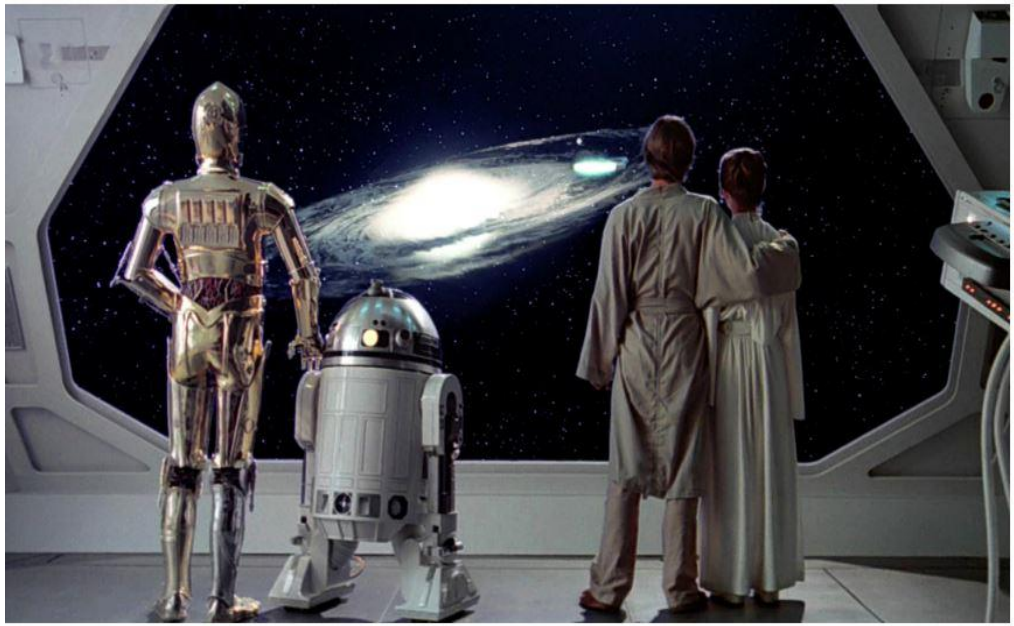
Security Onion



Ending the Tyranny of Expensive Security Tools:

A New Hope

Security Isn't About Managing Tools

- Good information security (and engineering) is about solving problems.
- You don't always need to buy a product.
- Be Creative.

So Many Tools….

So Little Budget

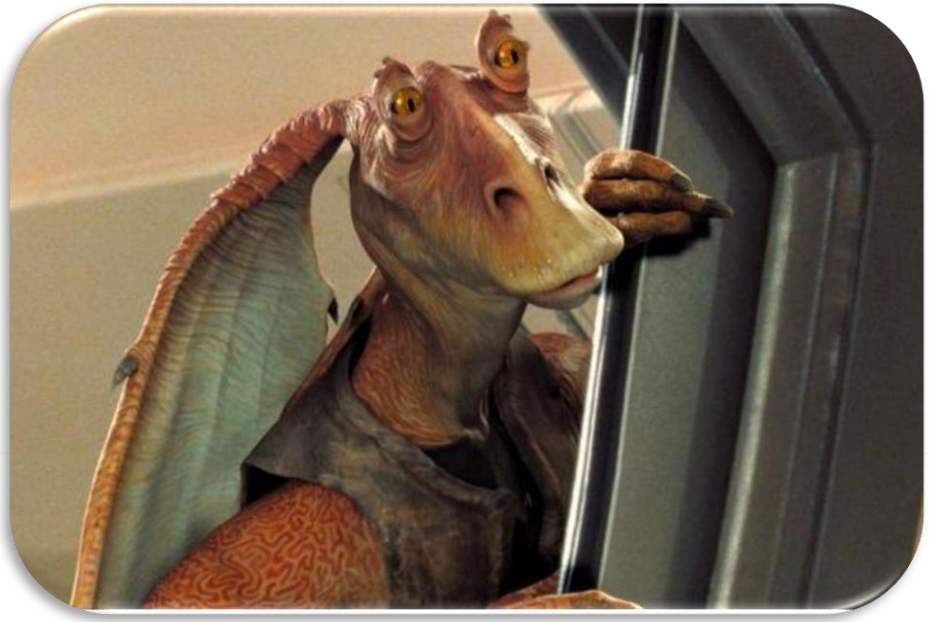
What is Security Onion?

Security Onion is a FREE Linux distro for:

- intrusion detection
- network security monitoring
- log management

What's Inside?

- Snort
- Suricata
- Bro Network Security Monitor
- Argus and Ra
- Xplico
- Network Miner
- Squil and Snorby
- ELSA

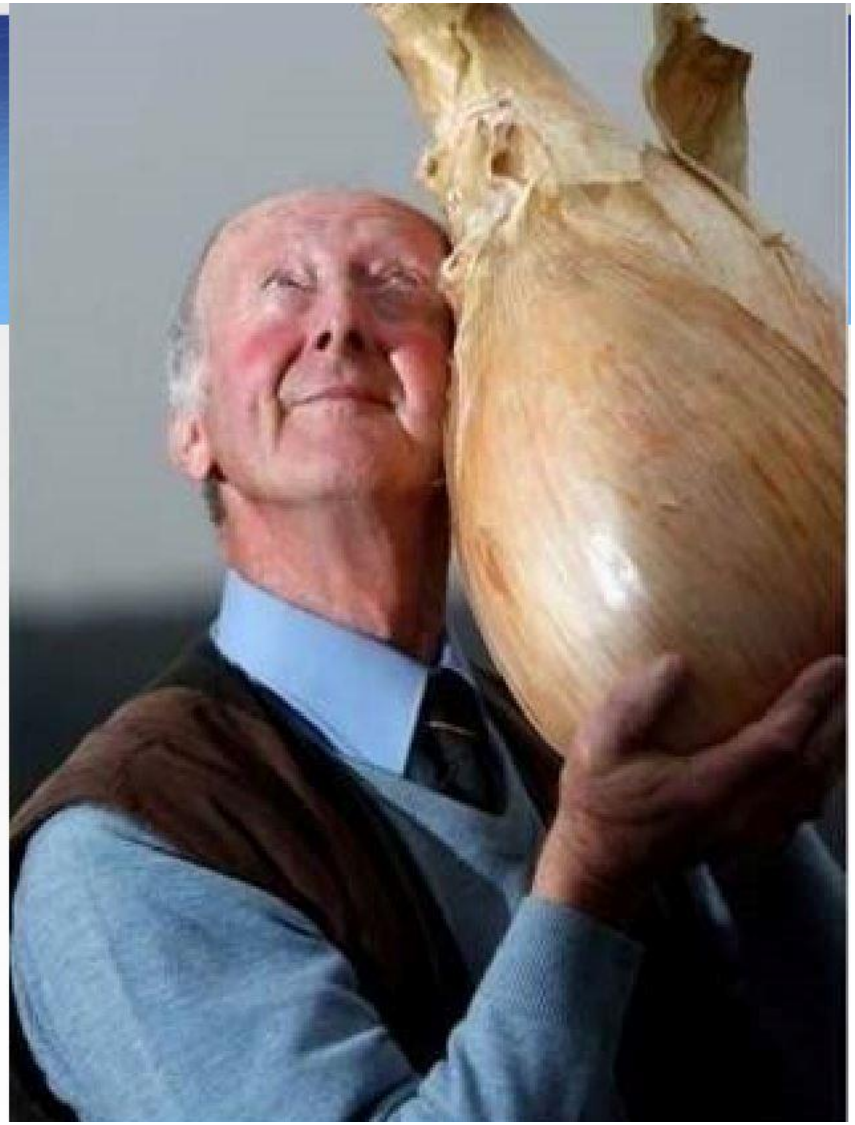


What data does it give me?

