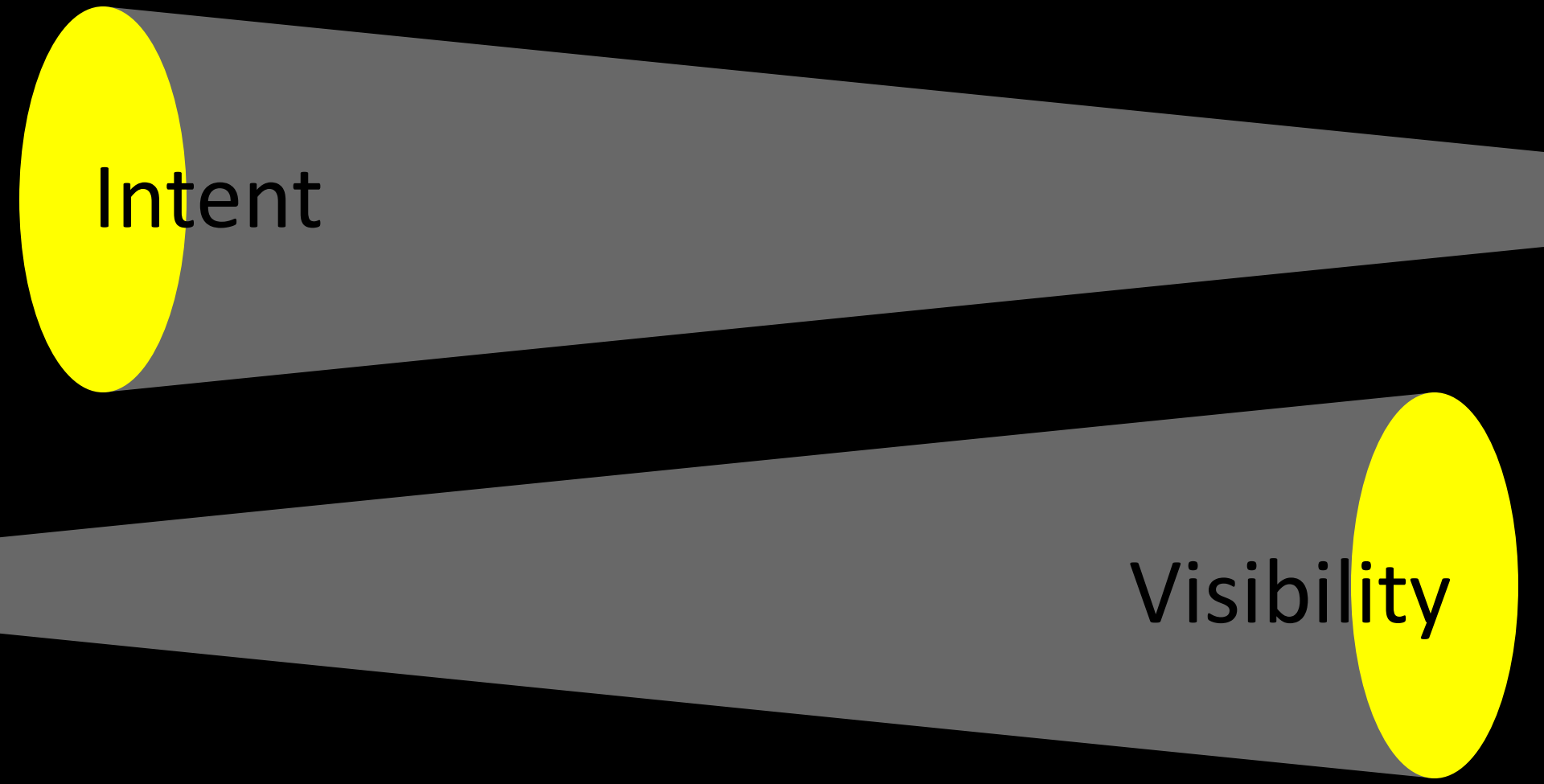
Missing the Obvious:
Network Security Monitoring for ICS

If ICS are so vulnerable, why haven't we seen more attacks?

We aren't looking!

Two Key Reasons



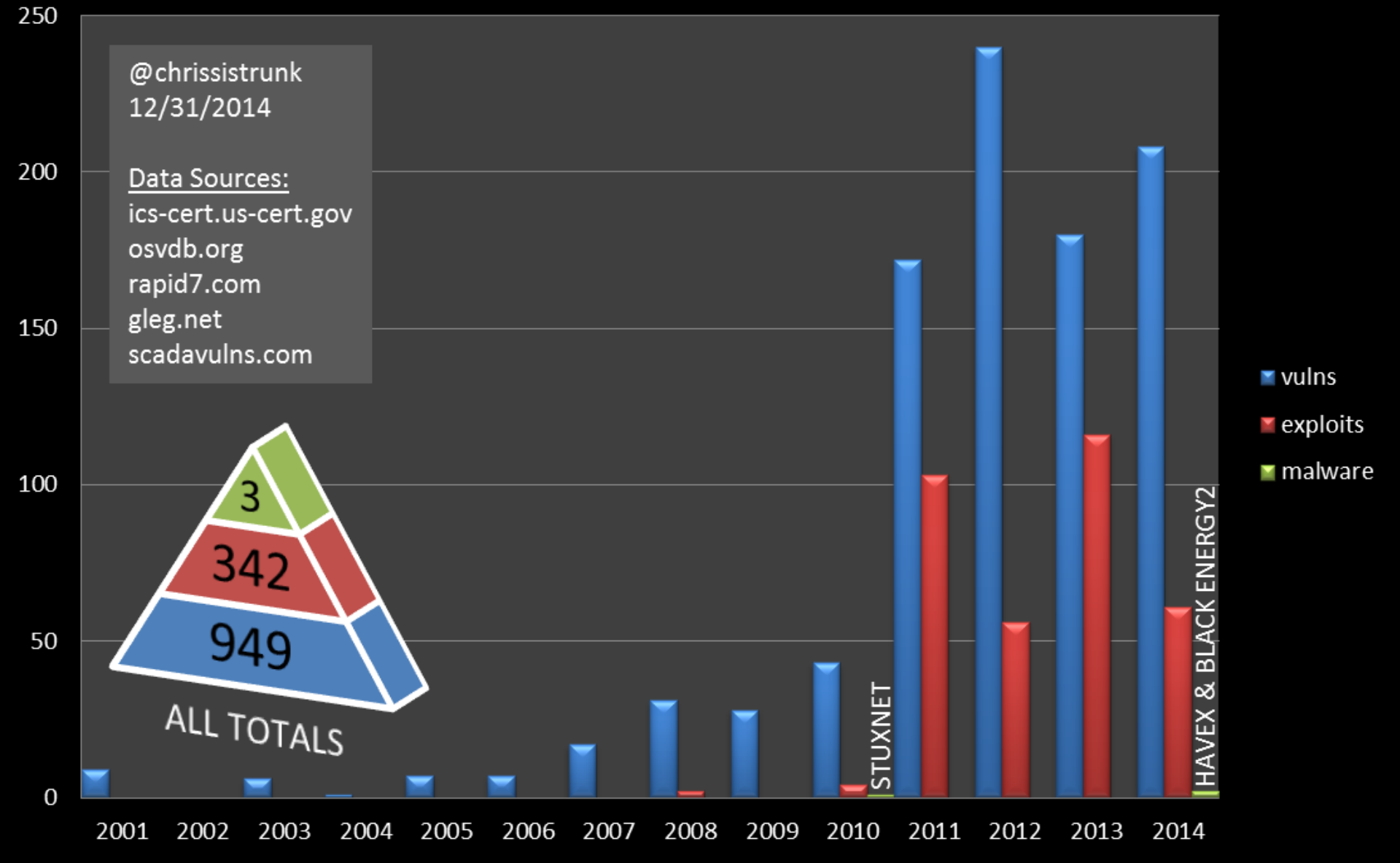
Intent

Why are targeted attacks different?

- It's a "Who" not a "What"
- Professional, organized, well-funded
- If you kick them out, they will return

Visibility

Public ICS Vulnerabilities Per Year



Now what?

- More Gov’t security regulations
- ICS security still lagging
- Breaches are inevitable
  - Attacks aren’t stopping
  - Every sector
  - Including ICS

What can we do to get ahead of this???

Network Security Monitoring

"The collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. NSM is a way to find intruders on your network and do something about them before they damage your enterprise."

- *The Practice of Network Security Monitoring*

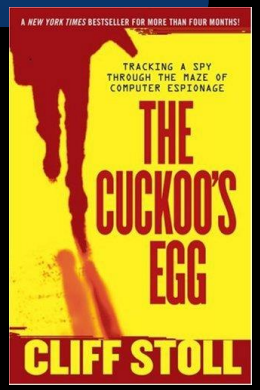
Network Security Monitoring

Invented in 1986, still in use today

Cliff Stoll

"Stalking the Wily Hacker"

1988



Todd Herberlein et al.

