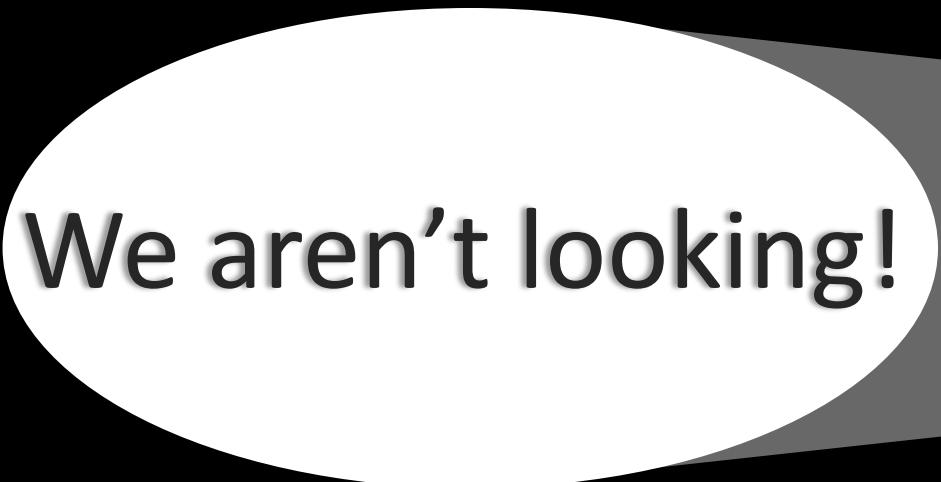




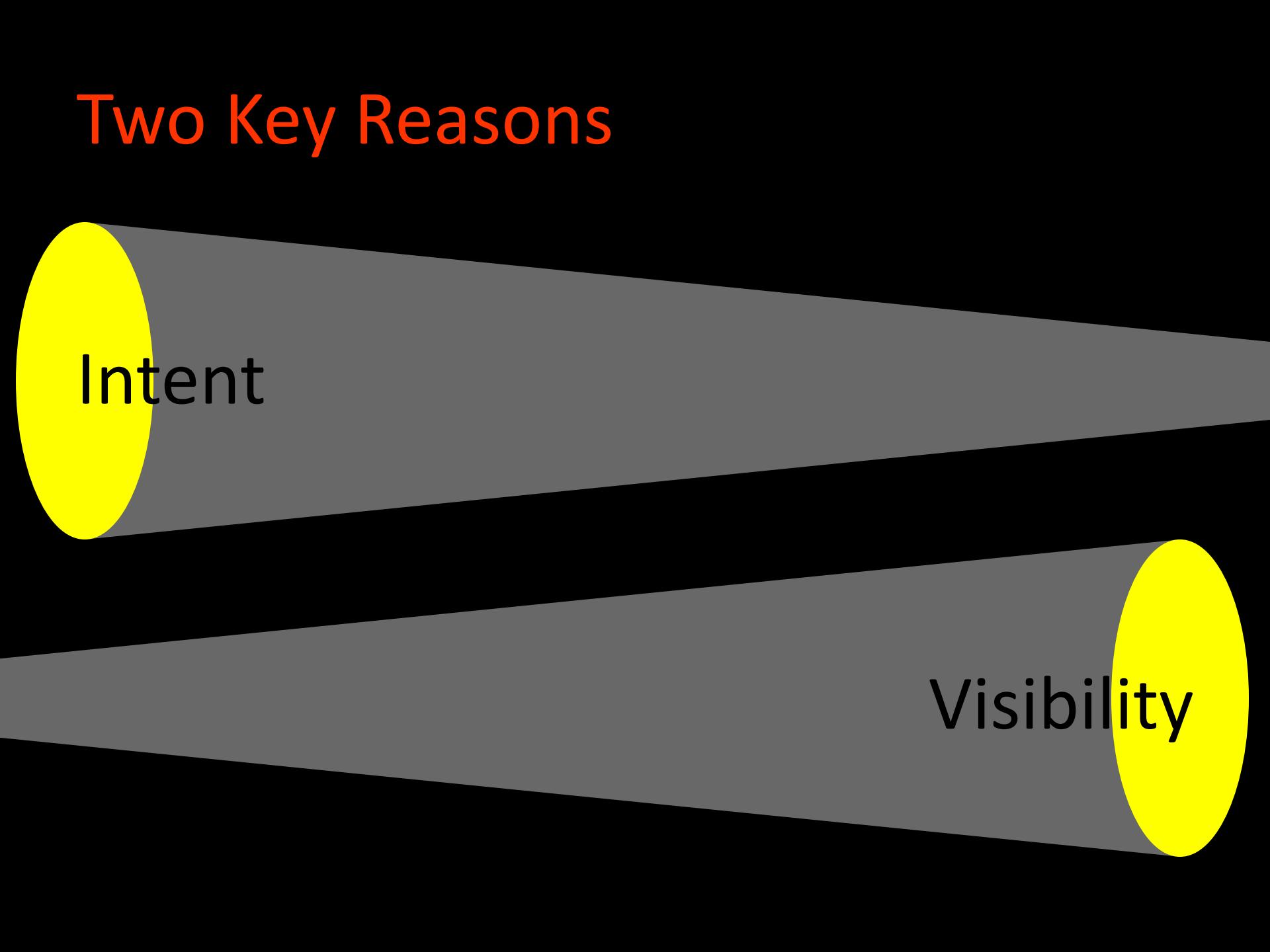
Missing the Obvious: Network Security Monitoring for ICS

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



We aren't looking!

Two Key Reasons



Intent

Visibility

Intent

Why are targeted attacks different?

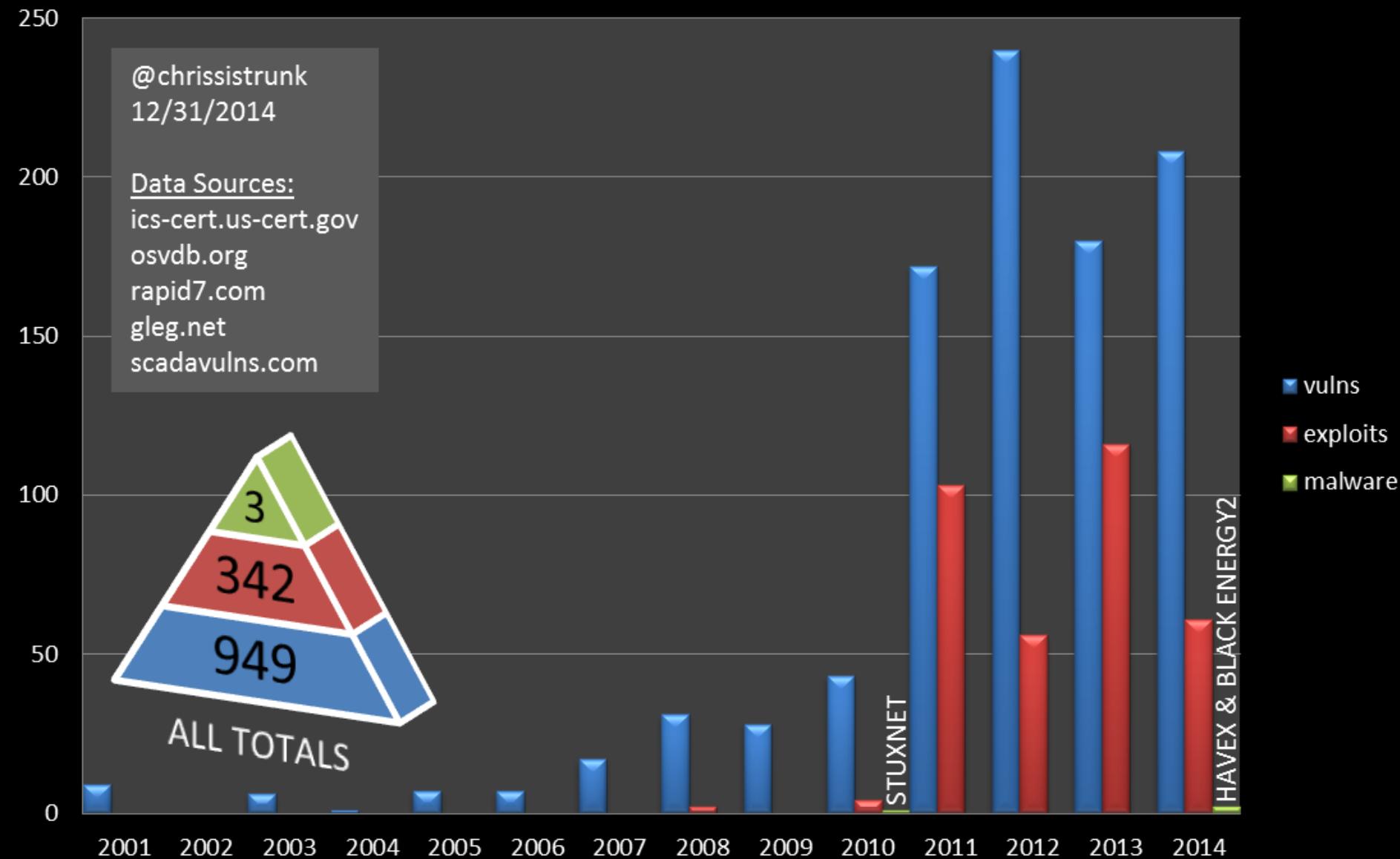
- It's a “Who” not a “What”
- Professional, organized, well-funded
- If you kick them out, they will return



