Enterprise Information Services

Remote DFIR Investigations - Introducing the OAFE

Rich Baker

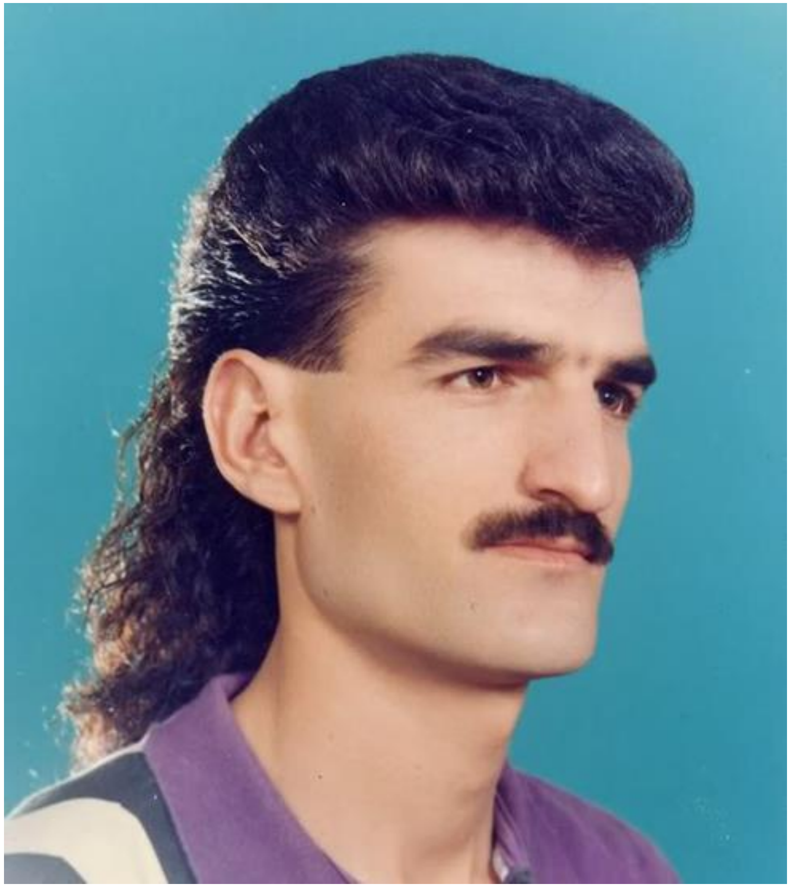
Optum Technology

June 23, 2017

BrrCon

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

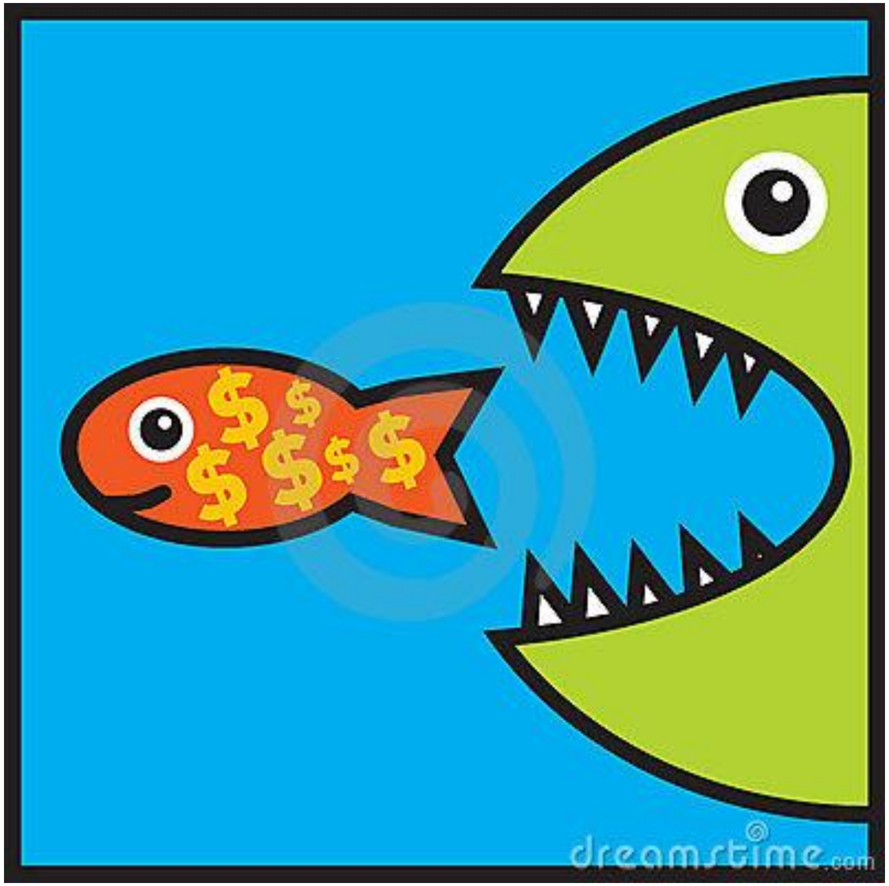
Business in the Front, Party in the Back



© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

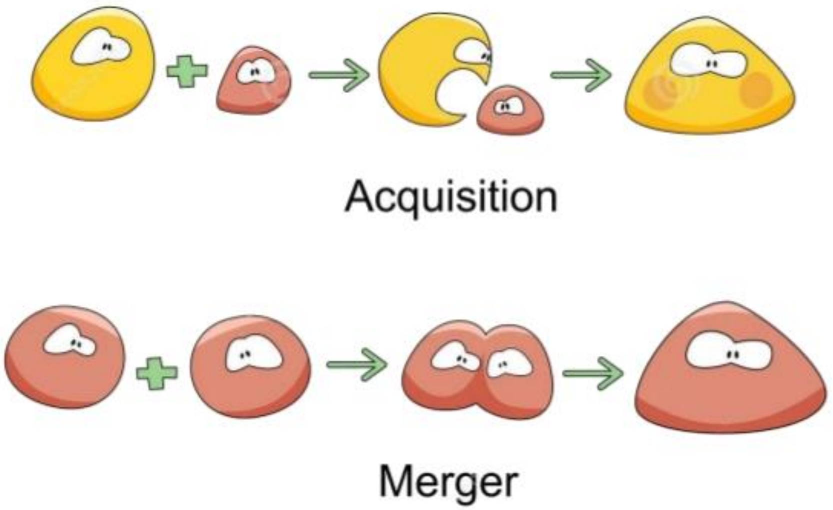
Mergers and Acquisitions (Acquired Entities)

- Big companies are purchasing smaller, high margin companies to sustain growth
- The smaller companies are usually in the process of purchasing even smaller companies to sustain growth…



© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Merger vs Acquisition



Company A merges with Company B but is owned by Company C.

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Advantages of the M&A Process

- ✓ Increased market share
- ✓ Diversification
- ✓ Lower costs of operation
- ✓ Gain a higher level of competitiveness
- ✓ Improve profitability
- ✓ New career advancement opportunities for employees
- ✓ International expansion