"A Network Security Monitor"

1990

US Air Force

Defense Information Systems Agency

Lawrence Livermore National Lab

Early 1990s

NetRanger

RealSecure

Snort

and many others

Late 1990s - early 2000s

Formal definition of NSM

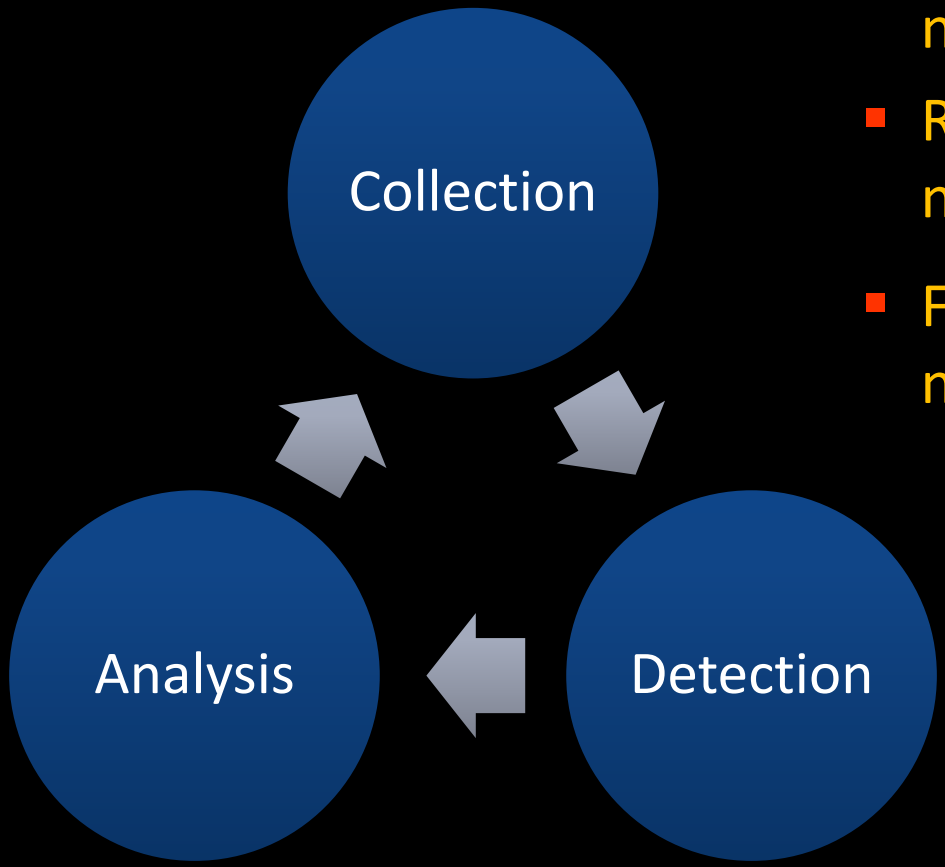
2002

Before we start looking…

We need

- At least one person (to watch and hunt)
- The right tools to collect and analyze the data

The NSM Cycle



- Model for action, based on network-derived data
- Requires people and process, not just technology
- Focuses on the adversary, not the vulnerability

Methods of Monitoring

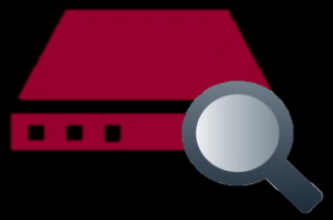
- **Network tap** – physical device which relays a copy of packets to an NSM sensor
- **SPAN or mirrored ports** – switch configuration which sends copies of packets to a separate port where NSM sensor can connect
- **Host NIC** – configured to watch all network traffic flowing on its segment (usually on NSM sensor)
- **Serial port tap** – physical device which relays serial traffic to another port, usually requires additional software to interpret data

Stratus Engineering

Fluke Networks

Types of Data Collected

- Full content data – unfiltered collection of packets
- Extracted content – data streams, files, Web pages, etc.
- Session data – conversation between nodes
- Transaction data – requests and replies between nodes
- Statistical data – description of traffic, such as protocol and volume
- Metadata – aspects of data, e.g. who owns this IP address
- Alert/log data – triggers from IDS tools, tracking user logins, etc.

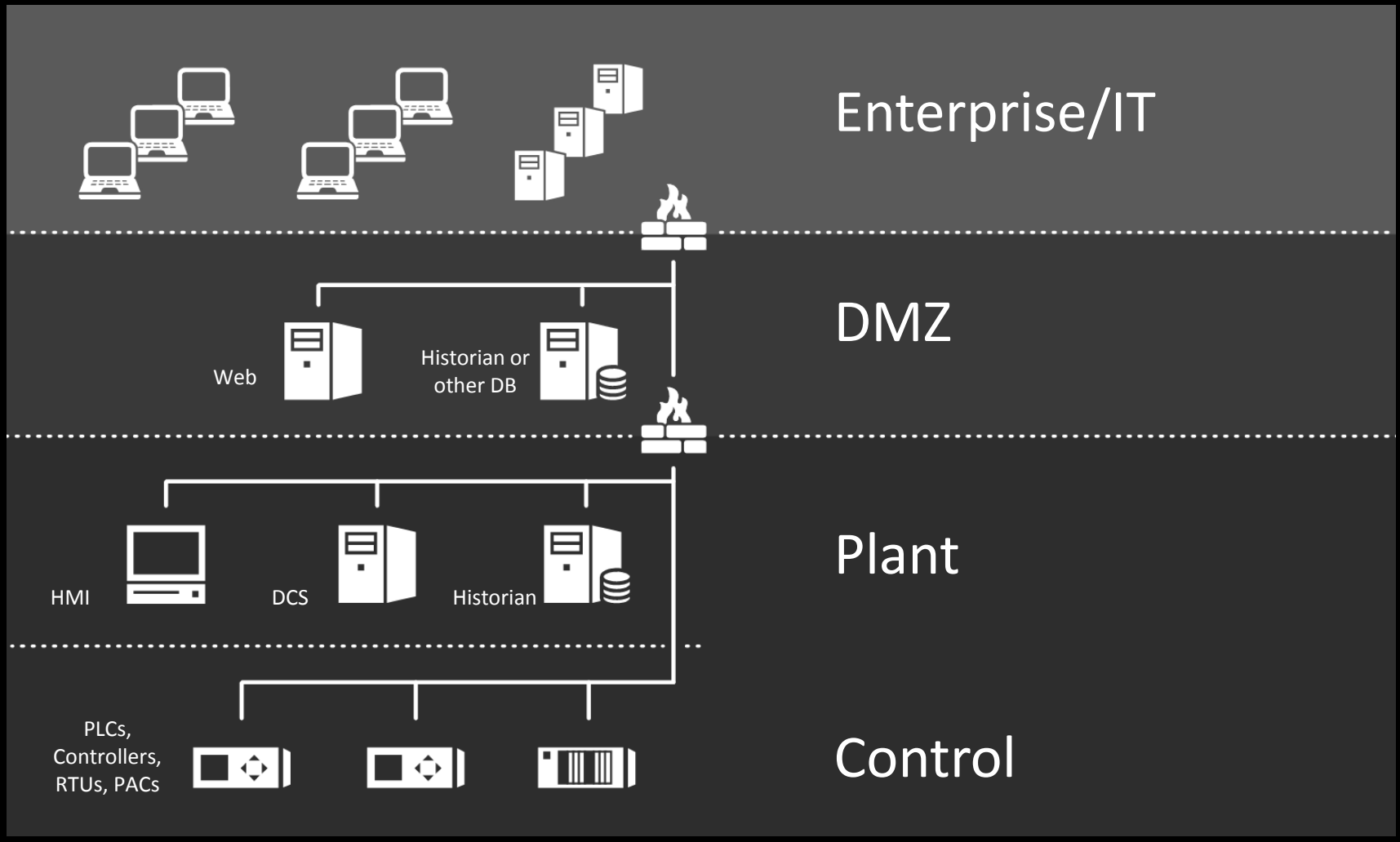


Difficulties for NSM

- Encrypted networks
- Widespread NAT
- Devices moving between network segments
- Extreme traffic volume
- Privacy concerns

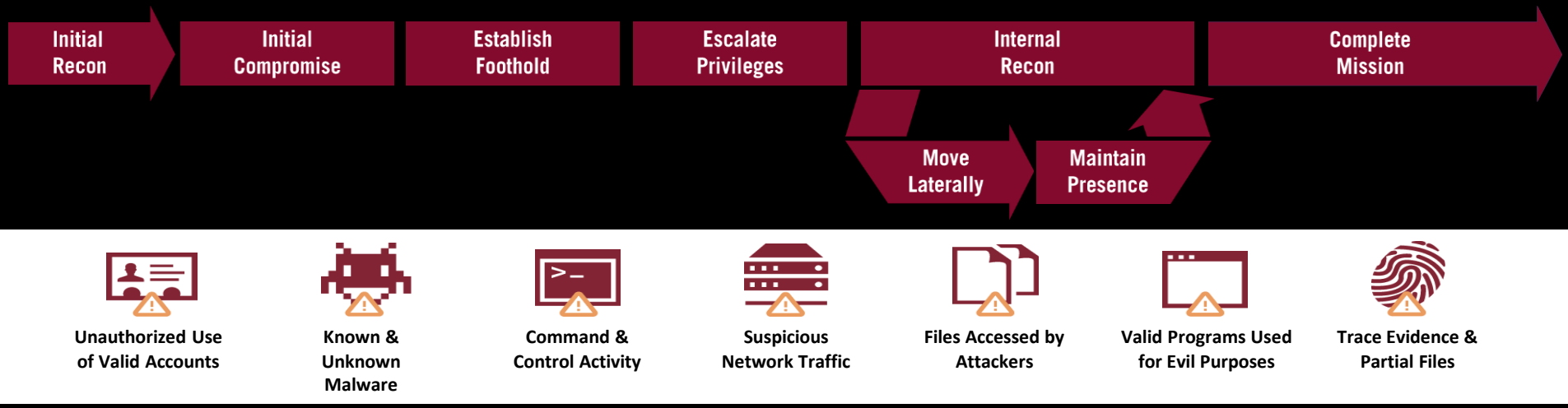
Issues that most ICS do not face!

