Bro Overview

2014-7

Overview

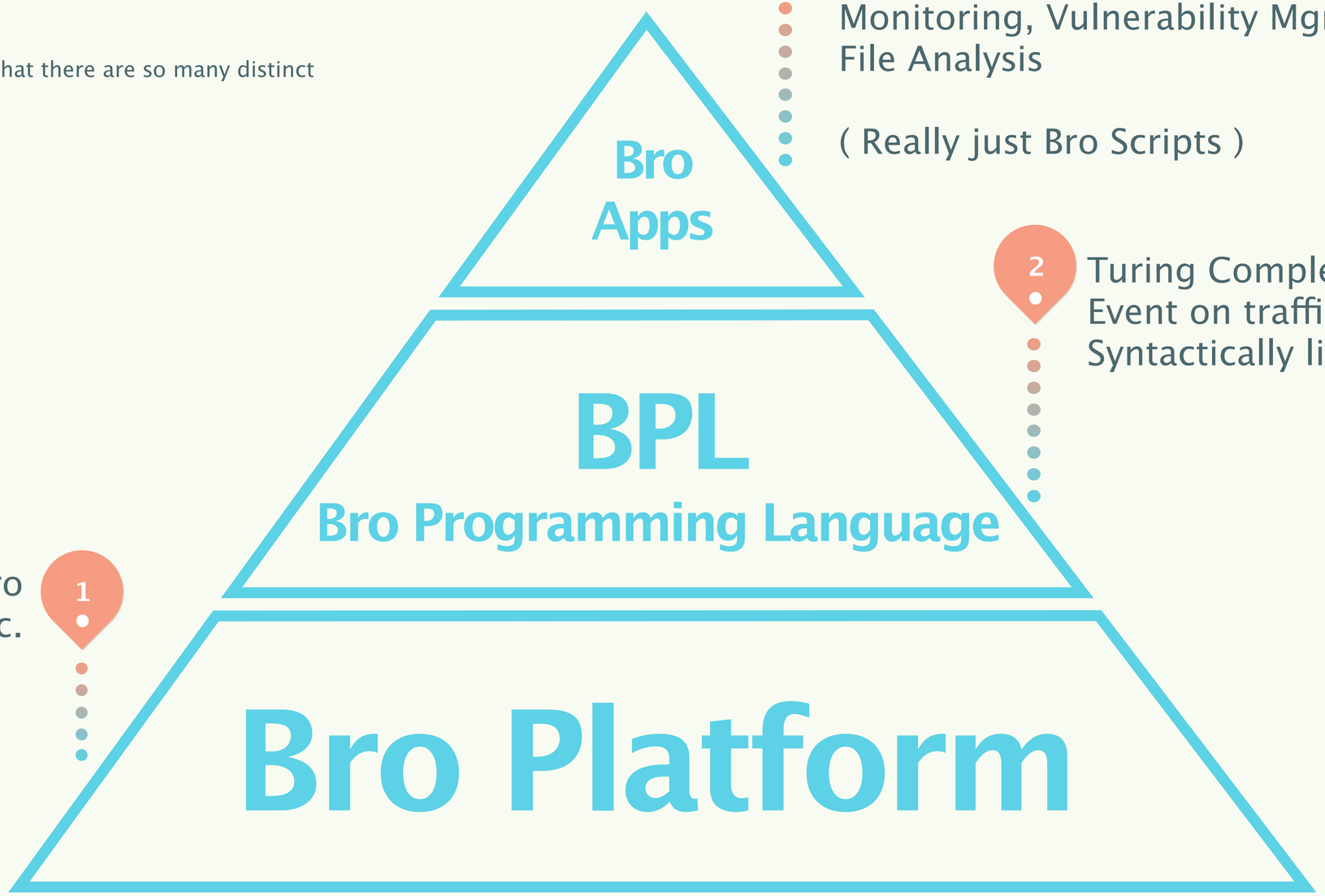
Liam Randall
Critical Stack LLC

Critical Stack

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



3 Bro-IDS

Monitoring, Vulnerability Mgmt, DLP, Analysis, File Analysis

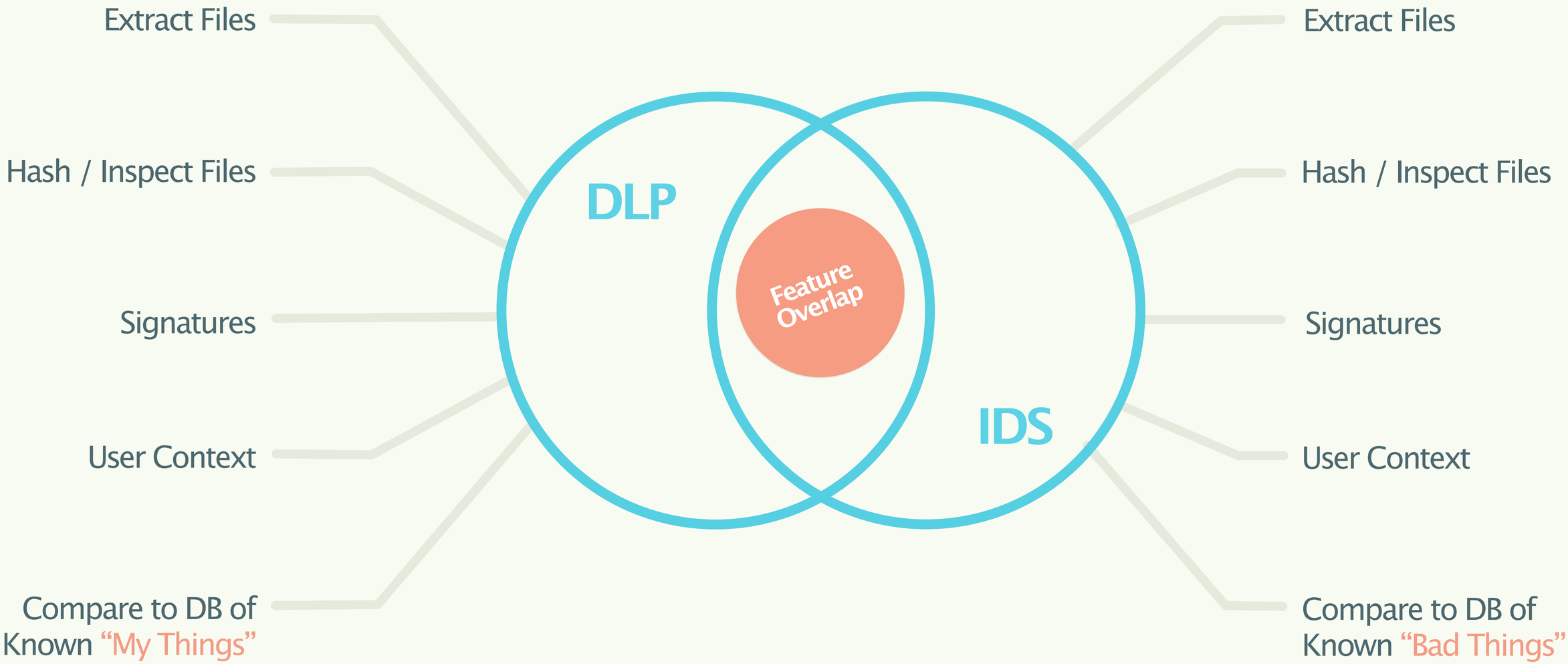
(Really just Bro Scripts)

2 Turing Complete PL
Event on traffic, files, protocols
Syntactically like Python

1 Utilities to manage Bro
API, Interfaces, etc.

Critical Stack

Functional Requirements – DLP vs. IDS; major functional overlap



Critical Stack

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

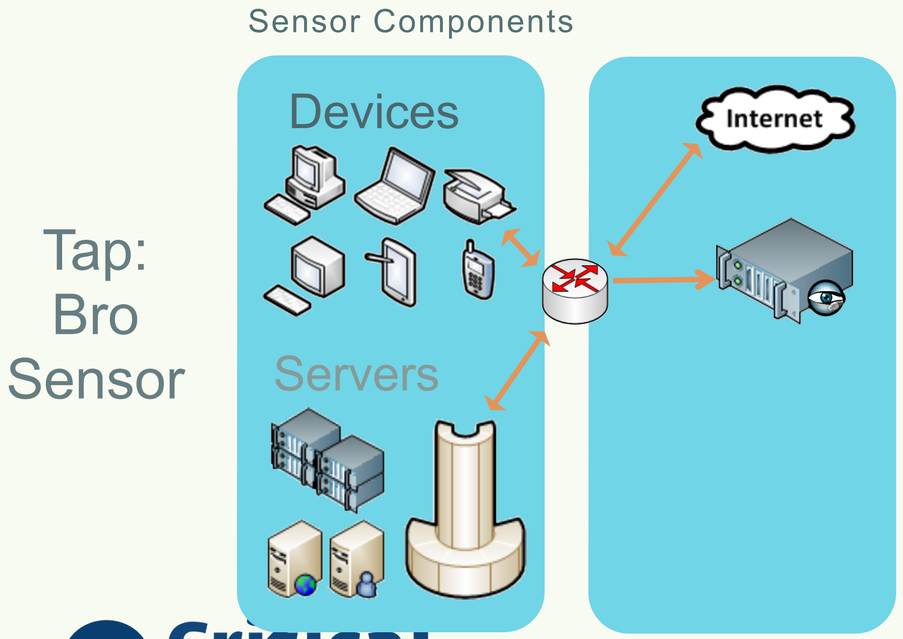
Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

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.



