# Network Security Monitoring: An Open Community Approach

IUP- Information Assurance Day, 2011

Greg Porter
11/10/11

ALLEGHENY DIGITAL

# Agenda

- Introduction
- Current State
- NSM & Open Community Options
- Conclusion

# Introduction

- Greg Porter
- Working in the field, ~ 10 years
  - Vulnerability Assessments
  - Penetration Testing
  - Incident Response
  - Security Governance
- Primarily “Big 4” consulting
- Visiting Scientist, SEI-CERT
- Founder, Allegheny Digital

# This Presentation

- Based on technical and non-technical security assessment activities and direct observations made over the past several years
- Lack of reasonable network security monitoring in many organizations is…*rather pervasive*
- Intent is to provide an overview of some promising "open community" platforms

# Agenda

- Introduction
- Current State
- NSM & Open Community Options
- Conclusion

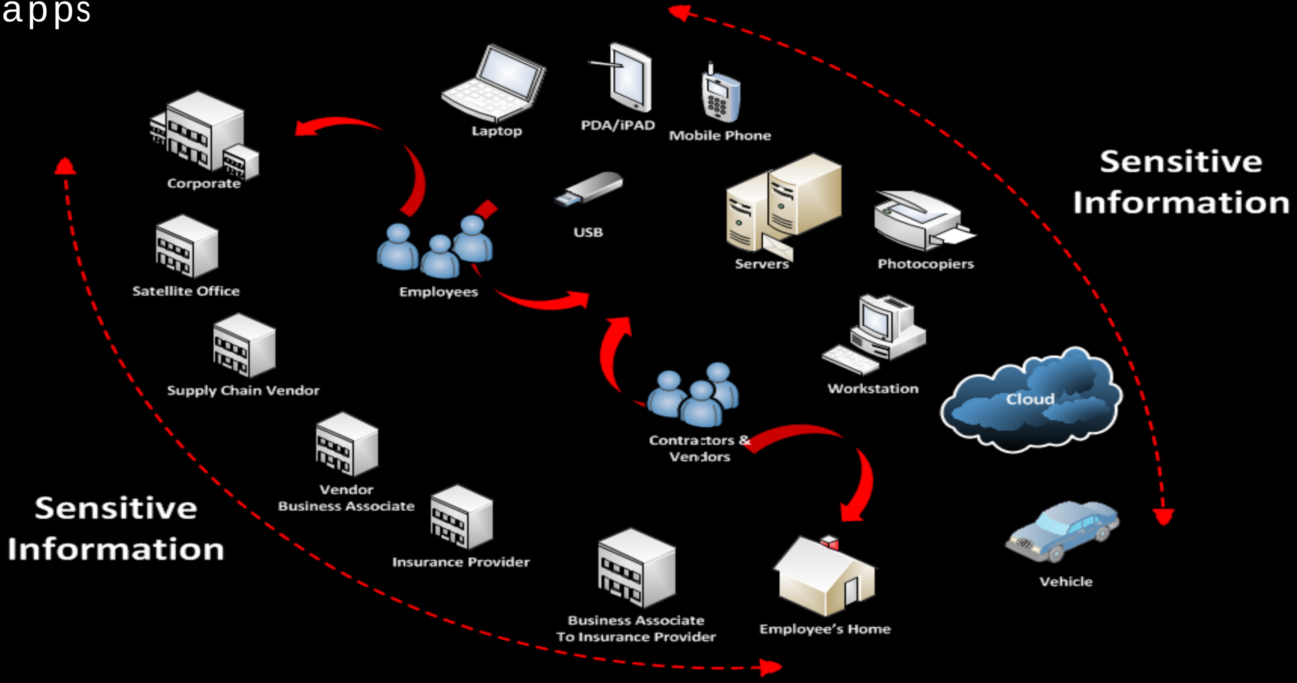
# Current State

- Where are we today?
- The proliferation of malware isn't slowing
- 2010 the biggest year ever for total malware production
  - At least 20 million new pieces of malware last year alone
- 55,000 new instances of malware/day[1]
- *There is now more malicious code being created today, worldwide, than there is legitimate software[2]*

[1] Source: McAfee
[2] Source: Symantec

# The Unbounded Enterprise

- Data Anywhere ≠ Data Everywhere
- More endpoints, more mobile devices add to the challenge of protecting sensitive information
  - A general lack of security awareness among end users
  - Limited offerings and maturity of mobile safeguards, widespread non-secure apps



# Every Business is a Target

- Even seemingly “well defended” organizations are getting compromised
- The past 24 months have seen the likes of Google, RSA, AT&T, IBM, Northrop Grumman, and numerous others fall to targeted cyber attacks
- How do many successful businesses often find out they’ve had a breach of sensitive information?
- Does your company have the necessary network visibility to detect and mitigate potential risks before they occur?

# What’s Changed?

- Attacks are increasing at an exponential rate
- This is contrary to what many people think because the attackers have changed how they operate
  - (Past) Visible → Stealthy (Today)
  - (Past) Disruptive → Data driven (Today)
  - (Past) Low hanging fruit → Targeted (Today)
  - (Past) Static → Dynamic (Today)
  - (Past) Ad hoc → Persistent (Today)
  - (Past) Basic → Advanced (Not an absolute)

