Increase Protection & Visibility with Reduced Network Complexity

Enterprise Level Protection at SMB Prices

Increase Protection

- Network Visibility & Segmentation
- Increase & Improve Security Controls
- Maintain or Improve Usability Locally & Remote
- Utilize Low or No Cost products

Increase Visibility

Basic Security Controls

- Performance Monitoring
- Central Log Collection

Advanced Security Controls

- IPS
- IDS
- Malware
- Proxy
- SIEM

Improve Security Controls

Basic Security Controls

- Central logging of devices allows for easy search and improved troubleshooting and forensics.

Advanced Security Controls

- In most cases Companies do not have any protection except what the firewall provides.

Maintain or Improve Usability

Maintain or Improve Usability

- Implementing a secure network will provide the capabilities to securely support remote workers as well as a BYOD infrastructure.

Low or No cost

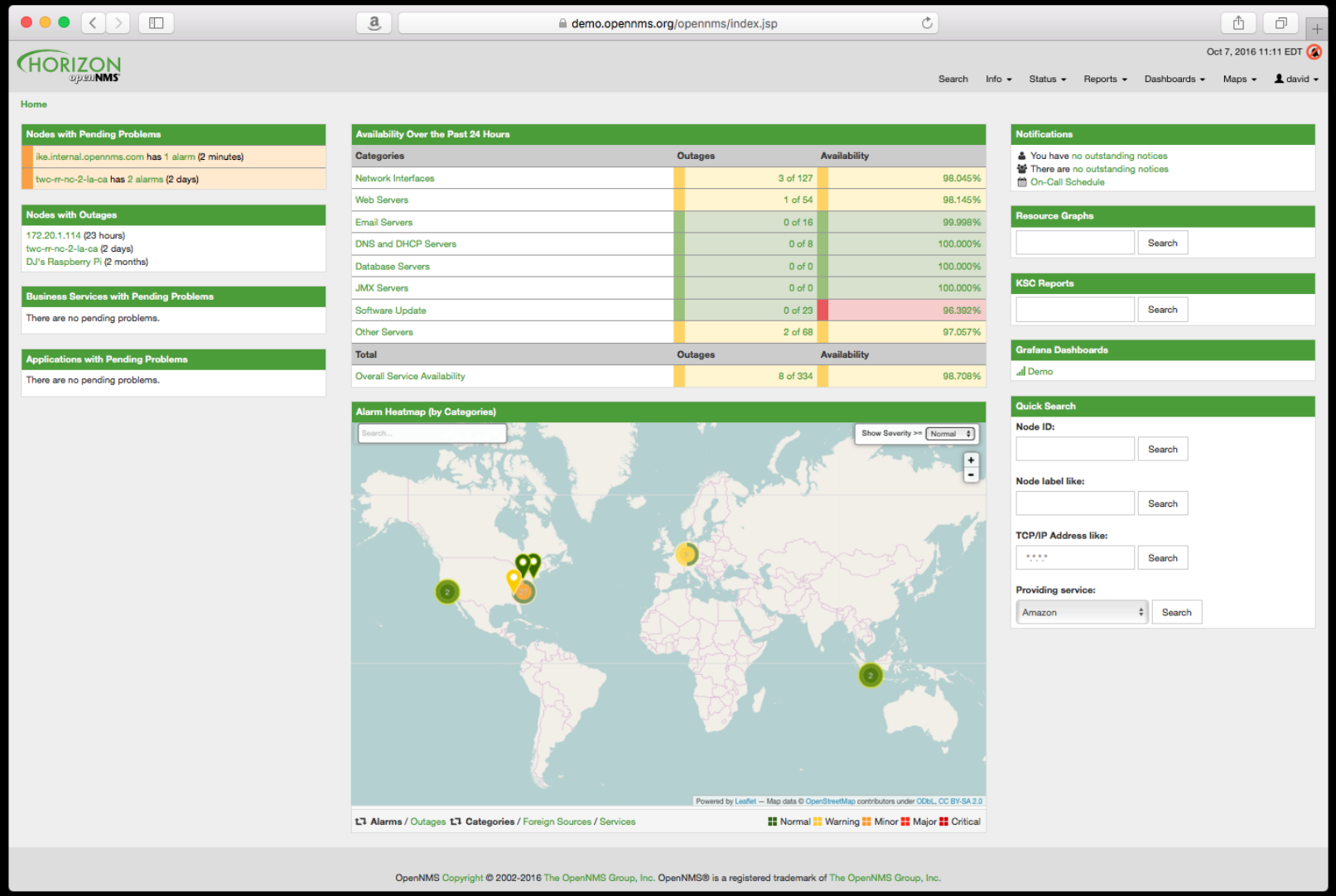
Basic Security Controls

- Performance Monitoring with openNMS
- Central Log Collection with Hydra or Rsyslog
  - Hydra must be purchased
  - Rsyslog (testing in progress)