Critical Stack

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	AZIHpPIejvi	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

Critical Stack

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	93CIvevOuxk	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	XLE8fYl5Tvg	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

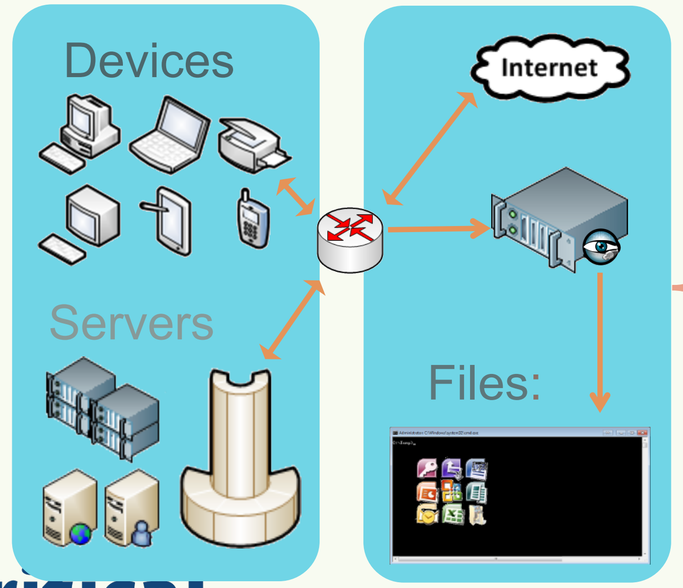
Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

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

Tap: Bro Sensor

Sensor Components



Extracted File Analysis

Signature Analysis
- Active Analysis→ Malware Hash Registry
- Intel Comparison → OSINT, FS-ISAC, DOE CIRC…

Active Analysis
- www.Malware-Tracker.com
- Static & Dynamic Analysis
- Cuckoo Box? Volatility

Long Term Analysis
- Coverage for Mobile Devices, Embedded
- Post Compromise Research
- Analysis- copy of every EXE in Company

Predicative Analysis
- AV, Malwarebytes→ Open a Ticket
- Content Analysis- Keywords,

Critical Stack

Market Trends – Diversity of devices driving the trend for network analytics

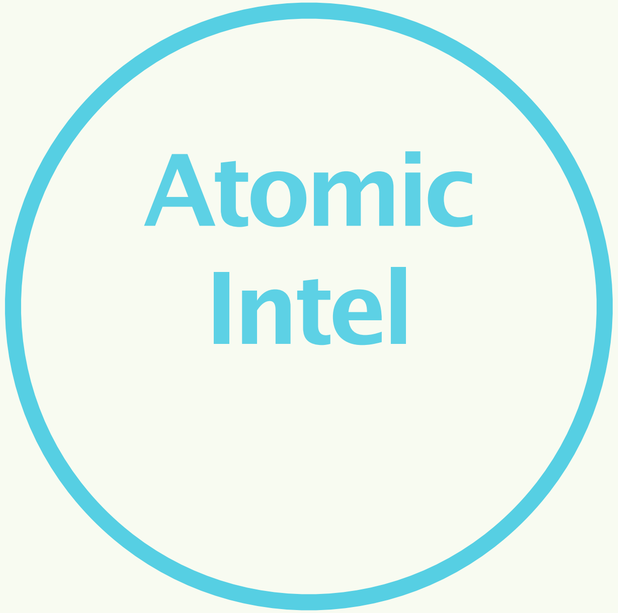
Cloud Computing

BYOD

Internet of Things

- **Dynamic Networks** – Network and components constantly changing;
- **Diverse OS Ecosystem** – Diversity of devices driving the trend for network analytics
- **Multitude of Vendors** – Unified through standard protocols
- **Lack of Management Tools** – Diversity of devices & OS with out central management or configuration
- **Device & Network Compliance** – Complex networks means additional compliance concerns

Critical Stack



Network Monitoring

Advanced Atomic Intelligence Application

Critical Stack

Terms & Definitions – Signature Detection vs. Anomaly Detection

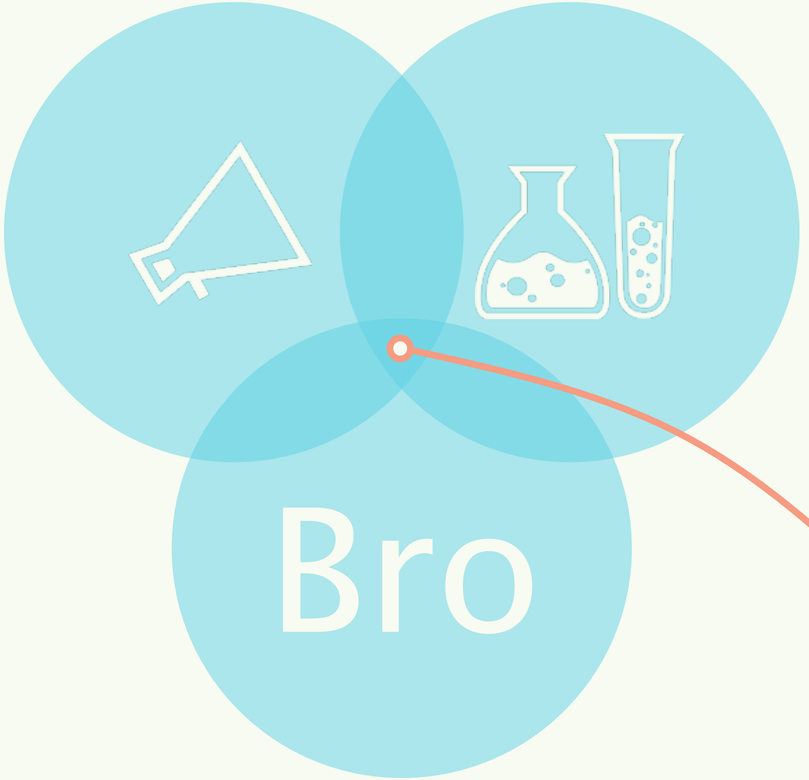
Signature Detection

atomic indicators

domains, file hashes, IPv4/6

Traditional Signatures

Algorithms



Anomaly Detection

Traffic Analysis

Flow Analysis

Protocol Analysis

Deployment

Today we concentrate on that

Classically Speaking...

In the literature you will typically find IDS's broken into two distinct categories– Signature or Anomaly based Detection.

Bro is designed to face Next Generation Challenges.