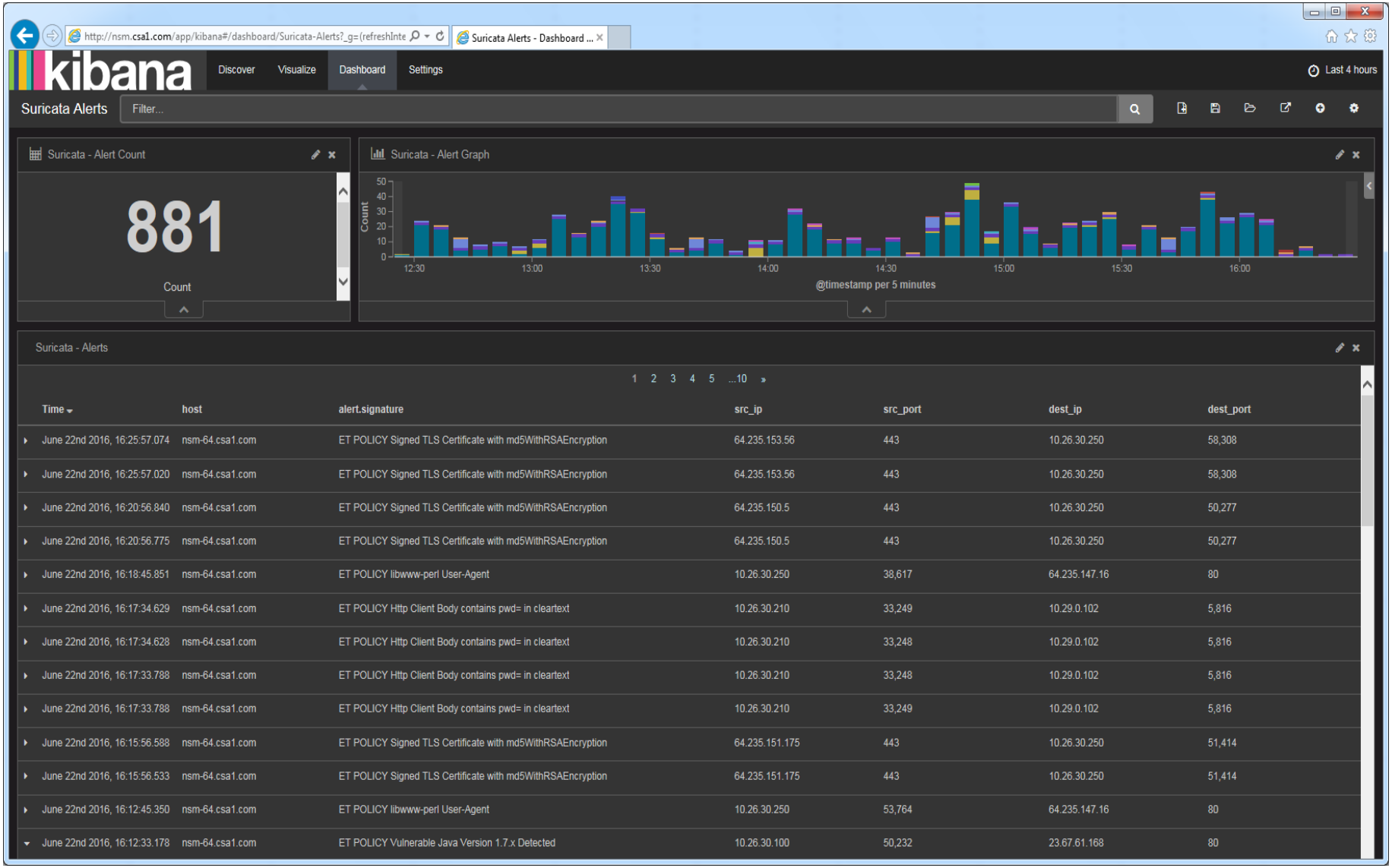
- Flow data from Argus, Bro, and PRADS
- Alert data
  - NIDS alerts from Snort/Suricata
  - HIDS alerts from OSSEC
- Syslog data received by syslog-ng or sniffed by Bro
- Asset data from Bro and PRADS
- Transaction data – http/ftp/dns/ssl/other logs from Bro
- Full content data from netsniff-ng

Does it scale?

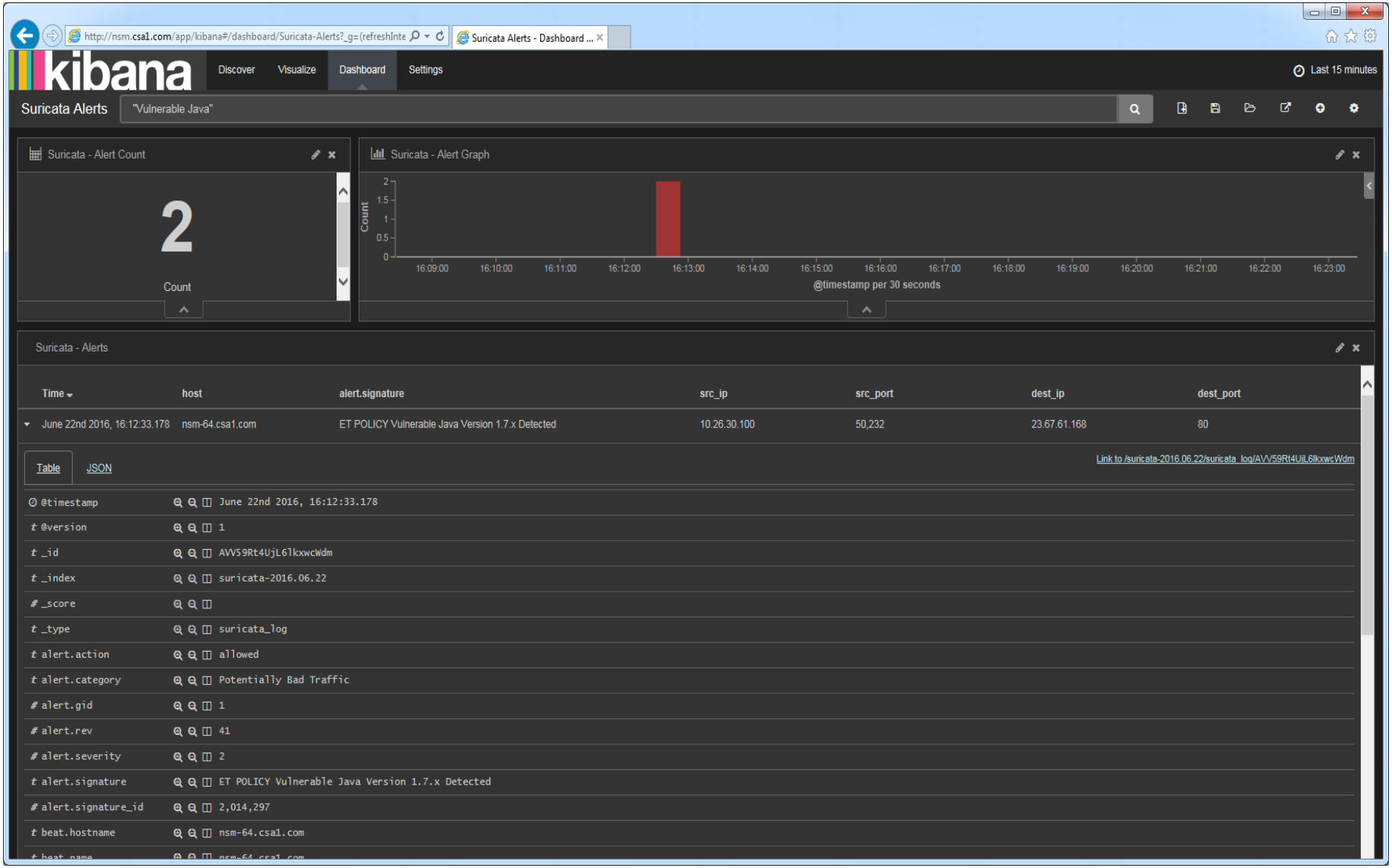
- Big Onions – 64-bit
- Big Traffic – PF_RING
- Big Data – ELSA