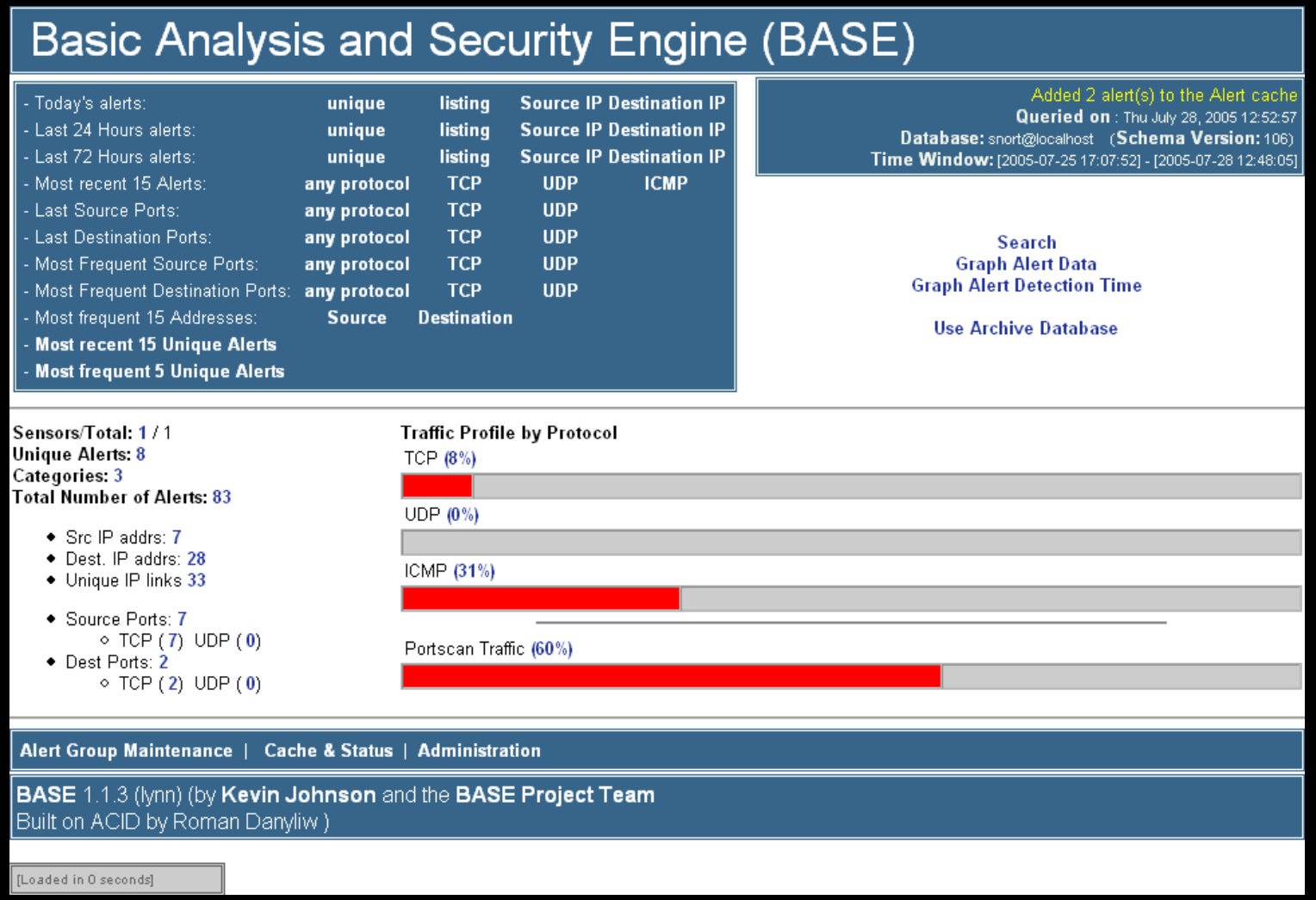
Advanced Security Controls

- IPS Using Snort
- Network level IDS Using Bro
- Network Level Malware Protection Using Mailtrail
- Proxy Using Squid *via WCCP if available*
- SIEM Using Siemonster

