



SOC Operations on the Autobahn

Don't let the green grass fool you...

Who am I?

- Adrian Kelley
- 15+ Years of IT Experience
 - Current: Sands Corp. (Vulnerability Management Engineer)
 - United States Computer Emergency Readiness Team (DHS/US-CERT)
 - National Credit Union Association (NCUA)
 - Office of the Director of Naval Intelligence (ONI)
 - Office of the Director of National Intelligence (ODNI)
 - General Dynamics Advanced Information Systems
 - Northrop Grumman Corporation
 - United States Marine Corps (0811-Artillery)

How I feel about certifications?

-CISSP 

-CISA

-GPEN

-C|EH

-C|HFI

-GMON

-GCED

-GSEC

-SFCEP 

-Security +

- ETC...

Mission


- Discovering Speed Isn't a Factor (Indicator Gathering)
- Navigate through Heavy Packet Traffic (Long Tail Analysis)
- Blocking Traffic in the Fast Lane (IDS vs IPS)
- Cloned Camera's on the Autobahn (Honeypot Networks)

Why These Will Help Your SOC?

- 5 Million Events Daily isn't Pleasant
 - We don't have an unlimited supply of analyst
 - Technology is good, human verification is still best
-
- If AI takes the wheel... Your network would look like this!

We All Seen the Movie





Indicator Reconnaissance

Alerts can only make so much noise!

What are Indicators?

- Cybersecurity Information Sharing Act of 2015 defines “cyber threat indicator” as information that is necessary to describe or identify:
 - Malicious reconnaissance
 - Remnant of exploiting a security vulnerability
 - A method that causes a legitimate users account to enable the defeat a security control
 - any combination thereof.

What are Indicators? (cont)

Basically... pieces of information that can be used to search and identify compromised systems

Commonly known as "Indicators of Compromise..."

What forms do Indicators come in?

- File Hashes, IP addresses, URL's, email addresses
- Unusual Outbound Network Traffic
- Anomalies in Privileged User Account Activity
- Unusual DNS Request
- Log-In Red Flags
- Increases in Database Read Volume
- Bundles of Data in the Wrong Place

Collect...

Collect OSINT
reports



- NCCIC CISCP program
 - public-private information sharing
- Open Threat Exchange (OTX)
- MISP - Open Source Threat Intelligence Platform
- Emerging Threat Rules
- IP Block List
- Malware Domain List

Extract...

Extract IOC's
from OSINT
reports



- File Hashes
- URL's
- Domain Names
- IP addresses
- Email addresses
- User Agents
- Registry Keys

Convert...

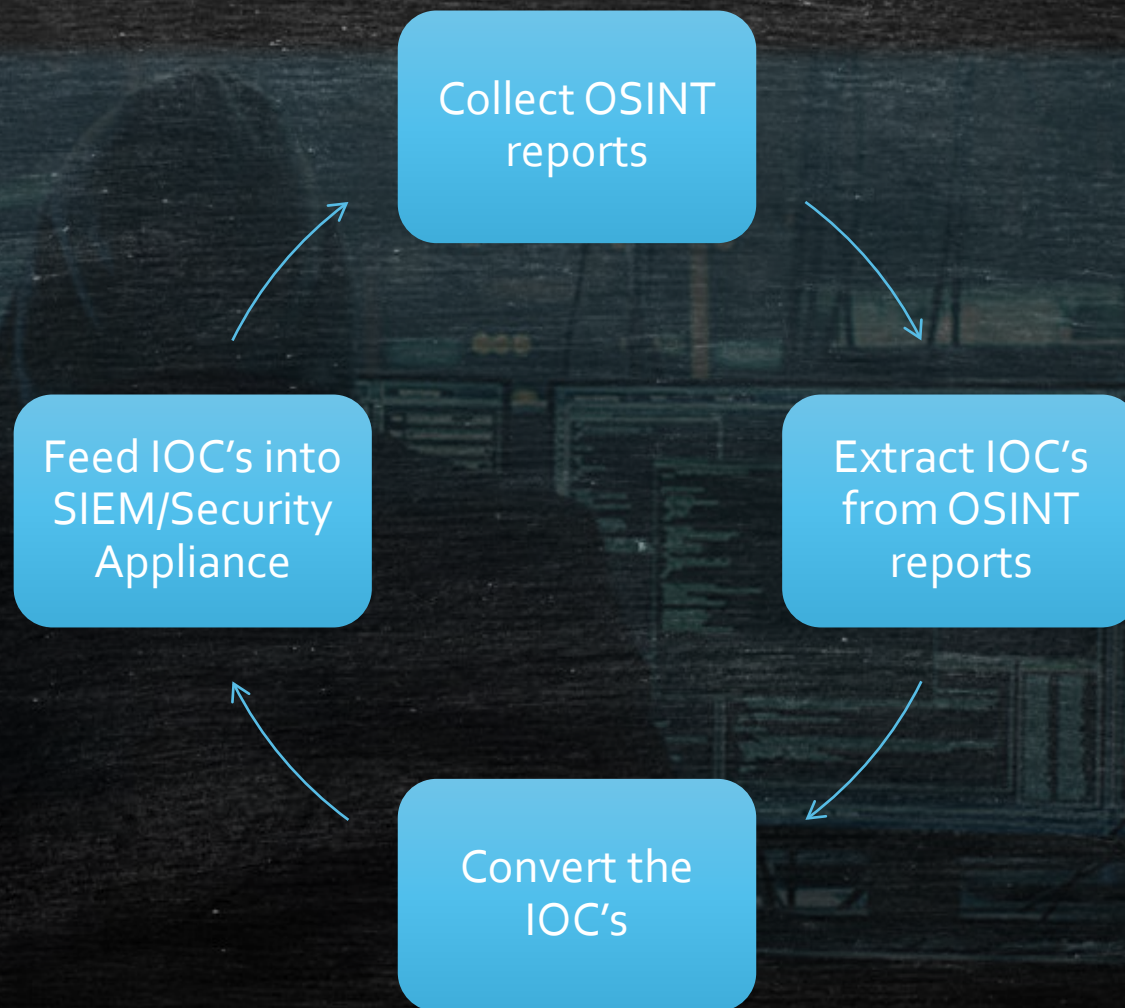
Convert the IOC's



- Snort signatures
- Suricata rules
- Bro IDS rule
- SQUID

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET  
TROJAN Likely Bot  
Nick in IRC (USA +..)"; flow:established,to_server;  
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK  
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;  
reference:url,doc.emergingthreats.net/2008124;  
reference:url,www.emergingthreats.net/cgi-  
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;  
sid:2008124; rev:2;)
```



Rinse & Repeat



Takeaway

- Reducing detection time saves lots of money and front page articles
 - and jobs, and reputations, and careers

***The running theme of this brief



Long Tail Analysis

Logs can only make so much noise!

What is Long Tail Analysis?

“We pay close attention to the stuff that makes the most noise when in actuality, the most interesting stuff is at the lower end of the spectrum.”

When do you use it?

- When looking at:
 - DNS Logs
 - Firewall Logs
 - Proxy Logs
 - DHCP Logs
 - Server Logs
 - IDS Logs