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

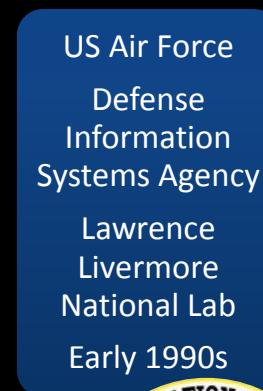
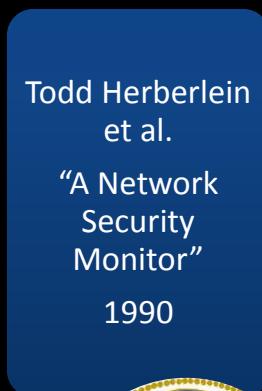
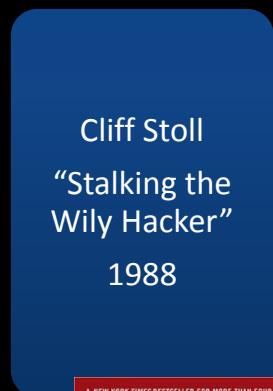
“The collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. **NSM** is a way to find intruders on your network and do something about them before they damage your enterprise.”

- *The Practice of Network Security Monitoring*



Network Security Monitoring

Invented in 1986, still in use today



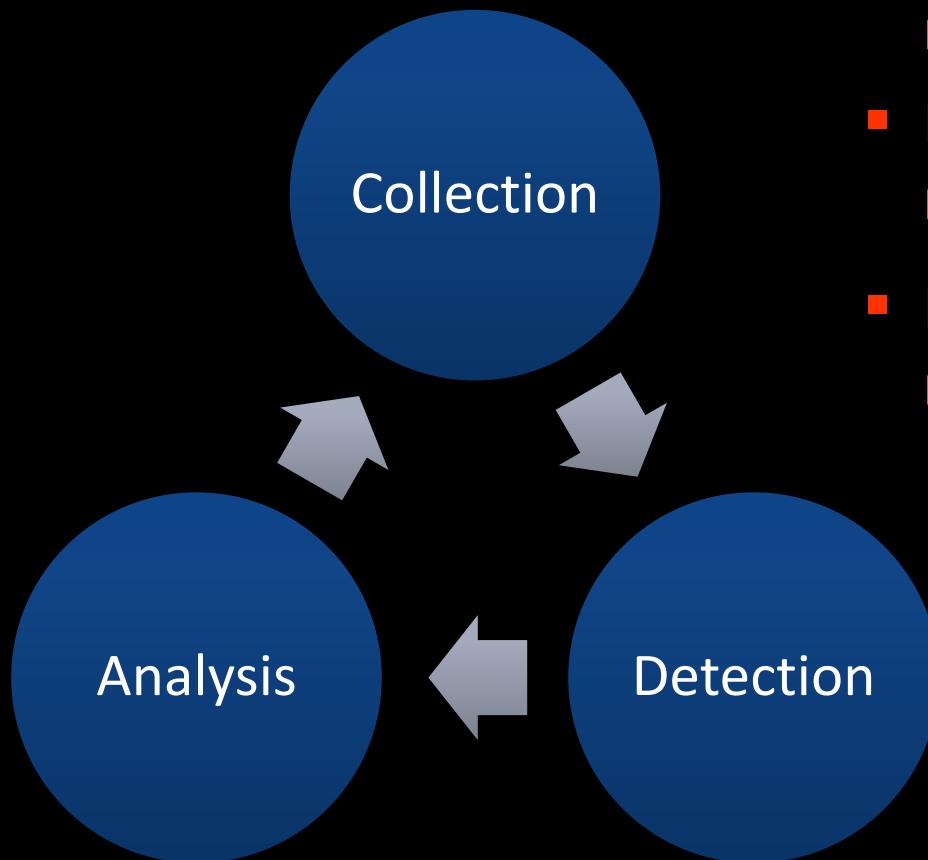
Before we start looking...

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



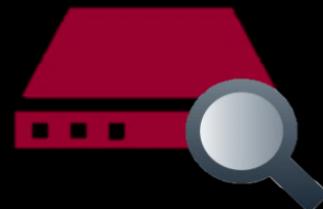
Stratus Engineering



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.