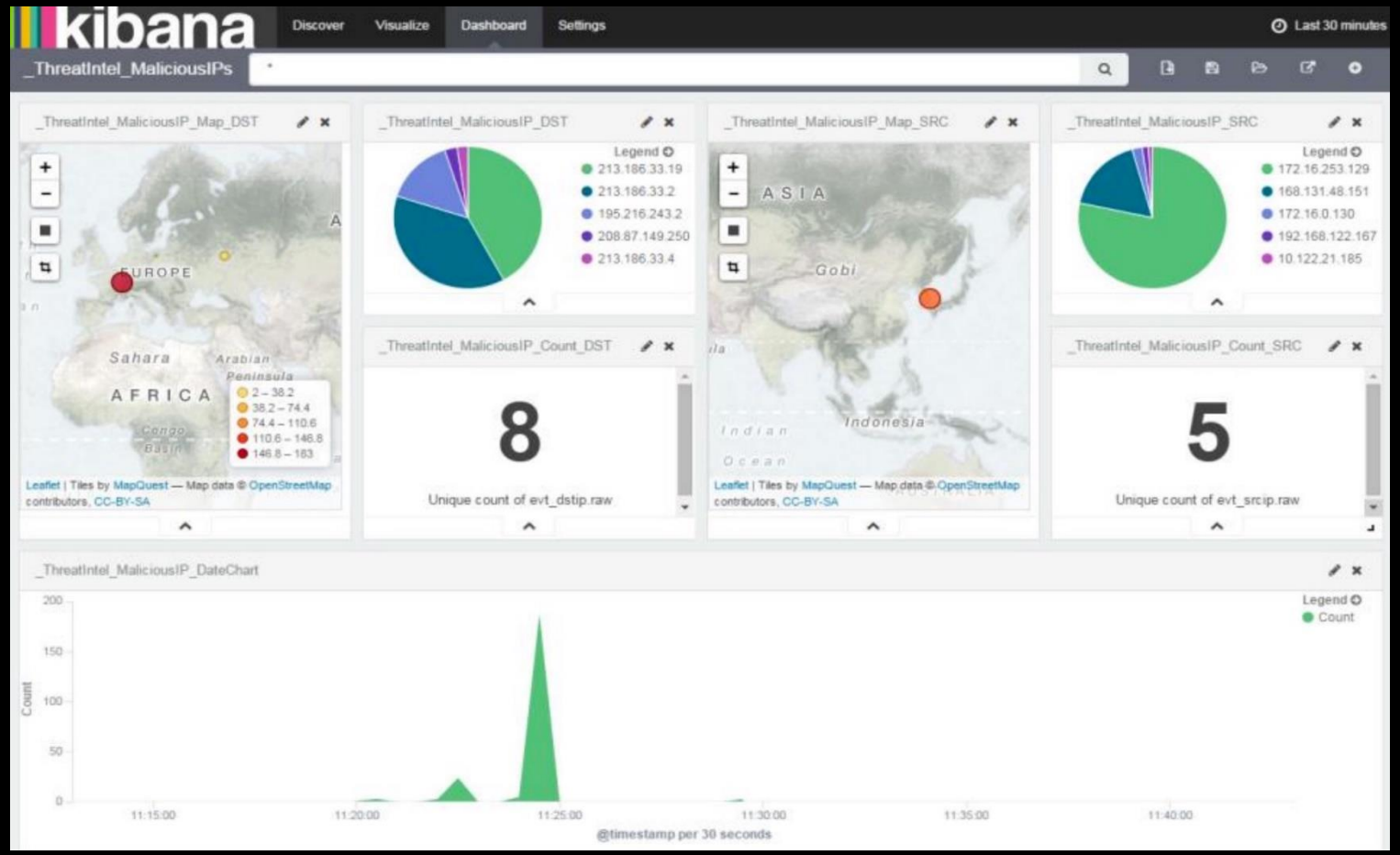
OpenNMS


demo.opennms.org/opennms/index.jsp
HORIZON openNMS
Oct 7, 2016 11:11 EDT
Search
Info
Status
Reports
Dashboards
Maps
david
Home
Nodes with Pending Problems
ike.internal.opennms.com has 1 alarm (2 minutes)
twc-rr-nc-2-la-ca has 2 alarms (2 days)
Nodes with Outages
172.20.1.114 (23 hours)
twc-rr-nc-2-la-ca (2 days)
DJ's Raspberry Pi (2 months)
Business Services with Pending Problems
There are no pending problems.
Applications with Pending Problems
There are no pending problems.
Availability Over the Past 24 Hours
Categories
Outages
Availability
Network Interfaces 3 of 127 98.045%
Web Servers 1 of 54 98.145%
Email Servers 0 of 16 99.998%
DNS and DHCP Servers 0 of 8 100.000%
Database Servers 0 of 0 100.000%
JMX Servers 0 of 0 100.000%
Software Update 0 of 23 96.392%
Other Servers 2 of 68 97.057%
Total Outages Availability
Overall Service Availability 8 of 334 98.708%
Alarm Heatmap (by Categories)
Show Severity >= Normal
Alarms / Outages Categories / Foreign Sources / Services
Normal Warning Minor Major Critical
Notifications
You have no outstanding notices
There are no outstanding notices
On-Call Schedule
Resource Graphs
Search
KSC Reports
Search
Grafana Dashboards
Demo
Quick Search
Node ID:
Search
Node label like:
Search
TCP/IP Address like:
Search
Providing service:
Amazon
Search
OpenNMS Copyright © 2002-2016 The OpenNMS Group, Inc. OpenNMS® is a registered trademark of The OpenNMS Group, Inc.

