The Modern SOC

Adapting the Security Operations model to how we work.

- The Classic SOC Model
- SOC as a Service
- The Security Landscape
- Gaps
- **Adapting to Now**

Security Operations

An Overview


Beijing
Tokyo
Los Angeles
New York
London
Berlin
Moscow
Cyber Security Operations Center

What the SOC is Protecting

- Data
- PII
- Users
- Systems

The SOC

How it works

Collect
IDS Alerts, Logs, Network Flow

Organize
Sinkhole, Databases, Categorization, Inventory, Log Aggregation

Analyze
Anomalies, Alerts, patterns

Report
Stats, Communication, contact levels, consistent info

Incident Response
Your customers

Infrastructure

Infrastructure

IDS

NETFLOW

TVA

SIEM

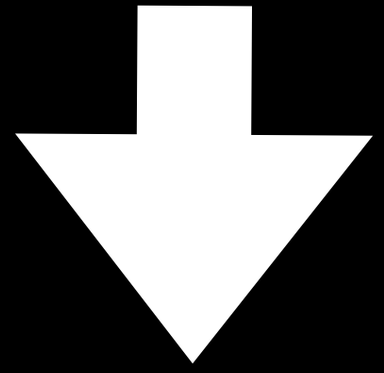
LOGGING

ANALYSIS SYSTEMS

INCIDENT RESPONSE

Network

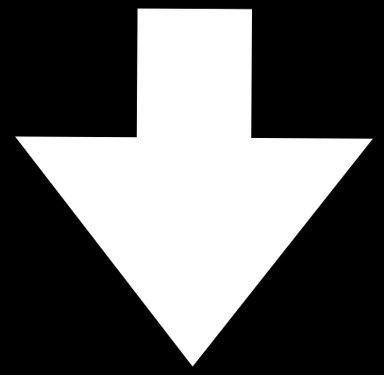
IDS Packets Flow DNS



SIEM

Log Aggregation

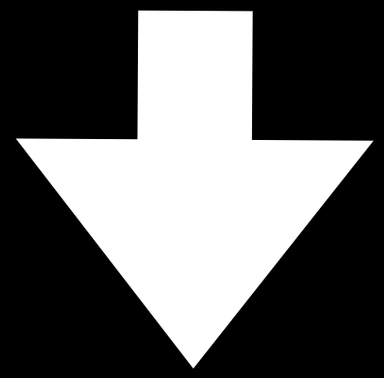
Firewall DNS AD Web Mail



SIEM/Splunk/ELK

Email

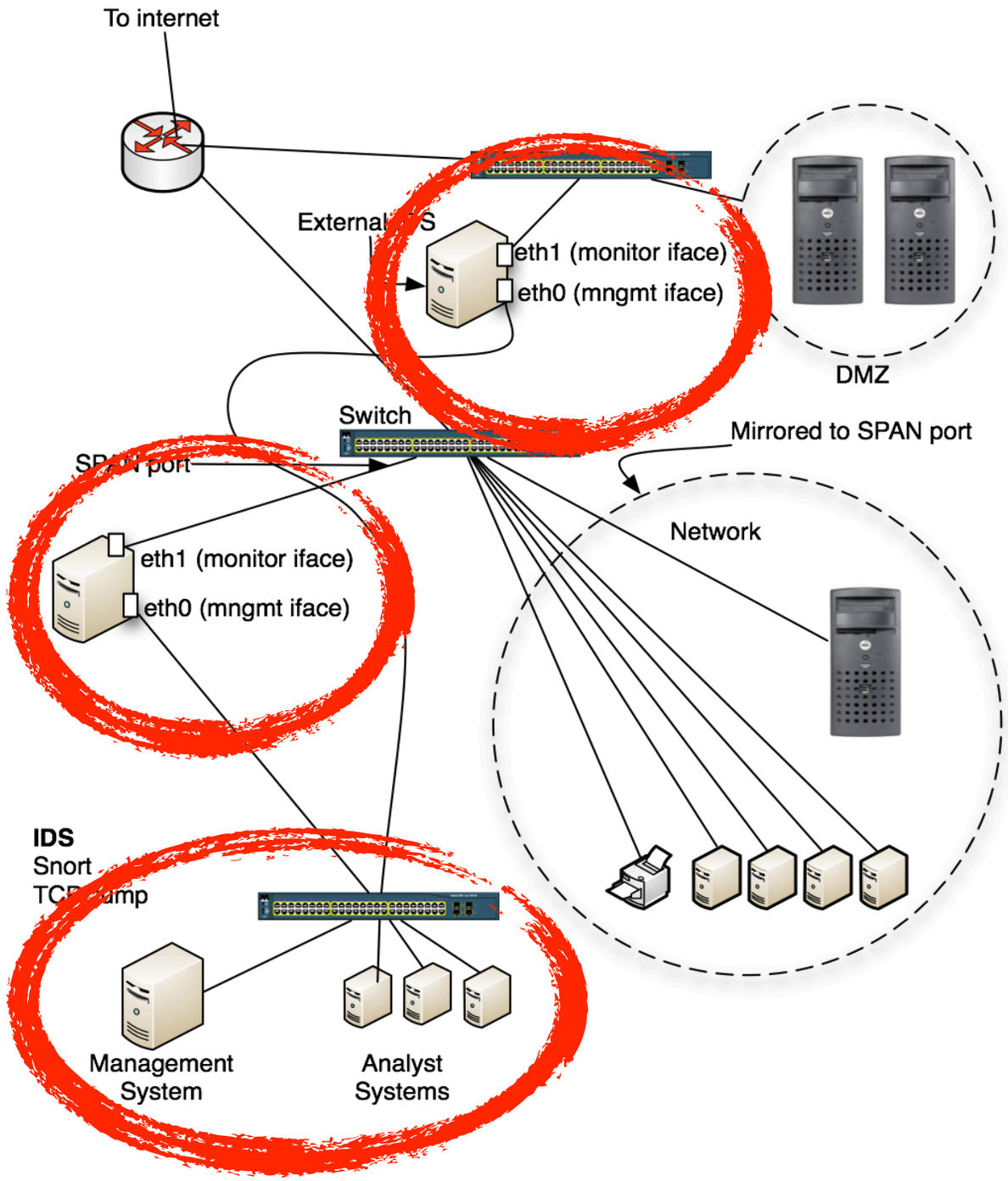
Flow Attachments



SIEM/Splunk/ELK

Infrastructure

The Classic Model



Don’t give the Interface an IP address

```
auto eth0
iface eth0 inet static
      address 192.168.1.205
      network 192.168.1.0
      netmask 255.255.255.0
      broadcast 192.168.1.255
      gateway 192.168.1.1
~
~
```

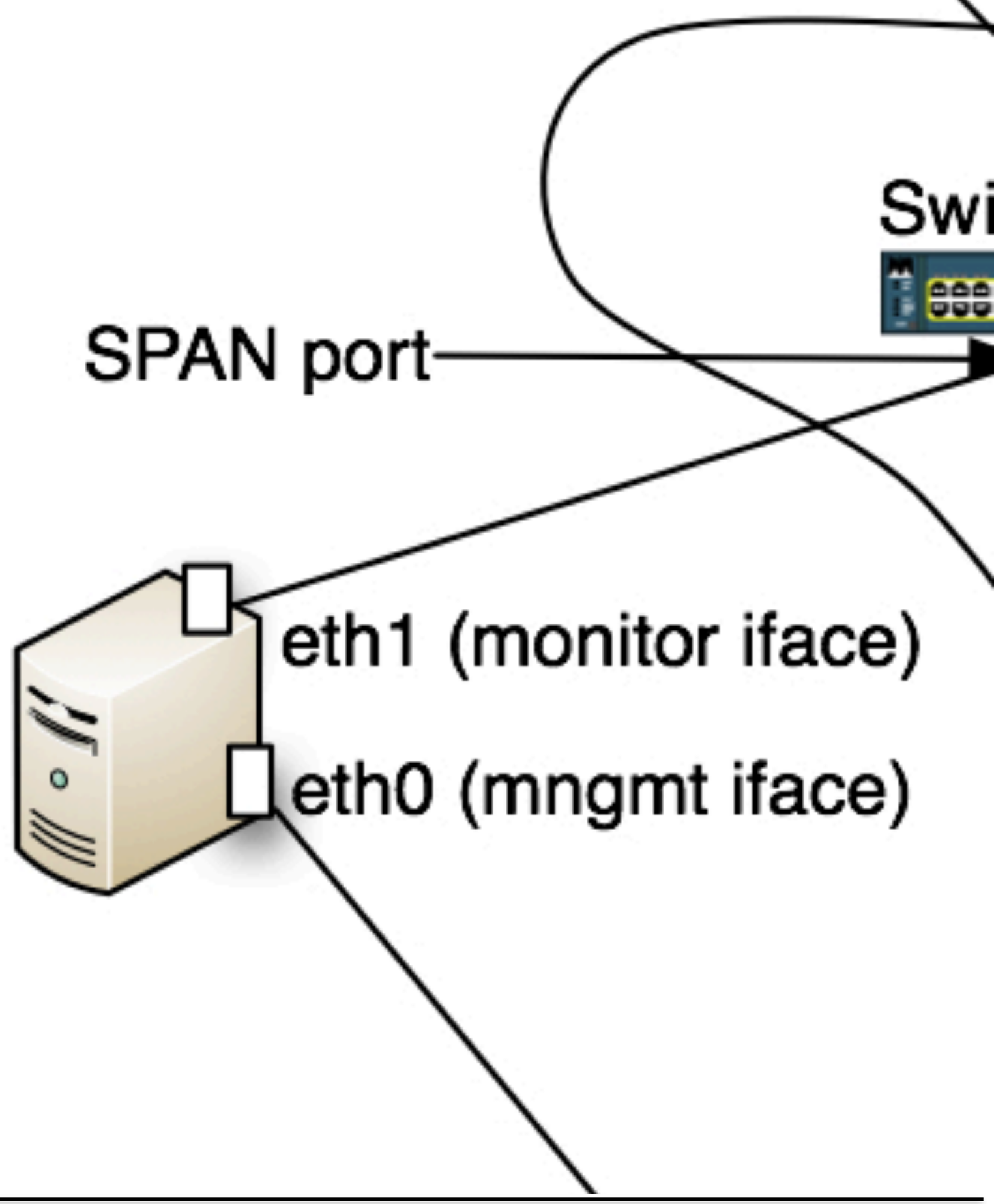
Can still respond to protocols below IP stack

Cut pin one (orange/white)
Solder a 23 pF capacitor

Cut pin one (orange/white)
Solder a 23 pF capacitor

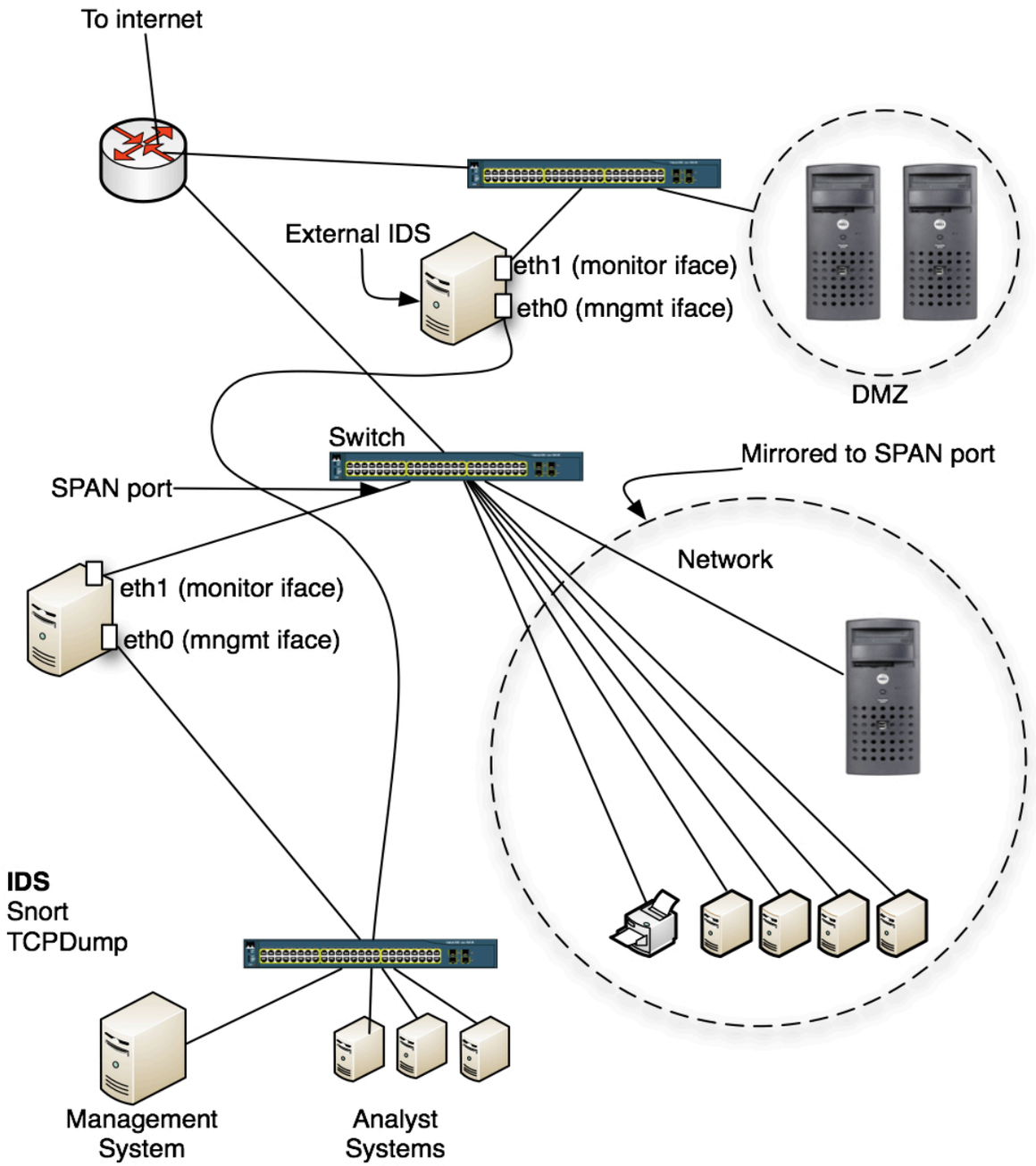
Infrastructure

The Classic Model



Infrastructure

The Classic Model



SIEM

- Log Collection
- Log Analysis
- Event Correlation
- Log Forensics
- IT Compliance
- Application Log Monitoring
- Object Access Auditing
- Real-time Alerting
- User Activity Monitoring
- Dashboards
- Reporting
- File Integrity Monitoring
- System & Device Log Monitoring
- Log Retention