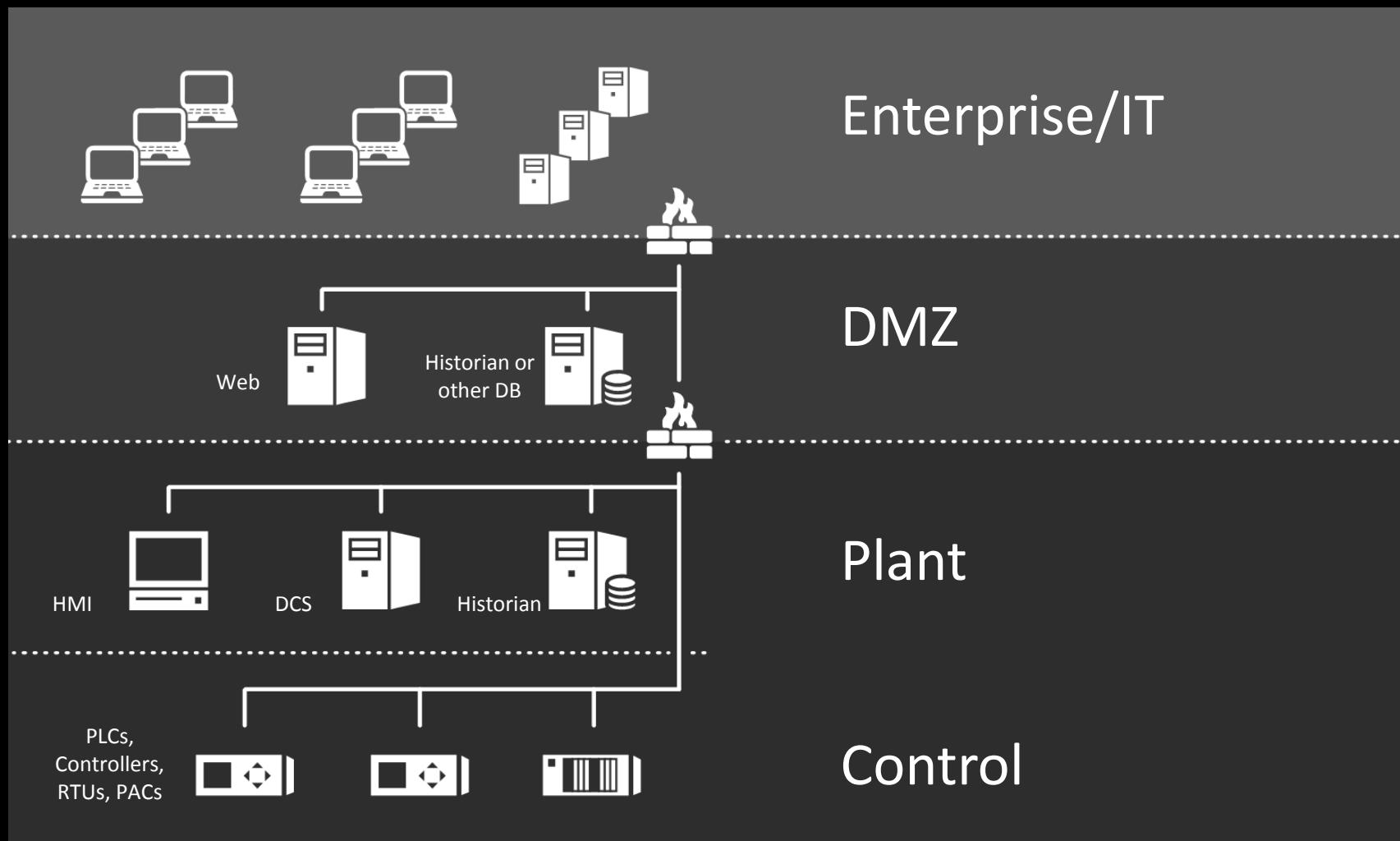


Difficulties for NSM

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

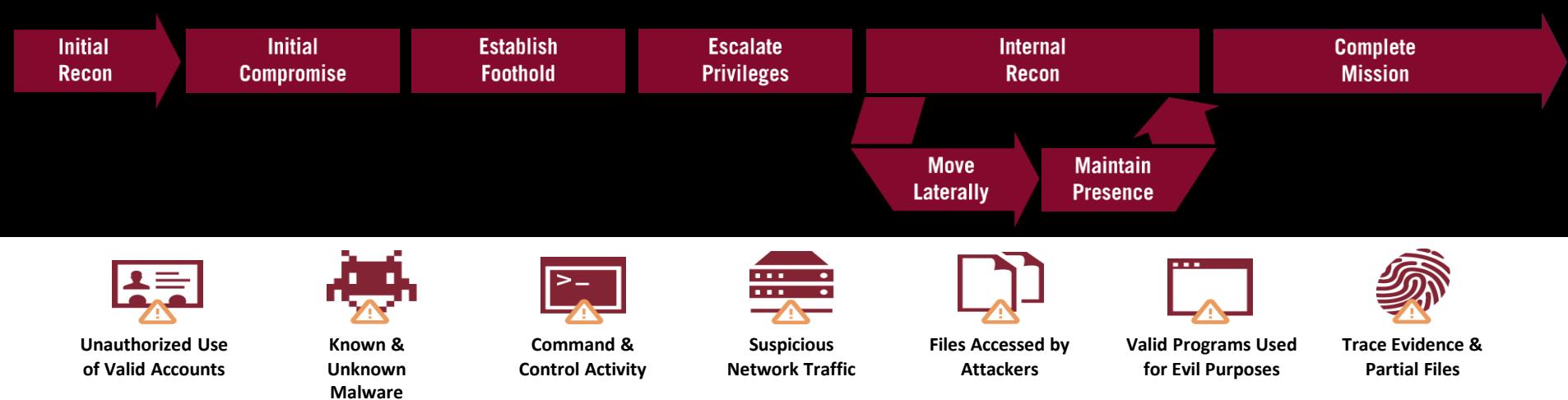
Issues that most ICS do not face!

