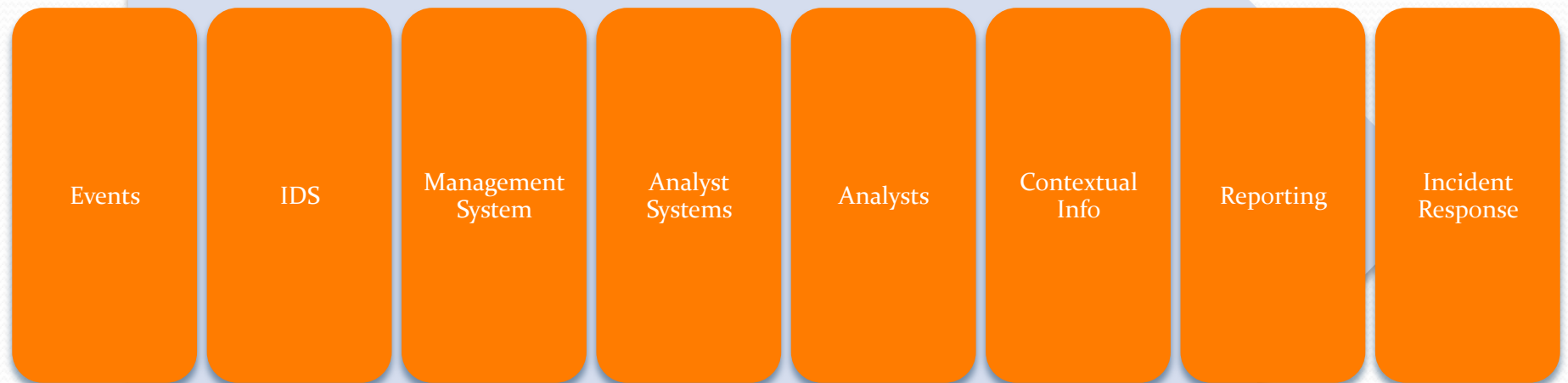


Building a Security Operations Center.

For little or no money...

