Shmoocon (or not)
2014-1

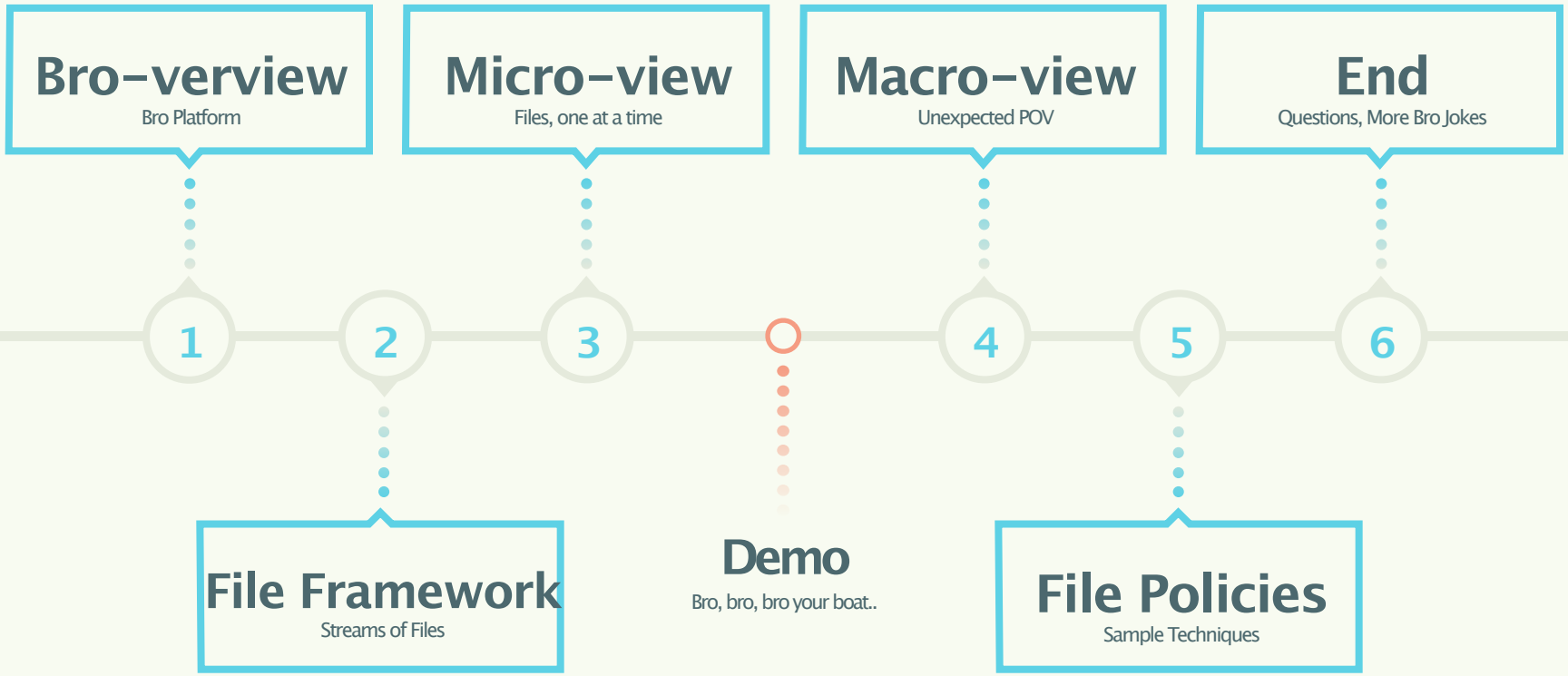
Liam Randall
Critical Stack LLC

Critical Stack

"The Bro files framework is a novel and powerful way to interact with data on your network."

Bro Platform

Agenda – Briefing Overview



Go Figure: This guys loves Bro.

Liam Randall

CEO, Critical Stack LLC
BS in Computer Science, Xavier University

Current Projects
- Incident Response
- Teach Bro Classes
- Recon Detection Framework

Upcoming Conferences

Feb 17–20, 2014– **MAAWG**
- Bro Classes, Speaking

?, 2014– **44Con**
- Bro Classes, Speaking

May, 2014– **Florida Somewhere**
- Bro Classes, Speaking

Link

http://www.Broala.com
http://www.bro.org

Critical Stack

BRO NETWORK SECURITY MONITOR

NSF

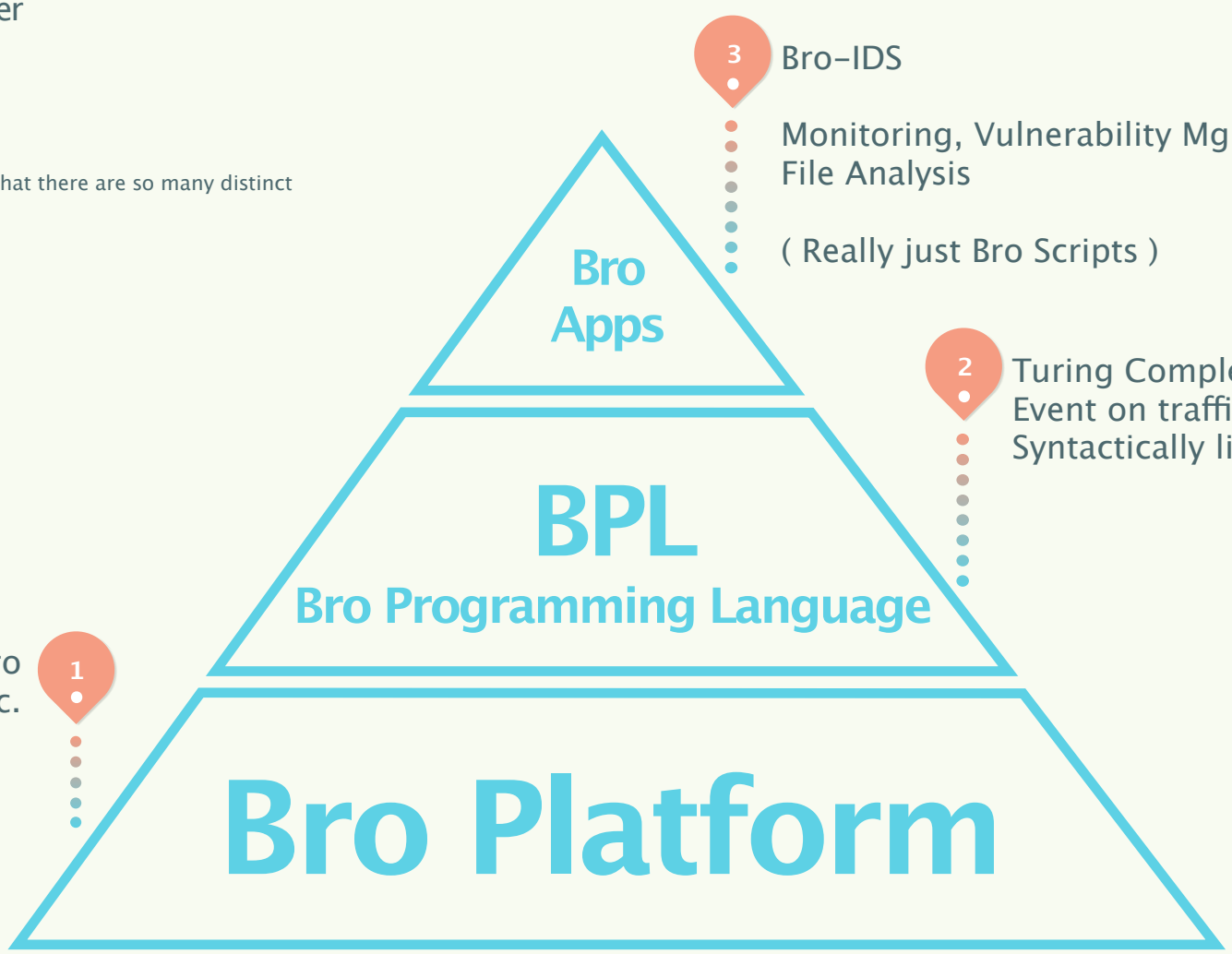
Bro Platform

Brief introduction to the Model.

Bro – is short for Big Brother

Bro is three things ...

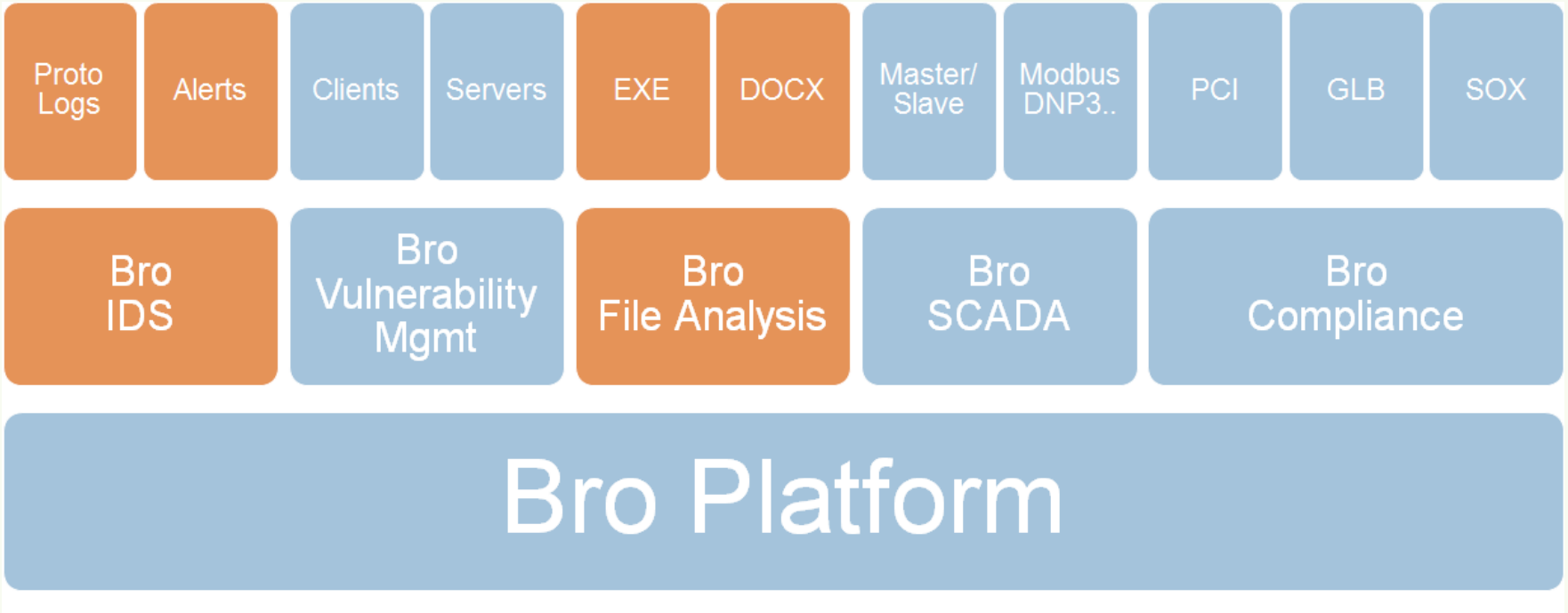
The hardest part about Bro is that there are so many distinct use cases for the Bro Platform



