NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Building Detection Capabilities

SANS North American SCADA 2012

January 2012

RELIABILITY | ACCOUNTABILITY



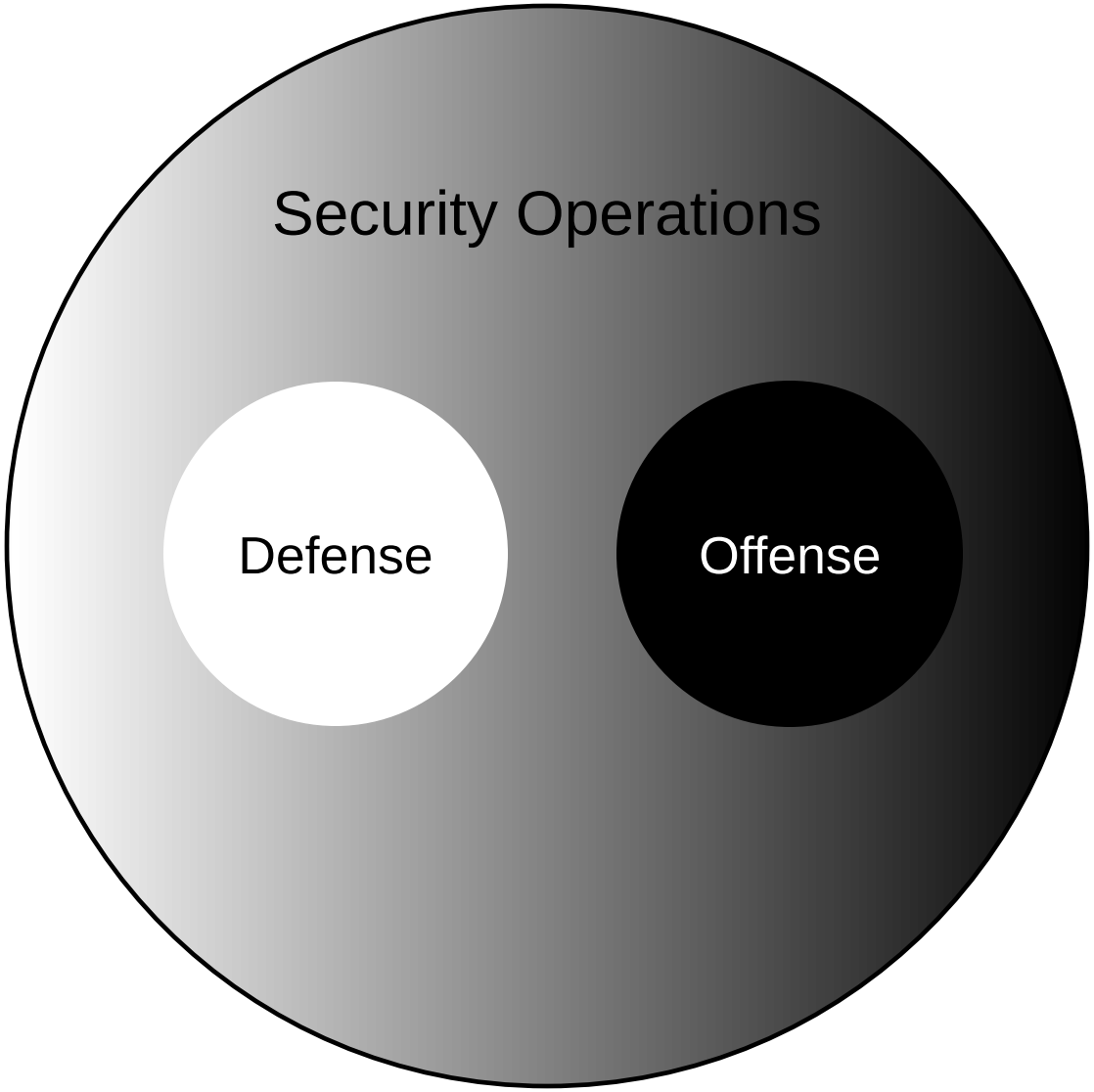

$ whoami

Ben Miller
NERC ES-ISAC
ben.miller@nerc.net

PGP: C7A6 A703 78EE 7134 7F82
3ED0 8A52 27B3 D99F 28DE

~
~
~
:w

Security Operations



"**Security Operations**" is how I refer to the idea that both offensive and defensive teams are in a constant competition. IMO, it's a good working mental model for defenders.

