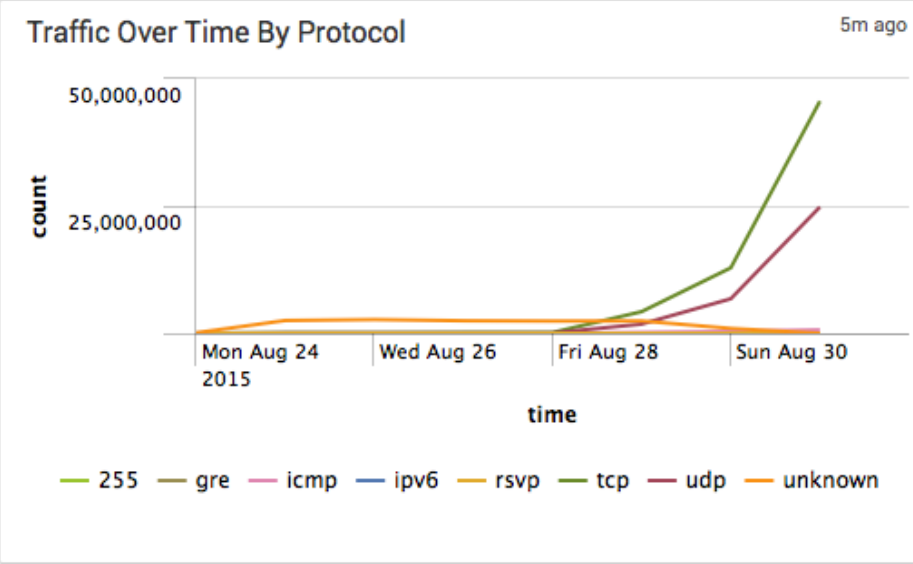
	tcp_flag AS All_Traffic.tcp_flag tos AS All_Traffic.tos ttl AS All_Traffic.ttl user_bunit AS All_Traffic.user_bunit user_category AS All_Traffic.user_category user_priority AS All_Traffic.user_priority vlan AS All_Traffic.vlan wifi AS All_Traffic.wifi action AS All_Traffic.action bytes AS All_Traffic.bytes bytes_in AS All_Traffic.bytes_in bytes_out AS All_Traffic.bytes_out dest AS All_Traffic.dest dest_port AS All_Traffic.dest_port dvc AS All_Traffic.dvc packets AS All_Traffic.packets packets_in AS All_Traffic.packets_in packets_out AS All_Traffic.packets_out rule AS All_Traffic.rule src AS All_Traffic.src src_port AS All_Traffic.src_port transport AS All_Traffic.transport user AS All_Traffic.user vendor_product AS All_Traffic.vendor_product is_Traffic_By_Action AS All_Traffic.is_Traffic_By_Action is_not_Traffic_By_Action AS All_Traffic.is_not_Traffic_By_Action | fields keepcolorder=t "*" "_bkt" "_cd" "_si" "host" "index" "linecount" "source" "sourcetype" "splunk_server" | remotetl nb=300 et=1441130794.000000 lt=1441131694.000000 remove=true max_count=1000 max_prefetch=100
numPreviews	6
pid	84275

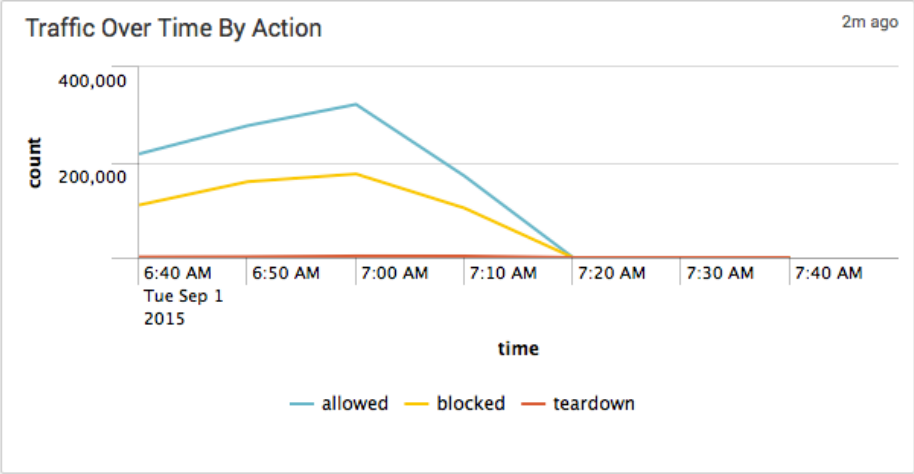

Network Traffic
Edit
Pivot
Network Traffic Data Model
MODEL
Objects ..... 4 Events Edit
Permissions ..... Shared Globally. Owned by nobody.
Edit
ACCELERATION
Rebuild Update Edit
Status ..... 20.11% Completed
Access Count ..... 191. Last Access: 2015-09-01T22:50
:06-04:00
Size on Disk 168877.93MB
Summary Range 7948800
Buckets 513
Updated 2015-09-01T22:03:43-04:00

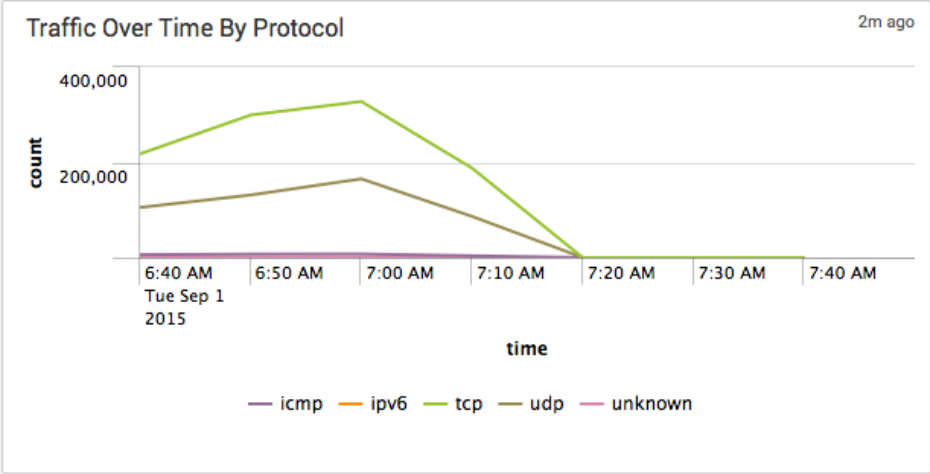


datamodel	is_inprogress	complete	cron	earliest	latest	mod_time	buckets	size	last_sid
Application_State	1	0.682400	3-58/5 * * * *	08/22/2014 20:02:01	09/09/2015 19:45:26	09/10/2015 23:14:54	1997	31029252096	scheduler__nobody_U... A70C-BA8825D3450
Authentication	1	0.698400	3-58/5 * * * *	01/16/2014 00:00:00	09/10/2015 22:45:30	09/10/2015 23:20:39	21797	143672094720	scheduler__nobody_U3Bs... A70C-BA8825D3450C
Certificates	0	0.000000	3-58/5 * * * *	12/31/1969 19:00:00	12/31/1969 19:00:00	12/31/1969 19:00:00	0	0	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD58983ee28ca85f23b_at_1441942080_2547_A27 A70C-BA8825D3450C
Change_Analysis	1	0.882700	2-57/5 * * * *	08/13/2013 11:07:53	09/10/2015 22:45:30	09/10/2015 23:28:34	26720	7359655936	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD554b34bdbf03a626a_at_1441941720_2509_A2 A70C-BA8825D3450C
Domain_Analysis	0	1.000000	3-58/5 * * * *	04/10/2015 09:25:14	04/23/2015 12:28:25	04/26/2015 23:49:02	4	96489472	scheduler__nobody_U0EtTmV0d29ya1Byb3RlY3Rpb24__RMD5d5956908d7791c1c_at_144194208 A70C-BA8825D3450C
Email	0	1.000000	3-58/5 * * * *	09/16/2014 10:22:09	09/10/2015 22:45:30	09/10/2015 23:23:36	887	1924763648	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD58f78d3aa3bcb464b_at_1441942080_2546_A2 A70C-BA8825D3450C
Incident_Management	0	1.000000	*/5 * * * *	01/22/2015 11:10:46	09/04/2015 18:15:20	09/10/2015 23:10:17	143	65716224	scheduler__nobody_U0EtVGhyZWF0SW50ZWxsaWdlbmNl__RMD59abc6ea17b28cb29_at_14419419 85ED-4F7F-A70C-BA8825D3450C
Intrusion_Detection	1	1.000000	4-59/5 * * * *	08/13/2013 11:07:53	09/10/2015 22:45:30	09/10/2015 23:20:12	29485	1997361152	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD5eddd0618b168fff8_at_1441941840_2518_A27 A70C-BA8825D3450C
Malware	0	1.000000	1-56/5 * * * *	08/13/2013 11:07:53	09/10/2015 22:45:30	09/10/2015 23:17:11	29509	905383936	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD5e95b3ad8791dbdcc_at_1441941960_2537_A2 A70C-BA8825D3450C
Network_Resolution	0	0.000000	2-57/5 * * * *	12/31/1969 19:00:00	12/31/1969 19:00:00	12/31/1969 19:00:00	0	0	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD55851c38d1ee9115f_at_1441942020_2542_A2 A70C-BA8825D3450C
Network_Sessions	1	1.000000	2-57/5 * * * *	06/11/2014 19:33:01	09/10/2015 22:45:30	09/10/2015 23:15:48	10317	338141184	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD5f5919e316e76d7e0_at_1441941720_2510_A2 A70C-BA8825D3450C
Network_Traffic	0	1.000000	1-56/5 * * * *	06/11/2014 19:33:01	09/10/2015 14:14:24	09/10/2015 23:17:41	2773	829377830912	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD5dbc859cde34b3bc6_at_1441941960_2536_A2 A70C-BA8825D3450C
Performance	1	1.000000	4-59/5 * * * *	08/11/2014 10:16...	09/10/2015 ...	09/10/2015 ...	3515	5304926208	scheduler__nobody_U3BsdW5rX1NBX0NJTQ__RMD5534aac642f80d961_at_1441941840_2517_A27 A70C-BA8825D3450C