Bro Platform

Hybrid System

Best of Both Worlds

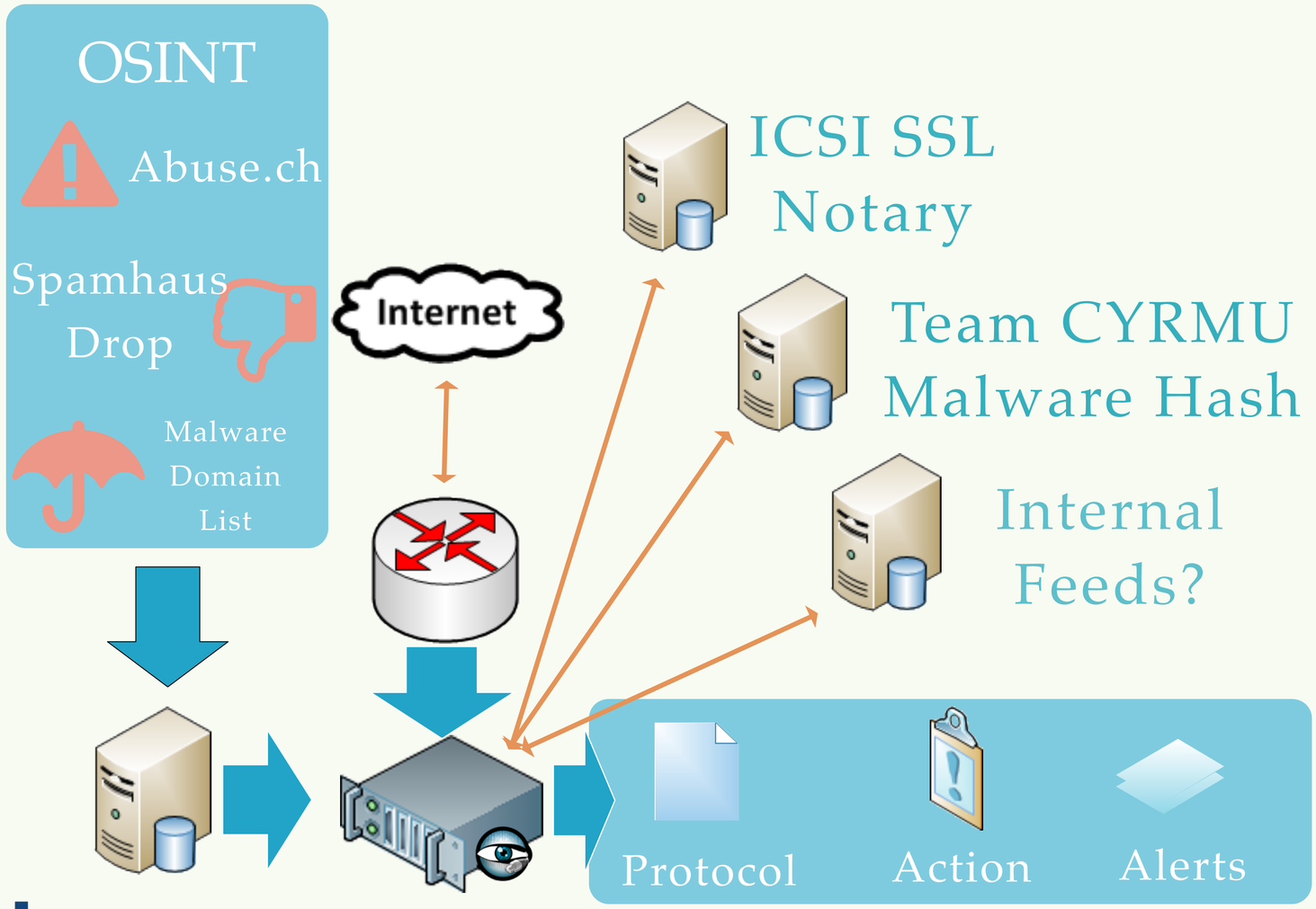
+ a programming language

Critical Stack

Current Paradigm

Finding the bad stuff we know about.

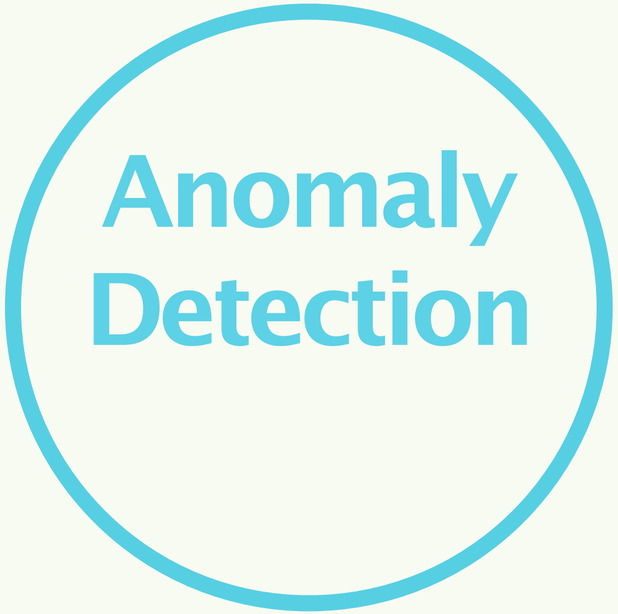
CRITs::Multiple_Campaign_Hits Recently 2 items on the zzAPT campaign were hit CRITs UIDs: 504f88abe0742e059a424144, 509697c6e0742e4d547a907d



Critical Stack

Protocol	Location	Intel Type
IP	Connection	Address
DNS	Request, Reply	Address, Domain
File	Hashes Generated	Hash
File	Name	Name
HTTP- HEADER	HOST	Domain
HTTP- HEADER	REFERER	Domain
HTTP- HEADER	X-FORWARDED-FOR	Domain
HTTP- HEADER	USER-AGENT	Software
SMTP-HEADER	FROM	Domain
SSL / TLS	X-509 Certificate CN	Domain

.. exhaustive to list all the permutations!