Richard Bejtlich aka @taosecurity aka Mandiant CSO

In 2004 authored *Tao of Network Security Monitoring*. NSM specifically can allow for great results with low investment (a few hours and a big hard drive)

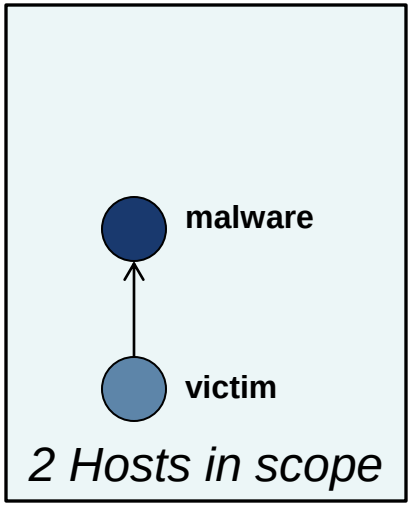
NSM Focus on 4 types Of Data:

Data	Tool examples
Alert	Snort, bro, scuracata
Session	Sancp, argus, netflow
Full Cap*	Daemonlogger
Statistical	Ntop
Transactional**	Httpry, dsniff, dnssnarf

*make sure your policy allows for monitoring of usage

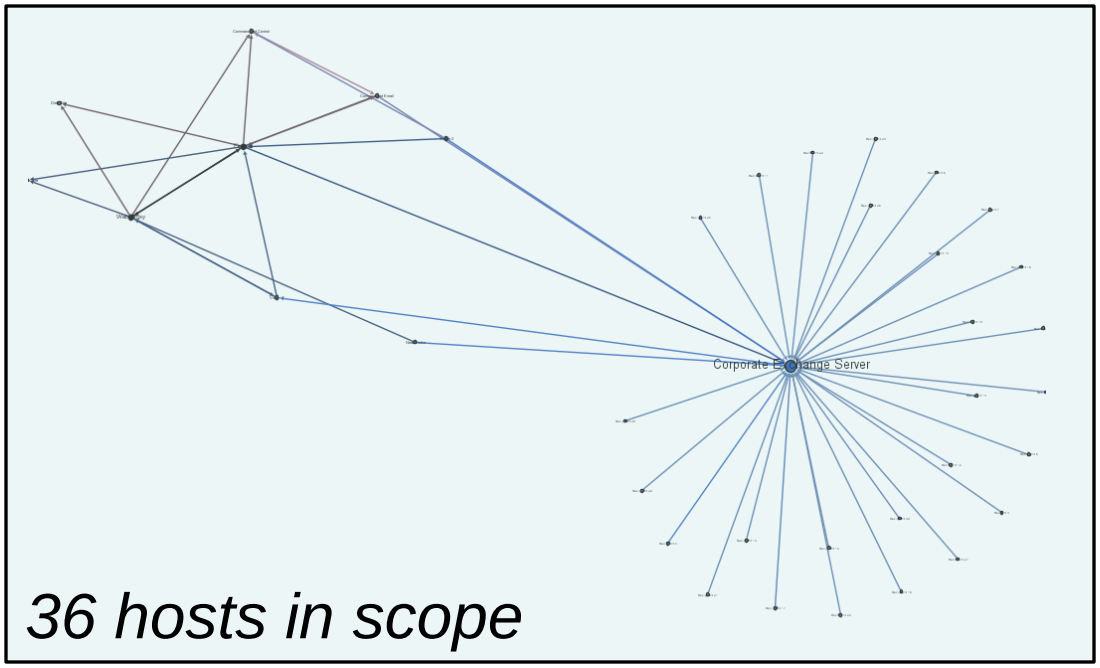
Data Pivoting

The idea behind data pivoting isn't to prove the scope of an incident; it's to prove the size of scope isn't bigger than what you believe it to be.

