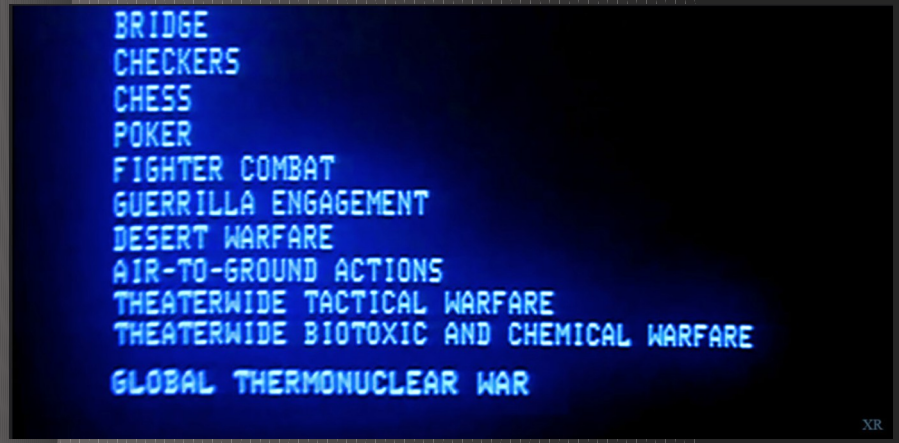
You are going to get hacked. It will not be over quickly. You will not enjoy it. Be prepared.