Network Monitoring

Understanding what is happening on your network

Critical Stack

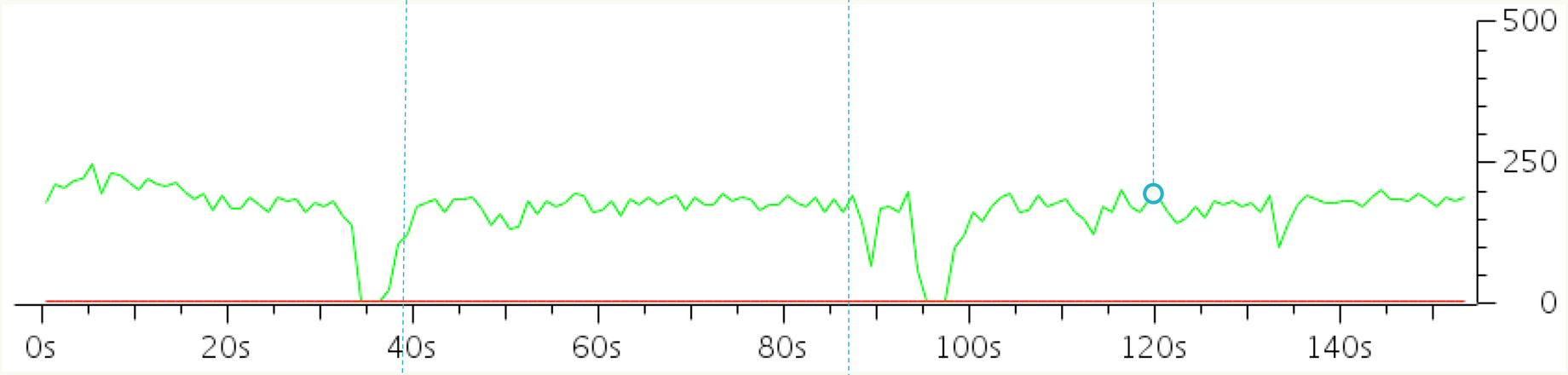
Socratic Ideal– Anomaly Detection

Pink
FTP–DATA

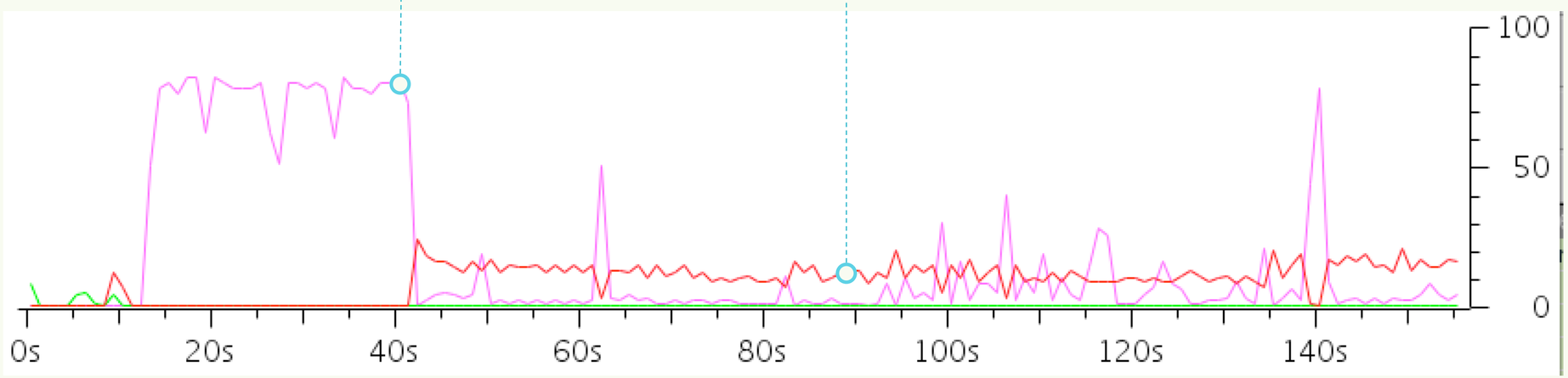
Red
FTP

Green
HTTP

Normal



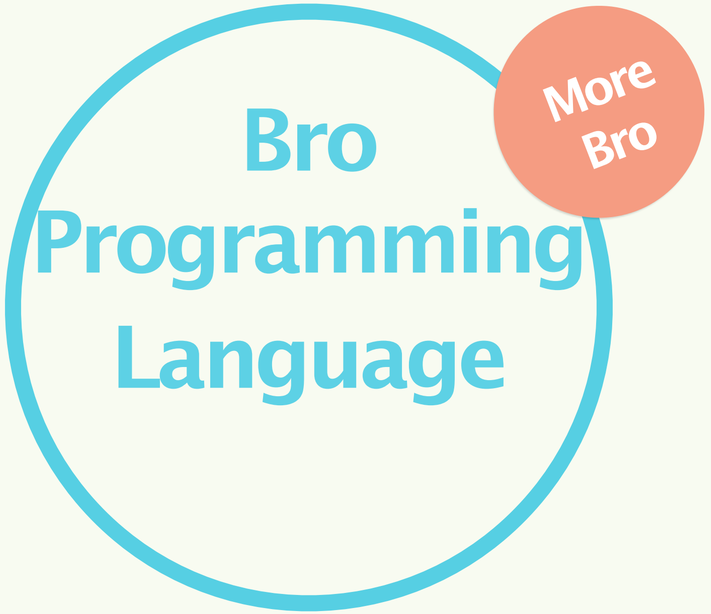
Payload
Upload



What should your network look like?

You can not secure what you do not understand.

Critical Stack



Advanced Analytics

Real Power of the Bro Platform

Critical Stack

Full Bro Script

Bro is event driven

Domain Specific PL

Fires for each new file

Base Abstraction

Generic Streaming Event

Attach Analyzers

```
event file_over_new_connection(f: fa_file, c: connection, is_orig: bool)
{
        if ( is_orig && c?$http && c$http$method == "POST" )
                Files::add_analyzer(f, Files::ANALYZER_EXTRACT);
}
```

Streaming Analyzers

Arbitrage Slow NICs vs Fast CPUs

Incrementally handle workload

What's Missing

Ports, protocols, IPv4 / IPv6, tunnel layer, etc..

If you want to care about these things, do so at script land

Critical Stack

Bro is a Platform

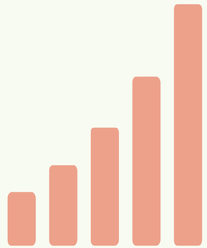
Develop Advanced Heuristics

Host Scan

Scan::Address_Scan X.X.X.X

scanned at least 25 unique hosts on

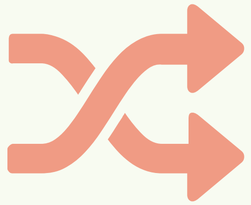
port 80/tcp in 0m29s



Rogue Access Point

Rogue access point detected
Jabber/9.2.1.147214

3.202.206.243



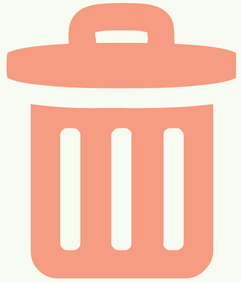
TOR

Tunneling Protocol.

Support dozens of Tunnels.