```
Connection received from 10.0.0.100 on port 50937 [08/08 14:38:21.658]
Read request for file <CTLSEP00127FDE8FC5.tlv>. Mode octet [08/08 14:38:21.674]
File <CTLSEP00127FDE8FC5.tlv> : error 2 in system call CreateFile The system cannot find the file specified. [08/08 14:38:21.674]
Connection received from 10.0.0.100 on port 50938 [08/08 14:38:21.689]
Read request for file <SEP00127FDE8FC5.cnf.xml>. Mode octet [08/08 14:38:21.705]
File <SEP00127FDE8FC5.cnf.xml> : error 2 in system call CreateFile The system cannot find the file specified. [08/08 14:38:21.705]
Connection received from 10.0.0.100 on port 50939 [08/08 14:38:21.736]
Read request for file <SIP00127FDE8FC5.cnf>. Mode octet [08/08 14:38:21.752]
File <SIP00127FDE8FC5.cnf> : error 2 in system call CreateFile The system cannot find the file specified. [08/08 14:38:21.752]
Connection received from 10.0.0.100 on port 50940 [08/08 14:38:21.768]
Read request for file <MGC00127FDE8FC5.cnf>. Mode octet [08/08 14:38:21.783]
File <MGC00127FDE8FC5.cnf> : error 2 in system call CreateFile The system cannot find the file specified. [08/08 14:38:21.783]
Connection received from 10.0.0.100 on port 50941 [08/08 14:38:21.799]
Read request for file <XMLDefault.cnf.xml>. Mode octet [08/08 14:38:21.814]
File <XMLDefault.cnf.xml> : error 2 in system call CreateFile The system cannot find the file specified. [08/08 14:38:21.814]
Connection received from 10.0.0.100 on port 50942 [08/08 14:38:21.846]