Critical Stack

Bro has use cases in…

Security, Monitoring, Reliability, Discovery, Compliance



Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

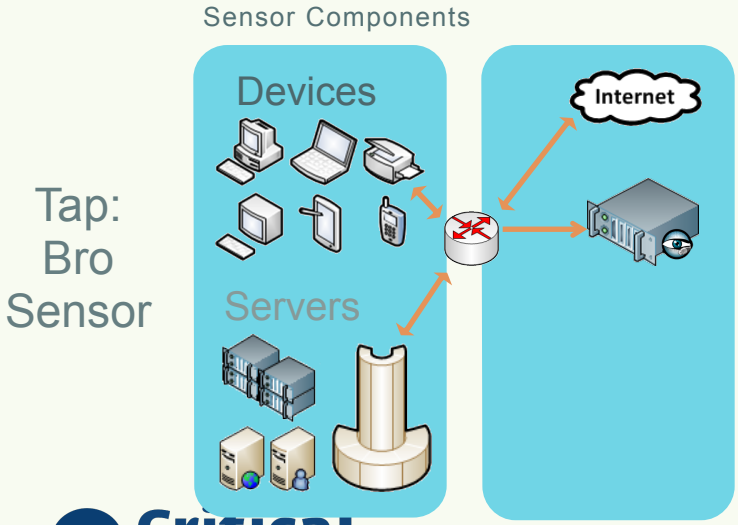
Alerts

Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

Sensor Components



Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

Ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service
Time	string	addr	port	addr	port	enum	string
1355284742	AZIHpPlejvi	192.168.4.138	68	192.168.4.1	67	udp	-
1326727285	K4xJ9AKH56g	192.168.4.148	55748	196.216.2.3	33117	tcp	ftp-data
1326727283	Jd11tlLtlE	192.168.4.148	58838	196.216.2.3	21	tcp	ftp
1326727287	bVQHYKEz2b4	192.168.4.148	54003	196.216.2.3	31093	tcp	ftp-data
1326727286	5Dki82HwJDk	192.168.4.148	58840	196.216.2.3	21	tcp	ftp
1355284761	YSJ6DDKEzGk	70.199.104.181	8391	192.168.4.20	443	tcp	ssl
1355284791	BqLVVfmVO6d	70.199.104.181	8393	192.168.4.20	443	tcp	ssl
1355284761	ya3SvH6ZxX4	70.199.104.181	8408	192.168.4.20	443	tcp	ssl
1355284812	sxrPWDvcGQ2	192.168.4.20	48433	67.228.181.219	80	tcp	http
1355284903	vlvQgRiHE54	192.168.4.20	14655	192.168.4.1	53	udp	dns
1355284792	gn5FV4jeOJ4	70.199.104.181	8387	192.168.4.20	443	tcp	ssl
1355285010	uEb3j6nYBS7	59.93.52.206	61027	192.168.4.20	25	tcp	smtp
1326962278	SE2LJ7PLwIg	189.77.105.126	3	192.168.4.20	3	icmp	-
1326962279	T6rMQFaMCie	95.165.30.73	3	192.168.4.20	3	icmp	-
1329400936	qtNmAmHhDM4	192.168.4.20	14419	65.23.158.132	6668	tcp	irc
1329400884	cOctAcZusv2	192.168.4.20	32239	89.16.176.16	6666	tcp	irc

Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

#fields ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	note
#types	time	string	addr	port	addr	port	enum
1359673187	TLDtWBOrstk	192.168.0.120	61537	50.76.24.57	8443	tcp	SSL::Invalid_Server_Cert
1359673187	L4bDTmPqvs2	192.168.1.8	49540	174.143.119.91	6697	tcp	SSL::Invalid_Server_Cert
1359673187	JAvYksFW1Qb	207.188.131.2	5373	160.109.68.199	8081	tcp	SSL::Invalid_Server_Cert
1359673188	-	192.168.0.57	62220	216.234.192.231 80		tcp	Rogue_Access_Point
1359673188	5OYpDdtlnfd	192.168.0.147	45009	93.174.170.9	443	tcp	SSL::Invalid_Server_Cert
1359673188	-	192.168.0.147	36511	74.125.225.194	80	tcp	Rogue_Access_Point
1359673188	-	-	-	-	-	-	Software::Vulnerable_Version
1359673188	93ClvevOuxk	192.168.0.147	51897	98.136.223.39	8996	tcp	SSL::Invalid_Server_Cert
1359673209	YpCOvC9p4Ef	208.89.42.50	48620	207.188.131.2	22	tcp	SSH::Login
1359673210	SaKFGzmdXLI	207.188.131.2	11175	23.5.112.107	443	tcp	SSL::Invalid_Server_Cert
1359673214	XLE8fYI5Tvg	207.188.131.2	11677	208.66.139.142	2145	tcp	SSL::Invalid_Server_Cert
1359673214	-	192.168.1.120	60141	74.125.225.195	80	tcp	Rogue_Access_Point
1359673218	NyPHd3qjIKe	208.89.42.50	43891	207.188.131.2	22	tcp	SSH::Login
1359673223	0skn2N4oYbj	192.168.1.116	49249	15.201.49.137	80	tcp	HTTP::MD5
1359673224	Q83ji8AFOO1	192.168.1.116	49250	15.192.45.26	80	tcp	HTTP::MD5
1359673229	WU57HOSwkEj	208.89.42.50	62165	207.188.131.2	22	tcp	SSH::Login

Bro Functions – Three things Bro does

Protocol Logs

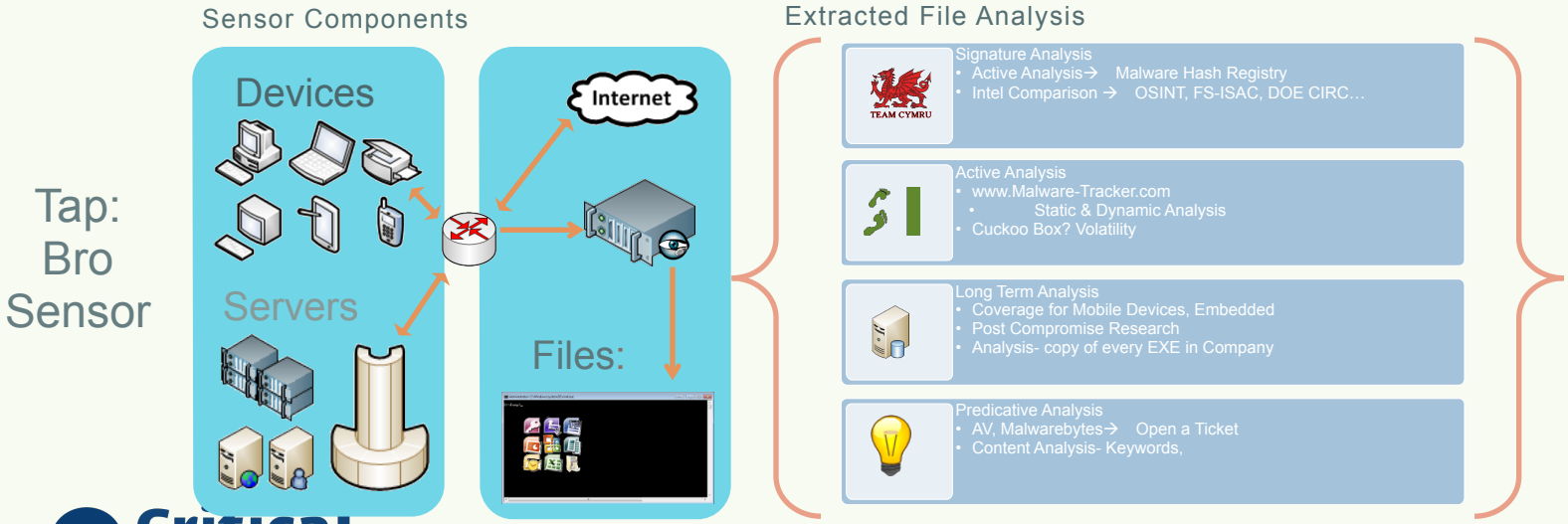
Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.



Bro Platform

Capabilities, use cases, & direction.

Legacy File Handling

- In 2.1 and prior, "file" handling...
  - performance impact
  - is not extensible

Protocol	File Handling
HTTP	redef HTTP::extract_file_types = /application\/.*/;
SMTP	redef SMTP::extract_file_types = /application\/.*/;
FTP	redef FTP::extract_file_types = /application\/.*/;
IRC	redef IRC::extract_file_types = /application\/.*/;

Inspiration

- Charles Smutz and his Ruminate-IDS project.
  - File reassembly.
  - Passing files to other tools and parsers.

Realizations

- A "file" is a single flow bytestream
  (hint: a connection is bidirectional so it's a dual flow bytestream)
  - Bro can have file analyzers that work incrementally like our protocol analyzers.
  - How many file types would you like to be able to parse?