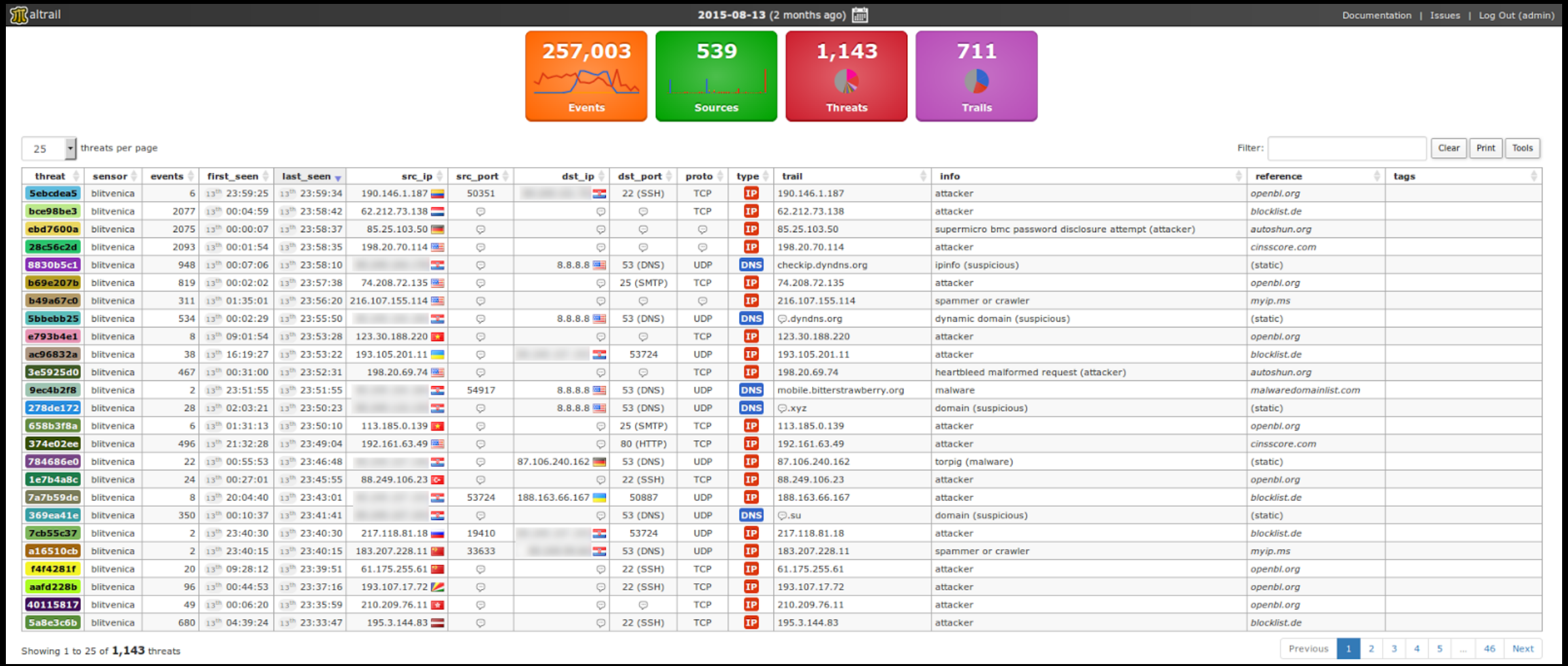
SNORT W/ BASE


Basic Analysis and Security Engine (BASE)
- Today's alerts: unique listing Source IP Destination IP
- Last 24 Hours alerts: unique listing Source IP Destination IP
- Last 72 Hours alerts: unique listing Source IP Destination IP
- Most recent 15 Alerts: any protocol TCP UDP ICMP
- Last Source Ports: any protocol TCP UDP
- Last Destination Ports: any protocol TCP UDP
- Most Frequent Source Ports: any protocol TCP UDP
- Most Frequent Destination Ports: any protocol TCP UDP
- Most frequent 15 Addresses: Source Destination
- Most recent 15 Unique Alerts
- Most frequent 5 Unique Alerts
Added 2 alert(s) to the Alert cache
Queried on : Thu July 28, 2005 12:52:57
Database: snort@localhost (Schema Version: 106)
Time Window: [2005-07-25 17:07:52] - [2005-07-28 12:48:05]
Search
Graph Alert Data
Graph Alert Detection Time
Use Archive Database
Sensors/Total: 1 / 1
Unique Alerts: 8
Categories: 3
Total Number of Alerts: 83
Src IP addrs: 7
Dest. IP addrs: 28
Unique IP links 33
Source Ports: 7
TCP (7) UDP (0)
Dest Ports: 2
TCP (2) UDP (0)
Traffic Profile by Protocol
TCP (8%)
UDP (0%)
ICMP (31%)
Portscan Traffic (60%)
Alert Group Maintenance | Cache & Status | Administration
BASE 1.1.3 (lynn) (by Kevin Johnson and the BASE Project Team
Built on ACID by Roman Danyliw)
[Loaded in 0 seconds]

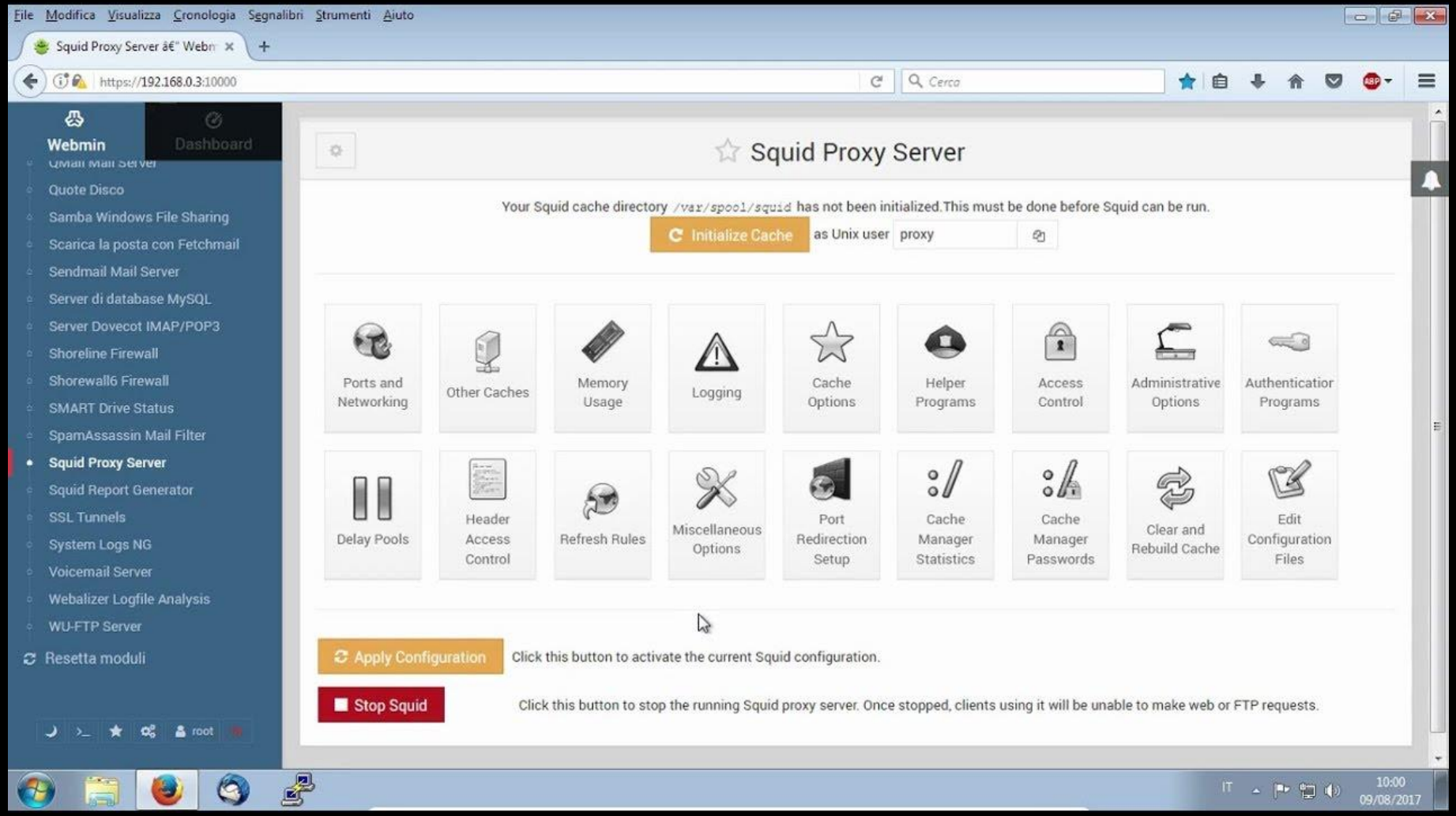
BRO W/ Kabana


kibana
Discover
Visualize
Dashboard
Settings
Last 30 minutes
_ThreatIntel_MaliciousIPs
_ThreatIntel_MaliciousIP_Map_DST
EUROPE
Sahara
Arabian Peninsula
AFRICA
Congo Basin
2 – 38.2
38.2 – 74.4
74.4 – 110.6
110.6 – 146.8
146.8 – 183
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
_ThreatIntel_MaliciousIP_DST
Legend
213.186.33.19
213.186.33.2
195.216.243.2
208.87.149.250
213.186.33.4
_ThreatIntel_MaliciousIP_Count_DST
8
Unique count of evt_dstip.raw
_ThreatIntel_MaliciousIP_Map_SRC
ASIA
Gobi
Indian Ocean
Indonesia
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA
_ThreatIntel_MaliciousIP_SRC
Legend
172.16.253.129
168.131.48.151
172.16.0.130
192.168.122.167
10.122.21.185
_ThreatIntel_MaliciousIP_Count_SRC
5
Unique count of evt_srcip.raw
_ThreatIntel_MaliciousIP_DateChart
Legend
Count
200
150
100
50
0
Count
11:15:00
11:20:00
11:25:00
11:30:00
11:35:00
11:40:00
@timestamp per 30 seconds

