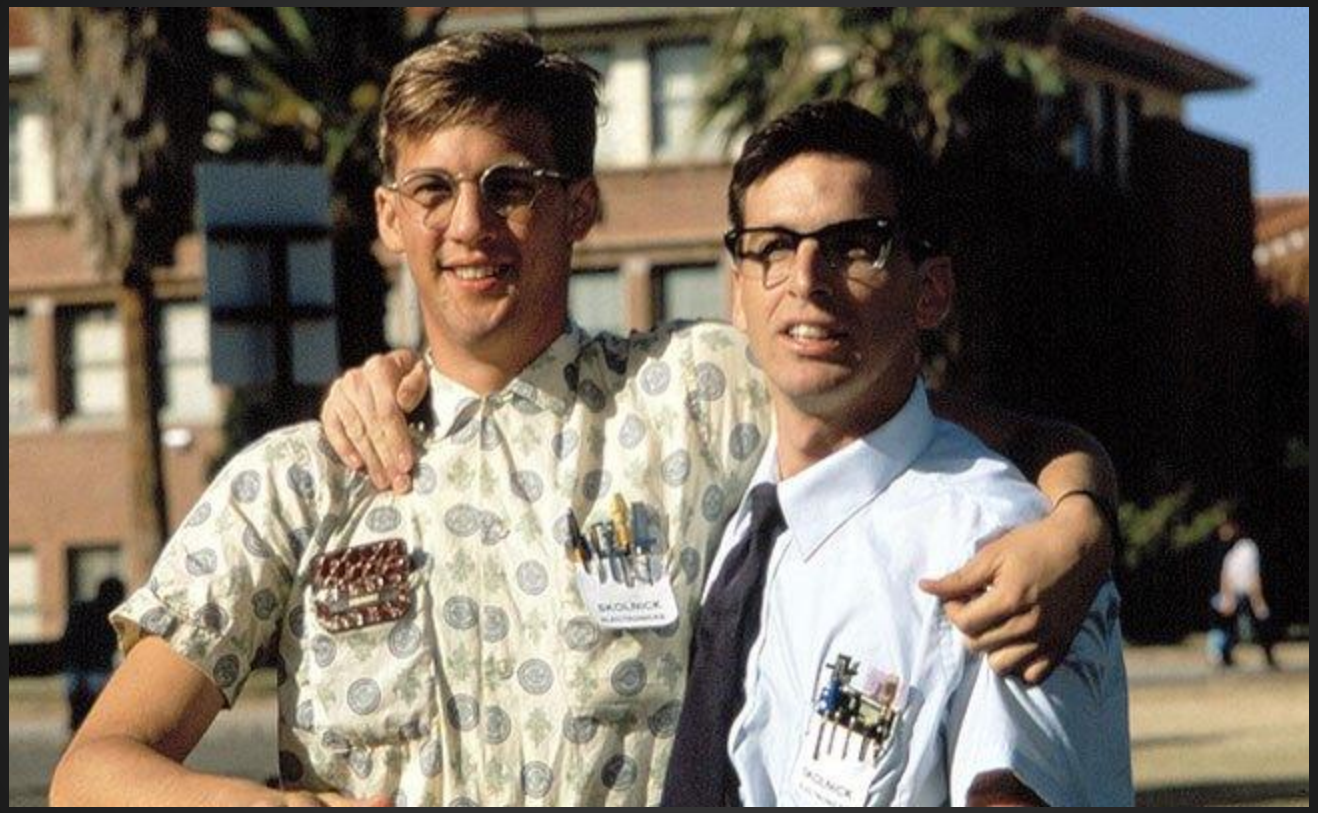
Suricata

Open Source Network IDS/IPS Engine

Introductions



Matt Jonkman
President,
OISF

Victor Julien
Lead Developer,
Suricata

T.B.A.