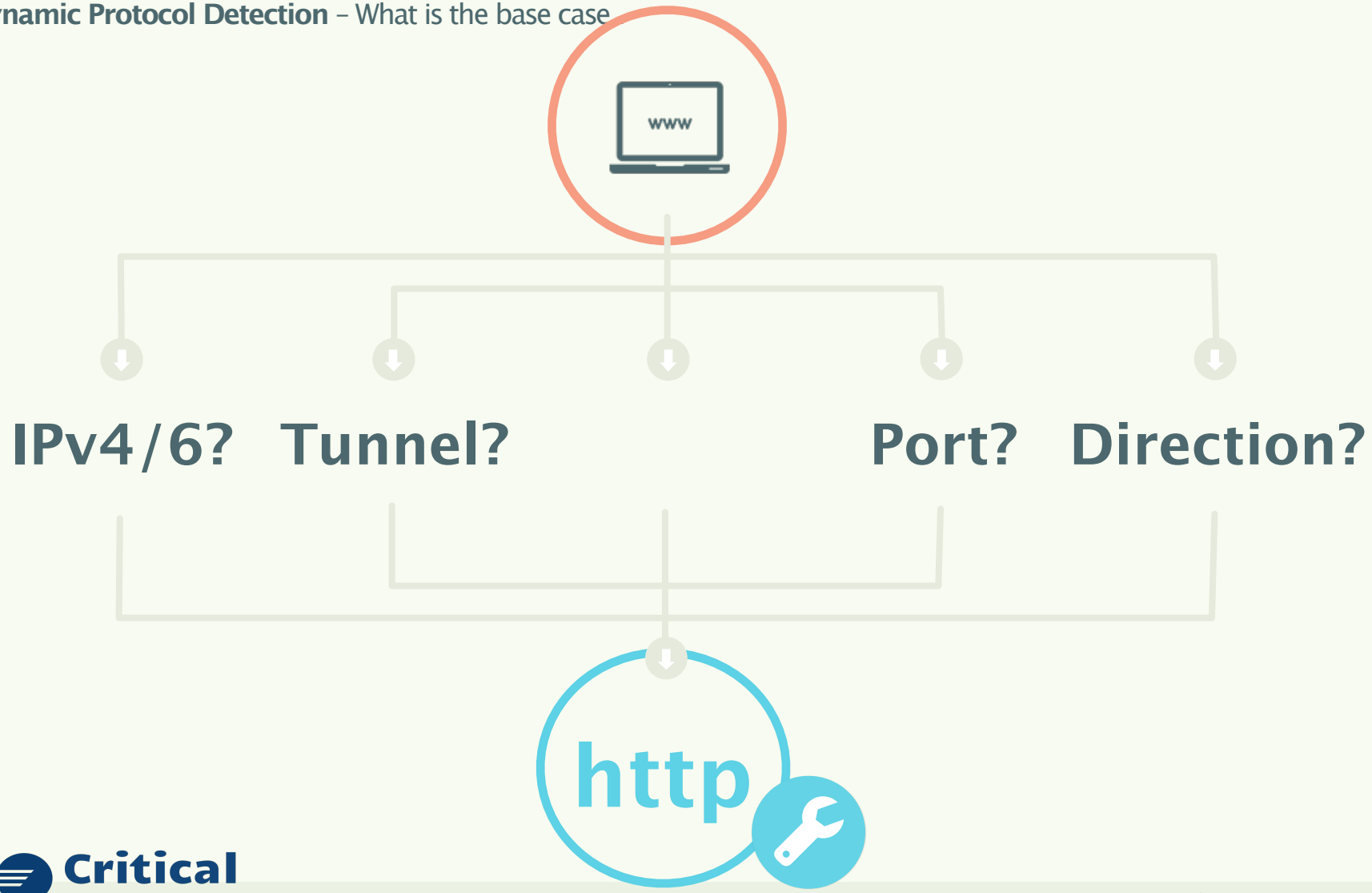
Files are source agnostic

- Files out of files.
- Files out of any unencrypted file protocol.
- Input framework.

Implementation

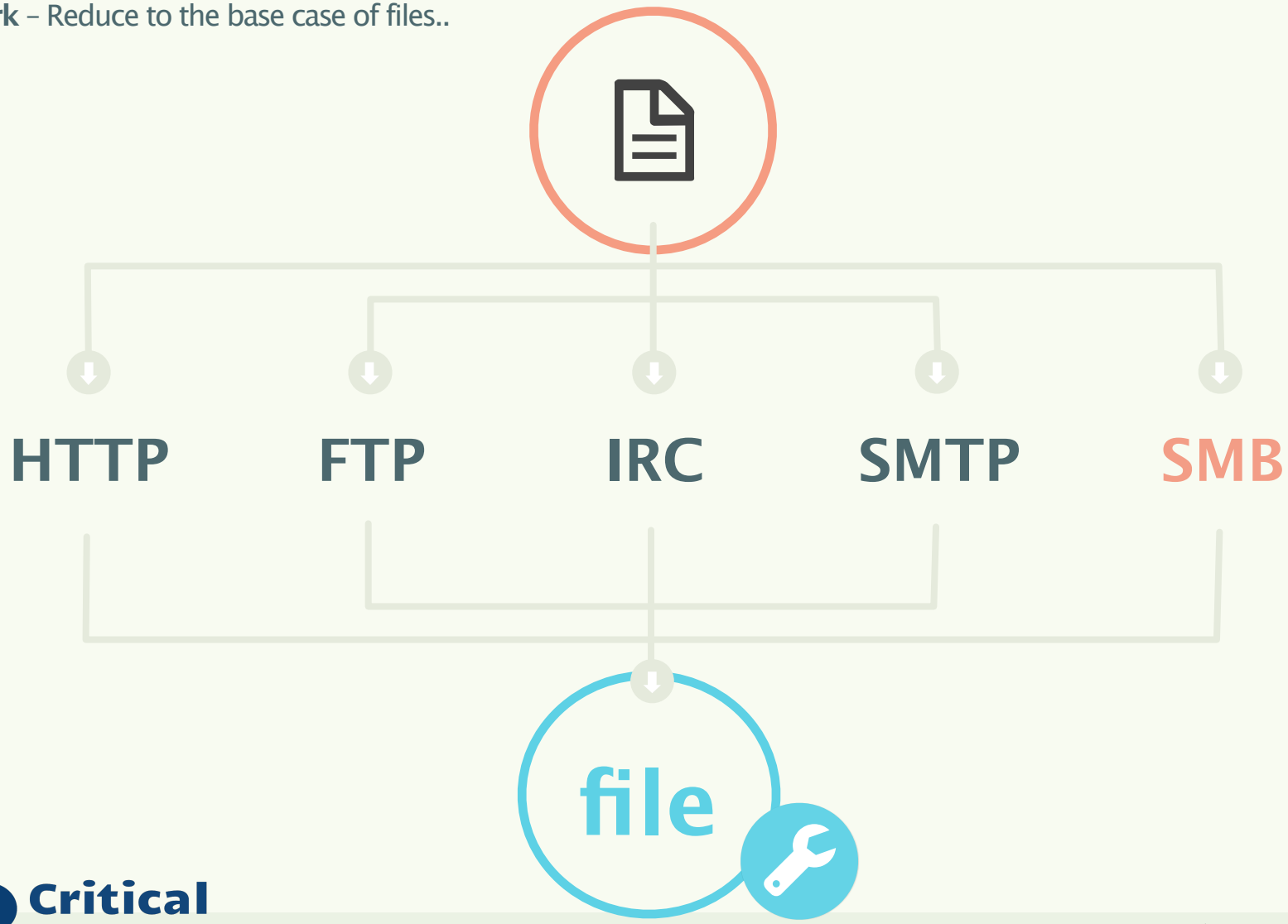
- Keep file data **out** of script land.
- No reassembly yet, but design decisions were made to support it in a future release.
- File manager is a completely new internal component of Bro that accepts file data from anywhere it can be acquired

Compare Dynamic Protocol Detection – What is the base case



```
event http_header(c: connection, is_orig: bool,
                  name: string, value: string)
{

   if ( name == "CONTENT-TYPE" && value == "text/
   html; charset=win-1251" )




}
```

Files Framework – Reduce to the base case of files..



file_new – Reduce to the base case of files..

```
event file_new(f: fa_file)
{
  if ( f?$mime_type && f$mime_type == "application/x-dosexec")
  {

   Files::add_analyzer(f, Files::ANALYZER_EXTRACT);


  }

}
```

Forensic Logging - conn.log

ts	1232039481.41058
uid	**wd5Gv4mDKY**
id	10.0.0.245 1066 78.109.18.210 80
proto	tcp
service	http
duration	1.492474
orig_bytes	66
resp_bytes	49337
conn_state	RSTO
missed_bytes	0
history	ShADadfR

Forensic Logging - http.log

ts	1232039481.56861
uid	**wd5Gv4mDKY**
id	10.0.0.245 1066 78.109.18.210 80
trans_depth	1
method	GET
host	78.109.18.210
uri	/lprx.php
referrer	-
user_agent	-
request_body_len	0
response_body_len	49152
resp_fuids	hVkwqld1J1h
resp_mime_types	application/x-dosexec