Traffic Over Time By Action
5m ago
50,000,000
25,000,000
count
Mon Aug 24
2015
Wed Aug 26
Fri Aug 28
Sun Aug 30
time
allowed
blocked
notified
teardown
unknown

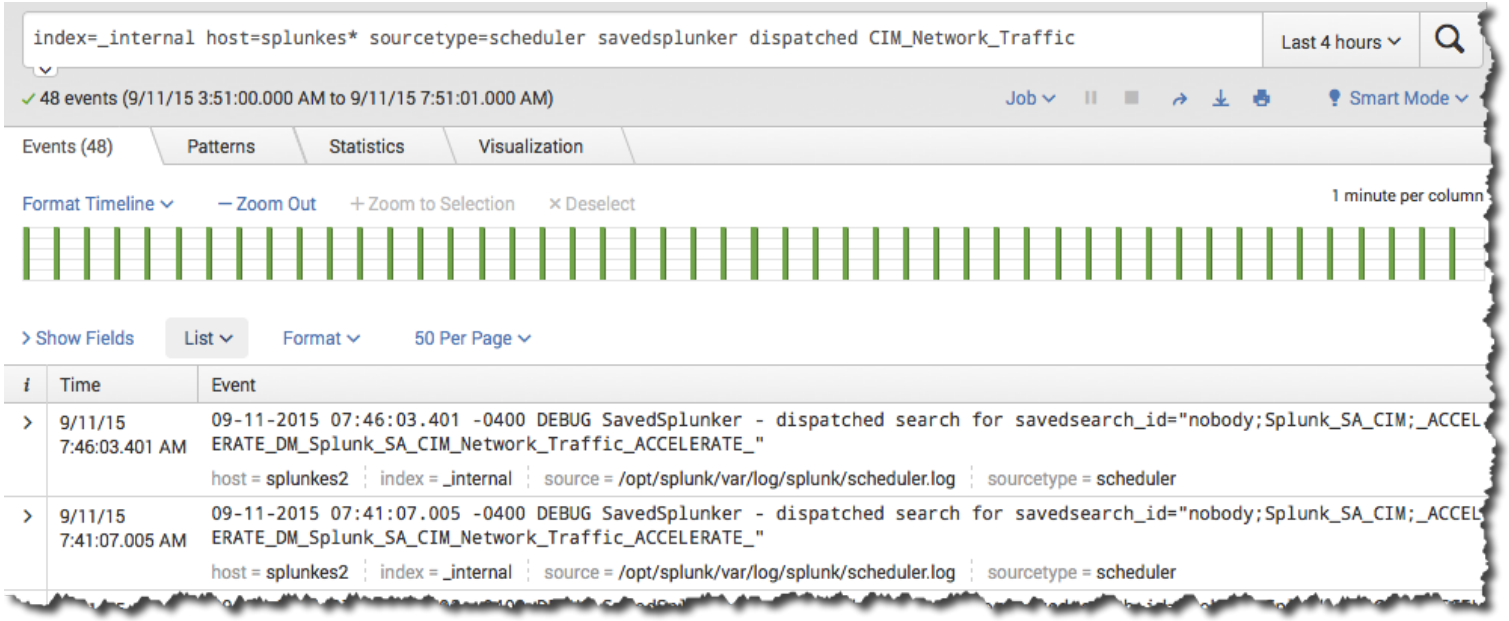

Traffic Over Time By Protocol
5m ago
50,000,000
25,000,000
count
Mon Aug 24
2015
Wed Aug 26
Fri Aug 28
Sun Aug 30
time
255
gre
icmp
ipv6
rsvp
tcp
udp
unknown

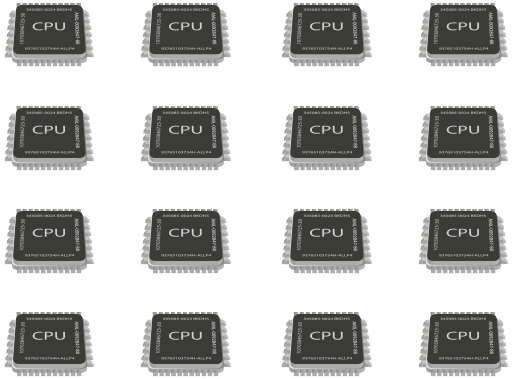

Traffic Over Time By Action
2m ago
400,000
200,000
count
6:40 AM
Tue Sep 1
2015
6:50 AM
7:00 AM
7:10 AM
7:20 AM
7:30 AM
7:40 AM
time
allowed
blocked
teardown


Traffic Over Time By Protocol
2m ago
400,000
200,000
count
6:40 AM
Tue Sep 1
2015
6:50 AM
7:00 AM
7:10 AM
7:20 AM
7:30 AM
7:40 AM
time
icmp
ipv6
tcp
udp
unknown

$SPLUNK_HOME/etc/log.cfg

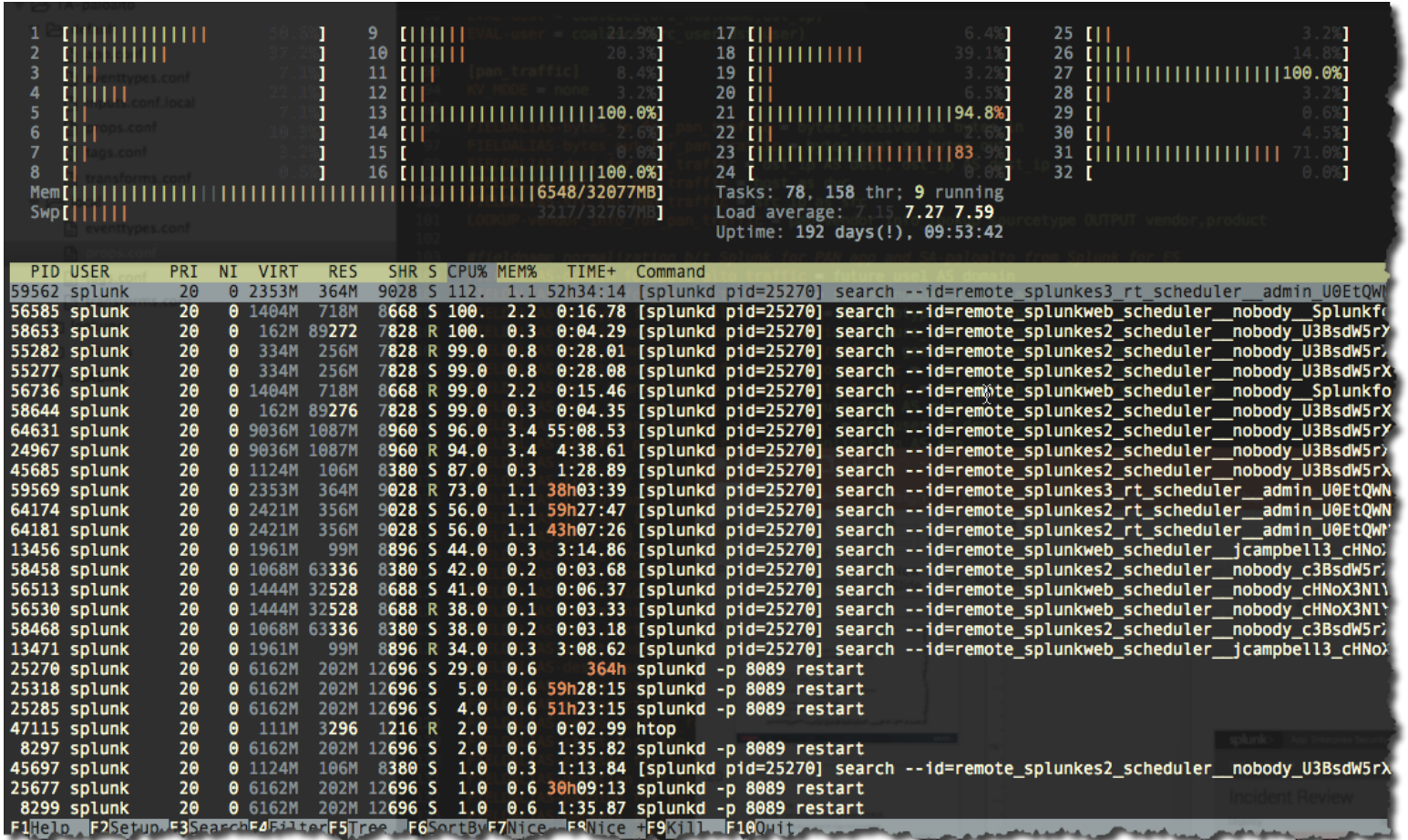
```
##log.cfg

category.SavedSplunker = DEBUG,scheduler
```