Read request for file <SIPDefault.cnf>. Mode octet [08/08 14:38:21.861]
File <SIPDefault.cnf> : error 2 in system call CreateFile The system cannot find the file specified. [08/08 14:38:21.861]
Connection received from 10.0.0.100 on port 50943 [08/08 14:38:21.877]
Read request for file <MGCDdefault.cnf>. Mode octet [08/08 14:38:21.877]
File <MGCDdefault.cnf> : error 2 in system call CreateFile The system cannot find the file specified. [08/08 14:38:21.893]
```


Why do you use it?

- When the Autobahn is too much
- When something suspicious has occurred
- Looking for rogue activity
- Enhance hunt capability

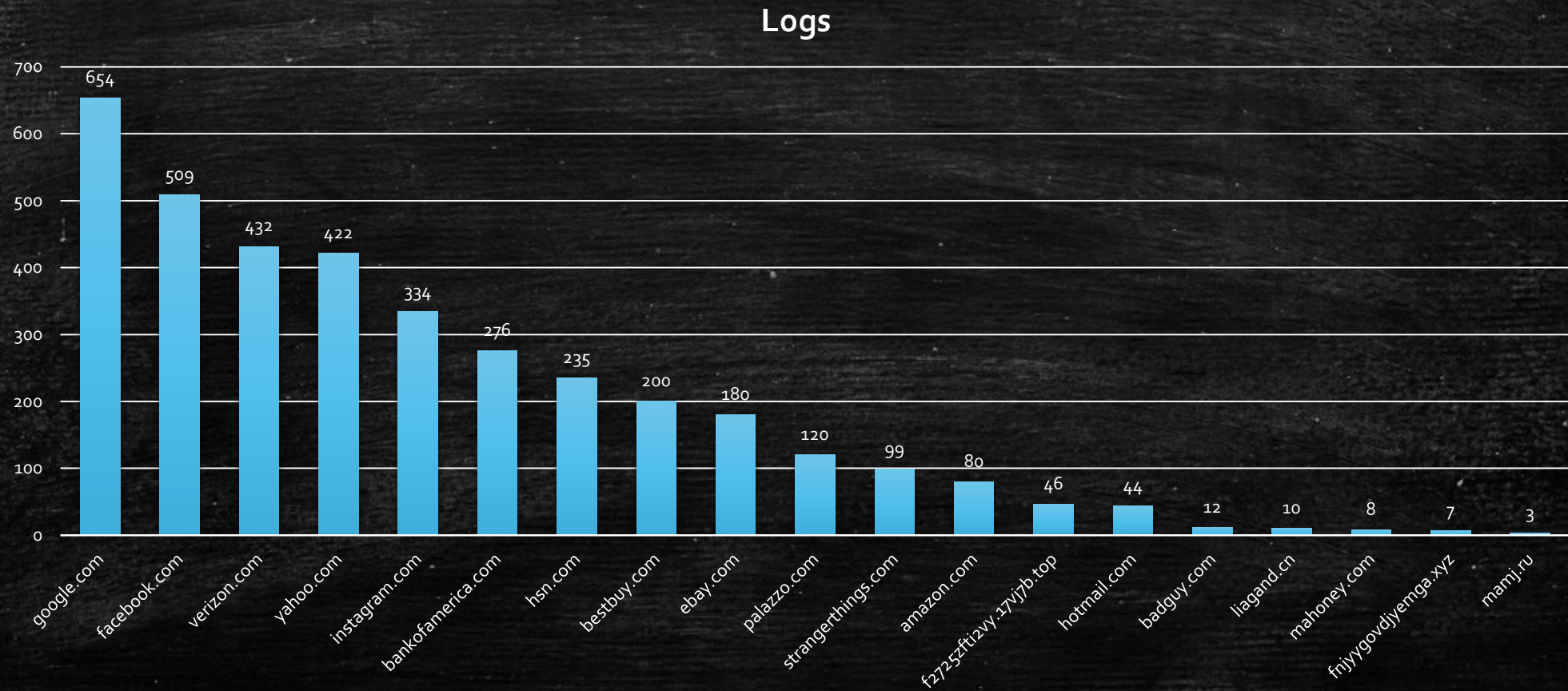
The HUNT

- Lets jump in head first! Sort through the logs...

@	Date/Time	Source	Destination	Destination Port	Protocol	Application Name	Security Action	Security Events	Sent / Received	Action
	22:22:38	2001:db8:48:0:16fe:b5ff:feb2:3fe8	2001:db8:47:0:221:70ff:fee9:bb47	5001	tcp	Iperf	Allowed	1	53.97 MB / 1.18 MB	close
	22:22:28	2001:db8:47:0:221:70ff:fee9:bb47	2001:db8:48:0:16fe:b5ff:feb2:3fe8	5001	tcp	Iperf	Allowed	1	238.41 MB / 2.72 MB	close
	22:22:14	2001:db8:48:0:16fe:b5ff:feb2:3fe8	2001:db8:47:0:221:70ff:fee9:bb47	5001	tcp	Iperf	Allowed	1	54.38 MB / 1.12 MB	close
	22:22:03	2001:db8:47:0:221:70ff:fee9:bb47	2001:db8:48:0:16fe:b5ff:feb2:3fe8	5001	tcp	Iperf	Allowed	1	239.29 MB / 2.72 MB	close