Example ICS



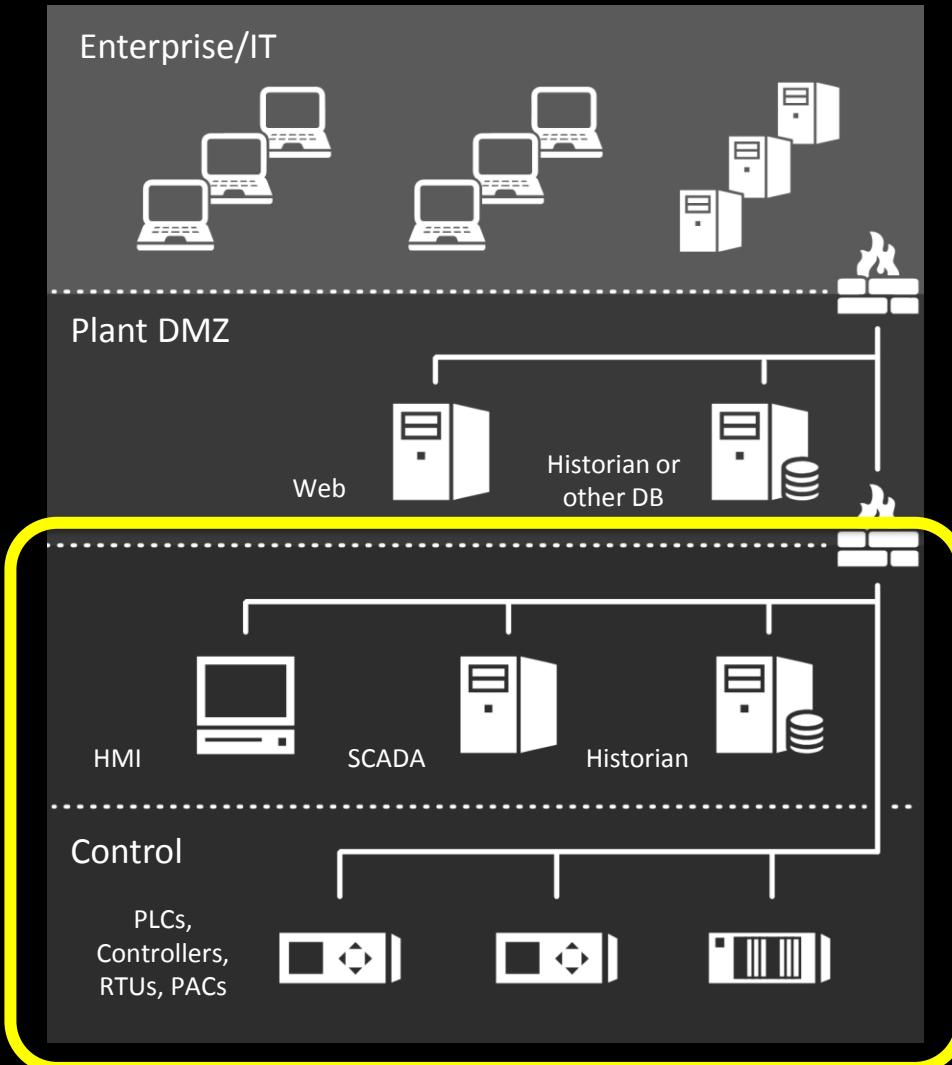
Anatomy of an Attack

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

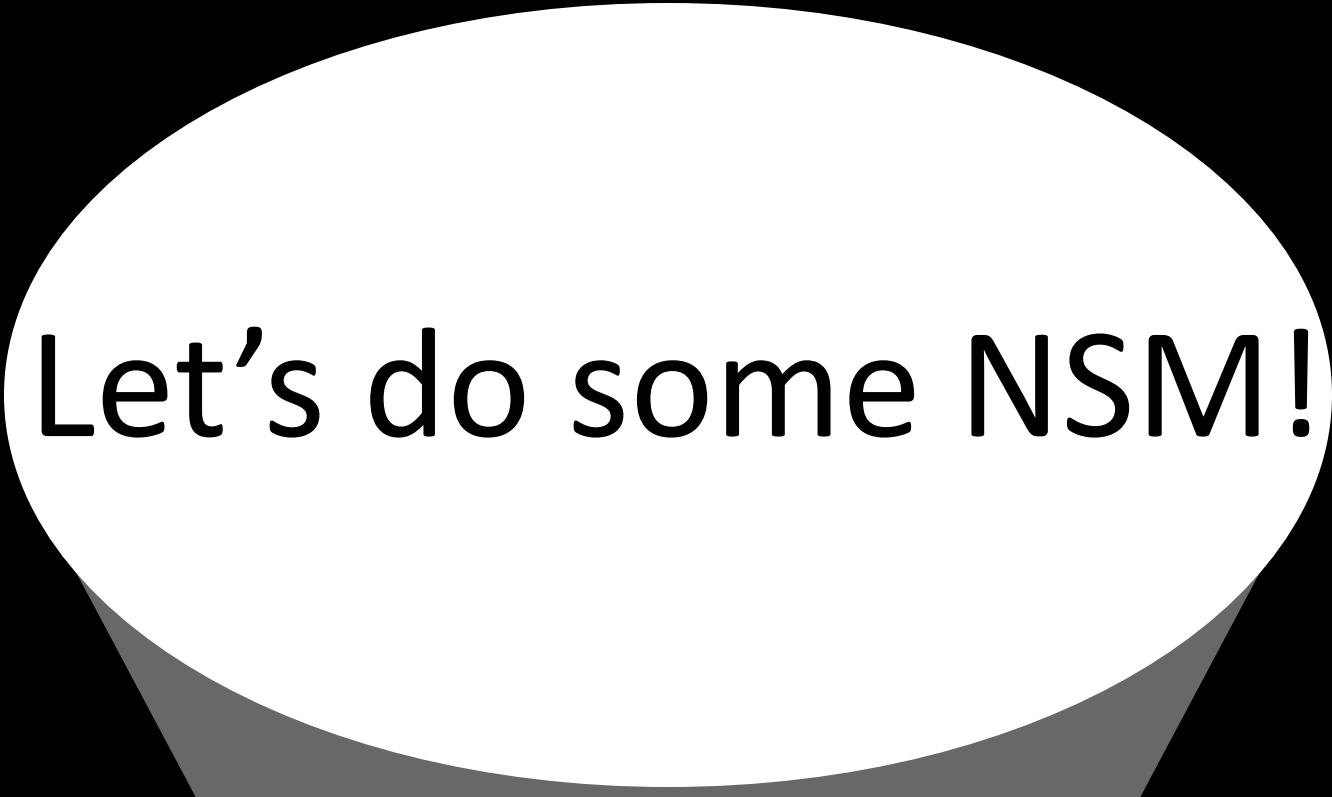


Attacker's goals:

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

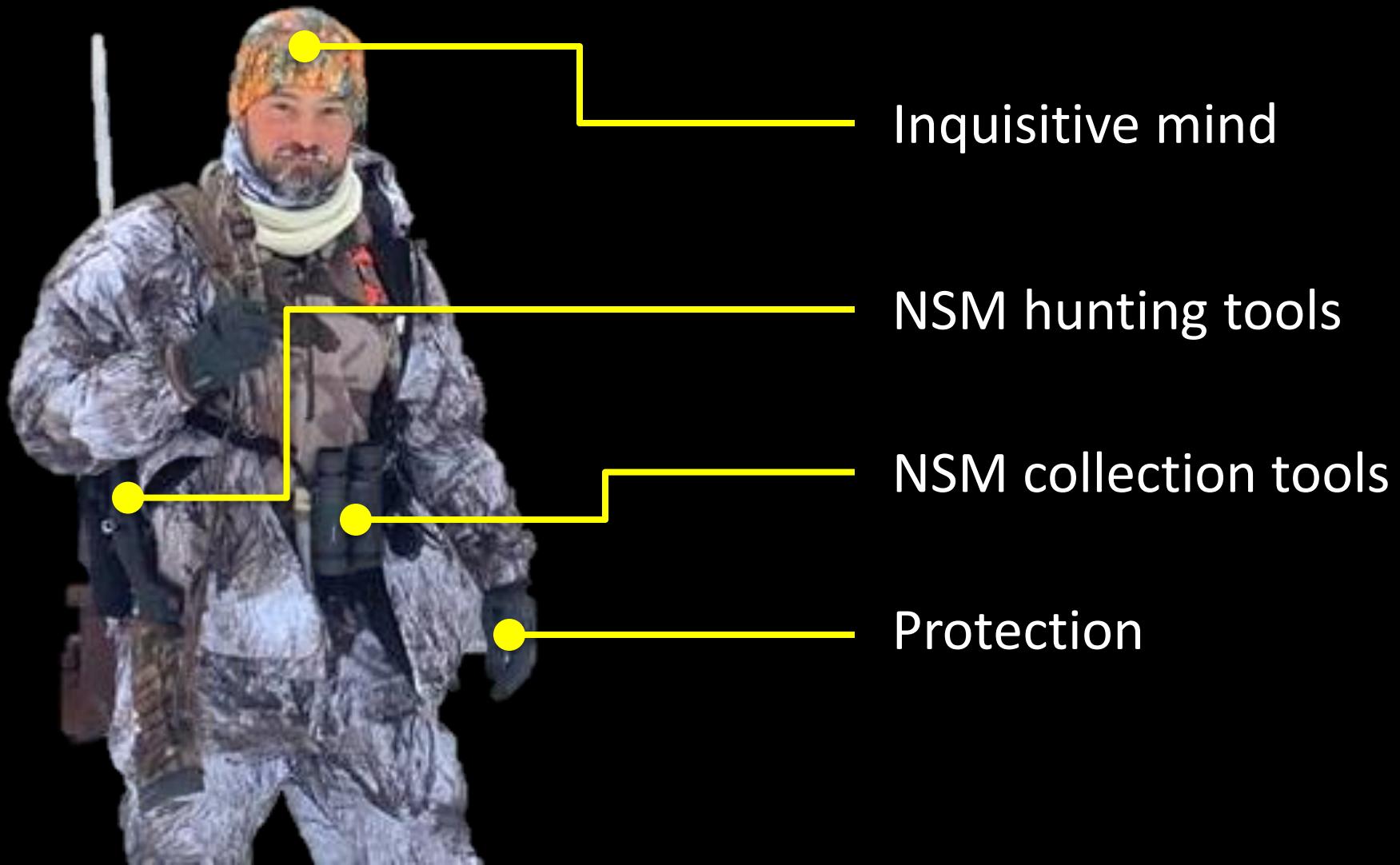
Attacker's options:

- 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



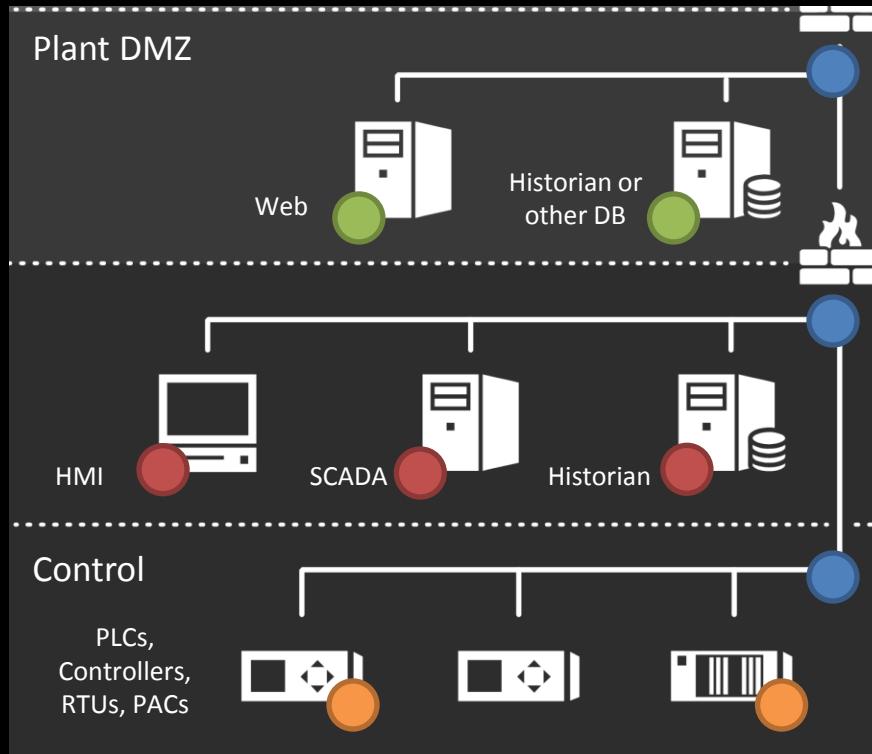
Let's do some NSM!

Let's do some NSM!