Source: Dr. Eric Cole

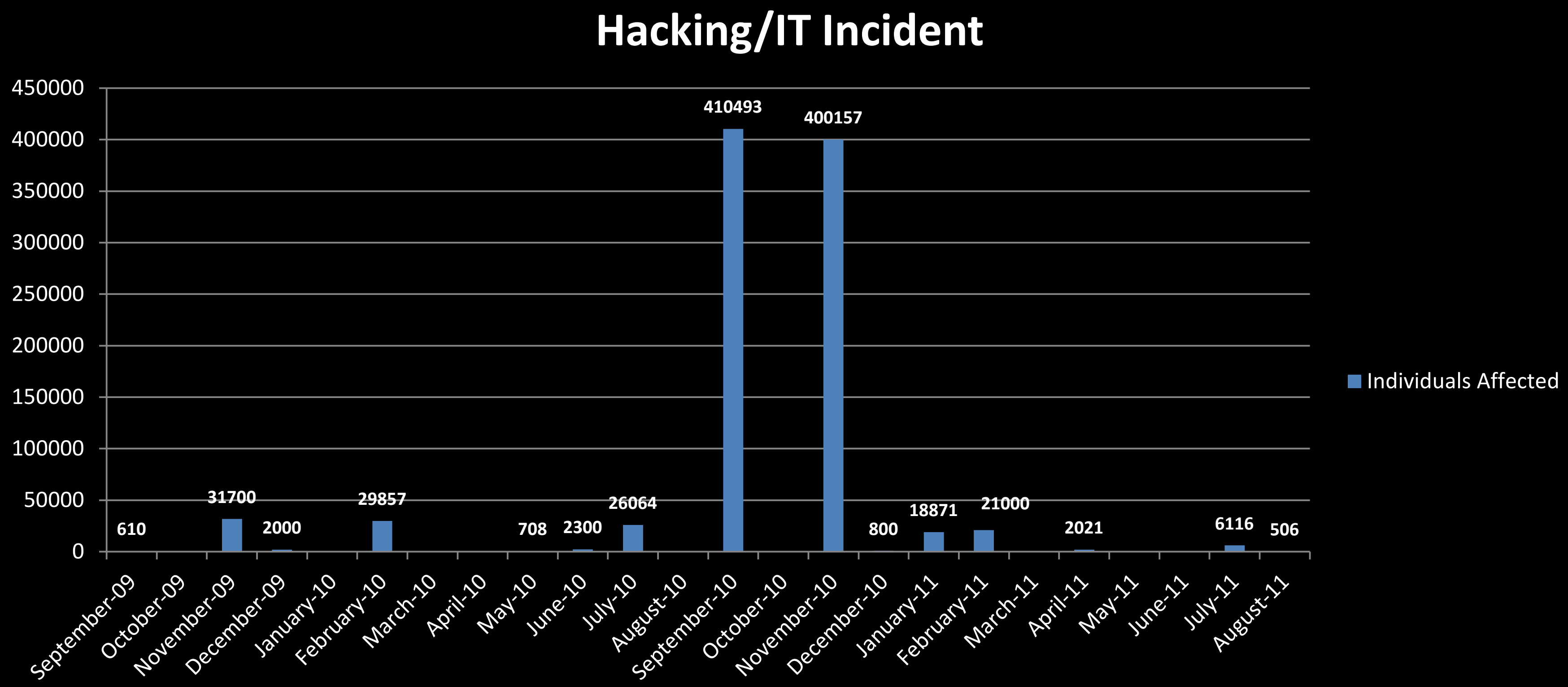
# Your Information @ Stake

- Healthcare: NEA Baptist Clinic
  - 3,116 affected
  - Clinic’s web site compromised, usernames, passwords, and in some cases additional details
- Retail: Adidas
  - 500,000
  - Website compromised, email addresses and passwords dumped by hacker
- Education: Florida International University
  - 19,500
  - Emoticon discovered in internal database suggested that database with 19,500 students' names, dates of birth, Social Security numbers, and GPAs might have been accessed by hacker
- Government: BART Police Officer Association
  - Hackers released the private data of more than 100 BART police officers
  - Disclosure of 2,000 usernames and passwords by the hacking collective Anonymous against a San Francisco transportation website

Source: http://datalossdb.org

# An Anecdote? Healthcare & Breaches

- As required by the HITECH Act, the Secretary of HHS must post a list of breaches of unsecured protected health information (PHI) affecting 500 or more individuals.



Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

# Agenda

- Introduction
- Current State
- NSM & Open Community Options
- Conclusion

# Network Security Monitoring

- Preventative measures will eventually fail…some intruders are smarter, more patient than you
- NSM is the collection, analysis, and escalation of indications and warnings (I&W) to detect and respond to intrusions
- An IDS alert provides a potential indicator that of a security related event
- IDS != NSM
- Prepare for an incident before it occurs, collect as much as you technically and legally can

Source: Richard Bejtlich

# Network Security Monitoring – ii

- Regarding data collection
  - Storage costs are decreasing
  - Data sampling and traffic analysis is better than doing nothing

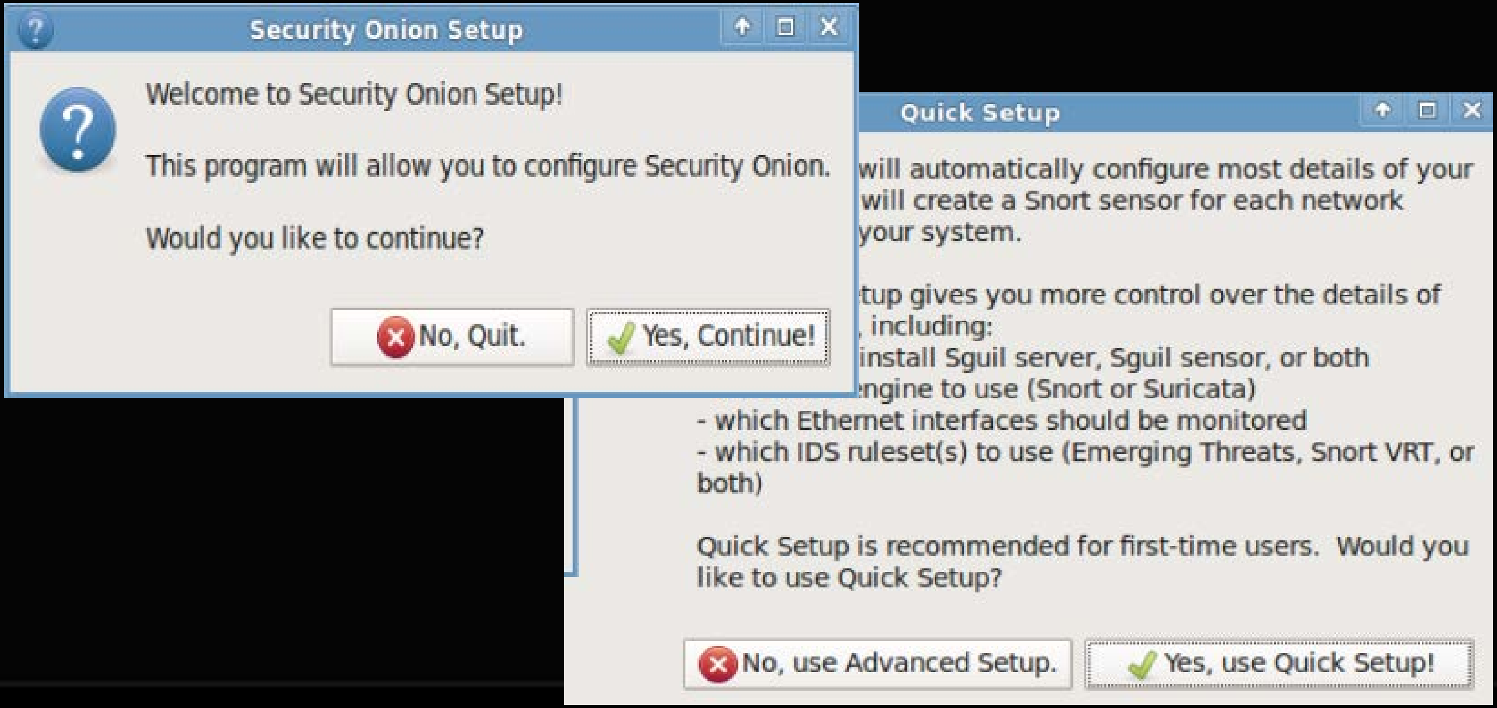
- NSM provides needed context to make intelligent decisions
  - *Alert* data provides a potential indicator of security incidents
  - *Session* data is a content neutral summary of transactions
  - *Full content* data captures packet-level details, including application content
  - *Statistical* data summarizes traffic

# Security Onion

- A Linux distro developed by Doug Burks
- Excellent resource for IDS and NSM
  - Available at http://securityonion.blogspot.com/
- Contains a breadth of NSM tools
  - Snort, Suricata, Sguil, Wireshark, Squert, etc.
- Sguil is the de facto reference implementation of NSM
  - Alert data (NIDS alerts from Snort/Suricata *and* HIDS alerts from OSSEC)
  - Session data (Security Analyst Network Connection Profiler SANCP)
  - Transaction data (HTTP logs from httpry)
  - Full content data (daemonlogger)

# Security Onion -ii

- SO’s Quick Setup feature will automatically configure the essential details of your system, creating a Snort sensor for each network interface on your system



Welcome to Security Onion Setup!