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

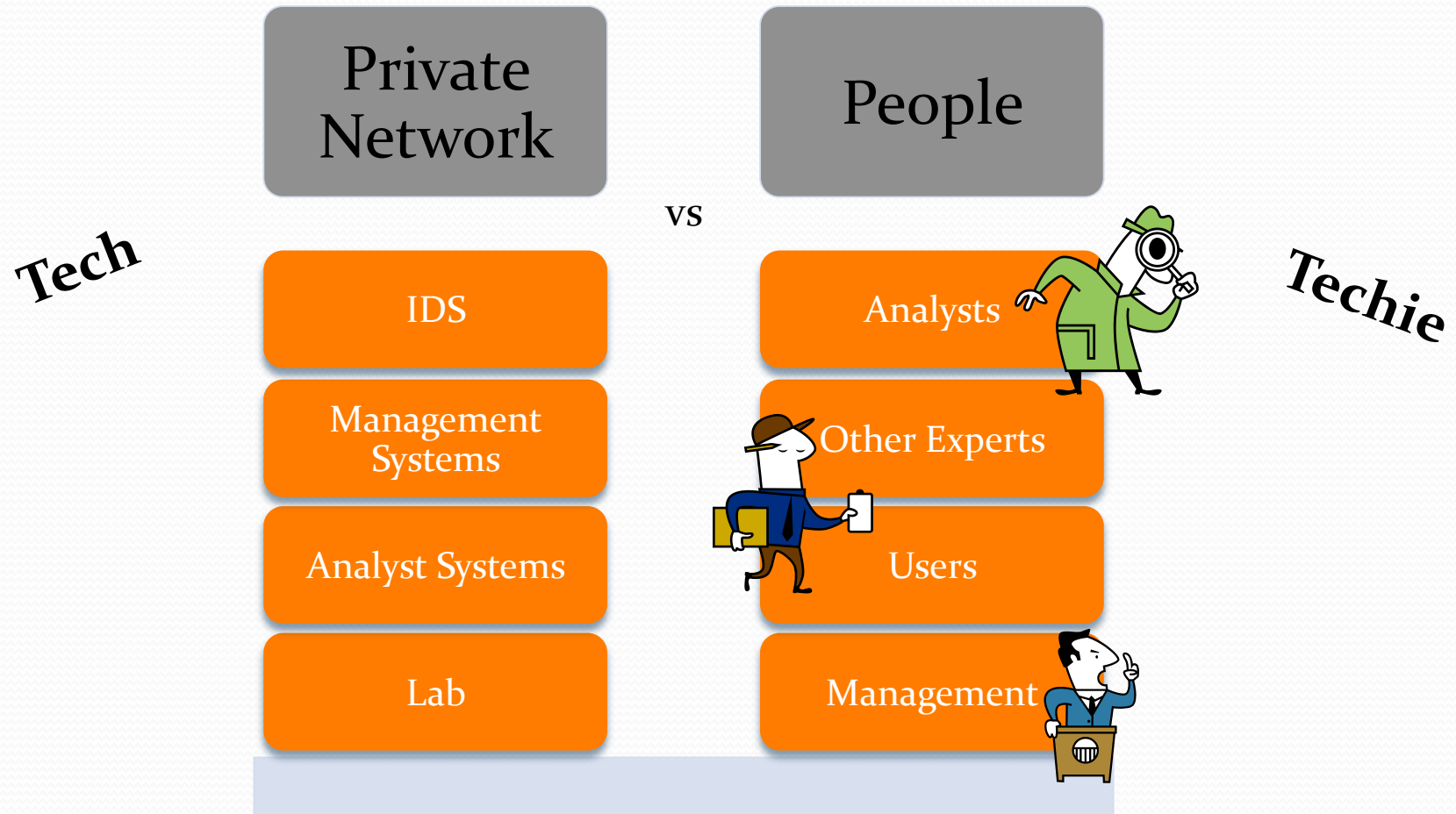
- Health of your network and systems



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



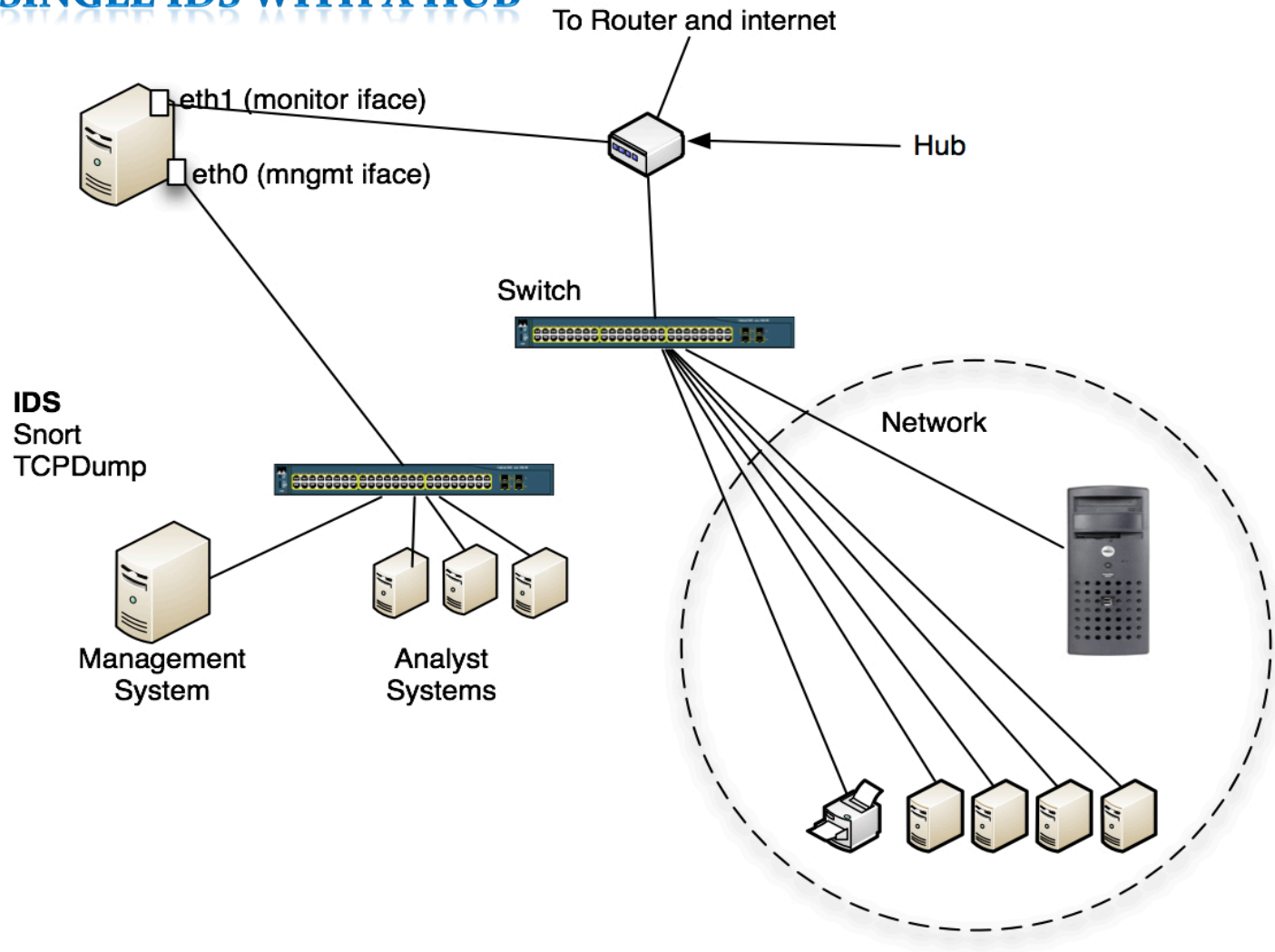