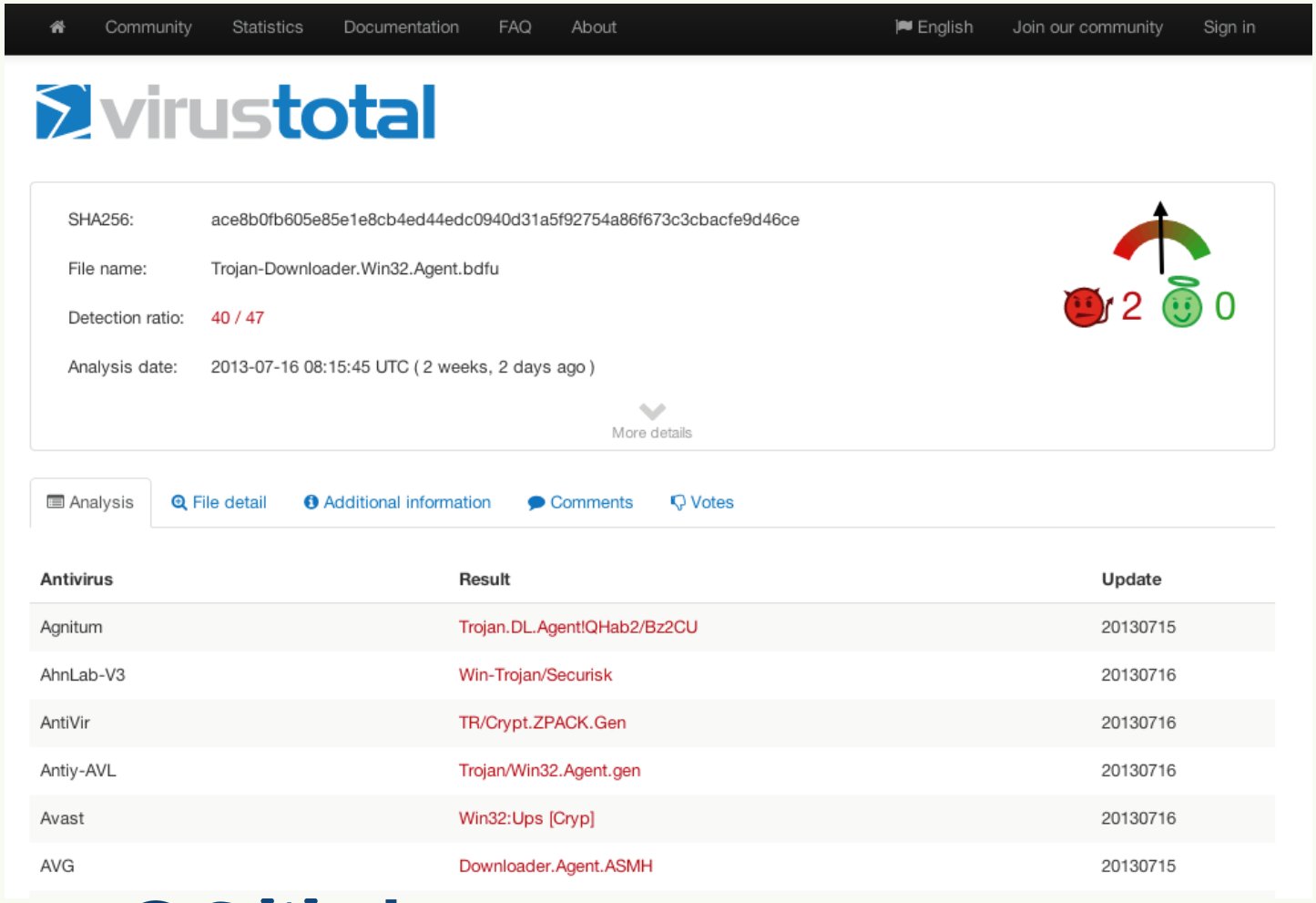
Forensic Logging - files.log

ts	1232039481.72727
fuid	**hVkwqId1J1h**
tx_hosts	78.109.18.210
rx_hosts	10.0.0.245
conn_uids	**wd5Gv4mDKY** *—> File attached to a flow*
source	HTTP
depth	0
analyzers	SHA1, MD5, PE
mime_type	application/x-dosexec
duration	1.151308
is_orig	F
seen_bytes	49152
total_bytes	49152
md5	1d016184387937e2f81da268dace5758
sha1	9fba10c34168496486cd4205cb7c9cda41abf8b9
extracted	-

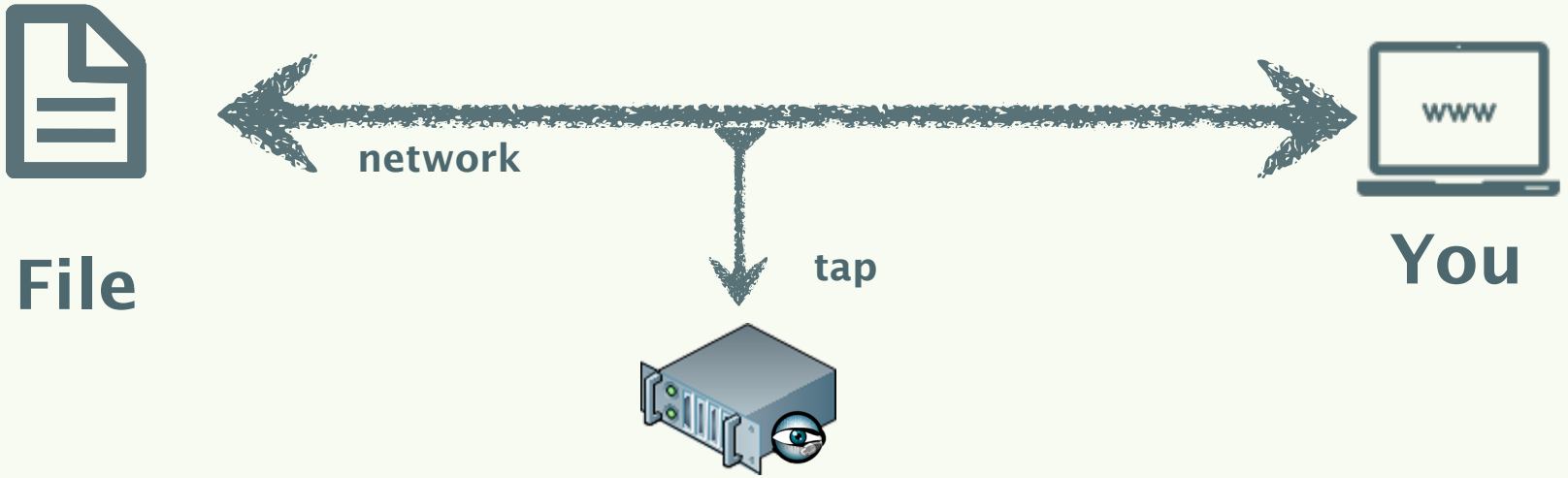
Forensic Logging - notice.log

ts	1232039482.87858
uid	**wd5Gv4mDKY**
id	10.0.0.245 1066 78.109.18.210 80
fuid	**hVkwqId1J1h**
file_mime_type	application/x-dosexec
file_desc	http://78.109.18.210/lprx.php
note	TeamCymruMalwareHashRegistry::Match
msg	Malware Hash Registry Detection rate: 11% Last seen: 2009-01-12 14:01:04
sub	https://www.virustotal.com/en/file/9fba10c34168496486cd4205cb7c9cda41abf8b9/analysis/

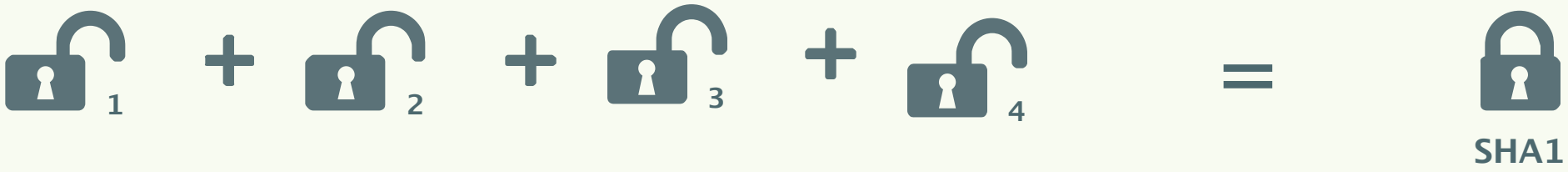
Integrations – Pivoting to external resources, databases



Incremental Calculation – Blockwise hashing algorithms?



SHA1 Calculation



Hash: MD5, SHA1, SHA256

File Extraction

Data

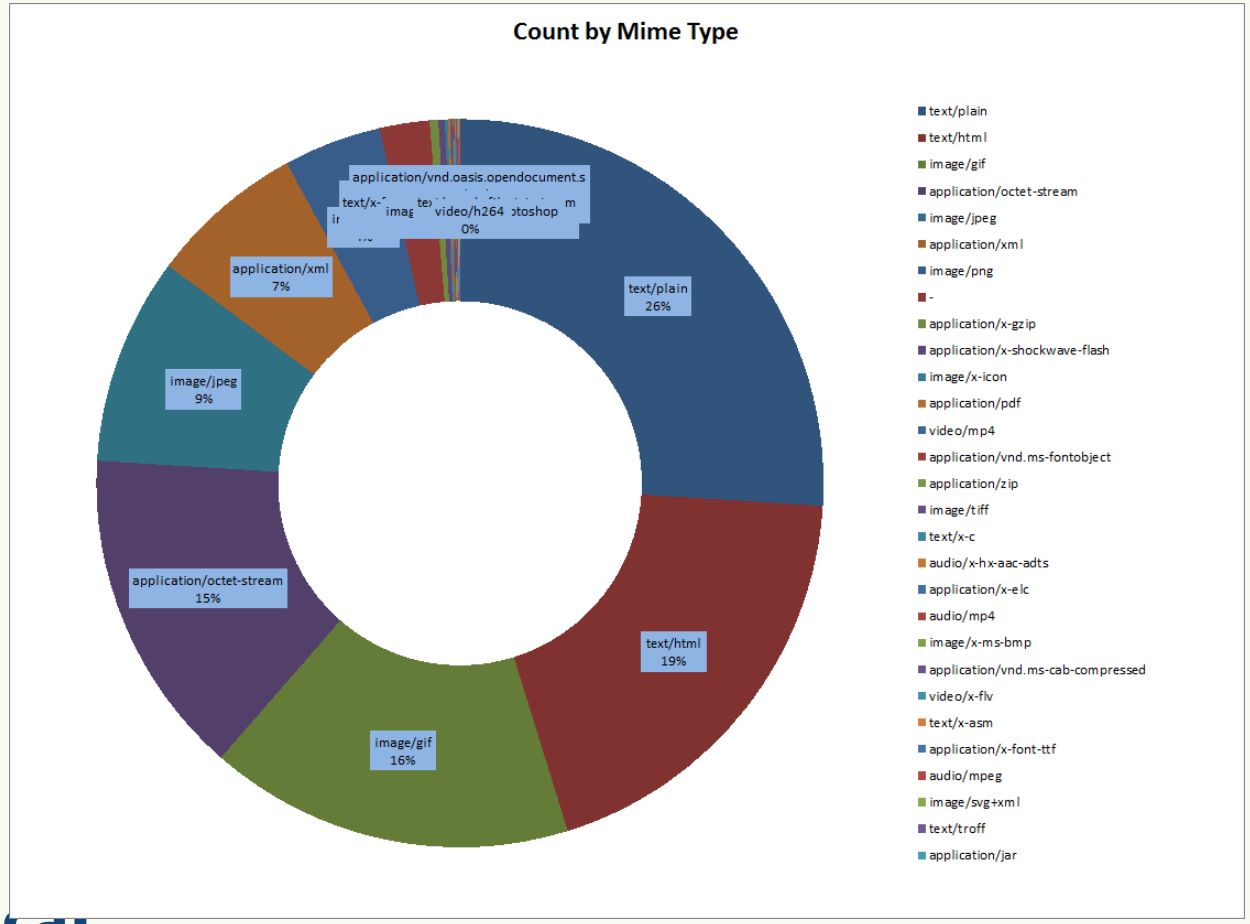
Entropy Analyzer (Git)