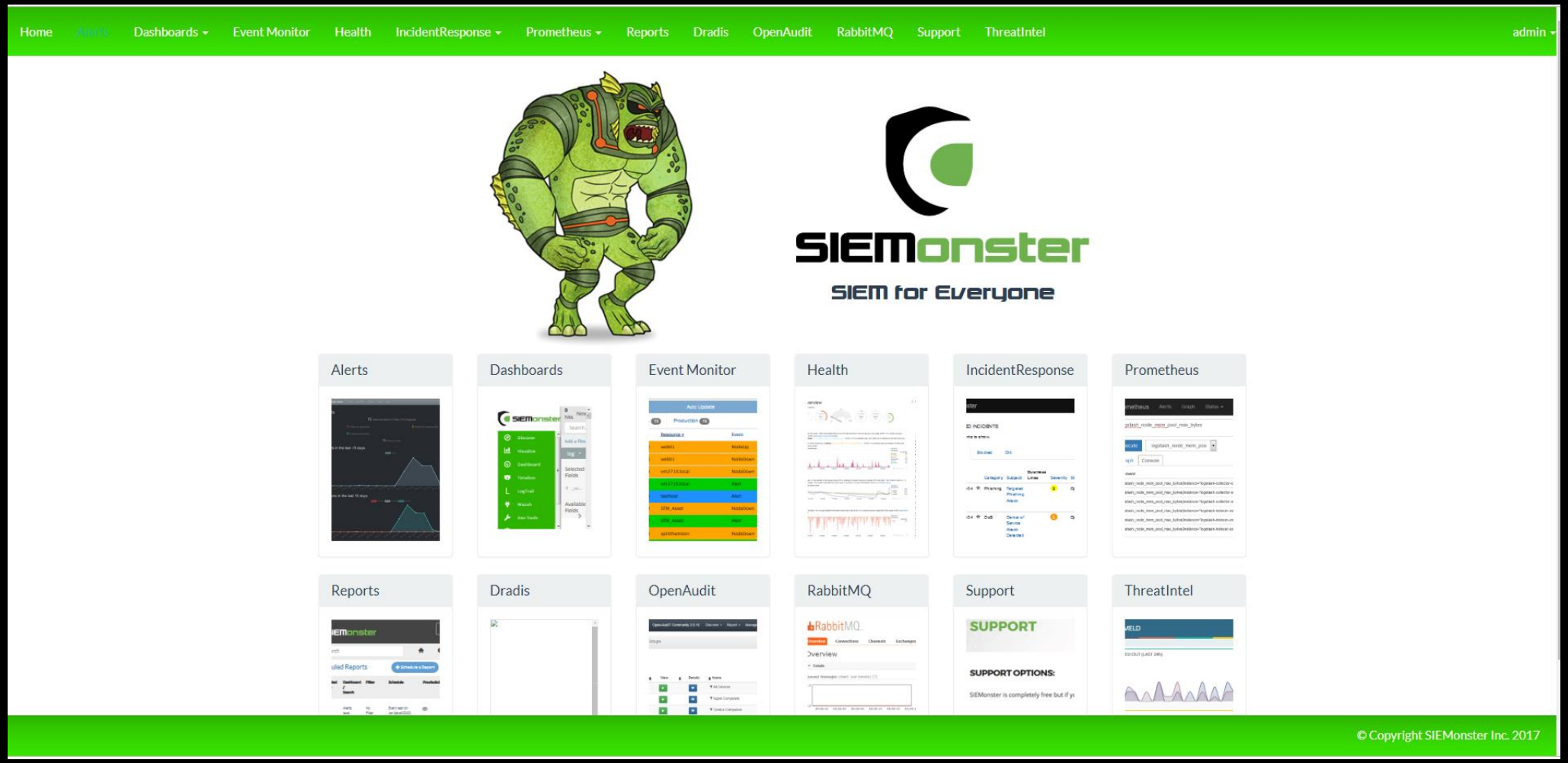
Mailtrail

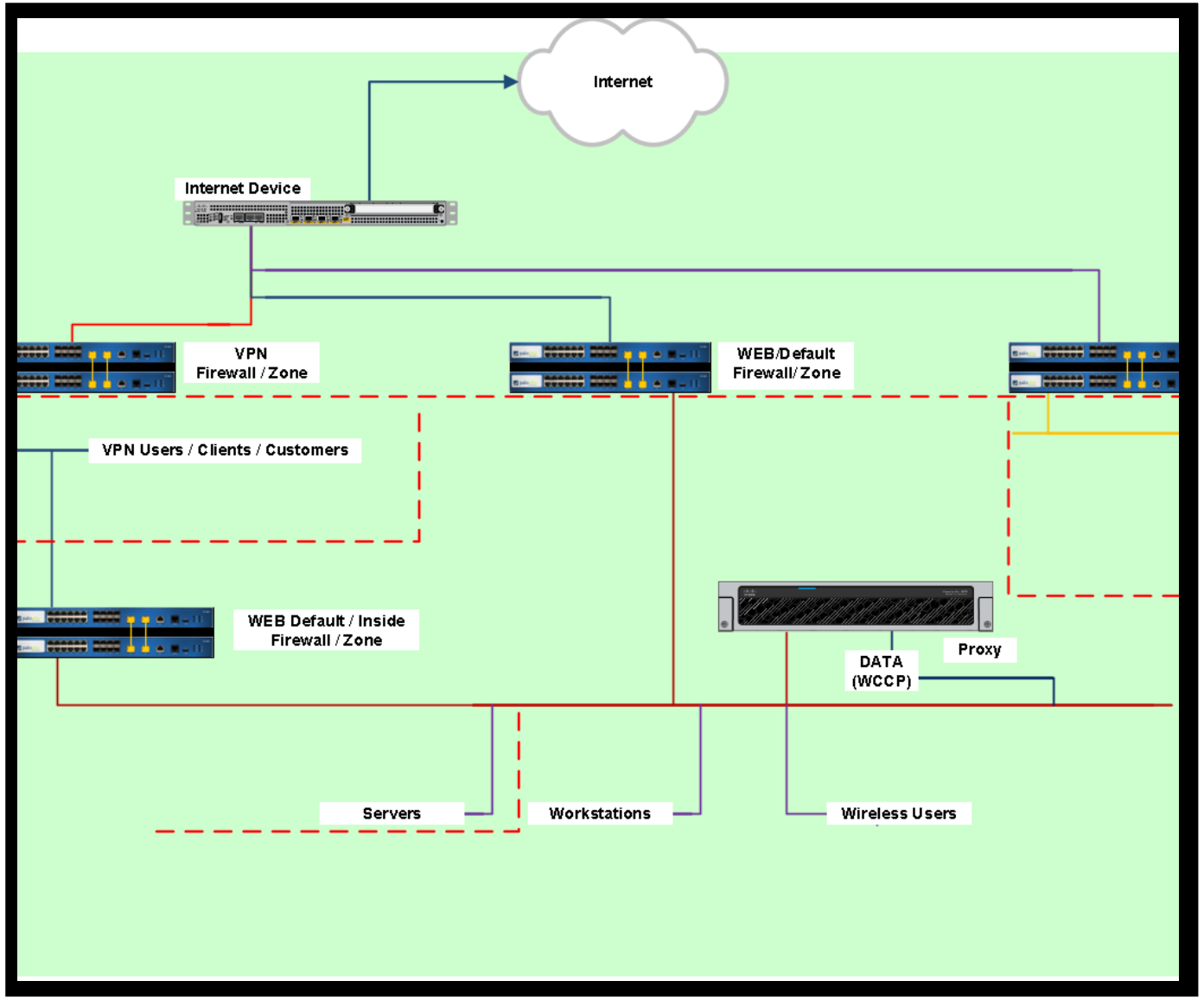

altrail
2015-08-13 (2 months ago)
Documentation | Issues | Log Out (admin)
257,003
Events
539
Sources
1,143
Threats
711
Trails
25 threats per page
Filter:
Clear
Print
Tools
threat | sensor | events | first_seen | last_seen | src_ip | src_port | dst_ip | dst_port | proto | type | trail | info | reference | tags
5ebcdea5 | blitvenica | 6 | 13th 23:59:25 | 13th 23:59:34 | 190.146.1.187 | 50351 | [redacted] | 22 (SSH) | TCP | IP | 190.146.1.187 | attacker | openbl.org
bce98be3 | blitvenica | 2077 | 13th 00:04:59 | 13th 23:58:42 | 62.212.73.138 | | | | TCP | IP | 62.212.73.138 | attacker | blocklist.de
ebd7600a | blitvenica | 2075 | 13th 00:00:07 | 13th 23:58:37 | 85.25.103.50 | | | | | IP | 85.25.103.50 | supermicro bmc password disclosure attempt (attacker) | autoshun.org
28c56c2d | blitvenica | 2093 | 13th 00:01:54 | 13th 23:58:35 | 198.20.70.114 | | | | | IP | 198.20.70.114 | attacker | cinsscore.com
8830b5c1 | blitvenica | 948 | 13th 00:07:06 | 13th 23:58:10 | [redacted] | | 8.8.8.8 | 53 (DNS) | UDP | DNS | checkip.dyndns.org | ipinfo (suspicious) | (static)
b69e207b | blitvenica | 819 | 13th 00:02:02 | 13th 23:57:38 | 74.208.72.135 | | | 25 (SMTP) | TCP | IP | 74.208.72.135 | attacker | openbl.org
b49a67c0 | blitvenica | 311 | 13th 01:35:01 | 13th 23:56:20 | 216.107.155.114 | | | | | IP | 216.107.155.114 | spammer or crawler | myip.ms
5bbebb25 | blitvenica | 534 | 13th 00:02:29 | 13th 23:55:50 | [redacted] | | 8.8.8.8 | 53 (DNS) | UDP | DNS | .dyndns.org | dynamic domain (suspicious) | (static)
e793b4e1 | blitvenica | 8 | 13th 09:01:54 | 13th 23:53:28 | 123.30.188.220 | | | | TCP | IP | 123.30.188.220 | attacker | openbl.org
ac96832a | blitvenica | 38 | 13th 16:19:27 | 13th 23:53:22 | 193.105.201.11 | | [redacted] | 53724 | UDP | IP | 193.105.201.11 | attacker | blocklist.de
3e5925d0 | blitvenica | 467 | 13th 00:31:00 | 13th 23:52:31 | 198.20.69.74 | | | | TCP | IP | 198.20.69.74 | heartbleed malformed request (attacker) | autoshun.org