2003: “IDS is Dead” -- *Gartner*

The World has Changed

- Direct Attack Exploits Down
  - Attacking the User is easier
  - Attack the Browser/Plugins

Massively obfuscatable

The World has Changed

- Traffic Volumes Up
- Data Theft Rewards Up
- Costs of Compromise Up
- Nation State Activity

The World has Changed

- Computational Power Up
- Database Capabilities Up
- Defensive Spending Up
- Available Intelligence Up

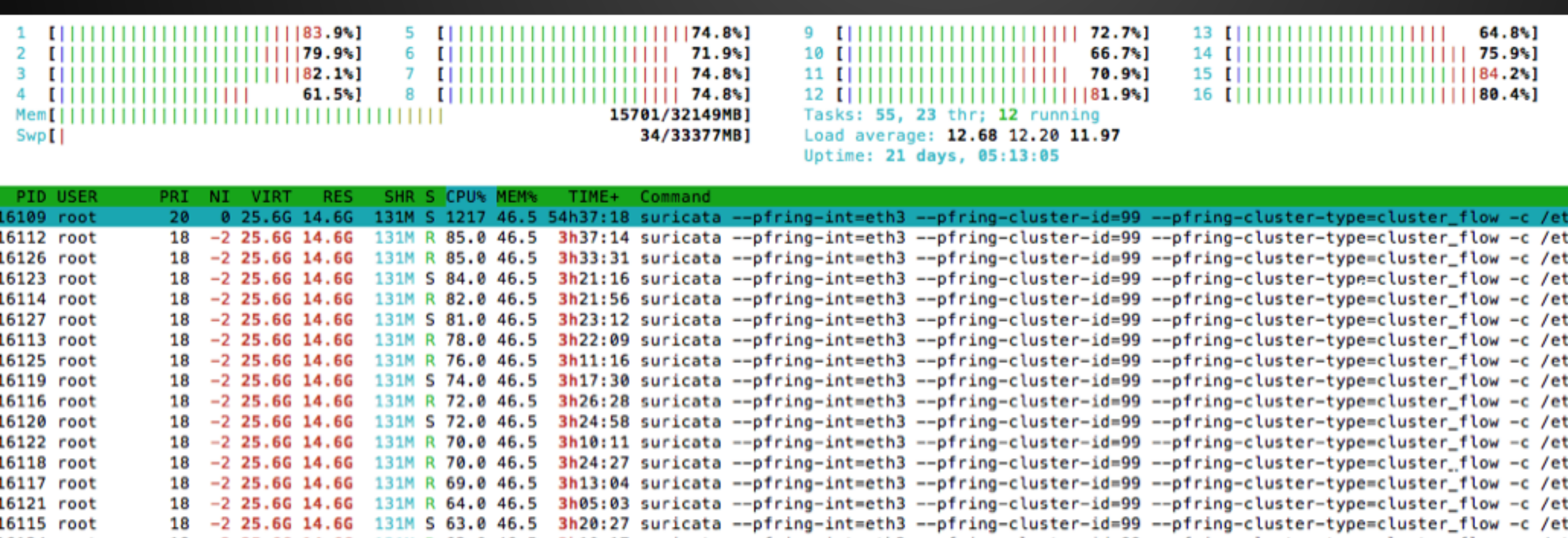
IDS Needs to Change!

- Signatures are still good
- Apply More Intelligence
- DB Analysis Tools are Easy

Think Larger Picture

What do we need?

- Engine that will use Modern Multi-core Hardware



What do we need?

- Full logging of the Network
  - DNS
  - HTTP
  - TLS Certs
  - Netflow
  - SMTP
  - SSH
  - IDS Alert Events

What do we need?

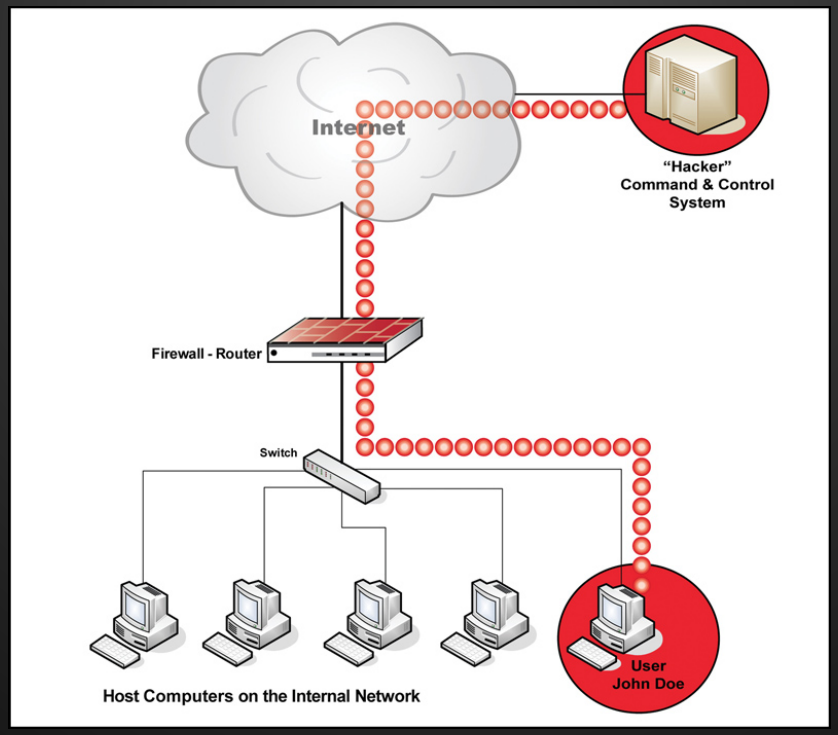
- Complex Analysis of a Stream
  - Deconstruct PDF, Java, OLE, etc