This program will allow you to configure Security Onion.

Would you like to continue?

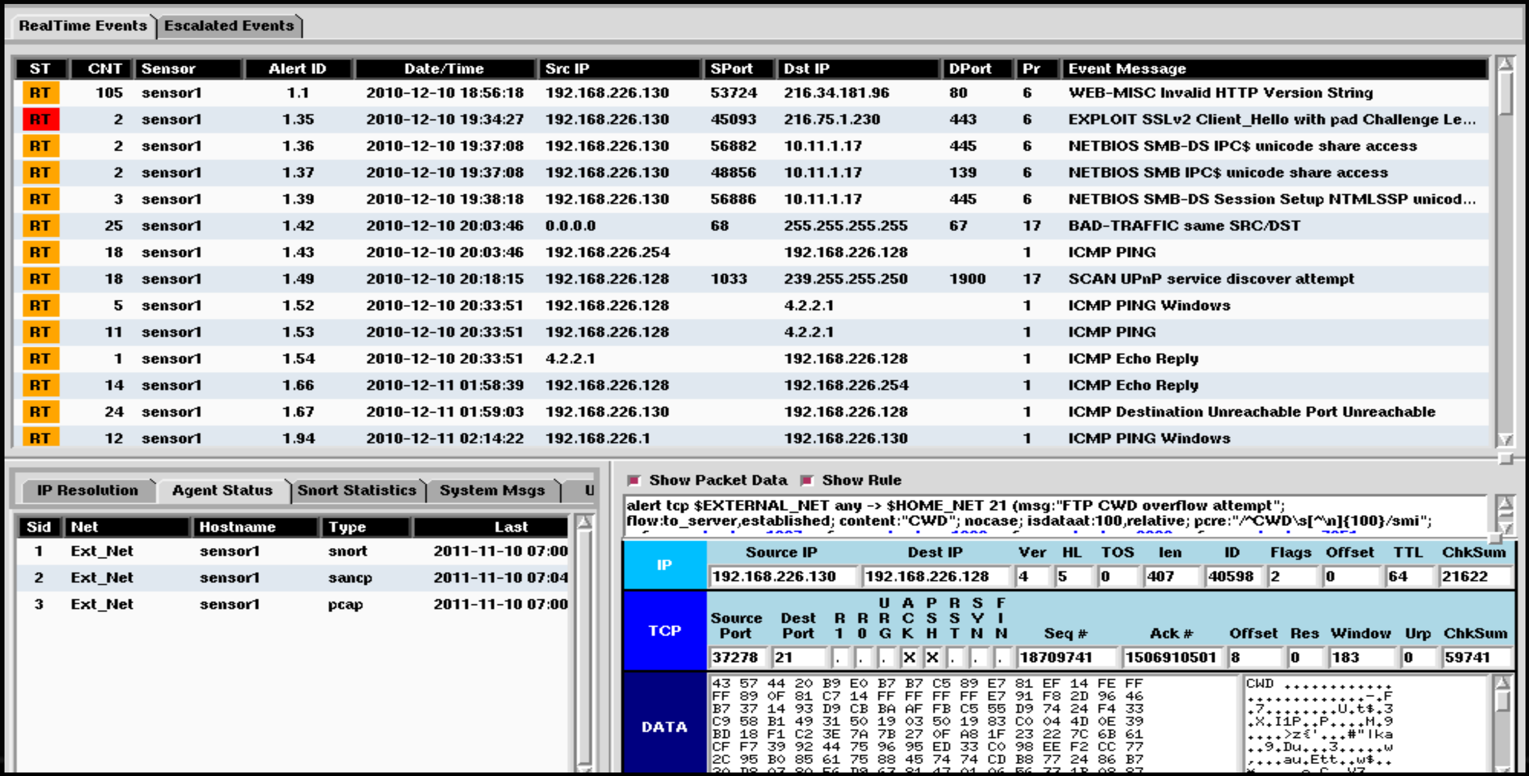
will automatically configure most details of your
will create a Snort sensor for each network
your system.

tup gives you more control over the details of
, including:
install Sguil server, Sguil sensor, or both
ngine to use (Snort or Suricata)
- which Ethernet interfaces should be monitored
- which IDS ruleset(s) to use (Emerging Threats, Snort VRT, or both)

Quick Setup is recommended for first-time users. Would you like to use Quick Setup?

# Security Onion -Sguil

- Sguil's interface provides the analyst with the ability to contextualize network traffic via Alert, Session, Full Content, and/or Statistical Data



| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 105 | sensor1 | 1.1 | 2010-12-10 18:56:18 | 192.168.226.130 | 53724 | 216.34.181.96 | 80 | 6 | WEB-MISC Invalid HTTP Version String |
| RT | 2 | sensor1 | 1.35 | 2010-12-10 19:34:27 | 192.168.226.130 | 45093 | 216.75.1.230 | 443 | 6 | EXPLOIT SSLv2 Client_Hello with pad Challenge Le... |
| RT | 2 | sensor1 | 1.36 | 2010-12-10 19:37:08 | 192.168.226.130 | 56882 | 10.11.1.17 | 445 | 6 | NETBIOS SMB-DS IPC$ unicode share access |
| RT | 2 | sensor1 | 1.37 | 2010-12-10 19:37:08 | 192.168.226.130 | 48856 | 10.11.1.17 | 139 | 6 | NETBIOS SMB IPC$ unicode share access |
| RT | 3 | sensor1 | 1.39 | 2010-12-10 19:38:18 | 192.168.226.130 | 56886 | 10.11.1.17 | 445 | 6 | NETBIOS SMB-DS Session Setup NTMLSSP unicod... |
| RT | 25 | sensor1 | 1.42 | 2010-12-10 20:03:46 | 0.0.0.0 | 68 | 255.255.255.255 | 67 | 17 | BAD-TRAFFIC same SRC/DST |
| RT | 18 | sensor1 | 1.43 | 2010-12-10 20:03:46 | 192.168.226.254 |  | 192.168.226.128 |  | 1 | ICMP PING |
| RT | 18 | sensor1 | 1.49 | 2010-12-10 20:18:15 | 192.168.226.128 | 1033 | 239.255.255.250 | 1900 | 17 | SCAN UPnP service discover attempt |
| RT | 5 | sensor1 | 1.52 | 2010-12-10 20:33:51 | 192.168.226.128 |  | 4.2.2.1 |  | 1 | ICMP PING Windows |
| RT | 11 | sensor1 | 1.53 | 2010-12-10 20:33:51 | 192.168.226.128 |  | 4.2.2.1 |  | 1 | ICMP PING |
| RT | 1 | sensor1 | 1.54 | 2010-12-10 20:33:51 | 4.2.2.1 |  | 192.168.226.128 |  | 1 | ICMP Echo Reply |
| RT | 14 | sensor1 | 1.66 | 2010-12-11 01:58:39 | 192.168.226.128 |  | 192.168.226.254 |  | 1 | ICMP Echo Reply |
| RT | 24 | sensor1 | 1.67 | 2010-12-11 01:59:03 | 192.168.226.130 |  | 192.168.226.128 |  | 1 | ICMP Destination Unreachable Port Unreachable |
| RT | 12 | sensor1 | 1.94 | 2010-12-11 02:14:22 | 192.168.226.1 |  | 192.168.226.130 |  | 1 | ICMP PING Windows |

| Sid | Net | Hostname | Type | Last |
|---|---|---|---|---|
| 1 | Ext_Net | sensor1 | snort | 2011-11-10 07:00 |
| 2 | Ext_Net | sensor1 | sancp | 2011-11-10 07:04 |
| 3 | Ext_Net | sensor1 | pcap | 2011-11-10 07:00 |