9ec4b2f8 | blitvenica | 2 | 13th 23:51:55 | 13th 23:51:55 | [redacted] | 54917 | 8.8.8.8 | 53 (DNS) | UDP | DNS | mobile.bitterstrawberry.org | malware | malwaredomainlist.com
278de172 | blitvenica | 28 | 13th 02:03:21 | 13th 23:50:23 | [redacted] | | 8.8.8.8 | 53 (DNS) | UDP | DNS | .xyz | domain (suspicious) | (static)
658b3f8a | blitvenica | 6 | 13th 01:31:13 | 13th 23:50:10 | 113.185.0.139 | | | 25 (SMTP) | TCP | IP | 113.185.0.139 | attacker | openbl.org
374e02ee | blitvenica | 496 | 13th 21:32:28 | 13th 23:49:04 | 192.161.63.49 | | | 80 (HTTP) | TCP | IP | 192.161.63.49 | attacker | cinsscore.com
784686e0 | blitvenica | 22 | 13th 00:55:53 | 13th 23:46:48 | [redacted] | | 87.106.240.162 | 53 (DNS) | UDP | IP | 87.106.240.162 | torpig (malware) | (static)
1e7b4a8c | blitvenica | 24 | 13th 00:27:01 | 13th 23:45:55 | 88.249.106.23 | | | 22 (SSH) | TCP | IP | 88.249.106.23 | attacker | openbl.org
7a7b59de | blitvenica | 8 | 13th 20:04:40 | 13th 23:43:01 | [redacted] | 53724 | 188.163.66.167 | 50887 | UDP | IP | 188.163.66.167 | attacker | blocklist.de
369ea41e | blitvenica | 350 | 13th 00:10:37 | 13th 23:41:41 | [redacted] | | | 53 (DNS) | UDP | DNS | .su | domain (suspicious) | (static)
7cb55c37 | blitvenica | 2 | 13th 23:40:30 | 13th 23:40:30 | 217.118.81.18 | 19410 | [redacted] | 53724 | UDP | IP | 217.118.81.18 | attacker | blocklist.de
a16510cb | blitvenica | 2 | 13th 23:40:15 | 13th 23:40:15 | 183.207.228.11 | 33633 | [redacted] | 53 (DNS) | UDP | IP | 183.207.228.11 | spammer or crawler | myip.ms
f4f4281f | blitvenica | 20 | 13th 09:28:12 | 13th 23:39:51 | 61.175.255.61 | | | 22 (SSH) | TCP | IP | 61.175.255.61 | attacker | openbl.org
aafd228b | blitvenica | 96 | 13th 00:44:53 | 13th 23:37:16 | 193.107.17.72 | | | 22 (SSH) | TCP | IP | 193.107.17.72 | attacker | openbl.org
40115817 | blitvenica | 49 | 13th 00:06:20 | 13th 23:35:59 | 210.209.76.11 | | | | TCP | IP | 210.209.76.11 | attacker | openbl.org
5a8e3c6b | blitvenica | 680 | 13th 04:39:24 | 13th 23:33:47 | 195.3.144.83 | | | 22 (SSH) | TCP | IP | 195.3.144.83 | attacker | blocklist.de
Showing 1 to 25 of 1,143 threats
Previous 1 2 3 4 5 ... 46 Next