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



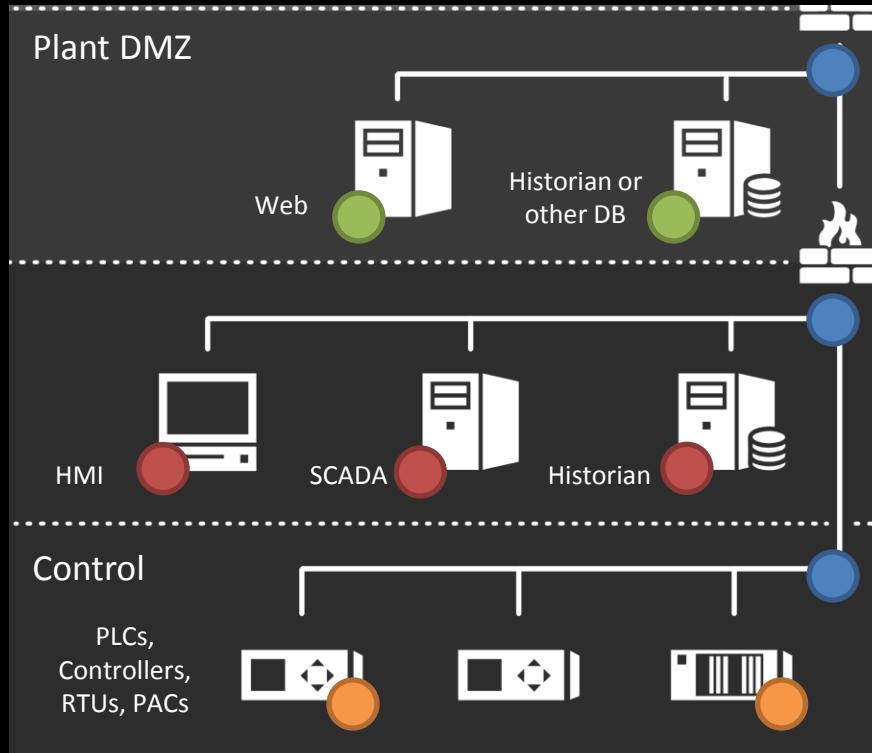
http://3.bp.blogspot.com/-B6PtheVJ9Jg/Uj4EErYhHdI/AAAAAAAAFE/i_2dk9emrp4/s1600/Deer+tracks.jpg

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



Cuddeback Digital Camera 10/11/08 1:56 AM

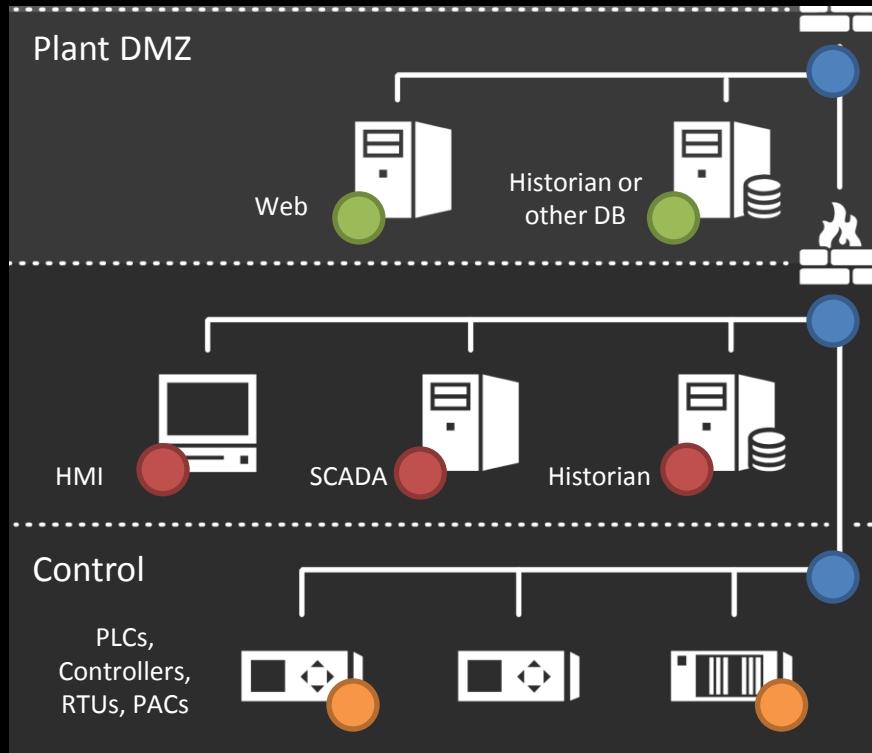
Non Typical, Inc

<http://www.buckmasters.com>

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

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



FLYING SQUIRREL ATTACK!!!!

WILD

11/17/2011 9:50 PM



ICS NSM Examples

Security@onion

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		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
74. [REDACTED]	192.168.133.128	443	38310		6	9	4663	SPA	2015/01/06 21:22:12.548	11.484
74. [REDACTED]	192.168.133.128	443	40065		6	8	4622	SPA	2015/01/06 21:22:12.523	11.510
74. [REDACTED]	192.168.133.128	443	44475		6	8	4622	SPA	2015/01/06 21:22:12.521	11.512
192.168.133.128	74. [REDACTED]	38310	443		6	11	933	SRPA	2015/01/06 21:22:12.548	11.484
192.168.133.128	74. [REDACTED]	40065	443		6	10	893	SRPA	2015/01/06 21:22:12.523	11.510
192.168.133.128	74. [REDACTED]	44475	443		6	10	893	SRPA	2015/01/06 21:22:12.521	11.512
192.168.133.1	192.168.133.255	138	138		2	469			18.788	2015/01/06 21:12:5
149. [REDACTED]	192.168.133.128	123	123		27	380			32.192	2015/01/06 21:11:0

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)

The screenshot shows the NetworkMiner interface with a list of errors. A red box highlights the following error message:

Ethernet MAC has changed, possible ARP spoofing!

Below this message, the list of errors continues:

- [8/28/2014 8:48:40 PM] Error : UDP defined length (119) differs from actual length (94), [38,39] (frame nr: 41033)
- [8/28/2014 8:48:40 PM] Error : Ethernet MAC has changed, possible ARP spoofing! IP 10.██████, MAC █████ -> █████ (frame 41119)
- [8/28/2014 8:48:40 PM] Error : UDP defined length (109) differs from actual length (94), [38,39] (frame nr: 41159)
- [8/28/2014 8:48:40 PM] Error : UDP defined length (109) differs from actual length (94), [38,39] (frame nr: 41160)
- [8/28/2014 8:48:40 PM] Error : UDP defined length (126) differs from actual length (94), [38,39] (frame nr: 41981)
- [8/28/2014 8:48:40 PM] Error : UDP defined length (126) differs from actual length (94), [38,39] (frame nr: 41982)
- [8/28/2014 8:48:40 PM] Error : Ethernet MAC has changed, possible ARP spoofing! IP 10.██████, MAC █████ -> █████ (frame 42093)
- [8/28/2014 8:48:40 PM] Error : UDP defined length (171) differs from actual length (94), [38,39] (frame nr: 42105)
- [8/28/2014 8:48:40 PM] Error : Cannot parse DNS packet (Array index is out of range.), [42,127] (frame nr: 42105)
- [8/28/2014 8:48:40 PM] Error : UDP defined length (171) differs from actual length (94), [38,39] (frame nr: 42106)
- [8/28/2014 8:48:40 PM] Error : Cannot parse DNS packet (Array index is out of range.), [42,127] (frame nr: 42106)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (131) differs from actual length (94), [38,39] (frame nr: 42986)
- [8/28/2014 8:48:41 PM] Error : Ethernet MAC has changed, possible ARP spoofing! IP 172.██████, MAC █████ -> █████ (frame 43091)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (242) differs from actual length (94), [38,39] (frame nr: 43627)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (242) differs from actual length (94), [38,39] (frame nr: 43629)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (188) differs from actual length (94), [38,39] (frame nr: 44212)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (191) differs from actual length (94), [38,39] (frame nr: 44475)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (512) differs from actual length (94), [38,39] (frame nr: 44476)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (191) differs from actual length (94), [38,39] (frame nr: 44481)
- [8/28/2014 8:48:41 PM] Error : Ethernet MAC has changed, possible ARP spoofing! IP 10.██████.34, MAC █████ -> █████ (frame 44481)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (512) differs from actual length (94), [38,39] (frame nr: 44482)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (283) differs from actual length (94), [38,39] (frame nr: 44498)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (283) differs from actual length (94), [38,39] (frame nr: 44509)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (512) differs from actual length (94), [38,39] (frame nr: 44526)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (512) differs from actual length (94), [38,39] (frame nr: 44543)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (513) differs from actual length (94), [38,39] (frame nr: 44788)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (513) differs from actual length (94), [38,39] (frame nr: 44789)
- [8/28/2014 8:48:41 PM] Error : Ethernet MAC has changed, possible ARP spoofing! IP 10.██████.2, MAC █████ -> █████ (frame 44811)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (513) differs from actual length (94), [38,39] (frame nr: 44977)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (513) differs from actual length (94), [38,39] (frame nr: 44984)
- [8/28/2014 8:48:41 PM] Error : Ethernet MAC has changed, possible ARP spoofing! IP 10.██████.79, MAC █████ -> █████ (frame 45000)
- [8/28/2014 8:48:41 PM] Error : Ethernet MAC has changed, possible ARP spoofing! IP 10.██████.1, MAC █████ -> █████ (frame 45187)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (136) differs from actual length (94), [38,39] (frame nr: 45481)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (136) differs from actual length (94), [38,39] (frame nr: 45484)
- [8/28/2014 8:48:41 PM] Error : Ethernet MAC has changed, possible ARP spoofing! IP 10.██████, MAC █████ -> █████ (frame 45733)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (136) differs from actual length (94), [38,39] (frame nr: 45791)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (136) differs from actual length (94), [38,39] (frame nr: 45792)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (136) differs from actual length (94), [38,39] (frame nr: 46263)
- [8/28/2014 8:48:41 PM] Error : UDP defined length (136) differs from actual length (94), [38,39] (frame nr: 46264)