What do we need?

- File Extraction
  - payroll.pdf == exe?
  - AV Analysis
  - MD5 Matching

What do we need?

- Signature Matching
  - Malware Must Communicate



What do we need?

- File Extraction
- Full Logging
- Complex Analysis
- Multi-Threading
- Signature Matching
- Apply New Intelligence Streams
- Forensic History

What do we need?

This is where we were in 2009!!!

IDS is NOT Dead!

The Future is Now!

It's FREE!
and Open Source!

Suricata Today

- Apply tens of thousands of attack patterns to your traffic
- Detect protocol anomalies in HTTP and others
- Extract files from HTTP and SMTP
- Fast, scalable and stable
- IP reputation
- Lua scripting for advanced detection logic
- Many helpful additions for researchers
- Netflow output (JSON)

OISF
OPEN INFORMATION SECURITY FOUNDATION

Suricata Development Today

- Active development community
- Public roadmap
- Public bug trackers
- Git, github, wiki, mailing lists, IRC, etc

{"timestamp":"2014-11-18T12:40:42.744230","flow_id":2901423184,"event_type":"fileinfo","src_ip":"213.136.29.218","src_port":80,"dest_ip":"192.168.1.4","dest_port":53652,"proto":"TCP",
"http":{"url":"/ubuntu/pool/main/u/util-linux/bsdutils_2.20.1-5.1ubuntu20.3_i386.deb","hostname":"nl.archive.ubuntu.com","http_user_agent":"Debian APT-HTTP/1.3(1.0.1ubuntu2)"},"fileinfo":{"filename":"/ubuntu/pool/main/u/util-linux/bsdutils_2.20.1-5.1ubuntu20.3_i386.deb","magic":"Debian binary package (format2.0)","state":"CLOSED","md5":"6a1a4e3b53d4ff02cd3ded3cf0ce3a42","stored":false,"size":5475,"tx_id":2}}

{"timestamp":"2014-11-18T12:40:42.744230","flow_id":2901423184,"event_type":"fileinfo","src_ip":"213.136.29.218","src_port":80,"dest_ip":"192.168.1.4","dest_port":53652,"proto":"TCP",
"http":{"url":"/ubuntu/pool/main/u/util-linux/bsdutils_2.20.1-5.1ubuntu20.3_i386.deb","hostname":"nl.archive.ubuntu.com","http_user_agent":"Debian APT-HTTP/1.3(1.0.1ubuntu2)"},"fileinfo":{"filename":"/ubuntu/pool/main/u/util-linux/bsdutils_2.20.1-5.1ubuntu20.3_i386.deb","magic":"Debian binary package (format2.0)","state":"CLOSED","md5":"6a1a4e3b53d4ff02cd3ded3cf0ce3a42","stored":false,"size":5475,"tx_id":2}}

{"timestamp":"2014-11-18T12:40:42.744230","flow_id":
2901423184,"event_type":"fileinfo","src_ip":"
213.136.29.218","src_port":80,"dest_ip":"
192.168.1.4","dest_port":53652,"proto":"TCP",
"http":{"url":"/ubuntu/pool/main/u/util-linux/bsdutils_2.
20.1-5.1ubuntu20.3_i386.deb","hostname":"nl.archive.
ubuntu.com","http_user_agent":"Debian APT-HTTP/1.
3(1.0.1ubuntu2)"},"fileinfo":{"filename":"
/ubuntu/pool/main/u/util-linux/bsdutils_2.20.1-5.1
ubuntu20.3_i386.deb","magic":"Debian binary package
(format2.0)","state":"CLOSED","md5":"
6a1a4e3b53d4ff02cd3ded3cf0ce3a42","stored":false,"
size":5475,"tx_id":2}}