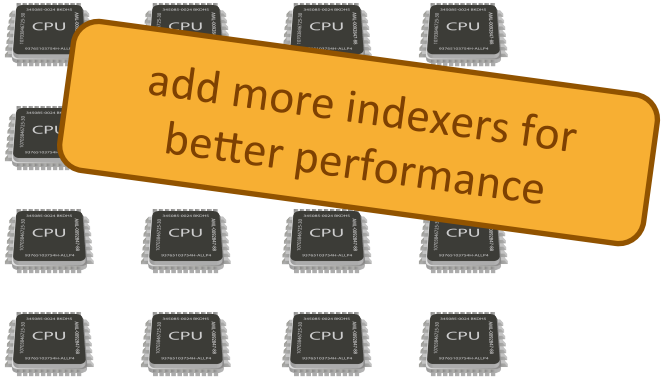




max 1 CPU
core per search

splunk> (index=* OR index=_*) (tag=network tag=communicate)


1 [|||||||||||||| 50.8%]
2 [|||||||||| 37.2%]
3 [||| 7.1%]
4 [|||||| 22.1%]
5 [|| 7.1%]
6 [||| 10.3%]
7 [|| 9.2%]
8 [| 0.6%]
9 [|||||| 21.9%]
10 [|||||| 20.3%]
11 [||| 8.4%]
12 [|| 3.2%]
13 [||||||||||||||||||100.0%]
14 [|| 2.6%]
15 [0.0%]
16 [||||||||||||||||||100.0%]
17 [|| 6.4%]
18 [|||||||||| 39.1%]
19 [|| 3.2%]
20 [|| 6.5%]
21 [||||||||||||||||||94.8%]
22 [|| 2.6%]
23 [||||||||||||||||||83.9%]
24 [0.0%]
25 [|| 3.2%]
26 [|||| 14.8%]
27 [||||||||||||||||||100.0%]
28 [|| 3.2%]
29 [| 0.6%]
30 [|| 4.5%]
31 [|||||||||||||||||| 71.0%]
32 [0.0%]
Mem[||||||||||||||||||||||||||||||||||6548/32077MB]
Swp[|||||| 3217/32767MB]
Tasks: 78, 158 thr; 9 running
Load average: 7.27 7.59
Uptime: 192 days(!), 09:53:42
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
59562 splunk 20 0 2353M 364M 9028 S 112. 1.1 52h34:14 [splunkd pid=25270] search --id=remote_splunkes3_rt_scheduler__admin_U0EtQW
56585 splunk 20 0 1404M 718M 8668 S 100. 2.2 0:16.78 [splunkd pid=25270] search --id=remote_splunkweb_scheduler__nobody__Splunkf
58653 splunk 20 0 162M 89272 7828 R 100. 0.3 0:04.29 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_U3BsdW5rY
55282 splunk 20 0 334M 256M 7828 R 99.0 0.8 0:28.01 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_U3BsdW5rZ
55277 splunk 20 0 334M 256M 7828 S 99.0 0.8 0:28.08 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_U3BsdW5rX
56736 splunk 20 0 1404M 718M 8668 R 99.0 2.2 0:15.46 [splunkd pid=25270] search --id=remote_splunkweb_scheduler__nobody__Splunkfo
58644 splunk 20 0 162M 89276 7828 S 99.0 0.3 0:04.35 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_U3BsdW5rX
64631 splunk 20 0 9036M 1087M 8960 S 96.0 3.4 55:08.53 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_U3BsdW5rY
24967 splunk 20 0 9036M 1087M 8960 R 94.0 3.4 4:38.61 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_U3BsdW5rZ
45685 splunk 20 0 1124M 106M 8380 S 87.0 0.3 1:28.89 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_U3BsdW5rX
59569 splunk 20 0 2353M 364M 9028 R 73.0 1.1 38h03:39 [splunkd pid=25270] search --id=remote_splunkes3_rt_scheduler__admin_U0EtQWN
64174 splunk 20 0 2421M 356M 9028 S 56.0 1.1 59h27:47 [splunkd pid=25270] search --id=remote_splunkes2_rt_scheduler__admin_U0EtQWN
64181 splunk 20 0 2421M 356M 9028 S 56.0 1.1 43h07:26 [splunkd pid=25270] search --id=remote_splunkes2_rt_scheduler__admin_U0EtQW
13456 splunk 20 0 1961M 99M 8896 S 44.0 0.3 3:14.86 [splunkd pid=25270] search --id=remote_splunkweb_scheduler__jcampbell3_cHNo
58458 splunk 20 0 1068M 63336 8380 S 42.0 0.2 0:03.68 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_c3BsdW5r
56513 splunk 20 0 1444M 32528 8688 S 41.0 0.1 0:06.37 [splunkd pid=25270] search --id=remote_splunkweb_scheduler__nobody_cHNoX3Nl
56530 splunk 20 0 1444M 32528 8688 R 38.0 0.1 0:03.33 [splunkd pid=25270] search --id=remote_splunkweb_scheduler__nobody_cHNoX3Nl
58468 splunk 20 0 1068M 63336 8380 S 38.0 0.2 0:03.18 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_c3BsdW5r
13471 splunk 20 0 1961M 99M 8896 R 34.0 0.3 3:08.62 [splunkd pid=25270] search --id=remote_splunkweb_scheduler__jcampbell3_cHNo
25270 splunk 20 0 6162M 202M 12696 S 29.0 0.6 364h splunkd -p 8089 restart
25318 splunk 20 0 6162M 202M 12696 S 5.0 0.6 59h28:15 splunkd -p 8089 restart
25285 splunk 20 0 6162M 202M 12696 S 4.0 0.6 51h23:15 splunkd -p 8089 restart
47115 splunk 20 0 111M 3296 1216 R 2.0 0.0 0:02.99 htop
8297 splunk 20 0 6162M 202M 12696 S 2.0 0.6 1:35.82 splunkd -p 8089 restart
45697 splunk 20 0 1124M 106M 8380 S 1.0 0.3 1:13.84 [splunkd pid=25270] search --id=remote_splunkes2_scheduler__nobody_U3BsdW5rX
25677 splunk 20 0 6162M 202M 12696 S 1.0 0.6 30h09:13 splunkd -p 8089 restart
8299 splunk 20 0 6162M 202M 12696 S 1.0 0.6 1:35.87 splunkd -p 8089 restart
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit



max 1 CPU core per search

splunk> (index=* OR index=_*) (tag=network tag=communicate)

Splunk packages CIM-compliant technology add-ons with Enterprise Security

- Splunk_TA_bro
- Splunk_TA_cisco-asa
- Splunk_TA_cisco-esa
- Splunk_TA_cisco-wsa
- Splunk_TA_flowfix
- Splunk_TA_mcafee
- Splunk_TA_nessus
- Splunk_TA_nix
- Splunk_TA_norse
- Splunk_TA_sophos
- Splunk_TA_windows
- TA-airdefense
- TA-alcatel
- TA-bluecoat
- TA-cef
- TA-fireeye
- TA-fortinet
- TA-ftp
- TA-juniper
- TA-ncircle
- TA-nmap
- TA-oracle
- TA-ossec
- TA-paloalto
- TA-rsa
- TA-sav
- TA-sep
- TA-snort
- TA-sos
- TA-tippingpoint
- TA-trendmicro
- TA-websense

1: disable included Technology Add-Ons

2: enable relevant TAs one-by-one to ensure CIM-compliant extractions

```
index=_internal host=splunkes* sourcetype=scheduler savedsplunker CIM_Network_Traffic DEBUG dispatched OR completed |
transaction maxevents=2 startswith=dispatched endswith=completed | timechart span=4h perc90(duration) as duration
```