China Chopper

Develop Advanced Heuristics



Custom C2 Demonstration

Identify

Decode

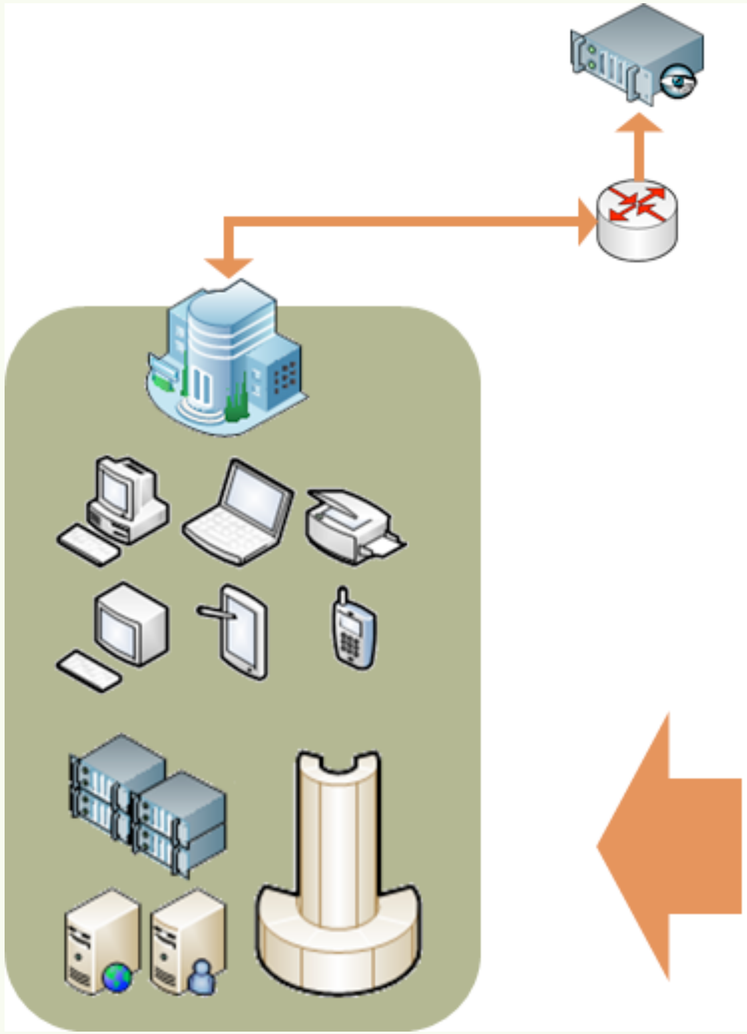
Detect

Application Level Detail

Ground Truth of your Network Applications

Critical Stack

Compliance Management – Ground Truth of Applications

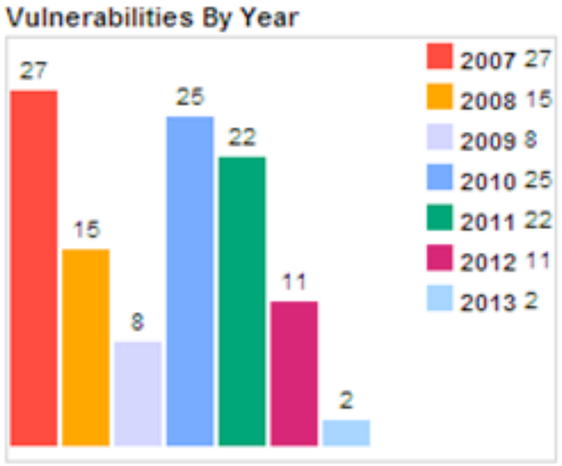


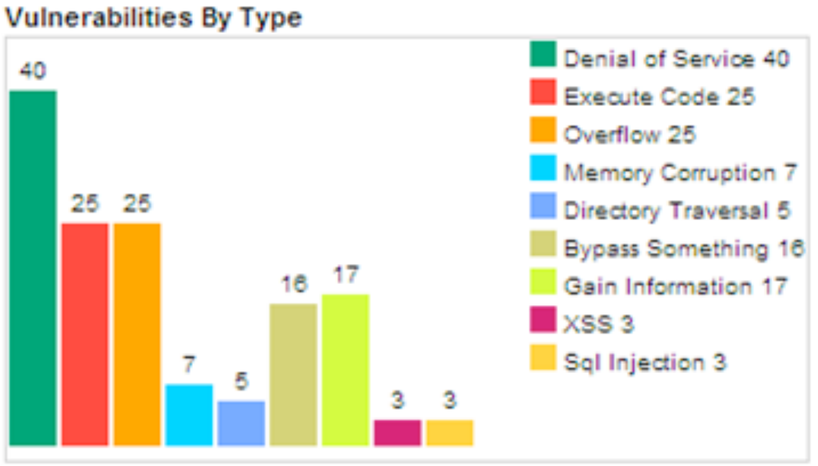
PHP/4.2.2
PHP/4.3.10
PHP/4.3.2
PHP/4.3.4
PHP/4.3.8
PHP/4.3.9
PHP/4.4.0
PHP/4.4.7
PHP/4.4.9
PHP/5.1.2
PHP/5.1.4
PHP/5.1.6
PHP/5.2.0
PHP/5.2.1
PHP/5.2.10
PHP/5.2.11
PHP/5.2.12
PHP/5.2.14
PHP/5.2.15
PHP/5.2.16
PHP/5.2.17
PHP/5.2.3
PHP/5.2.4-2ubuntu5.10
PHP/5.2.4-2ubuntu5.14
PHP/5.2.4-2ubuntu5.26
PHP/5.2.4-2ubuntu5.6PHP/5.2.5
PHP/5.2.5 (x64)
PHP/5.2.6
PHP/5.2.6-1+lenny4
PHP/5.2.6-3ubuntu4
PHP/5.2.6-3ubuntu4.6
PHP/5.2.8
PHP/5.2.9
PHP/5.3.0
PHP/5.3.1
PHP/5.3.10
PHP/5.3.10-1ubuntu3.2
PHP/5.3.10-1ubuntu3.4
PHP/5.3.13
PHP/5.3.14
PHP/5.3.15
PHP/5.3.16
PHP/5.3.17
PHP/5.3.18-pl0-gentoo

Critical Stack

Compliance Management – Actual Truth

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2007	27	8	13	9	1			2		5	1				11
2008	15	3	4	4				2		3	1				1
2009	8	4					2								
2010	25	5	3	1	4	1	1			3	13				1
2011	22	16	1	8	2					3	1				5
2012	11	4	4	3		2		1		1					1
2013	2									1	1				
Total	110	40	25	25	7	3	3	5		16	17				19
% Of All		36.4	22.7	22.7	6.4	2.7	2.7	4.5	0.0	14.5	15.5	0.0	0.0	0.0	





Accurate Network Analysis

The Bro Platform is the Ground Truth of your network.

Critical Stack

Policy Enforcement

Transport, port, and OS agnostic Policy Enforcement
Range of techniques to lock systems down

- Software Versions
- SSL/TLS Configuration Details
- Network Controls– Record Host Access
- Software Versions
- Audit User Access
- File Access

Detect System Modification

Discover the network ground truth of actual system configuration
Transport, port, and OS agnostic System Pinning

- New Services
- New Hosts, Modified Hosts
- Change in current software version on host
- Known SSL/TLS Certificates
- Public Facing Hosts / Software / Certificates
- New Services
- Windows Administrative Access

Automated File Analysis

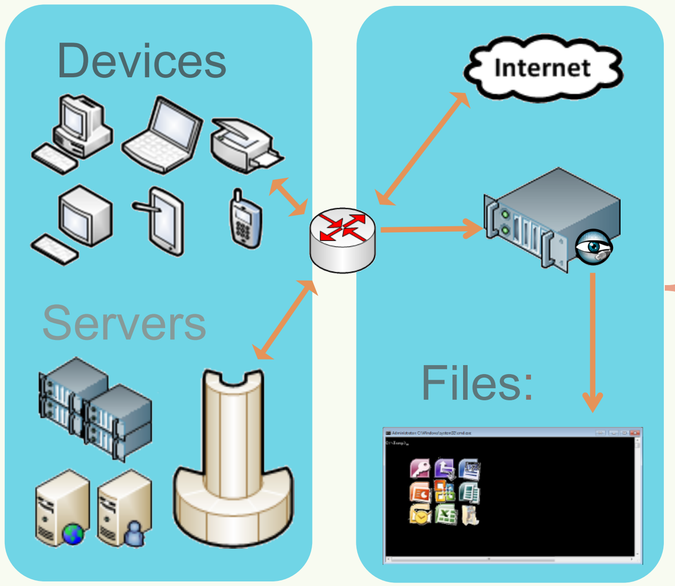
Bro allows network operators to perform advanced static and dynamic file analysis

Critical Stack

File Extraction – Extensive Real Time Analysis

Tap:
Bro
Sensor

Sensor Components



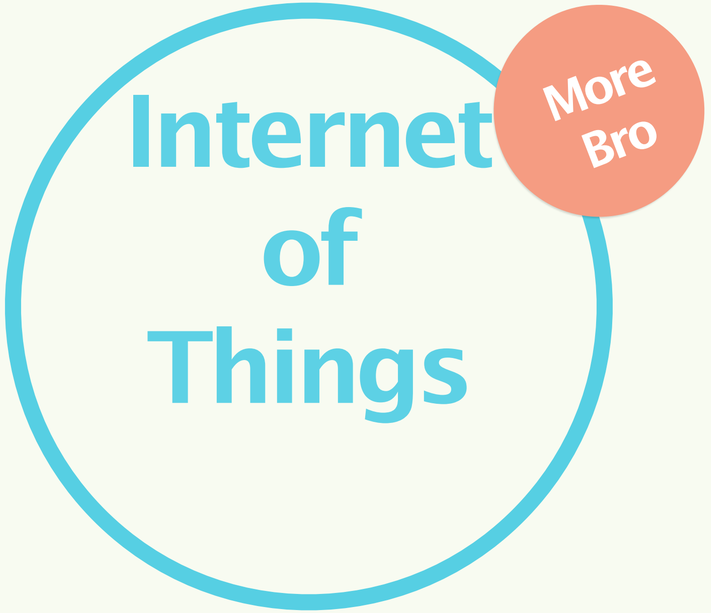
Extracted File Analysis

Signature Analysis
- Active Analysis→ Malware Hash Registry
- Intel Comparison → OSINT, FS-ISAC, DOE CIRC…

Active Analysis
- www.Malware-Tracker.com
- Static & Dynamic Analysis
- Cuckoo Box? Volatility

Long Term Analysis
- Coverage for Mobile Devices, Embedded
- Post Compromise Research
- Analysis- copy of every EXE in Company

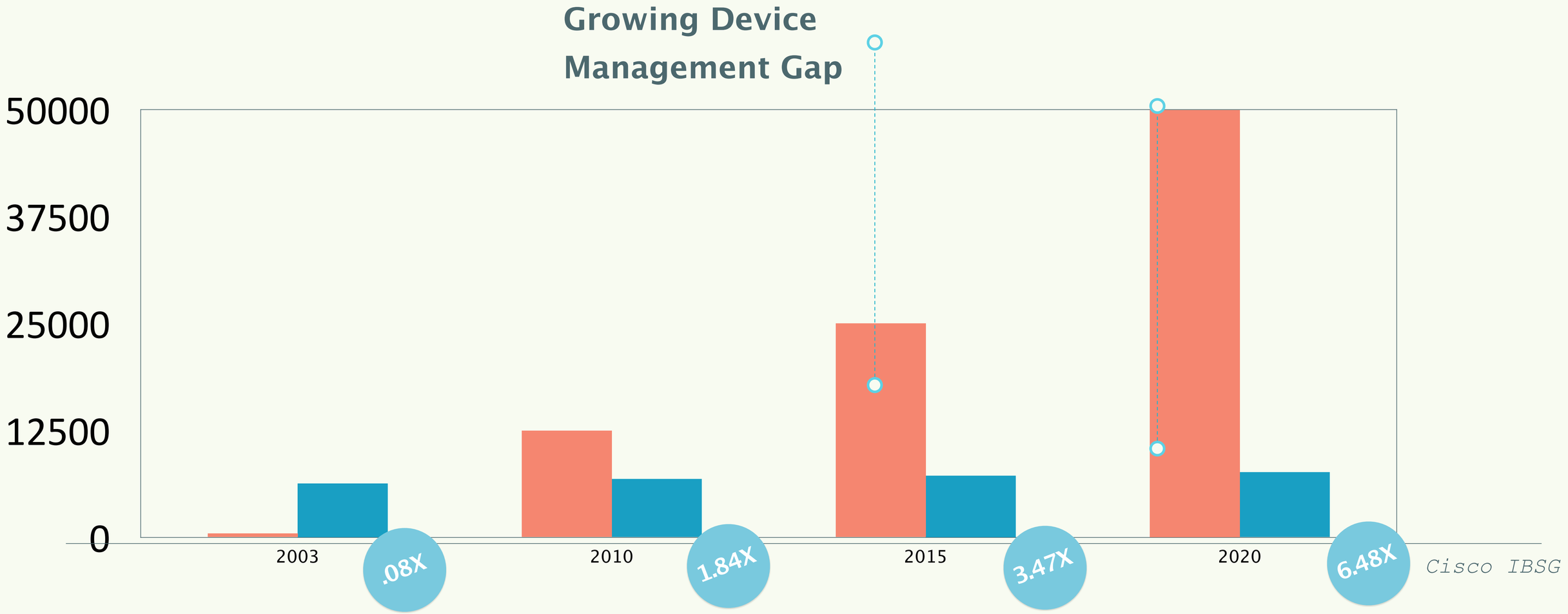
Predicative Analysis
- AV, Malwarebytes→ Open a Ticket
- Content Analysis- Keywords,



Device Management

Networks are now dominated by non-PC based devices.