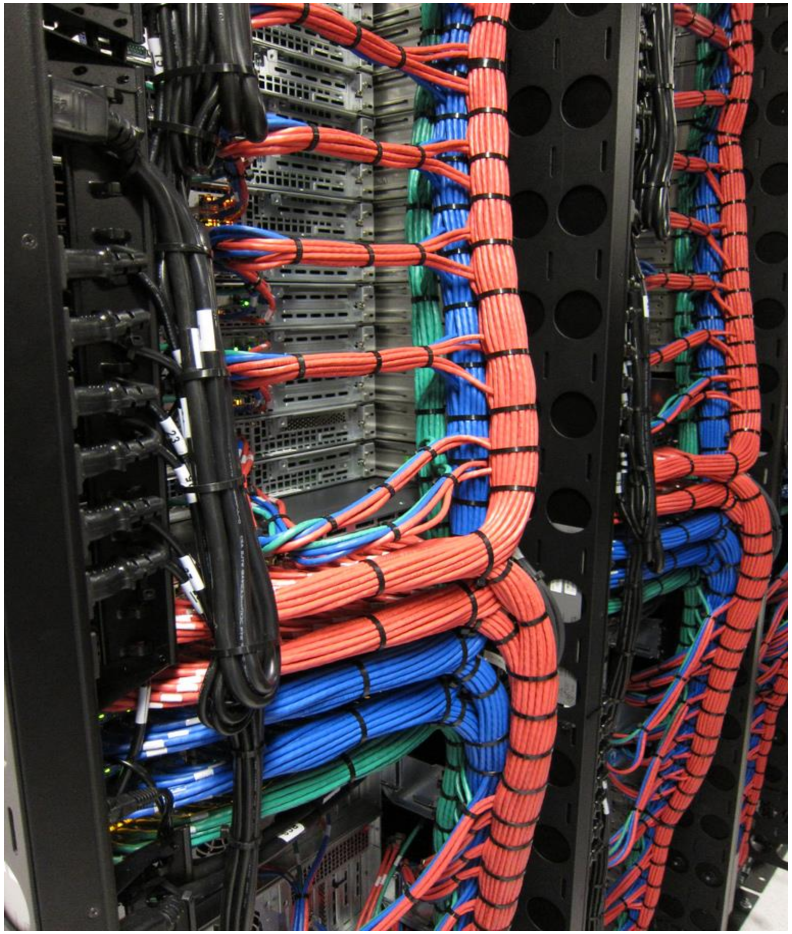
© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

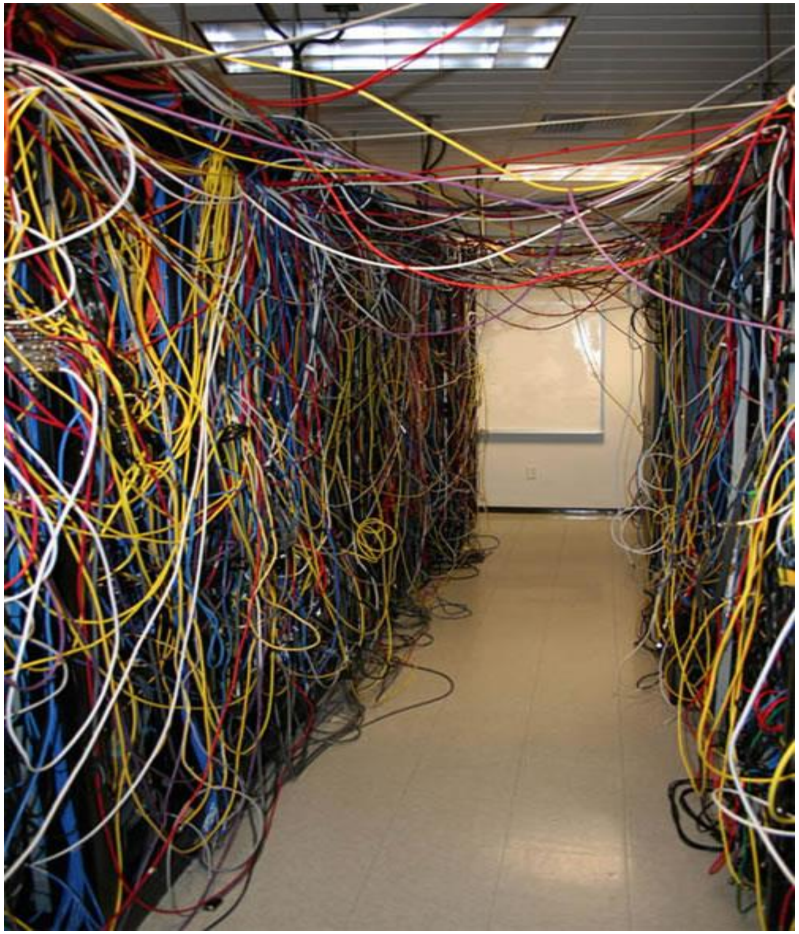
Disadvantages of the M&A Process

- ✓ Difficult to successfully ascertain fair market value. Especially difficult with privately held companies.
- ✓ **Ascertaining risk**
- ✓ Successful integration of culture. Moral issues.
- ✓ Merging/integrating information technology
- ✓ Increased debt

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

The Good and the Bad…





© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

DFIR Investigation Issues with Acquired Entities

- ✓ Network Visibility (DPI, Netflow)
- ✓ Lack of endpoint investigation resources
- ✓ Inconsistent or non-existent DNS logs
- ✓ Logging of critical infrastructure devices (Firewalls, proxies, domain controllers, dhcp, etc)
- ✓ Inexperienced personnel
- ✓ Centrally managed information security systems
- ✓ Old technology

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

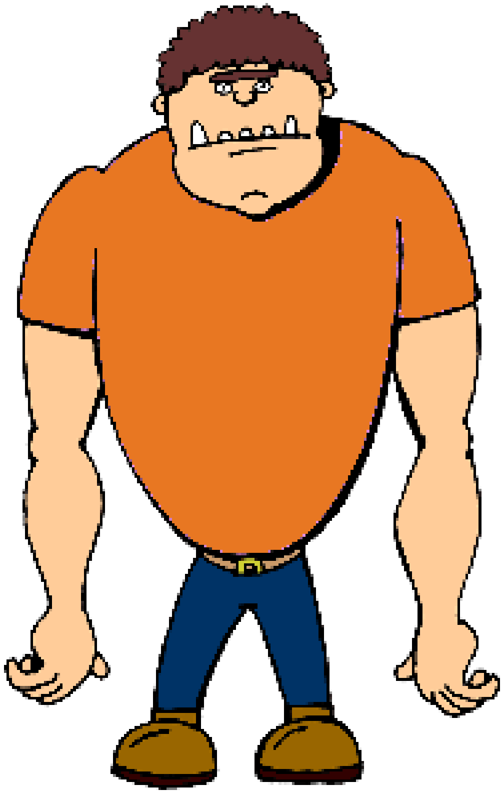
Addressing the DFIR Investigation Issues

- ✓ Rapidly deployed bastion host
- ✓ Minimal impact on AE staff and network
- ✓ Low cost toolset that maps to core commercial tool functionality
- ✓ Reduce the amount of time DFIR resources are deployed onsite
- ✓ Augment AE information security personnel
- ✓ Utilize commercial intelligence services (if available)

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

The Open Advanced Forensic Examiner™

O.A.F.E.™



© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

What is the OAFE™?

- ✓ Function – Assists with network and endpoint forensic analysis at remote locations.
- ✓ Design – Initially designed for centrally managed networks (hub and spoke), but can be utilized for small branches or entities. Originally forked from the SANS SIFT bootstrap[1].
- ✓ Hardware – Designed to operate on a modest platform. Previous generation servers work well.
- ✓ Deployment – Rapidly deployable on average hardware in a matter of hours.
- ✓ Technologies – Deep packet inspection, netflow, big data analytics and visualization, log aggregation, network malware detection, malware analysis, incident response tickteting, endpoint forensic analysis, endpoint detection and response, and many others…

