



**You are going to get hacked.
It will not be over quickly.
You will not enjoy it.
Be prepared.**

John Strand



© Black Hills Information Security | @BHInfoSecurity

Conversation



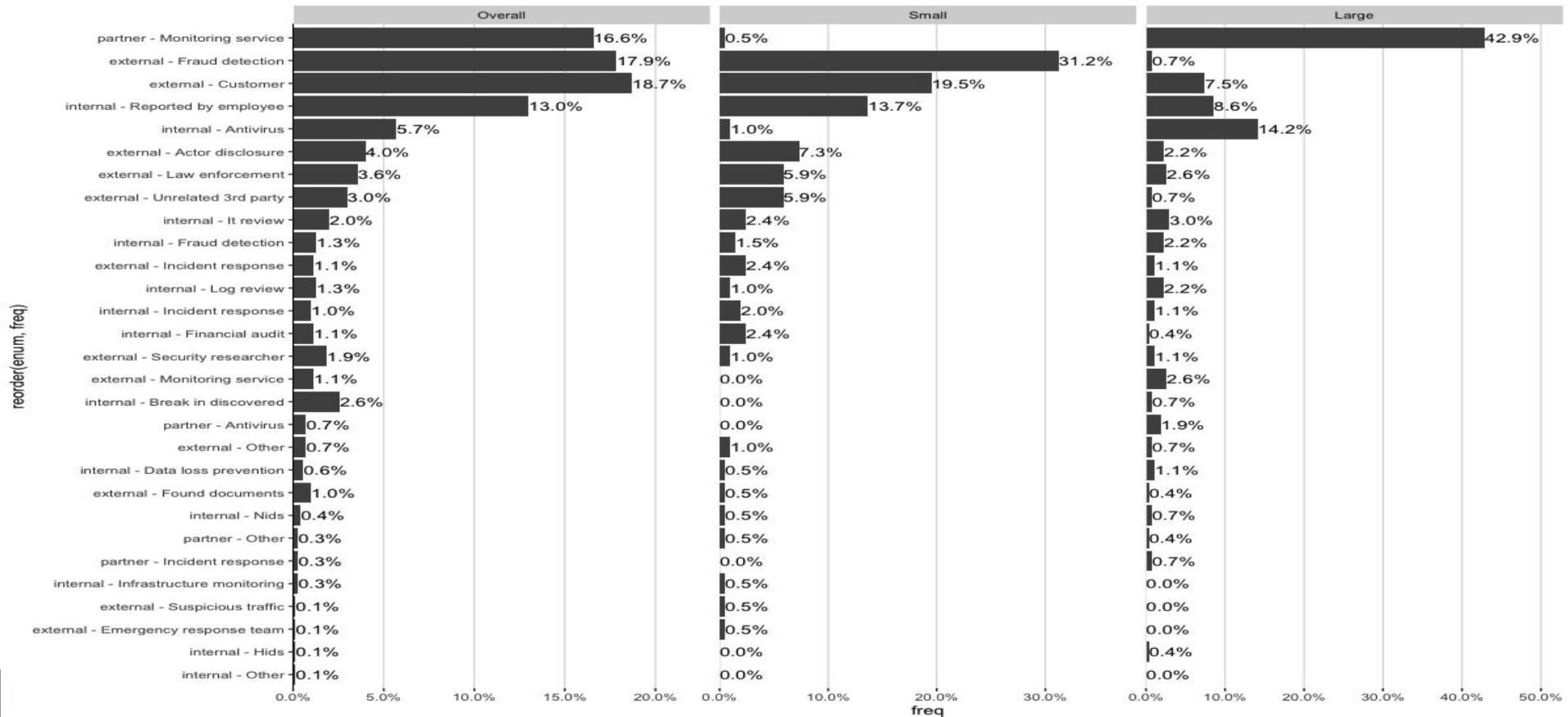
- There are a number of things that need to be aligned to be “ready”
- But, almost no one ever is
- We are not going to spend time on preparation
- But we have a game
- We think it can help