File Edit View Window Tools System Help

Navigator

Resources | Packages

Reports Ctrl+Alt+R

Reports | Trends | Queries | Templates | Archives

- Reports
  - admin's Reports
    - admin's Running Reports
  - Shared
    - All Reports
      - ArcSight Administration
      - ArcSight Foundation
      - ArcSight Solutions
      - ArcSight System
      - JumpStart
      - LOGbinder
        - SP
          - Information Management Policy Changes
          - SharePoint Access Control Changes
          - SharePoint Audit Trail Integrity Events
          - SharePoint Container Object Update Events
          - SharePoint Document Update Events
          - SharePoint Generic Object Change Events
          - SharePoint ImportExport Events
          - SharePoint List Update Events
          - SharePoint View Events
          - User Activity Report
      - Personal
      - Public
      - Unassigned

Viewer

Object Activity Summary | Search Activity | Security Changes | SharePoint Audit Snapshot | Audit Flag by User Snapshot

Active Channel: Audit Flag by User Snapshot Total Events: 135

Start Time: 14 Aug 2012 21:03:00 MDT
End Time: 14 Aug 2012 21:14:54 MDT
Filter: (Target User Name = "Richard Lowe" And Audit Flag = "View" And (Type != "Correlation" And Device Product = "SP" And Device Vendor = "LOG...
Inline Filter: No Filter
Verified Rules: No Rule

Very High: 0
High: 0
Medium: 135
Low: 0
Very Low: 0

Radar

End Time	Device Host Name	Device Event Class ID	Name	Object Title	Object Type	Target User N
8/14 21:08:40	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:40	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:40	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:36	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:37	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:44	LOGbinder-collector	49	List viewed	Tasks	Generic List	Richard Lowe
8/14 21:08:34	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:33	LOGbinder-collector	49	List viewed	Tasks	Generic List	Richard Lowe
8/14 21:08:30	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:25	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:21	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:17	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:14	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:08:14	LOGbinder-collector	48	Document library viewed	Health Records		Richard Lowe
8/14 21:08:04	LOGbinder-collector	49	List viewed	Tasks	Generic List	Richard Lowe
8/14 21:08:06	LOGbinder-collector	49	List viewed	Tasks	Generic List	Richard Lowe
8/14 21:08:07	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:07:27	LOGbinder-collector	48	Document library viewed	Shared Documents		Richard Lowe
8/14 21:07:13	LOGbinder-collector	47	Document viewed	n/a		Richard Lowe

Grid

IBM Security QRadar SIEM

admin ▼ Preferences ▼ Help ▼ Messages 5 ▼

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Vulnerabilities | Admin | System Ti

Show Dashboard: Vulnerability Management | New Dashboard | Rename Dashboard | Delete Dashboard | Add Item... ▼ | Refresh Paused: 00:00:35

Security News

Last updated Tue May 21 17:17:26 GMT 2013

- Third of Cyber Attacks Come From China
- Cisco to buy Israel-based software maker for $475 million
- School that expelled student hacker may have ignored 16-month-old security flaw
- FlightTrack Soars, FlightBoard Bores
- School Kicks Out Sophomore in RFID Student-ID Flap

Security Advisories

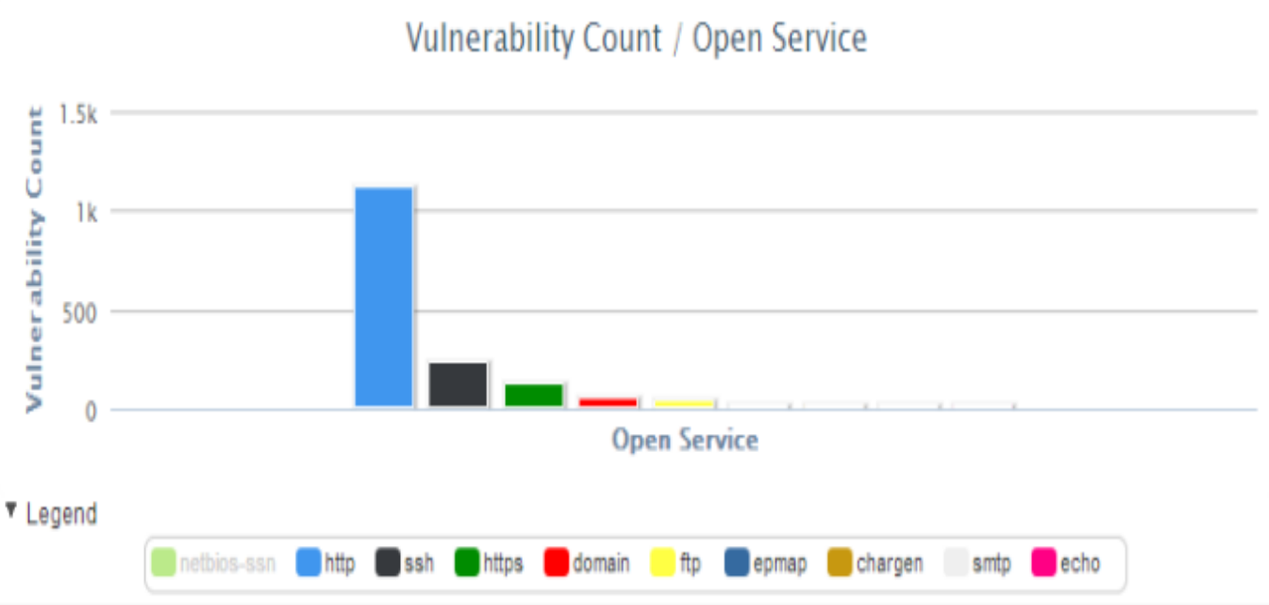
Last updated Tue May 21 17:17:26 GMT 2013

- ownCloud - Multiple Cross-Site Scripting Issues
- BIG-IP - SQL Injection Issue
- BIG-IP - XML External Entity Injection Issue
- DigiLIBE Management Console - Execution After Redirect Issue
- Linksys WRT54GL - Multiple Issues

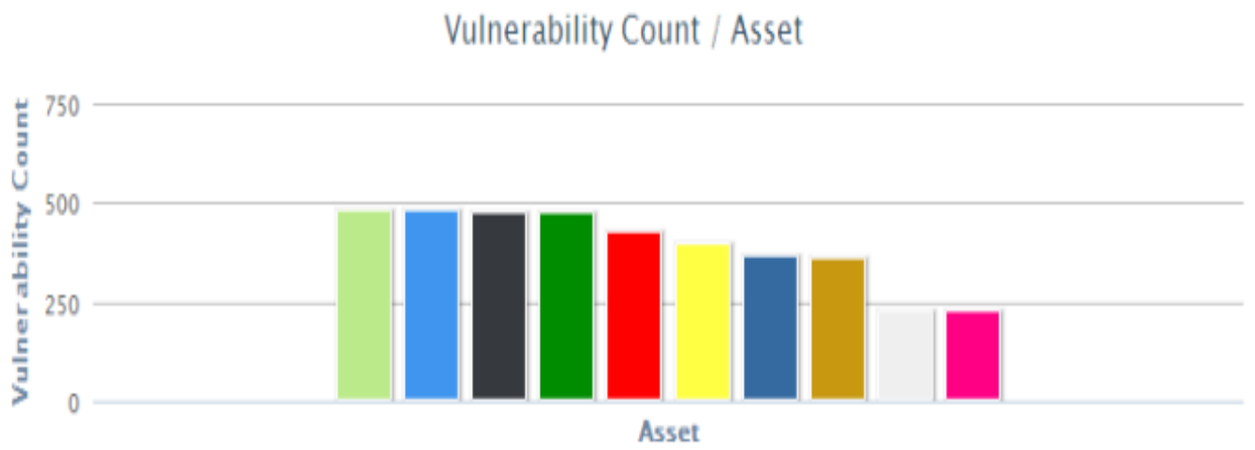
Network All

Vulnerability	Vulnerability Count
ICMP Timestamp Request	85
Trace Route Information	84
Web Service is Running	58
2012-0814 - OpenSSH - Information Disclosure Issue	41
2011-5000 - OpenSSH - Denial-Of-Service Issue	41
OpenSSH J-PAKE Public Parameter Validation Shared Secret Authentication Bypass	34
SSL - Self-Signed Certificate	32
Information Leak - NetBios Information Disclosure	29
TRACE - Possible Unnecessary Web Method	21
TRACK-TRACE - Cross-site tracing attack via HTTP	21

All



PCI Failures



Open Services All

Scans In Progress

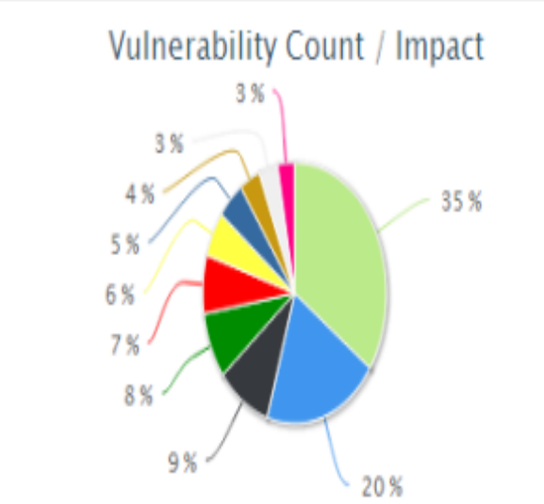
Last updated Tue May 21 17:17:26 GMT 2013

Scans Completed

Last updated Tue May 21 17:17:26 GMT 2013

- HMS test scan - 2013-05-09 16:53:16
- demo test - 2013-05-08 14:26:37
- Windows patch scan - 2013-05-07 16:07:38
- RC:Windows patch scan - 2013-04-30 16:32:05
- Windows patch scan - 2013-04-19 22:13:49

Impact All



Latest Published Vulnerabilities

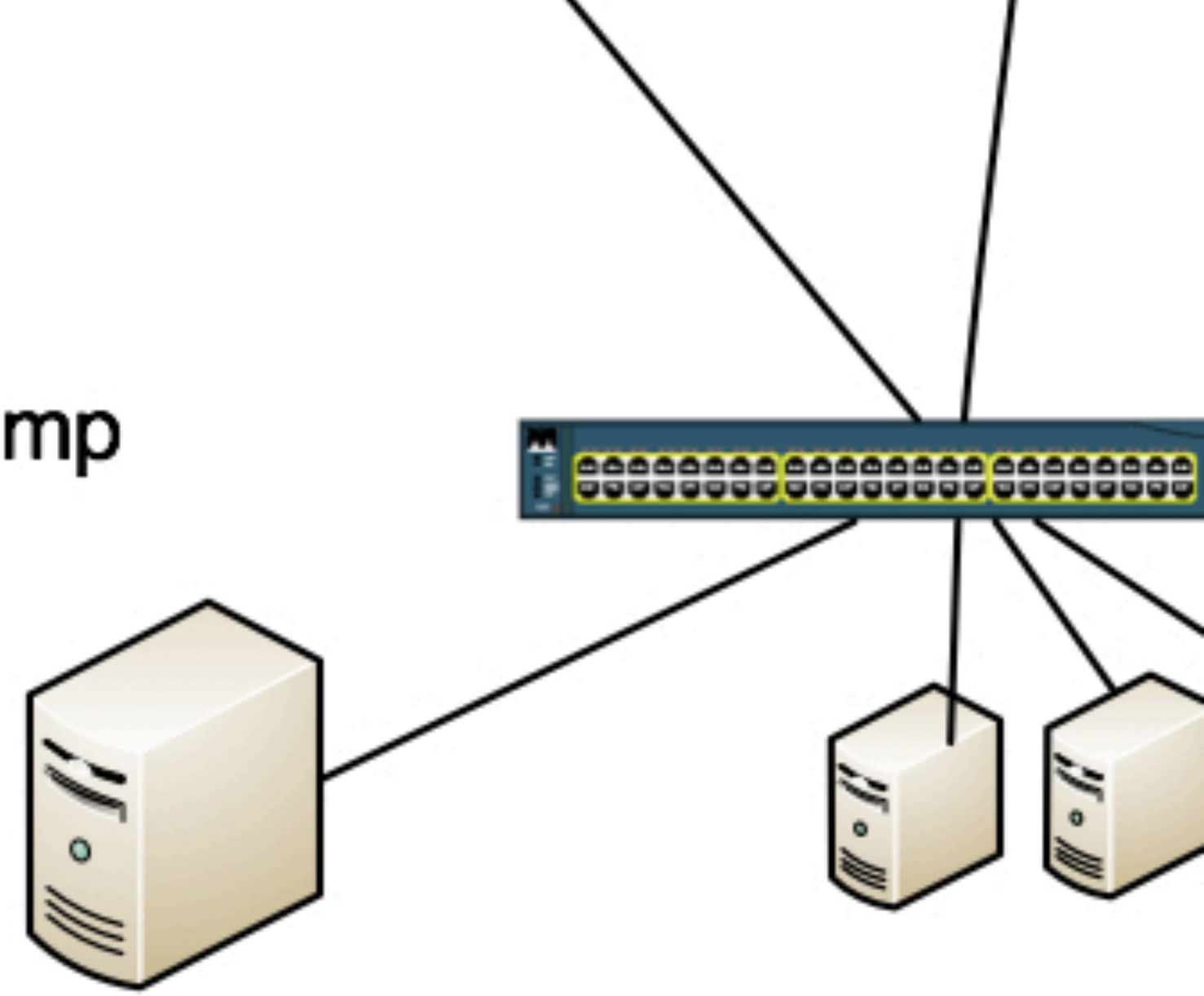
Last updated Tue May 21 17:17:26 GMT 2013