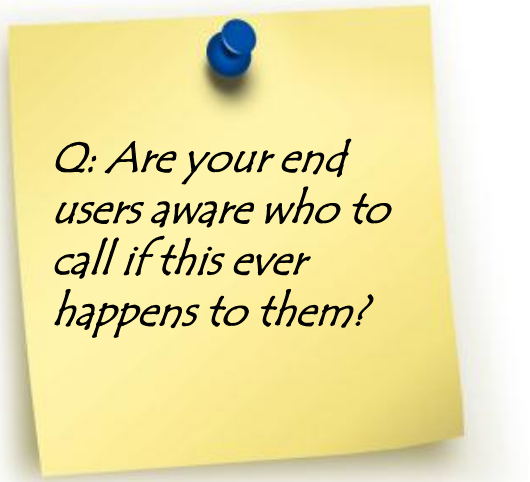


2 Hosts in scope

OR



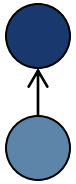
36 hosts in scope



"My adobe crashed. Uh, right after I opened a funny looking email.

End user report at 9:32

Automate or create a checklist for repetitive tasks

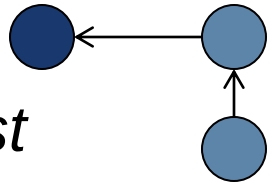


Prefetch shows 1.exe at 9:21; Funny email has funny.pdf attachment

Pivot off 9:32 timestamp

Keep logs as long as possible! It's rare to detect a breach in 10 minutes!

Web proxy shows 3 instances of 1.exe downloaded over last 30 minutes
http://evilinc.com/1.exe

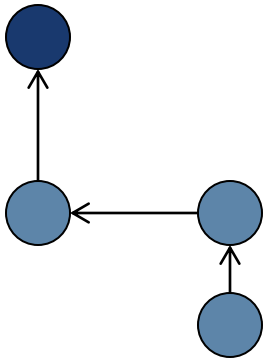


Pivot to 1.exe

Pivot off 9:32 timestamp

Web proxy shows 2 of these instances are followed 5 minutes later by large POSTs to http://evil2.com/save.php?

Your incident response plan should reflect all the actions you perform in the real world. Or it's just paper.



Pivot off activity of three victim hosts

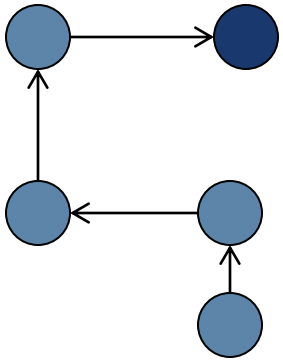
Pivot to 1.exe

Pivot off 9:32 timestamp

In house jabber/silc servers are great ways to share data and investigate as a team in real time .

DNS session data shows lookups to evil3example.com from victim hosts right before POSTs; no web proxy data; but we have the IP!

Pivot off +60mins after 1.exe



Pivot off activity of three victim hosts

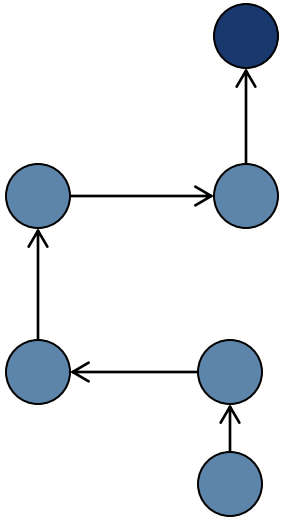
Pivot to 1.exe

Pivot off 9:32 timestamp

These examples do not show all the dead ends the analyst finds. This investigation may have taken a total of 2 or 3 hours.

Firewall sessions port 8181 traffic to evil3example.com immediately after DNS lookups

Pivot off +60mins after 1.exe



Pivot off IP Address

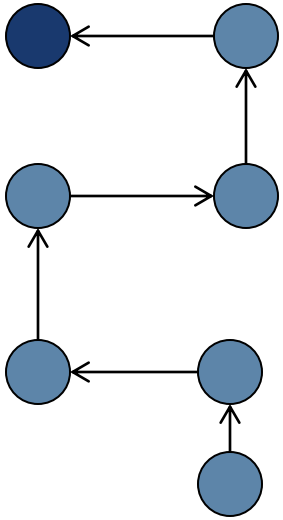
Pivot off activity of three victim hosts

Pivot to 1.exe

Pivot off 9:32 timestamp

The bad guys use your infrastructure against you. It's only fitting it also serves as an extremely valuable data source against them.

