Network Security Monitoring: Beyond Intrusion Detection

By: rewtninja

Agenda

- Overview of NSM
- Benefits of NSM
- NSM vs IDS
- Limitations of NSM
- Free solutions for implementing NSM
- DEMO

Whoami?

- Security enthusiast
- SecOps for an int’l software/cloud company. We are hiring!
- <Insert Certifications Here>

Disclaimer?

- The standard … blah blah blah

Why Monitor?

NSM Principle 1: Some intruders are smarter than you are

Why Monitor?

NSM Principle 2: Intruders are unpredictable

Why Monitor?

NSM Principle 3: Prevention eventually fails

Cute Bears! But what is NSM?

- 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.

- It is more than just waiting for an alert to trigger, Successful NSM operations are always collecting multiple forms of NSM data, using some of it for matching activities (via IDS and related systems) and hunting activities (via human review of NSM data)

- More info / Credits
  - "The practice of Network Security Monitoring" – R. Bejtlich
  - http://taosecurity.blogspot.com – Mandiant CSO blog
  - http://www.securityonion.net

Benefits of NSM

- Improve Detection of the following:
  - ✓ Potential network intrusions
  - ✓ Network resources abuse
  - ✓ Malware
  - ✓ Data exfiltration/leakage

- Improve Incident Response

- Improve Evidence Collection - Law enforcement, Legal

- Improve security visibility into network

- Additional tool against Advance Persistent Threats (APT)

“**Retrospective Security Analysis**: checking your old **#NSM** data for Indicators Of Compromise that you didn't know were applicable at the time the intruder acted”

I have an IDS, what makes NSM better?

- NSM takes IDS into a whole new level

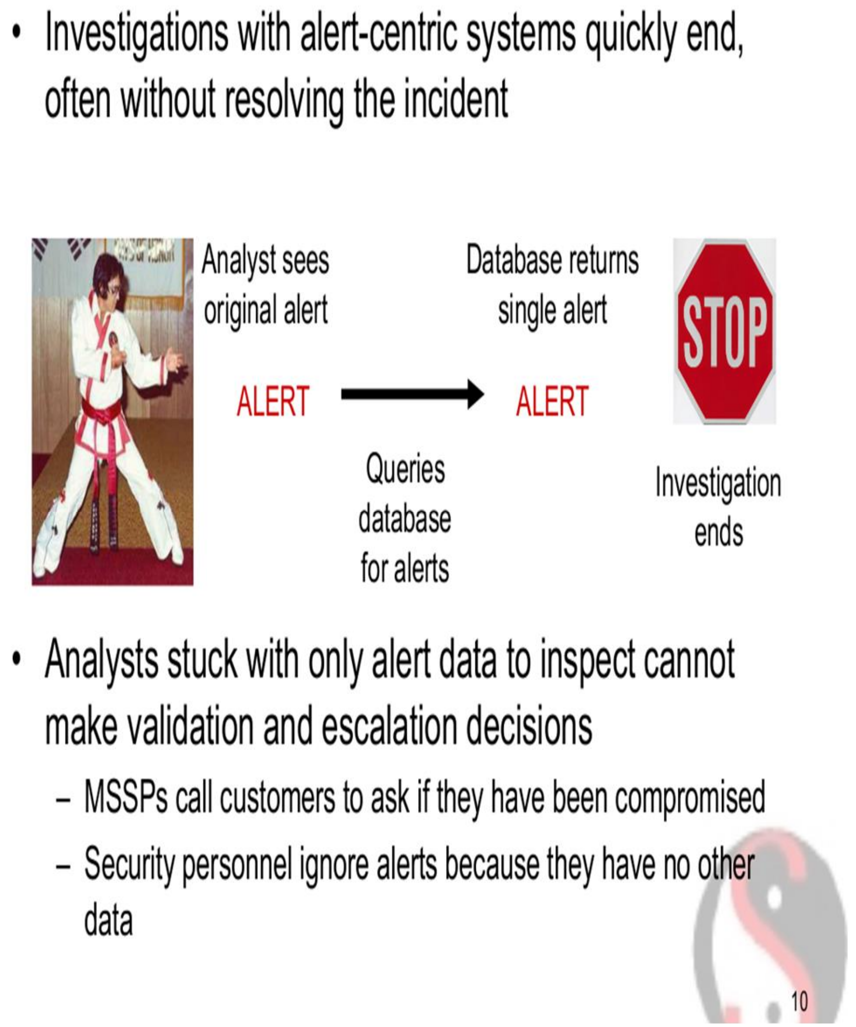
- Better data for analysis, validation, escalation
  - **Alert Data** - Pointer to the data that triggers an anomaly. Usually by a tool such as IDS
  - **Transaction Data** - Focuses on understanding the requests and replies exchanged between two network devices.(e.g. HTTP,FTP,SMTP)
  - **Session Data** - Conversation Flow. Network connections to and from a device
  - **Full Content Data** - Full accounting for every data packet transmitted between two endpoints.
  - **Statistical data** Descriptive information that characterizes network activity, like counts of various aspects of conversations
  - **Log data** – eg. Syslog, OS/Firewall/Router logs