Case Panel:

- File...
- MDS

first50... 9aa6...

Clear

Reload Case Files

Pcaps - Abnormal DNS Traffic

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

NetworkMiner 1.6.1

File Tools Help

Hosts (455) | Frames (50xxx) | Files | Images | Messages | Credentials | Sessions (13498) | DNS (80) | Parameters (1) | Keywords | Cleartext | Anomalies

Fra...	Tim...	Client	Client ...	Server	Ser...	IP TTL	DNS TTL ...	Tra...	Type	DNS Query	DNS Answer	Alexa Top 1M
25231	8/28...	156.1...	62427	156....	53	127	00:00:00	0xCE28	0x0000		NXDOMAIN (flags 0x8593)	N/A (Pro vers)
25232	8/28...	156.1...	62427	156....	53	126	00:00:00	0xCE28	0x0000		NXDOMAIN (flags 0x8593)	N/A (Pro vers)
39569	8/28...	10.16...	64478	146....	53	125	01:00:00	0x3B7	0x0...			N/A (Pro vers)
39570	8/28...	10.16...	64478	146....	53	124	01:00:00	0x3B7	0x0...			N/A (Pro vers)
4226	8/28...	10.16...	2455	156....	53	126	00:20:00	0xB9A	0x0...			N/A (Pro vers)
4207	8/28...	156.1...	61291	10.3...	53	124	00:20:00	0x4777	0x0...			N/A (Pro vers)
4209	8/28...	156.1...	61291	10.3...	53	123	00:20:00	0x4777	0x0...			N/A (Pro vers)
4224	8/28...	10.16...	2455	156....	53	127	00:20:00	0xB9A	0x0...			N/A (Pro vers)
18740	8/28...	156.1...	52998	10.3...	53	123	00:00:00	0x...	0x0000	flashservice.adobe.com	SERVFAIL (flags 0x8192)	N/A (Pro vers)
18738	8/28...	156.1...	52998	10.3...	53	124	00:00:00	0x...	0x0000	flashservice.adobe.com	SERVFAIL (flags 0x8192)	N/A (Pro vers)
35597	8/28...	10.13...	51883	146....	53	126	00:00:00	0xE2F	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
32465	8/28...	146.6...	59101	10.3...	53	123	00:00:00	0x5FB5	0x0000		NXDOMAIN (flags 0x8593)	N/A (Pro vers)
32464	8/28...	146.6...	59101	10.3...	53	124	00:00:00	0x5FB5	0x0000		NXDOMAIN (flags 0x8593)	N/A (Pro vers)
32475	8/28...	10.13...	55424	146....	53	126	00:00:00	0x5BEB	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
32470	8/28...	10.13...	55424	146....	53	127	00:00:00	0x5BEB	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
35595	8/28...	10.13...	51883	146....	53	127	00:00:00	0xE2F	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
36209	8/28...	10.13...	56302	146....	53	126	00:00:00	0x6F1	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
33015	8/28...	10.13...	54907	146....	53	127	00:00:00	0xADFD	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
33016	8/28...	10.13...	54907	146....	53	126	00:00:00	0xADFD	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
33013	8/28...	146.6...	57230	10.3...	53	124	00:00:00	0x3FD2	0x0000		NXDOMAIN (flags 0x8193)	N/A (Pro vers)
33014	8/28...	146.6...	57230	10.3...	53	123	00:00:00	0x3FD2	0x0000		NXDOMAIN (flags 0x8193)	N/A (Pro vers)
36208	8/28...	10.13...	56302	146....	53	127	00:00:00	0x6F1	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
32697	8/28...	10.13...	64219	146....	53	126	00:00:00	0x19D1	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
32696	8/28...	10.13...	64219	146....	53	127	00:00:00	0x19D1	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
32692	8/28...	146.6...	58604	10.3...	53	124	00:00:00	0xC29D	0x0000		NXDOMAIN (flags 0x8593)	N/A (Pro vers)
32695	8/28...	146.6...	58604	10.3...	53	123	00:00:00	0xC29D	0x0000		NXDOMAIN (flags 0x8593)	N/A (Pro vers)
36006	8/28...	10.13...	49786	146....	53	126	00:00:00	0xEB65	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
36005	8/28...	10.13...	49786	146....	53	127	00:00:00	0xEB65	0x0000		NXDOMAIN (flags 0x8183)	N/A (Pro vers)
18735	8/28...	156.1...	53322	10.3...	53	123	00:00:00	0x3329	0x0000	infoc2.duba.net	SERVFAIL (flags 0x8182)	N/A (Pro vers)
18733	8/28...	156.1...	53322	10.3...	53	124	00:00:00	0x3329	0x0000	infoc2.duba.net	SERVFAIL (flags 0x8182)	N/A (Pro vers)
32514	8/28...	156.1...	51251	10.3...	53	123	00:00:00	0x6843	0x0000	ivt.ihaveit.biz	SERVFAIL (flags 0x8192)	N/A (Pro vers)
32513	8/28...	156.1...	51251	10.3...	53	124	00:00:00	0x6843	0x0000	ivt.ihaveit.biz	SERVFAIL (flags 0x8192)	N/A (Pro vers)
32033	8/28...	156.1...	51251	10.3...	53	123	00:00:00	0x6843	0x0000	ivt.ihaveit.biz	SERVFAIL (flags 0x8192)	N/A (Pro vers)
32032	8/28...	156.1...	51251	10.3...	53	124	00:00:00	0x6843	0x0000	ivt.ihaveit.biz	SERVFAIL (flags 0x8192)	N/A (Pro vers)
8069	8/28...	10.36...	60766	156....	53	126	00:00:00	0x8075	0x0000		SERVFAIL (flags 0x8192)	N/A (Pro vers)
8066	8/28...	10.36...	60766	156....	53	127	00:00:00	0x8075	0x0000		SERVFAIL (flags 0x8192)	N/A (Pro vers)

Case Panel

File... MD5
first50... 9aa6...

Reload Case Files

Running NetworkMiner with Mono

IDS alerts - Abnormal DNS Traffic

DNS requests shown in the Bro IDS log in ELSA

The screenshot shows the ELSA (Event Log Search Application) interface running in a Chromium browser window. The URL is <https://localhost/elsa/>. The main content area displays a table of DNS requests. The query used is `class=BRO_DNS dstport="53" groupby:hostname`. The results are grouped by hostname, with 158 entries. The table has two columns: "Count" and "Value". The "Value" column contains hostnames like rdns.orionvm.com.au, 181digitalwebcontrol.us, flashservice.adobe.com, consumeronlineproducts-p.us, e173.primody.com, infoc2.duba.net, and launchermsg.3g.cn. Some hostnames are redacted with black boxes. The left sidebar shows a navigation menu with various network protocol sections like Connections, DHCP, DNS, and HTTP.