BRIDGE
CHECKERS
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE
GLOBAL THERMONUCLEAR WAR

XR



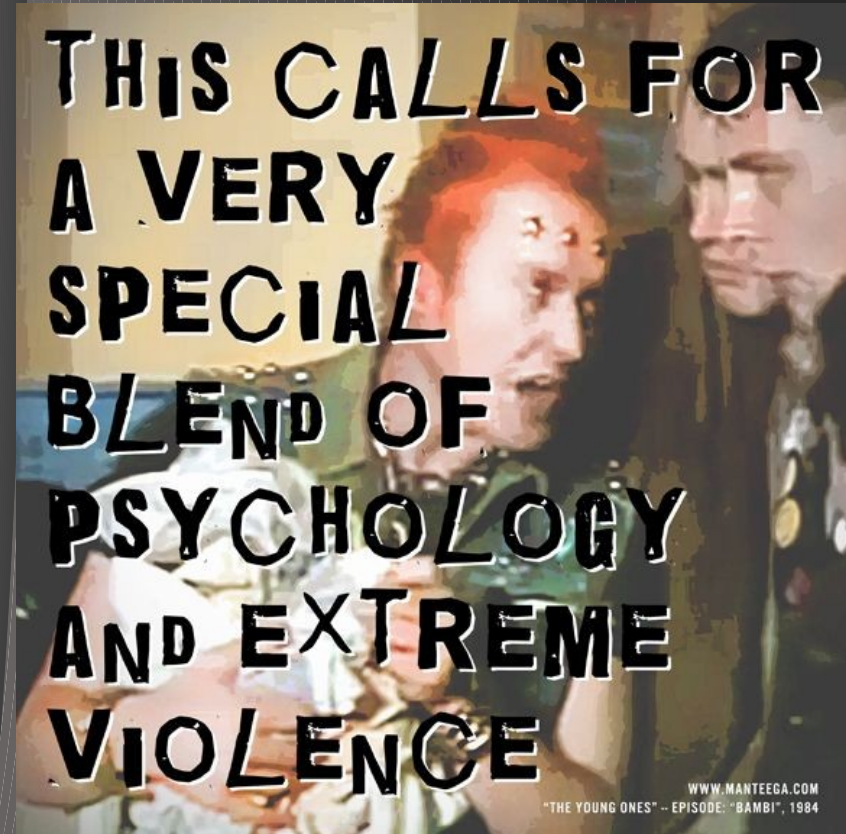
We Have a Problem



Politics and Psychology



- There is a need to prepare your org mentally
- Not “If”... “When”
- Roles, responsibilities and....
AUTHORIZATIONS!!!!
- Table top exercises



Server Analysis



- Servers are “different” from workstations
- Specific roles
- Software
- Critical files and configurations
- “Normal” access to applications
- Yes, this applies to cloud



© Black Hills Information Security | @BHInfoSecurity

SERVER ANALYSIS

The ability to baseline and verify a system is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe

TOOLS

DeepBlueCLI
SANS Analysis Cheat Sheets



<https://github.com/sans-blue-team/DeepBlueCLI>

SIEM



- SIEM is pretty broken....
 - But!!!!
- You need it for so many compliance reasons
- JPCert Helps
- What are you logging?
- Sysmon?
- A note on application logs



© Black Hills Information Security | @BHInfoSecurity

SECURITY INFORMATION AND EVENT MANAGEMENT LOG ANALYSIS (SIEM) LOG ANALYSIS

Yeah...good luck with this one. Are you logging the right things? Do you regularly emulate attacks to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tools Analysis



JPCERT **CC**®

<https://github.com/philhagen/sof-elk>

<https://jpcertcc.github.io/ToolAnalysisResultSheet>

Firewall Logs



- So many questions
 - How many hit this IP?
 - When was the connection made?
 - Can we block?
- Firewalls tend to be great choke points
- Critical to know how to use them properly



© Black Hills Information Security | @BHInfoSecurity

FIREWALL LOG REVIEW

Can your organization analyze and understand firewall logs? Do you regularly run attack scenarios and verify that your procedures work?