Techie using real-time tech 24/7



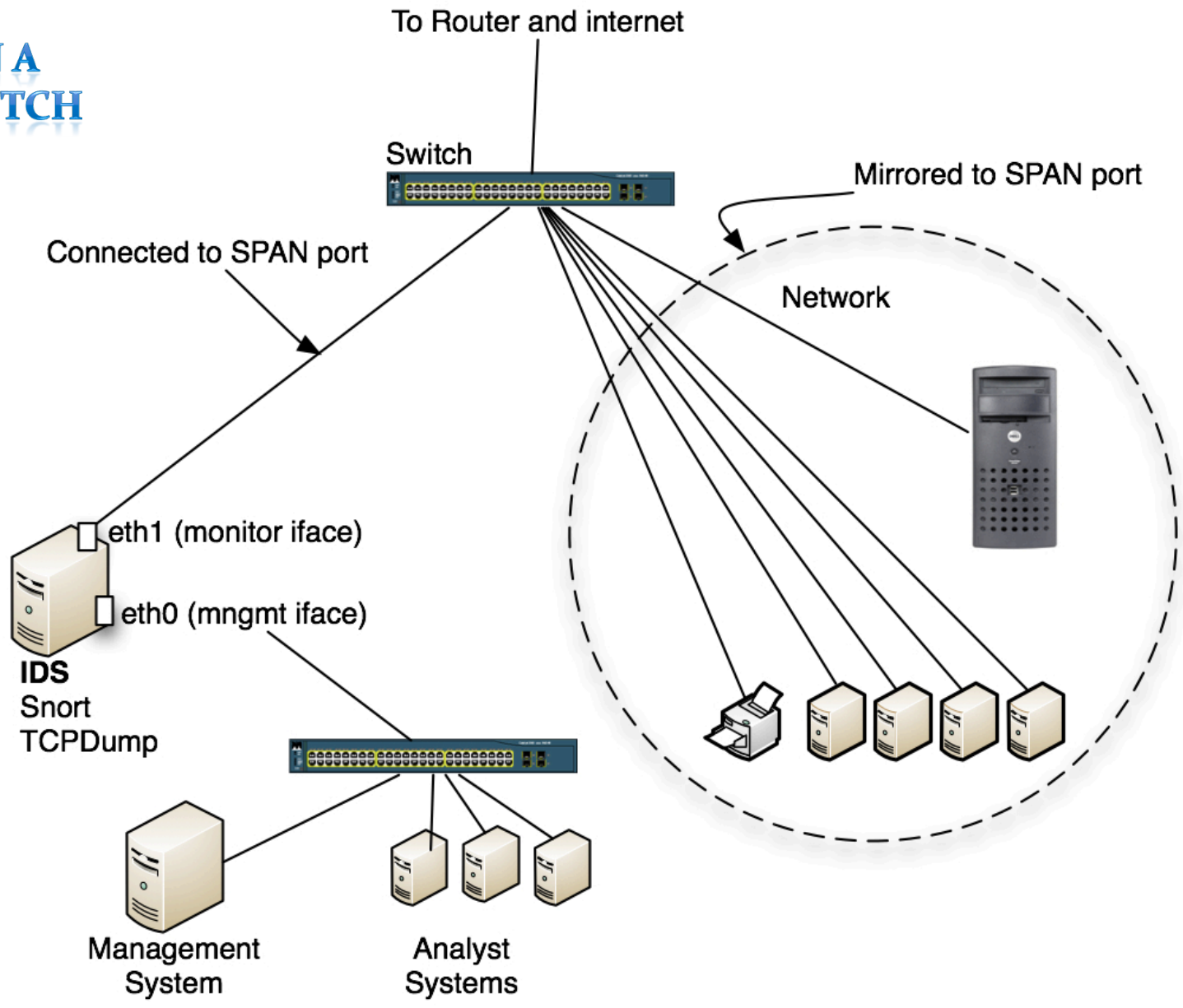
Private network

- Secure communication between
 - IDS
 - Management System
 - Analyst Systems
- Management and update of IDS and rules