1 - https://github.com/sans-dfir/sift-bootstrap

OPTUM®

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

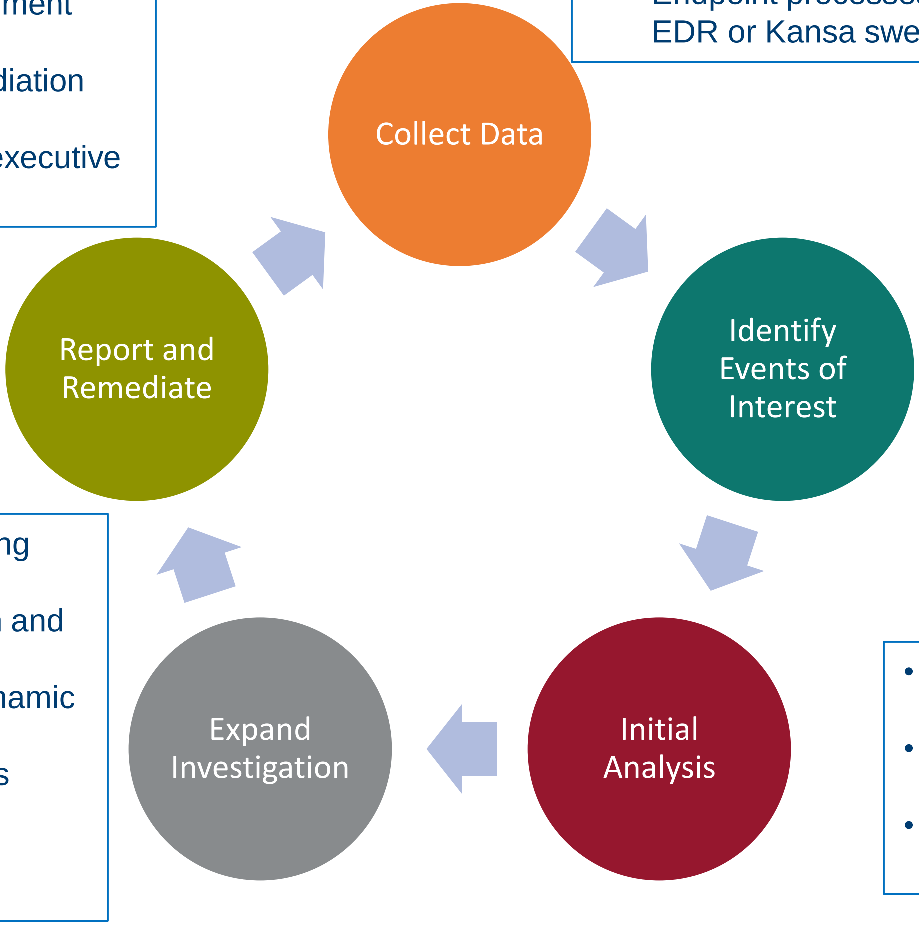
Enterprise System to OAFE™ Technology Mapping

Technology	Enterprise System	OAFE™ Tools	Notes
Deep Packet Inspection	Symantec/BlueCoat/Solera	Moloch, Bro	
Network Malware Inspection	Cisco AMP, McAfee Advance Threat Defense, FireEye	Maltrail	
Endpoint Forensics	FTK, X-Ways, F-Response, EnCase	Google Rapid Response	
Incident Response Ticketing	ServiceNow, Remedy, Resilient	Fast Incident Response	
Data Analytics and Visualization	Cybereason, IBM, Fortscale	Elasticsearch, Logstash, Kibana	
Log Management	Qradar, Splunk	Filebeat ingest to ELK	
Endpoint Detection & Response	Tanium, CarbonBlack, RSA eCat, FireEye HX	Lima Charlie	Integration in early July. Currently in dev branch.
Malware Static Analysis		Viper, FAME	FAME is currently in testing.
Neflow	Cisco, ManageEngine	Ntopng	
DNS Logging	InfoBlox, BIND, AD DNS	Bro w/ Logstash ingest to Elastic	
Malware Dynamic Analysis	Cisco ThreatGrid, Joe Sandbox	Cuckoo	FAME may necessitate the addition of cuckoo modified.
Intrusion Detection/Prevention	IBM, TippingPoint, Radware, Cisco	Suricata, Bro	

OPTUM®

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Analysis Process



- Ingress and egress network traffic
- Passive DNS request and response data
- Netflow
- Endpoint processes imported from EDR or Kansa sweeps

- Review Maltrail and EDR alerts
- Visualize Kansa data for potentially malicious software

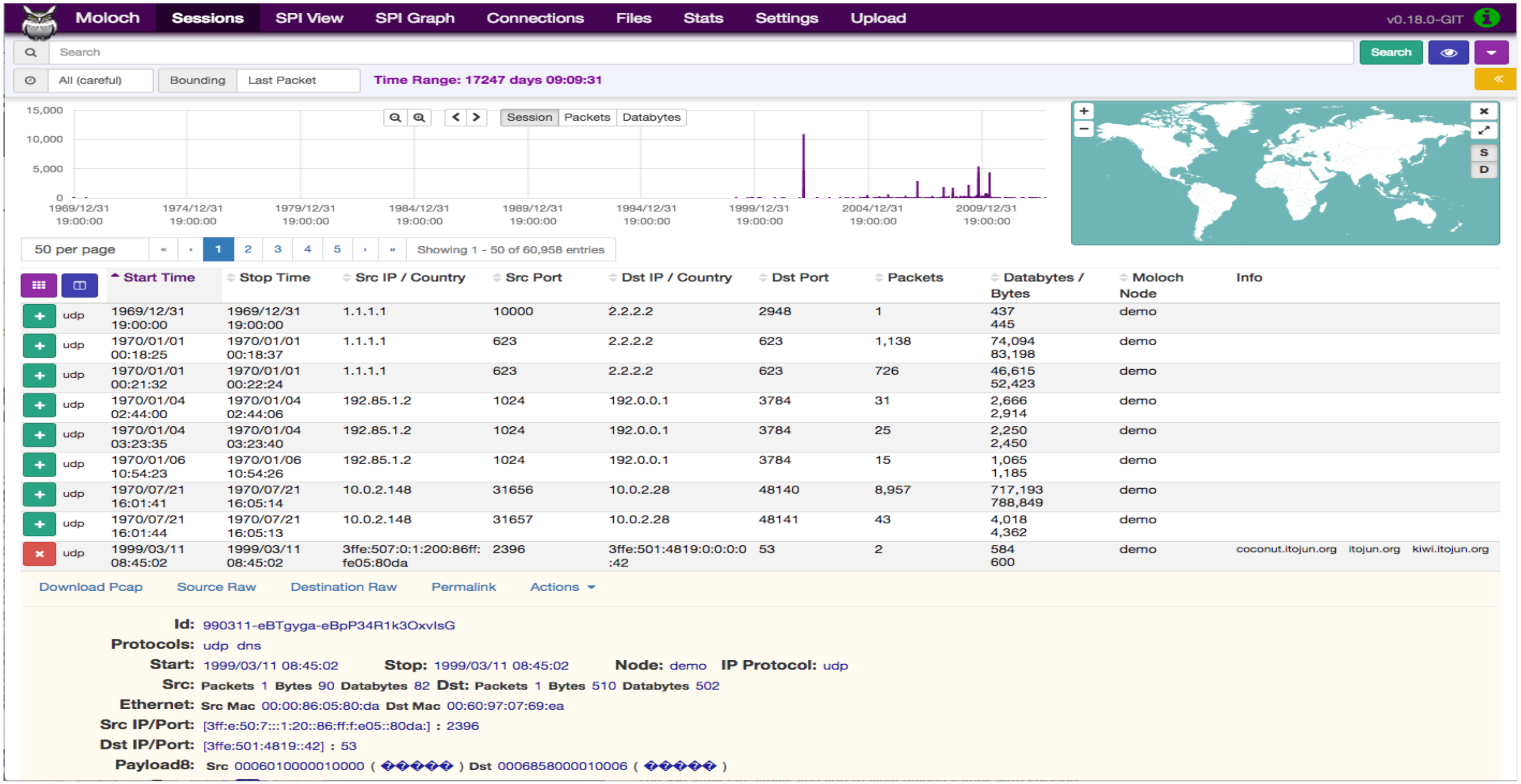
- Validate alerts from EDR, Kansa, and Maltrail
- Hunt threats via DNS, DPI, GRR, and EDR
- Investigate endpoints, utilizing collected data

- In-depth investigations utilizing tactics including
    - Event log aggregation and analysis
    - Malware analysis (dynamic and static)
    - Netflow traffic analysis
    - Network forensics
    - Memory analysis
    - Endpoint forensics

- Escalate priority issues for legal/executive review
- Pursue short term containment tactics
- Identify longer term remediation
- Construct attack timeline
- Issue report to legal and executive leadership