Count	Value
44	[REDACTED]
7	[REDACTED]
6	rdns.orionvm.com.au
6	[REDACTED]
6	[REDACTED]
6	[REDACTED]
5	181digitalwebcontrol.us
5	flashservice.adobe.com
4	consumeronlineproducts-p.us
4	[REDACTED]
4	[REDACTED]
4	e173.primody.com
4	[REDACTED]
3	infoc2.duba.net
3	launchermsg.3g.cn

Pcaps - Malformed Modbus

Deep packet inspection of Modbus by Wireshark

The screenshot shows a Wireshark interface with the following details:

- Protocol Hierarchy Statistics Dialog:** A modal window titled "Wireshark: Protocol Hierarchy Statistics" is open, displaying the following table:

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End	Bytes	End	Mbit/s
Frame	100.00 %	1440	100.00 %	93324	0.057	0	0	0	0.000	0	0.000
Ethernet	100.00 %	1440	100.00 %	93324	0.057	0	0	0	0.000	0	0.000
Internet Protocol Version 4	100.00 %	1440	100.00 %	93324	0.057	0	0	0	0.000	0	0.000
Transmission Control Protocol	100.00 %	1440	100.00 %	93324	0.057	0	0	0	0.000	0	0.000
Modbus/TCP	100.00 %	1440	100.00 %	93324	0.057	0	0	0	0.000	0	0.000
Text item	100.00 %	1440	100.00 %	93324	0.057	1152	74748	0.046			
Malformed Packet	20.00 %	288	19.90 %	18576	0.011	288	18576	0.011			

- Packet List View:** The main window displays a list of captured packets. The 14th packet (Index 3968) is selected and highlighted in blue. The details pane shows the following structure:
 - Frame 3968: 65 bytes on wire (512 bits on air)
 - Ethernet II, Src: WistronI_a4 (00:0c:04:00:00:a4), Dst: Modbus (00:00:00:00:00:00)
 - Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.1
 - Transmission Control Protocol, Src Port: 502, Dst Port: 502, Seq: 1, Ack: 1, Len: 60
 - Modbus/TCP
 - Modbus
 - [Malformed Packet: Modbus]
 - [Expert Info (Error/Malformed)]
 - [Malformed Packet (Exception)]
 - [Severity level: Error]
 - [Group: Malformed]
- Hex and ASCII View:** The bottom panes show the raw hex and ASCII representations of the selected packet (Index 3968). The ASCII view shows the following data:

0000 00 30 a7 05 d4 94 3c 97 0e a4 f5 3a 08 00 45 00 .0....<.. .:..E.
0010 00 33 08 09 40 00 80 06 00 00 c0 a8 00 01 c0 a8 .3...@...: ..:..:..
0020 00 03 ec 18 01 f6 ae 32 c3 b9 46 e2 7b 35 50 182 ..F.{5P..
0030 40 21 81 7a 00 00 00 01 00 00 05 01 01 00 00 @!z.....
0040 00

IDS Logs

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

The screenshot displays a desktop environment with several windows open, illustrating the integration of Bro IDS and ELSA for network log analysis.

Bro IDS Log View: A terminal window titled "weird.log" shows a list of network events. The log includes fields such as timestamp (ts), source IP (id.orig_h), destination IP (id.resp_h), port numbers (port, id.resp_p), and various status codes and error messages. Two specific sections are highlighted with yellow boxes: "Modbus" and "DNP3".

- Modbus:** This section highlights several Modbus-related events. One event is shown in detail: a ReadCoilsRequest from 192.168.0.1 to 192.168.0.3 port 12423, which failed with a binpac exception: out_of_bound. Other entries show similar errors for ReadDiscreteInputsRequest, ReadHoldingRegistersRequest, and ReadInputRegistersRequest.
- DNP3:** This section highlights several DNP3-related events. One event is shown in detail: a DNS request from 192.168.0.1 to 192.168.0.3 port 12614, which failed with a dnp3_unexpected_flow_direction error. Other entries show similar errors for dns_unmatched_msg and dnp3_header_lacks_magic.

ELSA - Chromium: A browser window titled "weird.log" shows the ELSA interface. It displays a timeline of events and allows users to search and filter logs by source and type. The interface includes a sidebar with links to various log types like Connections, DNS, and Host Logs.

Security Onion Dashboard: A separate window titled "Security Onion: HOME" shows a dashboard with various monitoring and reporting tools, including Snorby and FlowBAT.

ELSA Query Results: A results window titled "ELSA - Admin" shows a detailed list of log entries grouped by name. The results include a count of 61 for dnp3_header_lacks_magic, 34 for dns_unmatched_msg, 18 for dnp3_unexpected_flow_direction, and 8 for binpac exception: out_of_bound: DNP3_Application_Request_Header. The results also mention active_connection_reuse, bad_SYN_ack, DNS_truncated_len_lt_hdr_len, binpac exception: out_of_bound: ReadInputRegistersRequest, binpac exception: out_of_bound: ReadHoldingRegistersRequest, DNS_Conn_count_too_large, unknown_protocol_2, binpac exception: out_of_bound: ReadInputRegistersRequest, and binpac exception: out_of_bound: ReadCoilsRequest.

IDS GUIs

Alerts in Sguil of scanning activity

Sguil Realtime Events interface showing alerts and packet details.

RealTime Events tab (selected):

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	102.168.0.1	54360	102.168.0.3	111	17	PADS New Asset - unknown @sunrce

IP Resolution, **Agent Status**, **Snort Statistics**, **System Msgs**, **User Msgs** tabs are also present.

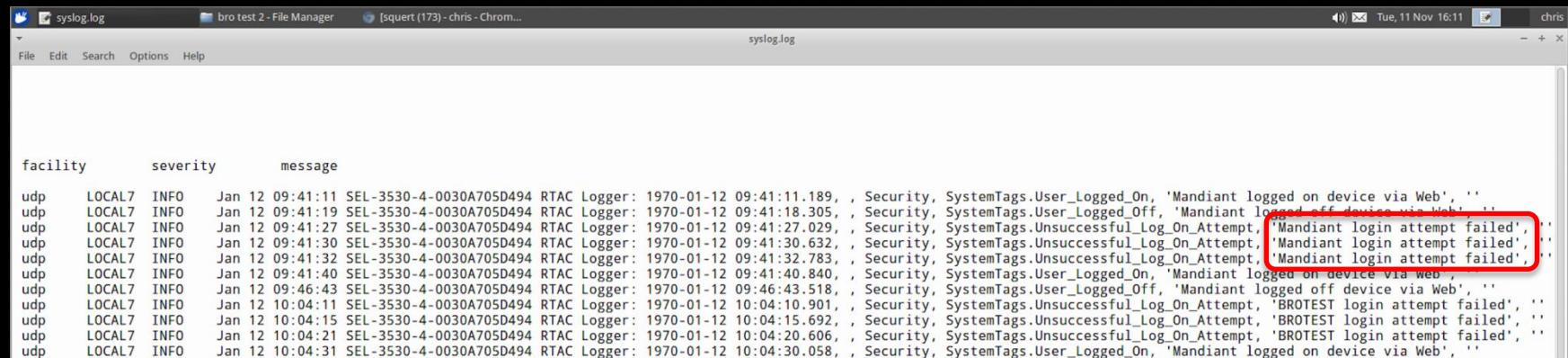
Show Packet Data tab:

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum			
192.168.0.3	192.168.0.1		4	5	0	1153	39128	2	0	64	7242			
TCP	Source Port	Dest Port	R	R	R	C	S	S	Y	I				
443	1482	.	.	.	X	X	.	.	3505235830	1421189568	5			
DATA	Seq #								Ack #	Offset	Res	Window	Urp	ChkSum
60	15	02	55	31	13	30	11	06	03	55	04	08	13	0A
57	61	73	68	69	66	74	6F	6E	31	10	00	03		
55	04	07	13	07	50	75	6C	6D	61	6E	31	32	30	
06	03	55	04	04	13	29	53	63	68	77	65	69	74	65
72	20	45	66	67	69	66	65	65	72	69	66	67	20	46
62	6F	72	61	74	6F	72	69	65	73	2C	20	49	63	2E
31	30	2D	06	03	55	04	08	13	26	41	75	74	6F	6D
61	74	69	6F	6E	20	61	6E	64	20	49	6E	74	65	72
61	74	69	6F	6E	20	45	6E	67	69	6E	65	72	69	6E
67	31	18	30	16	06	03	55	04	13	0F	53	45	4C	20
33	35	33	30	2D	34	20	52	54	41	43	30	1E	17	0D
34	30	38	31	33	32	33	30	33	33	37	5A	17	0D	33

Packet details show a TCP SYN-ACK exchange between 192.168.0.3 and 192.168.0.1, port 443. The sequence number is 3505235830, acknowledgement is 1421189568, offset is 5, window size is 1825, and TTL is 64. The ChkSum is 7242.