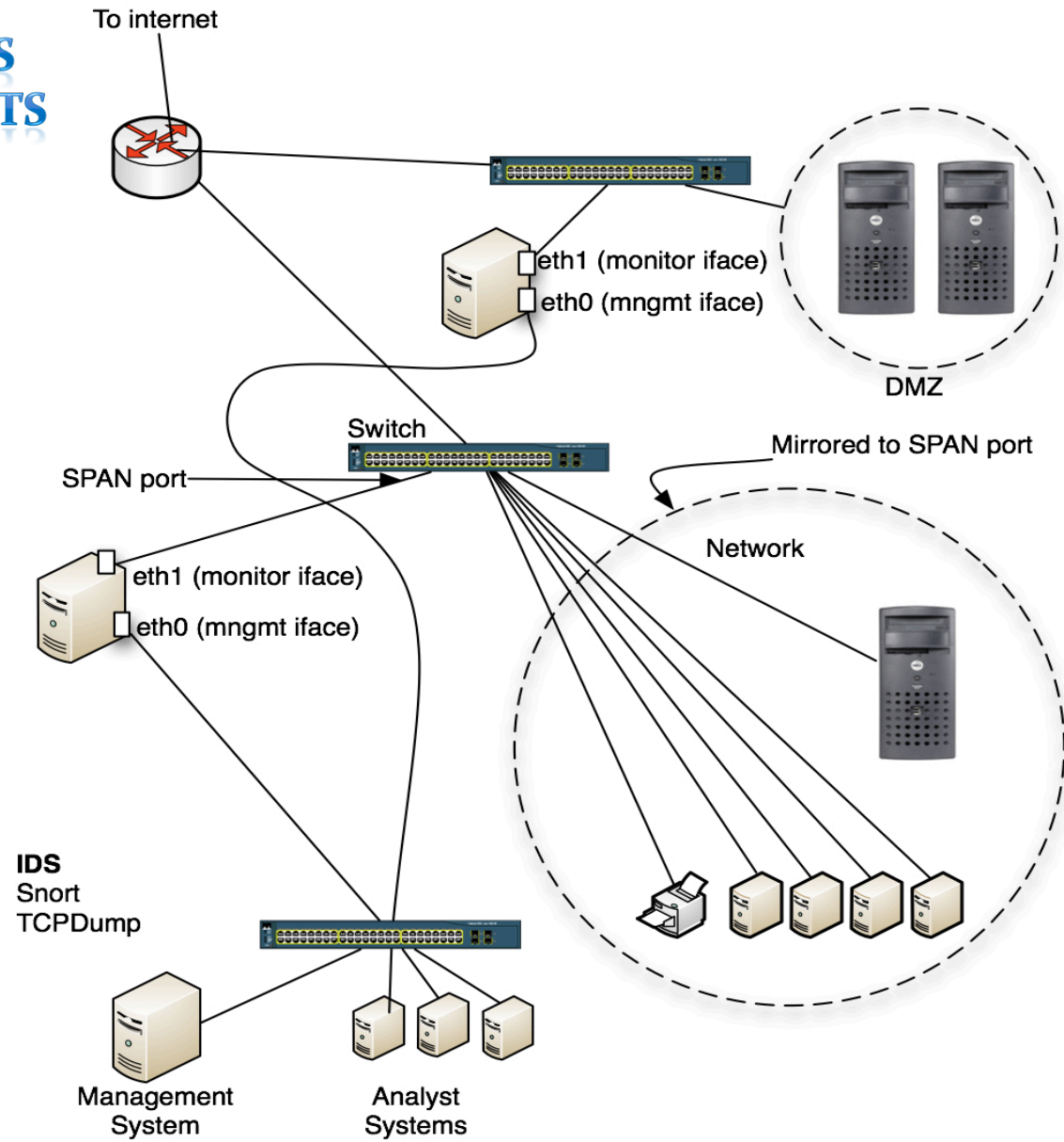
SINGLE IDS WITH A HUB



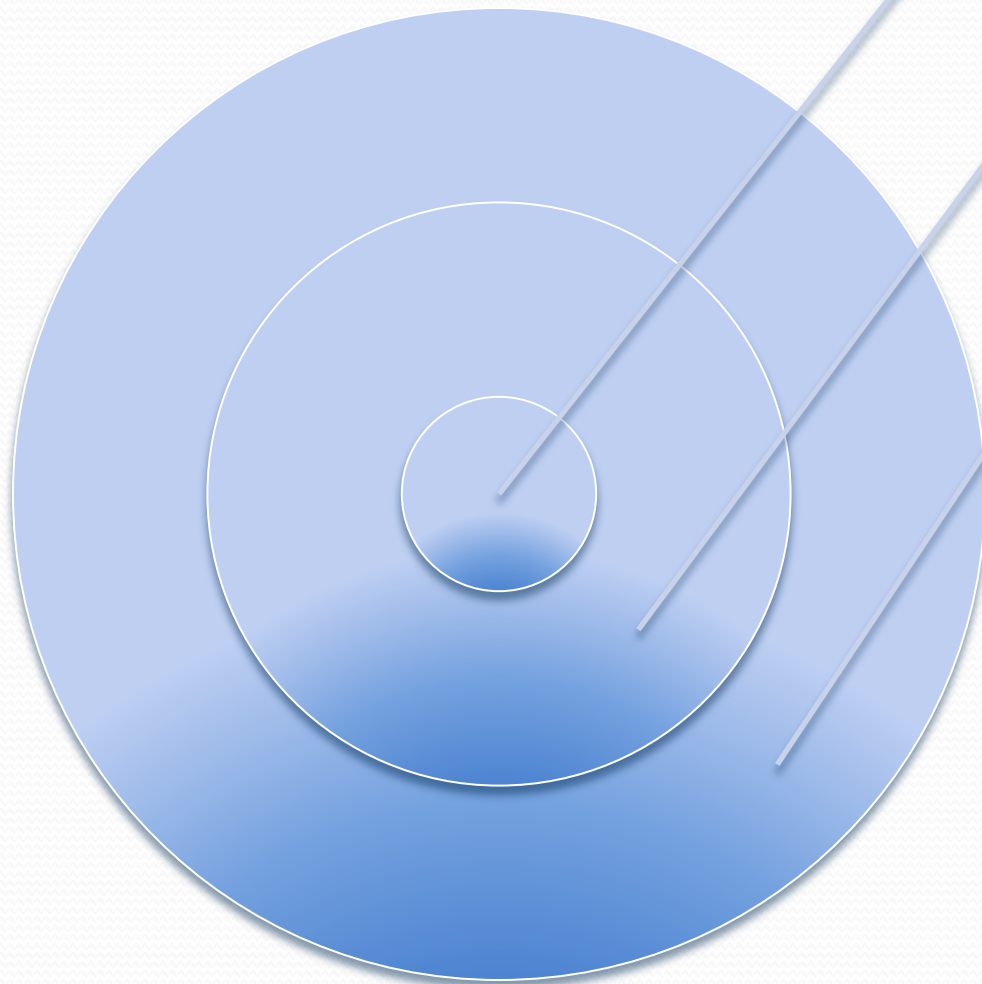
SINGLE IDS ON A MANAGED SWITCH



MULTIPLE IDS SYSTEMS TO MONITOR SEGMENTS



IDS system



Secured OS

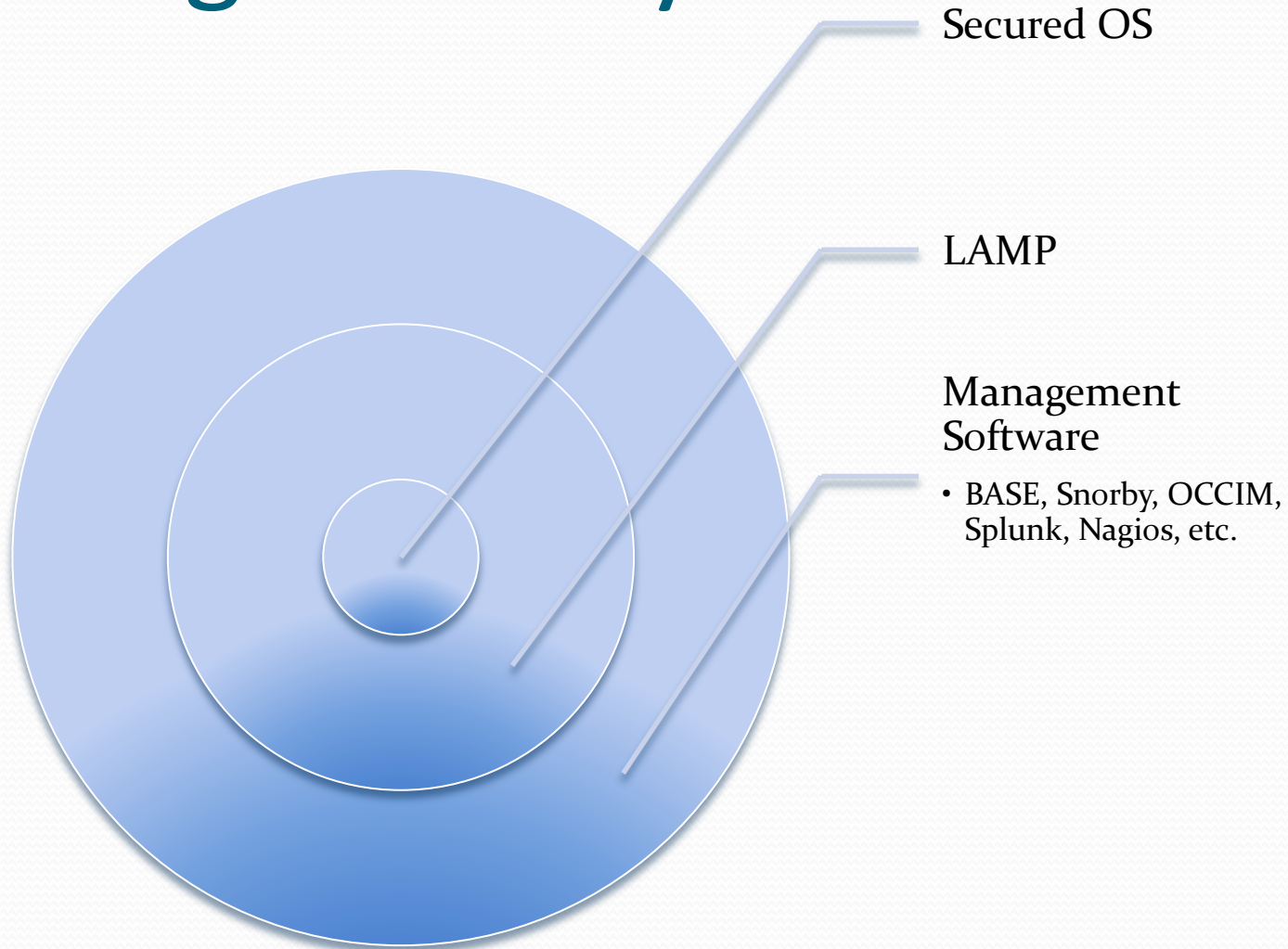
IDS Software

- Snort
- Barnyard2