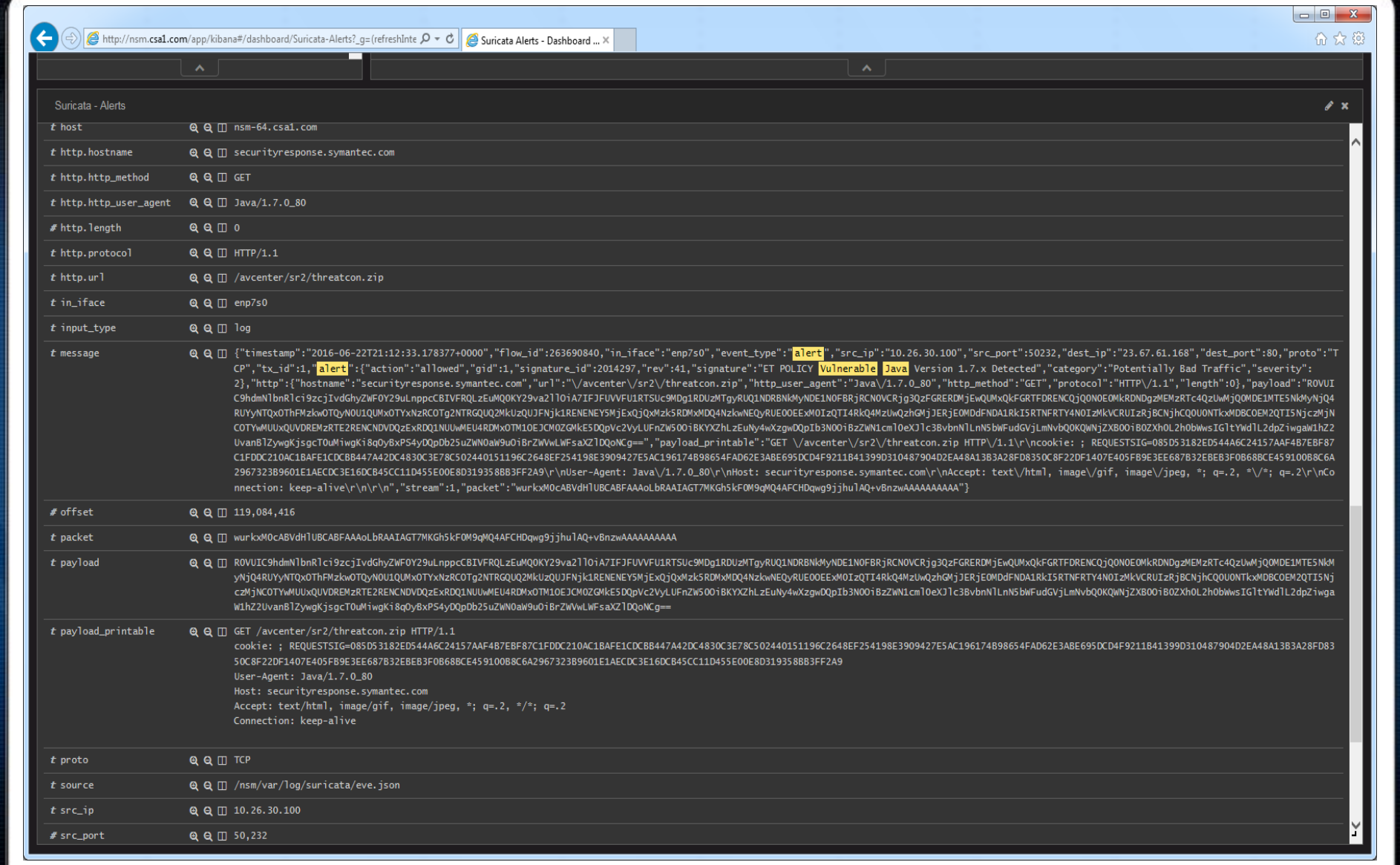
Central Service Association



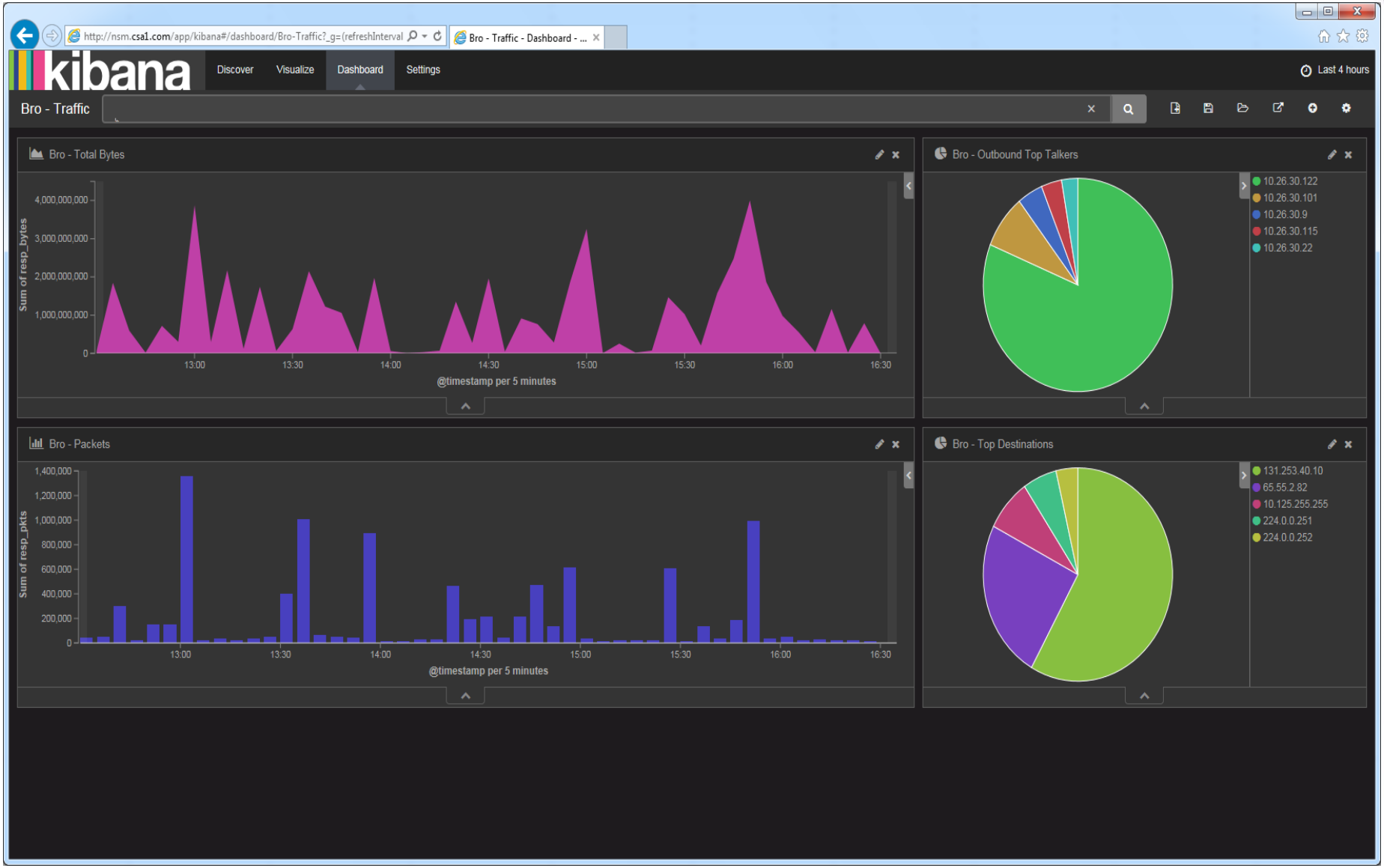
Time	host	alert.signature	src_ip	src_port	dest_ip	dest_port
June 22nd 2016, 16:25:57.074	nsm-64.csa1.com	ET POLICY Signed TLS Certificate with md5WithRSAEncryption	64.235.153.56	443	10.26.30.250	58,308
June 22nd 2016, 16:25:57.020	nsm-64.csa1.com	ET POLICY Signed TLS Certificate with md5WithRSAEncryption	64.235.153.56	443	10.26.30.250	58,308
June 22nd 2016, 16:20:56.840	nsm-64.csa1.com	ET POLICY Signed TLS Certificate with md5WithRSAEncryption	64.235.150.5	443	10.26.30.250	50,277
June 22nd 2016, 16:20:56.775	nsm-64.csa1.com	ET POLICY Signed TLS Certificate with md5WithRSAEncryption	64.235.150.5	443	10.26.30.250	50,277
June 22nd 2016, 16:18:45.851	nsm-64.csa1.com	ET POLICY libwww-perl User-Agent	10.26.30.250	38,617	64.235.147.16	80
June 22nd 2016, 16:17:34.629	nsm-64.csa1.com	ET POLICY Http Client Body contains pwd= in cleartext	10.26.30.210	33,249	10.29.0.102	5,816
June 22nd 2016, 16:17:34.628	nsm-64.csa1.com	ET POLICY Http Client Body contains pwd= in cleartext	10.26.30.210	33,248	10.29.0.102	5,816
June 22nd 2016, 16:17:33.788	nsm-64.csa1.com	ET POLICY Http Client Body contains pwd= in cleartext	10.26.30.210	33,248	10.29.0.102	5,816
June 22nd 2016, 16:17:33.788	nsm-64.csa1.com	ET POLICY Http Client Body contains pwd= in cleartext	10.26.30.210	33,249	10.29.0.102	5,816
June 22nd 2016, 16:15:56.588	nsm-64.csa1.com	ET POLICY Signed TLS Certificate with md5WithRSAEncryption	64.235.151.175	443	10.26.30.250	51,414
June 22nd 2016, 16:15:56.533	nsm-64.csa1.com	ET POLICY Signed TLS Certificate with md5WithRSAEncryption	64.235.151.175	443	10.26.30.250	51,414
June 22nd 2016, 16:12:45.350	nsm-64.csa1.com	ET POLICY libwww-perl User-Agent	10.26.30.250	53,764	64.235.147.16	80
June 22nd 2016, 16:12:33.178	nsm-64.csa1.com	ET POLICY Vulnerable Java Version 1.7.x Detected	10.26.30.100	50,232	23.67.61.168	80