■ Show Packet Data ■ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CWD overflow attempt";
flow:to_server,established; content:"CWD"; nocase; isdataat:100,relative; pcre:"/^CWD\s[^\n]{100}/smi";
```

| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum |
|---|---|---|---|---|---|---|---|---|---|---|---|
|  | 192.168.226.130 | 192.168.226.128 | 4 | 5 | 0 | 407 | 40598 | 2 | 0 | 64 | 21622 |

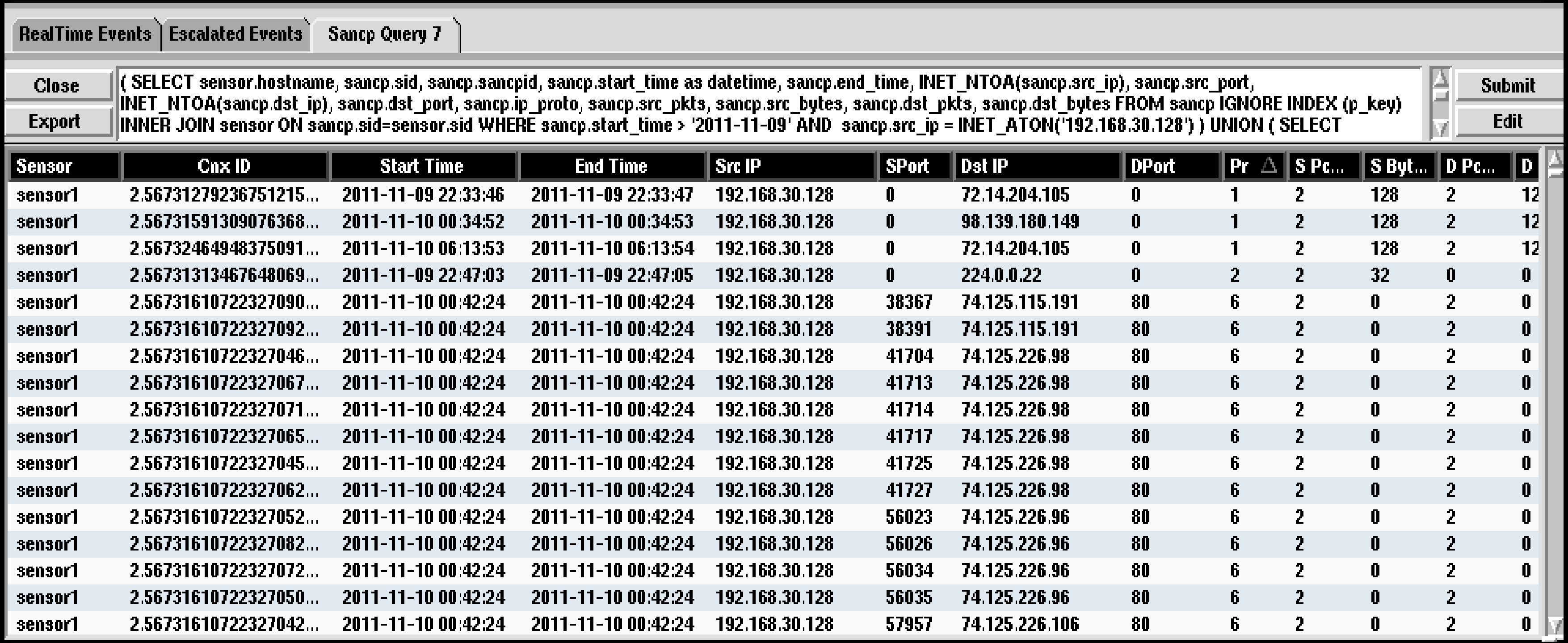
| TCP | Source Port | Dest Port | R 1 | R 0 | U R G | A C K | P S H | R S T | S Y N | F I N | Seq # | Ack # | Offset | Res | Window | Urp | ChkSum |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | 37278 | 21 | . | . | . | X | X | . | . | . | 18709741 | 1506910501 | 8 | 0 | 183 | 0 | 59741 |

DATA

```
43 57 44 20 B9 E0 B7 B7 C5 89 E7 81 EF 14 FE FF    CWD ............
FF 89 0F 81 C7 14 FF FF FF FF E7 91 F8 2D 96 46    .............-.F
B7 37 14 93 D9 CB BA AF FB C5 55 D9 74 24 F4 33    .7........U.t$.3
C9 58 B1 49 31 50 19 03 50 19 83 C0 04 4D 0E 39    .X.I1P..P....M.9
BD 18 F1 C2 3E 7A 7B 27 0F A8 1F 23 22 7C 6B 61    ....>z{'...#"|ka
CF F7 39 92 44 75 96 95 ED 33 C0 98 EE F2 CC 77    ..9.Du...3.....w
2C 95 B0 85 61 75 88 45 74 74 CD B8 77 24 86 B7    ,...au.Ett..w$..
```

# Security Onion -iv

- Utilizing Squil to view session data

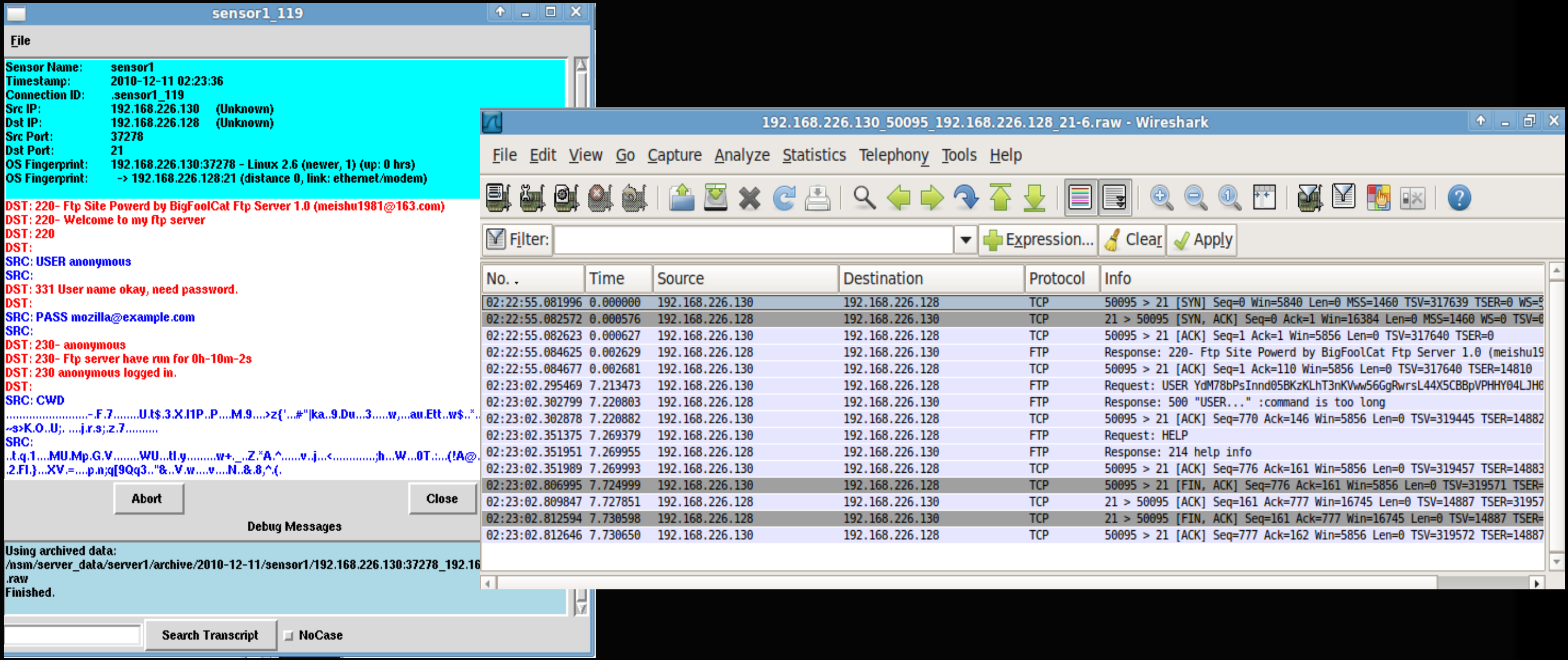