Example ICS


Enterprise/IT
DMZ
Web
Historian or other DB
Plant
HMI
DCS
Historian
Control
PLCs, Controllers, RTUs, PACs

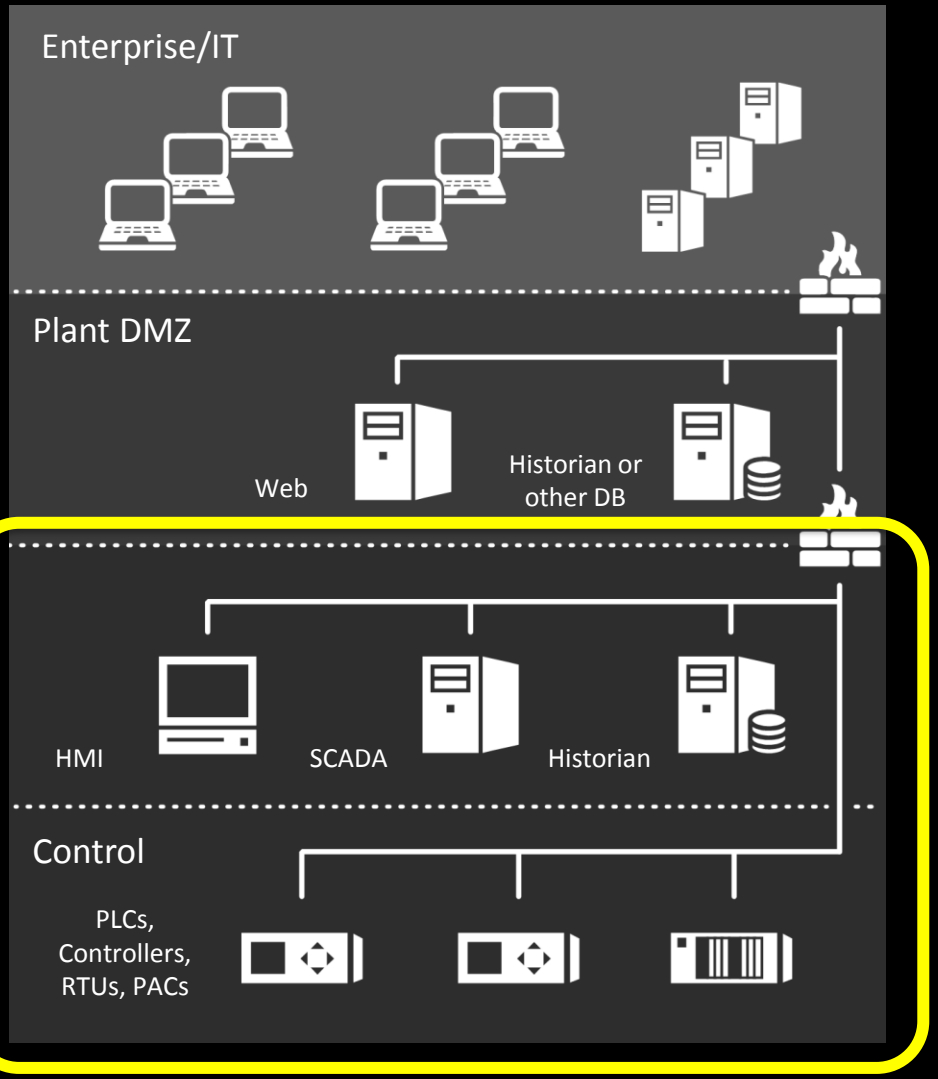
Anatomy of an Attack

While attackers often use malware to gain an initial foothold, they quickly move to other tactics to execute their attacks.



Over all Mandiant attack investigations, only a little more than half of victim computers have malware on them.

Attacker Objectives



Attacker's goals:

- Damage equipment
- Affect or steal process info
- Cause safety or compliance issue
- Pivot from vulnerable ICS to enterprise

Attacker's options:

- Gain physical access to an ICS host
- Gain remote access to an ICS host
- Compromise a highly-privileged client machine with access to the ICS network


Let’s do some NSM!

Let’s do some NSM!

Inquisitive mind

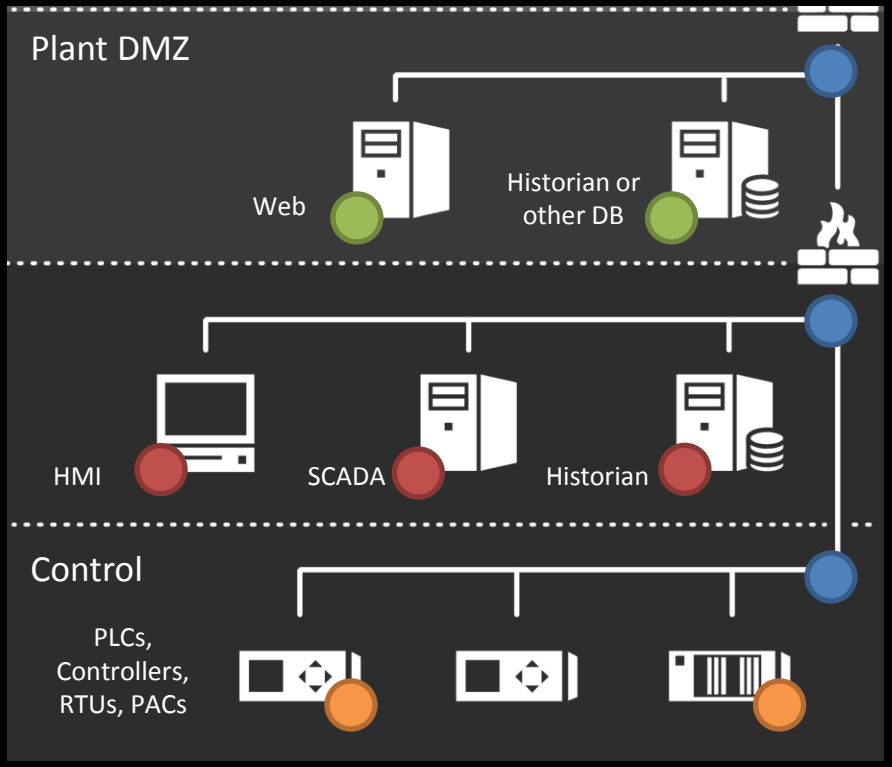
NSM hunting tools

NSM collection tools

Protection

NSM Collection

- Enterprise technology collectors
- Logs and/or Agent
- Network sensors
- Logs only



- Firewall Logs
- Session Data
- NIDS/HIDS Logs
- Full packet capture
- Windows Logs and syslog
- SNMP (CPU % etc.)
- Alerts from security agents (AV, whitelisting, etc.)

NSM Collection

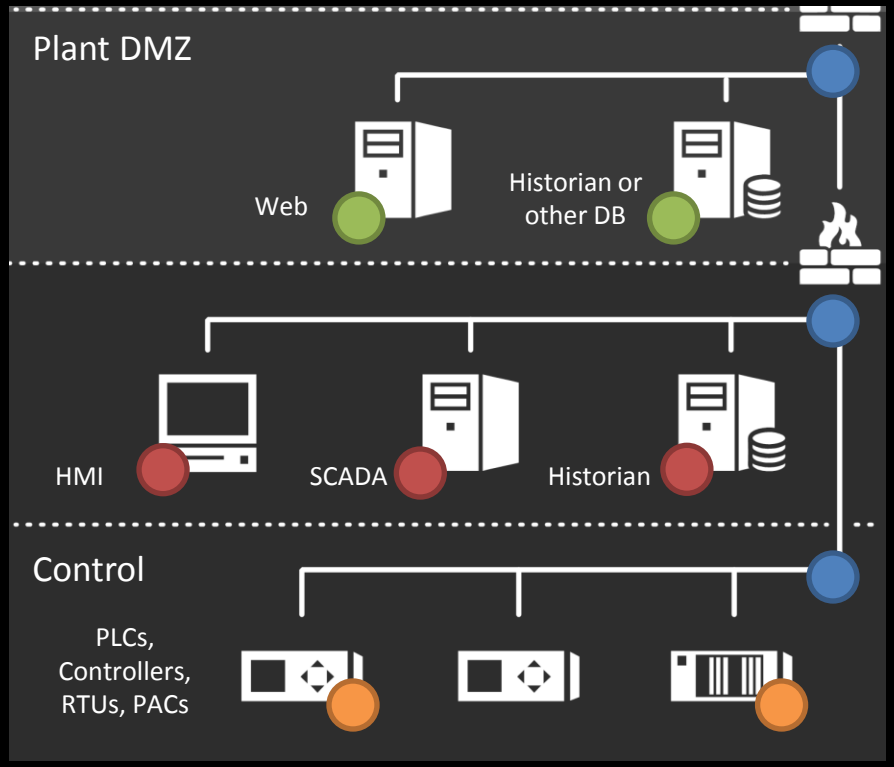
http://3.bp.blogspot.com/-B6PtheVJ9Jg/Uj4EErYhHdI/AAAAAAAAAFE/i_2dk9emrp4/s1600/Deer+tracks.jpg

What are we looking for?

- Exceptions from baseline (e.g. A talks to B but never C)
- “Top Talkers”
- Unexpected connectivity (to Internet, Business network)
- Known malicious IPs and domains
- Logins using default accounts
- Error messages that could correlate to vulnerabilities
- Unusual system and firewall log entries
- Host-based IDS or other security system alerts
- Unexpected file and firmware updates
- Antivirus alerts
- And others….