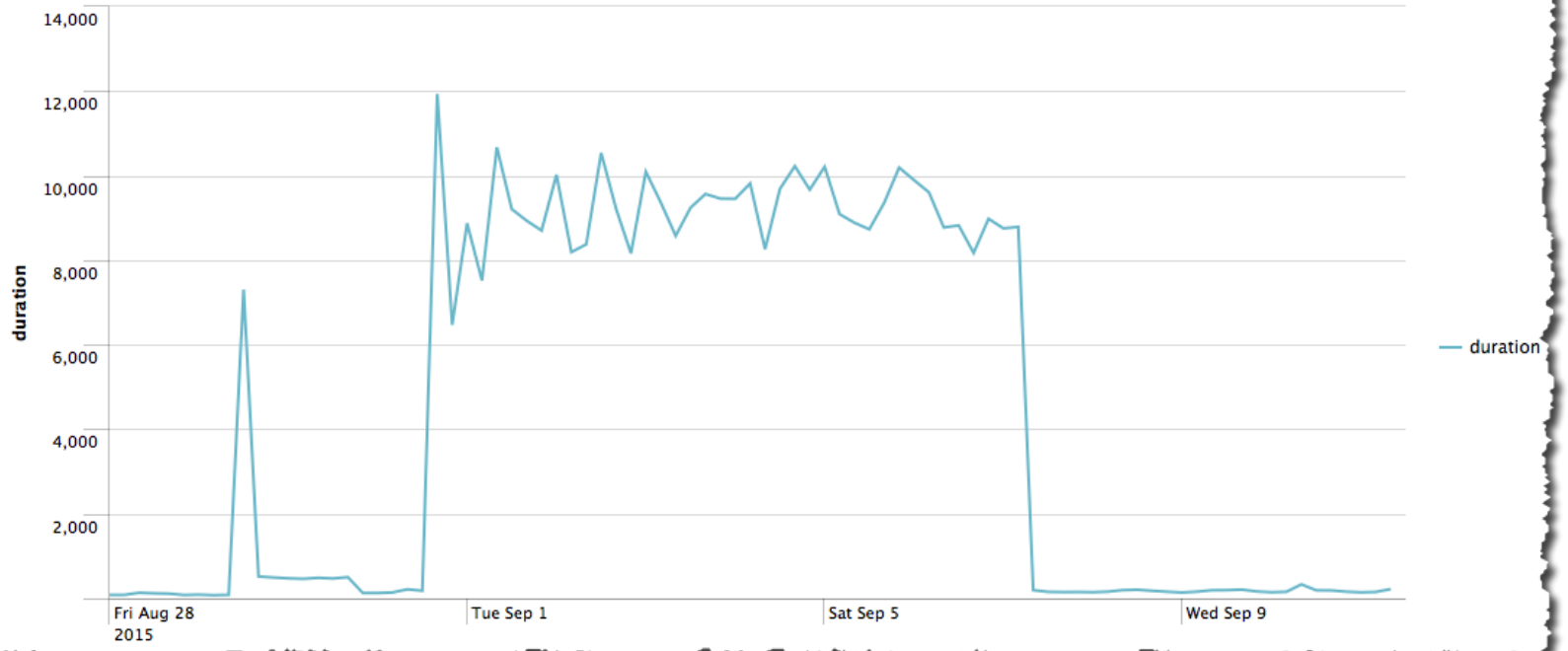
Last 14 days

✓ 2,005 events (8/28/15 12:00:00.000 AM to 9/11/15 8:16:45.000 AM)