- Pulled Pork
- stunnel

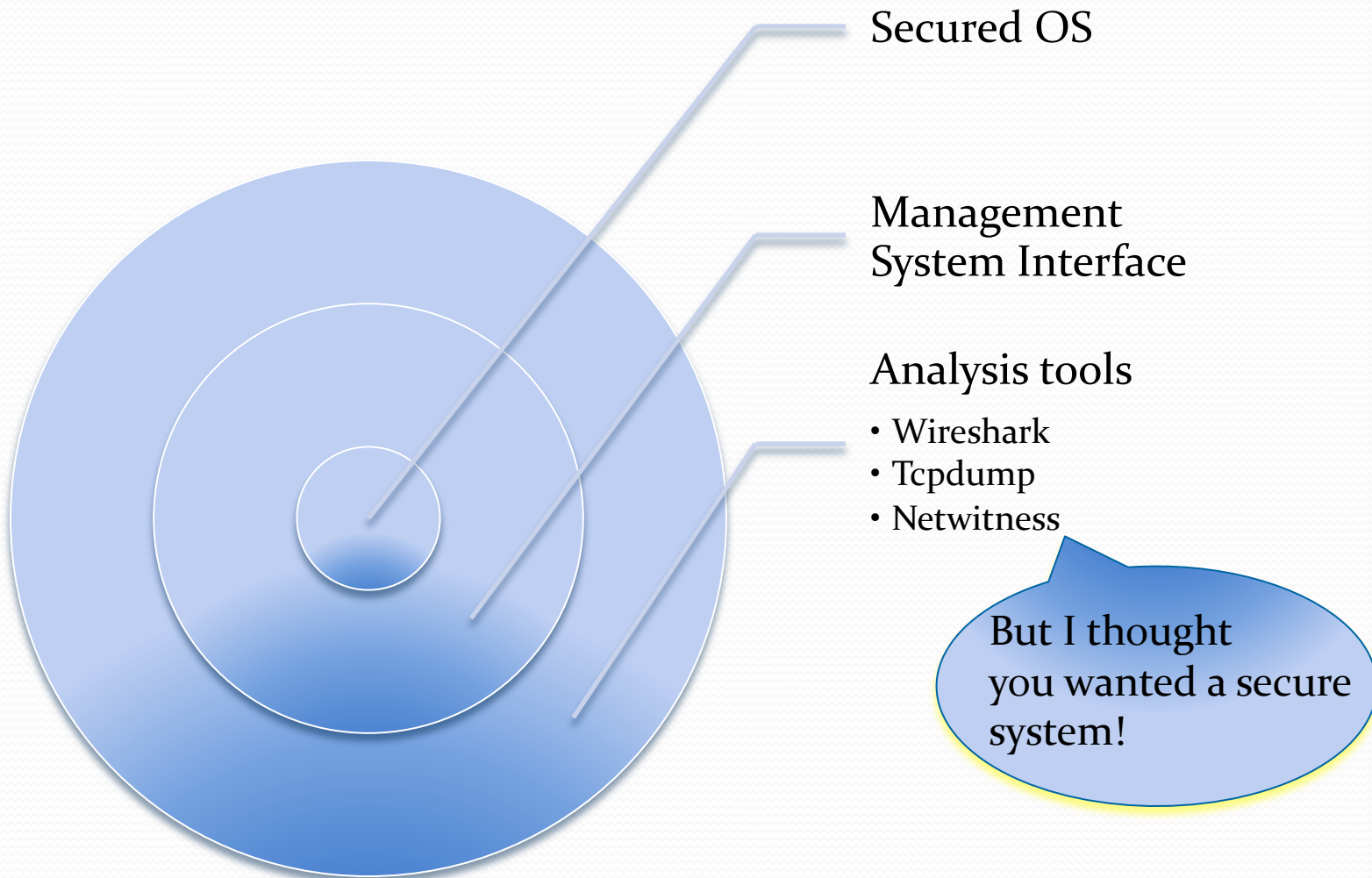
Packet capture

- TCPDump
- Daemonlogger

Management system



Analyst Systems





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

Are comfortable with things like source code, hex, etc...

Understand attacks