MIS|TI TRAINING INSTITUTE

Infrastructu

The Classic Model

IDS
Snort
TCPDump

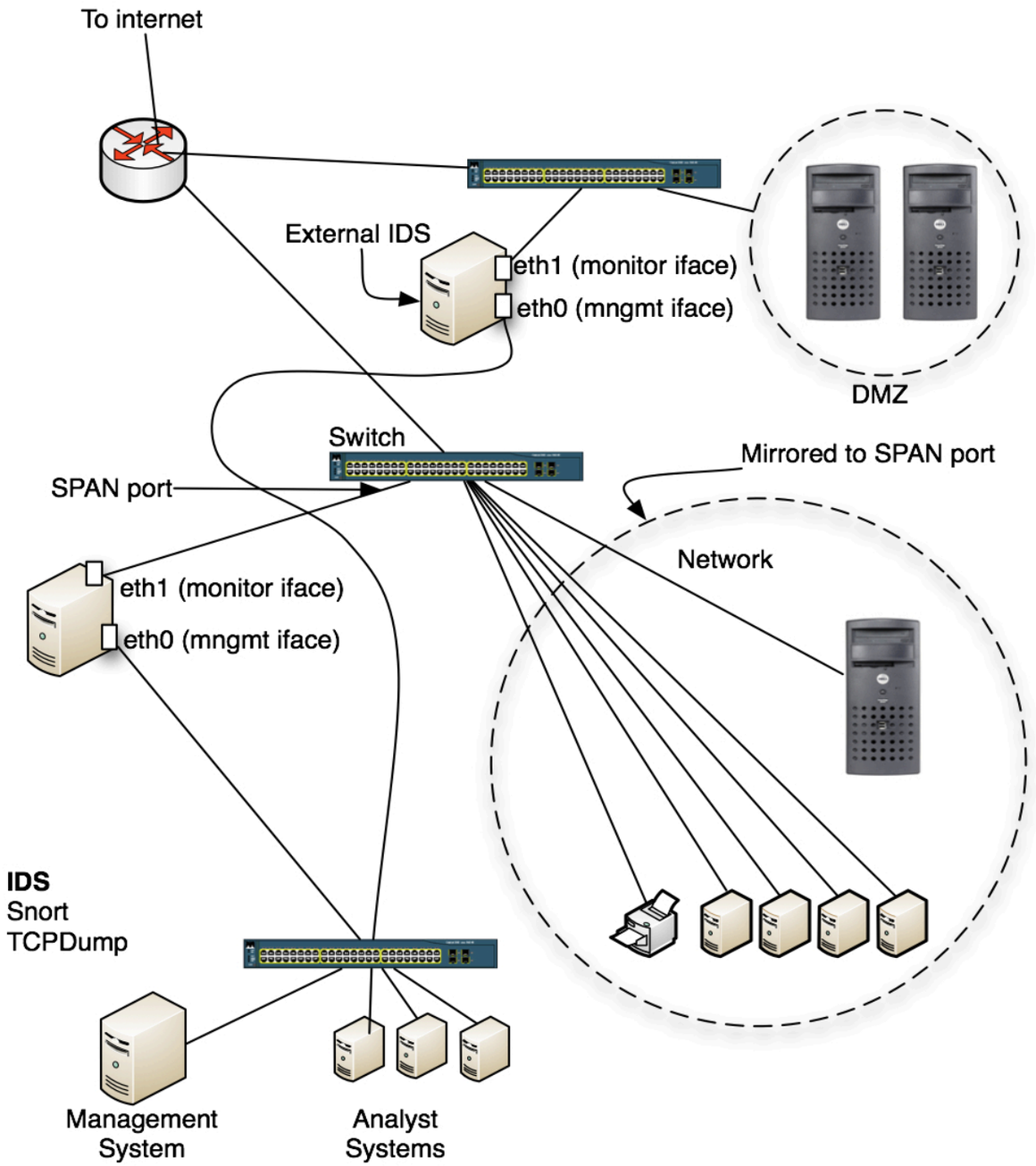


Management
System

Analyst
Systems

Infrastructure

The Classic Model



TICKETING

Description

https://[redacted]

That domain is def bad so please add it. Came in from a customer sideways to me and apparently is from an infected word doc.
[redacted]
But please also look at the bitcoin-dns stuff below also...Looks very suspicious. Also please report direct back to me with findings.

https://[redacted]

[Created via e-mail received from: "[redacted]a)" <[redacted]>]

Activity

All | **Comments** | Work Log | History | Activity | Transitions

Josh Pyorre added a comment - 14/Mar/16 2:30 PM

The domain ([redacted]) is already blocked. Currently looking into the bitcoin-dns activity.

Comment

Votes: [redacted] Vote for this issue

Watchers: 2 Stop watching this issue

Dates

Created: 14/Mar/16 12:55 PM

Updated: 6 days ago

Agile

View on Board

HipChat discussions

Dedicated room: Create a room | Choose a room

Other rooms: Issue mentioned in 0 rooms

TICKETING

Description

https://[redacted]

That domain is def bad so please add it. Came in from a customer sideways to me and apparently is from an infected word doc.

But please also look at the bitcoin-dns stuff below also...Looks very suspicious. Also please report direct back to me with findings.

https://[redacted]

[Created via e-mail received from: "[redacted]a)" <[redacted]>]

Activity

All | **Comments** | Work Log | History | Activity | Transitions

Josh Pyorre added a comment - 14/Mar/16 2:30 PM

The domain ([redacted]) is already blocked. Currently looking into the bitcoin-dns activity.

Comment

Votes: [redacted] Vote for this issue

Watchers: 2 Stop watching this issue

Dates

Created: 14/Mar/16 12:55 PM

Updated: 6 days ago

Agile

View on Board

HipChat discussions

Dedicated room: Create a room | Choose a room

Other rooms: Issue mentioned in 0 rooms

TICKETING

Description

https://[redacted]

That domain is def bad so please add it. Came in from a customer sideways to me and apparently is from an infected word doc.

But please also look at the bitcoin-dns stuff below also...Looks very suspicious. Also please report direct back to me with findings.

https://[redacted]

[Created via e-mail received from: "[redacted]a)" <[redacted]>]

Activity

All | **Comments** | Work Log | History | Activity | Transitions

Josh Pyorre added a comment - 14/Mar/16 2:30 PM

The domain ([redacted]) is already blocked. Currently looking into the bitcoin-dns activity.

Comment

Votes:

Watchers: 2 Stop watching this issue

Dates

Created: 14/Mar/16 12:55 PM

Updated: 6 days ago

Agile

View on Board

HipChat discussions

Dedicated room: Create a room | Choose a room

Other rooms: Issue mentioned in 0 rooms

TICKETING

Description

https://[redacted]

That domain is def bad so please add it. Came in from a customer sideways to me and apparently is from an infected word doc.

But please also look at the bitcoin-dns stuff below also...Looks very suspicious. Also please report direct back to me with findings.

https://[redacted]

[Created via e-mail received from: "[redacted]a)" <[redacted]>]

Activity

All | **Comments** | Work Log | History | Activity | Transitions

Josh Pyorre added a comment - 14/Mar/16 2:30 PM

The domain ([redacted]) is already blocked. Currently looking into the bitcoin-dns activity.

Comment

Votes: [redacted] Vote for this issue

Watchers: 2 Stop watching this issue

Dates

Created: 14/Mar/16 12:55 PM

Updated: 6 days ago

Agile

View on Board

HipChat discussions

Dedicated room: Create a room | Choose a room

Other rooms: Issue mentioned in 0 rooms

TICKETING

Description

https://[redacted]

That domain is def bad so please add it. Came in from a customer sideways to me and apparently is from an infected word doc.

But please also look at the bitcoin-dns stuff below also...Looks very suspicious. Also please report direct back to me with findings.

https://[redacted]

[Created via e-mail received from: "[redacted]a)" <[redacted]>]

Activity

All | **Comments** | Work Log | History | Activity | Transitions

Josh Pyorre added a comment - 14/Mar/16 2:30 PM

The domain ([redacted]) is already blocked. Currently looking into the bitcoin-dns activity.

Comment

Votes: [redacted] Vote for this issue

Watchers: 2 Stop watching this issue

Dates

Created: 14/Mar/16 12:55 PM

Updated: 6 days ago

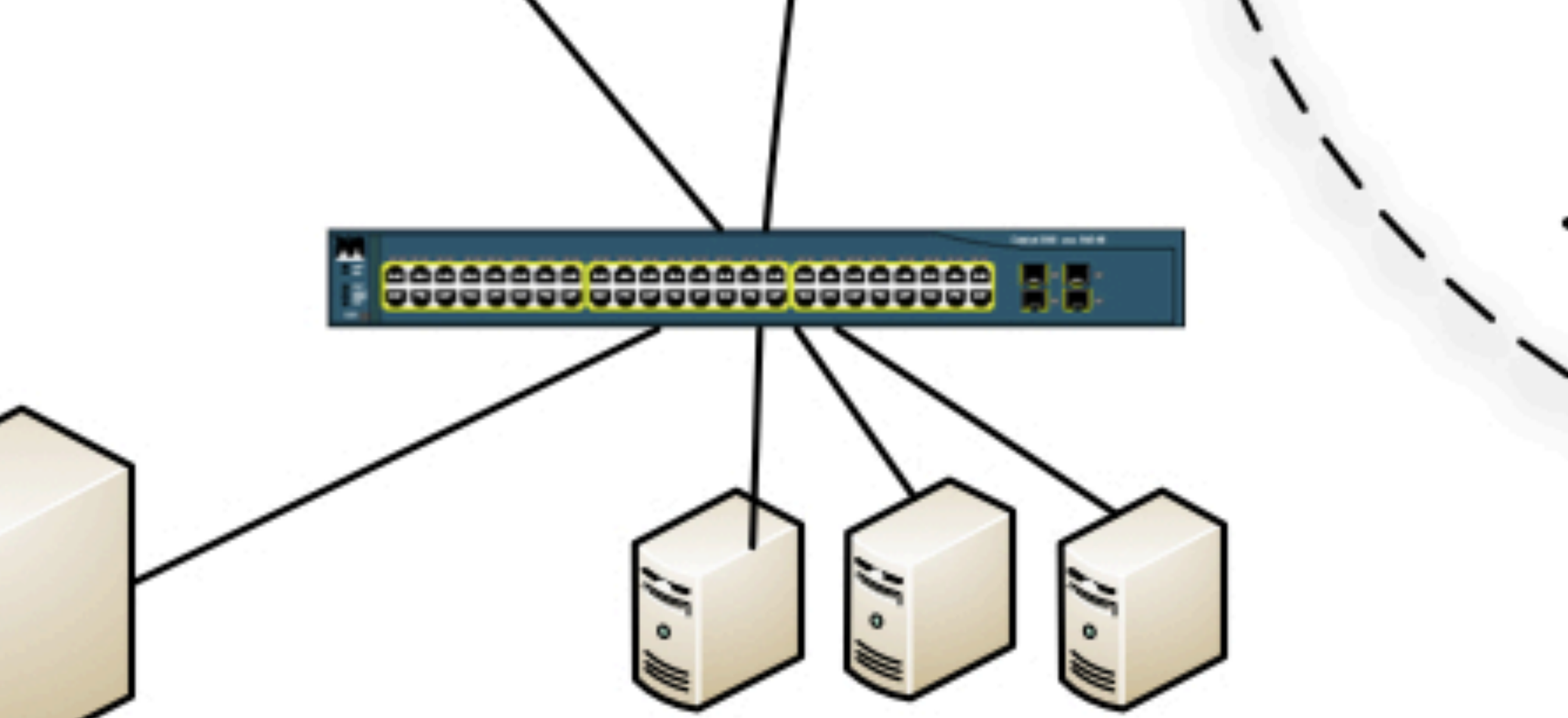
Agile

View on Board

HipChat discussions

Dedicated room: Create a room | Choose a room

Other rooms: Issue mentioned in 0 rooms



ement
tem

Analyst
Systems

Operations

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to

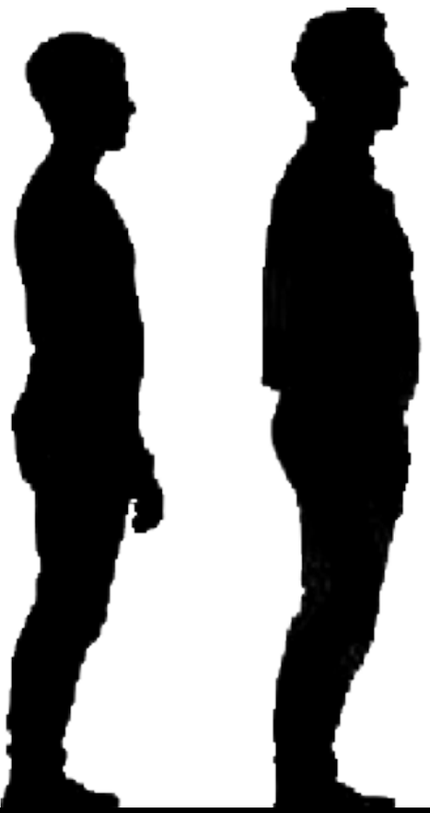
Categorization

CAT 4	Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes /Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes /Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

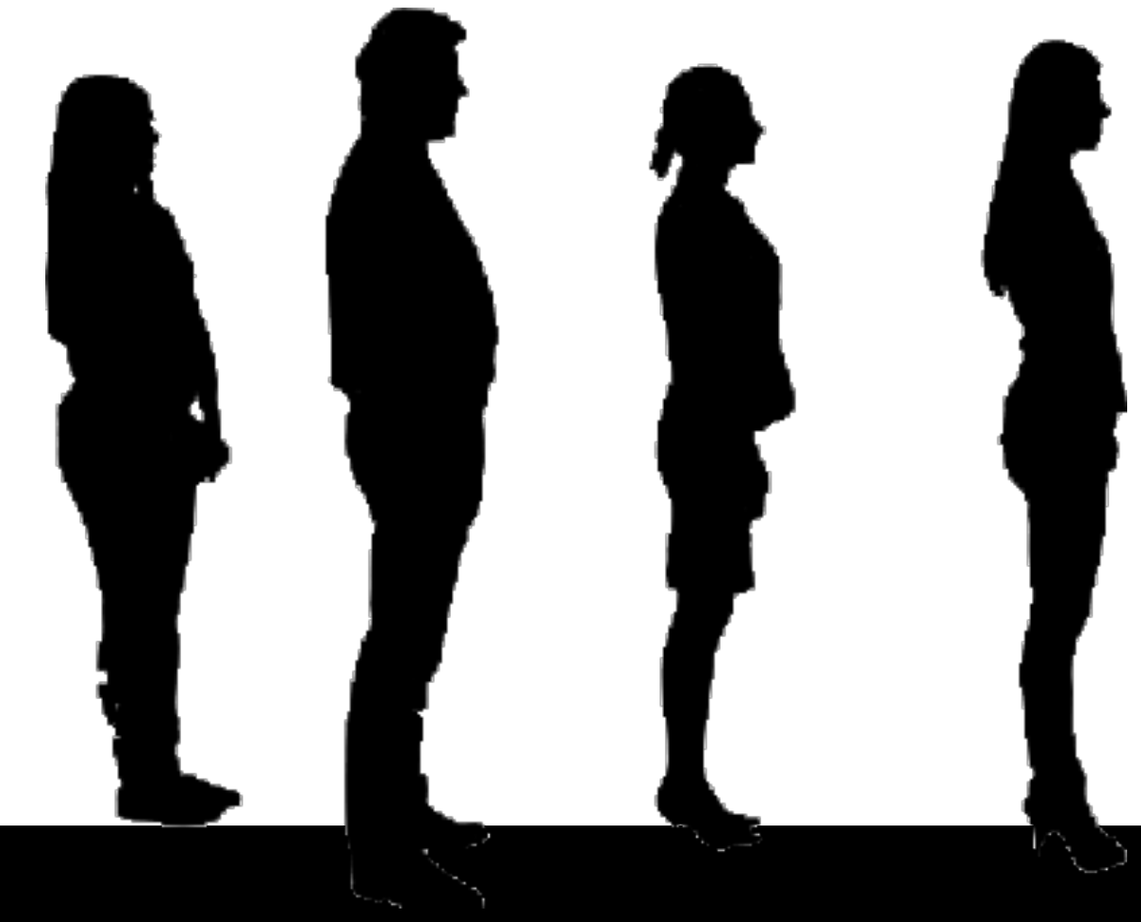
People

SYSTEM ADMINISTRATORS!