Scale of Devices – ICS Scada Controller



Trends Against Us

We are not only outnumbered the devices are growing in:

- complexity
- computational power
- variety

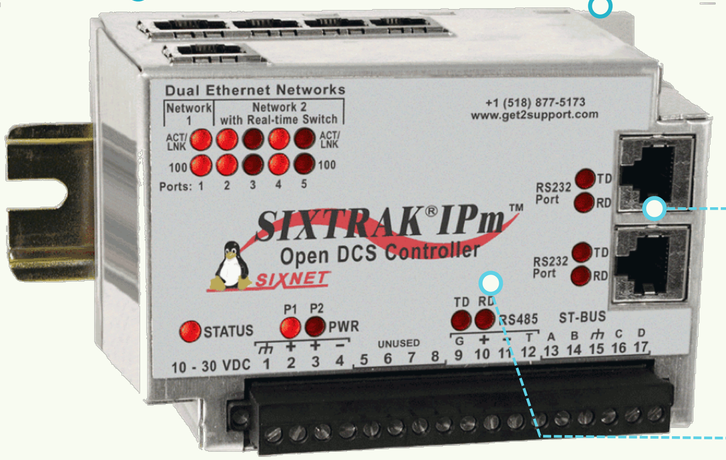
Lack of mgmt tools--> AV, HIDS, Update, Policy

Critical Stack

Sample Device – ICS Scada Controller

Hardware Details

Embedded Linux
Dynamic Memory: 16– 64 Mb
Flash Memory: 16 – 128 Mb
32 bit PowerPC



10/100 Ethernet

1 Port Primary (2 MACs)
4 Port Switch

Protocols

Sixnet, Modbus/TCP, DNP3
ARP, UDP, ICMP, DHCP, PPP...

RS232, RS485

Multiple configurations

Communication

Telemetry, Telephone (dialup, leased), radio...

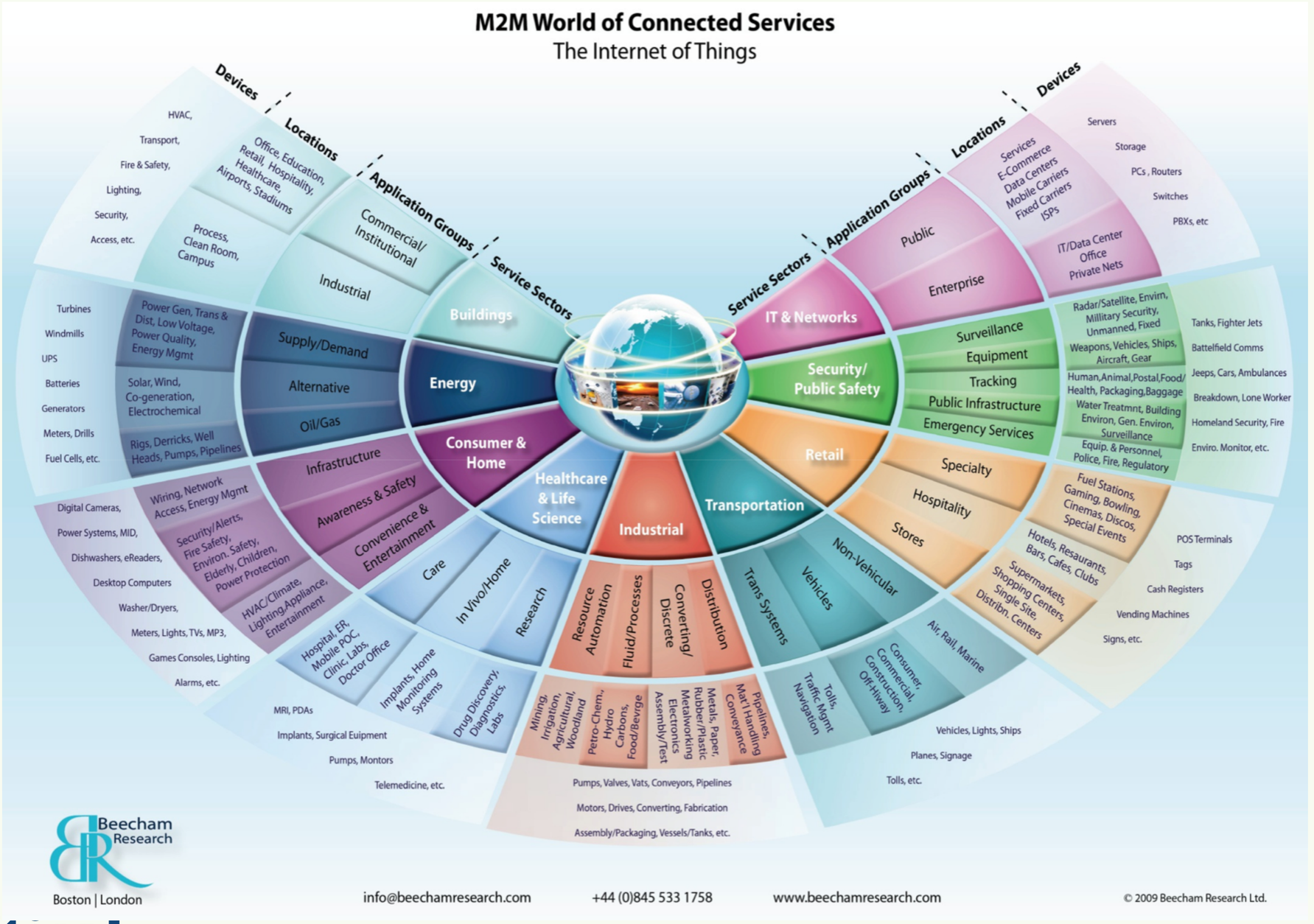
Capital Investments

ICS, Embedded, Medical, Infrastructure is not easy to replace and may be designed to run for 30+ years.

Embedded, TVs, mobile devices, gaming devices, packages...

Critical Stack

Devices – Network of things?



Specialized Traffic Modbus – 7 Days of Traffic

Examine Modbus

Count

All Participants by Exception

Anomaly?

1 Time

1 Host

1 Command

Count	Orig	Resp	Errors
1	10.67.4.147	10.18.226.13	-
6	10.1.1.35	10.72.230.36	GATEWAY_TARGET_FAILED_TO_RESPOND
18	10.1.1.35	10.60.30.73	ILLEGAL_FUNCTION
5189	10.1.1.35	10.60.30.73	ILLEGAL_DATA_ADDRESS
123513	10.1.1.35	10.60.30.73	-
164312	10.1.1.35	10.60.230.36	-

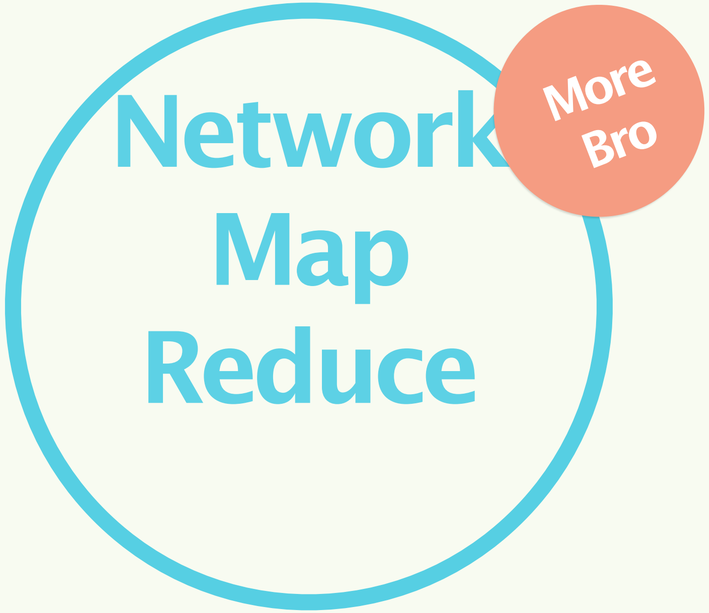
Normal Comms

Regular polling of data

Curious Anomalies

The frequency this host is participating in the network does not make sense.