http://nsm.csa1.com/app/kibana#/dashboard/Suricata-Alerts?_g=(refreshInte
Suricata Alerts - Dashboard ...
kibana
Discover
Visualize
Dashboard
Settings
Last 15 minutes
Suricata Alerts
"Vulnerable Java"
Suricata - Alert Count
2
Count
Suricata - Alert Graph
Count
2
1.5
1
0.5
0
16:09:00
16:10:00
16:11:00
16:12:00
16:13:00
16:14:00
16:15:00
16:16:00
16:17:00
16:18:00
16:19:00
16:20:00
16:21:00
16:22:00
16:23:00
@timestamp per 30 seconds
Suricata - Alerts
Time
host
alert.signature
src_ip
src_port
dest_ip
dest_port
June 22nd 2016, 16:12:33.178
nsm-64.csa1.com
ET POLICY Vulnerable Java Version 1.7.x Detected
10.26.30.100
50,232
23.67.61.168
80
Table
JSON
Link to /suricata-2016.06.22/suricata_log/AVV59Rt4UjL6lkxwcWdm
@timestamp June 22nd 2016, 16:12:33.178
@version 1
_id AVV59Rt4UjL6lkxwcWdm
_index suricata-2016.06.22
_score
_type suricata_log
alert.action allowed
alert.category Potentially Bad Traffic
alert.gid 1
alert.rev 41
alert.severity 2
alert.signature ET POLICY Vulnerable Java Version 1.7.x Detected
alert.signature_id 2,014,297
beat.hostname nsm-64.csa1.com