ANALYSTS!

THREAT ANALYSTS



Analysts

The Classic Model

Apply a display filter ... <⌘/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
48	0…	23.67.247.186	192.168.1.131	TCP	74	80 → 60551 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1379479904 TSe…
49	0…	192.168.1.131	23.67.247.186	TCP	66	60551 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=845684566 TSecr=1379479904
50	0…	192.168.1.131	23.67.247.186	HTTP	251	GET /bag HTTP/1.1
51	0…	23.67.247.186	192.168.1.131	TCP	66	80 → 60551 [ACK] Seq=1 Ack=186 Win=30048 Len=0 TSval=1379479917 TSecr=845684566
52	0…	23.67.247.186	192.168.1.131	TCP	1514	[TCP segment of a reassembled PDU]
53	0…	23.67.247.186	192.168.1.131	TCP	1514	[TCP segment of a reassembled PDU]
54	0…	192.168.1.131	23.67.247.186	TCP	66	60551 → 80 [ACK] Seq=186 Ack=2897 Win=129600 Len=0 TSval=845684586 TSecr=1379479918
55	0…	23.67.247.186	192.168.1.131	TCP	1514	[TCP segment of a reassembled PDU]
56	0…	192.168.1.131	23.67.247.186	TCP	66	60551 → 80 [ACK] Seq=186 Ack=4345 Win=131072 Len=0 TSval=845684586 TSecr=1379479918
57	0…	23.67.247.186	192.168.1.131	TCP	1514	[TCP segment of a reassembled PDU]
58	0…	23.67.247.186	192.168.1.131	HTTP	1100	HTTP/1.1 200 OK (application/x-apple-plist)
59	0…	23.67.247.186	192.168.1.131	TCP	66	[TCP Dup ACK 51#1] 80 → 60551 [ACK] Seq=6827 Ack=186 Win=30048 Len=0 TSval=1379479922 TSecr…
60	0…	192.168.1.131	23.67.247.186	TCP	66	60551 → 80 [ACK] Seq=186 Ack=6827 Win=130016 Len=0 TSval=845684587 TSecr=1379479918
61	0…	162.125.17.131	192.168.1.131	TCP	74	443 → 60548 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 MSS=1440 SACK_PERM=1 TSval=265073814 TSe…
62	0…	162.125.17.131	192.168.1.131	TCP	74	443 → 60549 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 MSS=1440 SACK_PERM=1 TSval=371176990 TSe…
63	0…	192.168.1.131	192.168.1.1	DNS	75	Standard query 0x7e3f A aia.entrust.net
64	0…	192.168.1.1	192.168.1.131	DNS	223	Standard query response 0x1cdd A www.apple.com CNAME www.apple.com.edgekey.net CNAME www.ap…
65	0…	162.125.17.131	192.168.1.131	TCP	74	443 → 60550 [SYN, ACK] Seq=0 Ack=1 Win=14280 Len=0 MSS=1440 SACK_PERM=1 TSval=287297681 TSe…
66	0…	192.168.1.131	162.125.17.131	TCP	66	60550 → 443 [ACK] Seq=1 Ack=1 Win=131360 Len=0 TSval=845684627 TSecr=287297681
67	0…	192.168.1.131	162.125.17.131	SSL	261	Client Hello
68	0…	192.168.1.1	192.168.1.131	DNS	200	Standard query response 0x858c A init-s01st.push.apple.com CNAME init-s01st.push.apple.com.…
69	0…	192.168.1.131	23.67.247.195	TCP	78	60552 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=845684706 TSecr=0 SACK_PERM=1

```
10:16:05.878830 IP 10.3.21.103.49196 > 46.30.45.206.80: Flags [P.], seq 383:972, ack 221314, win 63336, length 589: HTTP: POST /topic/30219-schoolmistress-
arbitral-swapped-accelerators-pavements-sending-categorical/?s=LpvZQ&e=Ug-&w=a-SW&x=NVVEU&o=pgx6eiO_-F6-Nrs64yssKVgJ6rbRDQ- HTTP/1.1
E..u..@...yK
..g..-..,.P.?.)7.T.P..hZ...POST /topic/30219-schoolmistress-arbitral-swapped-accelerators-pavements-sending-categorical/?s=LpvZQ&e=Ug-&w=a-SW&x=NVVEU&o=pgx
6eiO_-F6-Nrs64yssKVgJ6rbRDQ- HTTP/1.1
Accept: */*
Content-Type: text/html; charset=utf-8
Referer: http://abordonar.section75.eu/topic/30219-schoolmistress-arbitral-swapped-accelerators-pavements-sending-categorical/
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Host: abordonar.section75.eu
Content-Length: 188
DNT: 1
Connection: Keep-Alive
Cache-Control: no-cache


10:16:05.879804 IP 46.30.45.206.80 > 10.3.21.103.49196: Flags [.], ack 972, win 64240, length 0
E..(:y........-.
..g.P.,7.T..?.vP...~...
10:16:05.885240 IP 10.3.21.103.49197 > 46.30.45.206.80: Flags [P.], seq 1:422, ack 1, win 64240, length 421: HTTP: GET /?h=&l=UG_2mxoM-S&r=BWzQB&y=&s=ttFQ&
c=&b=DQBYj2Cn4j7k1GbMLUOs1cJ--v9Pl HTTP/1.1
E.....@...y.
..g..-..-.P...U...uP....\..GET /?h=&l=UG_2mxoM-S&r=BWzQB&y=&s=ttFQ&c=&b=DQBYj2Cn4j7k1GbMLUOs1cJ--v9Pl HTTP/1.1
Accept: */*
Referer: http://abordonar.section75.eu/topic/30219-schoolmistress-arbitral-swapped-accelerators-pavements-sending-categorical/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: abordonar.section75.eu
DNT: 1
Connection: Keep-Alive


10:16:05.885296 IP 46.30.45.206.80 > 10.3.21.103.49197: Flags [.], ack 422, win 64240, length 0
E..(:z........-.
..g.P.-...u....P.......
10:16:05.920015 IP 10.3.21.103.49196 > 46.30.45.206.80: Flags [P.], seq 972:1160, ack 221314, win 63336, length 188: HTTP
E.....@...z.
..g..-..,.P.?.v7.T.P..h`7..d1YheoBRBgS09ze61st0o7gunhOiU3EesJle5EDNAimWHQDNIkY/GhLEh3899hTji52p/hwFWs+hwrUYYYn5tD3rI9CpYJ1p2NfHyENAIhdTLPTFzVQ8IjcdqeFxwkUZ
rmw5KzFB/4X5G+t+mOQlTzEeQJi1l6zC5r047mpiCOqBjifc6wUxODE2Mw==
10:16:05.920077 IP 46.30.45.206.80 > 10.3.21.103.49196: Flags [.], ack 1160, win 64240, length 0
E..(:{........-.
..g.P.,7.T..?.2P...}...
10:16:06.107403 IP 46.30.45.206.80 > 10.3.21.103.49197: Flags [P.], seq 1:161, ack 422, win 64240, length 160: HTTP: HTTP/1.1 404 Not Found
```

CATEGORY 3

Malware on System

CATEGORY 3

Alert the IR team

Malware on System

CATEGORY 3

Threat Analysts

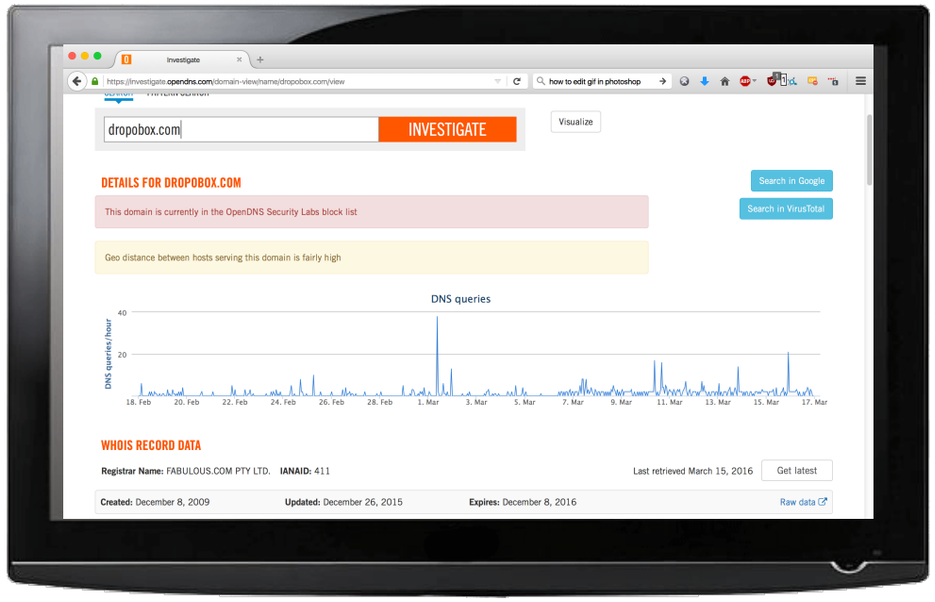
- Investigate phishing
- Analyze Malware
  - Writing new rules/updating existing rules
- Read a lot
- Programmers
- Thought leaders
  - Speak at conferences
  - Write blog posts

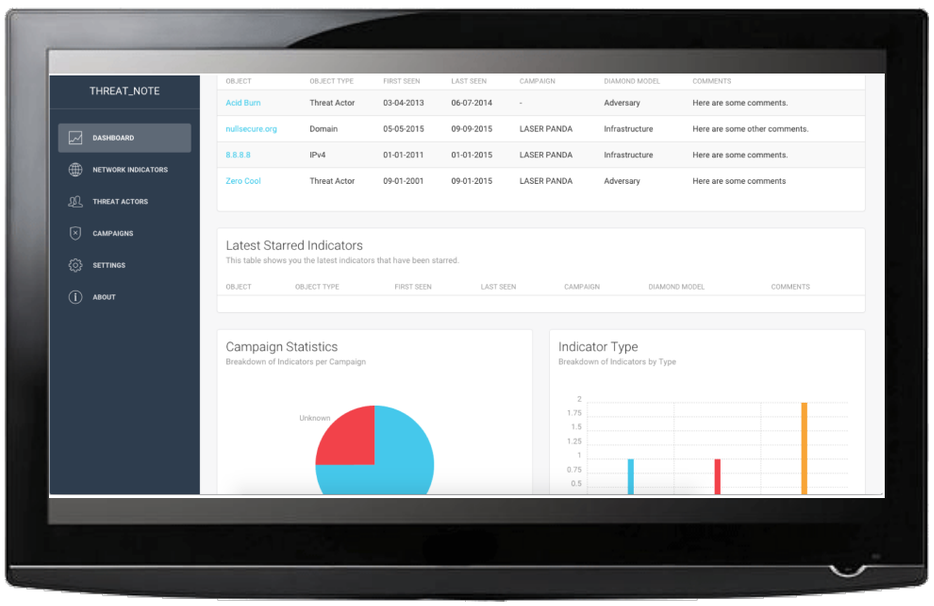
Threat Intel

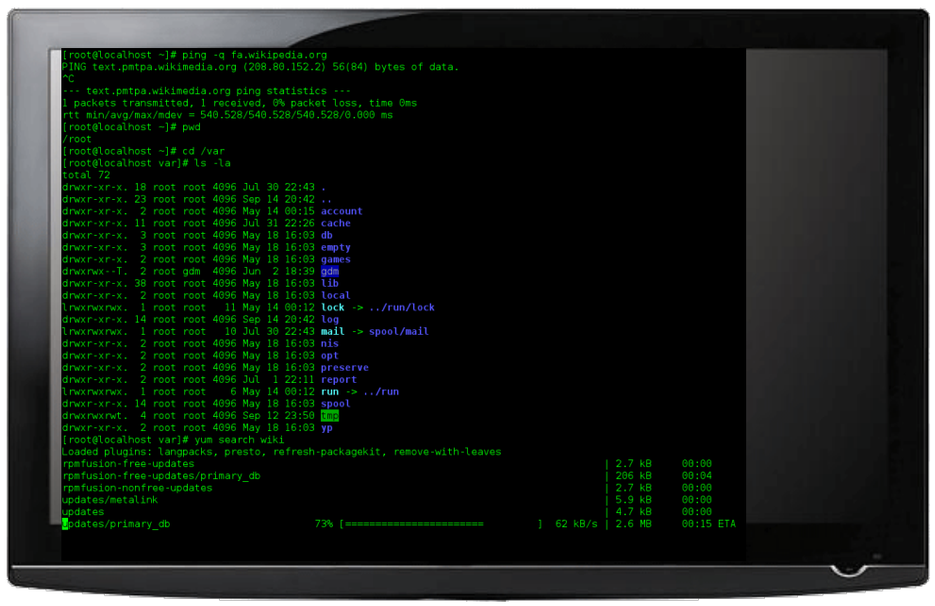
- Passive DNS
- Honeypots
- Hunting
- Third parties