	22:21:13	2001:db8:47:0:221:70ff:fee9:bb47	2001:db8:48:0:16fe:b5ff:feb2:3fe8	5001	tcp	Iperf	Allowed	1	58.79 MB / 566.79 KB	close
	22:21:03	2001:db8:48:0:16fe:b5ff:feb2:3fe8	2001:db8:47:0:221:70ff:fee9:bb47	5001	tcp	Iperf	Allowed	1	203.67 MB / 4.99 MB	close
	22:20:41	2001:db8:47:0:221:70ff:fee9:bb47	2001:db8:48:0:16fe:b5ff:feb2:3fe8	5001	tcp	Iperf	Allowed	1	58.24 MB / 563.77 KB	close
	22:20:30	2001:db8:48:0:16fe:b5ff:feb2:3fe8	2001:db8:47:0:221:70ff:fee9:bb47	5001	tcp	Iperf	Allowed	1	202.97 MB / 4.94 MB	close
	22:19:47	2001:db8:47:0:221:70ff:fee9:bb47	2001:db8:48:0:16fe:b5ff:feb2:3fe8	5001	tcp	Iperf	Allowed	1	211.35 MB / 2.47 MB	close
	22:19:41	2001:db8:48:0:16fe:b5ff:feb2:3fe8	2001:db8:47:0:221:70ff:fee9:bb47		icmp6	IPv6.ICMP	Allowed	1	208 B / 208 B	accept
	22:19:33	2001:db8:48:0:16fe:b5ff:feb2:3fe8	2001:db8:47:0:221:70ff:fee9:bb47	5001	tcp	Iperf	Allowed	1	202.84 MB / 4.96 MB	close
	22:16:01	192.168.48.10	192.168.47.11	5001	tcp	Iperf	Allowed	1	52.41 MB / 811.78 KB	close
	22:15:51	192.168.47.11	192.168.48.10	5001	tcp	Iperf	Allowed	1	237.37 KB / 996 B	close
	22:15:31	192.168.48.10	192.168.47.11	5001	tcp	Iperf	Allowed	1	52.41 MB / 790.56 KB	close
	22:15:21	192.168.47.11	192.168.48.10	5001	tcp	Iperf	Allowed	1	235.75 KB / 1.11 KB	close
	22:14:52	192.168.47.11	192.168.48.10	5001	udp	Iperf			32.90 MB / 19.01 KB	accept
	22:14:52	192.168.47.11	192.168.48.10	5001	udp	Iperf	Allowed	1		ip-conn
	22:14:41	192.168.48.10	192.168.47.11	5001	udp	Iperf			37.09 MB / 10.49 KB	accept