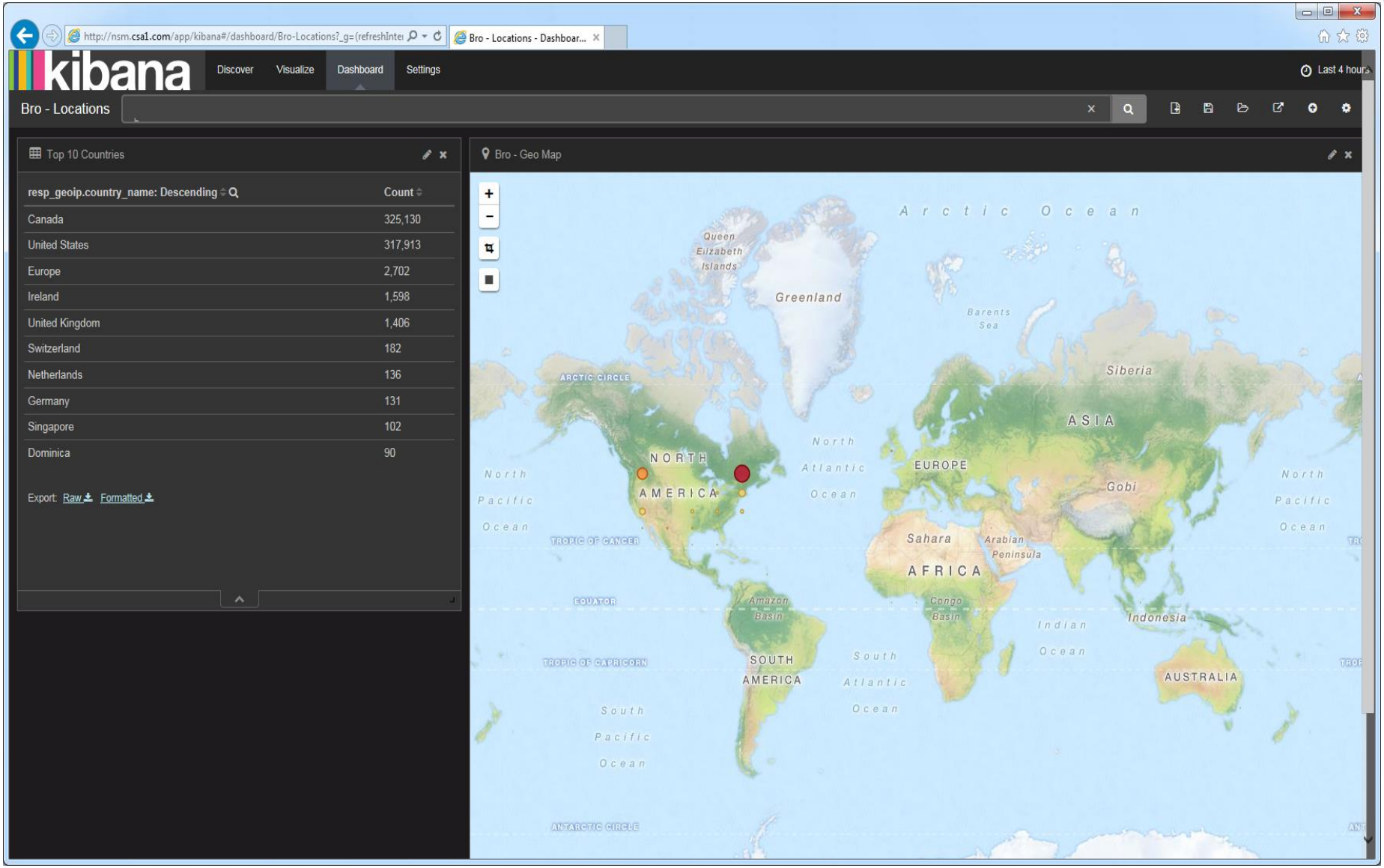

accounts


http://nsm.csa1.com/app/kibana#/dashboard/Suricata-Alerts?_g=(refreshInte
Suricata Alerts - Dashboard ...
Suricata - Alerts
t host nsm-64.csa1.com
t http.hostname securityresponse.symantec.com
t http.http_method GET
t http.http_user_agent Java/1.7.0_80
http.length 0
t http.protocol HTTP/1.1
t http.url /avcenter/sr2/threatcon.zip
t in_iface enp7s0
t input_type log
t message {"timestamp":"2016-06-22T21:12:33.178377+0000","flow_id":263690840,"in_iface":"enp7s0","event_type":"alert","src_ip":"10.26.30.100","src_port":50232,"dest_ip":"23.67.61.168","dest_port":80,"proto":"TCP","tx_id":1,"alert":{"action":"allowed","gid":1,"signature_id":2014297,"rev":41,"signature":"ET POLICY Vulnerable Java Version 1.7.x Detected","category":"Potentially Bad Traffic","severity":2},"http":{"hostname":"securityresponse.symantec.com","url":"\/avcenter\/sr2\/threatcon.zip","http_user_agent":"Java\/1.7.0_80","http_method":"GET","protocol":"HTTP\/1.1","length":0},"payload":"ROVUIC9hdmNlbnRlci9zcjIvdGhyZWF0Y29uLnppcCBIVFRQLzEuMQOKY29va2llOiA7IFJFUVVFU1RTSUc9MDg1RDUzMTgyRUQ1NDRBNkMyNDE1NOFBRjRCNOVCRjg3QzFGRERDMjEwQUMxQkFGRTFDRENCQjQONOEOMkRDNDgzMEMzRTc4QzUwMjQOMDE1MTE5NkMyNjQ4RUYyNTQxOThFMzkwOTQyN0U1QUMxOTYxNzRCOTg2NTRGQUQ2MkUzQUJFNjk1RENENEY5MjExQjQxMzk5RDMxMDQ4NzkwNEQyRUE0OEExMOIzQTI4RkQ4MzUwQzhGMjJERjEOMDdFNDA1RkI5RTNFRTY4NOIzMkVCRUIzRjBCNjhCQOUONTkxMDBCOEM2QTI5NjczMjNCOTYwMUUxQUVDREMzRTE2RENCNDVDQzExRDQ1NUUwMEU4RDMxOTM1OEJCM0ZGMkE5DQpVc2VyLUFnZW5OOiBKYXZhLzEuNy4wXzgwDQpIb3NOOiBzZWN1cml0eXJlc3BvbnNlLnN5bWFudGVjLmNvbQOKQWNjZXBOOiBOZXhOL2hObWwsIGltYWdlL2dpZiwgaW1hZ2UvanBlZywgKjsgcT0uMiwgKi8qOyBxPS4yDQpDb25uZWN0aW9uOiBrZWVwLWFsaXZlDQoNCg==","payload_printable":"GET \/avcenter\/sr2\/threatcon.zip HTTP\/1.1\r\ncookie: ; REQUESTSIG=085D53182ED544A6C24157AAF4B7EBF87C1FDDC210AC1BAFE1CDCBB447A42DC4830C3E78C5024401511196C2648EF254198E3909427E5AC196174B98654FAD62E3ABE695DCD4F9211B41399D310487904D2EA48A13B3A28FD8350C8F22DF1407E405FB9E3EE687B32EBEB3F0B68BCE45910OB8C6A2967323B9601E1AECDC3E16DCB45CC11D455E00E8D319358BB3FF2A9\r\nUser-Agent: Java\/1.7.0_80\r\nHost: securityresponse.symantec.com\r\nAccept: text\/html, image\/gif, image\/jpeg, *; q=.2, *\/*; q=.2\r\nConnection: keep-alive\r\n\r\n","stream":1,"packet":"wurkxMOcABVdHlUBCABFAAAoLbRAAIAGT7MKGh5kFOM9qMQ4AFCHDqwg9jjhulAQ+vBnzwAAAAAAAAAA"}
offset 119,084,416
t packet wurkxMOcABVdHlUBCABFAAAoLbRAAIAGT7MKGh5kFOM9qMQ4AFCHDqwg9jjhulAQ+vBnzwAAAAAAAAAA
t payload ROVUIC9hdmNlbnRlci9zcjIvdGhyZWF0Y29uLnppcCBIVFRQLzEuMQOKY29va2llOiA7IFJFUVVFU1RTSUc9MDg1RDUzMTgyRUQ1NDRBNkMyNDE1NOFBRjRCNOVCRjg3QzFGRERDMjEwQUMxQkFGRTFDRENCQjQONOEOMkRDNDgzMEMzRTc4QzUwMjQOMDE1MTE5NkMyNjQ4RUYyNTQxOThFMzkwOTQyN0U1QUMxOTYxNzRCOTg2NTRGQUQ2MkUzQUJFNjk1RENENEY5MjExQjQxMzk5RDMxMDQ4NzkwNEQyRUE0OEExMOIzQTI4RkQ4MzUwQzhGMjJERjEOMDdFNDA1RkI5RTNFRTY4NOIzMkVCRUIzRjBCNjhCQOUONTkxMDBCOEM2QTI5NjczMjNCOTYwMUUxQUVDREMzRTE2RENCNDVDQzExRDQ1NUUwMEU4RDMxOTM1OEJCM0ZGMkE5DQpVc2VyLUFnZW5OOiBKYXZhLzEuNy4wXzgwDQpIb3NOOiBzZWN1cml0eXJlc3BvbnNlLnN5bWFudGVjLmNvbQOKQWNjZXBOOiBOZXhOL2hObWwsIGltYWdlL2dpZiwgaW1hZ2UvanBlZywgKjsgcT0uMiwgKi8qOyBxPS4yDQpDb25uZWN0aW9uOiBrZWVwLWFsaXZlDQoNCg==
t payload_printable GET /avcenter/sr2/threatcon.zip HTTP/1.1
cookie: ; REQUESTSIG=085D53182ED544A6C24157AAF4B7EBF87C1FDDC210AC1BAFE1CDCBB447A42DC4830C3E78C5024401511196C2648EF254198E3909427E5AC196174B98654FAD62E3ABE695DCD4F9211B41399D310487904D2EA48A13B3A28FD8350C8F22DF1407E405FB9E3EE687B32EBEB3F0B68BCE45910OB8C6A2967323B9601E1AECDC3E16DCB45CC11D455E00E8D319358BB3FF2A9
User-Agent: Java/1.7.0_80
Host: securityresponse.symantec.com
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
t proto TCP
t source /nsm/var/log/suricata/eve.json
t src_ip 10.26.30.100
src_port 50,232