ATTACK ORIGINS
COUNTRY
5216 China
6563 United States
2785 Mil/Gov
2704 Germany
1673 Russia
950 Taiwan
563 Netherlands
439 Turkey
414 Japan
351 France
COUNTRY
25577 United States
1973 Philippines
1244 Russia
848 Taiwan
310 France
69 Netherlands
64 Mil/Gov
16 Poland
10 South Korea
6 Germany
ATTACK TYPES
SERVICE PORT
2806 telnet 23
2025 http-alt 8080
1728 domain 53
1293 ms-wbt-server 3389
1246 unknown 9064
961 http 80
928 ms-sql-s 1433
760 ssh 22
LIVE ATTACKS
ATTACKER
TARGET
TIMESTAMP ORGANIZATION LOCATION IP LOCATION SERVICE PORT
2015-02-18 23:59:43.26 Georgia Tech Information Atlanta, United States 128.61.240.66 New York, United http 80
2015-02-18 23:59:43.58 Paltalk New York, United 64.40.6.28 Seattle, United States unknown 6912
2015-02-18 23:59:43.95 Road Runner Zenica Zenica, Bosnia- 92.240.53.97 Seattle, United States telnet 23
2015-02-18 23:59:44.30 Georgia Tech Information Atlanta, United States 128.61.240.66 Kirksville, United States http 80
2015-02-18 23:59:44.30 Georgia Tech Information Atlanta, United States 128.61.240.66 Kirksville, United States http 80
2015-02-18 23:59:44.58 Cabovisao, SA - Setúbal, Portugal 217.129.124.146 Saint Louis, United telnet 23
2015-02-18 23:59:45.00 Paltalk New York, United 64.40.6.28 Seattle, United States unknown 6912
2015-02-18 23:59:45.25 China TieTong Beijing, China 110.200.135.100 Kirksville, United States telnet 23


ATTACK ORIGINS
COUNTRY
China
United States
Mil/Gov
Germany
Russia
Taiwan
Netherlands
Turkey
Japan
France
COUNTRY
United States
Philippines
Russia
Taiwan
France
Netherlands
Mil/Gov
Poland
South Korea
Germany
ATTACK TYPES
SERVICE
PORT
telnet
http-alt
domain
ms-wbt-server
unknown
http
ms-sql-s
ssh
LIVE ATTACKS
TIMESTAMP
ATTACKER
ORGANIZATION
LOCATION
IP
HOST
LOCATION
TYPE
SERVICE
PORT


Investigate
https://investigate.opendns.com/domain-view/name/dropobox.com/view
how to edit gif in photoshop
dropobox.com
INVESTIGATE
Visualize
DETAILS FOR DROPOBOX.COM
This domain is currently in the OpenDNS Security Labs block list
Geo distance between hosts serving this domain is fairly high
Search in Google
Search in VirusTotal
DNS queries
DNS queries/hour
40
20
18. Feb
20. Feb
22. Feb
24. Feb
26. Feb
28. Feb
1. Mar
3. Mar
5. Mar
7. Mar
9. Mar
11. Mar
13. Mar
15. Mar
17. Mar
WHOIS RECORD DATA
Registrar Name: FABULOUS.COM PTY LTD.
IANAID: 411
Last retrieved March 15, 2016
Get latest
Created: December 8, 2009
Updated: December 26, 2015
Expires: December 8, 2016
Raw data


THREAT_NOTE
DASHBOARD
NETWORK INDICATORS
THREAT ACTORS
CAMPAIGNS
SETTINGS
ABOUT
OBJECT
OBJECT TYPE
FIRST SEEN
LAST SEEN
CAMPAIGN
DIAMOND MODEL
COMMENTS
Acid Burn
Threat Actor
03-04-2013
06-07-2014
-
Adversary
Here are some comments.
nullsecure.org
Domain
05-05-2015
09-09-2015
LASER PANDA
Infrastructure
Here are some other comments.
8.8.8.8
IPv4
01-01-2011
01-01-2015
LASER PANDA
Infrastructure
Here are some comments.
Zero Cool
Threat Actor
09-01-2001
09-01-2015
LASER PANDA
Adversary
Here are some comments
Latest Starred Indicators
This table shows you the latest indicators that have been starred.
Campaign Statistics
Breakdown of Indicators per Campaign
Unknown
Indicator Type
Breakdown of Indicators by Type
2
1.75
1.5
1.25
1
0.75
0.5


[root@localhost ~]# ping -q fa.wikipedia.org
PING text.pmtpa.wikimedia.org (208.80.152.2) 56(84) bytes of data.
^C
--- text.pmtpa.wikimedia.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 540.528/540.528/540.528/0.000 ms
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /var
[root@localhost var]# ls -la
total 72
drwxr-xr-x. 18 root root 4096 Jul 30 22:43 .
drwxr-xr-x. 23 root root 4096 Sep 14 20:42 ..
drwxr-xr-x. 2 root root 4096 May 14 00:15 account
drwxr-xr-x. 11 root root 4096 Jul 31 22:26 cache
drwxr-xr-x. 3 root root 4096 May 18 16:03 db
drwxr-xr-x. 3 root root 4096 May 18 16:03 empty
drwxr-xr-x. 2 root root 4096 May 18 16:03 games
drwxrwx--T. 2 root gdm 4096 Jun 2 18:39 gdm
drwxr-xr-x. 38 root root 4096 May 18 16:03 lib
drwxr-xr-x. 2 root root 4096 May 18 16:03 local
lrwxrwxrwx. 1 root root   11 May 14 00:12 lock -> ../run/lock
drwxr-xr-x. 14 root root 4096 Sep 14 20:42 log
lrwxrwxrwx. 1 root root   10 Jul 30 22:43 mail -> spool/mail
drwxr-xr-x. 2 root root 4096 May 18 16:03 nis
drwxr-xr-x. 2 root root 4096 May 18 16:03 opt
drwxr-xr-x. 2 root root 4096 May 18 16:03 preserve
drwxr-xr-x. 2 root root 4096 Jul 1 22:11 report
lrwxrwxrwx. 1 root root   6 May 14 00:12 run -> ../run
drwxr-xr-x. 14 root root 4096 May 18 16:03 spool
drwxrwxrwt. 4 root root 4096 Sep 12 23:50 tmp
drwxr-xr-x. 2 root root 4096 May 18 16:03 yp
[root@localhost var]# yum search wiki
Loaded plugins: langpacks, presto, refresh-packagekit, remove-with-leaves
rpmfusion-free-updates | 2.7 kB 00:00
rpmfusion-free-updates/primary_db | 206 kB 00:04
rpmfusion-nonfree-updates | 2.7 kB 00:00
updates/metalink | 5.9 kB 00:00
updates | 4.7 kB 00:00
updates/primary_db 73% [==========] 62 kB/s | 2.6 MB 00:15 ETA

Tor Browser File Edit View History Bookmarks Tools Window Help

51% Mar 18 14:30

Tor Browser | Search or enter address

Search

Tor Browser
5.5.4

Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Disconnect.me.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

SOC as a Service

SOC as a Service

- Install their boxes
- They watch your network
- Alert when there's a problem
- They manage all that SOC stuff

SOC as a Service

What's their response time?
How do they innovate?
You aren't their only customer

The Security Landscape

We are working everywhere

Everyone brings their own devices

It can never happen to us

Malware is the best way into a network.

APT is over-hyped - just stop the big thing

The Modern SOC

Some of the gaps

- **Cloud Services**
- Behavioral Analysis
- BYOD
- Too much manual stuff

The Modern SOC

Some of the gaps

- Cloud Services
- **Behavioral Analysis**
- BYOD
- Too much manual stuff

The Modern SOC

Some of the gaps

- Cloud Services
- Behavioral Analysis
- **BYOD**
- Too much manual stuff

The Modern SOC

Some of the gaps

- Cloud Services
- Behavioral Analysis
- BYOD
- **Too much manual stuff**

Risk Assessment

What are you protecting?

- Depends on industry
- Depends on what you're running
  - Inventory lists
- Are networks segregated?
  - guest, VPN, Internal

DETECTION

DNS

- DGA's
  Complex domains, generated by malware
- Typosquatting
  wellsfarg0[.]com, Vistaprint
- **Known Bad**
  Third party, Hunting
- **Covert Tunneling**

2qkofvieqirmejqseorcg26ge23qmm5dimlg.gu2celbcm
e8vrnkv30k6ttei0ce2jchirgiob3mq5dondb.gvq0imbcfq
vmurcfqrgcir4ejrtamrvgvrtqmrqhbqtait7.az.r.ipass.com
u2qkofvieqirmejqseorcgi6dgndbgjs0em5f.mm2ce9iy.a
d0255cmf0fg7bcfqrgcir4ejqta25ggvrds3rt.gjsgmirmejrs
e8vrnkv30k6ttei0ce2jchirde23ugrtginlb.g7r0gmbcfqrg
avmurcfqrgcir4ei5dqob0me5to3rqmi5dait7.ay.a.r.ipass
u2qkofvieqsjcfqrgcir4ejsdintegu2gm3tf.gjrgmit7az.a.r.i
e8vrnkv30k6ttei0ce2jchirgcmbuha20gnbv.m260embc
avmurcfqrgcir4ei3tam31me5ggm5emi5tairm.ejrseorcg
abdthefwpuuqxwgddiiqagcrsiymnogqvxxxzw.2-01-2a

~/Desktop/dns/twodomains.txt

twodomains.txt

```
1  3kfbt77aa1zs3jmniqag3oaccpyhwtfqyj4oozm13ep94x3auyqcfg37g6h1449.s.lbl8.mailshell.net
2  orugs4zanfzsayjaorsxg5a.test.com
```

Line 2, Column 33 Tab Size: 4 Plain Text

dns — -bash — 112×12

```
JPYORRE-M-X254:dns jpyorre$
```

dns — -bash — 114×12

JPYORRE-M-X254:dns jpyorre$

~/Desktop/dns/twodomains.txt

twodomains.txt

```
1  3kfbt77aa1zs3jmniqag3oaccpyhwtfqyj4oozm13ep94x3auyqcfg37g6h1449.s.lbl8.mailshell.net
2  orugs4zanfzsayjaorsxg5a.test.com
```

~/Desktop/dns/twodomains.txt

twodomains.txt

```
1  3kfbt77aa1zs3jmniqag3oaccpyhwtfqyj4oozm13ep94x3auyqcfg37g6h1449.s.lbl8.mailshell.net
2  orugs4zanfzsayjaorsxg5a.test.com
```

Line 2, Column 33 Tab Size: 4 Plain Text

dns — -bash — 112×12

```
JPYORRE-M-X254:dns jpyorre$
```

dns — -bash — 114×12

```
JPYORRE-M-X254:dns jpyorre$
```

twodomains.txt

```
1  3kfbt77aa1zs3jmniqag3oaccpyhwtfqyj4oozm13ep94x3auyqcfg37g6h1449.s.lbl8.mailshell.net
2  orugs4zanfzsayjaorsxg5a.test.com
```

Line 2, Column 33 Tab Size: 4 Plain Text

```
JPYORRE-M-X254:dns jpyorre$ ./server.py
Unable to de-obfuscate: 3kfbt77aa1zs3jmniqag3oacc94x3auyqcfg37g6h14
orugs4zanfzsayjaorsxg5a.test.com: this is a test
```

dns — -bash — 114×12

```
JPYORRE-M-X254:dns jpyorre$ ./client.py twodomains.txt
3kfbt77aa1zs3jmniqag3oaccpyhwtfqyj4oozm13ep94x3auyqcfg37g6h1449.s.lbl8.mailshell.net
orugs4zanfzsayjaorsxg5a.test.com
JPYORRE-M-X254:dns jpyorre$
```

Email

- **Attachments**
- Headers

PayPal Security Team June 2, 2016 at 11:48 AM

Account Notification

Dear Valued Client,

Your account has been limited until we hear from you.

We regularly monitor the activity of our clients account.
Recently, we detected multiple violations from your PayPal account.

Thus, our security team had to limit your account and
awaits further information from you in order to recover
the access in your account.

We have provided an attachment file for you to simply open and confirm
your identity with us. Please do this as soon as you can.

We apologize for the inconvenience.

Sincerely,
PayPal Security Team

Attached_Form141.htm

stuff

untitled folder

Devices
evol13
Remote Disc

Favorites
josh
Desktop
DATA
OpenDNS
DNS_Scripts
PERSONAL
SOC
Applications
Documents
Dropbox

Name
PayPal.eml
unpack.py

Date Modified
Today, 7:10 PM
Jun 16, 2012, 1:29 PM

2 items, 353.74 GB available

2016-0...PM.png

Email

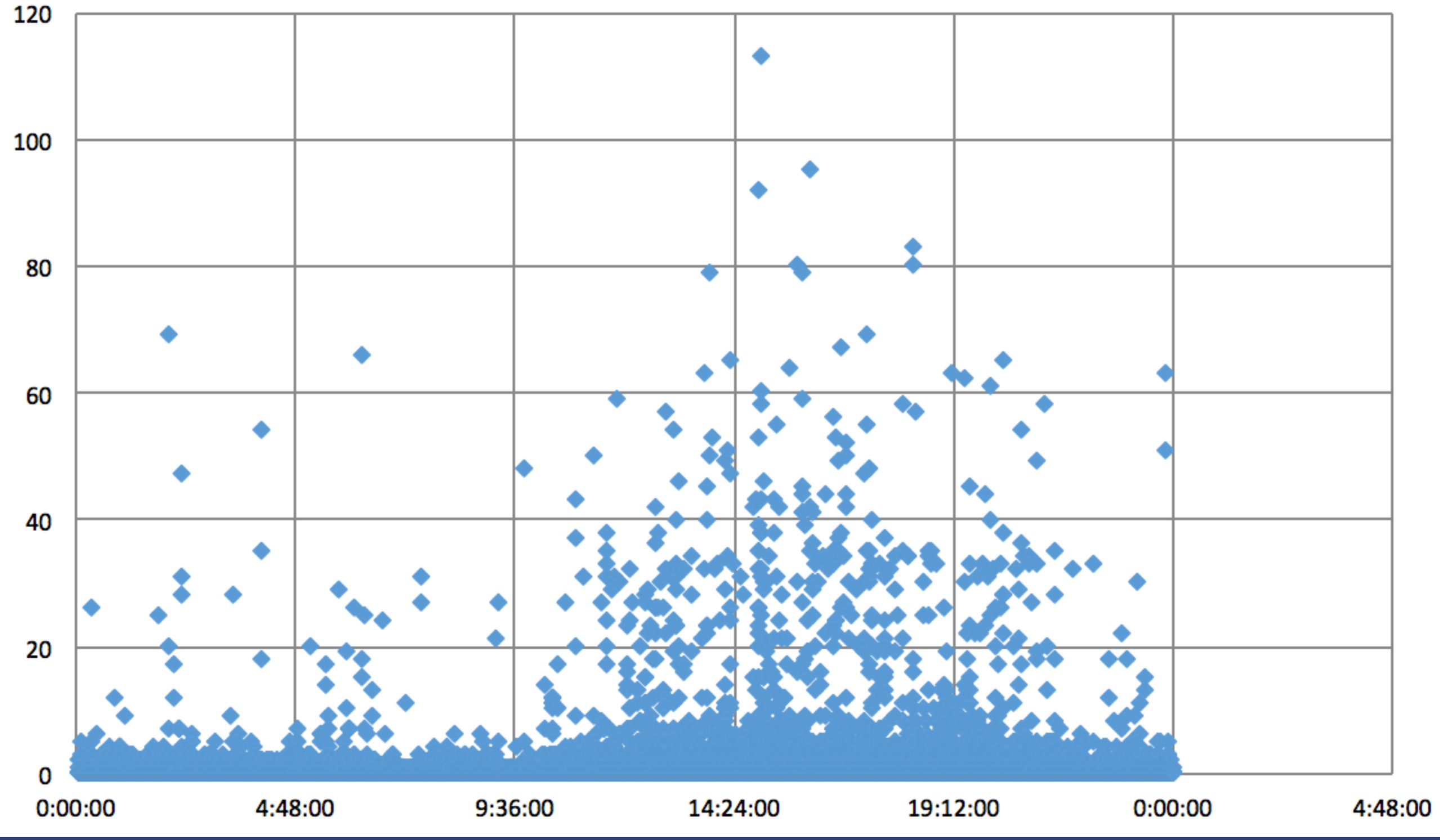
- Attachments
  - Unsigned, exe's
- **Headers**