Job | Smart Mode

Events | Patterns | Statistics (87) | Visualization

Line | Format

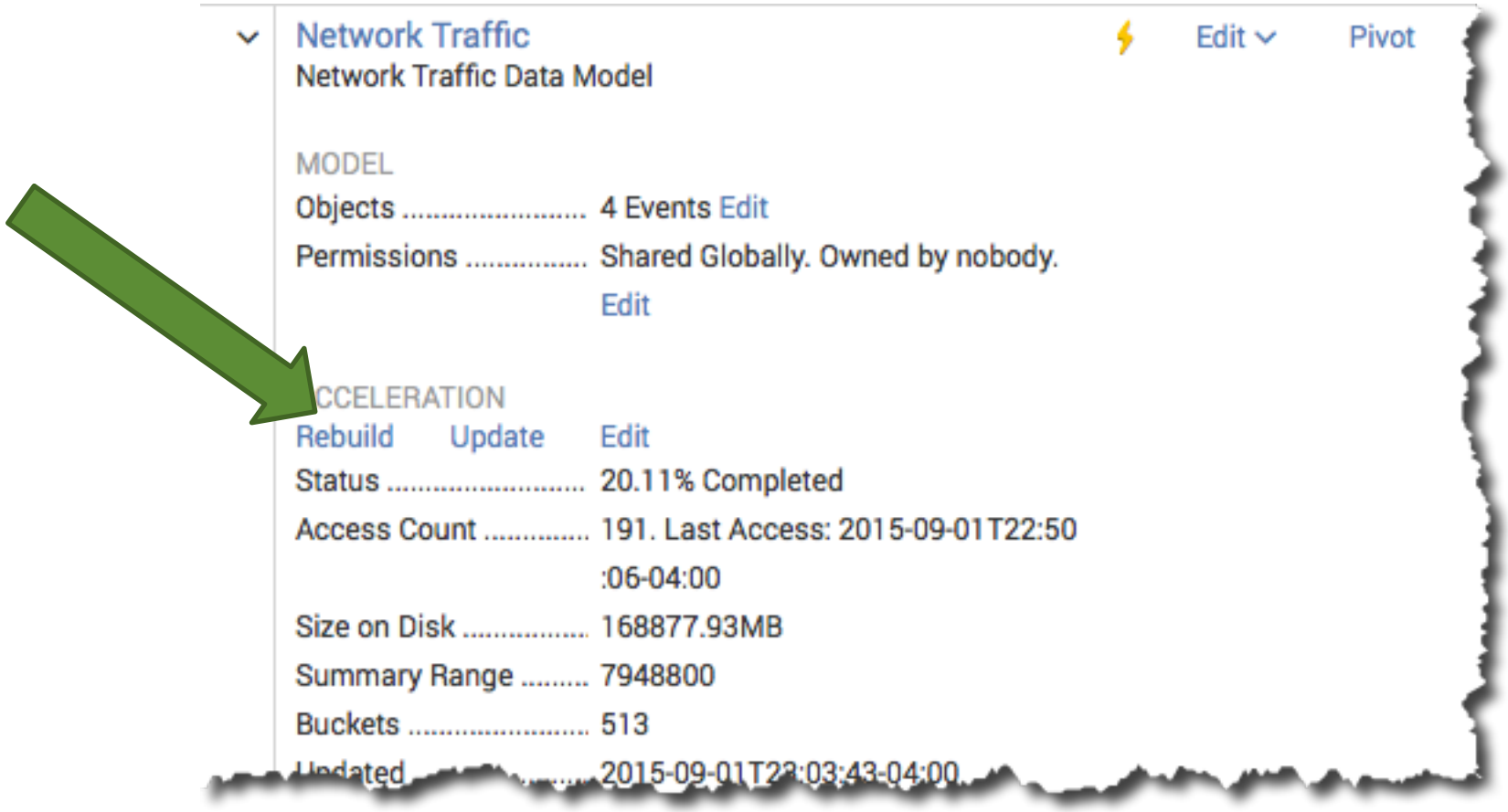


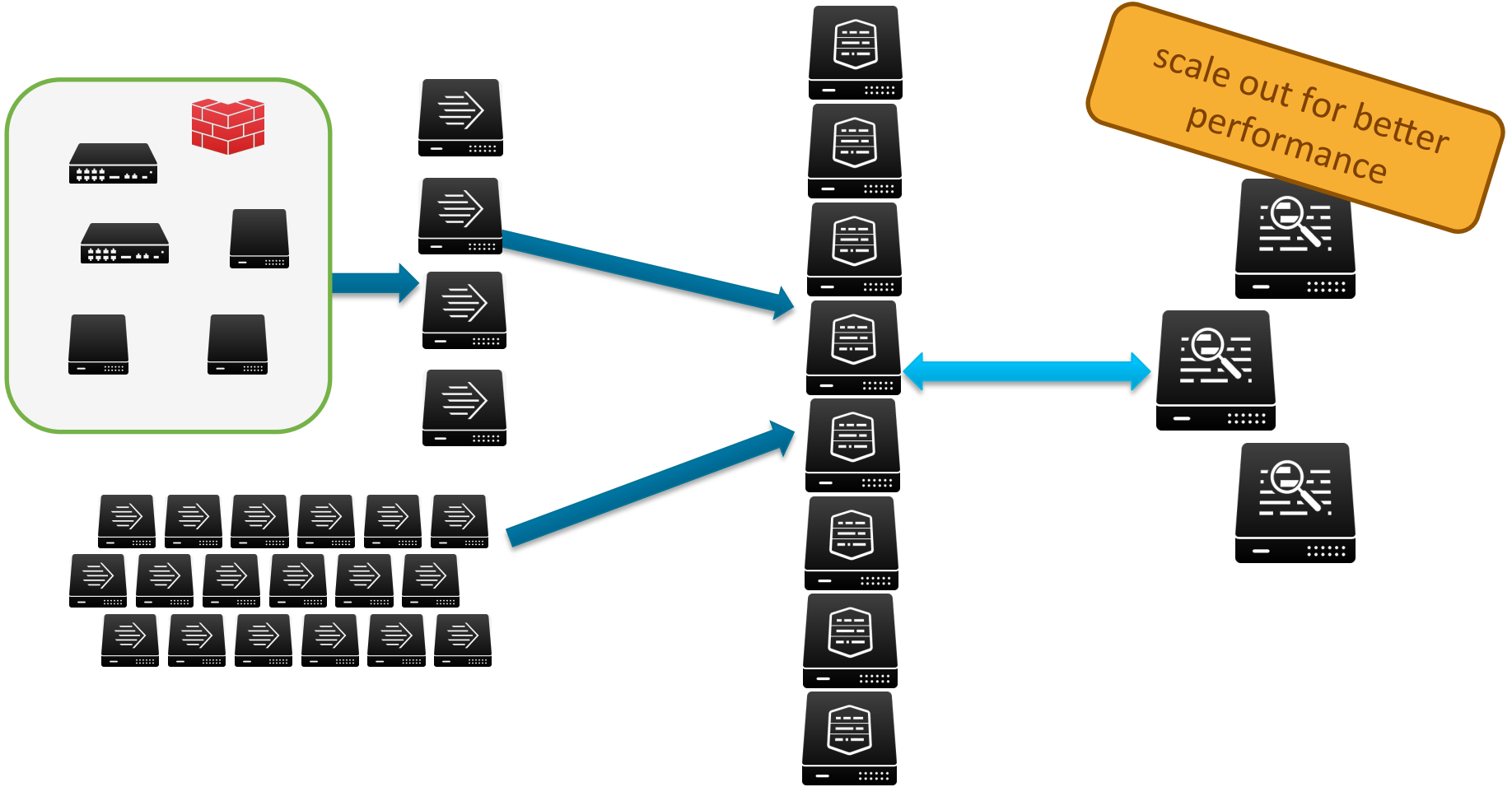
$SPLUNK_HOME/etc/apps/Splunk_SA_CIM/local/datamodels.conf

```
##datamodels.conf

[Authentication]
acceleration = true
acceleration.manual_rebuilds = true

#configure to limit backfill during initial build
#  - only effective when rebuild initiated
acceleration.backfill_time = -7d
```

CIM datamodels in Splunk for Enterprise Security do not automatically rebuild

limit backfill range for faster production readiness


Network Traffic
Edit
Pivot
Network Traffic Data Model
MODEL
Objects ..... 4 Events Edit
Permissions ..... Shared Globally. Owned by nobody.
Edit
CCELERATION
Rebuild Update Edit
Status ..... 20.11% Completed
Access Count ..... 191. Last Access: 2015-09-01T22:50
:06-04:00
Size on Disk 168877.93MB
Summary Range 7948800
Buckets 513
Updated 2015-09-01T22:03:43-04:00