NSM vs IDS Data Comparison

Data	NSM	IDS
Alert Data – Pointer to the data that triggers an anomaly. Usually by a tool such as IDS	✓ YES	YES
Transaction Data - Focuses on understanding the requests and replies exchanged between two network devices.(e.g. HTTP,FTP,SMTP)	✓ YES	NO
Session Data – Conversation Flow. Network connections to and from a device	✓ YES	NO
Full Content Data - Full accounting for every data packet transmitted between two endpoints.	✓ YES	NO
Statistical Data - Descriptive information that characterizes network activity, like counts of various aspects of conversations	✓ YES	NO

NSM vs IDS Workflow comparison

IDS



- Investigations with alert-centric systems quickly end, often without resolving the incident

Analyst sees original alert

ALERT → ALERT

Queries database for alerts

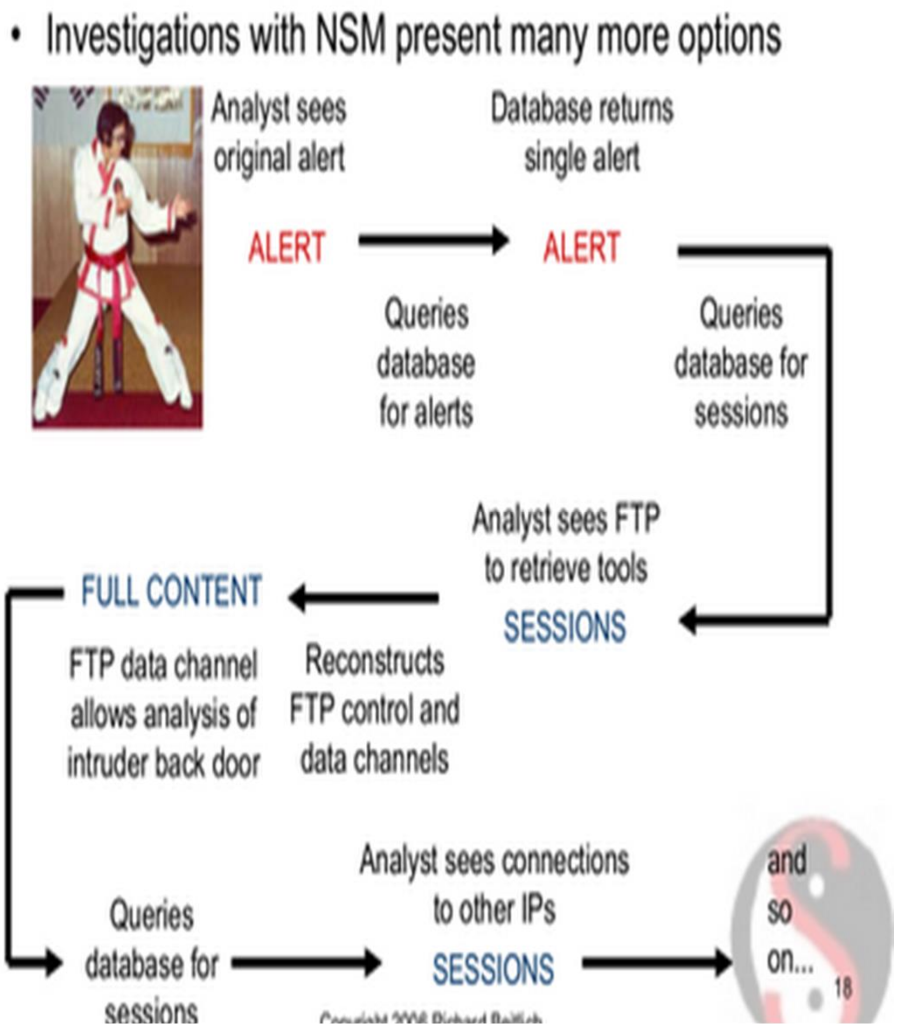
Database returns single alert

STOP

Investigation ends

- Analysts stuck with only alert data to inspect cannot make validation and escalation decisions
  - MSSPs call customers to ask if they have been compromised
  - Security personnel ignore alerts because they have no other data

NSM



- Investigations with NSM present many more options

Analyst sees original alert

ALERT → ALERT

Queries database for alerts

Database returns single alert

Queries database for sessions

Analyst sees FTP to retrieve tools

SESSIONS

Reconstructs FTP control and data channels

FULL CONTENT

FTP data channel allows analysis of intruder back door

Queries database for sessions

Analyst sees connections to other IPs

SESSIONS

and so on...

NSM vs IDS

- All these NSM data makes it easier for an analyst to validate alerts and make decisions or escalations

- In the case of IDS, when an analyst does not have enough information on a particular alert, they tend to just ignore it.

OK.. But what are NSM Limitations?