PE Header Analyzer (Git)

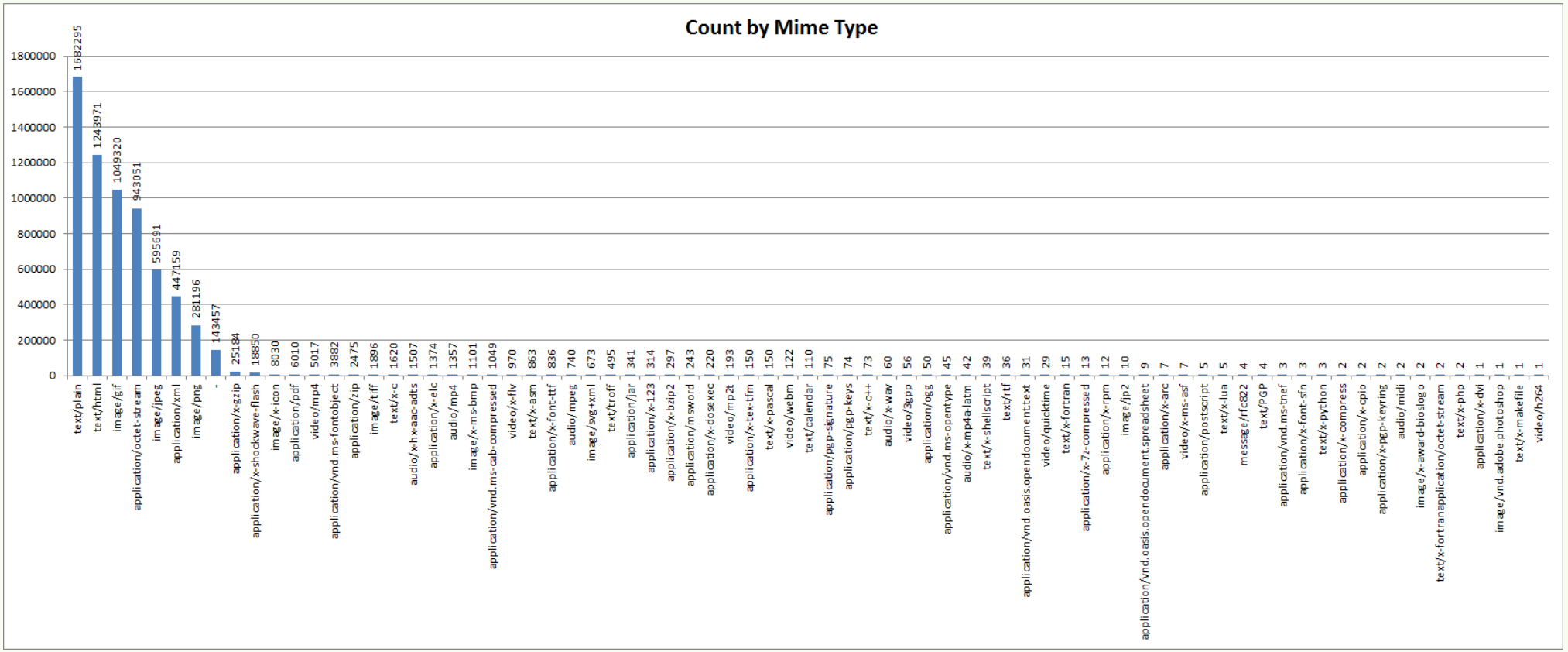
Files, one at a time

Capabilities, use cases, & direction.

zcat files.* | bro-cut mime_type | sort | uniq -c | sort -n



zcat files.* | bro-cut mime_type | sort | uniq -c | sort -n



Files by CC – Mime type by country code

```
liamrandall@ids001:/nsm/bro/logs/2014-01-18$ zcat files.13\:00\:00-14\:00\:00.log.gz | bro-cut mime_type tx_cc
rx_cc | awk '{split($0,a,"\t"); if ((a[2]=="-" && a[3]!="-") || (a[2]!="-" && a[3]=="-")) print $0}' | sort |
uniq -c | sort -n
```

Count	mime_type	Source_CC	Dest_CC
1	application/octet-stream	-	CN
1	application/octet-stream	-	CZ
1	text/plain	-	DE
1	text/plain	-	TW
1	text/plain	UA	-
4	text/plain	-	FR
5	text/plain	-	GB
7	application/xml	-	US
11	application/xml	-	AU
11	text/plain	-	CA
35	application/octet-stream	-	GB
160	text/plain	US	-
862	application/octet-stream	-	US
3609	text/plain	-	US

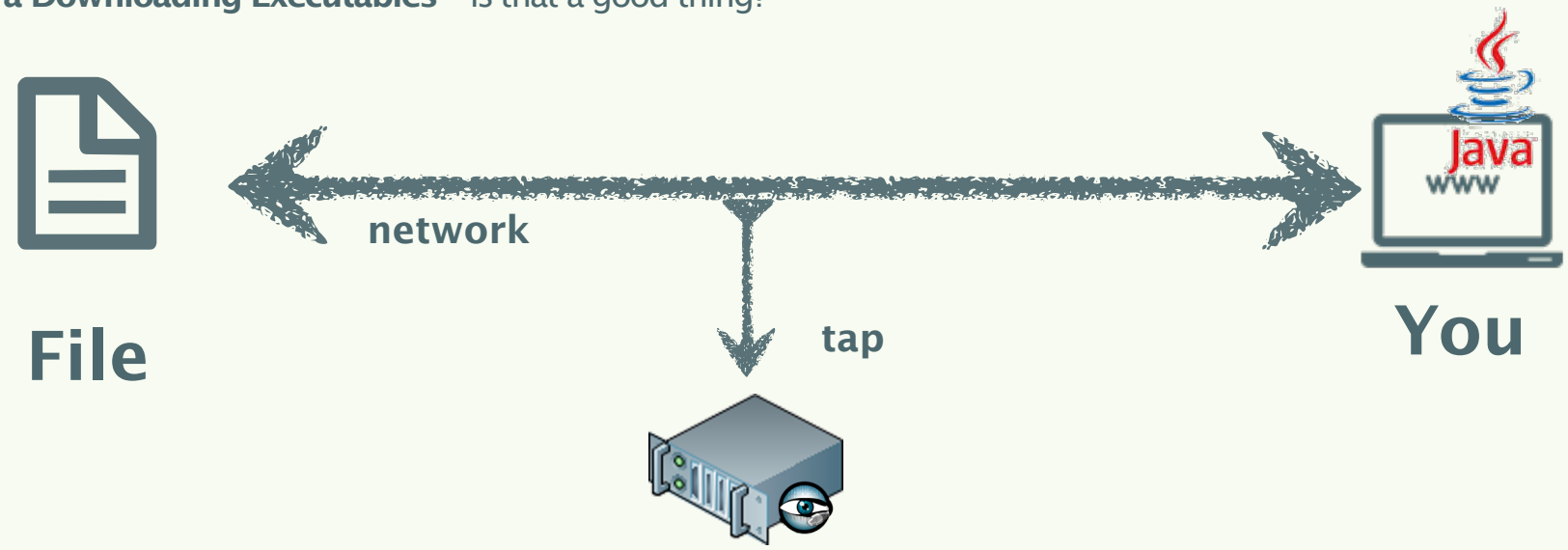
Files by CC – Mime type by country code

```
zgrep FZu7yi2ixt5mKFaUKa  http_eth1.13\:00\:00-14\:00\:00.log.gz

timestamp:       1390050048.383389
UID:             CadAFz45gCqmjo5Z1c
Source           10.97.33.36
Dest:            202.133.227.43
Port:            80
Trans_Depth:     1
Method:          POST
Host:            ns.dipmap.com
URI:             /updateip.aspx
Referrer:        -
User Agent:      Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)

Orig_File:       FZu7yi2ixt5mKFaUKa
Orig_type:       text/plain
Resp_File:       FZmaMR3xjn8J7oq7a4
Resp_mime:       text/html
```

Files, one at a time

Capabilities, use cases, & direction.

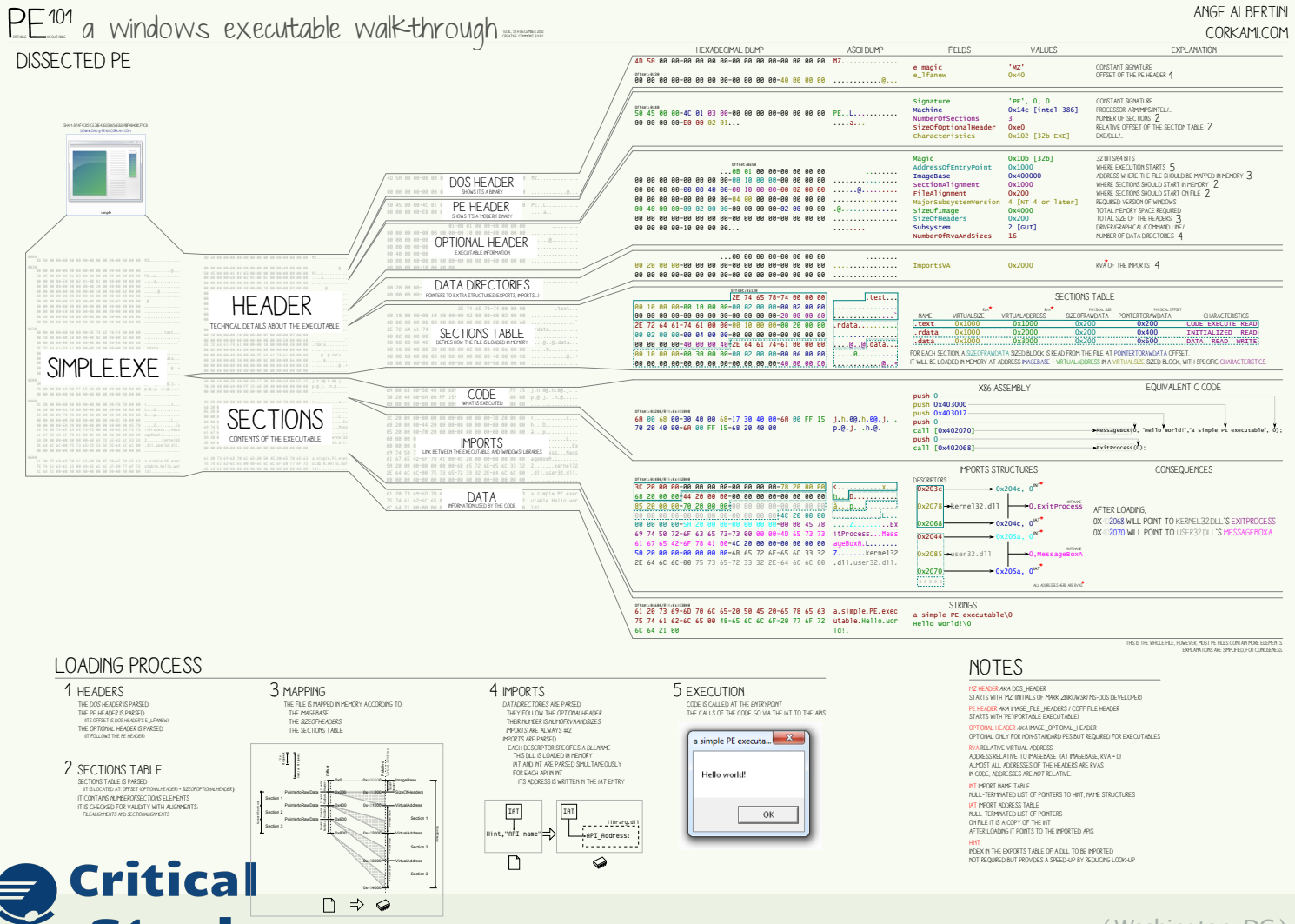
Java Downloading Executables – is that a good thing?