scale out for better performance

*nix Splunk Add-on for Unix and Linux

$SPLUNK_HOME/etc/apps/Splunk_TA_nix/local/eventtypess.conf

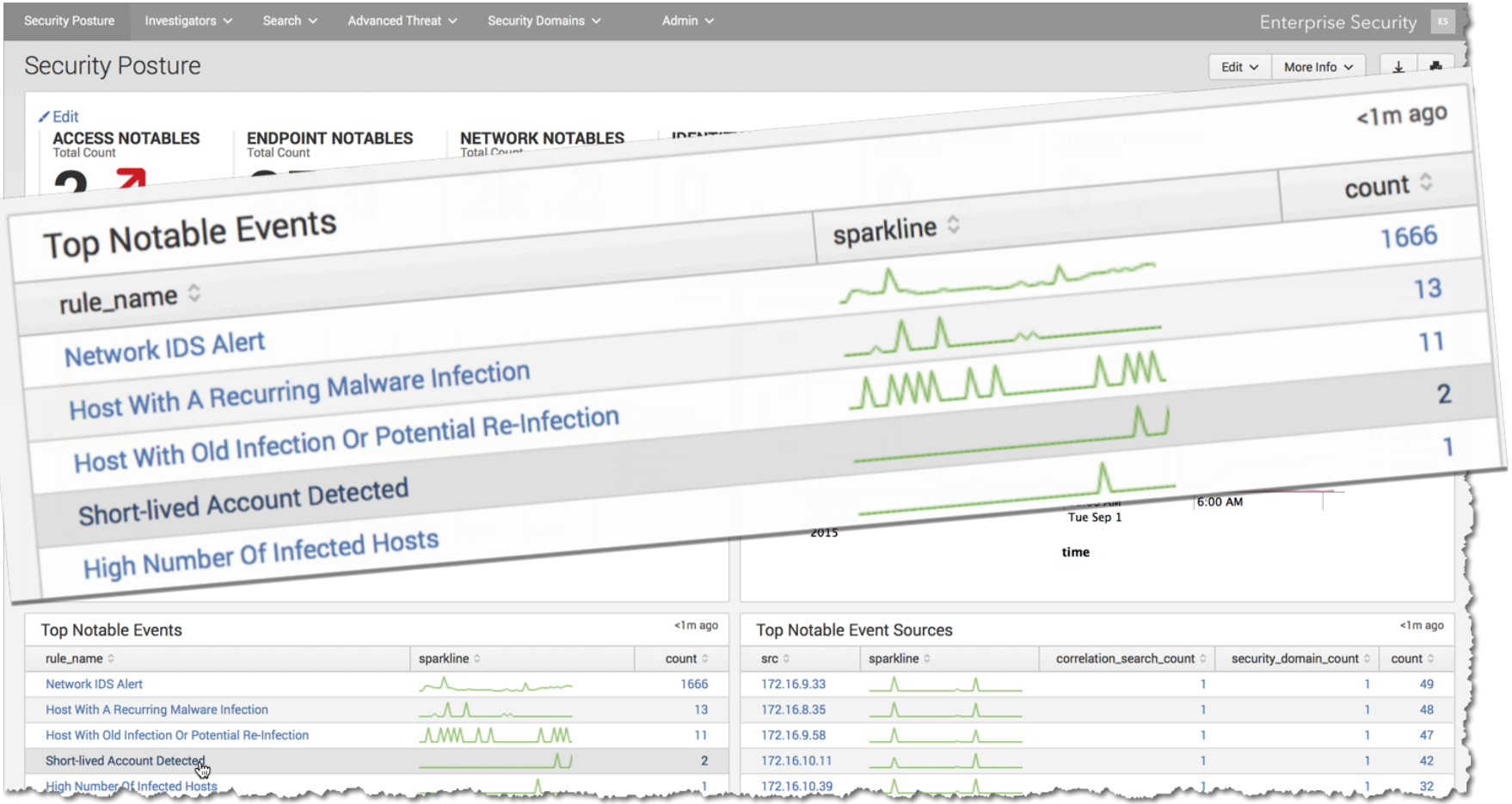
data models search across all indexes

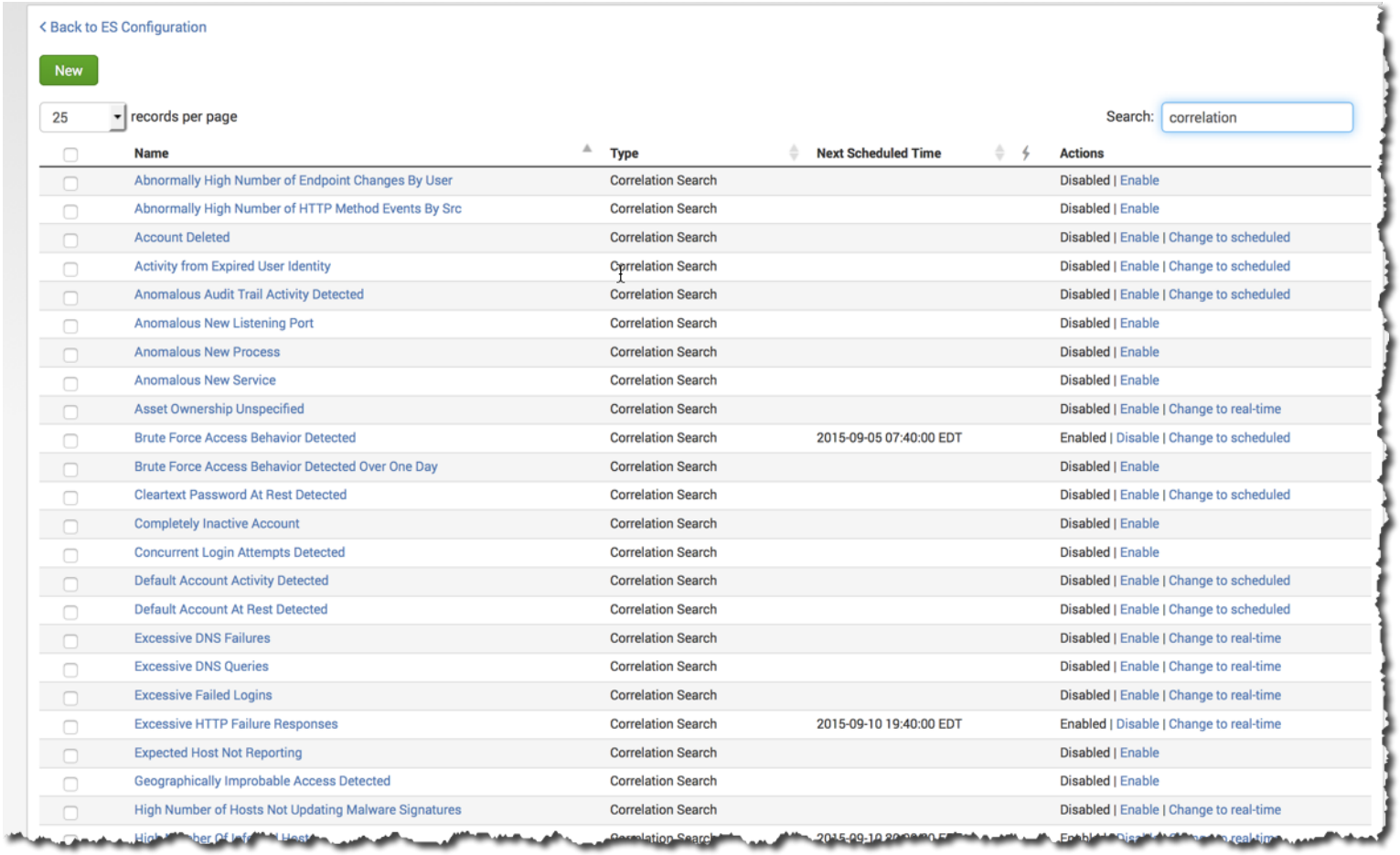
consider modifying eventtypes (tags) with additional constraints

```
##eventtypes.conf

[iptables_firewall_accept]
#search = (NOT sourcetype=stash) signature=firewall
         action=PASS OR action=permit
search = index=os (NOT sourcetype=stash) signature=firewall
         action=PASS OR action=permit
#tags = os unix host firewall communicate success
```

line wrapping for readability only

>300% increase in data model acceleration performance after adding index constraints in select TAs


Security Posture
Investigators
Search
Advanced Threat
Security Domains
Admin
Enterprise Security
Security Posture
Edit
More Info
Edit
ACCESS NOTABLES
Total Count
ENDPOINT NOTABLES
Total Count
NETWORK NOTABLES
Total Count
Top Notable Events
<1m ago
rule_name
sparkline
count
Network IDS Alert
1666
Host With A Recurring Malware Infection
13
Host With Old Infection Or Potential Re-Infection
11
Short-lived Account Detected
2
High Number Of Infected Hosts
1
6:00 AM
Tue Sep 1
2015
time
Top Notable Events
<1m ago
rule_name
sparkline
count
Network IDS Alert
1666
Host With A Recurring Malware Infection
13
Host With Old Infection Or Potential Re-Infection
11
Short-lived Account Detected
2
High Number Of Infected Hosts
1
Top Notable Event Sources
<1m ago
src
sparkline
correlation_search_count
security_domain_count
count
172.16.9.33
1
1
49
172.16.8.35
1
1
48
172.16.9.58
1
1
47
172.16.10.11
1
1
42
172.16.10.39
1
1
32


Back to ES Configuration
New
25 records per page
Search: correlation
Name
Type
Next Scheduled Time
Actions
Abnormally High Number of Endpoint Changes By User | Correlation Search | | Disabled | Enable
Abnormally High Number of HTTP Method Events By Src | Correlation Search | | Disabled | Enable
Account Deleted | Correlation Search | | Disabled | Enable | Change to scheduled
Activity from Expired User Identity | Correlation Search | | Disabled | Enable | Change to scheduled
Anomalous Audit Trail Activity Detected | Correlation Search | | Disabled | Enable | Change to scheduled
Anomalous New Listening Port | Correlation Search | | Disabled | Enable
Anomalous New Process | Correlation Search | | Disabled | Enable
Anomalous New Service | Correlation Search | | Disabled | Enable
Asset Ownership Unspecified | Correlation Search | | Disabled | Enable | Change to real-time
Brute Force Access Behavior Detected | Correlation Search | 2015-09-05 07:40:00 EDT | Enabled | Disable | Change to scheduled
Brute Force Access Behavior Detected Over One Day | Correlation Search | | Disabled | Enable
Cleartext Password At Rest Detected | Correlation Search | | Disabled | Enable | Change to scheduled
Completely Inactive Account | Correlation Search | | Disabled | Enable
Concurrent Login Attempts Detected | Correlation Search | | Disabled | Enable
Default Account Activity Detected | Correlation Search | | Disabled | Enable | Change to scheduled
Default Account At Rest Detected | Correlation Search | | Disabled | Enable | Change to scheduled
Excessive DNS Failures | Correlation Search | | Disabled | Enable | Change to real-time
Excessive DNS Queries | Correlation Search | | Disabled | Enable | Change to real-time
Excessive Failed Logins | Correlation Search | | Disabled | Enable | Change to real-time
Excessive HTTP Failure Responses | Correlation Search | 2015-09-10 19:40:00 EDT | Enabled | Disable | Change to real-time
Expected Host Not Reporting | Correlation Search | | Disabled | Enable
Geographically Improbable Access Detected | Correlation Search | | Disabled | Enable
High Number of Hosts Not Updating Malware Signatures | Correlation Search | | Disabled | Enable | Change to real-time

Correlation Search

Search Name *: Short-lived Account Detected

Application Context: DA-ESS-AccessProtection

Description: Detects when a account or credential is created an

Describes what kind of issues this search is intended to detect

Search *:

```
| datamodel Change_Analysis Account_Management search | search "All_Changes.action"="created" OR "All_Changes.action"="deleted" | rename All_Changes.* as * | streamstats range(_time) as delta count by user,dest window=2 global=f | where count>1 AND delta<`useraccount_minimal_lifetime` | `get_relative_time_str(delta, "timestr")` | `get_event_id` | `map_notable_fields` | fields + orig_event_id, orig_raw, user, dest, delta, timestr
```

Edit search in guided mode

Time Range

Start time: -61m@m

End time: +0m@m

Cron Schedule *: */15 * * * *

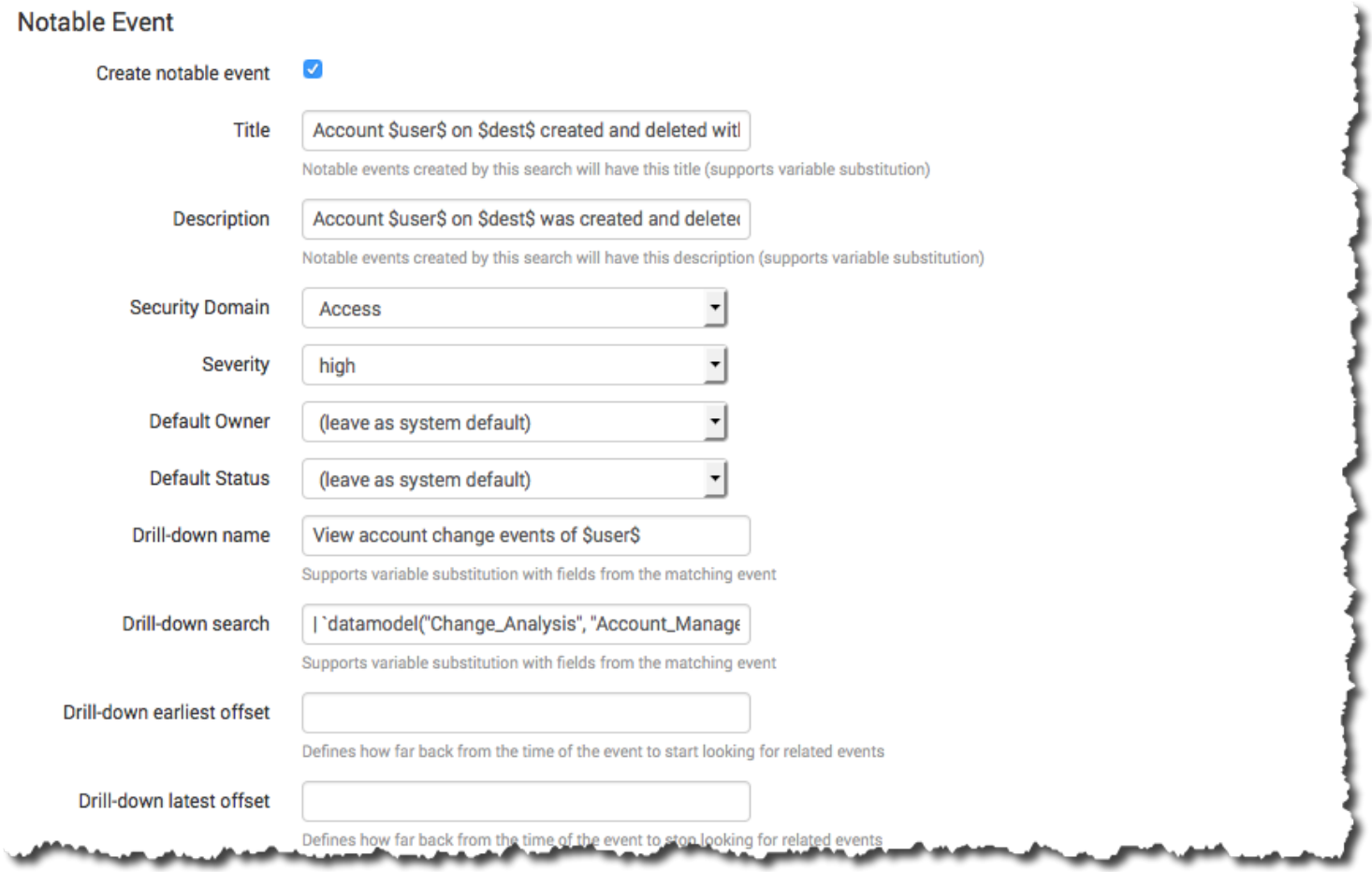
Enter a cron-style schedule.