Are open to new ideas

Understand Malware

Don't blink

Don't ever call in sick

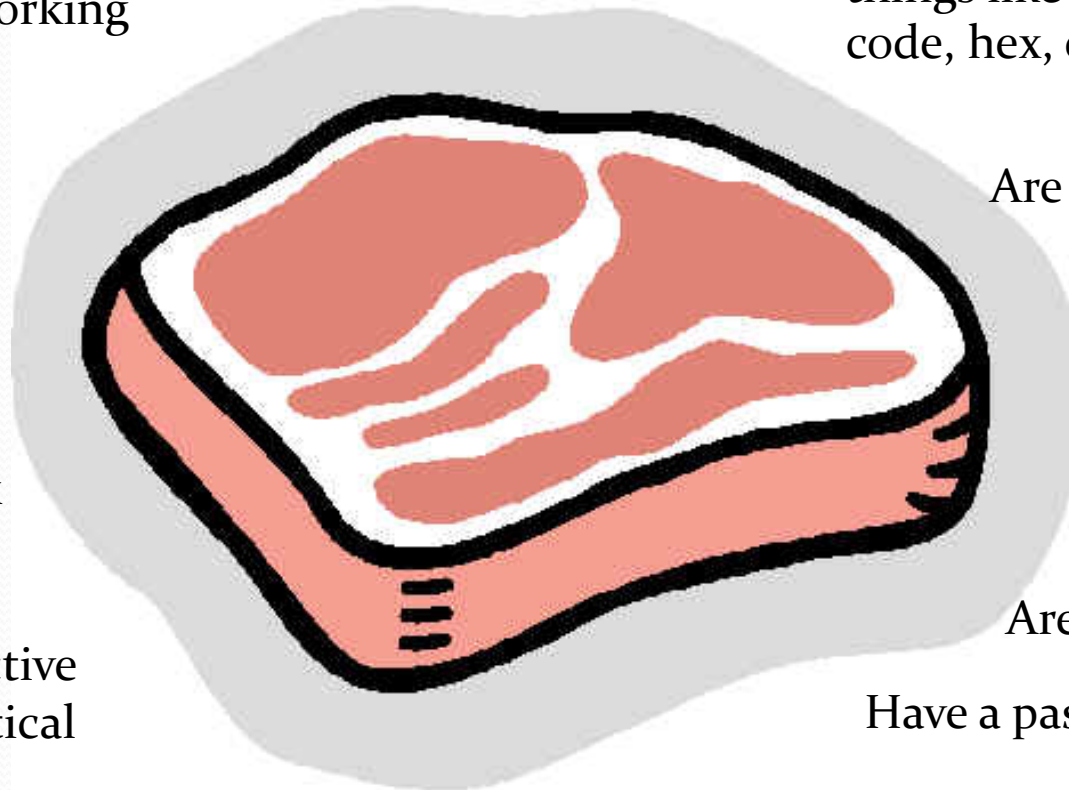
Are creative thinkers

Are good at deductive reasoning and critical thinking

Have a passion for this

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...