{"timestamp":"2014-11-18T12:40:42.744230","flow_id":2901423184,"event_type":"fileinfo","src_ip":"213.136.29.218","src_port":80,"dest_ip":"192.168.1.4","dest_port":53652,"proto":"TCP",
"http":{"url":"/ubuntu/pool/main/u/util-linux/bsdutils_2.20.1-5.1ubuntu20.3_i386.deb","hostname":"nl.archive.ubuntu.com","http_user_agent":"Debian APT-HTTP/1.3(1.0.1ubuntu2)"},"fileinfo":{"filename":"/ubuntu/pool/main/u/util-linux/bsdutils_2.20.1-5.1ubuntu20.3_i386.deb","magic":"Debian binary package (format2.0)","state":"CLOSED","md5":"6a1a4e3b53d4ff02cd3ded3cf0ce3a42","stored":false,"size":5475,"tx_id":2}}

{"timestamp":"2014-11-18T12:40:42.744230","flow_id":
2901423184,"event_type":"fileinfo","src_ip":"
213.136.29.218","src_port":80,"dest_ip":"
192.168.1.4","dest_port":53652,"proto":"TCP",
"http":{"url":"/ubuntu/pool/main/u/util-linux/bsdutils_2.
20.1-5.1ubuntu20.3_i386.deb","hostname":"nl.archive.
ubuntu.com","http_user_agent":"Debian APT-HTTP/1.
3(1.0.1ubuntu2)"},"fileinfo":{"filename":"
/ubuntu/pool/main/u/util-linux/bsdutils_2.20.1-5.1
ubuntu20.3_i386.deb","magic":"Debian binary package
(format2.0)","state":"CLOSED","md5":"
6a1a4e3b53d4ff02cd3ded3cf0ce3a42","stored":false,"
size":5475,"tx_id":2}}

{"timestamp":"2014-11-21T08:11:45.222089","flow_id":2896612328,"event_type":"tls","src_ip":"23.206.115.50","src_port":443,"dest_ip":"10.8.0.6","dest_port":47063,"proto":"TCP",
"tls":{"subject":"serialNumber=5189573, unknown=US, unknown=Delaware, unknown=Private Organization, C=US, unknown=94107, ST=California, L=San Francisco, unknown=855 FOLSOM ST APT 535, O=Remember The Milk Inc., OU=Comodo EV SAN SSL,CN=www.rememberthemilk.com","issuerdn":"C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO Extended Validation Secure Server CA 2", "fingerprint":"0b:1e:68:8c:ec:9f:7a:9c:70:4f:58:41:fb:c6:53:ba:ba:e1:6c:af","version":"TLS 1.2"}}

{"timestamp":"2014-11-21T08:32:22.001162","
flow_id":2904615464,"event_type":"netflow","
src_ip":"23.206.107.75","src_port":443,"
dest_ip":"10.8.0.6","dest_port":52556,"proto":"
TCP",
"netflow":{"app_proto":"tls","pkts":73,"bytes":
66135,"start":"2014-11-21T08:28:08.789426","
end":"2014-11-21T08:30:19.242083","age":
131},"tcp":{"tcp_flags":"1b","syn":true,"fin":true,"
psh":true,"ack":true}}