```
( SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port,
INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts, sancp.dst_bytes FROM sancp IGNORE INDEX (p_key)
INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2011-11-09' AND  sancp.src_ip = INET_ATON('192.168.30.128') ) UNION ( SELECT
```

| Sensor | Cnx ID | Start Time | End Time | Src IP | SPort | Dst IP | DPort | Pr △ | S Pc... | S Byt... | D Pc... | D |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| sensor1 | 2.56731279236751215... | 2011-11-09 22:33:46 | 2011-11-09 22:33:47 | 192.168.30.128 | 0 | 72.14.204.105 | 0 | 1 | 2 | 128 | 2 | 12 |
| sensor1 | 2.56731591309076368... | 2011-11-10 00:34:52 | 2011-11-10 00:34:53 | 192.168.30.128 | 0 | 98.139.180.149 | 0 | 1 | 2 | 128 | 2 | 12 |
| sensor1 | 2.56732464948375091... | 2011-11-10 06:13:53 | 2011-11-10 06:13:54 | 192.168.30.128 | 0 | 72.14.204.105 | 0 | 1 | 2 | 128 | 2 | 12 |
| sensor1 | 2.56731313467648069... | 2011-11-09 22:47:03 | 2011-11-09 22:47:05 | 192.168.30.128 | 0 | 224.0.0.22 | 0 | 2 | 2 | 32 | 0 | 0 |
| sensor1 | 2.56731610722327090... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 38367 | 74.125.115.191 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327092... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 38391 | 74.125.115.191 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327046... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 41704 | 74.125.226.98 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327067... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 41713 | 74.125.226.98 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327071... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 41714 | 74.125.226.98 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327065... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 41717 | 74.125.226.98 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327045... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 41725 | 74.125.226.98 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327062... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 41727 | 74.125.226.98 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327052... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 56023 | 74.125.226.96 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327082... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 56026 | 74.125.226.96 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327072... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 56034 | 74.125.226.96 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327050... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 56035 | 74.125.226.96 | 80 | 6 | 2 | 0 | 2 | 0 |
| sensor1 | 2.56731610722327042... | 2011-11-10 00:42:24 | 2011-11-10 00:42:24 | 192.168.30.128 | 57957 | 74.125.226.106 | 80 | 6 | 2 | 0 | 2 | 0 |

# Security Onion -ii

- Squil can render full content data via its transcript function or by calling Wireshark


sensor1_119
File
Abort
Close
Debug Messages
Search Transcript
□ NoCase
192.168.226.130_50095_192.168.226.128_21-6.raw - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply

```
Sensor Name:      sensor1
Timestamp:        2010-12-11 02:23:36
Connection ID:    .sensor1_119
Src IP:           192.168.226.130    (Unknown)
Dst IP:           192.168.226.128    (Unknown)
Src Port:         37278
Dst Port:         21
OS Fingerprint:   192.168.226.130:37278 - Linux 2.6 (newer, 1) (up: 0 hrs)
OS Fingerprint:     -> 192.168.226.128:21 (distance 0, link: ethernet/modem)

DST: 220- Ftp Site Powerd by BigFoolCat Ftp Server 1.0 (meishu1981@163.com)
DST: 220- Welcome to my ftp server
DST: 220
DST:
SRC: USER anonymous
SRC:
DST: 331 User name okay, need password.
DST:
SRC: PASS mozilla@example.com
SRC:
DST: 230- anonymous
DST: 230- Ftp server have run for 0h-10m-2s
DST: 230 anonymous logged in.
DST:
SRC: CWD
........................-.F.7........U.t$.3.X.I1P..P....M.9....>z{'...#"|ka..9.Du...3.....w,...au.Ett..w$..*..
~s>K.O..U;. ....j.r.s;.z.7..........
SRC:
..t.q.1....MU.Mp.G.V........WU...tl.y.........w+._..Z.*A.^......v..j...<............;h...W...0T.:...(!A@.
.2.Fl.}...XV.=....p.n;q[9Qq3.."&..V.w....v....N..&.8,^.(.
```