http.log

```
46.21.155.86  Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_26  application/x-dosexec  abccup.net   /?d4a7a142560899e60103f46d24e78e0c
46.21.155.86  Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_26  application/x-dosexec  abccup.net   /?8dd2a80721cae71c5964639bd7c8c55b
91.230.143.143  Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_26  application/x-dosexec  1h8.ru  /a.exe?s=0nir&
```

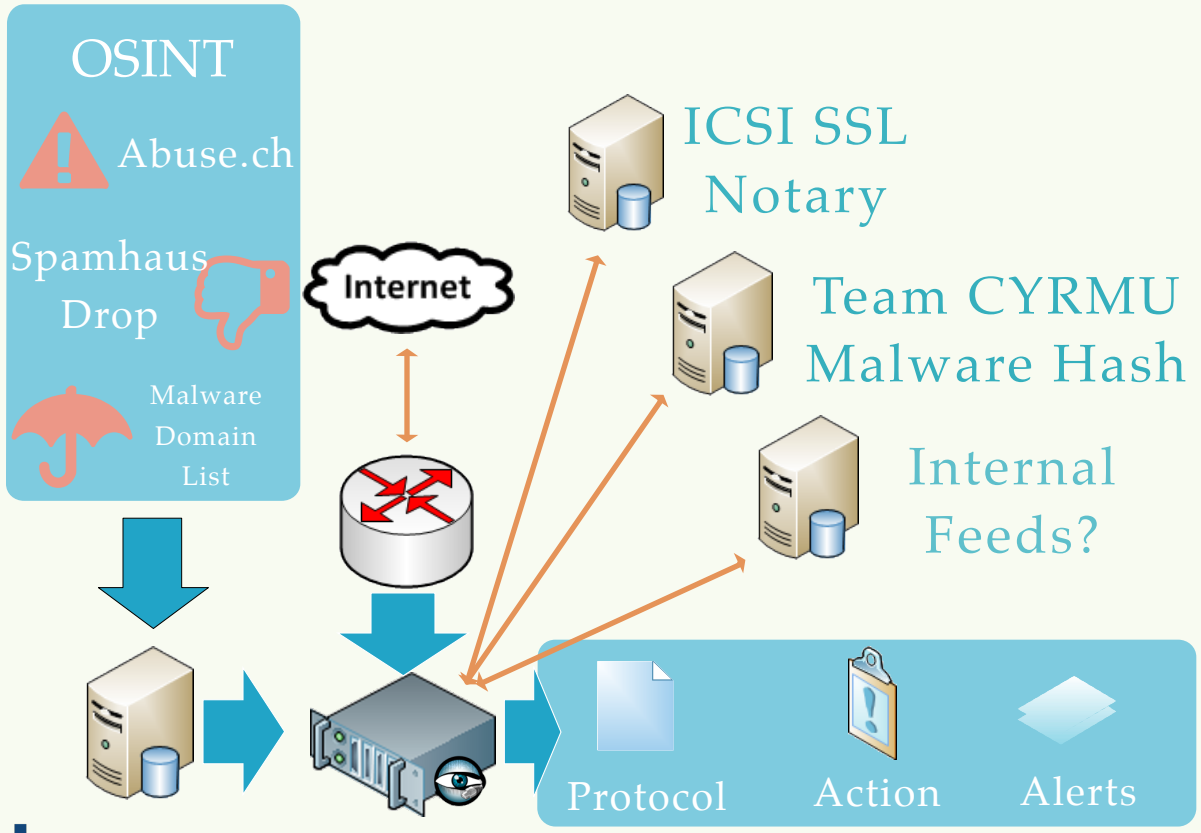
PE Header – Draft Analyzer available in Git



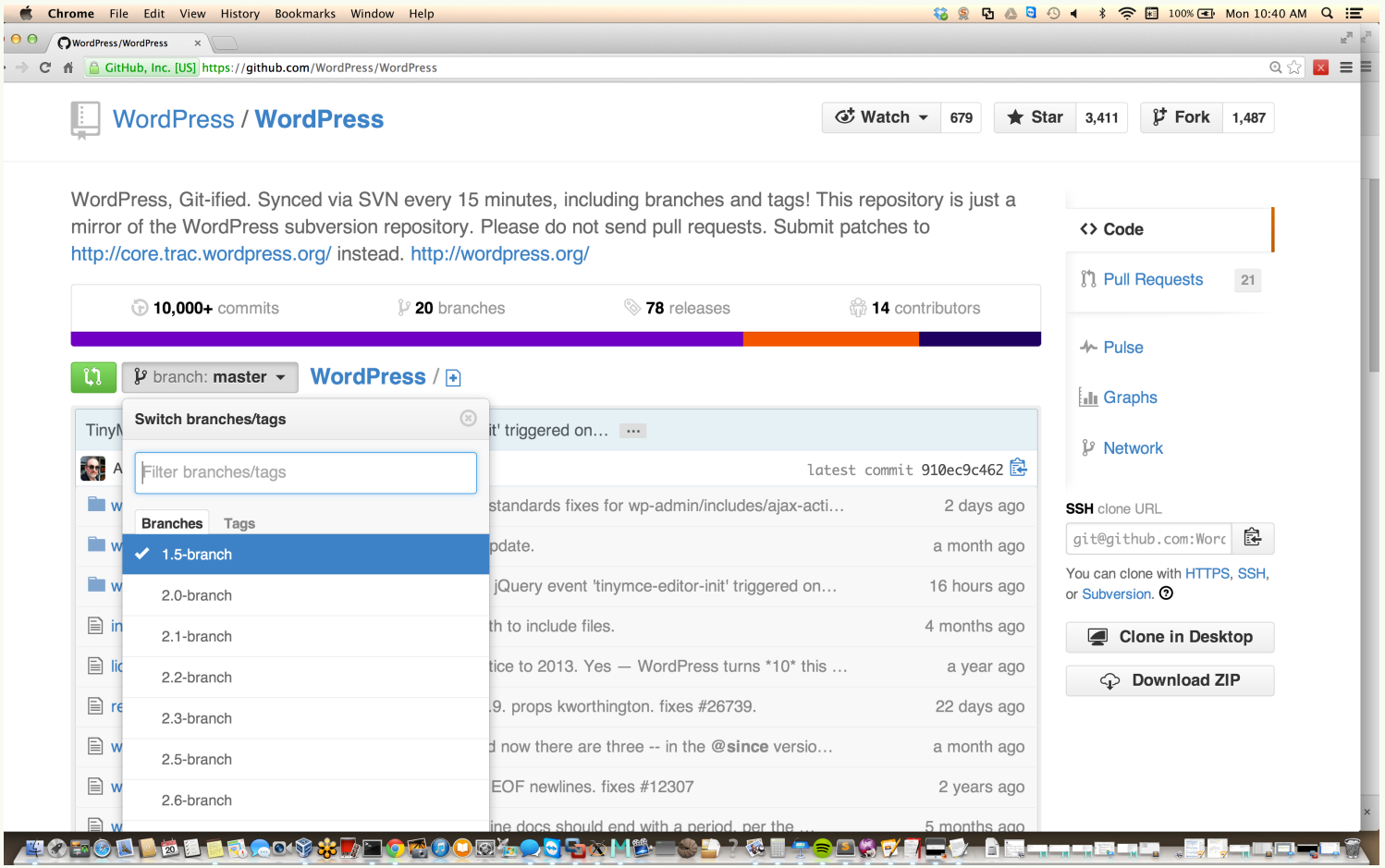
Forensic Logging - pe.log

ts	1232039481.72727
fuid	**hVkwqId1J1h**
machine	I386
compile_ts	1200557518
os	Windows NT 4.0
subsystem	WINDOWS_GUI
characteristics	32BIT_MACHINE,RELOCS_STRIPPED,EXECUTABLE_IMAGE,LOCAL_SYMS_STRIPPED,LINE_NUMS_STRIPPED
section_names	.text,.data,.rdata,.INIT,.edata

CRITs::Multiple_Campaign_Hits Recently 2 items on the zzAPT campaign were hit CRITs UIDs: 504f88abe0742e059a424144, 509697c6e0742e4d547a907d

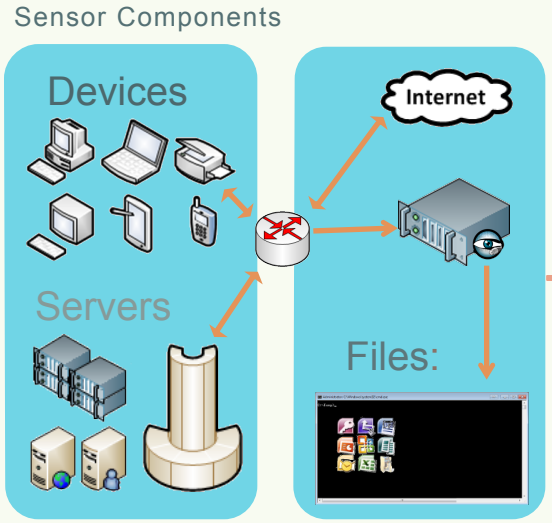


Mass Identification – Pivoting on File Hashes



ExifTool Integration – This isn't a great idea for production

Tap: Bro Sensor



"application/x-dosexec" or "image/jpeg"?