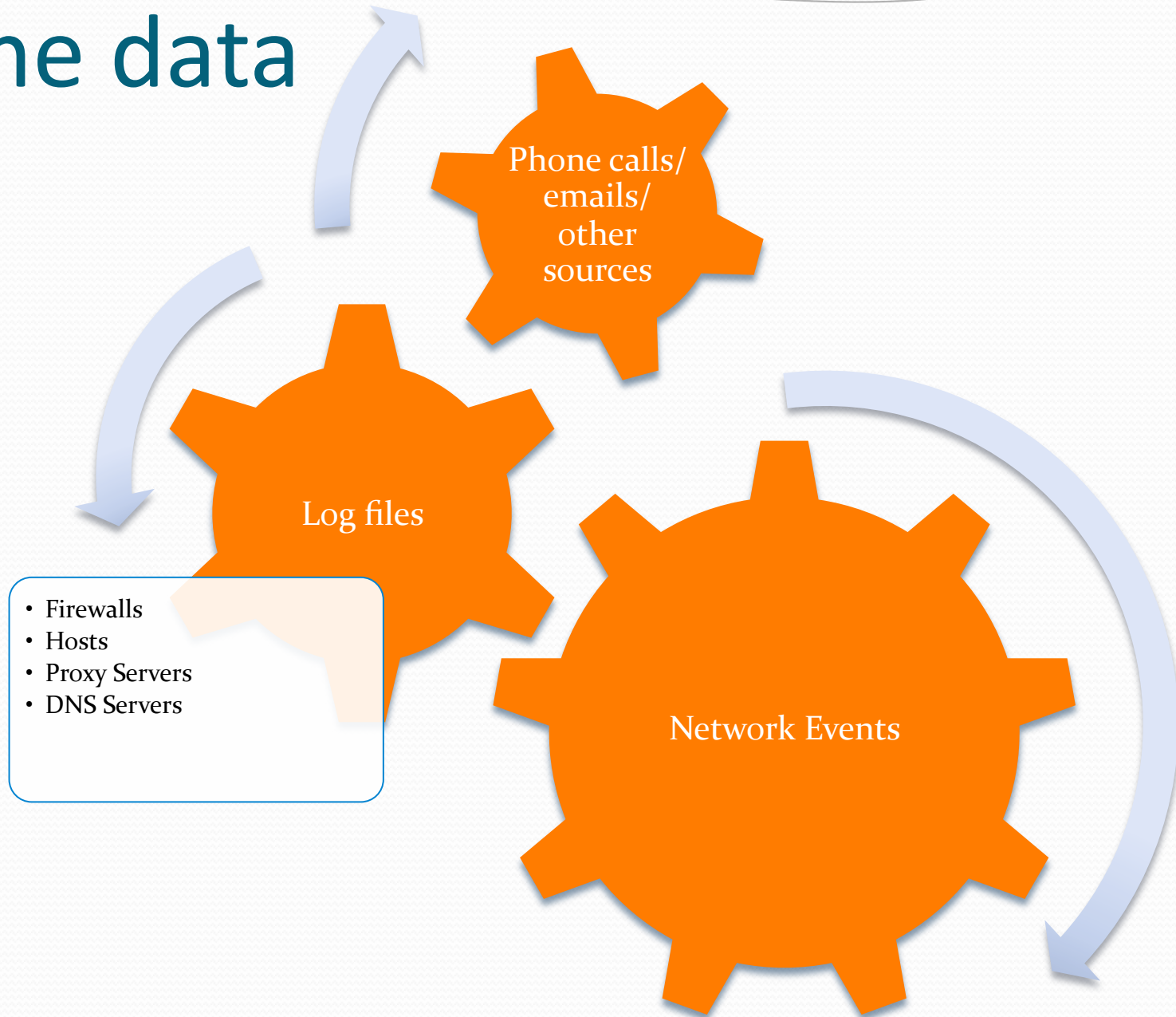




Management

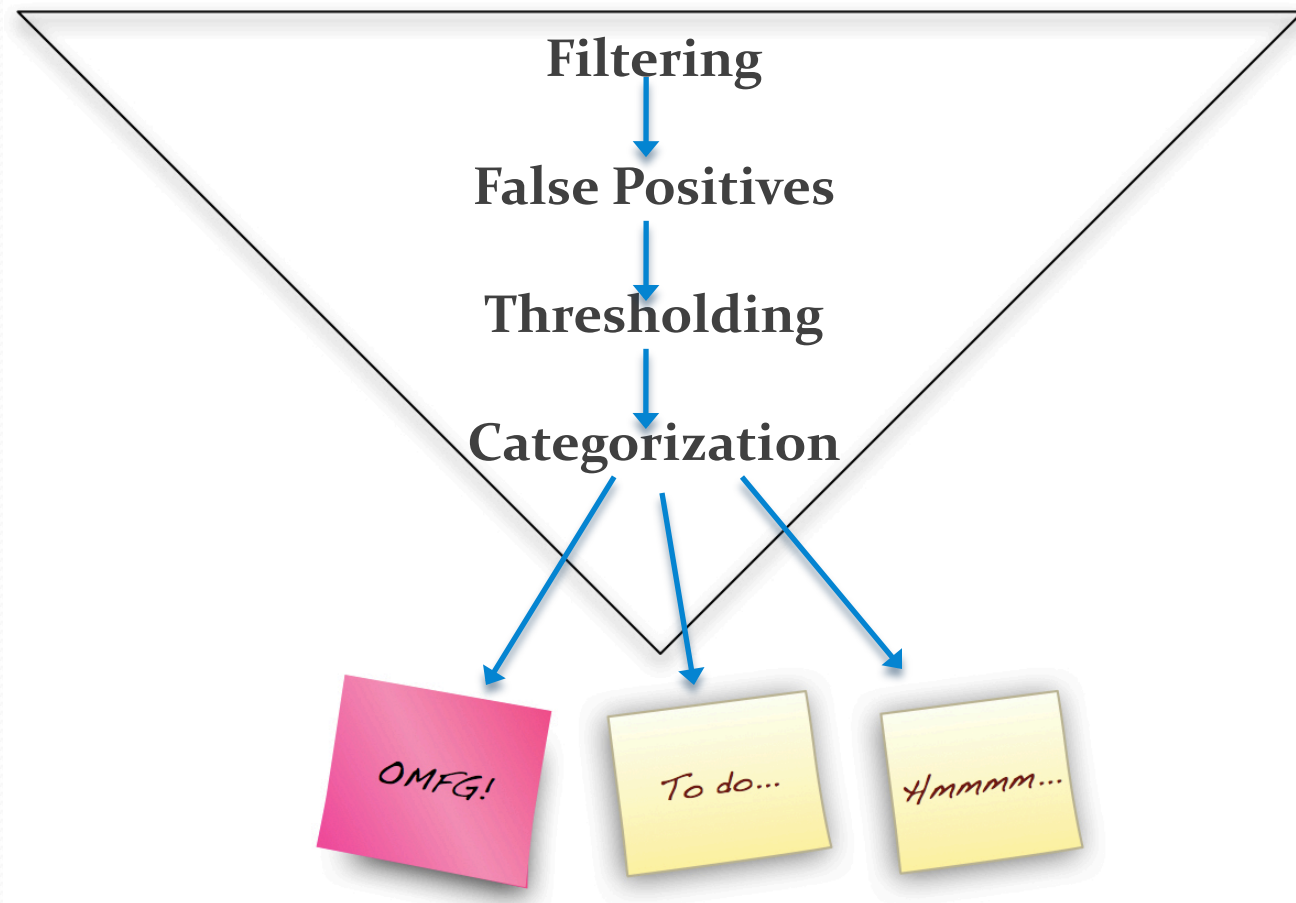
- To interface with other entities
- Keep all the pieces from falling apart
- Make it rain (decide who gets the money)
- I guess someone has to make decisions...