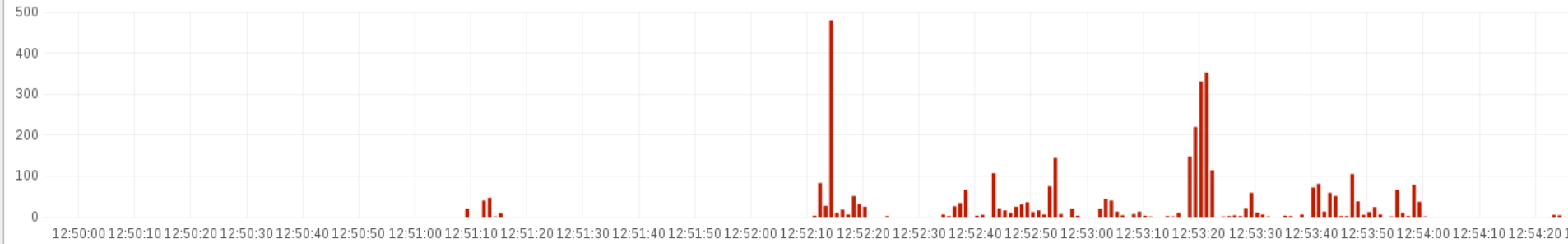
ALERTS

5 minutes ag

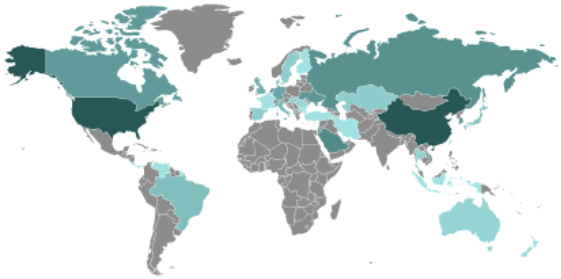
QUERY FILTERING

EVENTS OVER TIME

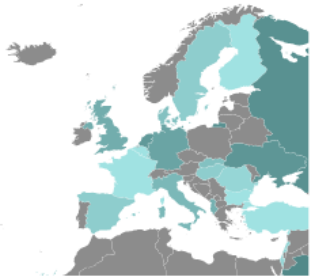
View | Zoom Out | Alerts (3643) count per **1s** | (**3643** hits)



WORLD



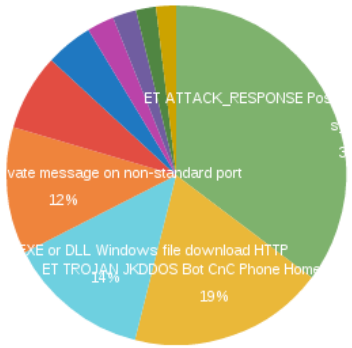
EUROPE



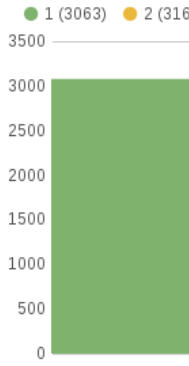
ALERT CATEGORIES

Term	Count	Action
A Network Trojan was detected	1982	
Successful Administrator Privilege Gain	722	
Potential Corporate Privacy Violation	347	
Misc activity	247	
Potentially Bad Traffic	222	
Misc Attack	73	
Detection of a non-standard protocol or event	13	
Generic Protocol Command Decode	9	
Attempted Information Leak	8	