```
Using archived data:
/nsm/server_data/server1/archive/2010-12-11/sensor1/192.168.226.130:37278_192.16
.raw
Finished.
```

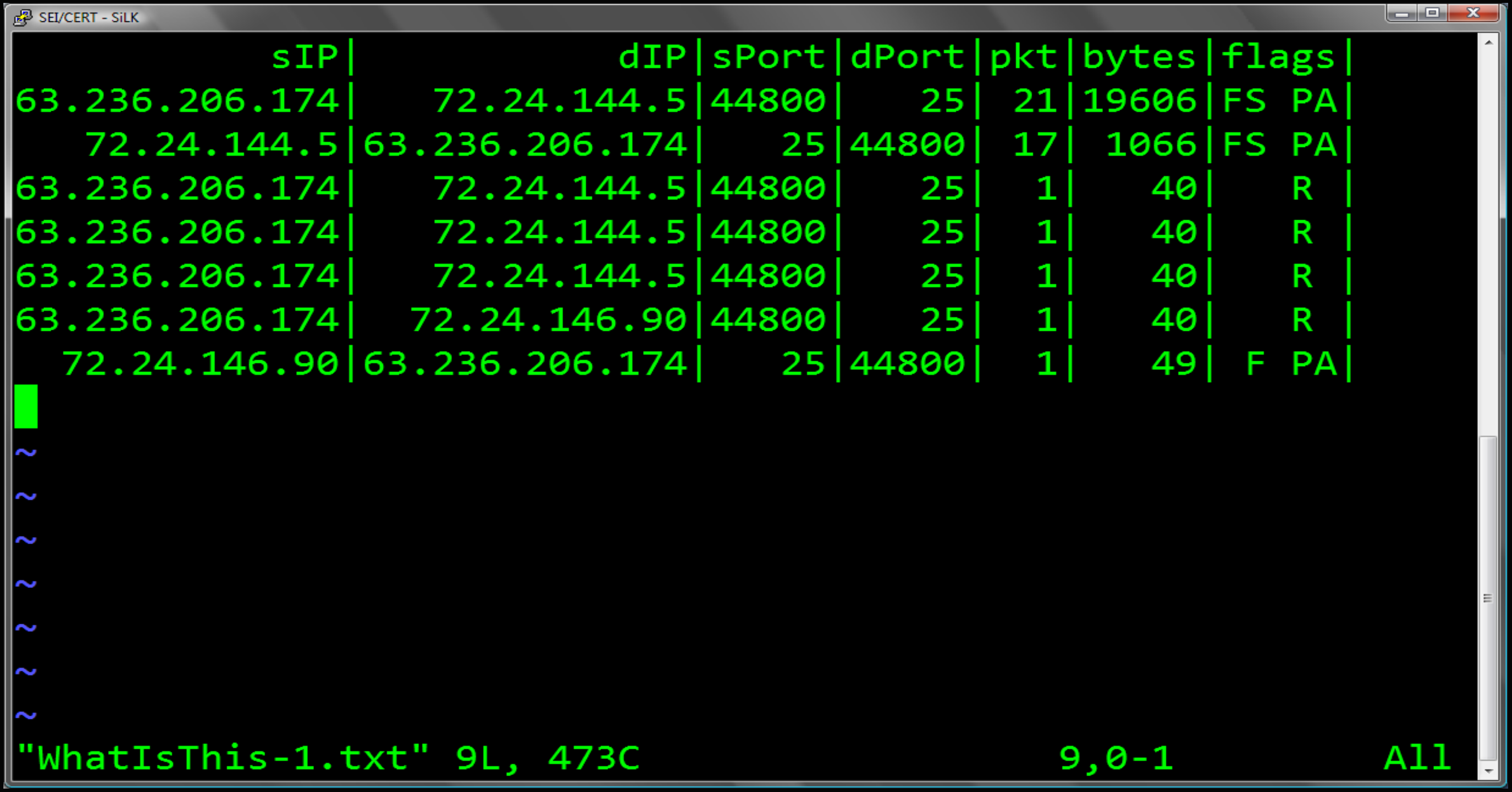
| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 02:22:55.081996 | 0.000000 | 192.168.226.130 | 192.168.226.128 | TCP | 50095 > 21 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=317639 TSER=0 WS=5 |
| 02:22:55.082572 | 0.000576 | 192.168.226.128 | 192.168.226.130 | TCP | 21 > 50095 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0 TSV=0 |
| 02:22:55.082623 | 0.000627 | 192.168.226.130 | 192.168.226.128 | TCP | 50095 > 21 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSV=317640 TSER=0 |
| 02:22:55.084625 | 0.002629 | 192.168.226.128 | 192.168.226.130 | FTP | Response: 220- Ftp Site Powerd by BigFoolCat Ftp Server 1.0 (meishu19 |
| 02:22:55.084677 | 0.002681 | 192.168.226.130 | 192.168.226.128 | TCP | 50095 > 21 [ACK] Seq=1 Ack=110 Win=5856 Len=0 TSV=317640 TSER=14810 |
| 02:23:02.295469 | 7.213473 | 192.168.226.130 | 192.168.226.128 | FTP | Request: USER YdM78bPsInnd05BKzKLhT3nKVww56GgRwrsL44X5CBBpVPHHY04LJH0 |
| 02:23:02.302799 | 7.220803 | 192.168.226.128 | 192.168.226.130 | FTP | Response: 500 "USER..." :command is too long |
| 02:23:02.302878 | 7.220882 | 192.168.226.130 | 192.168.226.128 | TCP | 50095 > 21 [ACK] Seq=770 Ack=146 Win=5856 Len=0 TSV=319445 TSER=14882 |
| 02:23:02.351375 | 7.269379 | 192.168.226.130 | 192.168.226.128 | FTP | Request: HELP |
| 02:23:02.351951 | 7.269955 | 192.168.226.128 | 192.168.226.130 | FTP | Response: 214 help info |
| 02:23:02.351989 | 7.269993 | 192.168.226.130 | 192.168.226.128 | TCP | 50095 > 21 [ACK] Seq=776 Ack=161 Win=5856 Len=0 TSV=319457 TSER=14883 |
| 02:23:02.806995 | 7.724999 | 192.168.226.130 | 192.168.226.128 | TCP | 50095 > 21 [FIN, ACK] Seq=776 Ack=161 Win=5856 Len=0 TSV=319571 TSER= |
| 02:23:02.809847 | 7.727851 | 192.168.226.128 | 192.168.226.130 | TCP | 21 > 50095 [ACK] Seq=161 Ack=777 Win=16745 Len=0 TSV=14887 TSER=31957 |
| 02:23:02.812594 | 7.730598 | 192.168.226.128 | 192.168.226.130 | TCP | 21 > 50095 [FIN, ACK] Seq=161 Ack=777 Win=16745 Len=0 TSV=14887 TSER= |
| 02:23:02.812646 | 7.730650 | 192.168.226.130 | 192.168.226.128 | TCP | 50095 > 21 [ACK] Seq=777 Ack=162 Win=5856 Len=0 TSV=319572 TSER=14887 |

# Session Data With NetFlow

- NetFlow is a traffic-summarization format that was first implemented by Cisco Systems and other router manufacturing companies, primarily for billing purposes
- Some of the NetFlow standard fields
  - source address, destination address
  - source port, destination port
  - protocol
  - bytes, packets
  - TCP flags
  - start time, duration
  - end time
  - sensor identification

# Session Data With NetFlow ii

- Sample flow data

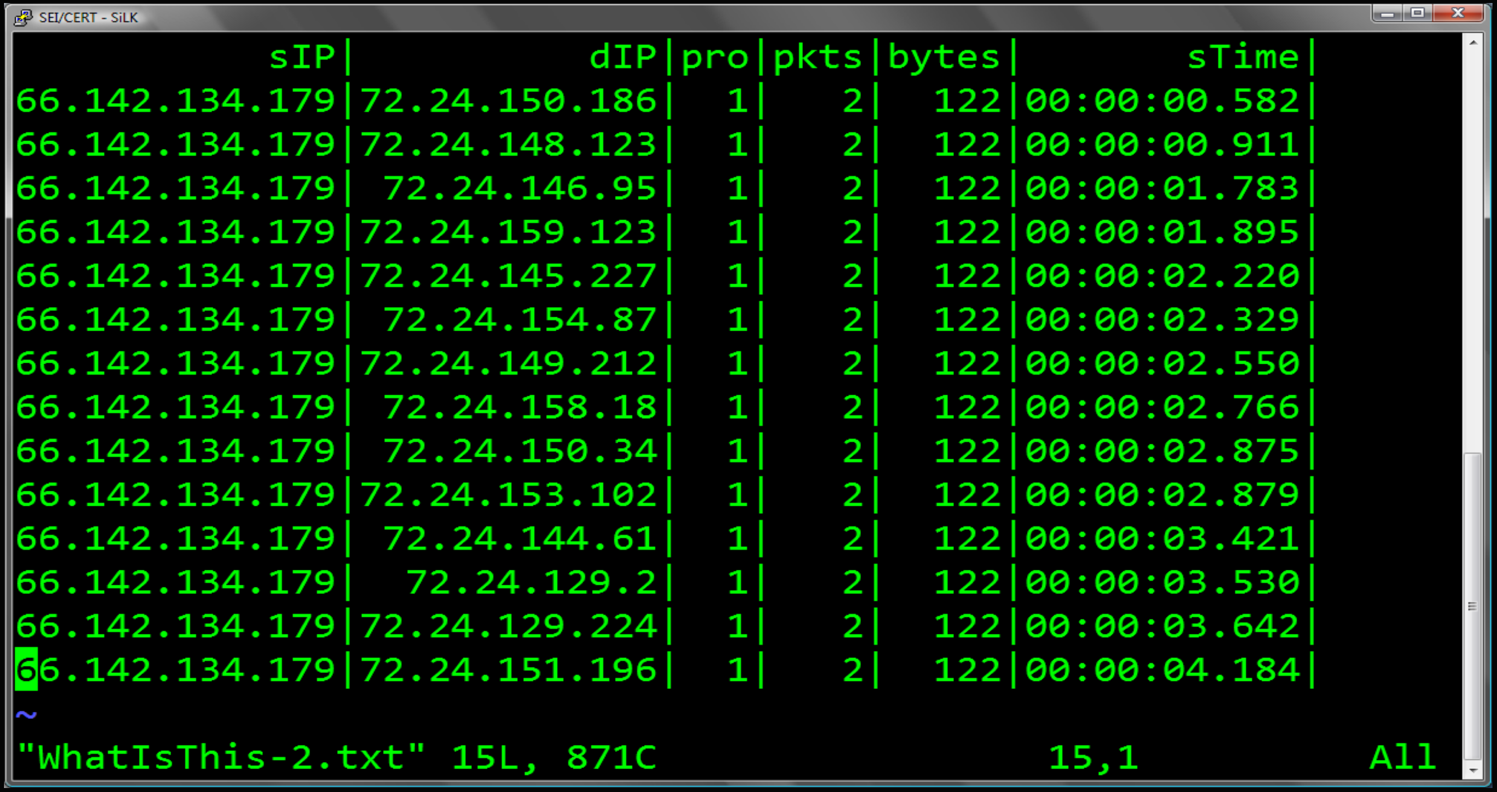