	22:14:41	192.168.48.10	192.168.47.11	5001	udp	Iperf	Allowed	2		ip-conn
	22:14:33	192.168.47.11	192.168.48.10	5001	tcp	Iperf	Allowed	1	57.98 MB / 443.93 KB	close
	22:14:22	192.168.48.10	192.168.47.11	5001	tcp	Iperf	Allowed	1	231.77 KB / 3.18 KB	close
	22:14:09	192.168.47.11	192.168.48.10	5001	udp	Iperf			5.19 MB / 13.94 KB	accept
	22:14:09	192.168.47.11	192.168.48.10	5001	udp	Iperf	Allowed	1		ip-conn

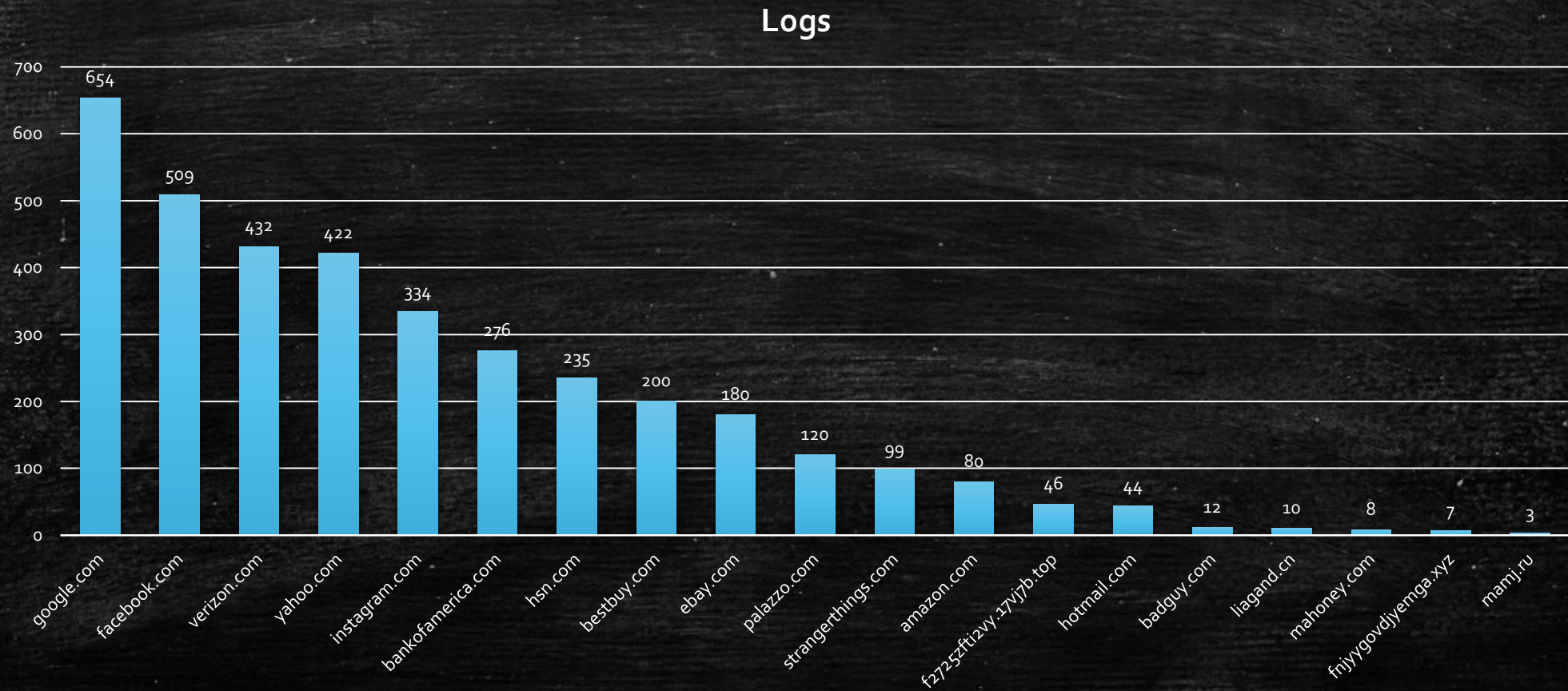
The HUNT is

- Turn them into visual bar graphs



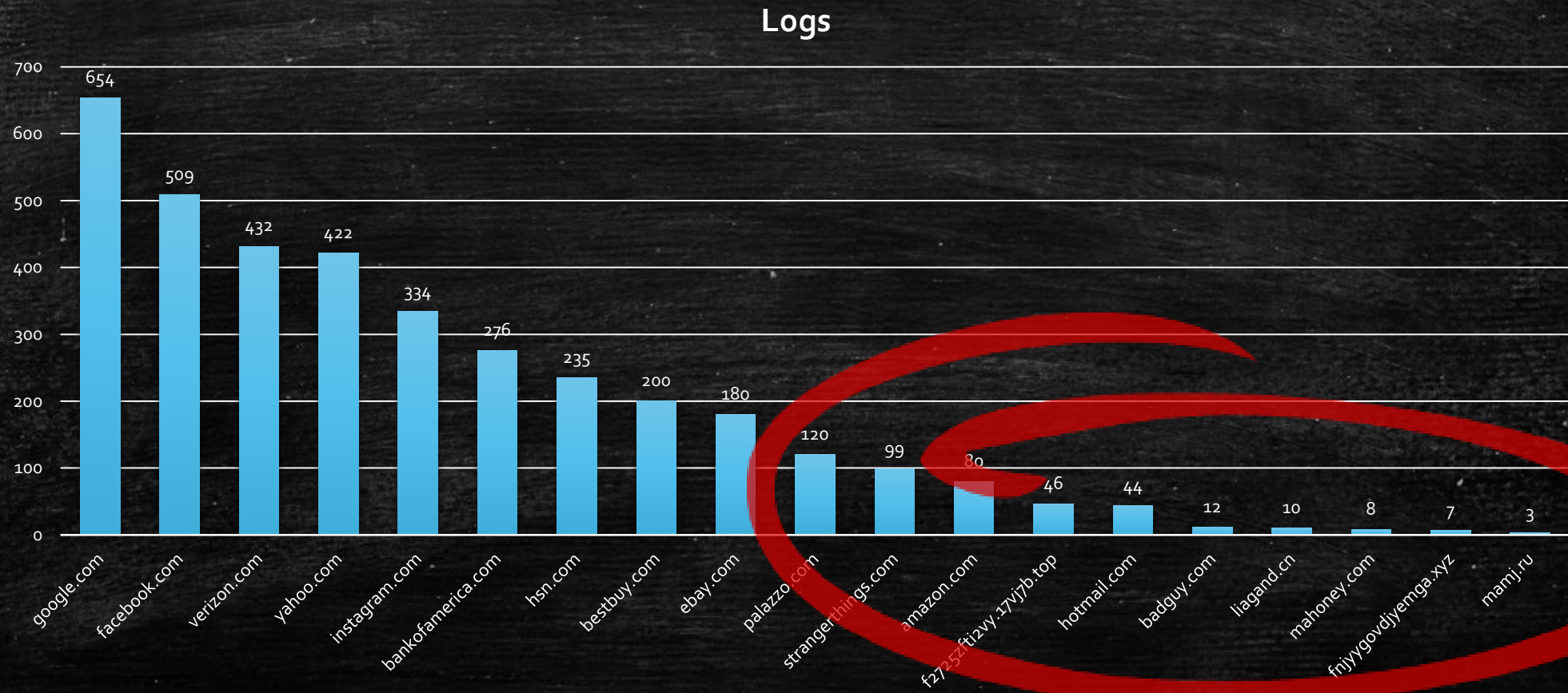
The HUNT is an

- Now what jumps out? Anything abnormal?



The HUNT is an ADVENTURE!

- Why are we getting hits on these domains?



Suspicious Domains

- Lets take a deeper look at liagand.cn

Domains	Count
f2725zfti2vy.17vj7b.top	46
hotmail.com	44
badguy.com	12
liagand.cn	10
mahoney.com	8
fnjyygovdjyemga.xyz	7
mamj.ru	3

Suspicious Domain

- Our search yielded results!

Blacklists				
MDL	No alerts detected			
OpenPhish	No alerts detected			
PhishTank	No alerts detected			
Fortinet's Web Filter	Added / Verified	Severity	Host	Comment
	2017-11-08	2	liagand.cn/	Malware
DNS-BH	Added / Verified	Severity	Host	Comment
	2016-05-27	2	liagand.cn	malicious
	2016-05-27	2	liagand.cn	malicious
	2016-05-27	2	liagand.cn	malicious
mnemonic secure dns	No alerts detected			

DOCK YOUR SHIP!



Long Tail Recap

- The noise doesn't mask the truth
- This methodology for logs of all types