NSM Detection & “Hunting”

Analyst looks at detected anomalies or alerts then escalates to IR



- IDS alerts
- Anomaly detection
- Firmware updates, other commands
- Login with default credentials
- High CPU or network bandwidth
- Door alarms when nobody is supposed to be working
- Devices going off-line or behaving strangely

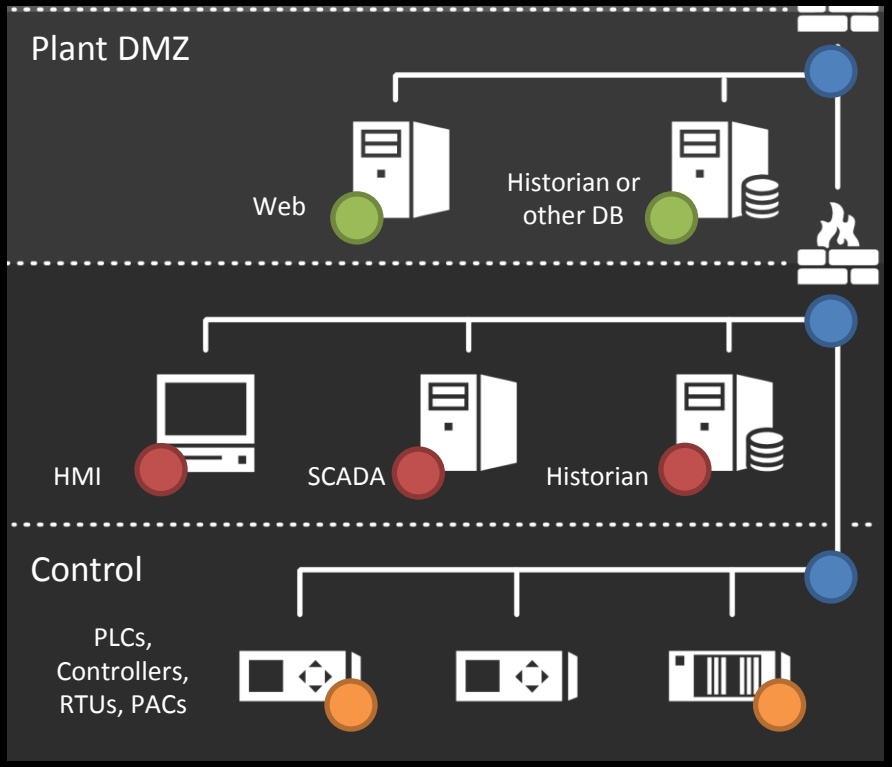
NSM Detection

http://www.jimyuskavitchphotography.com/data/photos/56_1wolf_track4.jpg

http://www.buckmasters.com

NSM Analysis

Incident responders analyze the detected anomalies to find evil



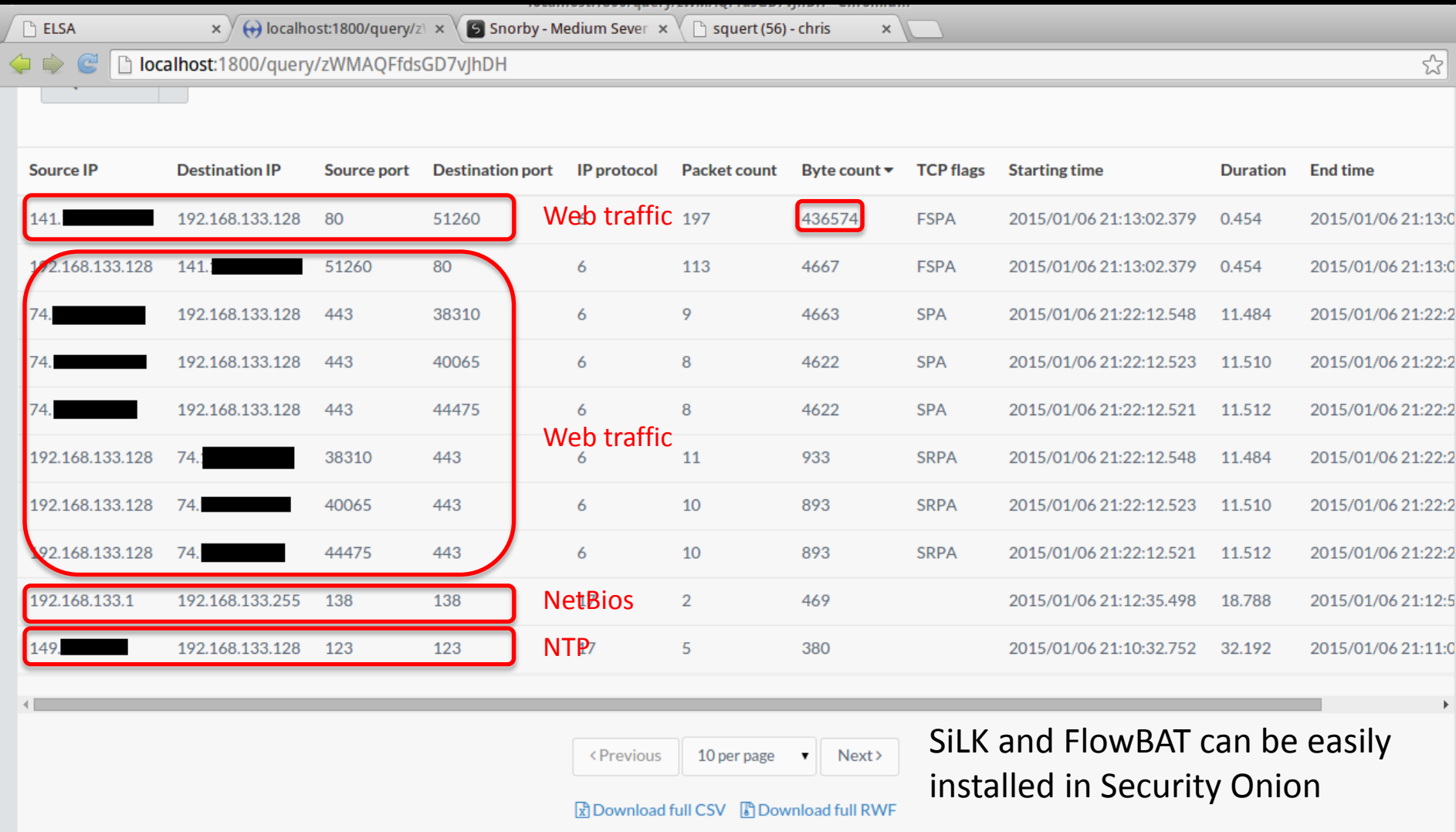
- Application exploitation
- Third-party connections (ex. ICCP or vendor access)
- ICS-specific communication protocol attacks (ex. Modbus, DNP3, Profinet, EtherNet/IP)
- Remote access exploitation
- Direct network access due to poor physical security
- USB-delivered malware

NSM Analysis

ICS NSM Examples

Session Data "Top Talkers"

FlowBAT characterizes Session Data, showing which nodes have the most traffic



Source IP	Destination IP	Source port	Destination port	IP protocol	Packet count	Byte count	TCP flags	Starting time	Duration	End time
141.[redacted]	192.168.133.128	80	51260	6	197	436574	FSPA	2015/01/06 21:13:02.379	0.454	2015/01/06 21:13:0
192.168.133.128	141.[redacted]	51260	80	6	113	4667	FSPA	2015/01/06 21:13:02.379	0.454	2015/01/06 21:13:0
74.[redacted]	192.168.133.128	443	38310	6	9	4663	SPA	2015/01/06 21:22:12.548	11.484	2015/01/06 21:22:2
74.[redacted]	192.168.133.128	443	40065	6	8	4622	SPA	2015/01/06 21:22:12.523	11.510	2015/01/06 21:22:2
74.[redacted]	192.168.133.128	443	44475	6	8	4622	SPA	2015/01/06 21:22:12.521	11.512	2015/01/06 21:22:2
192.168.133.128	74.[redacted]	38310	443	6	11	933	SRPA	2015/01/06 21:22:12.548	11.484	2015/01/06 21:22:2
192.168.133.128	74.[redacted]	40065	443	6	10	893	SRPA	2015/01/06 21:22:12.523	11.510	2015/01/06 21:22:2
192.168.133.128	74.[redacted]	44475	443	6	10	893	SRPA	2015/01/06 21:22:12.521	11.512	2015/01/06 21:22:2
192.168.133.1	192.168.133.255	138	138	17	2	469		2015/01/06 21:12:35.498	18.788	2015/01/06 21:12:5
149.[redacted]	192.168.133.128	123	123	17	5	380		2015/01/06 21:10:32.752	32.192	2015/01/06 21:11:0