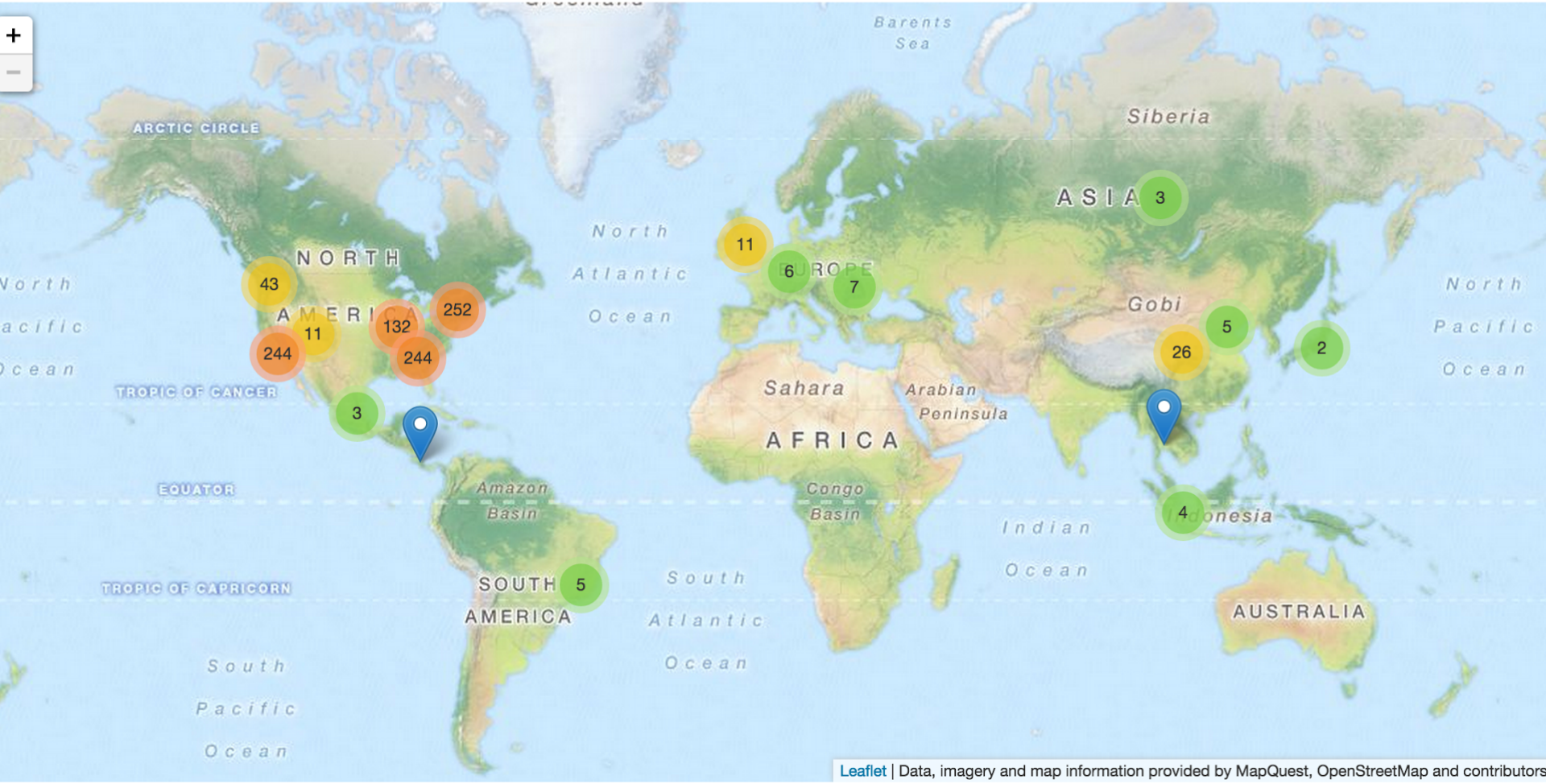
ALERT SIGNATURES



ALERTS SEVERITY

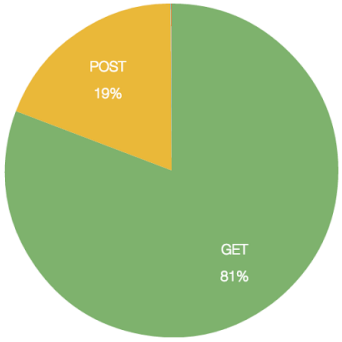


EOIP LOCALIZATION



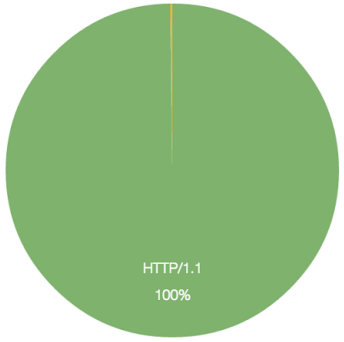
HTTP METHOD

GET (59689) POST (14123) OPTIONS (45) HEAD (23) PUT (6)



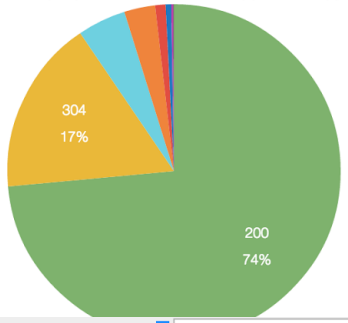
HTTP PROTOCOL

HTTP/1.1 (73749) HTTP/1.0 (138)