```
           sIP|           dIP|sPort|dPort|pkt|bytes|flags|
63.236.206.174|   72.24.144.5|44800|   25| 21|19606|FS PA|
   72.24.144.5|63.236.206.174|   25|44800| 17| 1066|FS PA|
63.236.206.174|   72.24.144.5|44800|   25|  1|   40|   R |
63.236.206.174|   72.24.144.5|44800|   25|  1|   40|   R |
63.236.206.174|   72.24.144.5|44800|   25|  1|   40|   R |
63.236.206.174|  72.24.146.90|44800|   25|  1|   40|   R |
  72.24.146.90|63.236.206.174|   25|44800|  1|   49| F PA|

~
~
~
~
~
~
~
"WhatIsThis-1.txt" 9L, 473C                  9,0-1         All
```

# Session Data With NetFlow iii

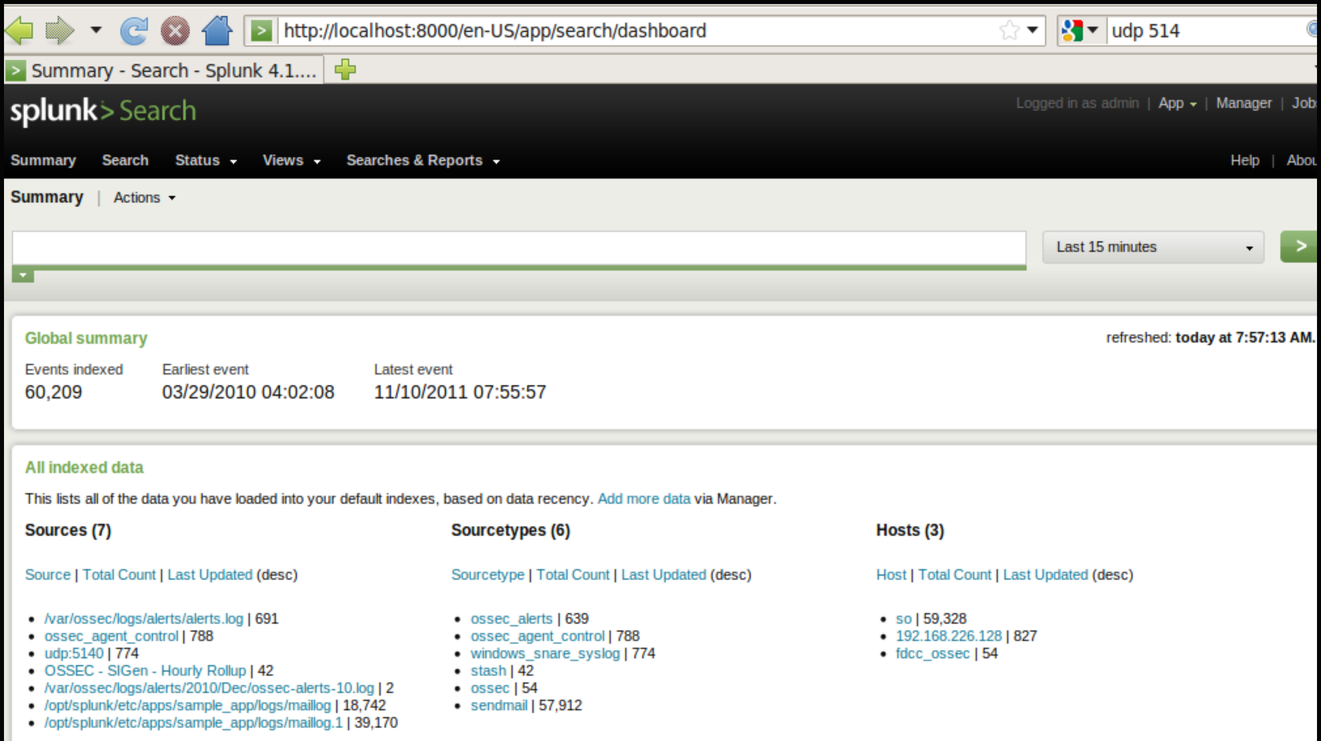
- Tools such as fprobe, and flow-tools can help