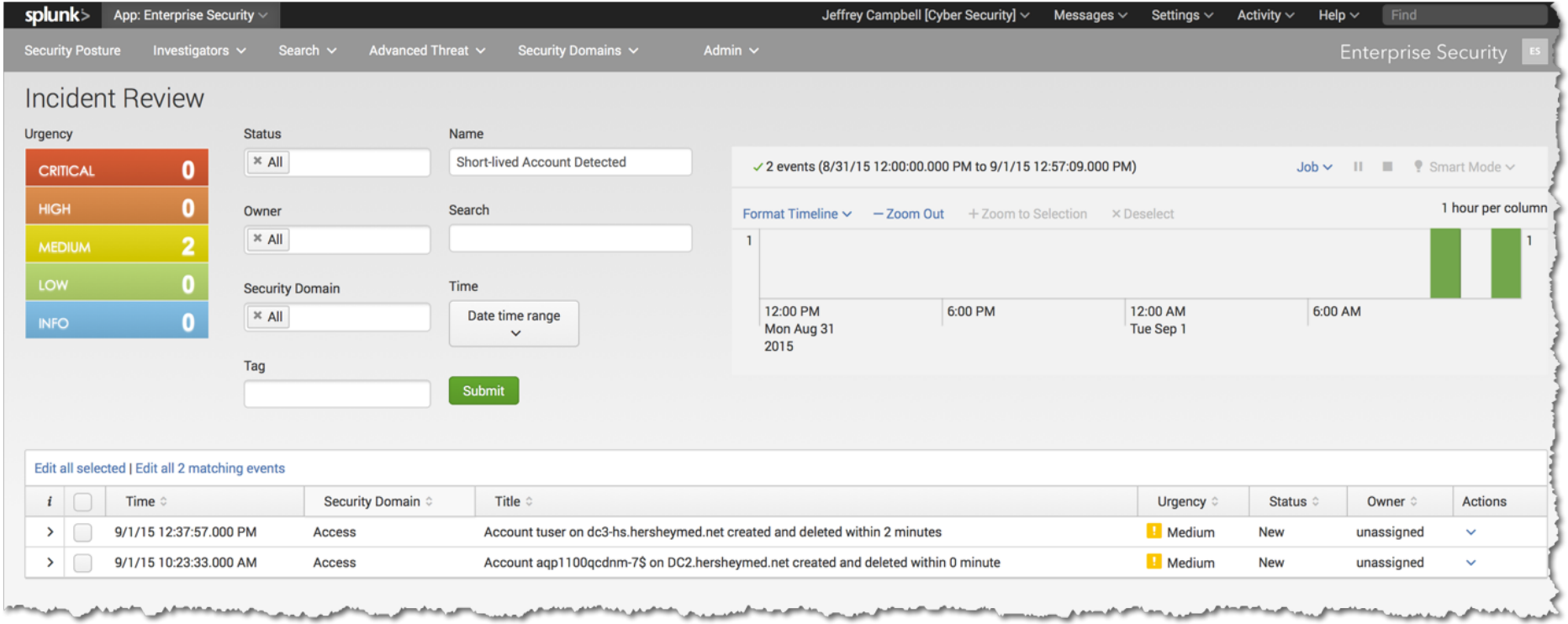
For example '*/5 * * * *' (every 5 minutes) or '0 21 * * *' (every day at 9 PM).

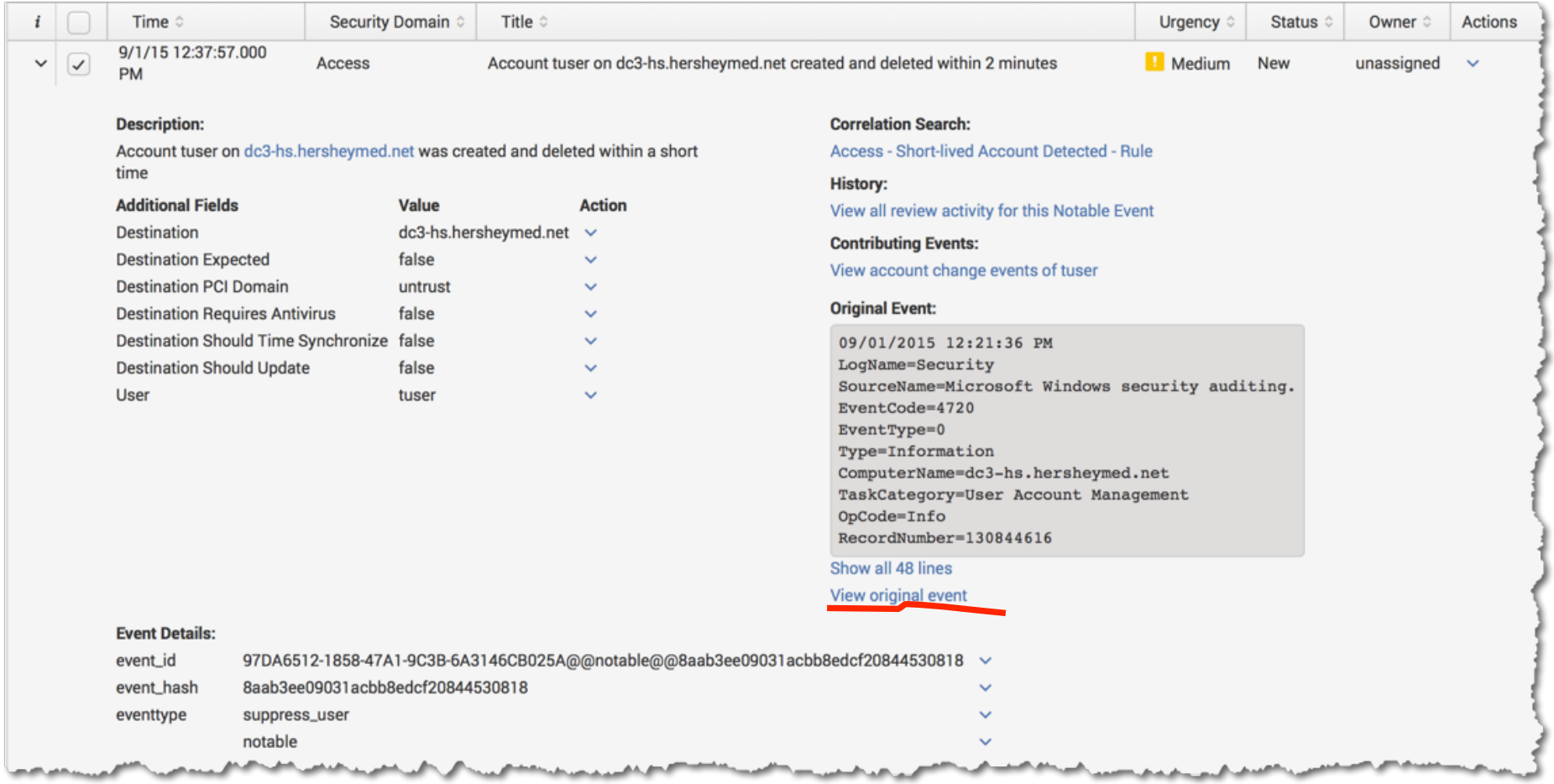
Realtime searches use a default schedule of '*/5 * * * *'.

