What is a Security Operations Center (SOC)
Why do you need a SOC?

Central location to collect information on threats
- External Threats
- Internal Threats
- User activity
- Loss of systems and personal or sensitive data
- Provide evidence in investigations

Keep your organization running
- Health of your network and systems
Isn’t a Firewall, IDS or AV enough?

- Firewall is active and known by attackers
  - Protects your systems, not your users
- Anti-Virus
  - Lag-time to catch new threats
  - Matches files, but not traffic patterns.
- IDS alerts on events, but doesn’t provide context
  - System logs
  - Proxy logs
  - DNS logs
  - Information from other people
Structure of a SOC

Private Network vs. People

Tech
- IDS
- Management Systems
- Analyst Systems
- Lab

Techie
- Analysts
- Other Experts
- Users
- Management

Techie using real-time tech 24/7
Private network

- Secure communication between
  - IDS
  - Management System
  - Analyst Systems
- Management and update of IDS and rules
SINGLE IDS WITH A HUB

eth1 (monitor iface)
eth0 (mngmt iface)

Hub

To Router and internet

Switch

IDS
Snort
TCPDump

Management System
Analyst Systems

Network
SINGLE IDS ON A MANAGED SWITCH

- Switch
  - Connected to SPAN port
  - Mirrored to SPAN port

- Network

- IDS
  - eth0 (mngmt iface)
  - eth1 (monitor iface)
  - Snort
  - TCPDump

- Management System

- Analyst Systems

- To Router and internet
IDS system

Secured OS

IDS Software
• Snort
• Barnyard2
• Pulled Pork
• stunnel

Packet capture
• TCPDump
• Daemonlogger
Management system

- Secured OS
- LAMP
- Management Software
  - BASE, Snorby, OCCIM, Splunk, Nagios, etc.
Analyst Systems

- Secured OS
- Management System Interface
- Analysis tools
  - Wireshark
  - Tcpdump
  - Netwitness

But I thought you wanted a secure system!
Lab

- Test system
  - Test rules on the IDS
  - Test Configuration changes
  - Can be used as a backup
- A safe environment to:
  - Play with malware
  - Try hacks

These activities can help you to discover the criteria to build custom rules for the IDS.
It’s probably a good idea to use VM’s for your lab.
Analysts (the meat of the operation)

- You need highly skilled people who:
  - Know networking
  - Understand attacks
  - Understand Malware
  - Don’t ever call in sick
  - Are good at deductive reasoning and critical thinking
  - Are comfortable with things like source code, hex, etc...
  - Are open to new ideas
  - Are creative thinkers
  - Don’t blink
  - Have a passion for this
  - Love to keep learning
  - Don’t need sleep
  - Love to keep learning
Other experts

- System/Network Administrators
  - Keep the whole thing working
  - Tune IDS rules
- Forensics Experts
  - For more in-depth analysis
- Incident Response
  - To mitigate incidents after they happen
- External entities
  - Government, law enforcement, etc...
Users (the other white meat)

- Report things
  - Phishing emails
  - Stolen property
  - Loss of data
- Do things
  - Download malware
  - Engage in inappropriate activities
- The most widely deployed IDS you have
  - If “tuned” properly...
Management

- To interface with other entities
- Keep all the pieces from falling apart
- Make it rain (decide who gets the money)
- I guess someone has to make decisions...
The data

- Log files
  - Firewalls
  - Hosts
  - Proxy Servers
  - DNS Servers

- Network Events

- Phone calls/emails/other sources
Handling all that data

All that data!

Filtering
False Positives
Thresholding
Categorization

OMFG!
To do...
Hmmm...
**Categorization**

US-CERT Recommends the following categories for events

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT 0</td>
<td>Exercise/Network Defense Testing</td>
</tr>
<tr>
<td>CAT 1</td>
<td>Successful unauthorized Access</td>
</tr>
<tr>
<td>CAT 2</td>
<td>Denial of service</td>
</tr>
<tr>
<td>CAT 3</td>
<td>Successful installation or post-install beaconing of malicious code</td>
</tr>
<tr>
<td>CAT 4</td>
<td>Improper Usage</td>
</tr>
<tr>
<td>CAT 5</td>
<td>Scans/probes/Attempted Access</td>
</tr>
<tr>
<td>CAT 6</td>
<td>Investigation</td>
</tr>
</tbody>
</table>
Analyzing something like malware

1. Input from IDS
2. Look at network capture
3. Look at Firewall log
4. Look at Proxy log
5. Look at AV Log
6. Look at System log
7. Talk to user
8. Incident Response
Mitigation/Incident Response

- User education
- User access controls
  - Stop giving users administrative access
- Proxy servers and firewalls
  - Deny access to known bad sites
  - Deny certain kinds of downloads
  - Block posting to known bad IP’s