Web traffic

Web traffic

NetBios

NTP

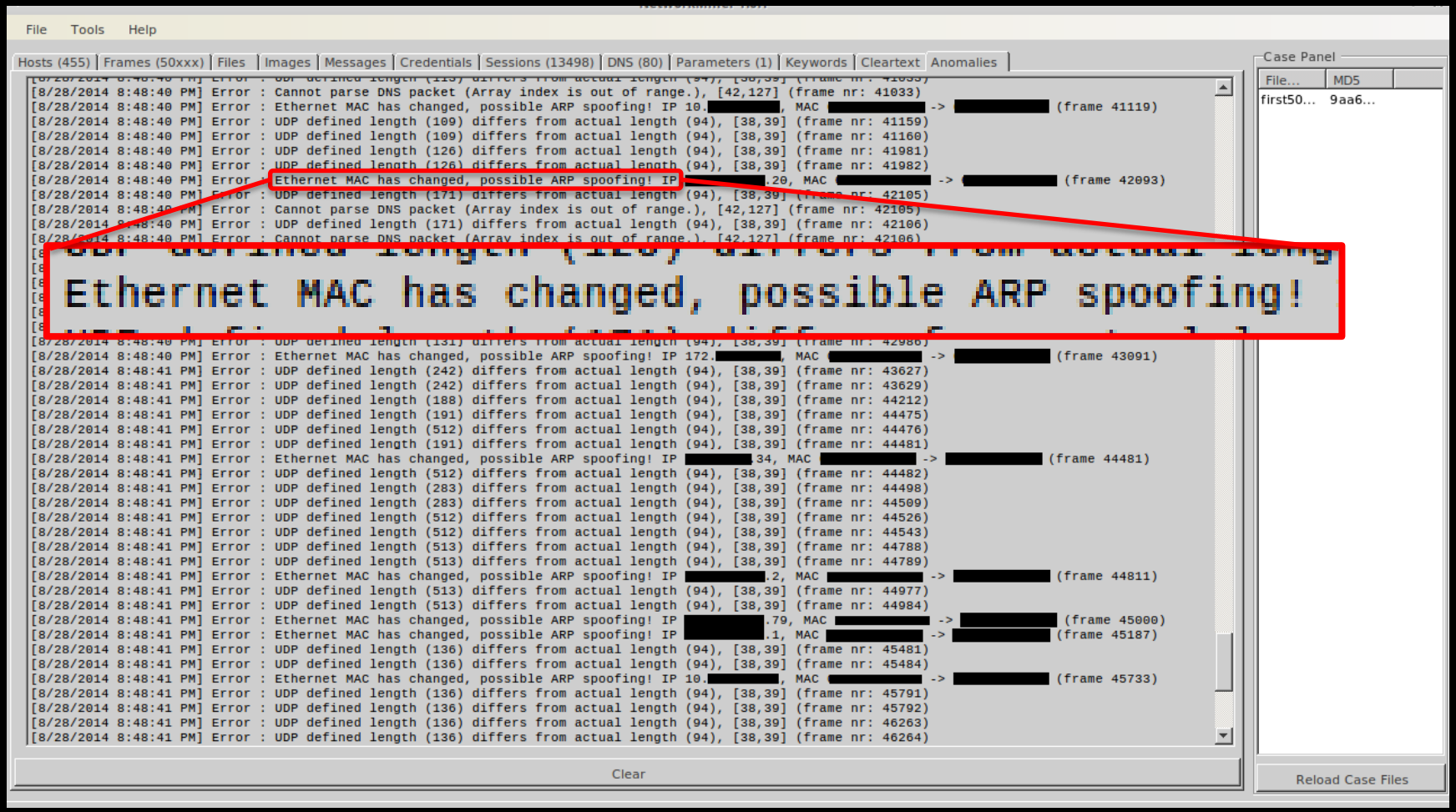
‹ Previous | 10 per page | Next ›

Download full CSV | Download full RWF

SiLK and FlowBAT can be easily installed in Security Onion

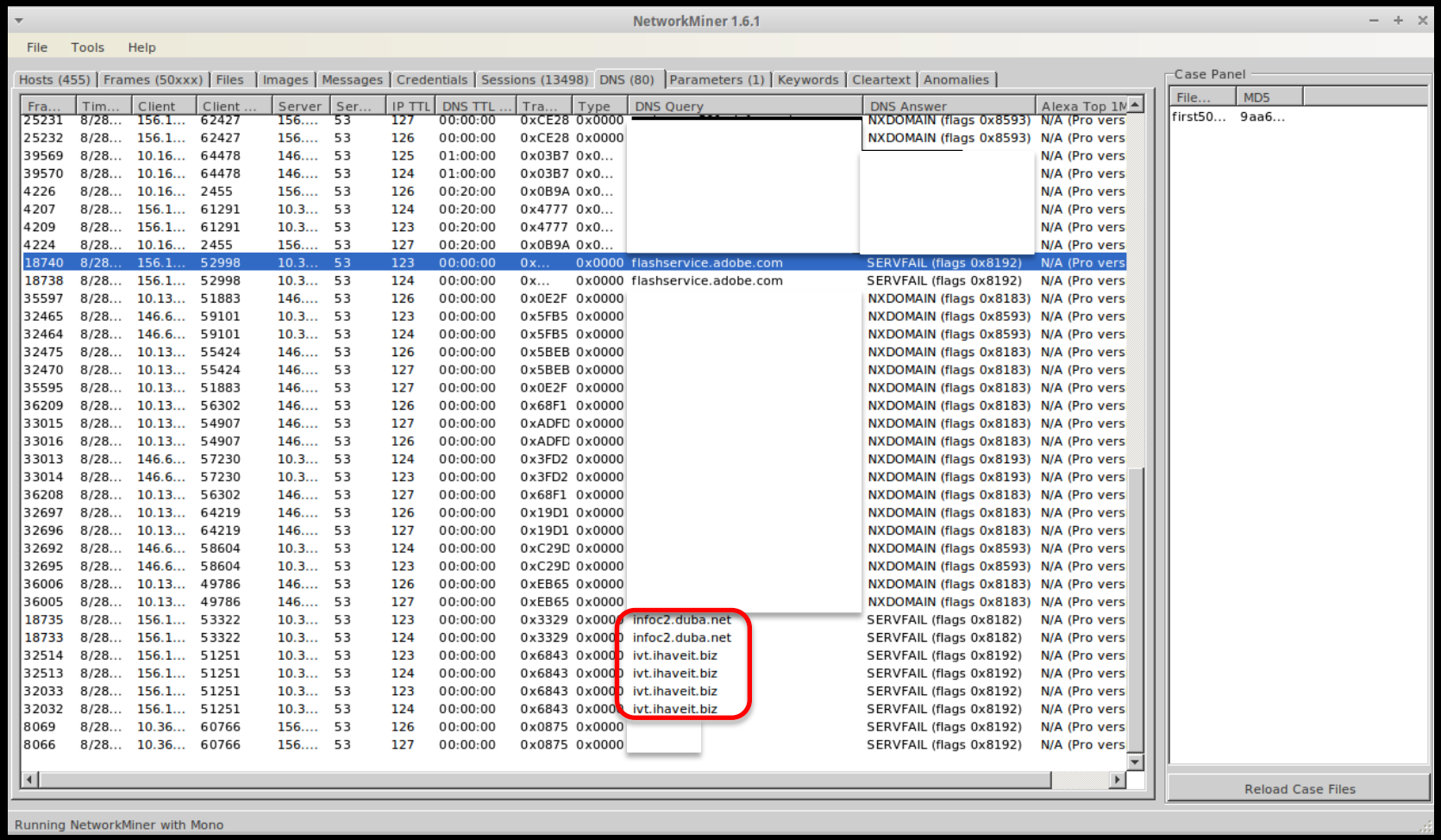
Pcap Analysis for anomalies

NetworkMiner can find potential ARP spoofing (as well as many other indicators)



