Finding Success with a SIM: Uncovering What You Need to Analyze

James Voorhees

July 2008

Finding the Needle

- Too many events–80 million per day
- How do you find what you need?
- How do you get the most out of your SIM?
- You need use cases

What's Important?

- The obvious: infections, intrusions
  - Find the events that work on your network
- Above all: Policy matters
  - It tells you what the organization cares about
  - It gives you a basis for action
    - If there is no policy, there can be no action
- At the IRS, it's PII
    - Who do you want to see your tax information?
    - Policy: PII cannot go outside unencrypted

How Do We Find It?

- A SIM depends on data it collects
  - From IDS, firewalls, routers, other devices
  - Know your data:
    - Where it comes from. What it means. What is not there.
- In this case, a Sourcefire rule written in-house:

alert tcp $HOME_NET any -> $EXTERNAL_NET any (content:"SSN"; nocase:; pcre:"/\b[0-7]\d{2}([-.\\ ])\d{2}\1\d{4}\b/"; msg:"ALERT DATA LEAK -- Social Security Number SSN Detected in Clear"; classtype:policy-violation; sid:2404023; gid:1; rev:1;)

  - Perl regex finds the SSN in tcp packets

The Filter to Find It

- A filter set up for that rule:
  - Device: Sourcefire
  - Event Name:
    - ALERT DATA LEAK -- Social Security Number SSN Detected in Clear
  - Filtered out some source and destination IPs allowed by Sourcefire

First Case

Found in the packet body in ArcSight:

From: gqsmith@gmail.com [mailto:gqsmith@gmail.com]

Sent: Monday, February 29, 2008 6:38 AM

To: Smith John Q

Subject: Re:

Can you look up xxx-xx-xxxx for Jennifer Jones.
She came to days from nights she is my friend
and her check is not in her account.

Starting Point

- This event gave source and destination addresses, a username, and a time.
- Could correlate information within ArcSight and with other sources
  - Needed to find evidence to confirm that it happened
- Case was sent to TIGTA for further investigation and possibly prosecution

Second Case

From: Brown Charlie H[mailto:Charlie.Brown@irs.gov]
Sent: Monday, January 10, 2008 7:15 AM
To: Johnson Josephine (StateDOT)

Subject: Vehicle Request

Good Morning Josephine,

When you get a chance, could you please fax to me information on any vehicles registered to the following individual:

xxxxx xxxxx
DOB: xx/xx/xxxx
SSN: xxx-xx-xxxx
License # xxxxxx

Thanks for all your help and always being so pleasant.

Charlie Brown
500-123-4567 - Office
500-123-5678 - Fax

Second Case, Resolved

- Event provided IP address, user names, the message, and a time
- Correlation with other data needed to confirm what happened
  - Logs not in ArcSight
  - IRS identification data
- Employee was reprimanded

Printers

- Found IPs connecting to an external IP address using a strange port
- Found that the printers were connecting to the manufacturer over the web
  - Accessible over HTTP with no password, administrator access
- Reached the administrator
  - He locked the printers down

Misconfiguration

- A workstation generated 140,000 XDMCP events in about 32 hours to 20 systems
  - The user did not know
    - He asked to have the application removed
- Procedure for misconfiguration incidents created.
- A chance to connect with the network team
  - They are vital allies of the security team

Find What is Not Allowed

- Find sources of malicious sites and addresses
  - Monitor ISC and other blogs and lists
- For government: US-CERT Cat 1 and Cat 3 Lists:
  - Lists of IPs that are associated with incidents of unauthorized access and malicious code
- Bogons: packets from unallocated IANA address space
  - List maintained at http://www.team-cymru.org/Services/Bogons/

Black Swans

- When sifting events, expect the unexpected
- Example: hostnames that made no sense on the network
  - Contacted the ISSO
    - Found they they were contractors' laptops
  - Later, found an entire unauthorized network

Building the Use of Arcsight

- Led to creation of an analyst's Active Channel
  - Central view of events deemed to be of interest
    - Use it to collect the events that are useful
  - Can establish channels for different types of analysis
- Sending notifications
  - Email and other ways
  - This makes it easy for those who cannot sit at a monitor all the time

Summary

- A SIM is only as good as its data
- Your work is only as effective as your policies
- Mold your search to your network
- Use cases can be simple
- A SIM alone is insufficient