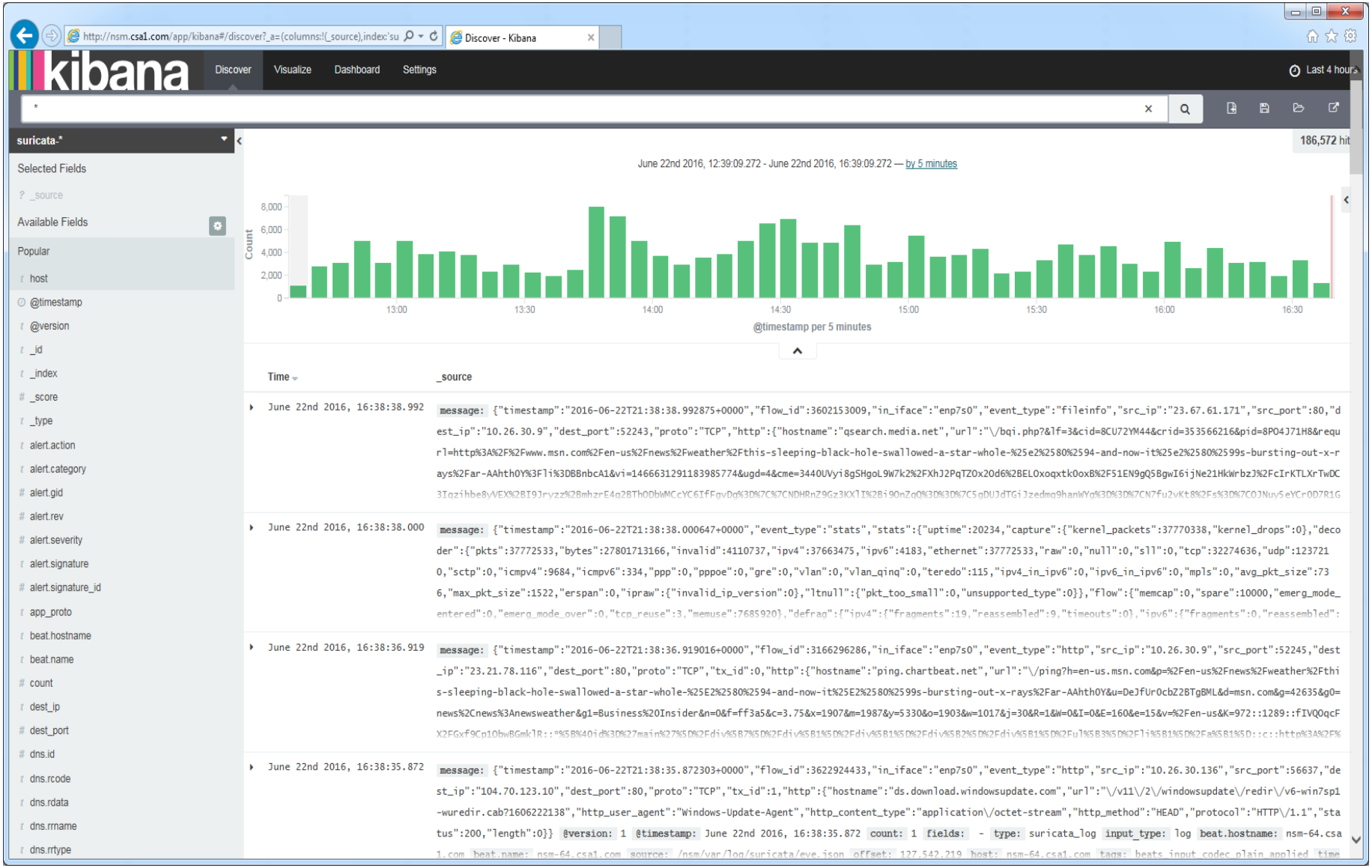

accounts


http://nsm.csa1.com/app/kibana#/dashboard/Bro-Traffic?_g=(refreshInterval
Bro - Traffic - Dashboard - ...
kibana
Discover
Visualize
Dashboard
Settings
Last 4 hours
Bro - Traffic
Bro - Total Bytes
Sum of resp_bytes
4,000,000,000
3,000,000,000
2,000,000,000
1,000,000,000
0
13:00
13:30
14:00
14:30
15:00
15:30
16:00
16:30
@timestamp per 5 minutes
Bro - Outbound Top Talkers
10.26.30.122
10.26.30.101
10.26.30.9
10.26.30.115
10.26.30.22
Bro - Packets
Sum of resp_pkts
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
13:00
13:30
14:00
14:30
15:00
15:30
16:00
16:30
@timestamp per 5 minutes
Bro - Top Destinations
131.253.40.10
65.55.2.82
10.125.255.255
224.0.0.251
224.0.0.252


accounts

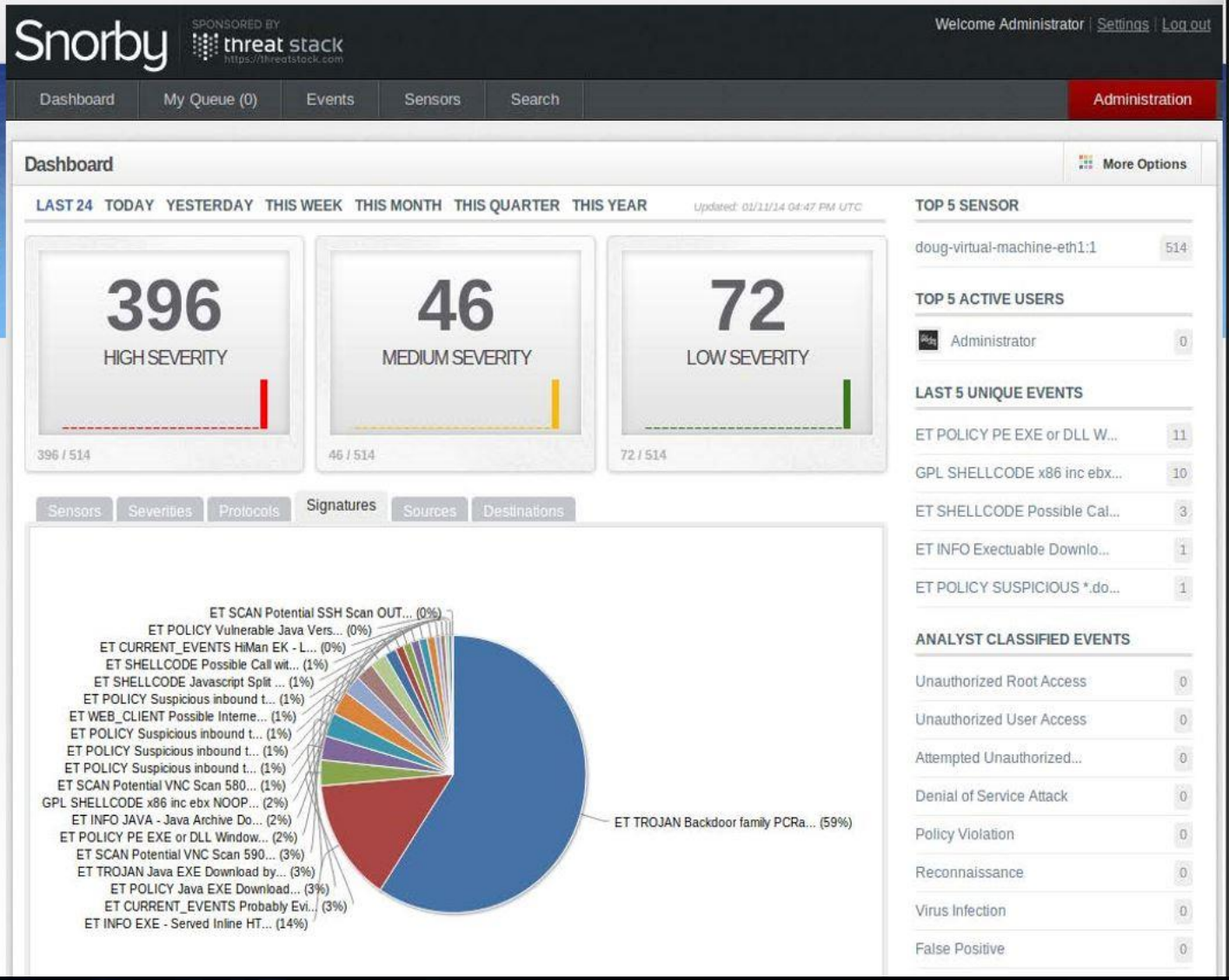

http://nsm.csa1.com/app/kibana#/dashboard/Bro-Locations?_g=(refreshInte
Bro - Locations - Dashboar...
kibana
Discover
Visualize
Dashboard
Settings
Last 4 hours
Bro - Locations
Top 10 Countries
resp_geoip.country_name: Descending
Count
Canada 325,130
United States 317,913
Europe 2,702
Ireland 1,598
United Kingdom 1,406
Switzerland 182
Netherlands 136
Germany 131
Singapore 102
Dominica 90
Export: Raw Formatted
Bro - Geo Map
Arctic Ocean
Queen Elizabeth Islands
Greenland
Barents Sea
ARCTIC CIRCLE
Siberia
ASIA
NORTH AMERICA
North Atlantic Ocean
EUROPE
Gobi
North Pacific Ocean
TROPIC OF CANCER
Sahara
Arabian Peninsula
AFRICA
EQUATOR
Amazon Basin
Congo Basin
Indonesia
Indian Ocean
TROPIC OF CAPRICORN
SOUTH AMERICA
South Atlantic Ocean
AUSTRALIA
South Pacific Ocean
ANTARCTIC CIRCLE