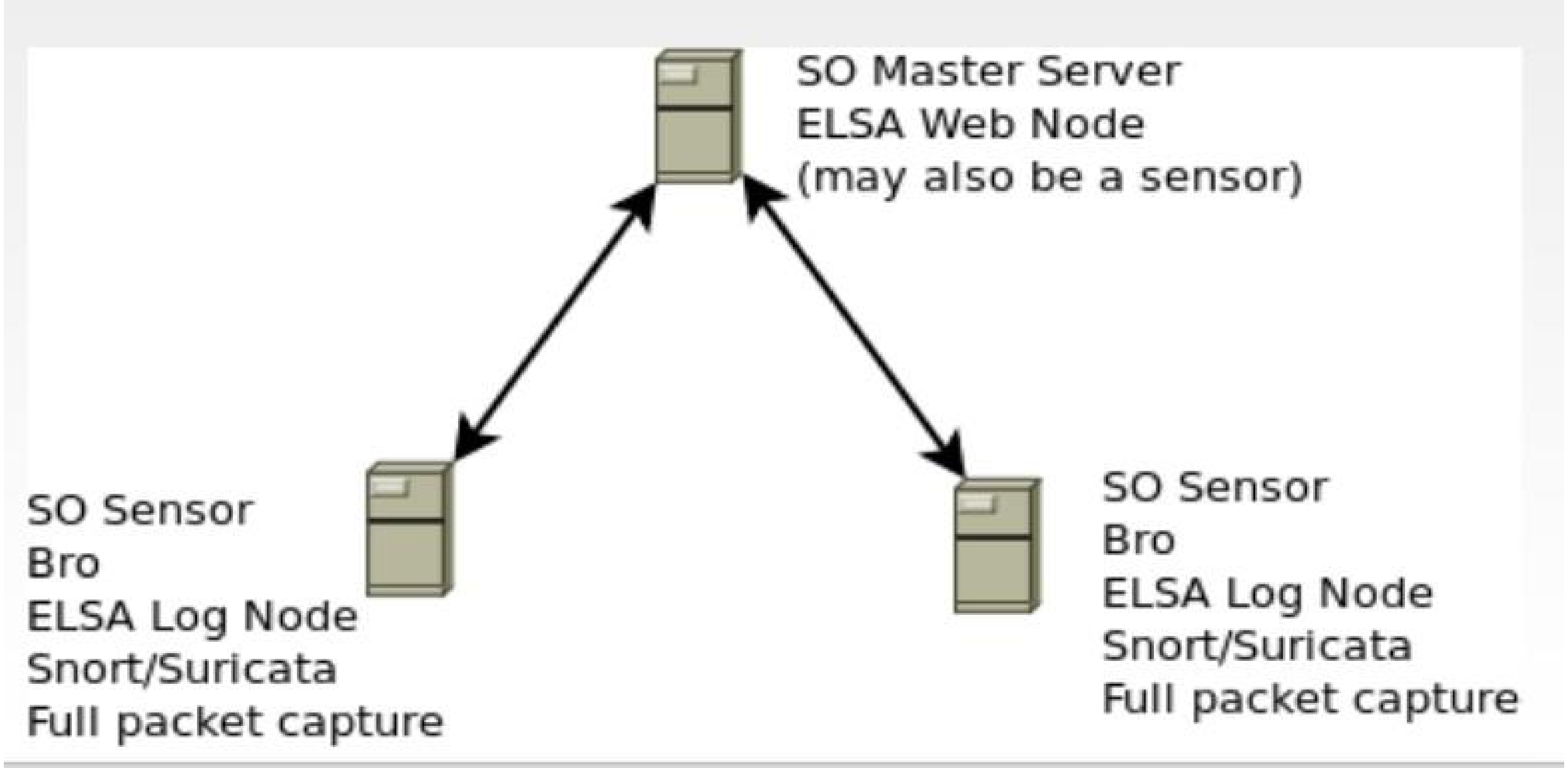
- Blind to Encrypted Traffic
  - Commercial web filtering solutions have the capability to decrypt SSL and offload decrypted SSL traffic into a port where you can connect the NSM solution
  - SSL Gateway
  - SSLSniff / ViewSSLD?
    - Considerations when **inspecting SSL traffic.**
      - Privacy / Legal – prohibited by laws from other countries
      - Compliance - sox/pci.
- **Mobile** platforms
- Extreme traffic volume may overwhelm NSM platforms

What NSM Solutions are freely available out there?

- SecurityOnion – www.securityonion.net
- Ubuntu Linux OS, Open Source - free – GNU GPL v2.0
- Leverages mature open source security products
  - Snort/Suricata, Bro, OSSEC
  - Elsa, Snorby, Squert
  - Sguil, Netsniff-ng, Argus
  - Etc …
- Actively maintained
  - Developer is the Deputy CSO of Mandiant (APT report)

Basic SecOnion Architecture

- Standalone
- Distributed



SO Master Server
ELSA Web Node
(may also be a sensor)

SO Sensor
Bro
ELSA Log Node
Snort/Suricata
Full packet capture

SO Sensor
Bro
ELSA Log Node
Snort/Suricata
Full packet capture

NSM Deployment Considerations

- Network traffic
- HD Space (lots of)
- Span vs Inline

DEMO!

- Enough of the boring stuff! :-D
- Let’s see the thing

Credits / References / Add'l Reading

- Richard Bejtlich – www. taosecurity.blogspot.com
- Doug Bourks – www.securityonion.net
- Securityonion Mailing List
- "The practice of Network Security Monitoring"
- "Applied Security Monitoring"

Questions?