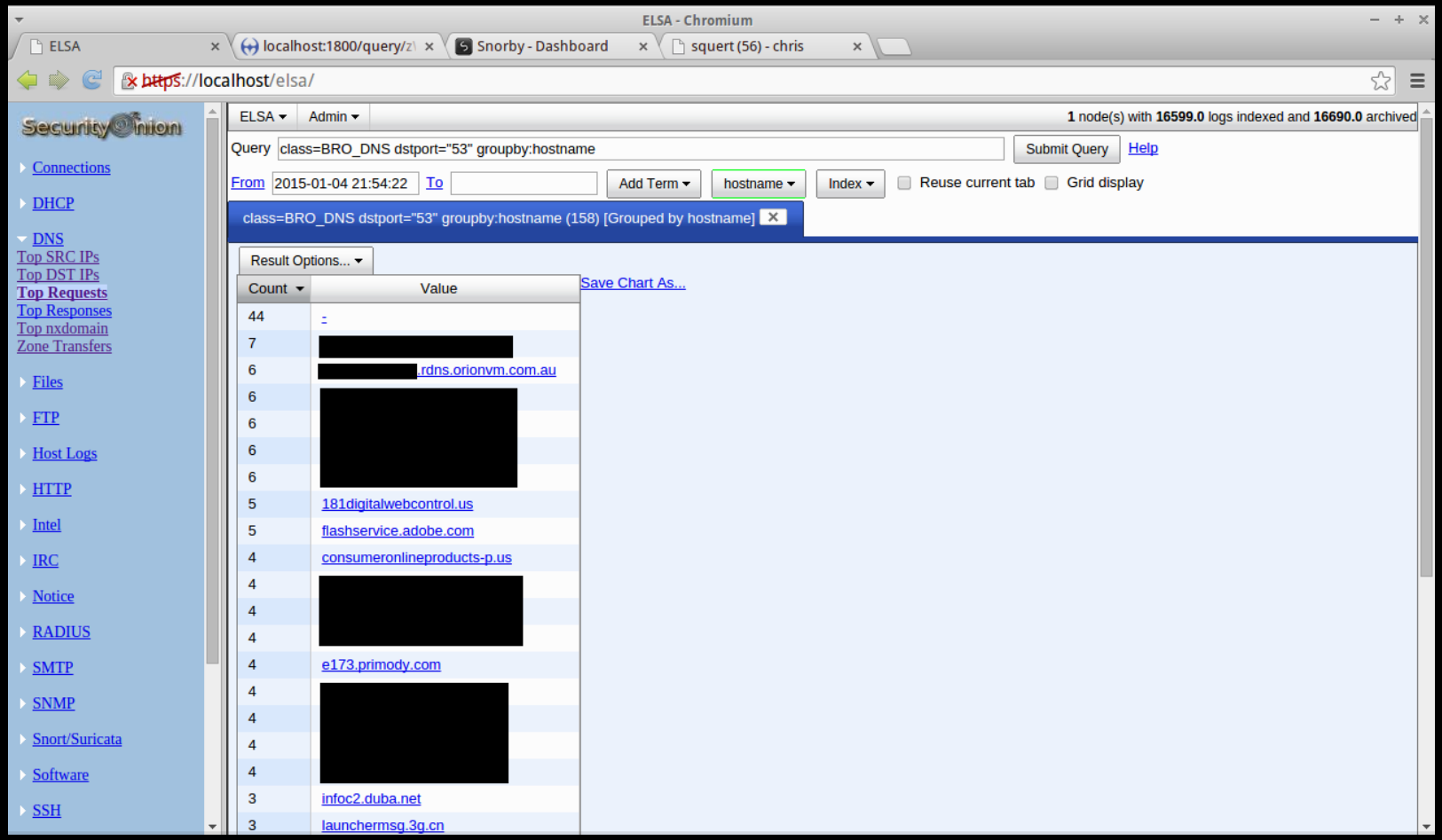
Pcaps - Abnormal DNS Traffic

NetworkMiner sees“strange” DNS requests originating from within the ICS



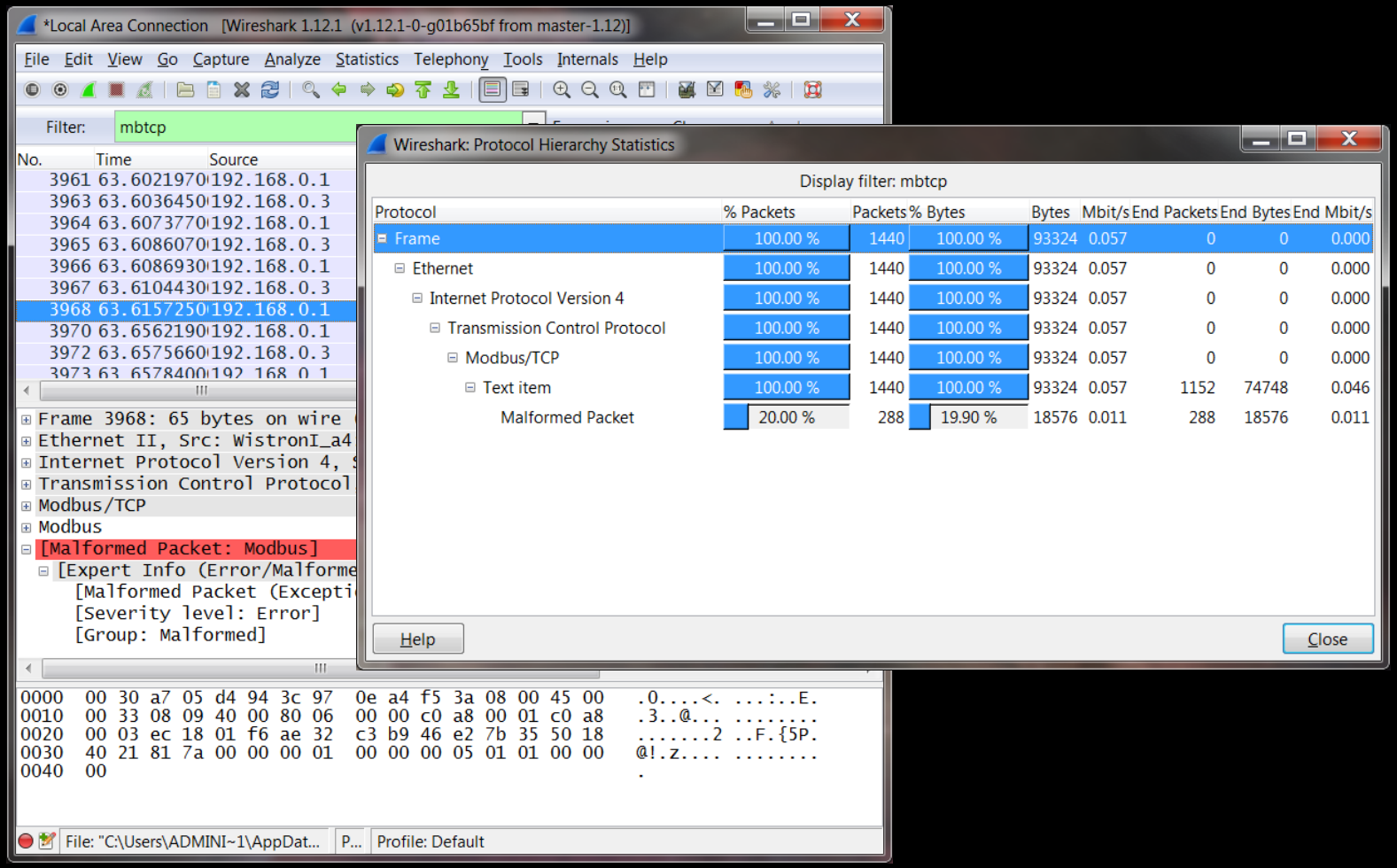
IDS alerts - Abnormal DNS Traffic

DNS requests shown in the Bro IDS log in ELSA



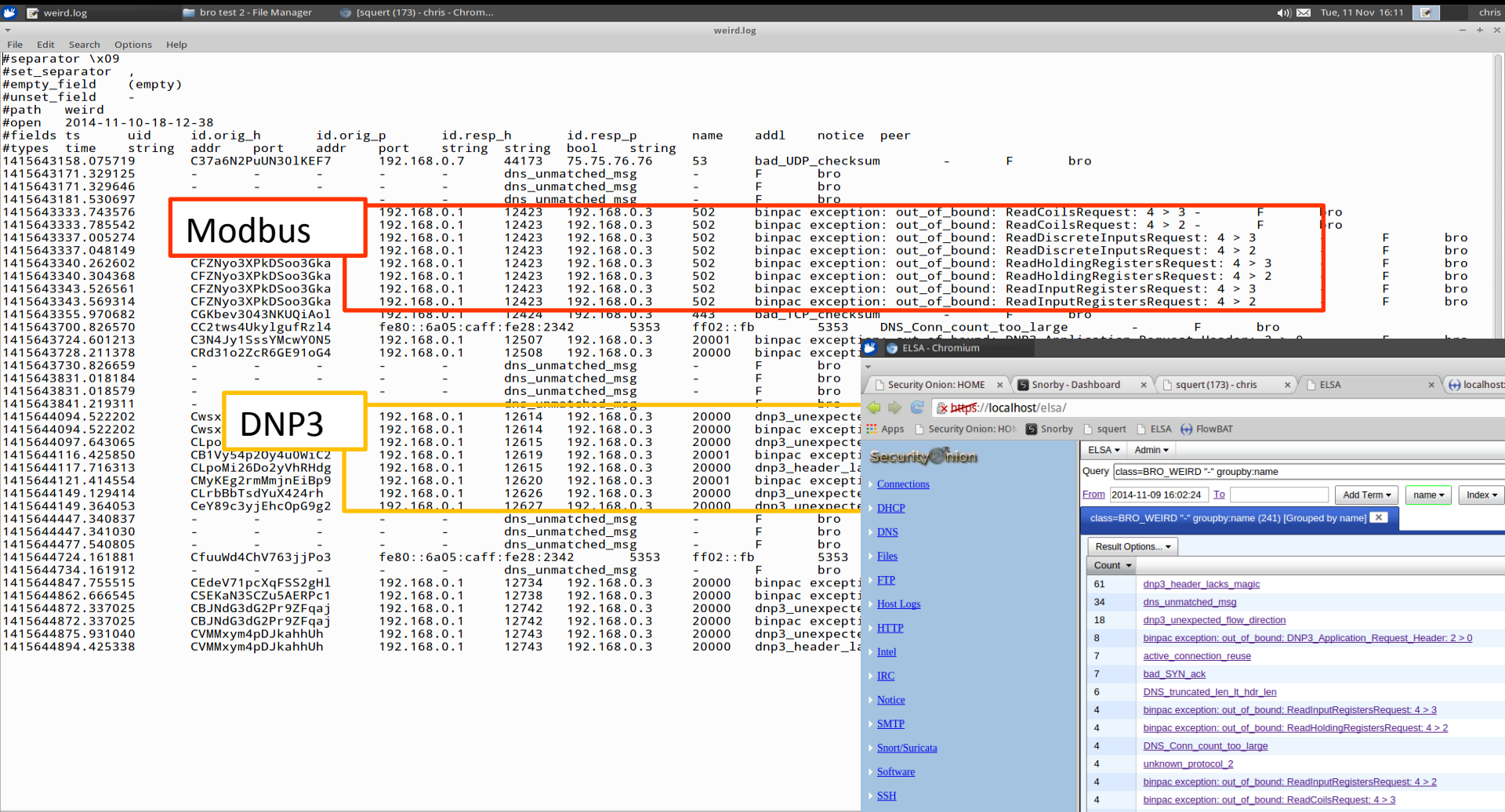
Pcaps - Malformed Modbus

Deep packet inspection of Modbus by Wireshark



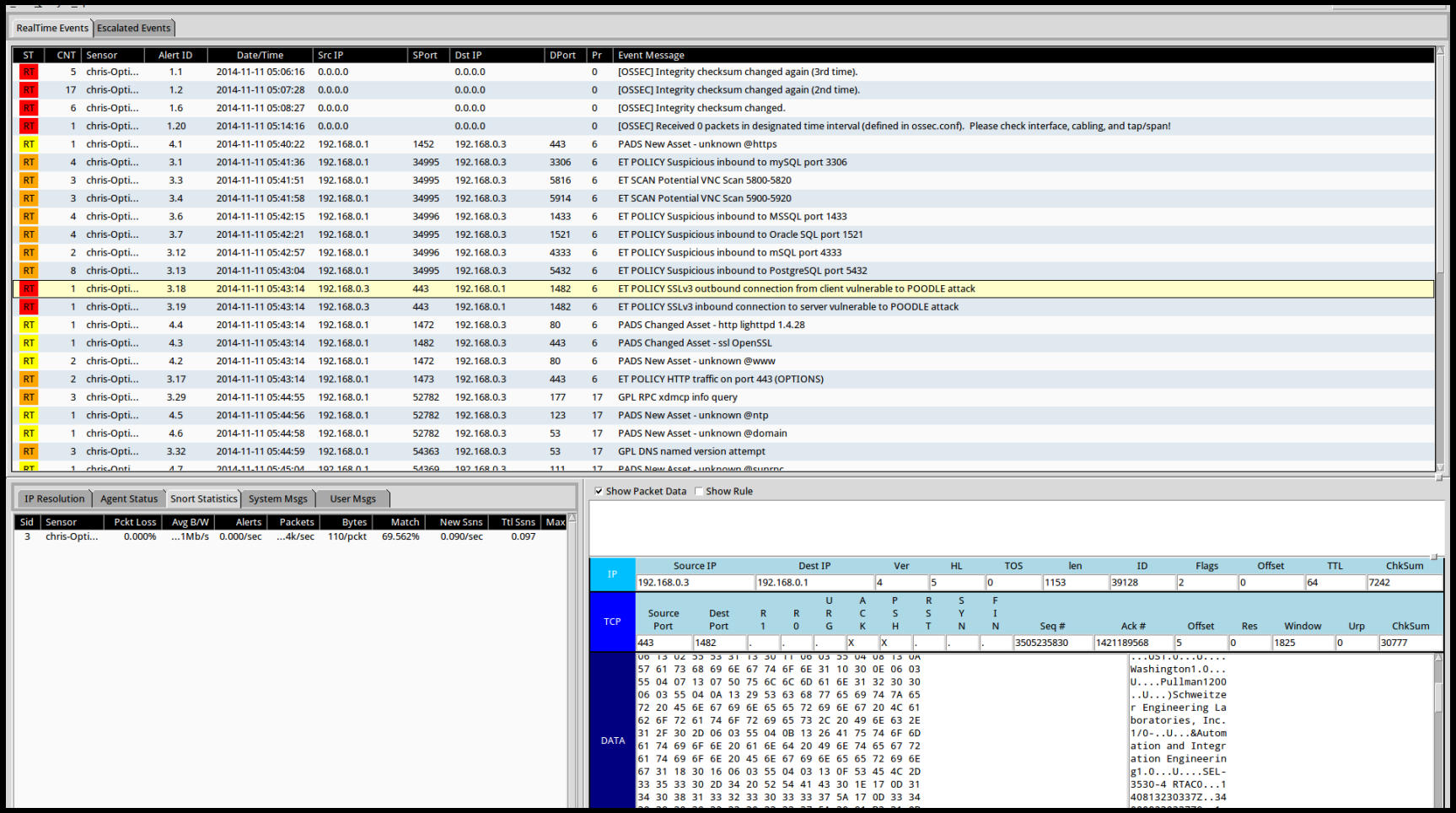
IDS Logs

Bro IDS parses Modbus and DNP3 packets, ELSA consolidates Bro logs



IDS GUIs

Alerts in Sguil of scanning activity



RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	5	chris-Opti...	1.1	2014-11-11 05:06:16	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed again (3rd time).
RT	17	chris-Opti...	1.2	2014-11-11 05:07:28	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed again (2nd time).
RT	6	chris-Opti...	1.6	2014-11-11 05:08:27	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.
RT	1	chris-Opti...	1.20	2014-11-11 05:14:16	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!
RT	1	chris-Opti...	4.1	2014-11-11 05:40:22	192.168.0.1	1452	192.168.0.3	443	6	PADS New Asset - unknown @https
RT	4	chris-Opti...	3.1	2014-11-11 05:41:36	192.168.0.1	34995	192.168.0.3	3306	6	ET POLICY Suspicious inbound to mySQL port 3306
RT	3	chris-Opti...	3.3	2014-11-11 05:41:51	192.168.0.1	34995	192.168.0.3	5816	6	ET SCAN Potential VNC Scan 5800-5820
RT	3	chris-Opti...	3.4	2014-11-11 05:41:58	192.168.0.1	34995	192.168.0.3	5914	6	ET SCAN Potential VNC Scan 5900-5920
RT	4	chris-Opti...	3.6	2014-11-11 05:42:15	192.168.0.1	34996	192.168.0.3	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	4	chris-Opti...	3.7	2014-11-11 05:42:21	192.168.0.1	34995	192.168.0.3	1521	6	ET POLICY Suspicious inbound to Oracle SQL port 1521
RT	2	chris-Opti...	3.12	2014-11-11 05:42:57	192.168.0.1	34996	192.168.0.3	4333	6	ET POLICY Suspicious inbound to mSQL port 4333
RT	8	chris-Opti...	3.13	2014-11-11 05:43:04	192.168.0.1	34995	192.168.0.3	5432	6	ET POLICY Suspicious inbound to PostgreSQL port 5432
RT	1	chris-Opti...	3.18	2014-11-11 05:43:14	192.168.0.3	443	192.168.0.1	1482	6	ET POLICY SSLv3 outbound connection from client vulnerable to POODLE attack
RT	1	chris-Opti...	3.19	2014-11-11 05:43:14	192.168.0.3	443	192.168.0.1	1482	6	ET POLICY SSLv3 inbound connection to server vulnerable to POODLE attack
RT	1	chris-Opti...	4.4	2014-11-11 05:43:14	192.168.0.1	1472	192.168.0.3	80	6	PADS Changed Asset - http lighttpd 1.4.28