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Interfaces – Moloch DPI



Time Range: 17247 days 09:09:31

Showing 1 - 50 of 60,958 entries

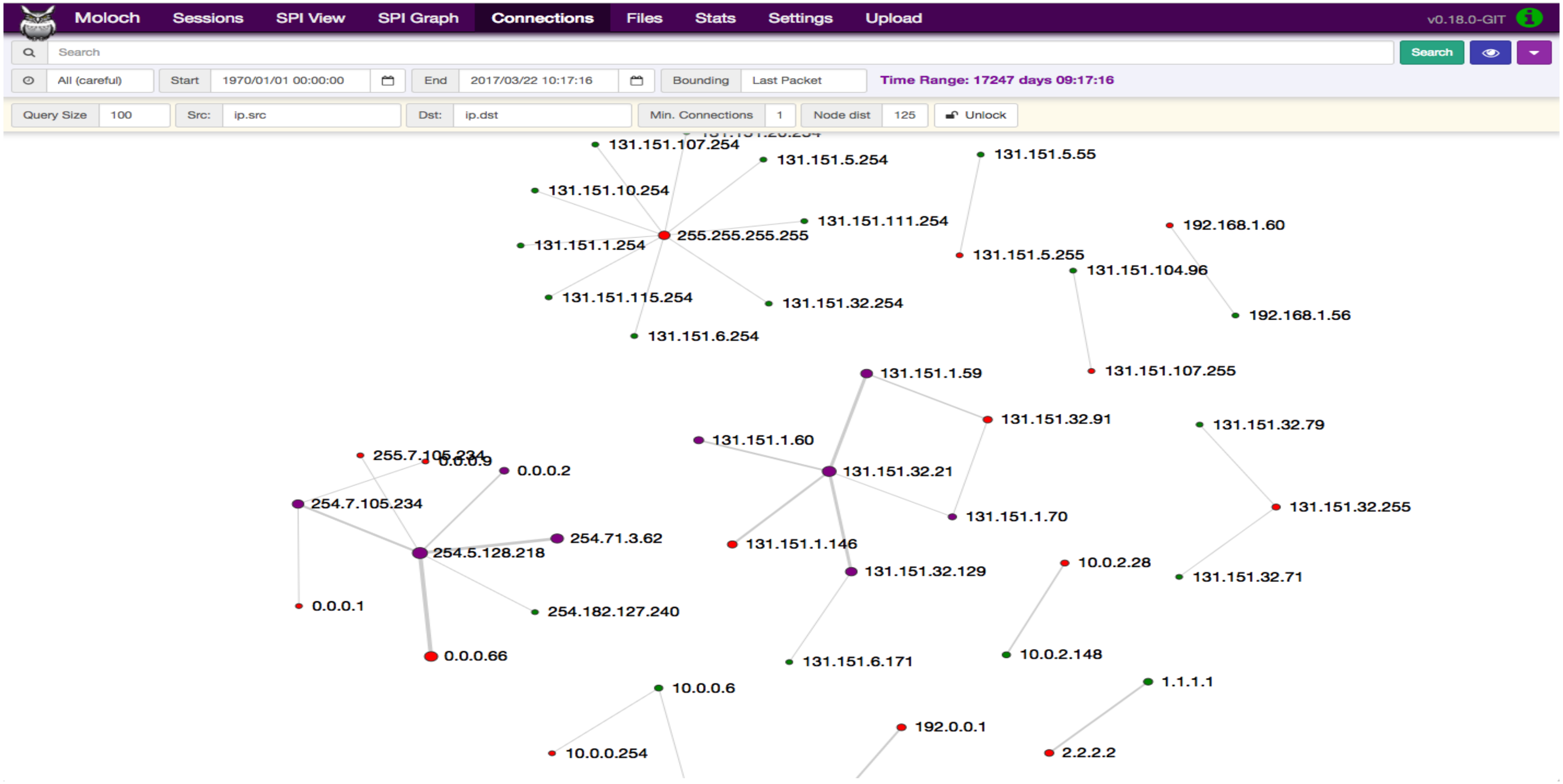
		Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
+	udp	1969/12/31 19:00:00	1969/12/31 19:00:00	1.1.1.1	10000	2.2.2.2	2948	1	437 445	demo	
+	udp	1970/01/01 00:18:25	1970/01/01 00:18:37	1.1.1.1	623	2.2.2.2	623	1,138	74,094 83,198	demo	
+	udp	1970/01/01 00:21:32	1970/01/01 00:22:24	1.1.1.1	623	2.2.2.2	623	726	46,615 52,423	demo	
+	udp	1970/01/04 02:44:00	1970/01/04 02:44:06	192.85.1.2	1024	192.0.0.1	3784	31	2,666 2,914	demo	
+	udp	1970/01/04 03:23:35	1970/01/04 03:23:40	192.85.1.2	1024	192.0.0.1	3784	25	2,250 2,450	demo	
+	udp	1970/01/06 10:54:23	1970/01/06 10:54:26	192.85.1.2	1024	192.0.0.1	3784	15	1,065 1,185	demo	
+	udp	1970/07/21 16:01:41	1970/07/21 16:05:14	10.0.2.148	31656	10.0.2.28	48140	8,957	717,193 788,849	demo	
+	udp	1970/07/21 16:01:44	1970/07/21 16:05:13	10.0.2.148	31657	10.0.2.28	48141	43	4,018 4,362	demo	
×	udp	1999/03/11 08:45:02	1999/03/11 08:45:02	3ffe:507:0:1:200:86ff: fe05:80da	2396	3ffe:501:4819:0:0:0:0 :42	53	2	584 600	demo	coconut.itojun.org itojun.org kiwi.itojun.org

Download Pcap   Source Raw   Destination Raw   Permalink   Actions ▾

Id: 990311-eBTgyga-eBpP34R1k3OxvIsG
Protocols: udp dns
Start: 1999/03/11 08:45:02 **Stop:** 1999/03/11 08:45:02 **Node:** demo **IP Protocol:** udp
Src: Packets 1 Bytes 90 Databytes 82 **Dst:** Packets 1 Bytes 510 Databytes 502
Ethernet: Src Mac 00:00:86:05:80:da Dst Mac 00:60:97:07:69:ea
Src IP/Port: [3ff:e:50:7:::1:20::86:ff:f:e05::80da:] : 2396
Dst IP/Port: [3ffe:501:4819::42] : 53
Payload8: Src 0006010000010000 (�����) Dst 0006858000010006 (�����)

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Interfaces – Moloch DPI - Connections