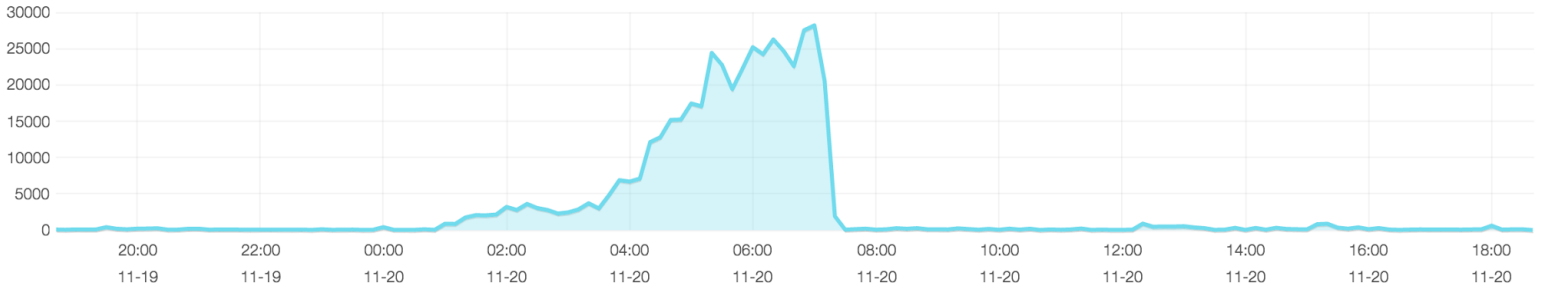
HTTP STATUS CODE

200 (47025) 304 (10844) 302 (3002) 301 (1923) 204 (645)
404 (343) 403 (133) 206 (23) 500 (7) 503 (6)



EVENTS OVER TIME

View | Zoom Out | DNS transactions (462869) count per **10m** | (**462869** hits)

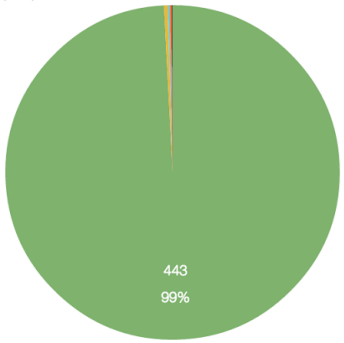


HTTP HOSTNAME

Term	Count	Action
10.55.59.23	31559	
10.55.56.20	7226	
10.55.56.218	4829	
10.55.56.57	3786	
10.55.58.15	3310	
etpro1.internal.emergingthreats.net	3220	
newdell01	3164	
10.55.56.24	3114	

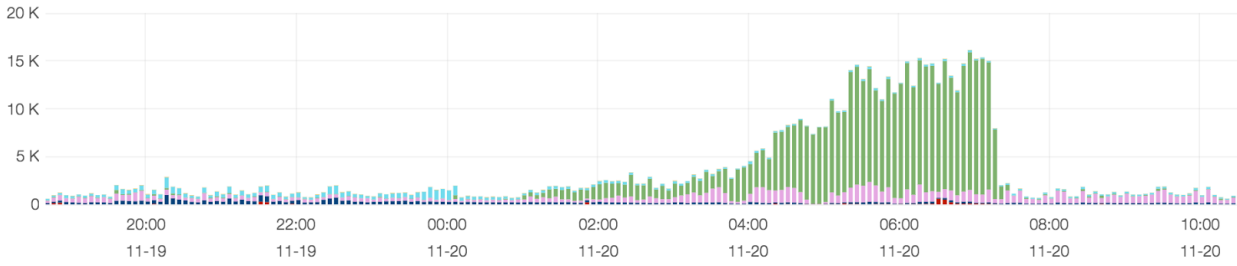
TLS TCP PORTS

443 (193469) 5989 (701) 8005 (357) 5223 (268) 993 (133)
465 (9) 5228 (2) 62062 (1) 62050 (1) 61875 (1)
Other values (131)



EVENTS OVER TIME

View | Zoom Out | Alerts (5372) Files (61914) TLS (195017) DNS (462859) HTTP (73879) SSH (5907) count per **5m** | (**804948** hits)



WORLD

EUROPE

Suricata's Development RoadMap

- ICS/SCADA
- SSL/TLS (no decryption)
- IP, DNS, URL Reputation
- Lowering bar for entry, both for users and developers
- Performance
- Protocols