TOOLS

SOF-ELK



<https://github.com/philhagen/sof-elk>

Zeek and RITA



- RITA is awesome
- I am very biased
- Nuance, TeamViewer, RDP
- Any other systems compromised?
- Easy to set up
- Lots of digging, lots to learn



© Black Hills Information Security | @BHInfoSecurity

NETFLOW, BRO/ZEK/ REAL INTELLIGENCE THREAT ANALYTICS (RITA) ANALYSIS

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids do?

TOOLS

RITA (Real Analysis and Threat Analytics)
Security Onion



<https://www.activecountermeasures.com/free-tools/rita>

<https://securityonion.net>

Segmentation



- Bulkheads and the Titanic
- The ability to quickly isolate network segments is key
- You do not want to be Googling this in the middle of an incident
- Firewalls in NYC and Amsterdam...

INTERNAL SEGMENTATION

Turn on your host based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

TOOLS

netsh advfirewall
iptables



Endpoint Protection Review



- Yes, I do have issues with most Blacklist AV
- However, it is a great place to quickly review potential malware across a whole org
- Many malware infections do show up on AV logs.. They are just not reviewed

ENDPOINT SECURITY PROTECTION ANALYSIS

I know, you have AV. Great!!! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes around you like a clueless action star?

TOOLS

Check with your vendor, they miss you and always want to chat.





- Two edged sword
- Very effective
- Lots of “false” positives
- Requires tuning
- Stacked analysis
- LogonTracer



USER BEHAVIORAL AND ENTITY ANALYTICS (UBEA)

It is like logging, but it actually works. Looks for multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays and more!

TOOLS

LogonTracer

abNORMAL

<https://github.com/JPCERTCC/LogonTracer>

Endpoint Analysis

- Cheat Sheets!!!
- DeepBlueCLI
- Sysmon
- Powershell and Command Logging
- Baselines
- Pratices... Pratices. Practice.



© Black Hills Information Security | @BHInfoSecurity

ENDPOINT ANALYSIS

This is where the defender uses their Cheat Sheets to detect attacks on workstations. Time to bring in the help desk.. And pray.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets



<https://github.com/sans-blue-team/DeepBlueCLI>

Crisis Management

- Oh boy...
- How to handle key events
- Public breach
- Legal requirements to notify
- Lawyers
- FBI and Secret Service coordination
- Dealing with Krebs
- Right and wrong ways



© Black Hills Information Security | @BHInfoSecurity

CRISIS MANAGEMENT

Your legal and management teams have procedures for effectively and ethically notifying impacted victims of compromises.

TOOLS

This almost never happens. But, a good notification strategy will really help deal with the political fallout.



Isolation

- Different from Segmentation
- This is specific to isolation of single systems
- Both skills are necessary
- This can be done at the switch level
- Multiple “levels” of isolation
- How far do you want to go?
 - Lock out?
 - Sandbox?
 - Upsidedowninternet



© Black Hills Information Security | @BHInfoSecurity

ISOLATION

Your Network team is on their game. They can easily isolate systems that are infected to an infected VLAN.

TOOLS

Simple switch and router commands



Losing People...



LEAD HANDLER TAKES MATERNITY OR PATERNITY LEAVE

Yea, there is always one person who pretty much runs the who IR process. That one essential person. Well, now it is time for the IM to silence that person.

NOTES

We have to be able to work effectively without the one or two most advanced people on the team. All of the quite people who are just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!



LEGAL TAKES YOUR ONLY SKILLED HANDLER INTO A MEETING TO EXPLAIN THE INCIDENT

Who brought a Lawyer to the party? There is always one person who pretty much runs the who IR process. That one essential person. Well, now it is time for the IM to silence that person.

NOTES

They may never come back...all of the quiet people who are just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!



A Note on Murder.



BOBBY THE INTERN KILLS THE SYSTEM YOU ARE REVIEWING

This. Happens. Far. Too. Often.

NOTES

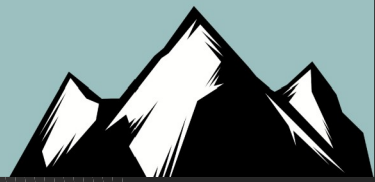
No. Murder is never ok. Don't even think that.

%@*#!



© Black Hills Information Security | @BHInfoSec

Questions?



© Black Hills Information Security | @BHInfoSecurity