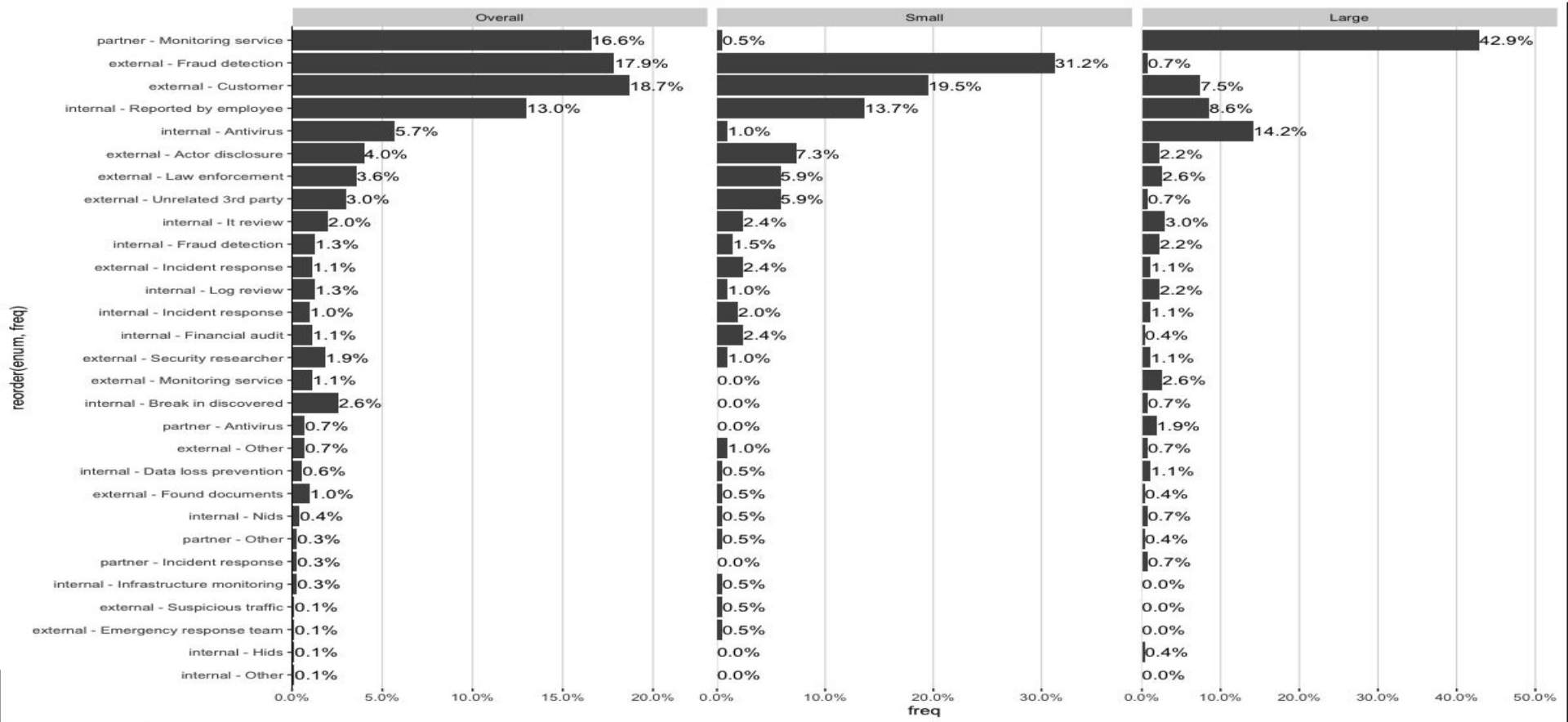
John Strand

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

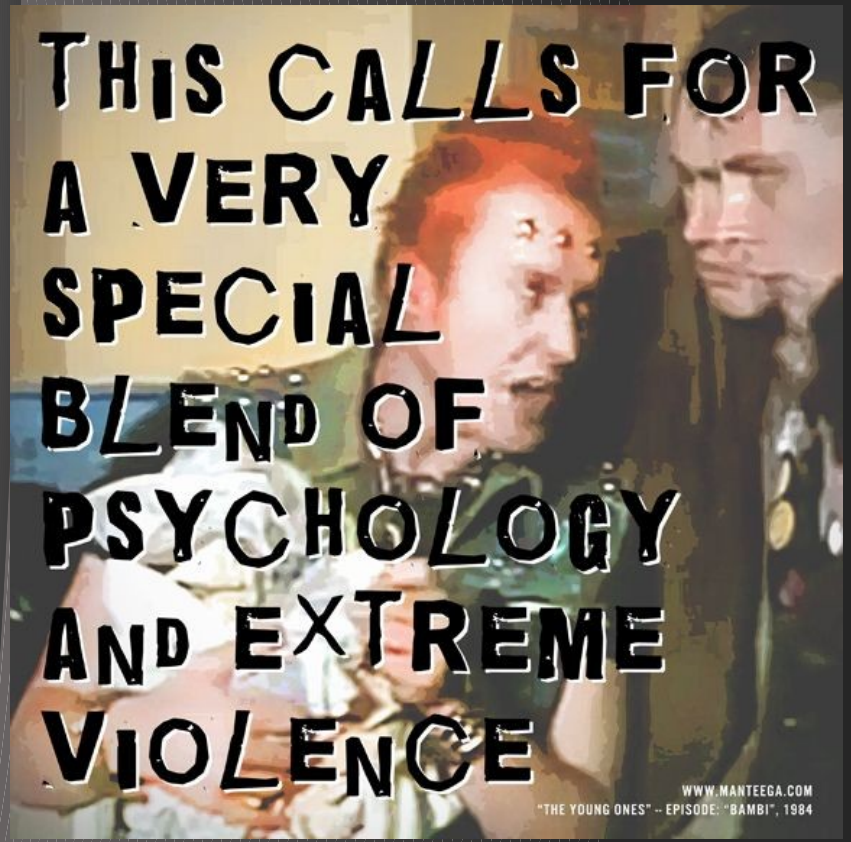


We Have a Problem



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

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

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

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

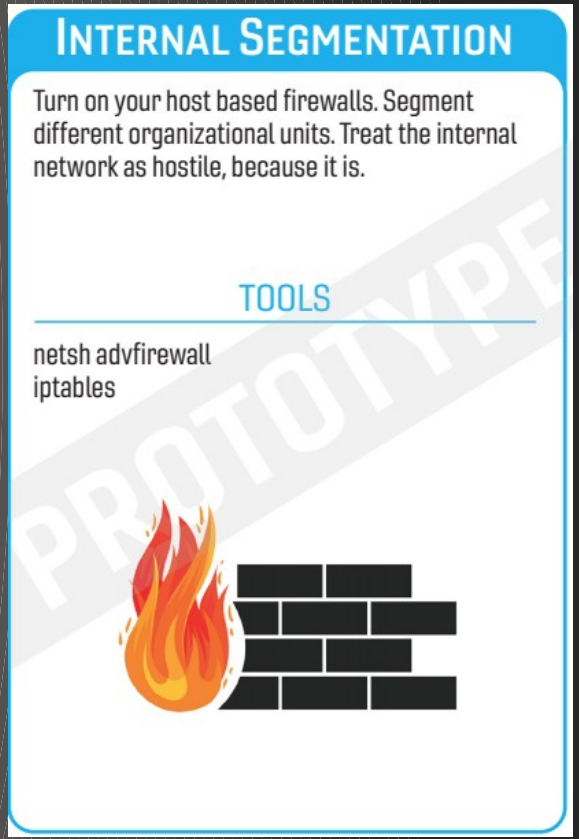
https://github.com/philhagen/sof-elk

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

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...