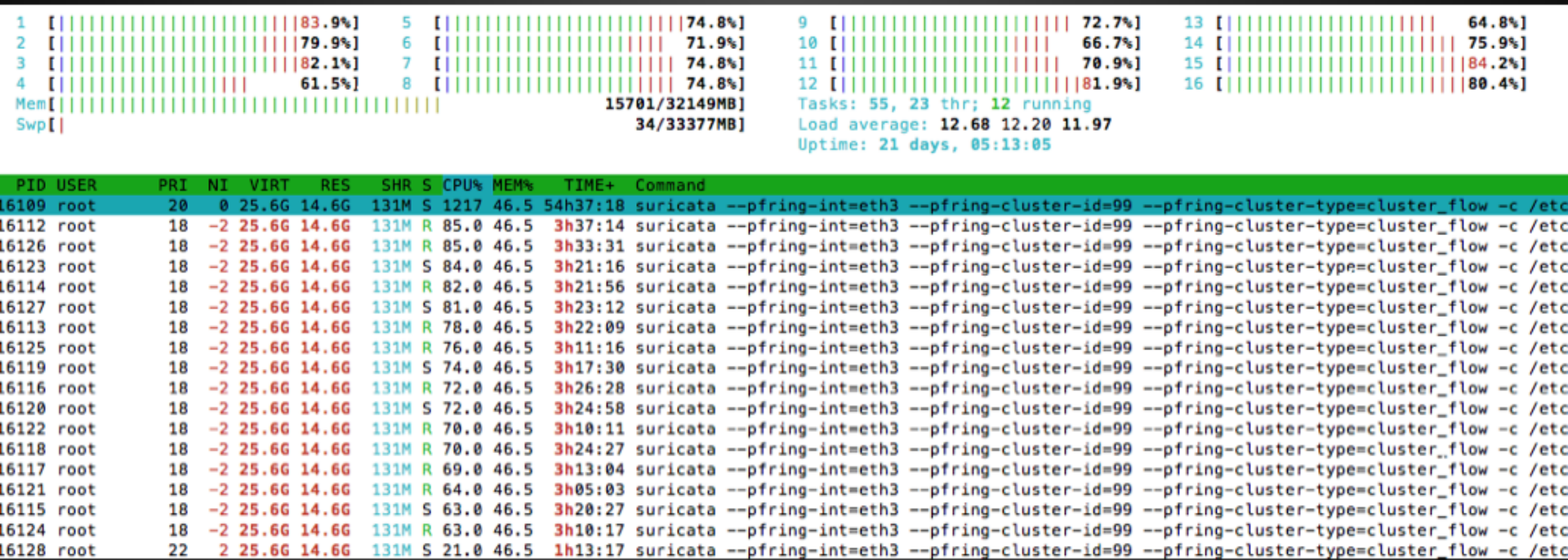

TAKE THAT
YOU PRAIRIE
DOGS!

What do we need?

- File Extraction
- Full Logging
- Complex Analysis
- Performance and scalability
- Signature Matching
- Apply New Intelligence Streams
- Forensic History

Scale

- 10gig on Standard Hardware



Our Mission

To foster and lead a community dedicated to ensuring open source technologies THRIVE!

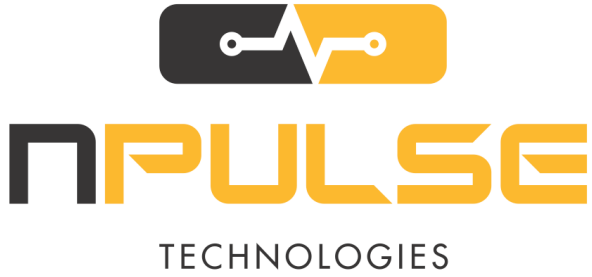
OISF
OPEN INFORMATION SECURITY FOUNDATION

Our Funding

Consortium Members,
Community Contributors, Grant Funding

Our Community

Industry Leaders, Individuals, Governments


nPULSE
TECHNOLOGIES


TILERA


CYPHORT
Advanced Malware Defense


LOCKHEED MARTIN


EMERGING
THREATS


FireEye™


endace


ALTERA®
MEASURABLE ADVANTAGE™


napatech


Homeland Open Security
Technology Program


EMULEX


TILERA


AlienVault


pf
Sense


SecurityOnion


FireEye


STAMUS
NETWORKS


napatech


SW
simplewall


endace


nPULSE
TECHNOLOGIES


IPFire

The IDS of the Future

Join us in 2015...

January: 2-Day Suri Training, San Jose, CA

February: 2-Day Suri Training, Washington DC

Spring: 2-Day Suri Training, EU (TBD)

Fall: 1-Week Suri Developer Training, Barcelona and 3-Day OISF Community Conference

For More Information...

www.openinfosecfoundation.org

www.suricata-ids.org

Follow Us on Twitter...

@OISFoundation

@Suricata_IDS