RT	1	chris-Opti...	4.3	2014-11-11 05:43:14	192.168.0.1	1482	192.168.0.3	443	6	PADS Changed Asset - ssl OpenSSL
RT	2	chris-Opti...	4.2	2014-11-11 05:43:14	192.168.0.1	1472	192.168.0.3	80	6	PADS New Asset - unknown @www
RT	2	chris-Opti...	3.17	2014-11-11 05:43:14	192.168.0.1	1473	192.168.0.3	443	6	ET POLICY HTTP traffic on port 443 (OPTIONS)
RT	3	chris-Opti...	3.29	2014-11-11 05:44:55	192.168.0.1	52782	192.168.0.3	177	17	GPL RPC xdmcp info query
RT	1	chris-Opti...	4.5	2014-11-11 05:44:56	192.168.0.1	52782	192.168.0.3	123	17	PADS New Asset - unknown @ntp
RT	1	chris-Opti...	4.6	2014-11-11 05:44:58	192.168.0.1	52782	192.168.0.3	53	17	PADS New Asset - unknown @domain
RT	3	chris-Opti...	3.32	2014-11-11 05:44:59	192.168.0.1	54363	192.168.0.3	53	17	GPL DNS named version attempt
RT	1	chris-Opti...	4.7	2014-11-11 05:45:04	192.168.0.1	54369	192.168.0.3	111	17	PADS New Asset - unknown @sunrpc

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

Sid	Sensor	Pckt Loss	Avg B/W	Alerts	Packets	Bytes	Match	New Ssns	Ttl Ssns	Max
3	chris-Opti...	0.000%	...1Mb/s	0.000/sec	...4k/sec	110/pckt	69.562%	0.090/sec	0.097	

Show Packet Data | Show Rule

	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	192.168.0.3	192.168.0.1	4	5	0	1153	39128	2	0	64	7242

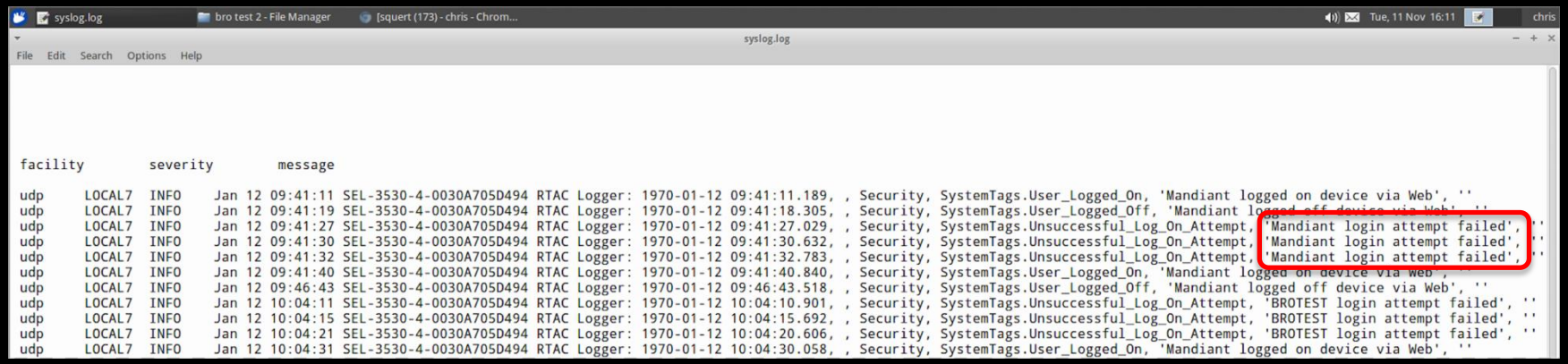
	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	443	1482	.	.	.	X	X	.	.	.	3505235830	1421189568	5	0	1825	0	30777

DATA

```
06 13 02 55 55 31 13 30 11 06 03 55 04 08 13 0A   ...UUT.0...U....
57 61 73 68 69 6E 67 74 6F 6E 31 10 30 0E 06 03   Washington1.0...
55 04 07 13 07 50 75 6C 6C 6D 61 6E 31 32 30 30   U....Pullman1200
06 03 55 04 0A 13 29 53 63 68 77 65 69 74 7A 65   ..U...)Schweitze
72 20 45 6E 67 69 6E 65 65 72 69 6E 67 20 4C 61   r Engineering La
62 6F 72 61 74 6F 72 69 65 73 2C 20 49 6E 63 2E   boratories, Inc.
31 2F 30 2D 06 03 55 04 0B 13 26 41 75 74 6F 6D   1/0-..U...&Autom
61 74 69 6F 6E 20 61 6E 64 20 49 6E 74 65 67 72   ation and Integr
61 74 69 6F 6E 20 45 6E 67 69 6E 65 65 72 69 6E   ation Engineerin
67 31 18 30 16 06 03 55 04 03 13 0F 53 45 4C 2D   g1.0...U....SEL-
33 35 33 30 2D 34 20 52 54 41 43 30 1E 17 0D 31   3530-4 RTAC0...1
34 30 38 31 33 32 33 30 33 33 37 5A 17 0D 33 34   40813230337Z..34
```

Syslog

Syslog can be configured to send to a NSM sensor or detected in network traffic if sent elsewhere. This is the Bro IDS Log for Syslog.