- Can be used to enhance cyber capabilities
- Gives analyst another tool to detect suspicious activity

Honeypot Networks

They waste our time... time to waste theirs!

History of this sweet stuff..

- The idea came from a book called "The Cuckoos Egg" by Clifford Stoll released in 1991.
- First type of honeypot was released in 1997
 - Deceptive Toolkit
- The Philippine Honeypot Project was started to promote computer safety over in the Philippines in 2005.



What is a Honeypot?

A honeypot is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

Generally, a honeypot consists of the following:

- A computer or interesting device on the network
- Data that would appear to be of value
- A network site that appears to be part of a network, but is actually isolated and monitored

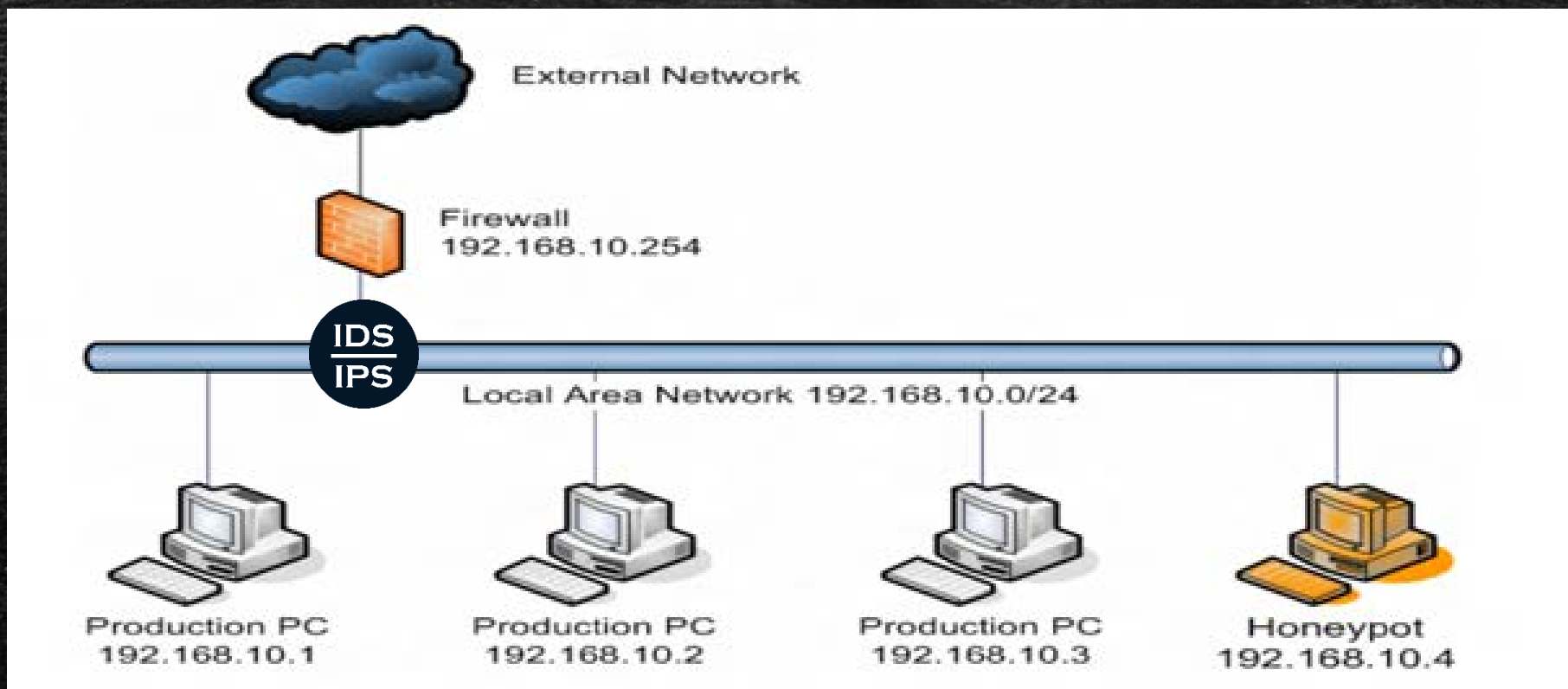
This is similar to the police baiting a criminal and then conducting undercover surveillance.

What can you do with a Honeypot?

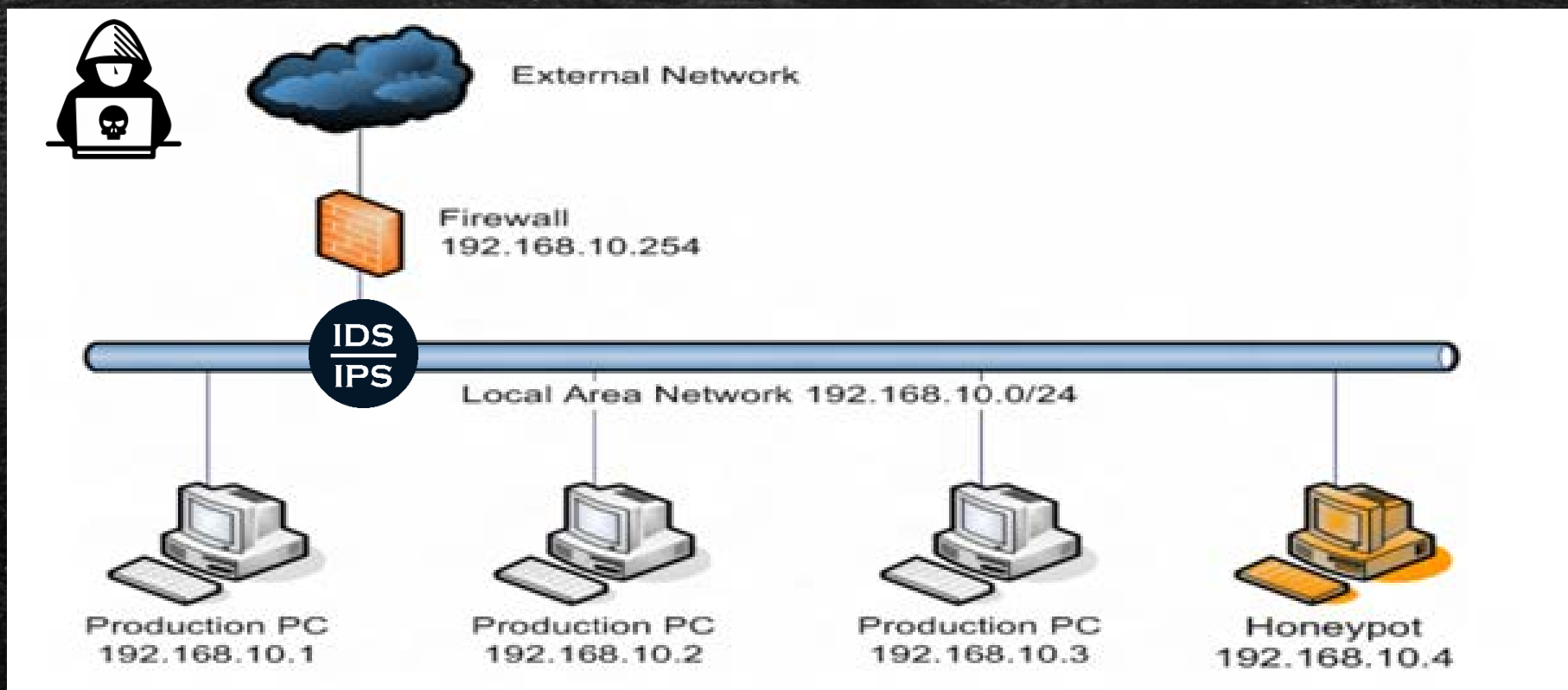
- **Great question!**

- Record actions, capture keystrokes, view their toolset, etc....
- Supplement IDS Detection
- Slow down or STOP the adversary (Defense in Depth)

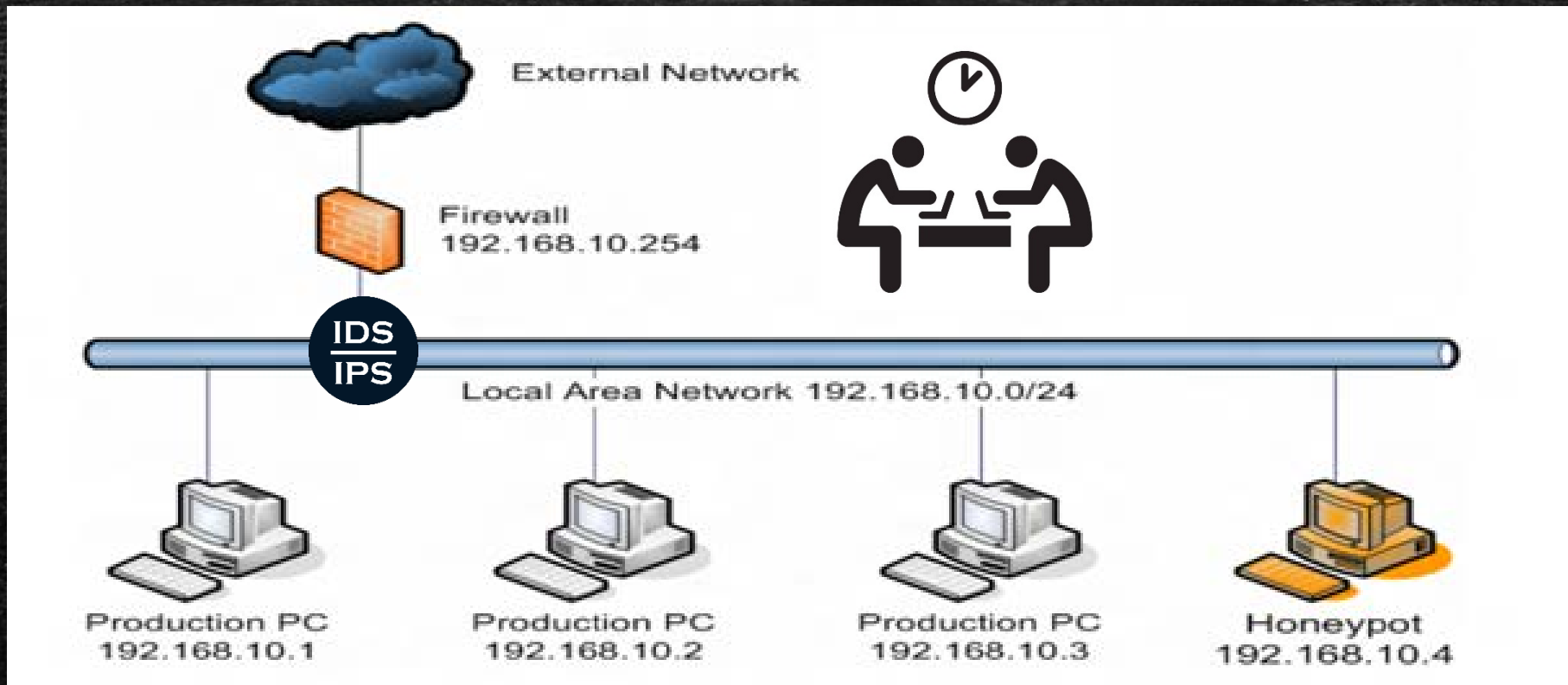
How is a Honeypot used?



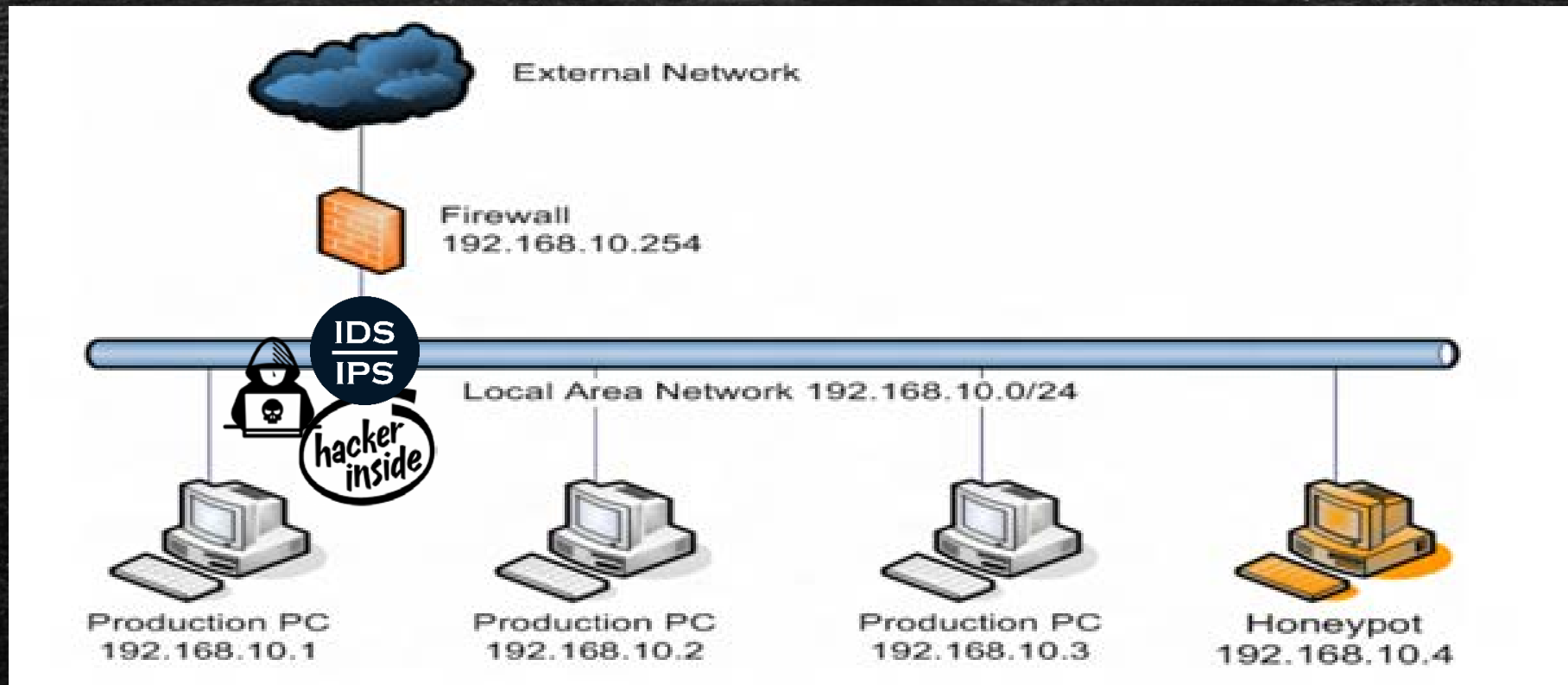
Bad Guys shows up...



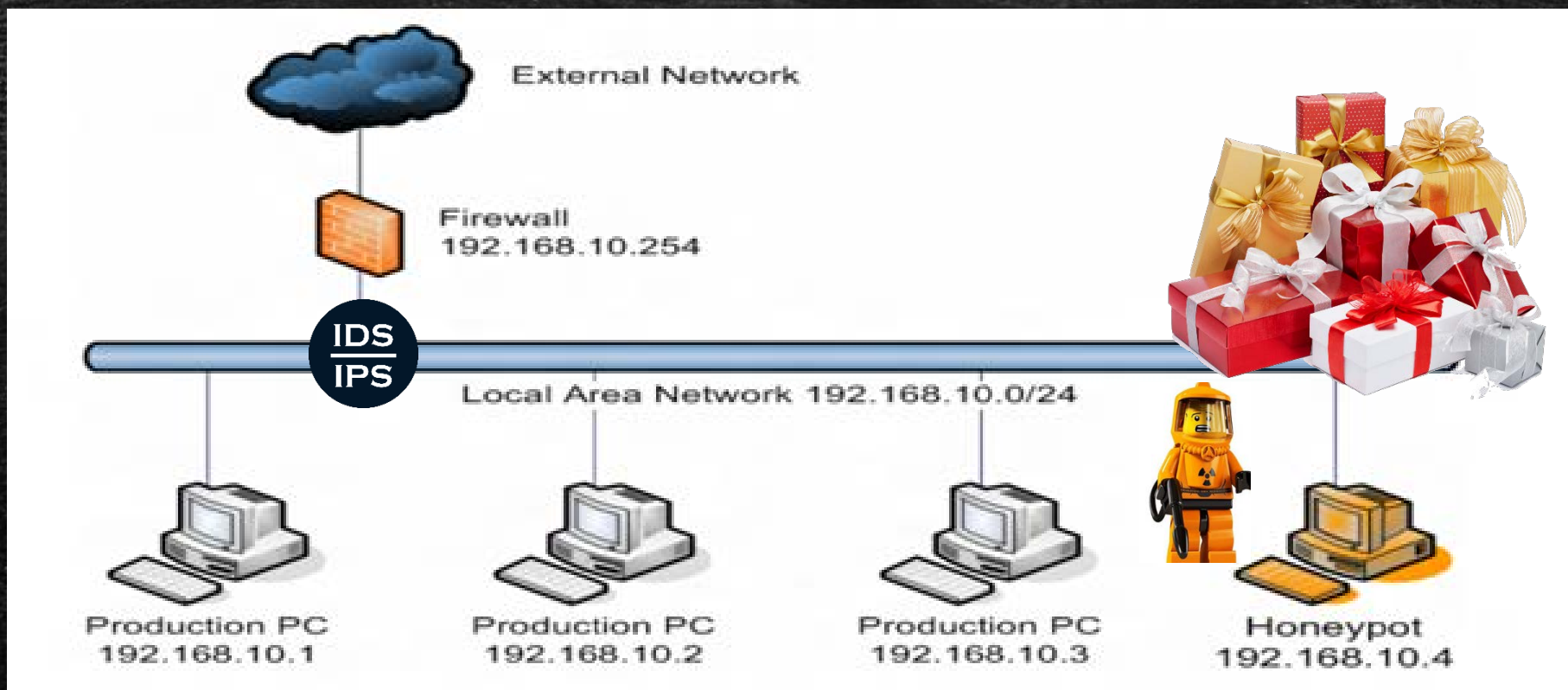
Bad Guys probs network...



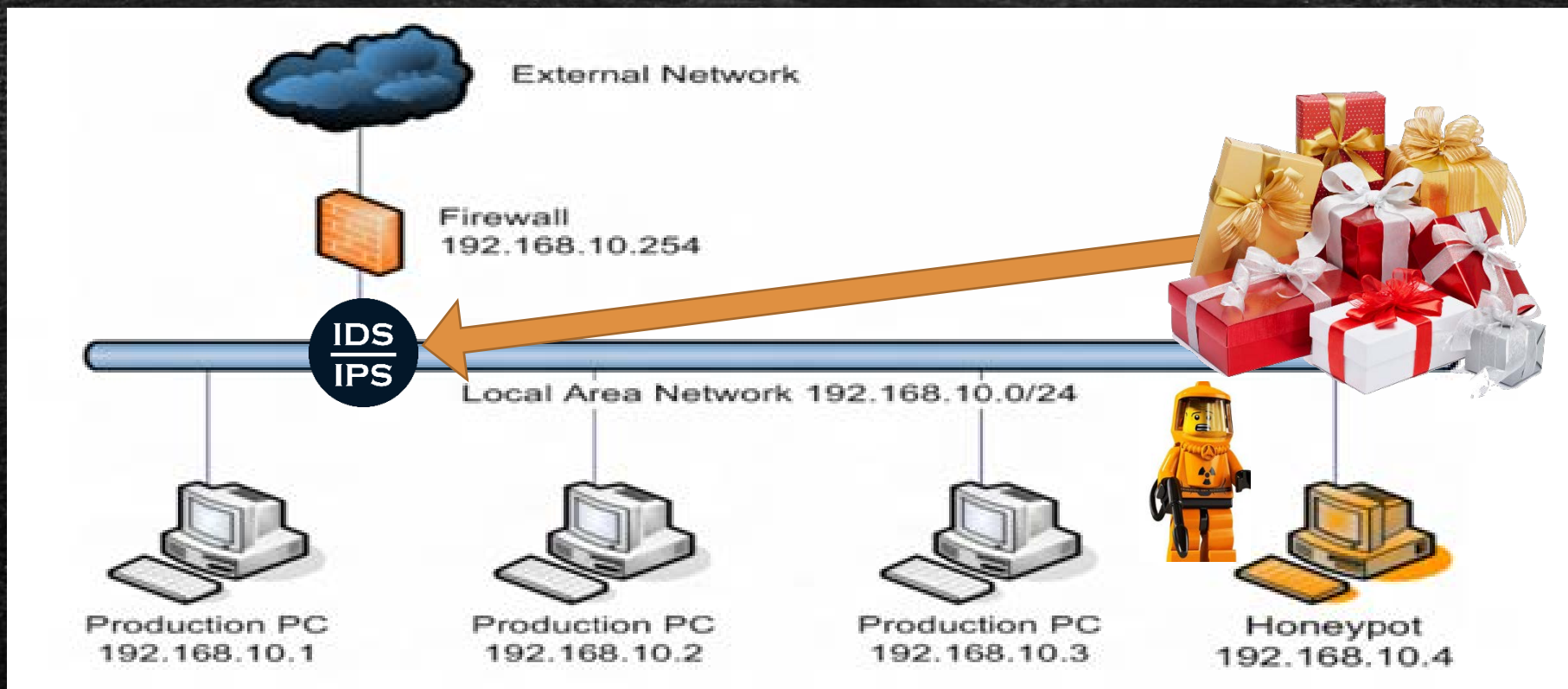