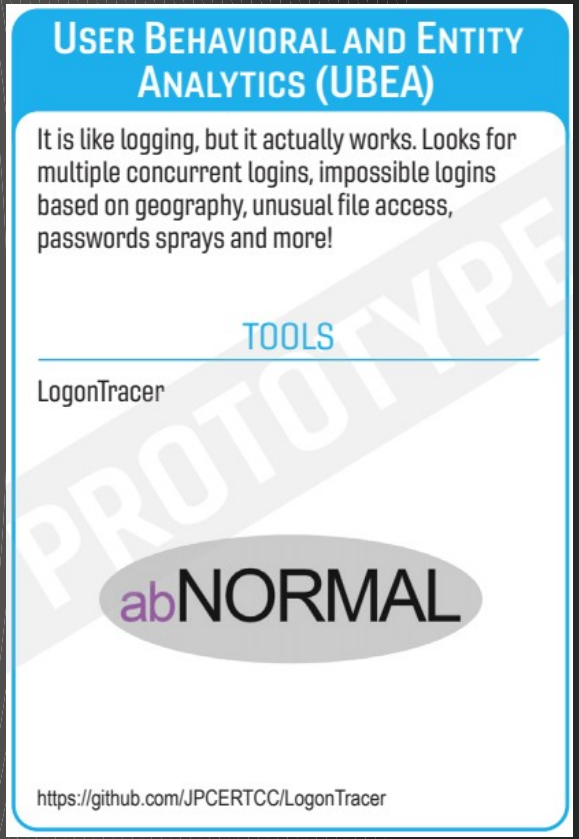


Endpoint Protection Review

- 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

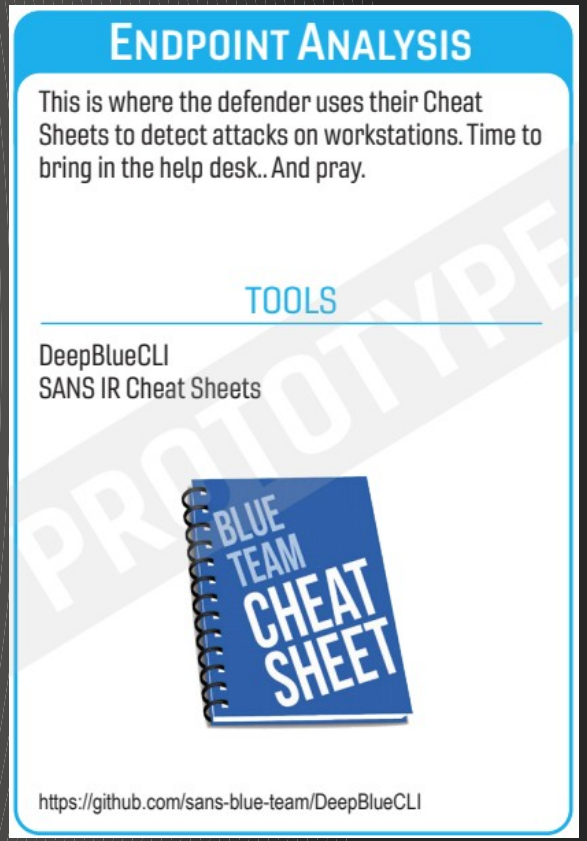
UBEA

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



Endpoint Analysis

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

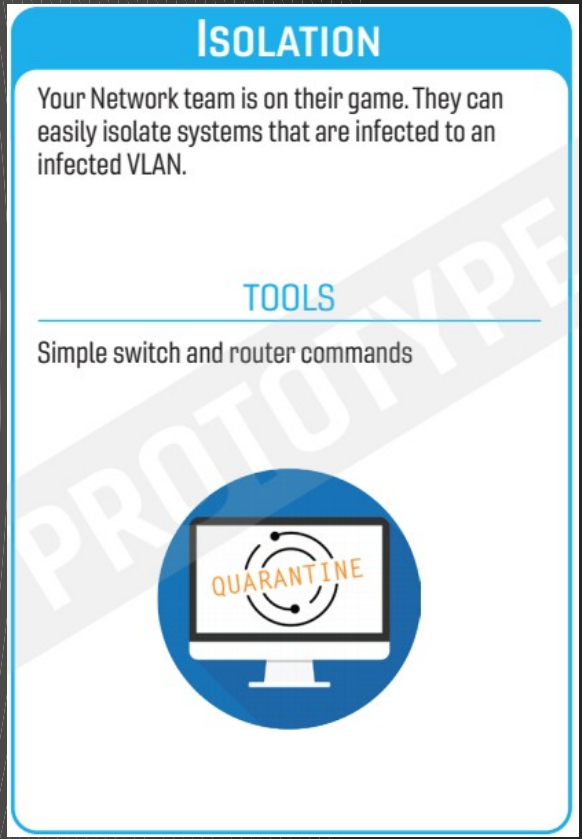


Crisis Management

- 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

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?
  - Upsidedownternet



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.

Questions?