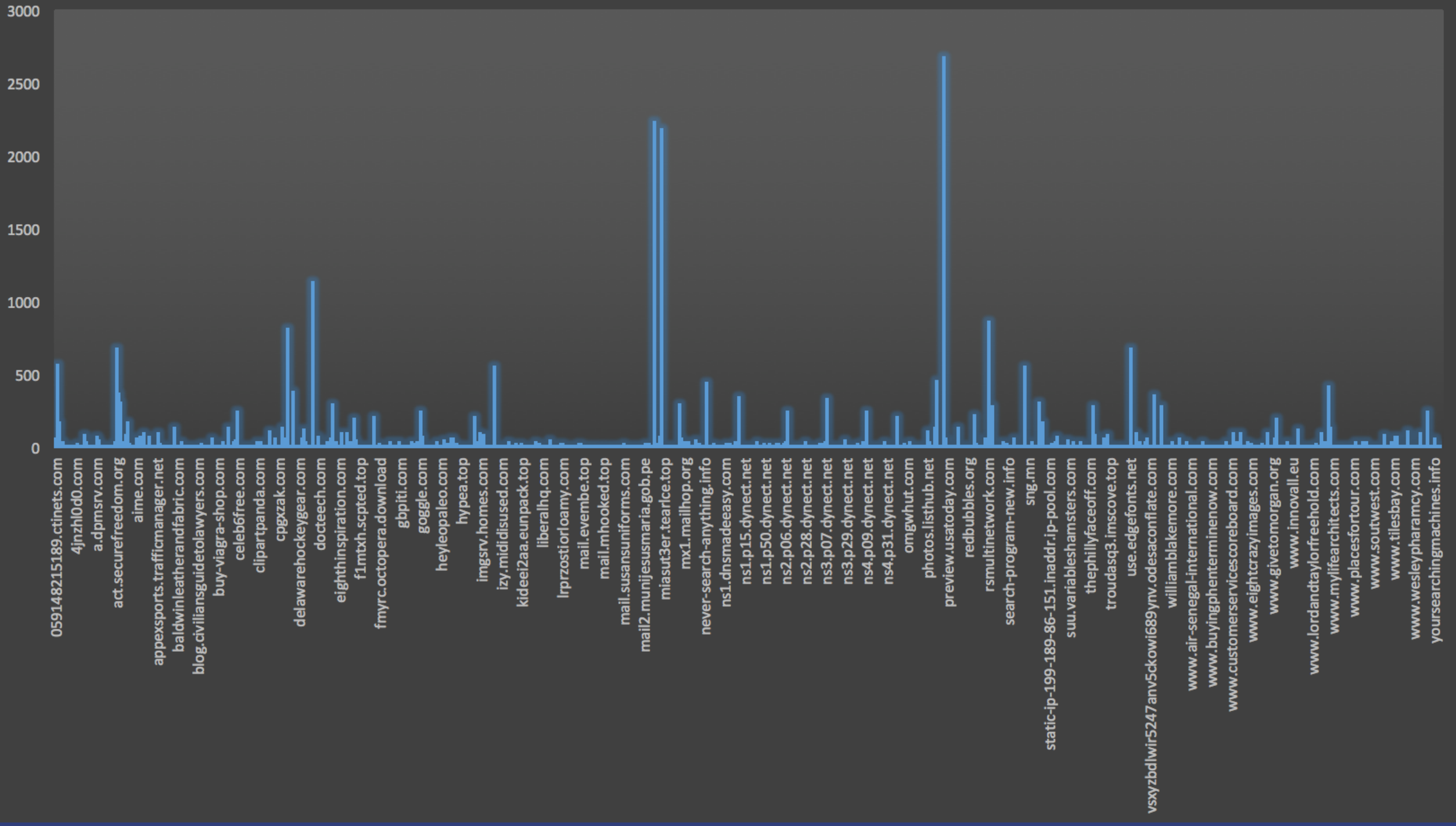
People

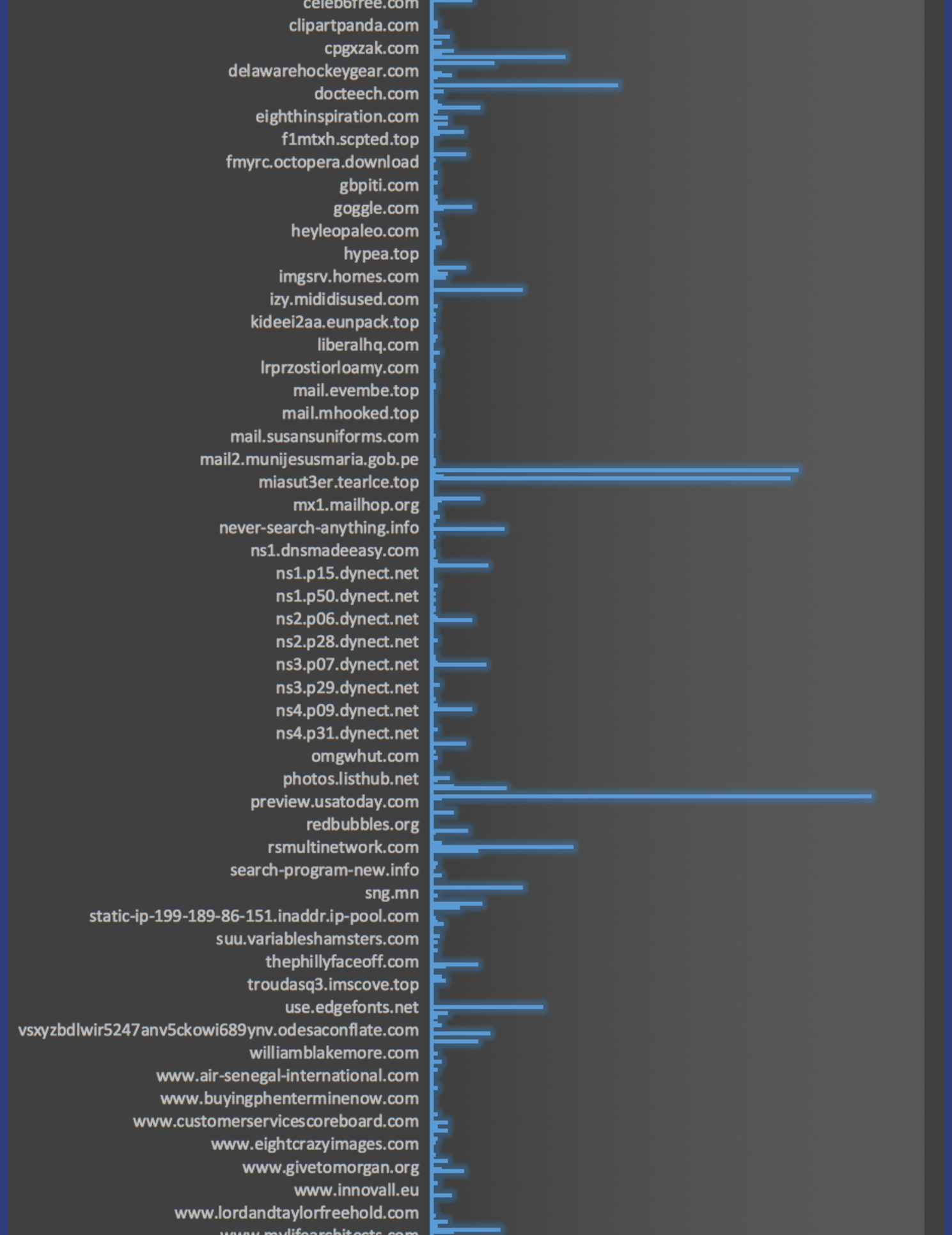
- Training
- Anomalies

People

- Training
  TRAINING!!!!!
- **Anomalies**
  Visits to somewhere different


120
100
80
60
40
20
0
0:00:00
4:48:00
9:36:00
14:24:00
19:12:00
0:00:00
4:48:00


3000
2500
2000
1500
1000
500
0
059148215189.ctinets.com
4jnzhl0d0.com
a.dpmsrv.com
act.securefreedom.org
aime.com
appexsports.trafficmanager.net
baldwinleatherandfabric.com
blog.civiliansguidetolawyers.com
buy-viagra-shop.com
celeb6free.com
clipartpanda.com
cpgxzak.com
delawarehockeygear.com
docteech.com
eighthinspiration.com
f1mtxh.scpted.top
fmyrc.octopera.download
gbpiti.com
goggle.com
heyleopaleo.com
hypea.top
imgsrv.homes.com
izy.mididisused.com
kideei2aa.eunpack.top
liberalhq.com
lrprzostiorloamy.com
mail.evembe.top
mail.mhooked.top
mail.susansuniforms.com
mail2.munijesusmaria.gob.pe
miasut3er.tearlce.top
mx1.mailhop.org
never-search-anything.info
ns1.dnsmadeeasy.com
ns1.p15.dynect.net
ns1.p50.dynect.net
ns2.p06.dynect.net
ns2.p28.dynect.net
ns3.p07.dynect.net
ns3.p29.dynect.net
ns4.p09.dynect.net
ns4.p31.dynect.net
omgwhut.com
photos.listhub.net
preview.usatoday.com
redbubbles.org
rsmultinetwork.com
search-program-new.info
sng.mn
static-ip-199-189-86-151.inaddr.ip-pool.com
suu.variableshamsters.com
thephillyfaceoff.com
troudasq3.imscove.top
use.edgefonts.net
vsxyzbdlwir5247anv5ckowi689ynv.odesaconflate.com
williamblakemore.com
www.air-senegal-international.com
www.buyingphenterminenow.com
www.customerservicescoreboard.com
www.eightcrazyimages.com
www.givetomorgan.org
www.innovall.eu
www.lordandtaylorfreehold.com
www.mylifearchitects.com
www.placesfortour.com
www.soutwest.com
www.tilesbay.com
www.wesleypharamcy.com
yoursearchingmachines.info


celeb6free.com
clipartpanda.com
cpgxzak.com
delawarehockeygear.com
docteech.com
eighthinspiration.com
f1mtxh.scpted.top
fmyrc.octopera.download
gbpiti.com
goggle.com
heyleopaleo.com
hypea.top
imgsrv.homes.com
izy.mididisused.com
kideei2aa.eunpack.top
liberalhq.com
lrprzostiorloamy.com
mail.evembe.top
mail.mhooked.top
mail.susansuniforms.com
mail2.munijesusmaria.gob.pe
miasut3er.tearlce.top
mx1.mailhop.org
never-search-anything.info
ns1.dnsmadeeasy.com
ns1.p15.dynect.net
ns1.p50.dynect.net
ns2.p06.dynect.net
ns2.p28.dynect.net
ns3.p07.dynect.net
ns3.p29.dynect.net
ns4.p09.dynect.net
ns4.p31.dynect.net
omgwhut.com
photos.listhub.net
preview.usatoday.com
redbubbles.org
rsmultinetwork.com
search-program-new.info
sng.mn
static-ip-199-189-86-151.inaddr.ip-pool.com
suu.variableshamsters.com
thephillyfaceoff.com
troudasq3.imscove.top
use.edgefonts.net
vsxyzbdlwir5247anv5ckowi689ynv.odesaconflate.com
williamblakemore.com
www.air-senegal-international.com
www.buyingphenterminenow.com
www.customerservicescoreboard.com
www.eightcrazyimages.com
www.givetomorgan.org
www.innovall.eu
www.lordandtaylorfreehold.com

izy.midi disused.com
kideei2aa.eunpack.top
liberalhq.com
lrprzostiorloamy.com
mail.evembe.top
mail.mhooked.top
mail.susansuniforms.com
mail2.munijesusmaria.gob.pe
miasut3er.tearlce.top
mx1.mailhop.org
never-search-anything.info
ns1.dnsmadeeasy.com
ns1.p15.dynect.net
ns1.p50.dynect.net
ns2.p06.dynect.net
ns2.p28.dynect.net
ns3.p07.dynect.net
ns3.p29.dynect.net
ns4.p09.dynect.net
ns4.p31.dynect.net
omgwhut.com
photos.listhub.net
preview.usatoday.com
redbubbles.org
rsmultinetwork.com
search-program-new.info

delawarehockeygear.com
docteech.com
eighthinspiration.com
f1mtxh.scpted.top
fmyrc.octopera.download
gbpiti.com
goggle.com
heyleopaleo.com
hypea.top
imgsrv.homes.com
izy.mididisused.com
kideei2aa.eunpack.top
liberalhq.com
lrprzostiorloamy.com
mail.evembe.top
mail.mhooked.top
mail.susansuniforms.com
mail2.munijesusmaria.gob.pe
miasut3er.tearlce.top
mx1.mailhop.org
never-search-anything.info
ns1.dnsmadeeasy.com
ns1.p15.dynect.net
ns1.p50.dynect.net
ns2.p06.dynect.net
ns2.p28.dynect.net

Management System

Snorby (web based)

SGUIL (Client)

ELK (Log Aggregation)