```
           sIP|          dIP|pro|pkts|bytes|       sTime|
66.142.134.179|72.24.150.186|  1|   2|  122|00:00:00.582|
66.142.134.179|72.24.148.123|  1|   2|  122|00:00:00.911|
66.142.134.179| 72.24.146.95|  1|   2|  122|00:00:01.783|
66.142.134.179|72.24.159.123|  1|   2|  122|00:00:01.895|
66.142.134.179|72.24.145.227|  1|   2|  122|00:00:02.220|
66.142.134.179| 72.24.154.87|  1|   2|  122|00:00:02.329|
66.142.134.179|72.24.149.212|  1|   2|  122|00:00:02.550|
66.142.134.179| 72.24.158.18|  1|   2|  122|00:00:02.766|
66.142.134.179| 72.24.150.34|  1|   2|  122|00:00:02.875|
66.142.134.179|72.24.153.102|  1|   2|  122|00:00:02.879|
66.142.134.179| 72.24.144.61|  1|   2|  122|00:00:03.421|
66.142.134.179|  72.24.129.2|  1|   2|  122|00:00:03.530|
66.142.134.179|72.24.129.224|  1|   2|  122|00:00:03.642|
66.142.134.179|72.24.151.196|  1|   2|  122|00:00:04.184|
~
"WhatIsThis-2.txt" 15L, 871C                 15,1          All
```

# Log Analysis

- Splunk, collects and indexes machine data, such as logging data
- Free to download



http://localhost:8000/en-US/app/search/dashboard
udp 514
Summary - Search - Splunk 4.1....
splunk> Search
Logged in as admin | App | Manager | Job
Summary Search Status Views Searches & Reports
Help | Abou
Summary | Actions
Last 15 minutes
>

Global summary

refreshed: **today at 7:57:13 AM.**

| Events indexed | Earliest event | Latest event |
|---|---|---|
| 60,209 | 03/29/2010 04:02:08 | 11/10/2011 07:55:57 |

All indexed data

This lists all of the data you have loaded into your default indexes, based on data recency. Add more data via Manager.

**Sources (7)**

Source | Total Count | Last Updated (desc)

- /var/ossec/logs/alerts/alerts.log | 691
- ossec_agent_control | 788
- udp:5140 | 774
- OSSEC - SIGen - Hourly Rollup | 42
- /var/ossec/logs/alerts/2010/Dec/ossec-alerts-10.log | 2
- /opt/splunk/etc/apps/sample_app/logs/maillog | 18,742
- /opt/splunk/etc/apps/sample_app/logs/maillog.1 | 39,170

**Sourcetypes (6)**

Sourcetype | Total Count | Last Updated (desc)

- ossec_alerts | 639
- ossec_agent_control | 788
- windows_snare_syslog | 774
- stash | 42
- ossec | 54
- sendmail | 57,912

**Hosts (3)**

Host | Total Count | Last Updated (desc)

- so | 59,328
- 192.168.226.128 | 827
- fdcc_ossec | 54

# Agenda

- Introduction
- Current State
- Defensive Strategies
- Conclusion

# Conclusion

- NSM uses an alert as the beginning of the investigative process, not the conclusion
  - Assists the analyst in establishing network situation awareness to track and suppress intrusions
- Data breaches are costing businesses millions of dollars
- Don’t let a  customer be your first notification that something is amiss within your current data protection and compliance program
- NSM can be initiated
- It is the responsibility of assigned organizational management to take reasonable and appropriate measures to safeguard sensitive information in line with regulatory demands and consumer expectations

# Resources

- Security Onion
  - http://securityonion.blogspot.com/
- Richard Bejtlich
  - "The Tao of Network Security Monitoring"
- CERT
  - http://www.cert.org
- Forum of Incident Response & Security Teams ("FIRST")
  - http://www.first.org

# Questions?

> there is no secure end-state - only constant vigilance

THANK YOU!

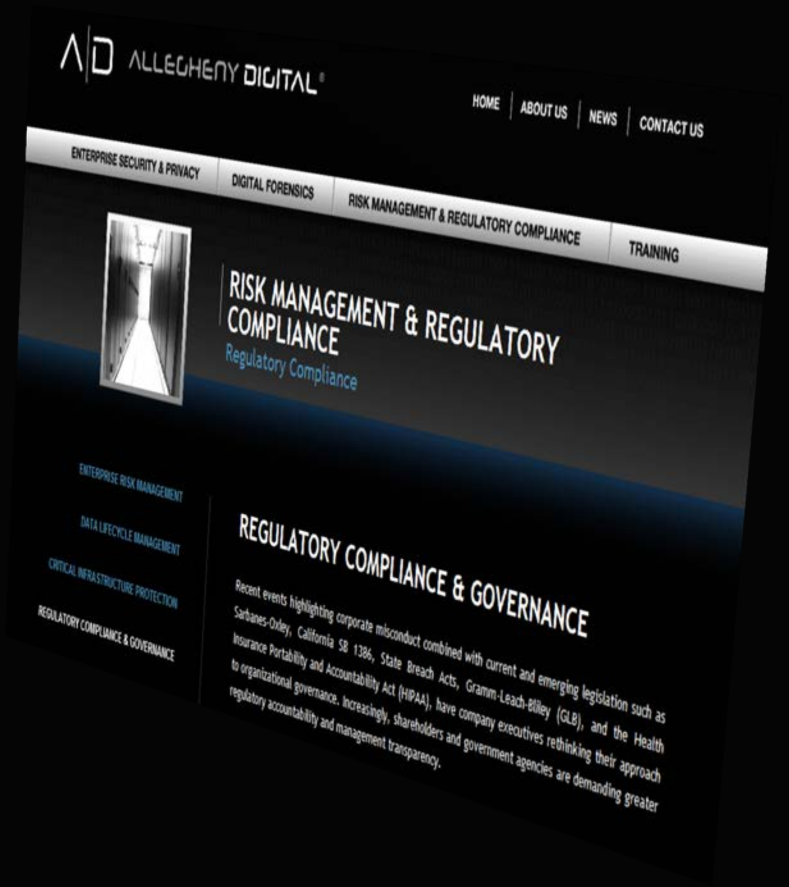
www.alleghenydigital.com

1.877.234.0001

ALLEGHENY DIGITAL

# ALLEGHENY DIGITAL

- Professional Services
  - Information Security Consulting
  - Managed Services
  - Training & Education
- Breadth of Experience
  - Healthcare
  - Manufacturing
  - Technology
  - Education
  - Finance
  - Energy
- Western PA based


A|D ALLEGHENY DIGITAL®
HOME
ABOUT US
NEWS
CONTACT US
ENTERPRISE SECURITY & PRIVACY
DIGITAL FORENSICS
RISK MANAGEMENT & REGULATORY COMPLIANCE
TRAINING
ENTERPRISE RISK MANAGEMENT
DATA LIFECYCLE MANAGEMENT
CRITICAL INFRASTRUCTURE PROTECTION
REGULATORY COMPLIANCE & GOVERNANCE

RISK MANAGEMENT & REGULATORY COMPLIANCE

Regulatory Compliance

REGULATORY COMPLIANCE & GOVERNANCE

Recent events highlighting corporate misconduct combined with current and emerging legislation such as Sarbanes-Oxley, California SB 1386, State Breach Acts, Gramm-Leach-Bliley (GLB), and the Health Insurance Portability and Accountability Act (HIPAA), have company executives rethinking their approach to organizational governance. Increasingly, shareholders and government agencies are demanding greater regulatory accountability and management transparency.