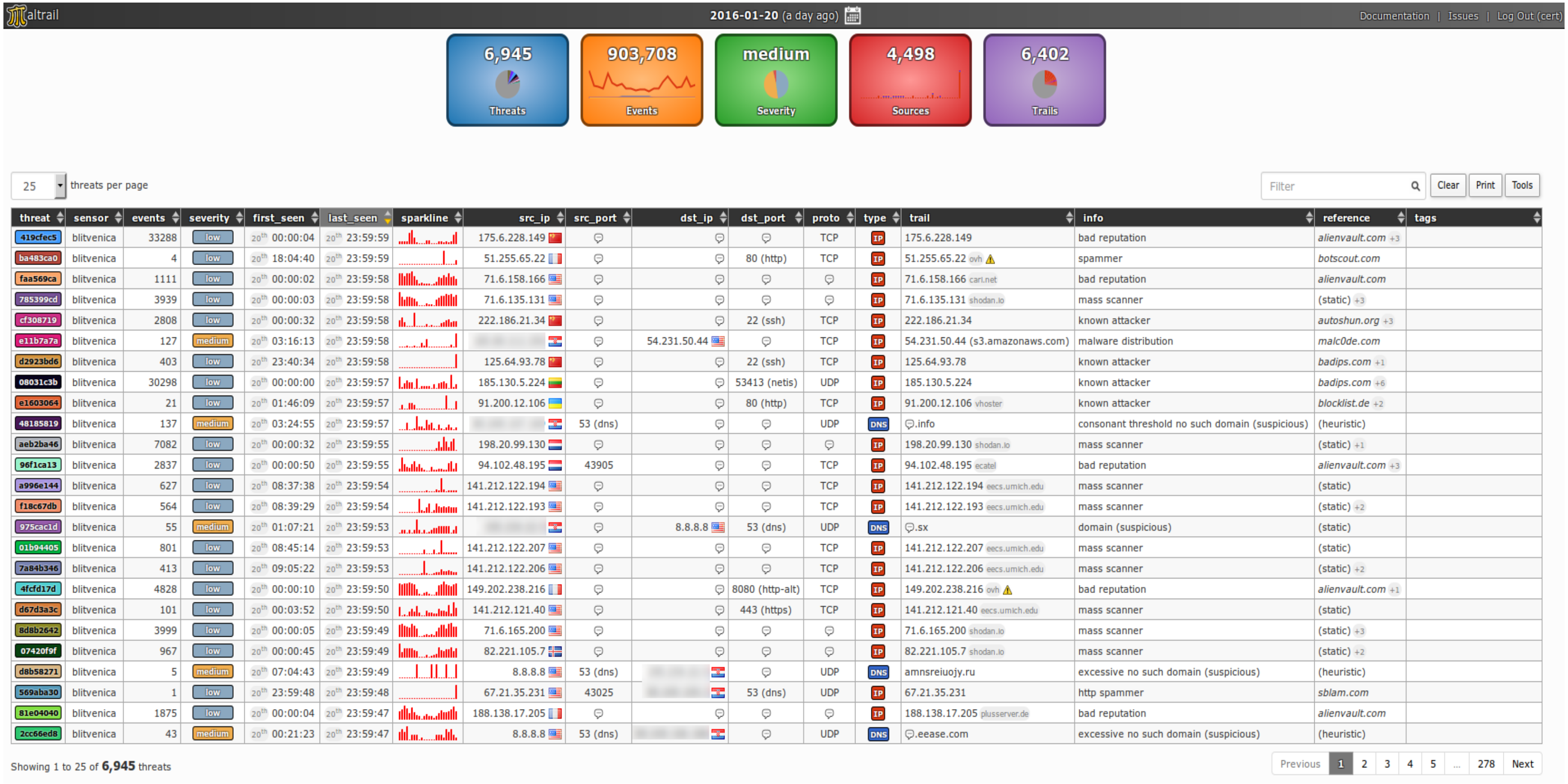


All (careful) | Start 1970/01/01 00:00:00 | End 2017/03/22 10:17:16 | Bounding Last Packet | Time Range: 17247 days 09:17:16

Query Size 100 | Src: ip.src | Dst: ip.dst | Min. Connections 1 | Node dist 125

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Interfaces - Maltrail



25 threats per page

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
419cfec5	blitvenica	33288	low	20th 00:00:04	20th 23:59:59		175.6.228.149	💬	💬	💬	TCP	IP	175.6.228.149	bad reputation	*alienvault.com* +3	
ba483ca0	blitvenica	4	low	20th 18:04:40	20th 23:59:59		51.255.65.22	💬	💬	80 (http)	TCP	IP	51.255.65.22 ovh ⚠	spammer	*botscout.com*	
faa569ca	blitvenica	1111	low	20th 00:00:02	20th 23:59:58		71.6.158.166	💬	💬	💬	💬	IP	71.6.158.166 cari.net	bad reputation	*alienvault.com*	
785399cd	blitvenica	3939	low	20th 00:00:03	20th 23:59:58		71.6.135.131	💬	💬	💬	💬	IP	71.6.135.131 shodan.io	mass scanner	(static) +3	
cf308719	blitvenica	2808	low	20th 00:00:32	20th 23:59:58		222.186.21.34	💬	💬	22 (ssh)	TCP	IP	222.186.21.34	known attacker	*autoshun.org* +3	
e11b7a7a	blitvenica	127	medium	20th 03:16:13	20th 23:59:58		[redacted]	💬	54.231.50.44	💬	TCP	IP	54.231.50.44 (s3.amazonaws.com)	malware distribution	*malc0de.com*	
d2923bd6	blitvenica	403	low	20th 23:40:34	20th 23:59:58		125.64.93.78	💬	💬	22 (ssh)	TCP	IP	125.64.93.78	known attacker	*badips.com* +1	
08031c3b	blitvenica	30298	low	20th 00:00:00	20th 23:59:57		185.130.5.224	💬	💬	53413 (netis)	UDP	IP	185.130.5.224	known attacker	*badips.com* +6	
e1603064	blitvenica	21	low	20th 01:46:09	20th 23:59:57		91.200.12.106	💬	💬	80 (http)	TCP	IP	91.200.12.106 vhoster	known attacker	*blocklist.de* +2	
48185819	blitvenica	137	medium	20th 03:24:55	20th 23:59:57		[redacted]	53 (dns)	💬	💬	UDP	DNS	💬.info	consonant threshold no such domain (suspicious)	(heuristic)	
aeb2ba46	blitvenica	7082	low	20th 00:00:32	20th 23:59:55		198.20.99.130	💬	💬	💬	💬	IP	198.20.99.130 shodan.io	mass scanner	(static) +1	
96f1ca13	blitvenica	2837	low	20th 00:00:50	20th 23:59:55		94.102.48.195	43905	💬	💬	TCP	IP	94.102.48.195 ecatel	bad reputation	*alienvault.com* +3	
a996e144	blitvenica	627	low	20th 08:37:38	20th 23:59:54		141.212.122.194	💬	💬	💬	TCP	IP	141.212.122.194 eecs.umich.edu	mass scanner	(static)	
f18c67db	blitvenica	564	low	20th 08:39:29	20th 23:59:54		141.212.122.193	💬	💬	💬	TCP	IP	141.212.122.193 eecs.umich.edu	mass scanner	(static) +2	
975cac1d	blitvenica	55	medium	20th 01:07:21	20th 23:59:53		[redacted]	💬	8.8.8.8	53 (dns)	UDP	DNS	💬.sx	domain (suspicious)	(static)	
01b94405	blitvenica	801	low	20th 08:45:14	20th 23:59:53		141.212.122.207	💬	💬	💬	TCP	IP	141.212.122.207 eecs.umich.edu	mass scanner	(static)	
7a84b346	blitvenica	413	low	20th 09:05:22	20th 23:59:53		141.212.122.206	💬	💬	💬	TCP	IP	141.212.122.206 eecs.umich.edu	mass scanner	(static) +2	
4fcfd17d	blitvenica	4828	low	20th 00:00:10	20th 23:59:50		149.202.238.216	💬	💬	8080 (http-alt)	TCP	IP	149.202.238.216 ovh ⚠	bad reputation	*alienvault.com* +1	
d67d3a3c	blitvenica	101	low	20th 00:03:52	20th 23:59:50		141.212.121.40	💬	💬	443 (https)	TCP	IP	141.212.121.40 eecs.umich.edu	mass scanner	(static)	
8d8b2642	blitvenica	3999	low	20th 00:00:05	20th 23:59:49		71.6.165.200	💬	💬	💬	💬	IP	71.6.165.200 shodan.io	mass scanner	(static) +3	
07420f9f	blitvenica	967	low	20th 00:00:45	20th 23:59:49		82.221.105.7	💬	💬	💬	💬	IP	82.221.105.7 shodan.io	mass scanner	(static) +2	
d8b58271	blitvenica	5	medium	20th 07:04:43	20th 23:59:49		8.8.8.8	53 (dns)	[redacted]	💬	UDP	DNS	amnsreiuojy.ru	excessive no such domain (suspicious)	(heuristic)	
569aba30	blitvenica	1	low	20th 23:59:48	20th 23:59:48		67.21.35.231	43025	[redacted]	53 (dns)	UDP	IP	67.21.35.231	http spammer	*sblam.com*	
81e04040	blitvenica	1875	low	20th 00:00:04	20th 23:59:47		188.138.17.205	💬	💬	💬	💬	IP	188.138.17.205 plusserver.de	bad reputation	*alienvault.com*	
2cc66ed8	blitvenica	43	medium	20th 00:21:23	20th 23:59:47		8.8.8.8	53 (dns)	[redacted]	💬	UDP	DNS	💬.eease.com	excessive no such domain (suspicious)	(heuristic)	