Snorby SPONSORED BY threat stack https://threatstack.com

Dashboard

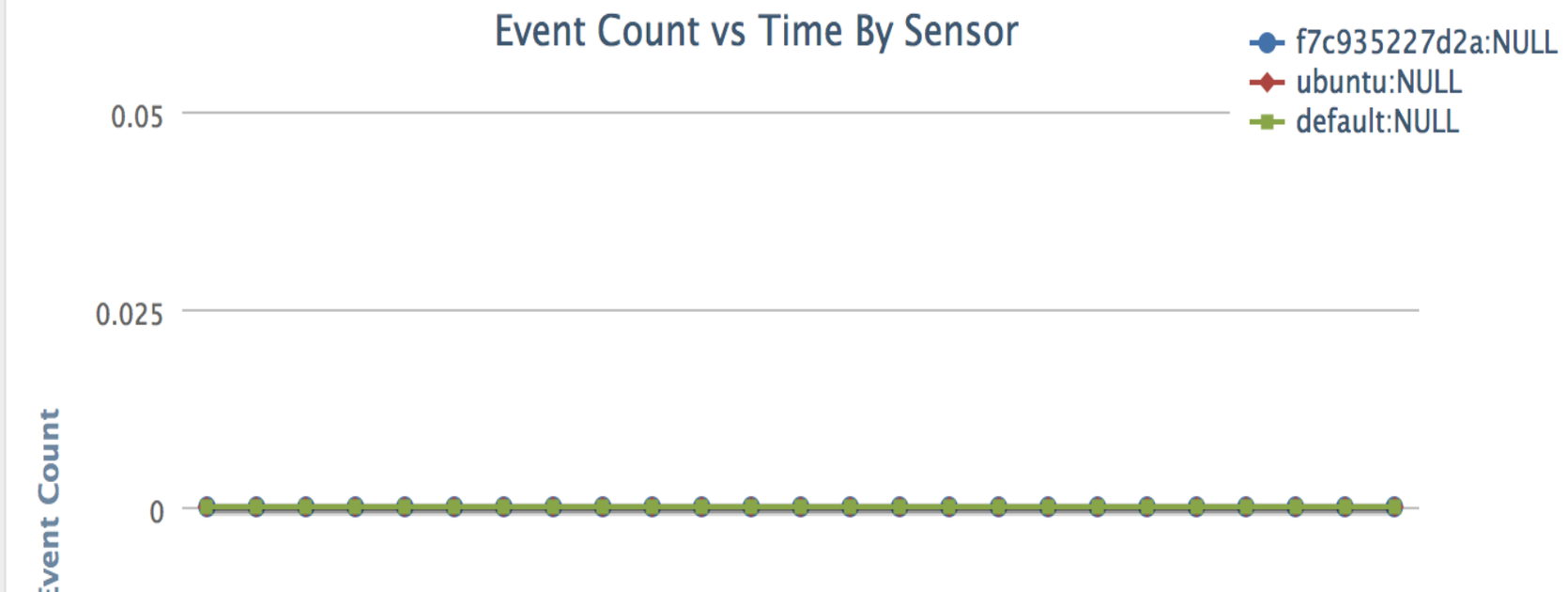
More Options

LAST 24 TODAY YESTERDAY LAST WEEK THIS MONTH THIS QUARTER THIS YEAR

Updated: 03/28/16 03:23 PM PDT

0	0	0
HIGH SEVERITY	MEDIUM SEVERITY	LOW SEVERITY
0 / 0	0 / 0	0 / 0

Sensors | Severities | Protocols | Signatures | Sources | Destinations



TOP 5 SENSOR

f7c935227d2a:NULL	0
ubuntu:NULL	0
default:NULL	0

TOP 5 ACTIVE USERS

Josh	0

LAST 5 UNIQUE EVENTS

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

SGUIL-0.6.0p1 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: sguil UserID: 2 2006-01-06 15:43:21 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gruden	1.1	2006-01-06 15:40:32	192.168.2.5	61519	192.168.2.121	22	6	EXPLOIT gobbles SSH exploit attempt
RT	1	gruden	1.3	2006-01-06 15:41:39	192.168.2.5	53190	192.168.2.22	3389	6	MISC MS Terminal Server no encryption session initiation attempt

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	gruden	1.2	2006-01-06 15:41:39	192.168.2.5	53190	192.168.2.22	3389	6	MISC MS Terminal server request

192.168.2.5_61519_192.168.2.121_22-6.raw - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
6	8.323638	192.168.2.5	192.168.2.121	SSH	Encrypted request packet len=38
7	8.325850	192.168.2.121	192.168.2.5	SSH	Encrypted response packet len=19
8	8.326763	192.168.2.121	192.168.2.5	TCP	22 > 61519 [FIN, ACK] Seq=59 Ack=39 Win=66608 L

Frame 6 (104 bytes on wire, 104 bytes captured)
Ethernet II, Src: 00:03:47:0f:1f:3c (00:03:47:0f:1f:3c), Dst: 00:0c:29:70:af:ae (00:0c:29:70:af:ae)
Internet Protocol, Src: 192.168.2.5 (192.168.2.5), Dst: 192.168.2.121 (192.168.2.121)
Transmission Control Protocol, Src Port: 61519 (61519), Dst Port: 22 (22), Seq: 1, Ack: 40, Len: 38
SSH Protocol

```
0030  82 18 22 bb 00 00 01 01  08 0a 00 27 44 d3 00 1a   ..".....  ...'D...
0040  d8 dd 47 4f 42 42 4c 45  53 20 6c 6f 76 65 73 20   ..GOBBLE S loves
0050  53 67 75 69 6c 20 61 6e  64 20 73 6f 20 73 68 6f   Sguil an d so sho
0060  75 6c 64 20 79 6f 75 0a                           uld you.
```

File: "/tmp/192.168.2.5_61519_192.168.2.121_22-6.raw" 1046 Bytes 00:... P: 11 D: 11 M: 0

es SSH exploit attempt";
reference:cve,2002-0390;

ID	Flags	Offset	TTL	ChkSum
48748	2	0	64	63074

#	Offset	Res	Window	Urp	ChkSum
318	8	0	33304	0	8891

3 67
5 6C

GOBBLES loves Sg
uil and so shoul
d you.

Search Packet Payload Hex Text NoCase

one xterm xterm xterm SGUIL-0.6.0p 192.168.2. 10:43

Connecting...

192.168.115.135:5601

Search

Building Systems for Adaptability

- Compartmentalized systems for quick deployment
  - One configuration file
  - Central ruleset
  - Purpose driven, one use
- IDS on every device
- Deploy as many as needed, really fast

Example

- Run a Docker IDS, connected to span port
- Run some malware in another system
- IDS picks up traffic and sends to idsify.com

```
josh@ubuntu:~$ docker run -it -p 80:80 --net=host jpyorre/snortbase
```

Cloud Services

We work fast, setting up devices and services quickly.

Cloud IDS

- Install IDS and configure
- Install Apache (or NginX)

Cloud IDS

- Modify Site Properties

Cloud IDS

```
<VirtualHost protectthisserver.tld:80>
    ProxyPreserveHost On
    ProxyPass / http://buildasoc.com/
    ProxyPassReverse / http://buildasoc.com/
    ServerName localhost
</VirtualHost>
```

Cloud IDS

Enable proxy:

a2enmod proxy

a2enmod proxy_http

Restart Apache2:

service apache2 restart


Where is buildasoc.com?

Where is buildasoc.com?

Go ask:

ns155.hostgator.com

ns156.hostgator.com

It’s here!
192.1232.251.97

HostGator
Web Hosting

ns1.hostgator.com
ns2.hostgator.com

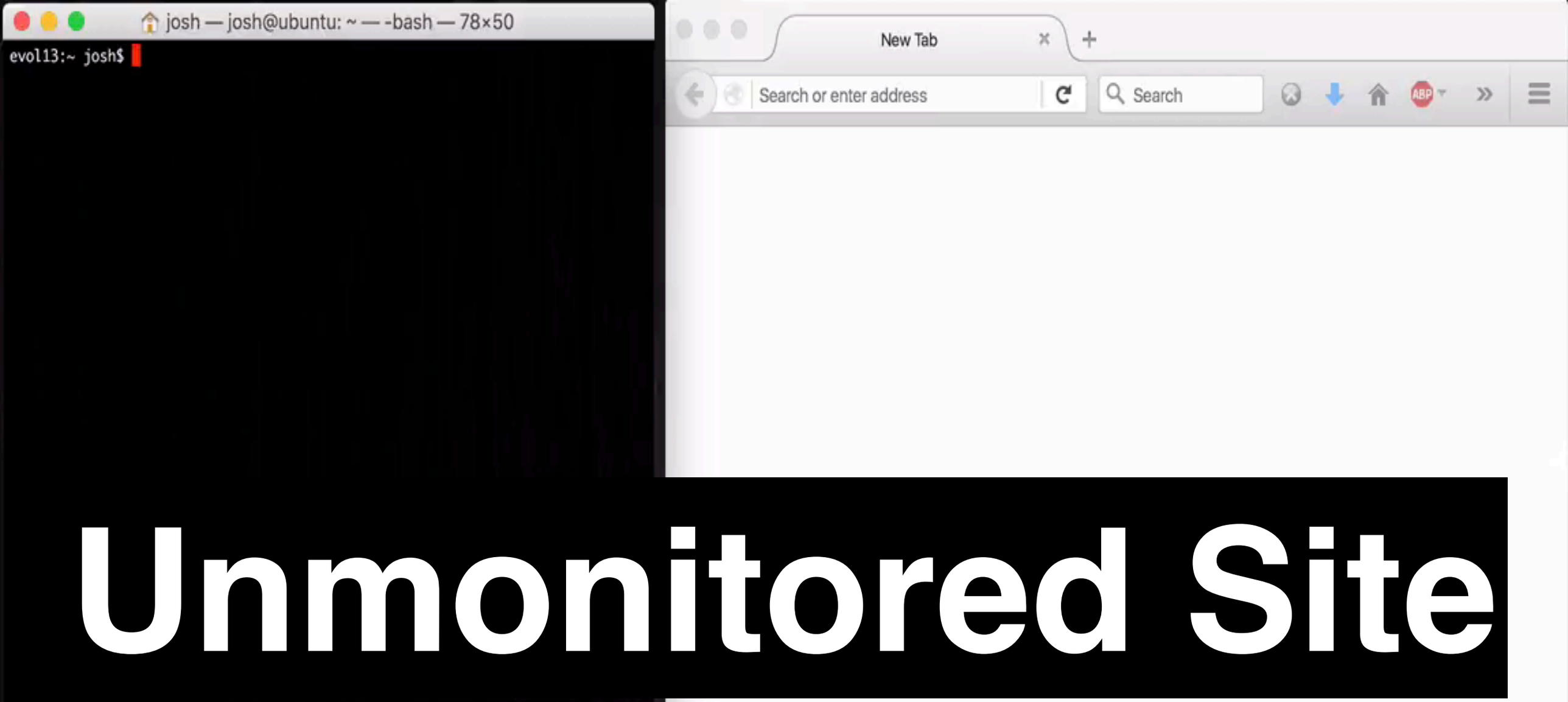
Thanks!

It’s here!
192.1232.251.97

HostGator
Web Hosting

ns1.hostgator.com
ns2.hostgator.com


buildasoc – SOC Building!
buildasoc.com
Search
buildasoc
SHOW ME


josh — josh@ubuntu: ~ — -bash — 78×50
evol13:~ josh$
New Tab
Search or enter address
Search
Unmonitored Site

Not Acceptable! | Domain name registrar and V...

Gandi S... (FR) | https://www.gandi.ne | Search

Josh Pyorre (JP10977-GAN

Service status

gandi.net my account

Services | Account management | Billing | Orders in progress | Messages (19)

Domains | SSL | Websites | Simple Hosting | Servers

Domain Names > buildasoc.com

General Information

Whois | View the website | Authorization key | Delete

Creation date: 01/16/2014

Expiration date: 01/16/2017 (in 294 days) ➔ Renew this domain

Renewal: Inactive (Manage)

Transfer Lock Inactive (Modify)

Last update: 03/28/2016 (history)

Operation in progress: 0

Contract: see

Procedure: see the information page

Tags: Add a tag

Add note

Mailboxes:
Email forwa
Gandi Mail

Web forwa

GandiBlog:

Websites: I

SSL Certific

Hosting: M

Contacts

Owner

Administrative

JP10977-GANDI

JP10977-GANDI


Where is buildasoc.com?

Where is buildasoc.com?

Go ask:
ns1.linode.com
ns2.linode.com

Thanks!

It’s here!
198.74.50.189

linode

ns1.linode.com
ns2.linode.com

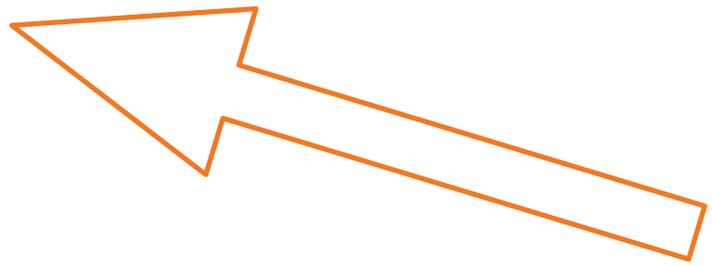
I’ve found buildasoc.com

198.74.50.189

```
[root@localhost ~]# ping -q fa.wikipedia.org
PING text.pmtpa.wikimedia.org (208.80.152.2) 56(84) bytes of data.
^C
--- text.pmtpa.wikimedia.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 540.528/540.528/540.528/0.000 ms
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /var
[root@localhost var]# ls -la
total 72
drwxr-xr-x. 18 root root 4096 Jul 30 22:43 .
drwxr-xr-x. 23 root root 4096 Sep 14 20:42 ..
drwxr-xr-x.  2 root root 4096 May 14 00:15 account
drwxr-xr-x. 11 root root 4096 Jul 31 22:26 cache
drwxr-xr-x.  3 root root 4096 May 18 16:03 db
drwxr-xr-x.  3 root root 4096 May 18 16:03 empty
drwxr-xr-x.  2 root root 4096 May 18 16:03 games
drwxrwx--T.  2 root gdm  4096 Jun  2 18:39 gdm
drwxr-xr-x. 38 root root 4096 May 18 16:03 lib
drwxr-xr-x.  2 root root 4096 May 18 16:03 local
lrwxrwxrwx.  1 root root   11 May 14 00:12 lock -> ../run/lock
drwxr-xr-x. 14 root root 4096 Sep 14 20:42 log
lrwxrwxrwx.  1 root root   10 Jul 30 22:43 mail -> spool/mail
drwxr-xr-x.  2 root root 4096 May 18 16:03 nis
drwxr-xr-x.  2 root root 4096 May 18 16:03 opt
drwxr-xr-x.  2 root root 4096 May 18 16:03 preserve
drwxr-xr-x.  2 root root 4096 Jul  1 22:11 report
lrwxrwxrwx.  1 root root    6 May 14 00:12 run -> ../run
drwxr-xr-x. 14 root root 4096 May 18 16:03 spool
drwxrwxrwt.  4 root root 4096 Sep 12 23:50 tmp
drwxr-xr-x.  2 root root 4096 May 18 16:03 yp
[root@localhost var]# yum search wikl
Loaded plugins: langpacks, presto, refresh-packagekit, remove-with-leaves
rpmfusion-free-updates                                                  | 2.7 kB     00:00
rpmfusion-free-updates/primary_db                                       | 206 kB     00:04
rpmfusion-nonfree-updates                                               | 2.7 kB     00:00
updates/metalink                                                        | 5.9 kB     00:00
updates                                                                 | 4.7 kB     00:00
updates/primary_db                      73% [==================       ]  62 kB/s | 2.6 MB     00:15 ETA
```