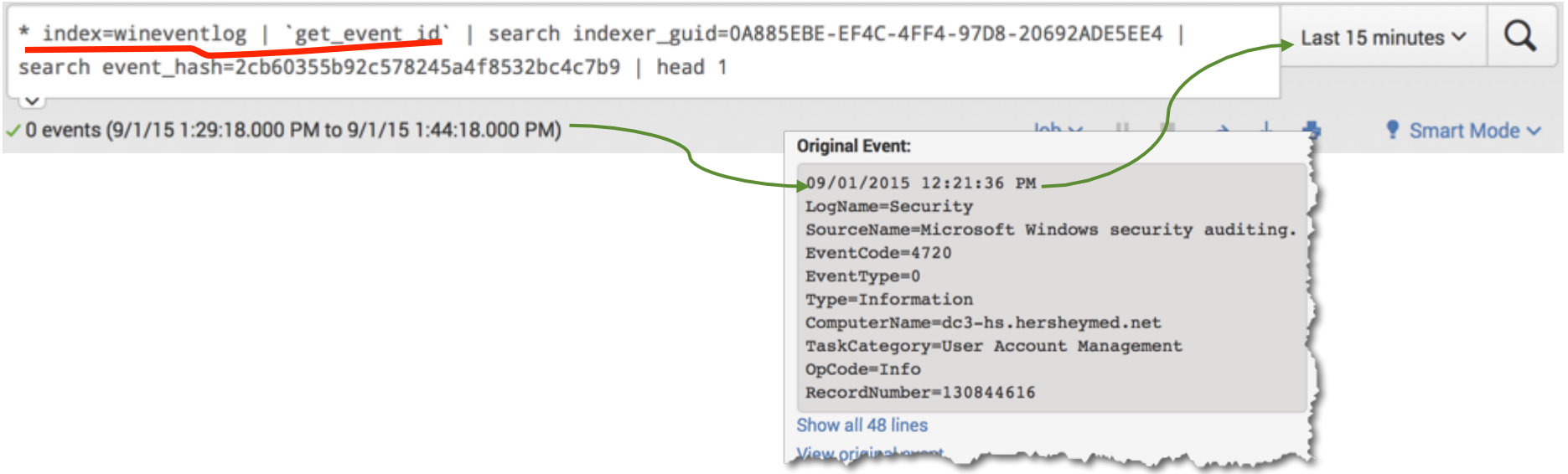
Throttling

Window duration: 14400


Notable Event
Create notable event
Title
Account $user$ on $dest$ created and deleted wit
Notable events created by this search will have this title (supports variable substitution)
Description
Account $user$ on $dest$ was created and delete
Notable events created by this search will have this description (supports variable substitution)
Security Domain
Access
Severity
high
Default Owner
(leave as system default)
Default Status
(leave as system default)
Drill-down name
View account change events of $user$
Supports variable substitution with fields from the matching event
Drill-down search
| `datamodel("Change_Analysis", "Account_Manage
Supports variable substitution with fields from the matching event
Drill-down earliest offset
Defines how far back from the time of the event to start looking for related events
Drill-down latest offset
Defines how far back from the time of the event to stop looking for related events


splunk> App: Enterprise Security
Jeffrey Campbell [Cyber Security]
Messages
Settings
Activity
Help
Find
Security Posture
Investigators
Search
Advanced Threat
Security Domains
Admin
Enterprise Security
Incident Review
Urgency
CRITICAL 0
HIGH 0
MEDIUM 2
LOW 0
INFO 0
Status
All
Owner
All
Security Domain
All
Tag
Name
Short-lived Account Detected
Search
Time
Date time range
Submit
2 events (8/31/15 12:00:00.000 PM to 9/1/15 12:57:09.000 PM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
12:00 PM Mon Aug 31 2015
6:00 PM
12:00 AM Tue Sep 1
6:00 AM
Edit all selected | Edit all 2 matching events
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/1/15 12:37:57.000 PM
Access
Account tuser on dc3-hs.hersheymed.net created and deleted within 2 minutes
Medium
New
unassigned
9/1/15 10:23:33.000 AM
Access
Account aqp1100qcdnm-7$ on DC2.hersheymed.net created and deleted within 0 minute
Medium
New
unassigned


i
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/1/15 12:37:57.000 PM
Access
Account tuser on dc3-hs.hersheymed.net created and deleted within 2 minutes
Medium
New
unassigned
Description:
Account tuser on dc3-hs.hersheymed.net was created and deleted within a short time
Additional Fields
Value
Action
Destination
dc3-hs.hersheymed.net
Destination Expected
false
Destination PCI Domain
untrust
Destination Requires Antivirus
false
Destination Should Time Synchronize
false
Destination Should Update
false
User
tuser
Correlation Search:
Access - Short-lived Account Detected - Rule
History:
View all review activity for this Notable Event
Contributing Events:
View account change events of tuser
Original Event:
09/01/2015 12:21:36 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4720
EventType=0
Type=Information
ComputerName=dc3-hs.hersheymed.net
TaskCategory=User Account Management
OpCode=Info
RecordNumber=130844616
Show all 48 lines
View original event
Event Details:
event_id
97DA6512-1858-47A1-9C3B-6A3146CB025A@@notable@@8aab3ee09031acbb8edcf20844530818
event_hash
8aab3ee09031acbb8edcf20844530818
eventtype
suppress_user
notable


* index=wineventlog | `get_event_id` | search indexer_guid=0A885EBE-EF4C-4FF4-97D8-20692ADE5EE4 | search event_hash=2cb60355b92c578245a4f8532bc4c7b9 | head 1
Last 15 minutes
0 events (9/1/15 1:29:18.000 PM to 9/1/15 1:44:18.000 PM)
Smart Mode
Original Event:
09/01/2015 12:21:36 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4720
EventType=0
Type=Information
ComputerName=dc3-hs.hersheymed.net
TaskCategory=User Account Management
OpCode=Info
RecordNumber=130844616
Show all 48 lines

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
✓	9/1/15 12:37:57.000 PM	Access	Account tuser on dc3-hs.hersheymed.net created and deleted within 2 minutes	Medium	New	unassigned	

Description:

Account tuser on dc3-hs.hersheymed.net was created and deleted within a short time

Additional Fields	Value	Action
Destination	dc3-hs.hersheymed.net	
Destination Expected	false	
Destination PCI Domain	untrust	
Destination Requires Antivirus	false	
Destination Should Time Synchronize	false	
Destination Should Update	false	
User	tuser	

Correlation Search:

Access - Short-lived Account Detected - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View account change events of tuser

Original Event:

```
09/01/2015 12:21:36 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4720
EventType=0
Type=Information
ComputerName=dc3-hs.hersheymed.net
TaskCategory=User Account Management
OpCode=Info
RecordNumber=130844616
```

Show all 48 lines

View original event

Event Details:

event_id	97DA6512-1858-47A1-9C3B-6A3146CB025A@@notable@@8aab3ee09031acbb8edcf20844530818
event_hash	8aab3ee09031acbb8edcf20844530818
eventtype	suppress_user
	notable

```
| `datamodel("Change_Analysis", "Account_Management")` | search All_Changes.user="tuser"
(All_Changes.action="created" OR All_Changes.action="deleted")
```

Date time range

✓ 2 events (9/1/15 12:00:00.000 PM to 9/1/15 1:00:00.000 PM)

Job | Smart Mode

run time: 12:31

```
index=* tag=change tag=account user=tuser (action=created OR action=deleted)
```

✓ 2 events (9/1/15 12:00:00.000 PM to 9/1/15 1:00:00.000 PM)

run time: 0:21

```
index=* tag=change tag=account user=tuser (action=created OR action=deleted) earlies
latest=1441124570
```

✓ 2 events (9/1/15 12:21:30.000 PM to 9/1/15 12:22:50.000 PM)

run time: 0:16

Dear Splunk,

please stop using "datamodel" to search in your drilldowns…

Love, your users

```
index=wineventlog tag=change tag=account user=tuser (action=created OR action=deleted) earliest=1441124490
latest=1441124570
```

Date time range

✓ 2 events (9/1/15 12:21:30.000 PM to 9/1/15 12:22:50.000 PM)

Job | Smart Mode

run time: 0:07

Notable Event

Create notable event ☑

Title: Account $user$ on $dest$ created and deleted wit

Notable events created by this search will have this title (supports variable substitution)

Description: Account $user$ on $dest$ was created and delete

Notable events created by this search will have this description (supports variable substitution)

Security Domain: Access

Severity: high

Default Owner: (leave as system default)

Default Status: (leave as system default)

Drill-down name: View account change events of $user$

Supports variable substitution with fields from the matching event

Drill-down search: | `datamodel("Change_Analysis", "Account_Manage

Supports variable substitution with fields from the matching event

Drill-down earliest offset:

Defines how far back from the time of the event to start looking for related events

Drill-down latest offset:

Defines how far back from the time of the event to stop looking for related events

- Prepare infrastructure – may need more hardware than you think
- Think through your authoritative user and asset inventories
- Be selective in your TAs and apps on the ES search head…
- Consider adding constraints to the TA eventtypes
- Take advantage of the acceleration you worked so hard for
  - Where possible, use tstats with “summariesonly=t”

Questions?

THANK YOU

splunk>