Critical Stack

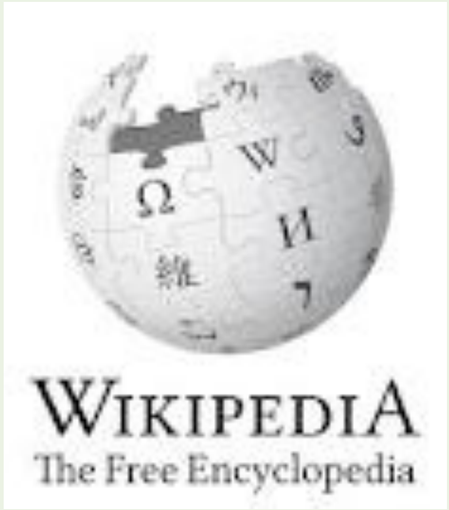


Sumstats: Bro Map Reduce

The Bro Platform allows you to perform map reduce operations on live streaming traffic.

"Summary statistics are used to summarize a set of observations, in order to communicate the largest amount as simply as possible."

General Purpose Measurement



Cluster Safe!

Critical Stack

Measurement

Sumstats is our cluster safe library for measuring "stuff"

Epoch

Discrete Time
Slices

Streaming

Realtime Data
Handling

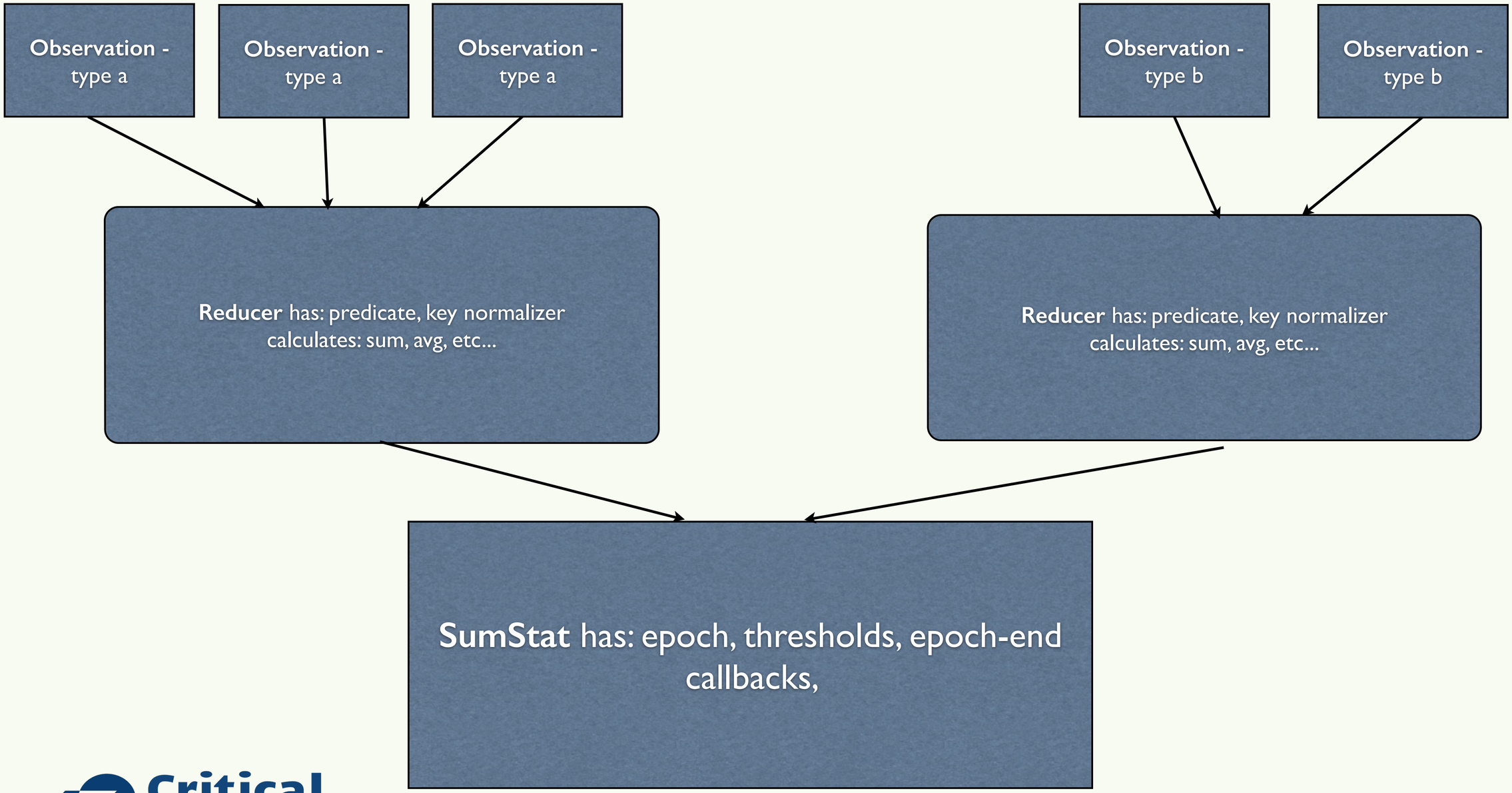
Composable

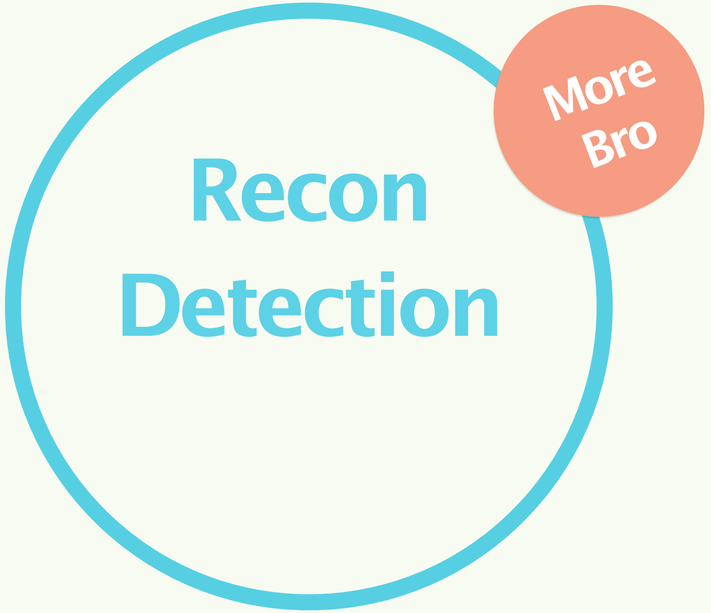
Measurements MUST be
merge-able
for Cluster Support

Probabilistic

HyperLogLog
Top-K

Model – She may not look like much, but she's got it where it counts..