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.



```
syslog.log
bro test 2 - File Manager [squert (173) - chris - Chrome...]
Tue, 11 Nov 16:11 chris

File Edit Search Options Help
syslog.log

facility      severity      message
udp    LOCAL7    INFO      Jan 12 09:41:11 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 09:41:11.189, , Security, SystemTags.User_Logged_On, 'Mandiant logged on device via Web', ''
udp    LOCAL7    INFO      Jan 12 09:41:19 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 09:41:18.305, , Security, SystemTags.User_Logged_Off, 'Mandiant logged off device via Web', ''
udp    LOCAL7    INFO      Jan 12 09:41:27 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 09:41:27.029, , Security, SystemTags.Unsuccessful_Log_On_Attempt, 'Mandiant login attempt failed', ''
udp    LOCAL7    INFO      Jan 12 09:41:30 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 09:41:30.632, , Security, SystemTags.Unsuccessful_Log_On_Attempt, 'Mandiant login attempt failed', ''
udp    LOCAL7    INFO      Jan 12 09:41:32 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 09:41:32.783, , Security, SystemTags.Unsuccessful_Log_On_Attempt, 'Mandiant login attempt failed', ''
udp    LOCAL7    INFO      Jan 12 09:41:40 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 09:41:40.840, , Security, SystemTags.User_Logged_On, 'Mandiant logged on device via web', ''
udp    LOCAL7    INFO      Jan 12 09:46:43 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 09:46:43.518, , Security, SystemTags.User_Logged_Off, 'Mandiant logged off device via Web', ''
udp    LOCAL7    INFO      Jan 12 10:04:11 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 10:04:10.901, , Security, SystemTags.Unsuccessful_Log_On_Attempt, 'BROTEST login attempt failed', ''
udp    LOCAL7    INFO      Jan 12 10:04:15 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 10:04:15.692, , Security, SystemTags.Unsuccessful_Log_On_Attempt, 'BROTEST login attempt failed', ''
udp    LOCAL7    INFO      Jan 12 10:04:21 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 10:04:20.606, , Security, SystemTags.Unsuccessful_Log_On_Attempt, 'BROTEST login attempt failed', ''
udp    LOCAL7    INFO      Jan 12 10:04:31 SEL-3530-4-0030A705D494 RTAC Logger: 1970-01-12 10:04:30.058, , Security, SystemTags.User_Logged_On, 'Mandiant logged on device via Web', ''
```

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

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter Expression... Clear Apply

WIRESHARK The World's Most Popular Network Protocol Analyzer

Capture Files Interface List Open Website

Snorby "All About Snorby!"

Dashboard My Queue (0) Events Sensors Search Administration

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR Updated: 11/19/11 9:30:00 PM

0 HIGH SEVERITY 0 MEDIUM SEVERITY 26 LOW SEVERITY

Event Count vs Time By Sensor Scipio - Suricata

Event Count 15
12.5
10
7.5
5
2.5
0
-2.5

Last 24 Hours 21 22 23 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

Xplico Interface User: xplico

Help Forum Wiki Change password Licenses Logout

Case Session Data Cap. Start Time 0000-00-00 00:00:00 Cap. End Time 0000-00-00 00:00:00 Status EMPTY Hosts ---

Pcap set SFTP uploading big pcap files. Add new pcap file. Choose File No file chosen Upload List of all pcap files.

HTTP MMS Emails FTP - TFTP - HTTP file Web Mail

Post 0 Number 0 Received 0 Total 0 Get 0 Contents 0 Sent 0 Received 0 Video 0 Images 0 Unread 0/0 Downloaded 0 0 Uploaded 0 - 0 HTTP 0 Sent 0

Enhance Facebook Chat / TCP/SSL/TLS DNS / DNS-TCP P2P / P2P-TCP RTSP / RTSP-TCP SQUIL-0.8.0 - Connected To OnionSensor2

File Query Reports Sound: Off ServerName: OnionSensor2 UserName: andy UserID: 2 2012-06-03 14:56:25 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	Sport	Dst IP	DPort	Pr	Event Message
RT	1	OnionSe...	13.35633	2012-06-03 14:55:27	172.31.254.32	60432	172.31.253.108	80	6	stream5: Reset outside window
RT	15	OnionSe...	13.35634	2012-06-03 14:55:28	172.31.254.32	38184	172.31.253.108	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)

IP Resolution Agent

Reverse DNS Enab

Src IP: Src Name: Dst IP: Dst Name:

Whois Query: None Selected

Show Packet Data Show Rule

alert tcp \$EXTERNAL_NET any -> SHOME_NET \$HTTP_PORTS (msg:"ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)"; flow:to_server,established; content:"User-Agent:[!a] Mozilla/5.0 (compatible; [b]Nmap Scripting Engine"; fast-pattern:38;20; http_header; nocase; reference:url,doc.emergingthreats.net/2009358; content-classification:web-application-attack; sid:2009358; rev:5); /nsm/server_data/securityonion/rules/OnionSensor2-eth3/downloaded.rules: Line 14220

Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum						
172.31.254.32	172.31.253.108	4	5	0	203	30059	2	0	63	29173						
Protocol	Source	Dest	R	A	P	R	S	F								
TCP	Source Port	Dest Port	1	0	G	K	H	T	N	N						
TCP	38184	80	.	.	X	X	.	.	150091614	3813005820						
DATA	47	45	54	20	2F	20	48	54	50	2F	31	2E	31	0D	0A	
	43	6F	6E	65	63	74	69	6F	6E	3A	20	63	6C	6F	73	
	65	0D	0A	55	73	65	72	2D	41	67	65	6E	74	3A	20	4D
	6F	7A	69	6C	61	2F	35	2E	30	28	63	6F	70	74	69	6E
	61	74	69	62	6C	65	3B	20	4E	6D	61	20	53	63	72	
	69	70	74	69	6E	67	20	45	6E	67	69	6E	65	3B	20	68
	74	74	70	3A	2F	2F	6E	6D	61	70	2E	6F	72	67	2F	62
	6F	6F	6B	2F	6E	73	65	2E	68	74	6D	29	0D	0A	48	
	6F	73	74	3A	20	31	37	32	2E	33	31	2E	32	35	33	2E
	31	30	38	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D
	108....															

Search Packet Payload Hex Text NoCase

NetFlow Tools

SiLK & FlowBAT

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

FLOWBAT

Dashboard Quick Query Saved Queries IP Sets Chris Sanders UTC: 2014/10/13 18:31

Execute Command line Query builder

rwfilter --type=all --any-address=162.212.181.0/24 --dport=53

Exclusions Use "OR" to separate exclusions, for example: --type=7 OR --dport=80

Output type

Records Stats Count

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



Remember

Adversaries are a “Who”, not a “What”

A close-up photograph of an owl's face, focusing on its large, expressive eyes. The owl has dark, mottled feathers on its head and a white patch on its ear. Its eyes are a vibrant, glowing orange-red color, looking directly at the viewer. The background is dark, making the owl's features stand out.

Find Evil

chris.sistrunk@mandiant.com

@chrissistrunk

robert.caldwell@mandiant.com

@robac3