Squid W/webmin

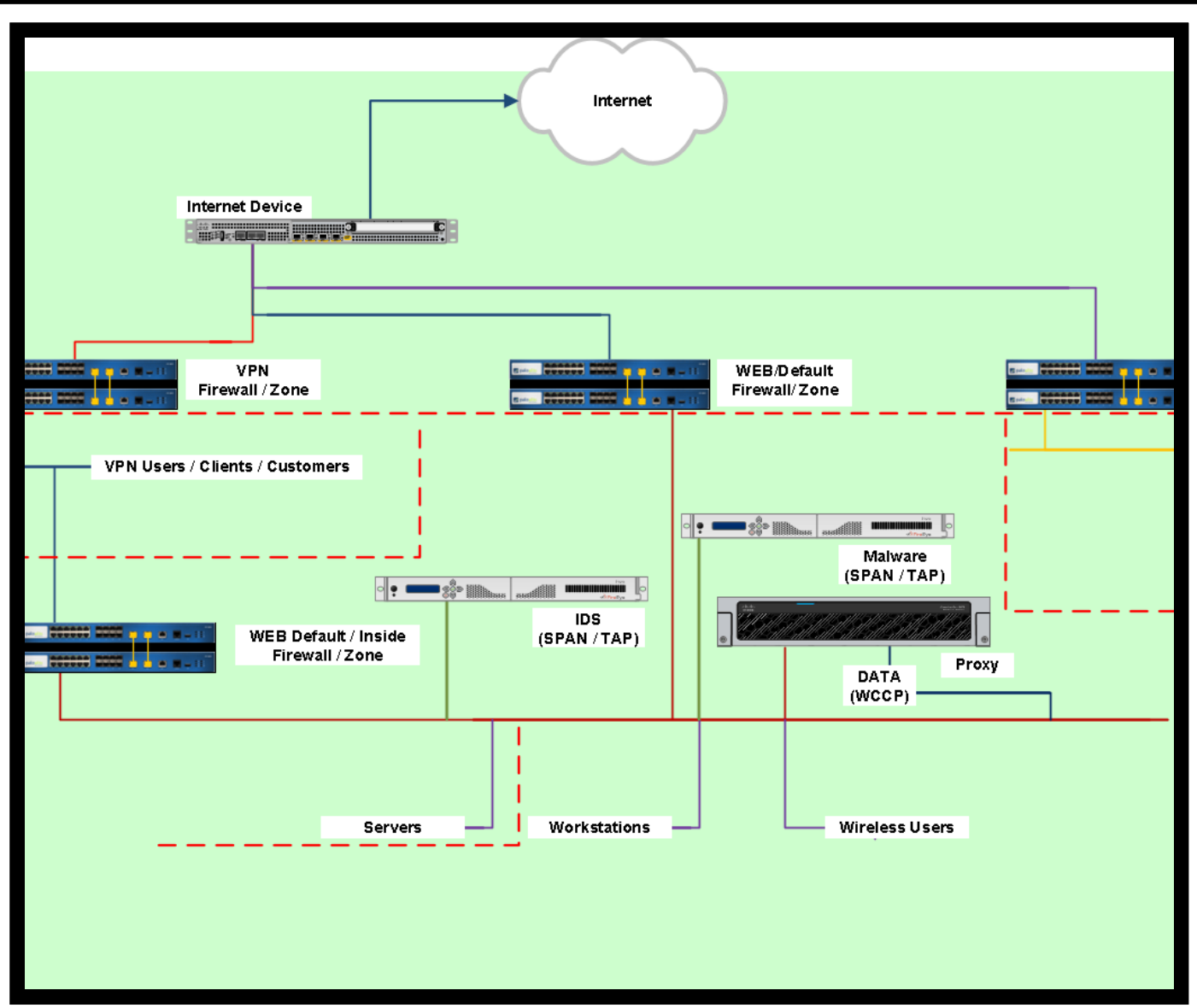


SIEMonster

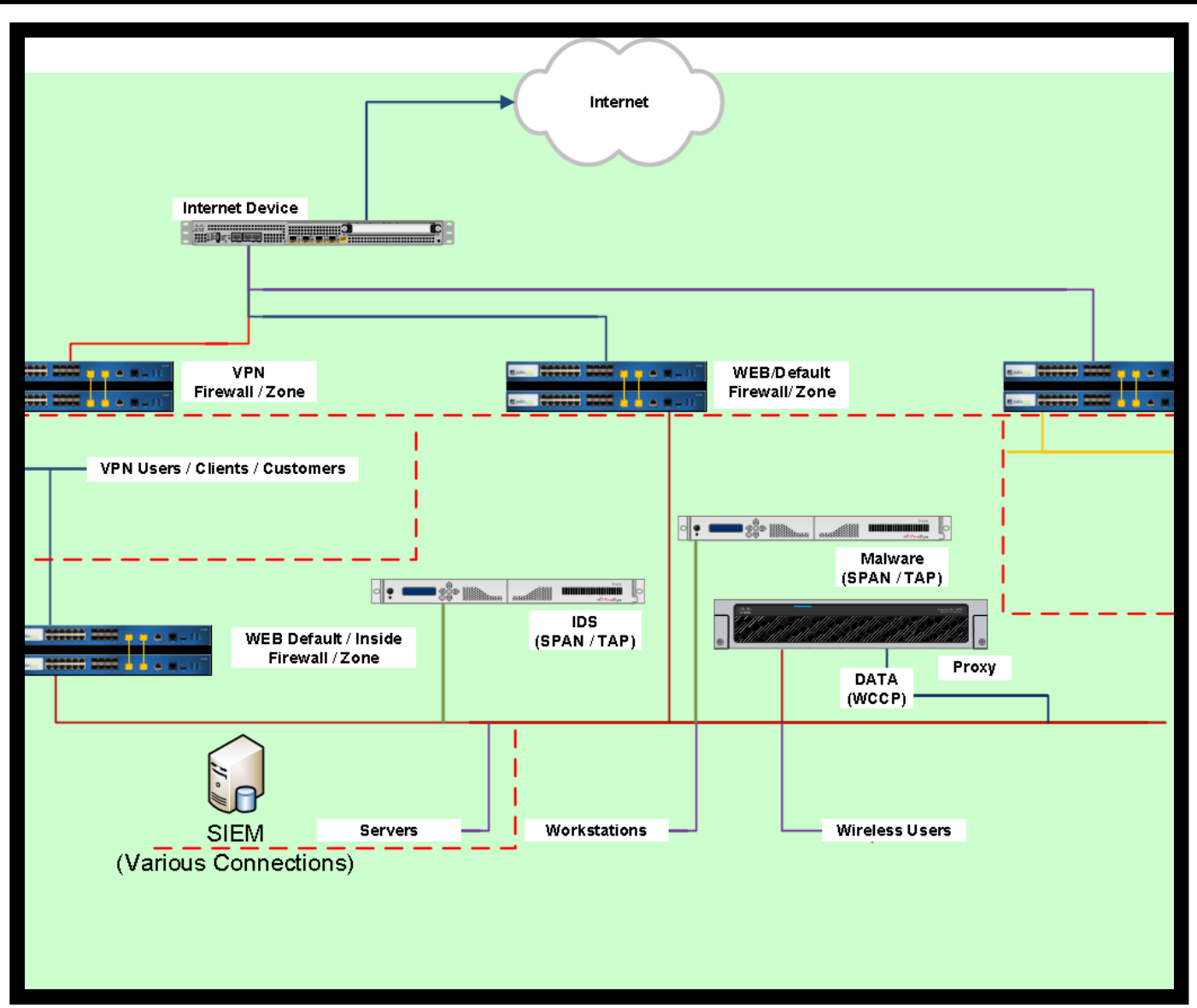

Home
Alerts
Dashboards
Event Monitor
Health
IncidentResponse
Prometheus
Reports
Dradis
OpenAudit
RabbitMQ
Support
ThreatIntel
admin
SIEMonster
SIEM for Everyone
Alerts
Dashboards
Event Monitor
Health
IncidentResponse
Prometheus
Reports
Dradis
OpenAudit
RabbitMQ
Support
ThreatIntel
SUPPORT
SUPPORT OPTIONS:
© Copyright SIEMonster Inc. 2017



Sample Basic Network



Sample Intermediate Network



Sample Advanced Network

Minimum Requirements

For Basic Protection

- Hypervisor (to deploy virtual proxy)
  - 64 GB RAM
  - HDD Space (Based on OS and events saved)
  - 4 Core Processor
  - 2 Network interfaces

Minimum Requirements

For Intermediate Protection

- Server
  - 16 GB RAM
  - 60GB Free HDD Space (Host Information)
  - 4 Core Processor
  - 2 Network interfaces
- Hypervisor
  - 64+ GB RAM
  - HDD Space (Based on OS and events saved)
  - 4 Core Processor
  - 4 Network interfaces

Minimum Requirements

For Advanced Protection

- 3 Servers
  - 32 GB RAM
  - 60GB Free HDD Space (Host Information)
  - 8 Core Processor