File

exiftool

logs

Lot's of files.

Capabilities, use cases, & direction.

Popular Files – What files are moving around your network?

Count	Mime/type	Hash	Byte Size
29218	image/png	5b68ce2e93a3b0108ab4727cd71f288d	63276
29534	text/plain	4713e1d9da3c057dcc9d221527eb3735	69
30040	text/html	27075f14ab3ea314e553d0c183687538	162
30111	text/plain	1ad6c6129770acfcce39291f3c276c80	10
31654	application/octet-stream	27ba19805d52e788ce7ee21d6f82137c	4
35107	image/gif	a9ee8e691ee0fbbc8de1034c3ddcfeb8	1366
35113	image/gif	fc9101c8cd522e4459e814cc9cae37f9	1365
43272	image/png	9fd1e5455611cf33ca2d18d9dd1efbbf	3698
44052	text/plain	dc0ea0aa1c5fe9aec2af13b0b016a817	29
44450	image/gif	024240b6b43e2e4bb91d7dd3b9f9d615	469
47275	image/png	9e814a1f719bfe4d4c4189fafd2ba874	962
48060	application/xml	eece07078ce27fc2734f15320684fd8f	2242
49641	text/html	46ef7a38938e4f08ca381a3fb780290c	341
53233	text/plain	72cc6a67abeea515c246ca0bfb457b0c	41
84517	text/plain	4bcbe4567773a3692bad5b05b075f281	13
97388	text/plain	7516fd43adaa5e0b8a65a672c39845d2	2
105390	text/plain	9977a0db0831971f1e3ef7ff9f282e54	38
666173	text/html	50509771df61af7daa5cec51a7e5a971	950

Popular Mime Types – What files are moving around your network?

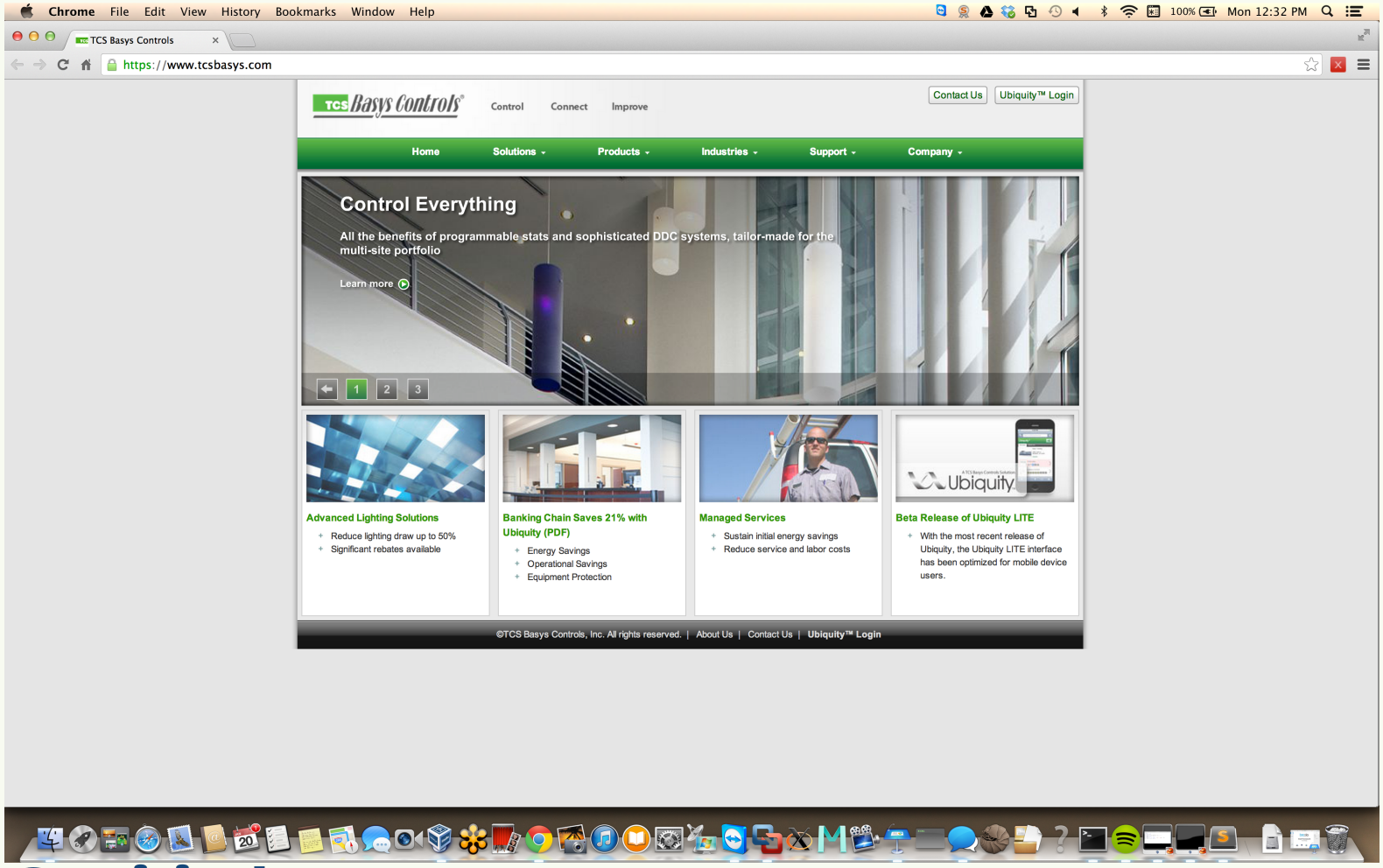
Count	Mime/Type	Hash	Byte Count
1	application/x-dosexec	ed8ec0b7fa0dabf45507907ec2438256	165434776
1	application/x-dosexec	f71bbd7e5bb7c4a37adc5619f8490912	1479312
2	application/x-dosexec	-	-
2	application/x-dosexec	-	570387
2	application/x-dosexec	5e8cb14f5264af82f66008306e56eaa8	921512
2	application/x-dosexec	8aeb3518dba084801af8fcf40f68f061	1479312
2	application/x-dosexec	a9657838240f084964ef69000f08327c	5697816
3	application/x-dosexec	-	231584
3	application/x-dosexec	-	270496
3	application/x-dosexec	dd49549a75adde0fc11308ff3dcaf918	895144
9	application/x-dosexec	3c5dc23b22f8b1578bc6ae8600a7791c	847128
10	application/x-dosexec	067898937ea64b69bdd680573814884d	847128
10	application/x-dosexec	621560ba91fa87b2adca692a313b09eb	847128
15	application/x-dosexec	1e6c1c60666c84b3cf594f03abbf5500	847128
15	application/x-dosexec	3efcb01e94563cf1913a1e5c32d81a5a	847128
21	application/x-dosexec	56a9e7aa037d23ec9c942ce902533226	847128
39	application/x-dosexec	c665a5ab6a49fa938a7f09011dfae67e	847128

```
less files.log | grep 4bcbe4567773a3692bad5b05b075f281 | head -n1
1390190400.371500       FUYUOc1Yp8FcDUavc1      198.35.50.99    10.80.88.98
COgilq4XrBbD7Ztv81      HTTP    0       SHA1,MD5,EXTRACT        text/plain
-       0.000000        F       F       13      13      0       0       F
-       4bc7773a3692bad5b05b075f281
84988154ea0ca95d84ea0eb424cea482f05e9e81        -       extract-HTTP-
```

```
<TCS>
</TCS>
```

Critical Stack

Popular Files – Building control system



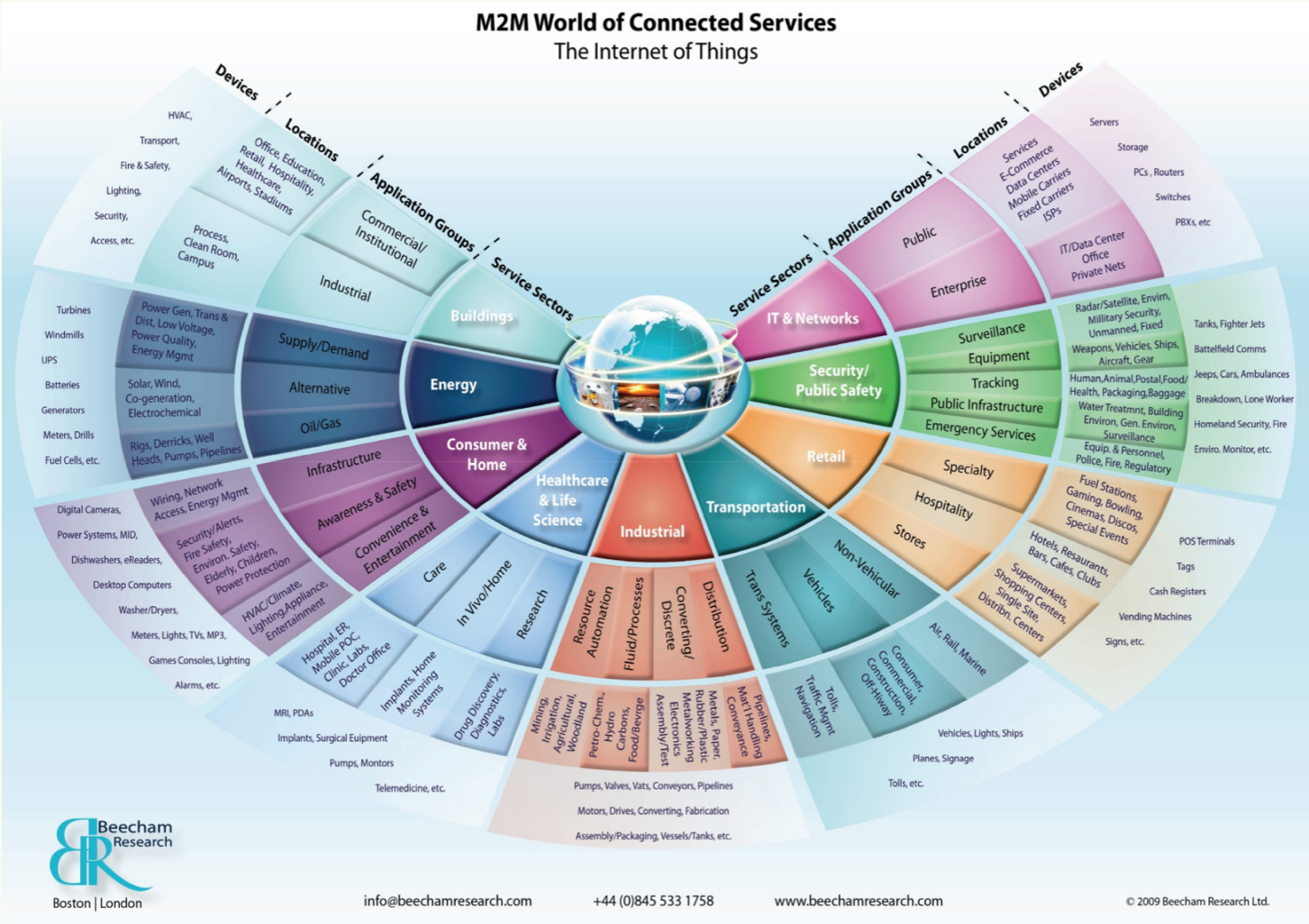
By Country – Is this interesting?