The data



Handling all that data

All that data!

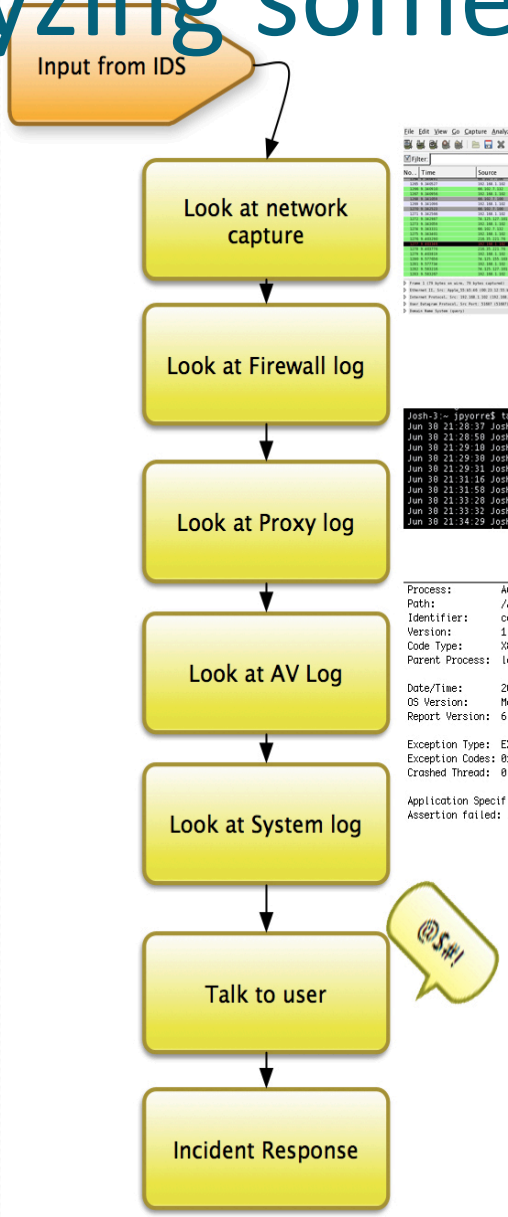


Categorization

US-CERT Recommends the following categories for events

Category	Name
CAT 0	Exercise/Network Defense Testing
CAT 1	Successful unauthorized Access
CAT 2	Denial of service
CAT 3	Successful installation or post-install beaoning of malicious code
CAT 4	Improper Usage
CAT 5	Scans/probes/Attempted Access
CAT 6	Investigation

Analyzing something like malware



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.10	192.168.1.1	TCP	64800 → 80 [RST] Seq=1000000000 Win=0 Len=0
2	0.000000	192.168.1.1	192.168.1.10	TCP	80 → 64800 [RST] Seq=1000000000 Win=0 Len=0
3	0.000000	192.168.1.10	192.168.1.1	TCP	64800 → 80 [RST] Seq=1000000000 Win=0 Len=0
4	0.000000	192.168.1.1	192.168.1.10	TCP	80 → 64800 [RST] Seq=1000000000 Win=0 Len=0

```
Josh-3 ~ jpyorres$ tail /var/log/appfirewall.log
Jun 30 21:20:37 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:20:50 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:29:10 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:29:30 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:29:31 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:31:16 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:31:53 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:33:28 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:33:32 Josh-3 Firewall[65]: Stealth Mode connection
Jun 30 21:34:29 Josh-3 Firewall[65]: Stealth Mode connection
```

```
Process: Audio Kontrol 1 [1134]
Path: /Applications/Audio Kontrol 1/Audio Kontrc
Identifier: com.native-instruments.Audio Kontrol 1
Version: 1.0.2.001 (1.0.2, Copyright © 2006 - 2007
Code Type: X86 (Native)
Parent Process: launchd [131]

Date/Time: 2010-03-07 10:33:03.365 -0800
OS Version: Mac OS X 10.6.2 (10C540)
Report Version: 6

Exception Type: EXC_CRASH (SIGABRT)
Exception Codes: 0x0000000000000000, 0x0000000000000000
Crashed Thread: 0 Dispatch queue: com.apple.main-thread

Application Specific Information:
Assertion failed: (s->stack->next != NULL), function CG6Stc
```





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