  - 2 Network interfaces
- 2 Servers
  - 64 GB RAM
  - 60GB Free HDD Space (Host Information)
  - 16 Core Processor
  - 2 Network interfaces
- Hypervisor
  - 224 GB RAM
  - HDD Space (Based on OS and events saved)
  - 56 Core Processor
  - 8 Network interfaces

NOTE Event Rate: ~ 47 million events per hour scalable upwards 30-day time frame for open indices 6 months' data maintained onsite / Weekly snapshots Data archive to AWS Glacier/S3

Install LINKS

Security Control	Website	Install link
OSSEC	https://www.ossec.net/	https://updates.atomicorp.com/channels/ossec-3-testing/windows/
Open NMS	https://www.opennms.org/en	https://www.opennms.org/en/install
SNORT	https://www.snort.org/	
BRO (Zeek)	https://www.zeek.org/index.html	https://www.vultr.com/docs/installing-bro-ids-on-ubuntu-16-04
Maltrail	https://github.com/stamparm/maltrail	https://www.howtoforge.com/tutorial/installation-and-usage-of-maltrail-detection-system-on-ubuntu/
Squid	http://www.squid-cache.org/	https://www.howtoforge.com/set-up-squid-siblings-on-centos-6.3-with-wccp
SIEMonster	https://siemonster.com/	https://plasso.com/s/wRQDBoUXK5/

QUESTIONS?