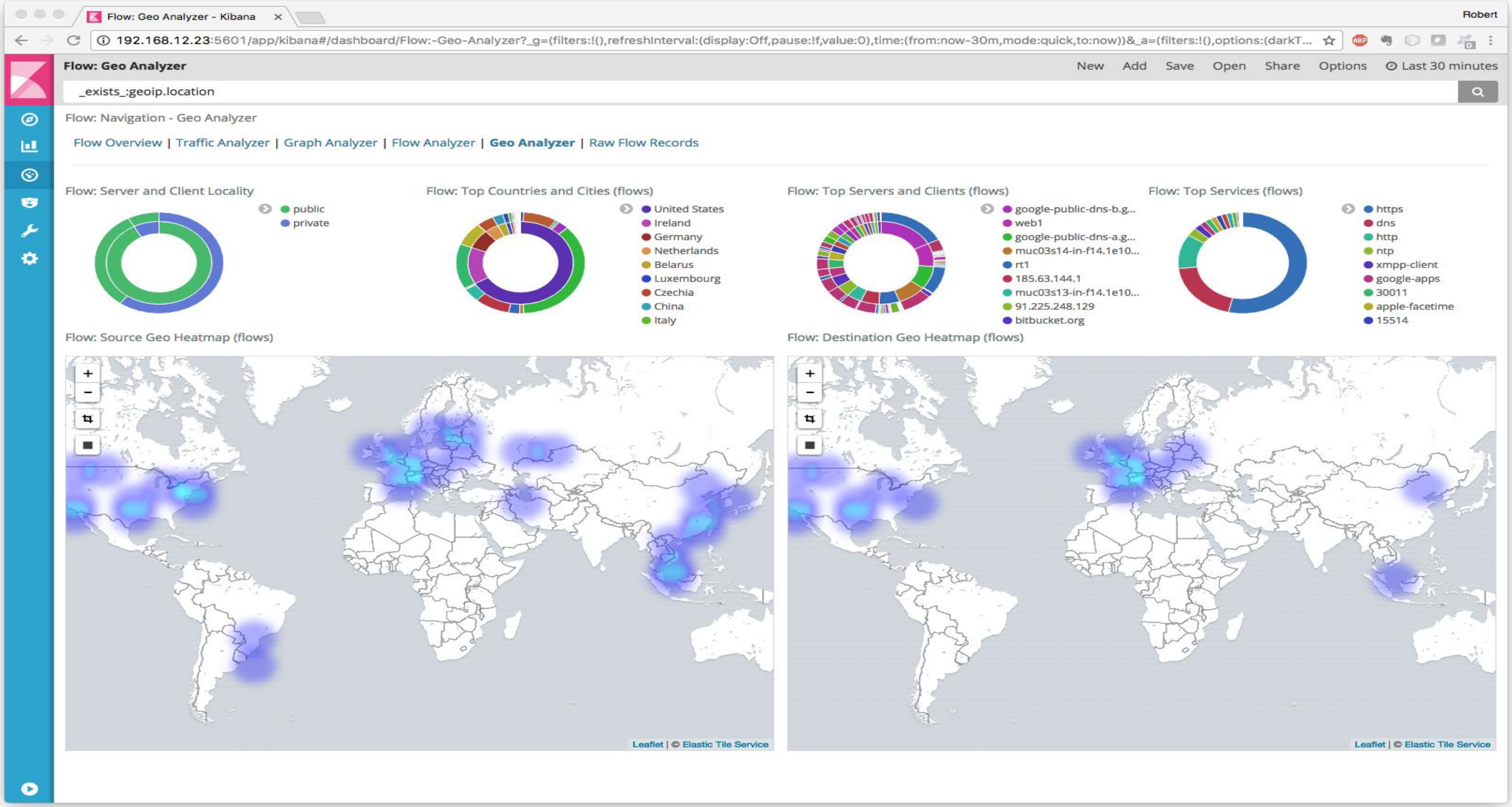
Showing 1 to 25 of **6,945** threats

Previous 1 2 3 4 5 … 278 Next

OPTUM®

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Interfaces - Kibana



Flow: Geo Analyzer - Kibana

192.168.12.23:5601/app/kibana#/dashboard/Flow:-Geo-Analyzer?_g=(filters:!(),refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-30m,mode:quick,to:now))&_a=(filters:!(),options:(darkT...

Flow: Geo Analyzer

exists:geoip.location

Flow: Navigation - Geo Analyzer

Flow Overview | Traffic Analyzer | Graph Analyzer | Flow Analyzer | **Geo Analyzer** | Raw Flow Records

Flow: Server and Client Locality

Flow: Top Countries and Cities (flows)

Flow: Top Servers and Clients (flows)

Flow: Top Services (flows)

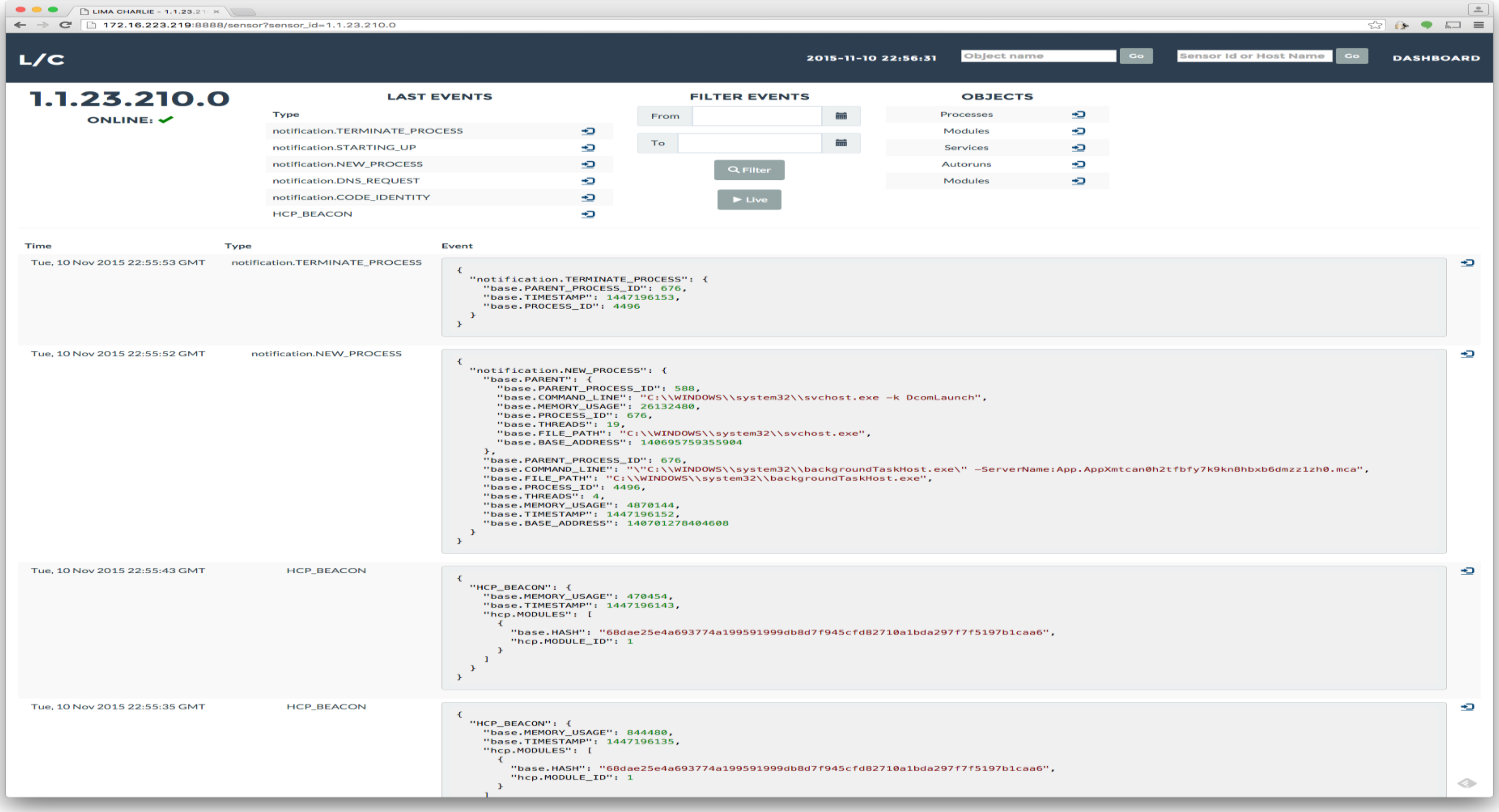
Flow: Source Geo Heatmap (flows)

Flow: Destination Geo Heatmap (flows)

OPTUM®

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Interfaces – Lima Charlie



1.1.23.210.0

ONLINE: ✓

LAST EVENTS

Type
notification.TERMINATE_PROCESS
notification.STARTING_UP
notification.NEW_PROCESS
notification.DNS_REQUEST
notification.CODE_IDENTITY
HCP_BEACON

FILTER EVENTS

OBJECTS

Time	Type	Event
Tue, 10 Nov 2015 22:55:53 GMT	notification.TERMINATE_PROCESS	see below

```
{
  "notification.TERMINATE_PROCESS": {
    "base.PARENT_PROCESS_ID": 676,
    "base.TIMESTAMP": 1447196153,
    "base.PROCESS_ID": 4496
  }
}
```