accounts


http://nsm.csa1.com/app/kibana#/discover?_a=(columns:!(_source),index:'su
Discover - Kibana
kibana
Discover
Visualize
Dashboard
Settings
Last 4 hours
*
suricata-*
Selected Fields
? _source
Available Fields
Popular
t host
@timestamp
t @version
t _id
t _index
_score
t _type
t alert.action
t alert.category
alert.gid
alert.rev
alert.severity
t alert.signature
alert.signature_id
t app_proto
t beat.hostname
t beat.name
count
t dest_ip
dest_port
dns.id
t dns.rcode
t dns.rdata
t dns.rrname
t dns.rrtype
186,572 hit
June 22nd 2016, 12:39:09.272 - June 22nd 2016, 16:39:09.272 — by 5 minutes
Count
8,000
6,000
4,000
2,000
0
13:00
13:30
14:00
14:30
15:00
15:30
16:00
16:30
@timestamp per 5 minutes
Time
_source
June 22nd 2016, 16:38:38.992
message: {"timestamp":"2016-06-22T21:38:38.992875+0000","flow_id":3602153009,"in_iface":"enp7s0","event_type":"fileinfo","src_ip":"23.67.61.171","src_port":80,"dest_ip":"10.26.30.9","dest_port":52243,"proto":"TCP","http":{"hostname":"qsearch.media.net","url":"\/bqi.php?&lf=3&cid=8CU72YM44&crid=353566216&pid=8PO4J71H8&requrl=http%3A%2F%2Fwww.msn.com%2Fen-us%2Fnews%2Fweather%2Fthis-sleeping-black-hole-swallowed-a-star-whole-%25e2%2580%2594-and-now-it%25e2%2580%2599s-bursting-out-x-rays%2Far-AAhth0Y%3Fli%3DBBnbcA1&vi=1466631291183985774&ugd=4&cme=344OUVyi8gSHgoL9W7k2%2FXhJ2PqTZOx2Od6%2BELOxoqxtkOoxB%2F51EN9gQ5BgwI6ijNe21HkWrbzJ%2FcIrKTLXrTwDC
June 22nd 2016, 16:38:38.000
message: {"timestamp":"2016-06-22T21:38:38.000647+0000","event_type":"stats","stats":{"uptime":20234,"capture":{"kernel_packets":37770338,"kernel_drops":0},"decoder":{"pkts":37772533,"bytes":27801713166,"invalid":4110737,"ipv4":37663475,"ipv6":4183,"ethernet":37772533,"raw":0,"null":0,"sll":0,"tcp":32274636,"udp":123721
0,"sctp":0,"icmpv4":9684,"icmpv6":334,"ppp":0,"pppoe":0,"gre":0,"vlan":0,"vlan_qinq":0,"teredo":115,"ipv4_in_ipv6":0,"ipv6_in_ipv6":0,"mpls":0,"avg_pkt_size":73
6,"max_pkt_size":1522,"erspan":0,"ipraw":{"invalid_ip_version":0},"ltnull":{"pkt_too_small":0,"unsupported_type":0}},"flow":{"memcap":0,"spare":10000,"emerg_mode_
June 22nd 2016, 16:38:36.919
message: {"timestamp":"2016-06-22T21:38:36.919016+0000","flow_id":3166296286,"in_iface":"enp7s0","event_type":"http","src_ip":"10.26.30.9","src_port":52245,"dest_ip":"23.21.78.116","dest_port":80,"proto":"TCP","tx_id":0,"http":{"hostname":"ping.chartbeat.net","url":"\/ping?h=en-us.msn.com&p=%2Fen-us%2Fnews%2Fweather%2Fthis-sleeping-black-hole-swallowed-a-star-whole-%25E2%2580%2594-and-now-it%25E2%2580%2599s-bursting-out-x-rays%2Far-AAhth0Y&u=DeJfUrOcbZ2BTgBML&d=msn.com&g=42635&g0=news%2Cnews%3Anewsweather&g1=Business%20Insider&n=0&f=ff3a5&c=3.75&x=1907&m=1987&y=5330&o=1903&w=1017&j=30&R=1&W=0&I=0&E=160&e=15&v=%2Fen-us&K=972::1289::fIVQOqcF
June 22nd 2016, 16:38:35.872
message: {"timestamp":"2016-06-22T21:38:35.872303+0000","flow_id":3622924433,"in_iface":"enp7s0","event_type":"http","src_ip":"10.26.30.136","src_port":56637,"dest_ip":"104.70.123.10","dest_port":80,"proto":"TCP","tx_id":1,"http":{"hostname":"ds.download.windowsupdate.com","url":"\/v11\/2\/windowsupdate\/redir\/v6-win7sp1-wuredir.cab?1606222138","http_user_agent":"Windows-Update-Agent","http_content_type":"application\/octet-stream","http_method":"HEAD","protocol":"HTTP\/1.1","status":200,"length":0}} @version: 1 @timestamp: June 22nd 2016, 16:38:35.872 count: 1 fields: - type: suricata_log input_type: log beat.hostname: nsm-64.csa1.com beat.name: nsm-64.csa1.com source: /nsm/var/log/suricata/eve.json offset: 127,542,219 host: nsm-64.csa1.com tags: beats_input_codec_plain_applied time