Bad Guys finds & Pops a box



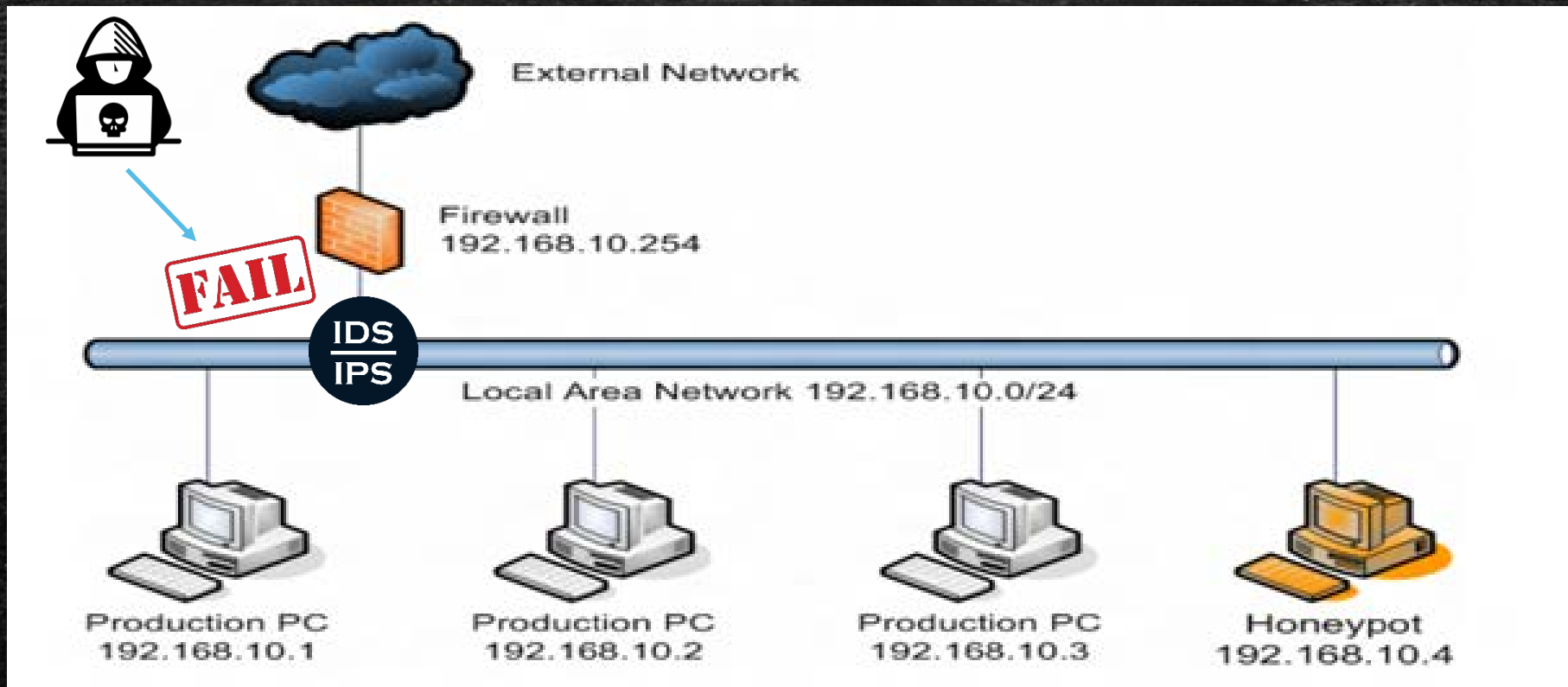
Bad Guy get quarantined



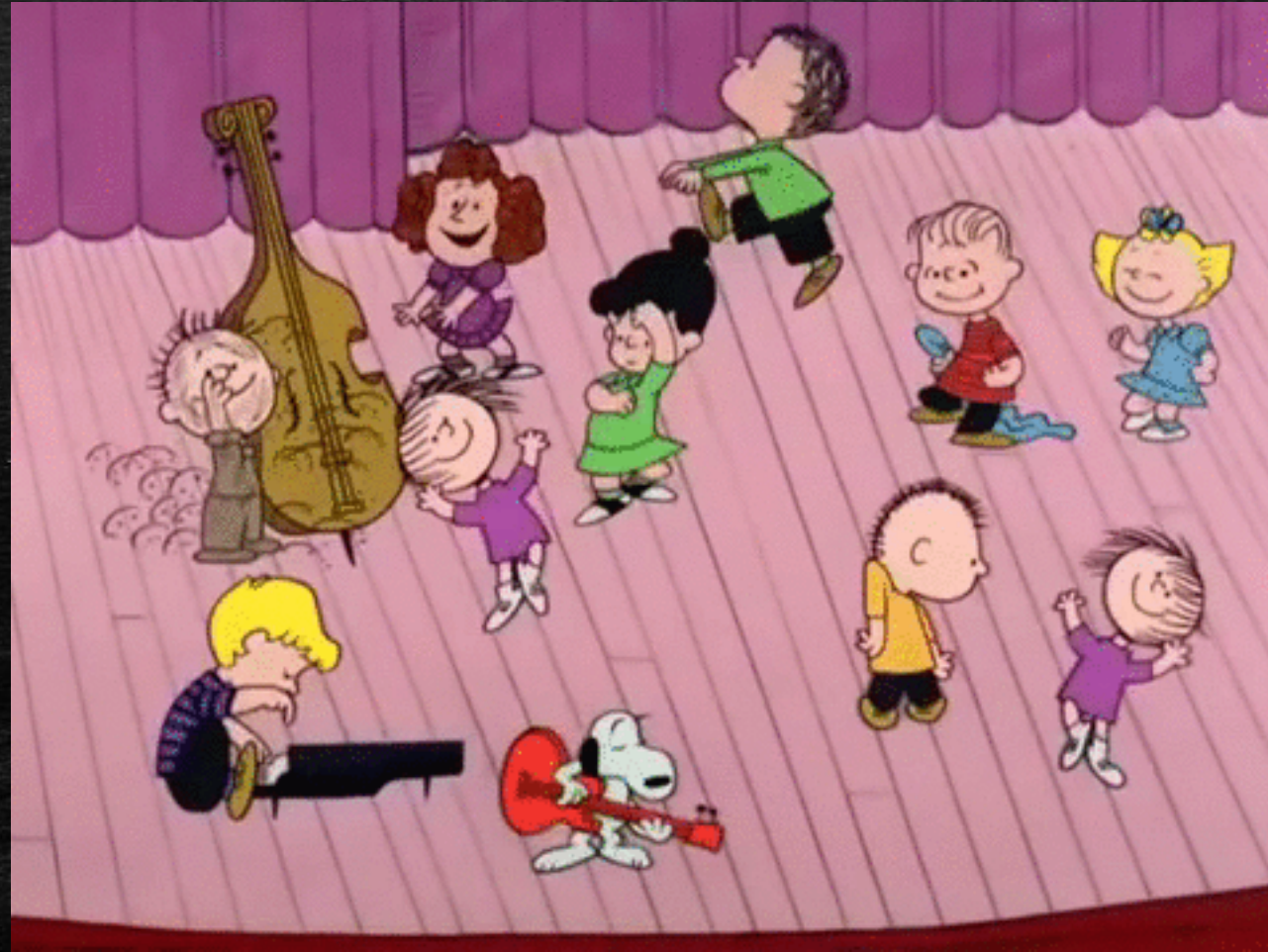
Bad Guy get quarantined



IOC's are blocked...



All is RIGHT IN THE WORLD!!



Why would you deploy a Honeypot?

- DETECTION
- Defense in Depth
 - Slow down or STOP the adversary (technology dependent)
- Low rate of false positive
- Record actions, capture keystrokes, view their toolset, etc....

Intrusion Detection & Prevention

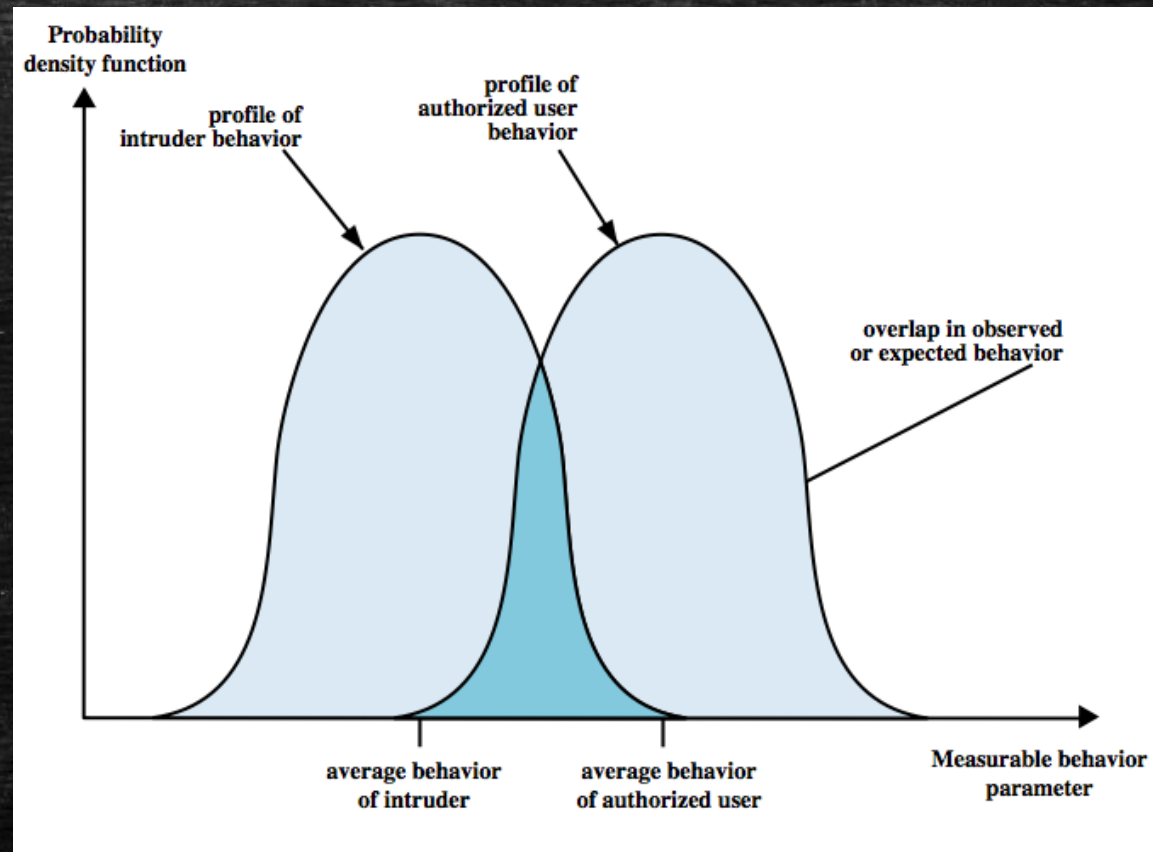
IPS vs IDS

Who is Who?



IDS Principles

- Assume that the users behavior is different than that of a normal user.
- Expect Overlap
- Problems include:
 - False Positives
 - False Negatives



What do you want from an IDS?

- Impose a minimal overhead on your network
- Run constantly
- Be scalable
- Be easily configurable
- Remain fault tolerant
- Catch the Bad Guy!



Types of IDS

▪ Host-Based IDS

- Primary purpose is to detect intrusions, log suspicious events, and send alert.
- Can detect both external and internal intrusions
- Anomaly-based vs Signature-based detection



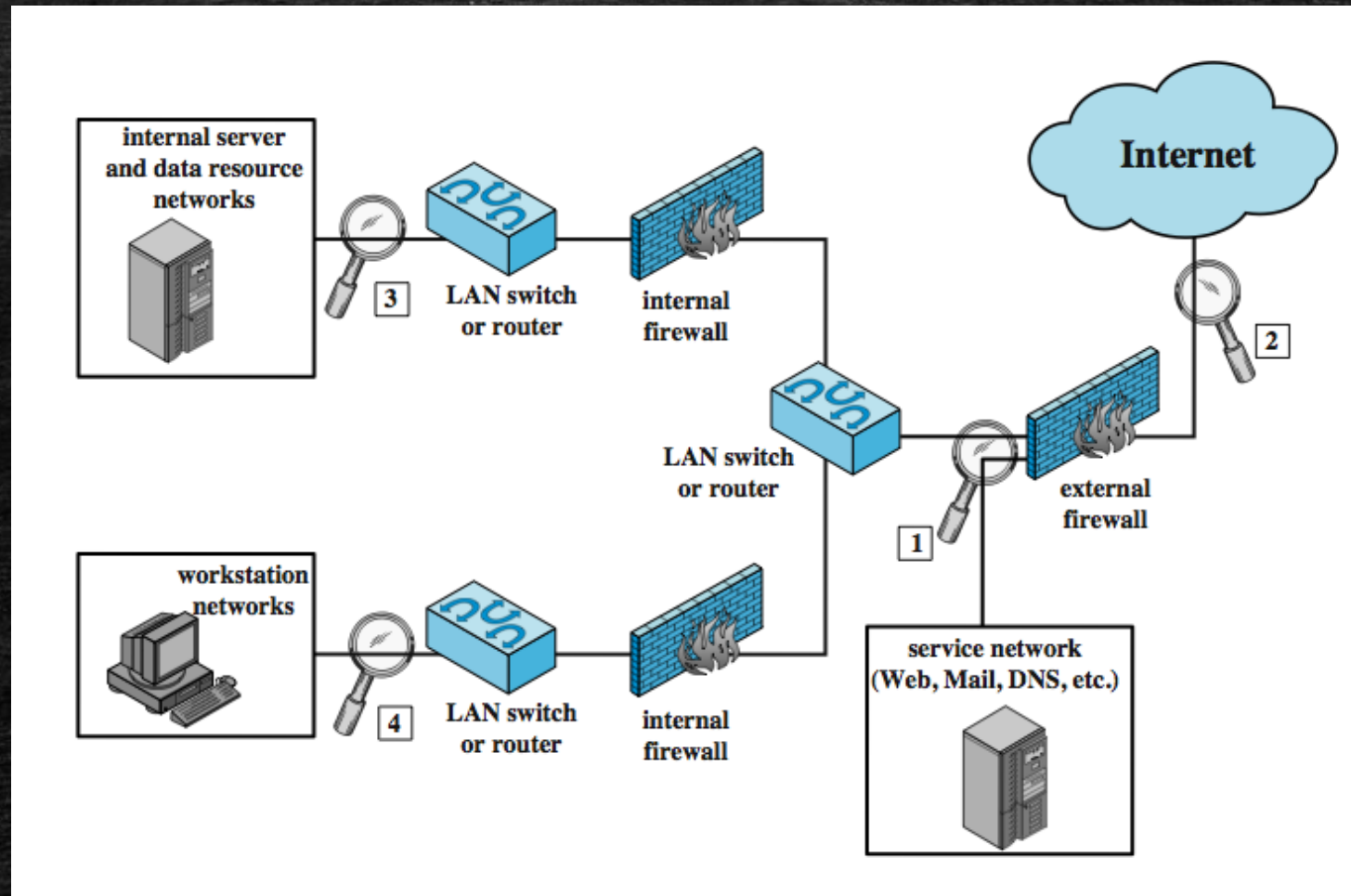
Types of IDS (cont)



▪ Network-Based IDS

- Monitor traffic at selected points on a network
- Detect intrusions in (near) real time
- Ability to examine high level protocol activity directed toward systems
- Modes
 - Signature-based detection
 - Anomaly-based detection