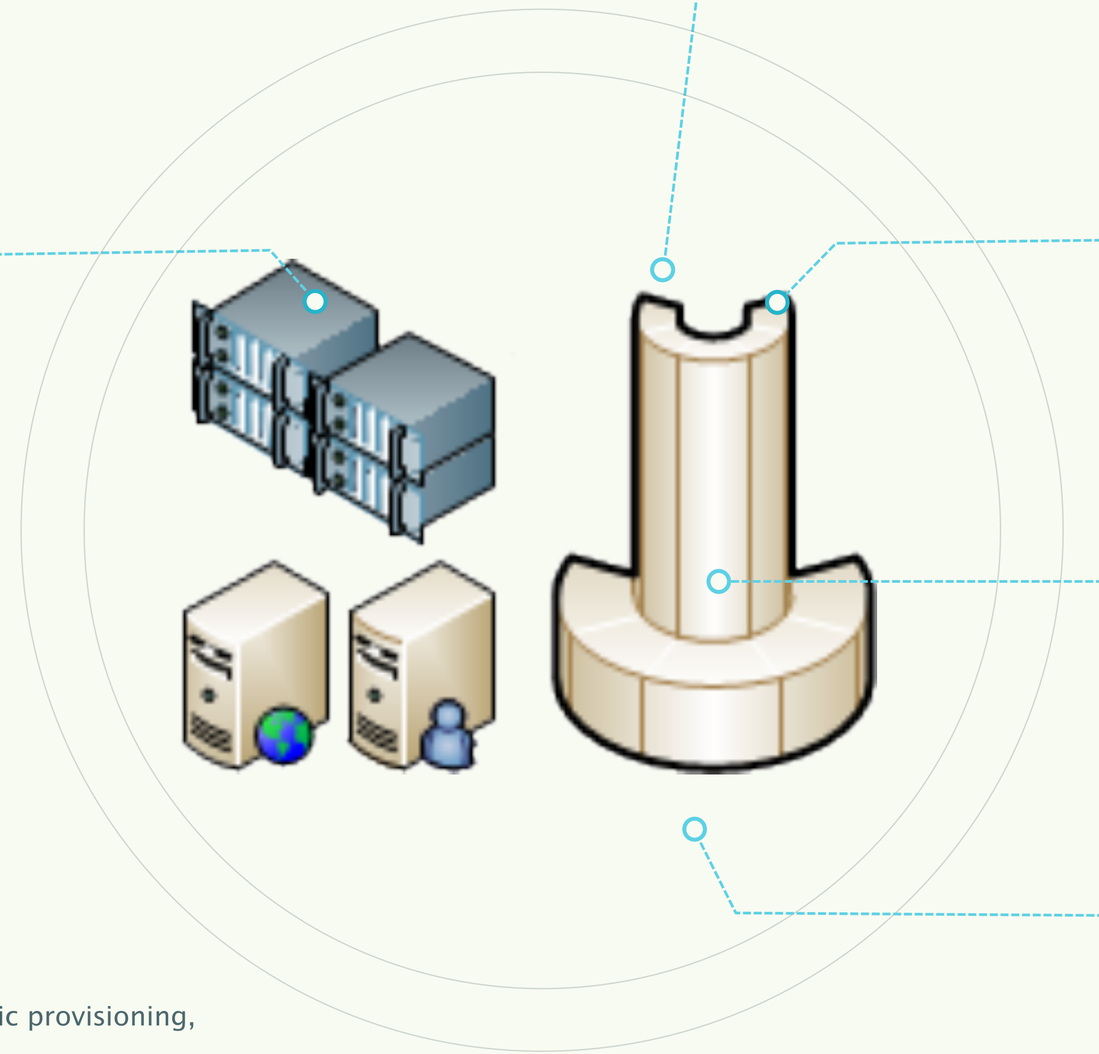
Advanced Reconnaissance Detection

Using the Bro Platform

Critical Stack

Concepts

General Case is Host / Port
Map the network
Forward / Reverse DNS
Lots of Record Types



Host Based

Laterally from host to host
Typically for a type of service
“Worm”

Abuse Tools

Dnmap, zenmap, scapy, nc, etc.

Protocol Tools

sipvicious, sslscan,

Tracerouting

Map depth and routes of the network

TCP, UDP, ICMP Probing

Key internet protocol frequently used for dynamic provisioning, service location; only some details documented

Critical Stack

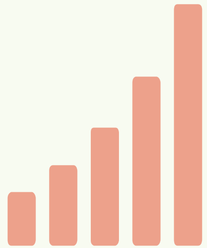
Traditional Scanning

Many people only think of traditional recon

Host Scan

Recon multiple ports for services, typically common, looking for banners.

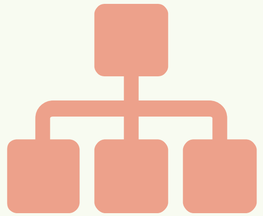
Tag out specific services.



Tracerouting

Probe infrastructure; relationships, depth.

Learn about network complexity.



Port Scan

Taking the general many DNS Attacks are noisy and fail.

Let's watch for some extreme failures.

Protocol Details

RFC 1035
Stateless
UDP or TCP

Concepts

Authoritative Server (Recursive)
Key / Value Store
Forward / Reverse DNS
Lots of Record Types

Abuse Tools

DNS Recon, DNS Map,
DNS Enum, DNS Tracer,
DNS Walk

Record Types

A, CNAME, SRV, AAAA, MX
DNAME, SOA

Security Problems

Information Disclosure, DNS
Amplification, Spoofing, MitM

Domain Name System

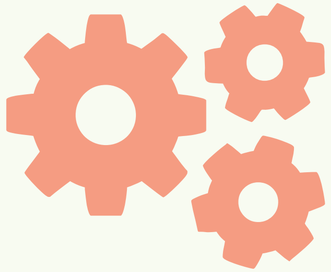
Key internet protocol frequently used for dynamic provisioning, service location; only some details documented

Critical Stack

AXFR / IXFR

Attacker asks DNS Server for a copy of the DNS Zone.

Frequently fails, try it anyway.



PTR Abuse

Attacker mines DNS infrastructure for host details PTR Records.

Typically see reverse of entire subnet.

NXDomain

Taking the general many DNS Attacks are noisy and fail.

Let's watch for some extreme failures.

Critical Stack

Protocol Details

RFC 2616
Stateless
TCP

Concepts

Common Exploit Vector
High Profile Attacks
Frequent Target

Abuse Tools

DirBuster
Burp
sqlmap

Exploitability

Abused frequently on both client side and server side assaults

Security Problems

sql injection, information disclosure, default apps

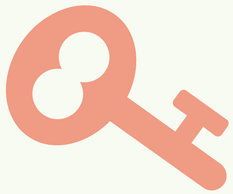
Hypertext Transfer Protocol

Key internet protocol frequently used for dynamic provisioning, service location; only some details documented

HTTP Bruteforce

Attacker queries server for common URIs.

May be used to look for default apps, CMSs, common names, etc.



HTTP Basic Auth

Attacker attempts brute force of protected web resources.

Hacking like it's 1996.

HTTP SQL Injection

Attacker abuses web resources to extract information from back end DB.

Common exploit vector.

TLS/SSL– Target 4, commonly used to transport…

Protocol Details

RFC 5246 + others
Stateful
TCP based

Concepts

Used to conceal traffic
Attacks Surface?
Little publicly known

Abuse Tools

sslscan
sslcaudit
tor, ssltrip

Exploitability

Typically used as a transport
Are you monitoring Gear?

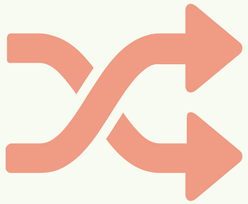
Security Problems

Running in / through your network

Transport Layer Security/ Secure Socket Layer

Key internet protocol frequently used for dynamic provisioning, service location; only some details documented

Critical Stack



TOR

Transport.

May be malicious.

Lucky 13

Latest in a series of high profile SSL/TLS Attacks.

This space is not nearly as safe as people assume.

SSL Attacks – Lucky 13 Attack

1

ssl_client_hello_count:	11
ssl_server_hello_count:	11
ssl_extension_count:	142
ssl_established_count:	11
ssl_alert_count:	0
ssl_ticket_handshake_count:	7
x509_certificate_count:	14
x509_extension_count:	0
x509_error_count:	0

2

ssl_client_hello_count:	12
ssl_server_hello_count:	12
ssl_extension_count:	128
ssl_established_count:	12
ssl_alert_count:	0
ssl_ticket_handshake_count:	6
x509_certificate_count:	21
x509_extension_count:	0
x509_error_count:	0

3

ssl_client_hello_count:	2
ssl_server_hello_count:	2
ssl_extension_count:	0
ssl_established_count:	2
ssl_alert_count:	0
ssl_ticket_handshake_count:	0
x509_certificate_count:	1
x509_extension_count:	0
x509_error_count:	0

4

ssl_client_hello_count:	4096
ssl_server_hello_count:	0
ssl_extension_count:	12288
ssl_established_count:	0
ssl_alert_count:	4
ssl_ticket_handshake_count:	0
x509_certificate_count:	0
x509_extension_count:	0
x509_error_count:	0

Thank you!