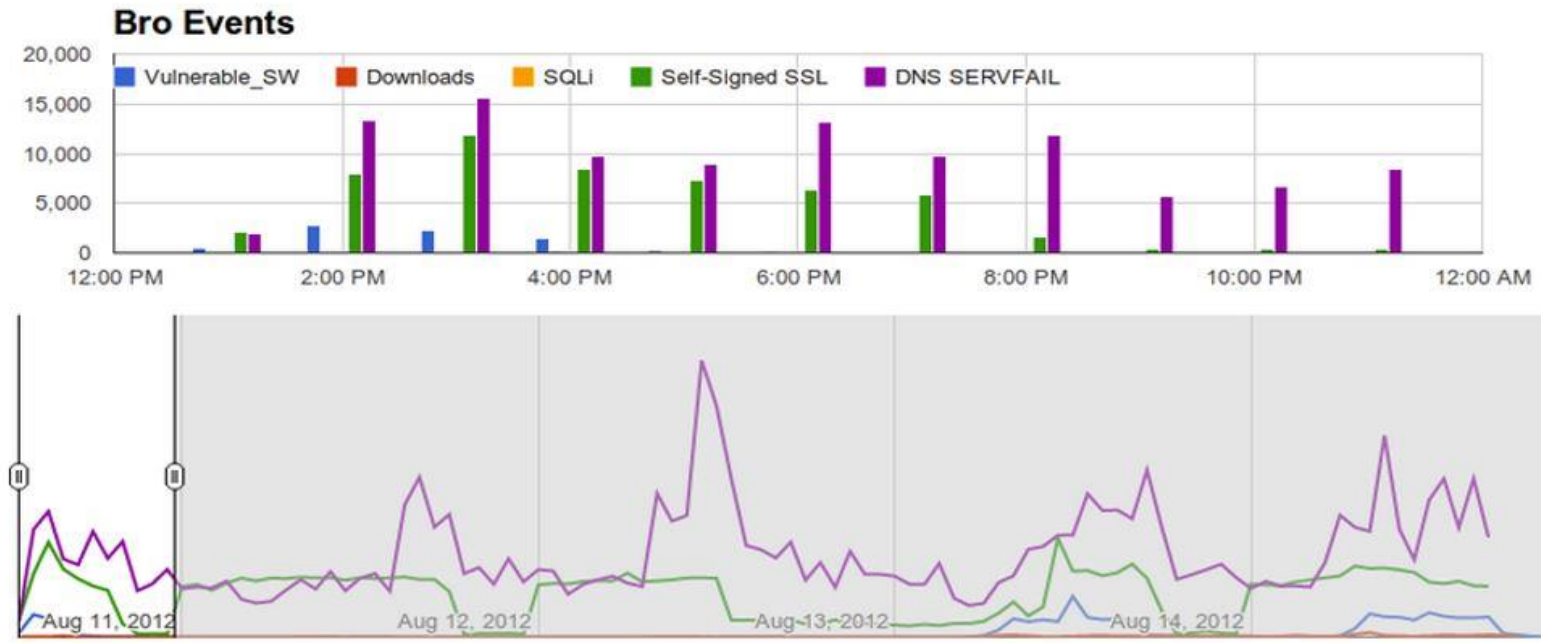

accounts

Snorby


Snorby
SPONSORED BY
threat stack
https://threatstack.com
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Dashboard
More Options
LAST 24
TODAY
YESTERDAY
THIS WEEK
THIS MONTH
THIS QUARTER
THIS YEAR
Updated: 01/11/14 04:47 PM UTC
396
HIGH SEVERITY
396 / 514
46
MEDIUM SEVERITY
46 / 514
72
LOW SEVERITY
72 / 514
Sensors
Severities
Protocols
Signatures
Sources
Destinations
ET SCAN Potential SSH Scan OUT... (0%)
ET POLICY Vulnerable Java Vers... (0%)
ET CURRENT_EVENTS HiMan EK - L... (0%)
ET SHELLCODE Possible Call wit... (1%)
ET SHELLCODE Javascript Split ... (1%)
ET POLICY Suspicious inbound t... (1%)
ET WEB_CLIENT Possible Interne... (1%)
ET POLICY Suspicious inbound t... (1%)
ET POLICY Suspicious inbound t... (1%)
ET POLICY Suspicious inbound t... (1%)
ET SCAN Potential VNC Scan 580... (1%)
GPL SHELLCODE x86 inc ebx NOOP... (2%)
ET INFO JAVA - Java Archive Do... (2%)
ET POLICY PE EXE or DLL Window... (2%)
ET SCAN Potential VNC Scan 590... (3%)
ET TROJAN Java EXE Download by... (3%)
ET POLICY Java EXE Download... (3%)
ET CURRENT_EVENTS Probably Evi... (3%)
ET INFO EXE - Served Inline HT... (14%)
ET TROJAN Backdoor family PCRa... (59%)
TOP 5 SENSOR
doug-virtual-machine-eth1:1 514
TOP 5 ACTIVE USERS
Administrator 0
LAST 5 UNIQUE EVENTS
ET POLICY PE EXE or DLL W... 11
GPL SHELLCODE x86 inc ebx... 10
ET SHELLCODE Possible Cal... 3
ET INFO Exectuable Downlo... 1
ET POLICY SUSPICIOUS *.do... 1
ANALYST CLASSIFIED EVENTS
Unauthorized Root Access 0
Unauthorized User Access 0
Attempted Unauthorized... 0
Denial of Service Attack 0
Policy Violation 0
Reconnaissance 0
Virus Infection 0
False Positive 0

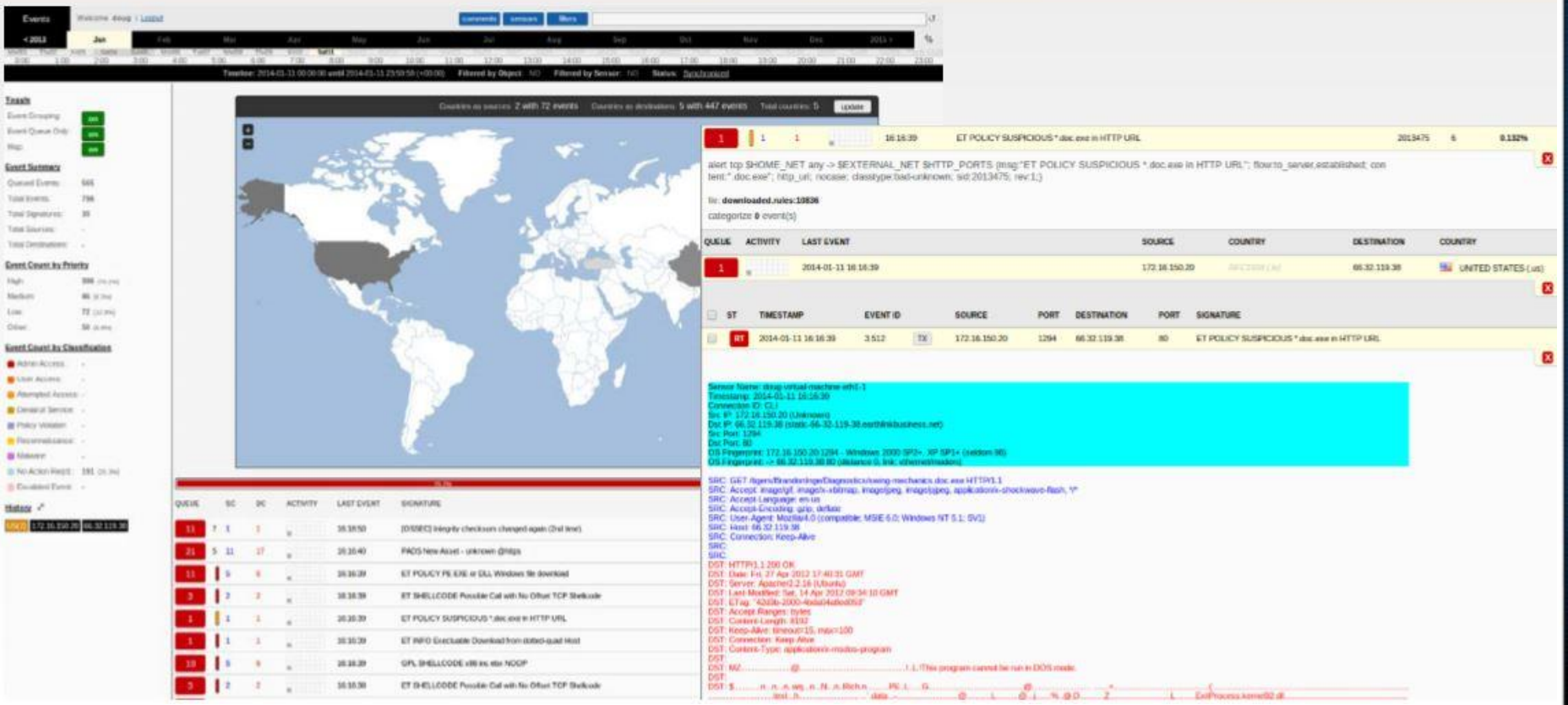

accounts

Bro IDS



subject
emailAddress=admin@wiredsolar.net,CN=secure.wiredsolar.net,OU=IT,O=Wired Solar,L=Flagler,ST=Florida,C=US
CN=rsip.monitoredsecurity.com,OU=IT Security,O=Symantec Corporation,L=Northern
emailAddress=dhoover@centonline.com,CN=Dean Hoover,OU=Network Admin,O=Ce Berlin,ST=Wisconsin,C=US
ST=Tokyo,OU=Remote Service,O=RICOH COMPANY\,LTD.,L=Aoyama,C=JP,CN=G
CN=mcs1hkg.live.citrixonline.com,OU=Operations,O=Citrix Online LLC,L=Fort Lauder
C=CA
C=US,CN=mail.tytix.com
CN=TrustedSourceServer_IMQA01

Squert web interface



Where do we go now?

http://securityonion.net

Updates are announced here and it also has the following links:

- Download/Install
- FAQ
- Mailing Lists
- IRC #securityonion on irc.freenode.net
- @securityonion
- Security Onion classes throughout 2014!

Questions?