Now know the full scope. But do I? Let's go back to the email and search exchange mailboxes for funny.pdf. 15 recipients!



Found evil3example.com

Pivot off +60mins after 1.exe

Pivot off IP address

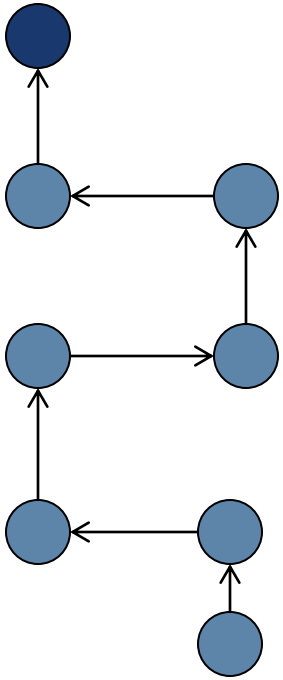
Pivot off activity of three victim hosts

Pivot to 1.exe

Pivot off 9:32 timestamp

Creativity is key. Your procedures or checklists should not stifle creativity but give it room to grow.

Hunch: broaden the email scope from funny.pdf to the sending MTA. Another 15 recipients found



Found evil3example.com

Pivot off +60mins after 1.exe

Pivot off IP address

Pivot off activity of three victim hosts

Pivot to 1.exe

Pivot off 9:32 timestamp

In Review

Uncovered malware host site and it's dropper file, 1.exe
Uncovered an exfiltration dropoff site
Uncovered the C2 server on port tcp/8181
Uncovered 3 users who opened the PDF; 2 of which were compromised
Uncovered a total of 30 potential victims

Knowledge

- **Incident logs** (tickets) create structured knowledge for metrics
  - ID, severity, date of first occurrence, date of detection, status of incident, notes, IOCs, attachments
- **Evidence retention** creates depth of knowledge and flexibility
  - Ability to revisit incidents and uncover previously unrecognized indicators which relate to another incident (begin mapping incidents to specific threats or campaigns)
- **Post incident reports** create an opportunity to learn – both short and long term
  - Gain insight on the attacker
  - Learn how to stop this attack and deter and detect similar attacks faster
  - Great case study for in the future
- **Information Sharing** develops a trust network where you can collaborate and learn from other defensive teams.
  - Learn how others deter, detect, response
  - Actively share your indicators of compromise
  - Can't figure out what a malware binary is doing? People like me love solving those sorts of problems. For free, even.

Training

Technical

- On The Job Training
  - Mentorship
  - Data Pivoting and Root Cause Analysis
- Drills
  - Technical Challenges (competition, or co-op CCTF)
  - Case Studies
- Books and Blogs
  - Both a physical and virtual bookshelf
- Conferences
  - Hacker Cons
  - Security Training
  - Security Conferences

Procedural

- Table Top Exercise Scenario (MSEL)
- Case Study
  - Historical
  - What If?

Things to do on Monday

Leverage existing data sources such as AV, IDS, netflow, web proxy logs and deploy NSM tools

Train for and actively seek security breaches.

Create structure through an incident response plan, but don't stifle creativity.

Seek out and understand the offensive operations TTP and resulting IOCs.

Question the implications of your own TTP and the resulting indicators.

Share your lessons and IOCs with a trusted community (hint :ES-ISAC)

Thank You

Books Worth Your Time:

- Tao of Network Security Monitoring by Bejtlich
- New School of Information Security by Shostack
- Checklist Manifesto: How to Get Things Right By Gawande
- The Art of War by Sunzi
- Strategies for Creative Problem Solving by LeBlanc
- Harvard Business Review on Leadership by HBR
- Managing Humans by @rands
- The Unthinkable: Who Survives When Disaster Strikes – and Why by Ripley

Ben Miller

NERC ES-ISAC

ben.miller@nerc.net

PGP: C7A6 A703 78EE 7134 7F82

3ED0 8A52 27B3 D99F 28DE

~

~

~

:wq