Critical Stack

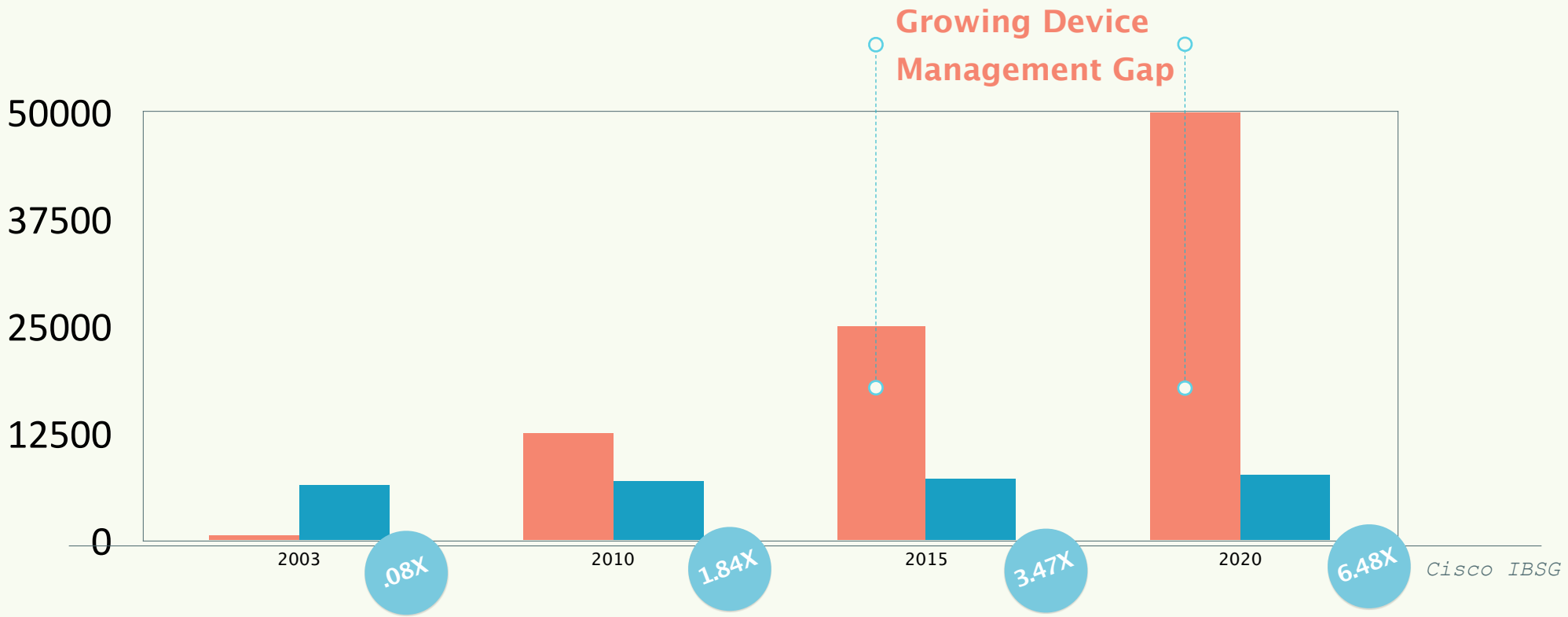
Lot's of files.

Capabilities, use cases, & direction.

Devices – Network of things?



Growth of Embedded Devices – We are on the wrong side of math



Trends Against Us

We are not only outnumbered the devices are growing in:

- complexity
- computational power
- variety

Lack of mgmt tools--> AV, HIDS, Update, Policy

Critical Stack

Another Embedded Target – Similar Threat Surface

10/100 Ethernet

Optional Wifi
Expansion Slots

I/O Options

3 Alarm Inputs
2 Alarm Outputs
RS-232C
RS-485

Protocols

ARP, HTTP, FTP, SMTP,
SNMP, DHCP, TCP/IP

System

Embedded Linux
8 MB of Storage
Expansion Slots

Sony SNC-RZ30n PTZ Camera

Sony cameras come in a large number of configurations.

Model appeared in 2003- similar to current models.

25x Optical Zoom

Multiple Codecs, Frame Rates, etc.

Sony SNC RZ30n – Firmware Update Process
October 2013 Demo– Deploying Malicious Payload to Clients

START

1. Authenticate to device

FAIL!

2. Enable FTP: http://<IP>/command/**ftpserver.cgi?FtpServerFunc=on**

3. FTP: `mkdir web\home`

:)

4. Upload resources

5. Install: http://<IP>/command/**main.cgi?System=versionup**

Step 1: Recon– Default Creds

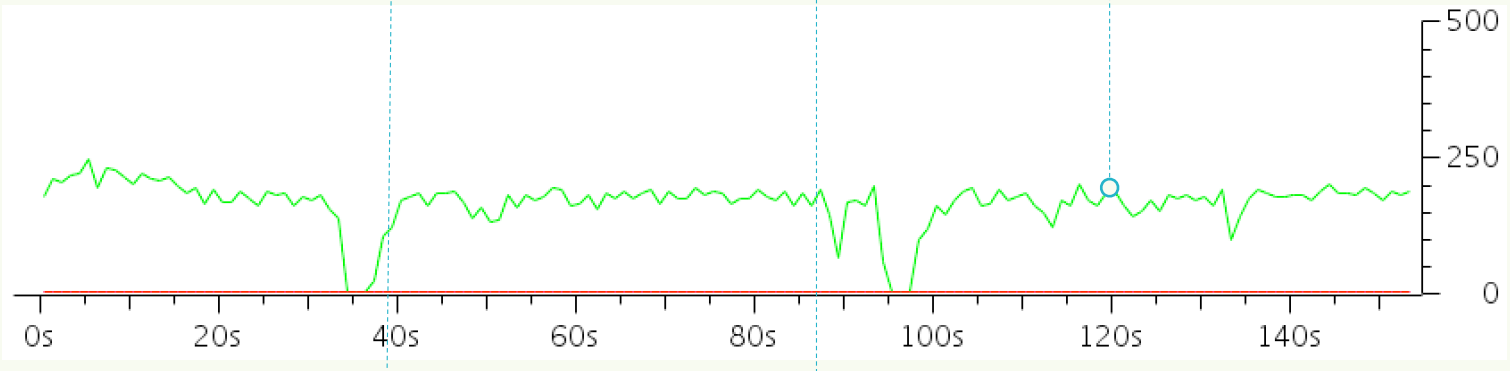
Socratic Ideal– Anomaly Detection

Pink
FTP–DATA

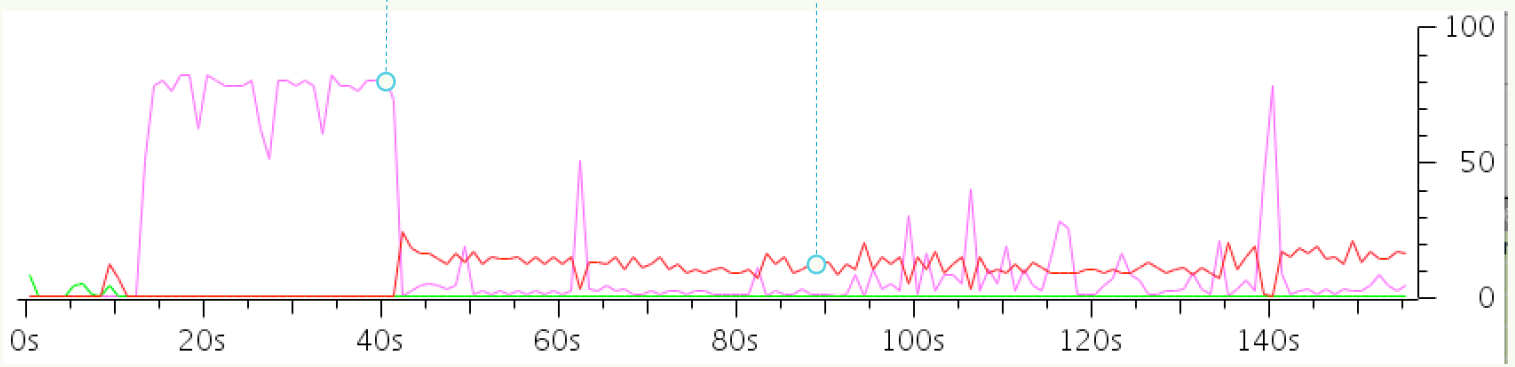
Red
FTP

Green
HTTP

Normal



Payload
Upload



What should your network look like?

You can not secure what you do not understand.

Real Time Response – On Violation, Extract Files.

```
add approved_comms[192.168.0.236, Analyzer::ANALYZER_HTTP]
```

```
if ([c$id$resp_h, atype] !in unapproved_comms)
        {
            add unapproved_comms[c$id$resp_h, atype];
```

```
Files::add_analyzer(f, Files::ANALYZER_EXTRACT);
```

Questions?

Thank you!