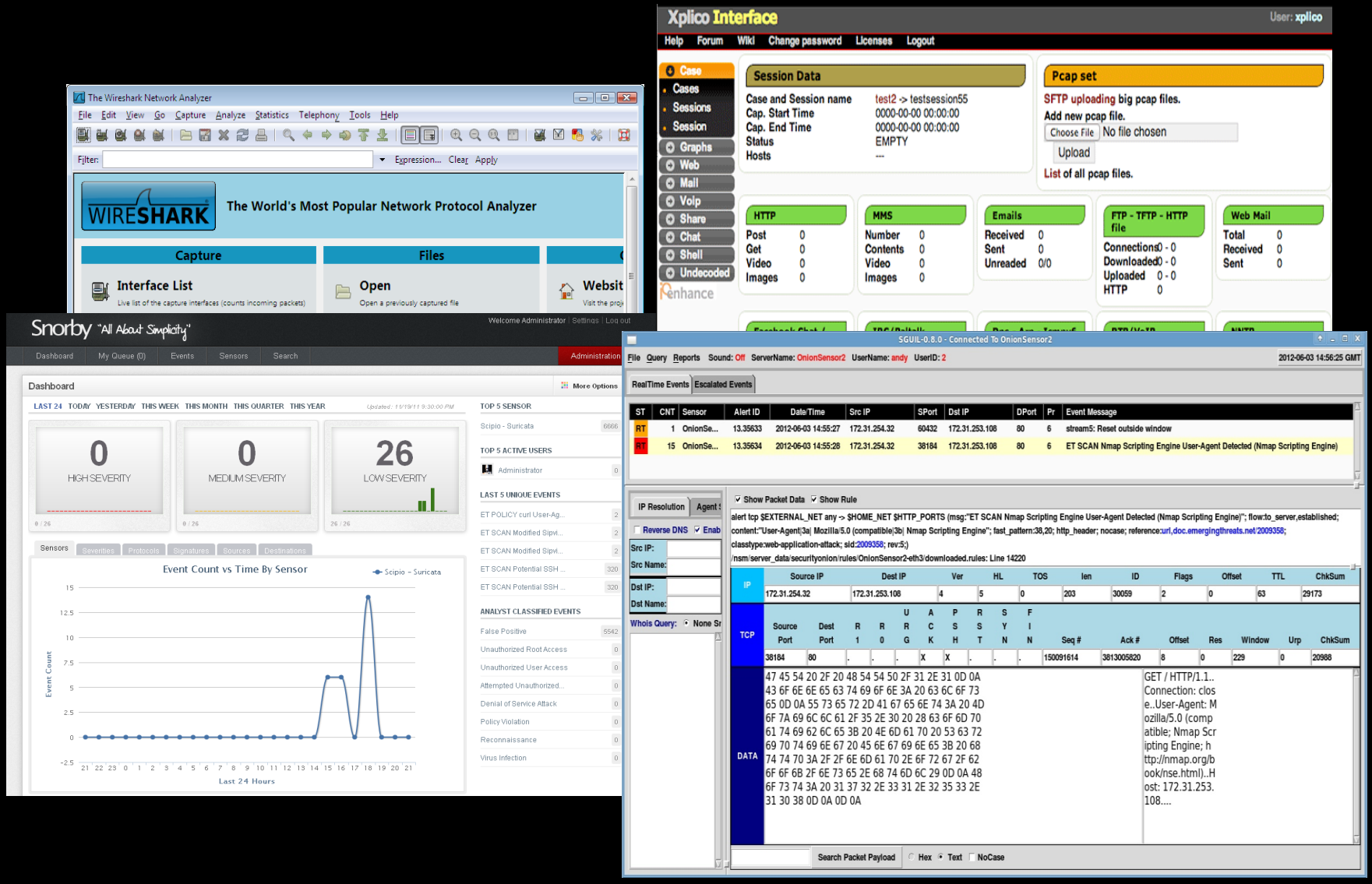


NSM Tools for the 7 Data Types

Security Onion Linux distribution
  - Easy to install and lots of documentation
- Full packet capture – Tcpdump/Wireshark/NetworkMiner
- Extracted content – Xplico/NetworkMiner
- Session data – Bro/FlowBAT
- Transaction data – Bro
- Statistical data – Capinfos/Wireshark
- Metadata – ELSA (Whois)
- Alert data – Snort, Suricata, Sguil, Snorby

Peel Back the Layers of Your Network

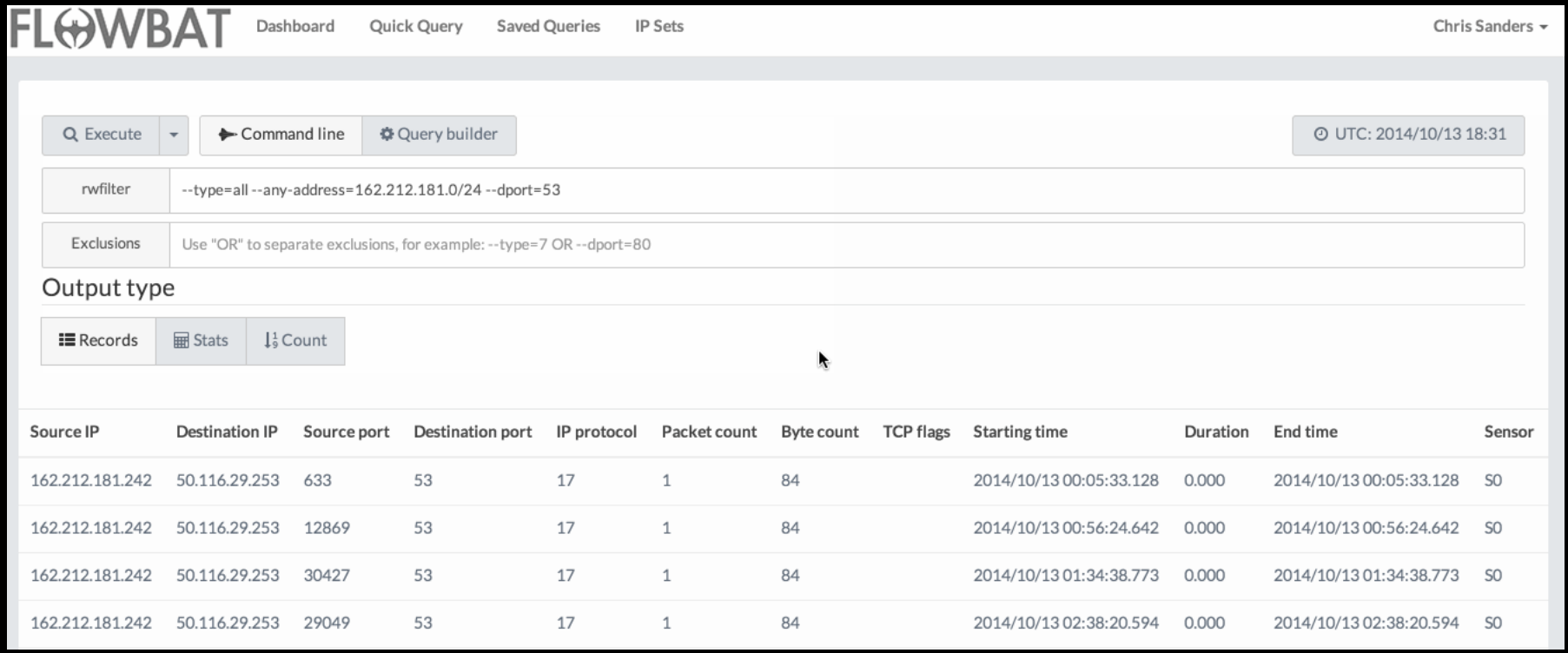
Security Onion Tools



NetFlow Tools

SiLK & FlowBAT

- Install on Security Onion with 2 scripts
- www.flowbat.com



Source IP	Destination IP	Source port	Destination port	IP protocol	Packet count	Byte count	TCP flags	Starting time	Duration	End time	Sensor
162.212.181.242	50.116.29.253	633	53	17	1	84		2014/10/13 00:05:33.128	0.000	2014/10/13 00:05:33.128	S0
162.212.181.242	50.116.29.253	12869	53	17	1	84		2014/10/13 00:56:24.642	0.000	2014/10/13 00:56:24.642	S0
162.212.181.242	50.116.29.253	30427	53	17	1	84		2014/10/13 01:34:38.773	0.000	2014/10/13 01:34:38.773	S0
162.212.181.242	50.116.29.253	29049	53	17	1	84		2014/10/13 02:38:20.594	0.000	2014/10/13 02:38:20.594	S0

Security Onion Implementation

- Test in a lab first
- Select suitable hardware platform
  - More RAM is better
  - Bigger hard drive is better (longer retention)
- Mirrored/SPAN port on router/switch or a good network tap
- Select proper placement of SO sensor
  - *The Practice of Network Security Monitoring*
  - *Applied Network Security Monitoring*
- Work with the right stakeholders if placing in production

NSM References/Resources

- *The Cuckoo's Egg* by Cliff Stoll
  https://www.youtube.com/watch?v=EcKxaq1FTac
  1-hour NOVA Special (1990)
- *The Practice of Network Security Monitoring*
  by Richard Bejtlich
  http://www.nostarch.com/nsm
- *Applied Network Security Monitoring*
  by Chris Sanders & Jason Smith
  http://www.appliednsm.com/
- The NSM Wiki http://nsmwiki.org
- http://securityonion.net

Takeaways

- ✓You can implement NSM in ICS today – without impacting your operations
- ✓There are free tools available to help you start looking at your ICS and hunting for evil

People…

…the most important part of NSM!

- Gigabytes of data and 1000s of IDS alerts are useless without interpretation
- Analyze data collected to understand what's normal – and what's not
- Identify adversary TTPs and act to disrupt them

<u>Remember</u>

Adversaries are a "Who", not a "What"

Find Evil

chris.sistrunk@mandiant.com
@chrissistrunk
robert.caldwell@mandiant.com
@robac3