198.74.50.189

```
[root@localhost ~]# ping -q fa.wikipedia.org
PING text.pmtpa.wikimedia.org (208.80.152.2) 56(84) bytes of data.
^C
--- text.pmtpa.wikimedia.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 540.528/540.528/540.528/0.000 ms
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /var
[root@localhost var]# ls -la
total 72
drwxr-xr-x. 18 root root 4096 Jul 30 22:43 .
dr-xr-xr-x. 23 root root 4096 Sep 14 20:42 ..
drwxr-xr-x.  2 root root 4096 May 14 00:15 account
drwxr-xr-x. 11 root root 4096 Jul 31 22:26 cache
drwxr-xr-x.  3 root root 4096 May 18 16:03 db
drwxr-xr-x.  3 root root 4096 May 18 16:03 empty
drwxr-xr-x.  2 root root 4096 May 18 16:03 games
drwxrwx--T.  2 root gdm  4096 Jun  2 18:39 gdm
drwxr-xr-x. 38 root root 4096 May 18 16:03 lib
drwxr-xr-x.  2 root root 4096 May 18 16:03 local
lrwxrwxrwx.  1 root root   11 May 14 00:12 lock -> ../run/lock
drwxr-xr-x. 14 root root 4096 Sep 14 20:42 log
lrwxrwxrwx.  1 root root   10 Jul 30 22:43 mail -> spool/mail
drwxr-xr-x.  2 root root 4096 May 18 16:03 nis
drwxr-xr-x.  2 root root 4096 May 18 16:03 opt
drwxr-xr-x.  2 root root 4096 May 18 16:03 preserve
drwxr-xr-x.  2 root root 4096 Jul  1 22:11 report
lrwxrwxrwx.  1 root root    6 May 14 00:12 run -> ../run
drwxr-xr-x. 14 root root 4096 May 18 16:03 spool
drwxrwxrwt.  4 root root 4096 Sep 12 23:50 tmp
drwxr-xr-x.  2 root root 4096 May 18 16:03 yp
[root@localhost var]# yum search wiki
Loaded plugins: langpacks, presto, refresh-packagekit, remove-with-leaves
rpmfusion-free-updates                                          | 2.7 kB     00:00
rpmfusion-free-updates/primary_db                               | 206 kB     00:04
rpmfusion-nonfree-updates                                       | 2.7 kB     00:00
updates/metalink                                                | 5.9 kB     00:00
updates                                                         | 4.7 kB     00:00
updates/primary_db                          73% [=================       ]  62 kB/s | 2.6 MB     00:15 ETA
```



198.74.50.189

```
[root@localhost ~]# ping -q fa.wikipedia.org
PING text.pmtpa.wikimedia.org (208.80.152.2) 56(84) bytes of data.
^C
--- text.pmtpa.wikimedia.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 540.528/540.528/540.528/0.000 ms
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /var
[root@localhost var]# ls -la
total 72
drwxr-xr-x. 18 root root 4096 Jul 30 22:43 .
drwxr-xr-x. 23 root root 4096 Sep 14 20:42 ..
drwxr-xr-x.  2 root root 4096 May 14 00:15 account
drwxr-xr-x. 11 root root 4096 Jul 31 22:26 cache
drwxr-xr-x.  3 root root 4096 May 18 16:03 db
drwxr-xr-x.  3 root root 4096 May 18 16:03 empty
drwxr-xr-x.  2 root root 4096 May 18 16:03 games
drwxrwx--T.  2 root gdm  4096 Jun  2 18:39 gdm
drwxr-xr-x. 38 root root 4096 May 18 16:03 lib
drwxr-xr-x.  2 root root 4096 May 18 16:03 local
lrwxrwxrwx.  1 root root   11 May 14 00:12 lock -> ../run/lock
drwxr-xr-x. 14 root root 4096 Sep 14 20:42 log
lrwxrwxrwx.  1 root root   10 Jul 30 22:43 mail -> spool/mail
drwxr-xr-x.  2 root root 4096 May 18 16:03 nis
drwxr-xr-x.  2 root root 4096 May 18 16:03 opt
drwxr-xr-x.  2 root root 4096 May 18 16:03 preserve
drwxr-xr-x.  2 root root 4096 Jul  1 22:11 report
lrwxrwxrwx.  1 root root    6 May 14 00:12 run -> ../run
drwxr-xr-x. 14 root root 4096 May 18 16:03 spool
drwxrwxrwt.  4 root root 4096 Sep 12 23:50 tmp
drwxr-xr-x.  2 root root 4096 May 18 16:03 yp
[root@localhost var]# yum search wikl
Loaded plugins: langpacks, presto, refresh-packagekit, remove-with-leaves
rpmfusion-free-updates                                          | 2.7 kB     00:00
rpmfusion-free-updates/primary_db                               | 206 kB     00:04
rpmfusion-nonfree-updates                                       | 2.7 kB     00:00
updates/metalink                                                | 5.9 kB     00:00
updates                                                         | 4.7 kB     00:00
updates/primary_db                          73% [==================       ]  62 kB/s | 2.6 MB     00:15 ETA
```

HostGator

Web Hosting


buildasoc – SOC Building!
buildasoc.com
Search
buildasoc
SHOW ME

josh — josh@zvmship: ~ — -bash — 75×51

evol13:~ josh$

debian-8.3.0-amd64-...tinst.iso

Screen Shot 2016-0...PM.png

stuff

clouds_formoving.psd

clouds

NLPRankinator

investigate-API

kevinsloganalysis.py

things for presentation

Screen Shot 2016-03...AM.png

Monitored Site

Threat Analysis

..or predicting the future

Systems that move

How do you detect mobile threats?

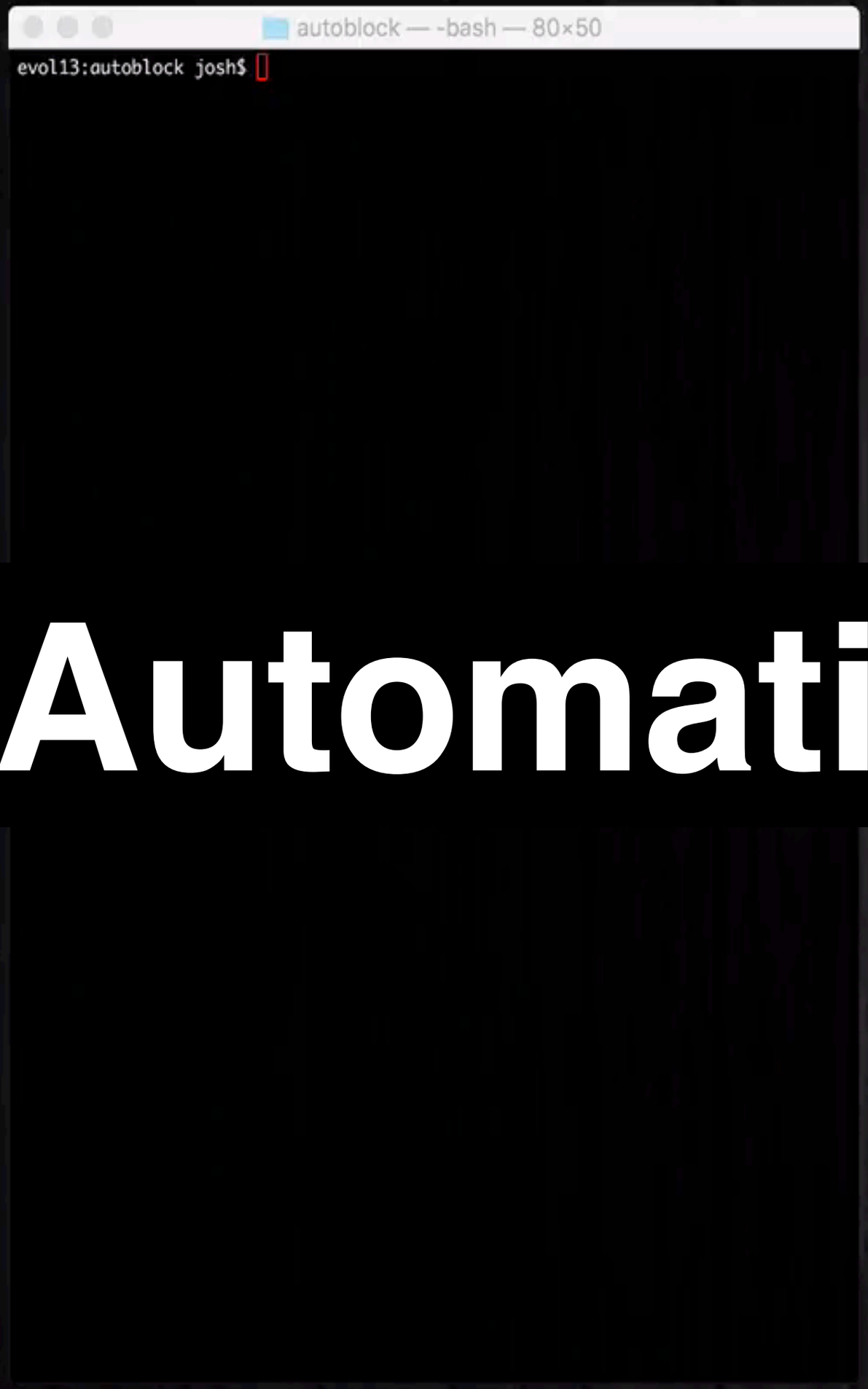
What about BYOD?

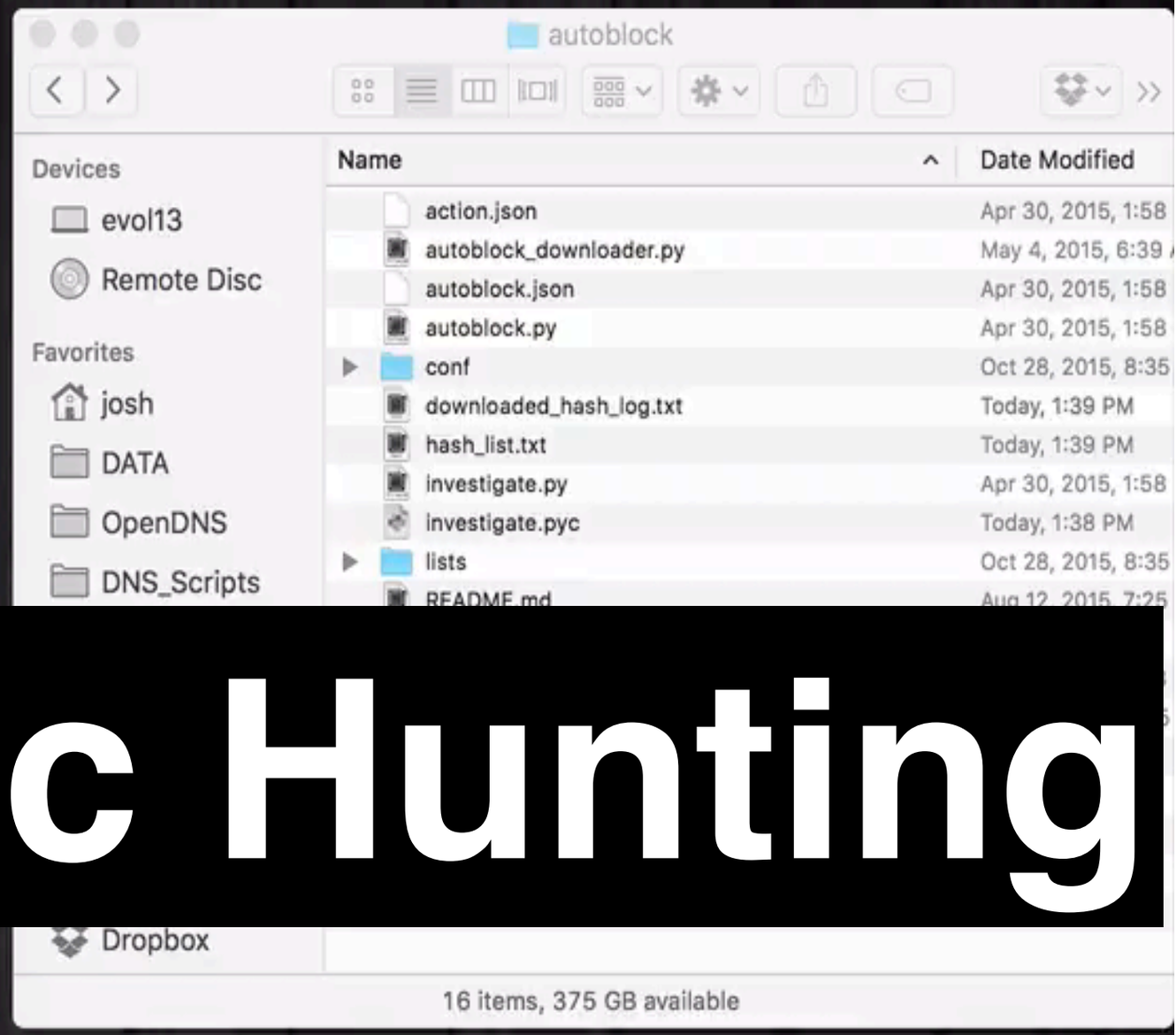
What if the laptop is outside the perimeter and off VPN?

Pointing DNS to custom DNS server

Automation

Automatic Hunting





Automatic Analysis

- Sending to Threat Services / Providing
- Sending to Cuckoo or malwr.com
- **Scraping Sites**

Limited Staff

How does one person monitor all this?

The Modern SOC
Adapting to how we work

@joshpyorre
rootaccesspodcast.com