Tue, 10 Nov 2015 22:55:52 GMT — notification.NEW_PROCESS

```
{
  "notification.NEW_PROCESS": {
    "base.PARENT": {
      "base.PARENT_PROCESS_ID": 588,
      "base.COMMAND_LINE": "C:\\WINDOWS\\system32\\svchost.exe -k DcomLaunch",
      "base.MEMORY_USAGE": 26132480,
      "base.PROCESS_ID": 676,
      "base.THREADS": 19,
      "base.FILE_PATH": "C:\\WINDOWS\\system32\\svchost.exe",
      "base.BASE_ADDRESS": 140695759355904
    },
    "base.PARENT_PROCESS_ID": 676,
    "base.COMMAND_LINE": "\"C:\\WINDOWS\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca",
    "base.FILE_PATH": "C:\\WINDOWS\\system32\\backgroundTaskHost.exe",
    "base.PROCESS_ID": 4496,
    "base.THREADS": 4,
    "base.MEMORY_USAGE": 4870144,
    "base.TIMESTAMP": 1447196152,
    "base.BASE_ADDRESS": 140701278404608
  }
}
```

Tue, 10 Nov 2015 22:55:43 GMT — HCP_BEACON

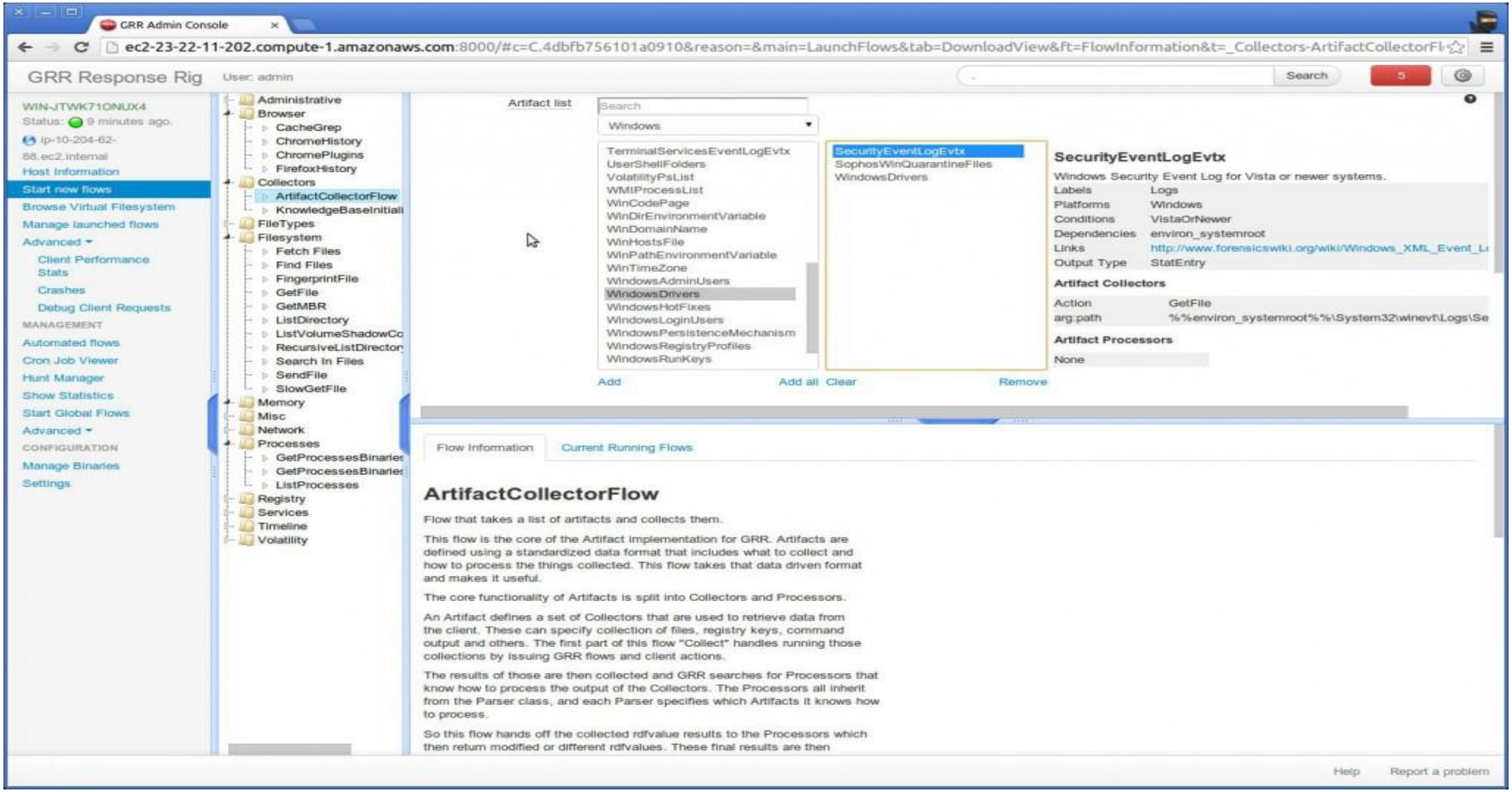
```
{
  "HCP_BEACON": {
    "base.MEMORY_USAGE": 470454,
    "base.TIMESTAMP": 1447196143,
    "hcp.MODULES": [
      {
        "base.HASH": "68dae25e4a693774a199591999db8d7f945cfd82710a1bda297f7f5197b1caa6",
        "hcp.MODULE_ID": 1
      }
    ]
  }
}
```

Tue, 10 Nov 2015 22:55:35 GMT — HCP_BEACON

```
{
  "HCP_BEACON": {
    "base.MEMORY_USAGE": 844480,
    "base.TIMESTAMP": 1447196135,
    "hcp.MODULES": [
      {
        "base.HASH": "68dae25e4a693774a199591999db8d7f945cfd82710a1bda297f7f5197b1caa6",
        "hcp.MODULE_ID": 1
      }
    ]
```

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Interfaces – Google Rapid Response (GRR)



SecurityEventLogEvtx

Windows Security Event Log for Vista or newer systems.

Labels	Logs
Platforms	Windows
Conditions	VistaOrNewer
Dependencies	environ_systemroot
Links	http://www.forensicswiki.org/wiki/Windows_XML_Event_L
Output Type	StatEntry

Artifact Collectors

Action	GetFile
arg:path	%%environ_systemroot%%\System32\winevt\Logs\Se

Artifact Processors

None

ArtifactCollectorFlow

Flow that takes a list of artifacts and collects them.

This flow is the core of the Artifact implementation for GRR. Artifacts are defined using a standardized data format that includes what to collect and how to process the things collected. This flow takes that data driven format and makes it useful.

The core functionality of Artifacts is split into Collectors and Processors.

An Artifact defines a set of Collectors that are used to retrieve data from the client. These can specify collection of files, registry keys, command output and others. The first part of this flow "Collect" handles running those collections by issuing GRR flows and client actions.

The results of those are then collected and GRR searches for Processors that know how to process the output of the Collectors. The Processors all inherit from the Parser class, and each Parser specifies which Artifacts it knows how to process.

So this flow hands off the collected rdfvalue results to the Processors which then return modified or different rdfvalues. These final results are then

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Requirements

- ✓ Semi-recent 4 core (or better) processor
- ✓ 250GB HDD (SSD or RAID preferred)
- ✓ 16GB RAM
- ✓ 2 Gigabit NICs
- ✓ Internet connection for install
- ✓ Ubuntu 16.04 LTS x64 desktop

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Our Preferred Hardware

- ✓ HPE DL Series Server
- ✓ 2 Processors – 36 Cores total
- ✓ 256GB RAM
- ✓ 10 – 1 TB Flash SSD RAID
- ✓ Quad Gigabit Ethernet and 2 – 10 Gigabit Ethernet
- ✓ $$$$$$

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Installation

- ✓ Fresh, updated build of Ubuntu 16.04 LTS x64 desktop
- ✓ Install nginx and git
- ✓ Clone the Github repository
- ✓ Start the bootstrap install script
- ✓ After the install (and reboot), install Google Rapid Response from the /opt/oafe/grr/ directory

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Customize For Your Platform

- ✓ Update /etc/rc.local to reflect your network interfaces
- ✓ /opt/oafe/maltrail/maltrail.conf – change MONITOR_INTERFACE to NIC with span/tap connection
- ✓ /data/moloch/etc/config.ini – interface line should reflect span/top connection
- ✓ /etc/nginx/sites-available/default – port changes for reverse proxy
- ✓ /etc/bro/node.cfg – update interface to span/tap NIC
- ✓ /etc/grr/server.local.yaml – Client.server_urls – change to IP address of management interface. Repack clients.