Types of IDS (cont)



Types of IPS

▪ Host-Based IPS

- Identifies attacks using both:
 - Signature detection techniques
 - Malicious application packets
 - Anomaly detection techniques
 - Behavior patterns that indicate malware.
- Can also sandbox applets to monitor behavior



Types of IPS (cont)



▪ Network-Based IPS

- Inline NIDS that can discard packets or terminate TCP connections
- Uses signature and anomaly detection
- Can identify malicious packets using:
 - pattern matching, stateful matching, protocol anomaly, traffic anomaly, statistical anomaly
 - **Disadvantage: Accidentally block all traffic if a mistake is made.**

Land Your Plane...



Detection Trifecta

Network-Based
IPS

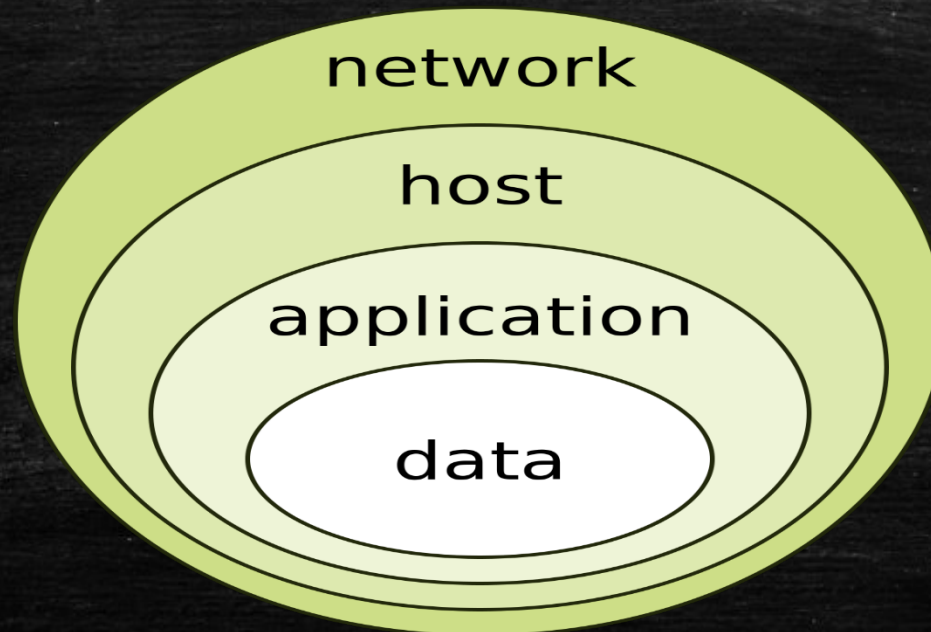
+

Network-Based IDS
(Internal & External Sensor)

+

Host-Based IPS

=



Mission Complete

- Discovering Speed Isn't a Factor (Indicator Gathering)
- Navigate through Heavy Packet Traffic (Long Tail Analysis)
- Cloned Camera's on the Autobahn (Honeypot Networks)
- Blocking Traffic in the Fast Lane (IDS vs IPS)

Connect with me



Adrian Kelley, CISSP, CISA, GPEN

Cyber Security Specialist

Las Vegas Sands Corp. • Strayer University-Maryland

Las Vegas, Nevada • 500+ 

Thank You!

Sands

LAS VEGAS SANDS CORP.

2017
FIRST
Technical
Colloquium

Las Vegas, US
Dec 05-06, 2017

FIRST
Improving Security Together



SOC Operations on the Autobahn

Don't let the green grass fool you...