OPTUM®

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

More Customization

- ✓ Change default passwords (MySQL, Ntopng, etc)
- ✓ Add users to Moloch, Ntopng, GRR, Lima Charlie, etc
- ✓ Lima Charlie will need customization from web interface (localhost:8888 by default)
- ✓ Dockerized FIR install will need customization to be useful
- ✓ Cuckoo – Guest VMs are not provided. We are working on some documentation for best practices when building the guest VMs, based on our successes and failures. Configuration files will need to be customized.

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Cyber Intelligence Integration

- ✓ Commercial feeds can be utilized for Moloch (with WISE service enabled), Maltrail, and Bro
- ✓ Utilize Logstash ingest scripts to insert Bro data into Elastisearch.
  - – Some basic functionality is enable by default
  - – https://github.com/fakrul/bro-elk has some good ingest configurations for Bro -> ELK
- ✓ Many great tutorials available with a quick Hooli search
  - – https://www.elastic.co/blog/bro-ids-elastic-stack#sthash.376DHeng.dpbs

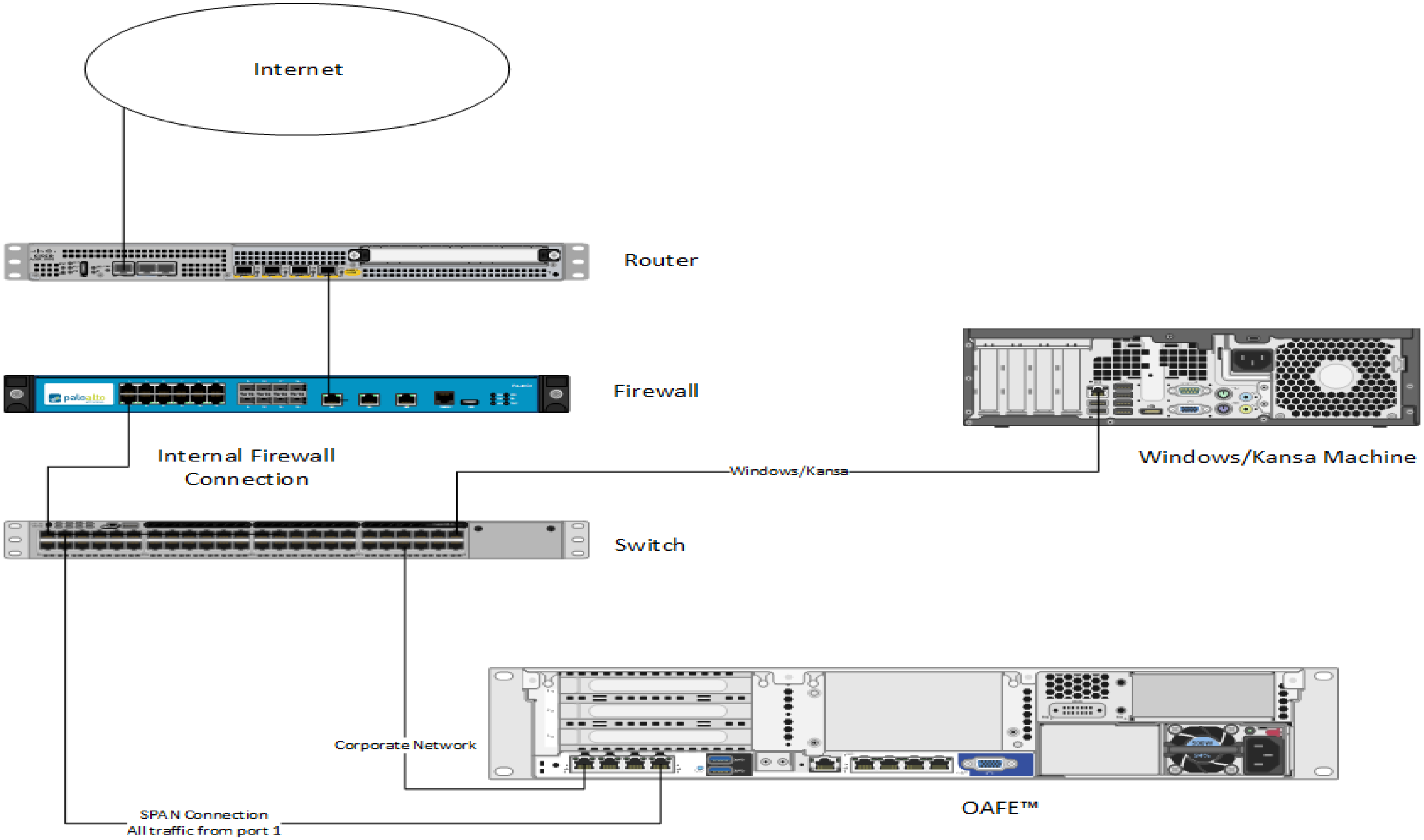
© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Occasional Issues

- ✓ Trouble starting services
  - – Grep processes to ensure successful startup
  - – ps -ef | grep moloch
  - – Use that for sensor, ntop, etc
- ✓ Startup services that may have failed
  - – systemctl start molochcapture.service
  - – Same syntax for molochviewer, maltrail, ntop, etc

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Network Diagram



© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Internal OAFE vs Open Source OAFE

Internal	Open Source
Centralized Logging	On Device Logging
SIEM	ELK (with customization)
Maltrail master trails server	Maltrail open source trails
Matchstick analytics	Not available
Shared sandboxes	Sandbox on device

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Centralize

- ✓ Add OpenVPN configurations
- ✓ SIEM
- ✓ Remote syslog server
- ✓ Maltrail trails server
  - Caveat – The Maltrail centralized server has an issue with https. This is an issue if you’re not pulling updates over an encrypted VPN session.

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Github

- ✓ Project will be available for download later today
- ✓ https://github.com/rebaker501/OAFE
- ✓ Feature requests and issues can be posted here (It will be best effort on these, as we are quite busy with our day jobs)

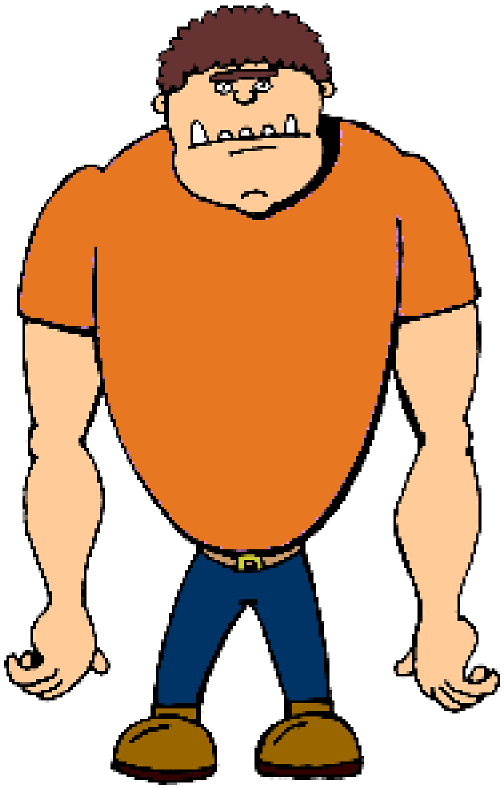
© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Contributions

- ✓ Designed to be customized
- ✓ Experienced shell scripting resources
- ✓ New technologies or updated technologies
- ✓ Constructive feedback
- ✓ Assistance with current issues (service autostart issues)

© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.

Questions/Discussion



© 2017 UnitedHealth Group. Any use, copying or distribution without written permission from UnitedHealth Group is prohibited.