Incident
Non-Response

When the worst response is non-response

Russell Brinson

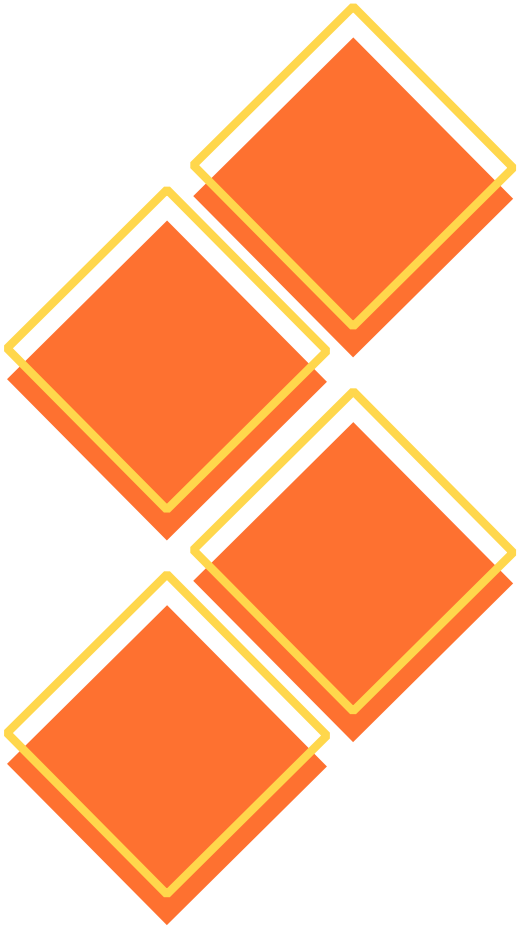
1 Pre-Presentation Game

Preparation 2

3 Detection & Analysis

Containment, Eradication,
& Recovery 4

5 Post-Incident Activity



1

Game

Guidelines

- The security team must get the exact amount of lateral movement
- All services must come back up
- You are to escalate your issues and resolve them - talking to people you are allowed to on your card

Incident Response Process

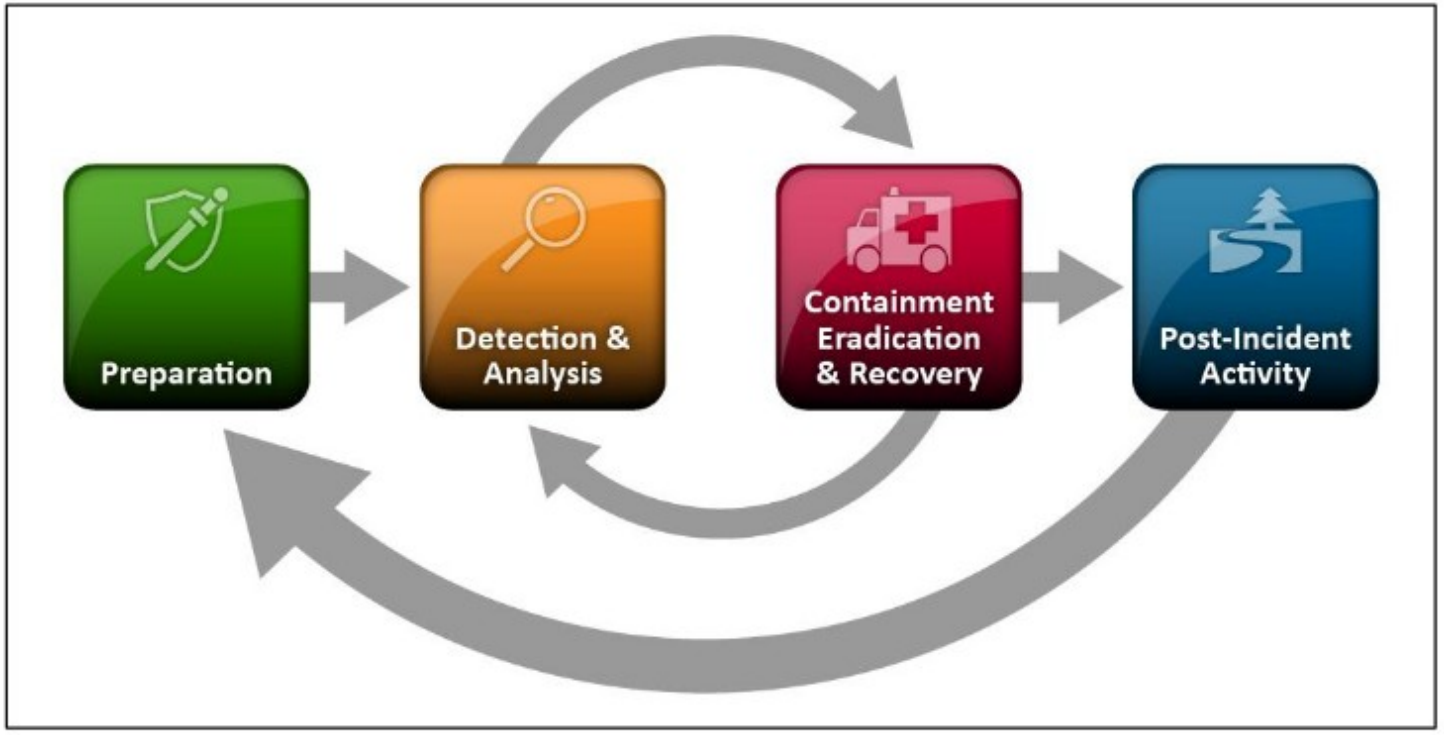


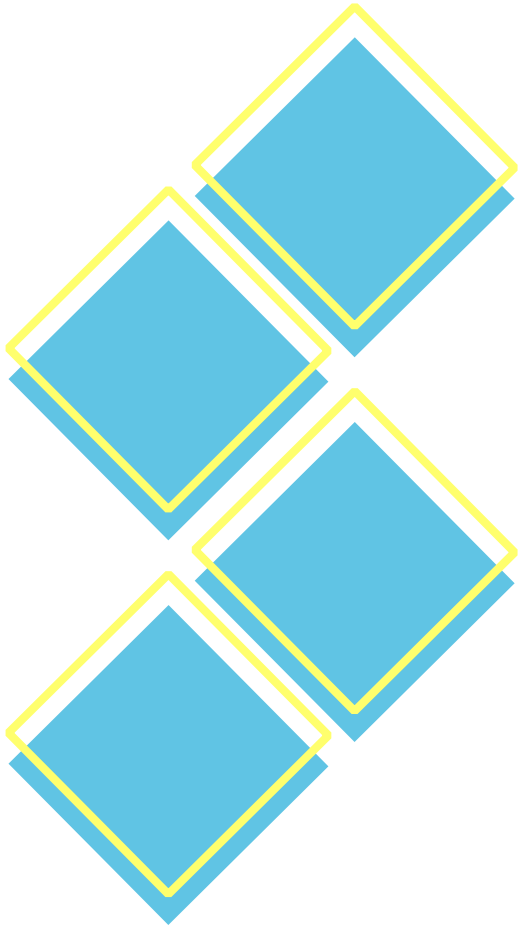
Figure 3-1. Incident Response Life Cycle

Stakeholders

- Have you ever got the entire response team together?
- Do you split into technical / management?
- Who is allowed to contact who?

Figure 2-1. Communications with Outside Parties

2 Preparation



Do NOT

- Prepare for an incident
- Prevent an incident

Prepare for an incident

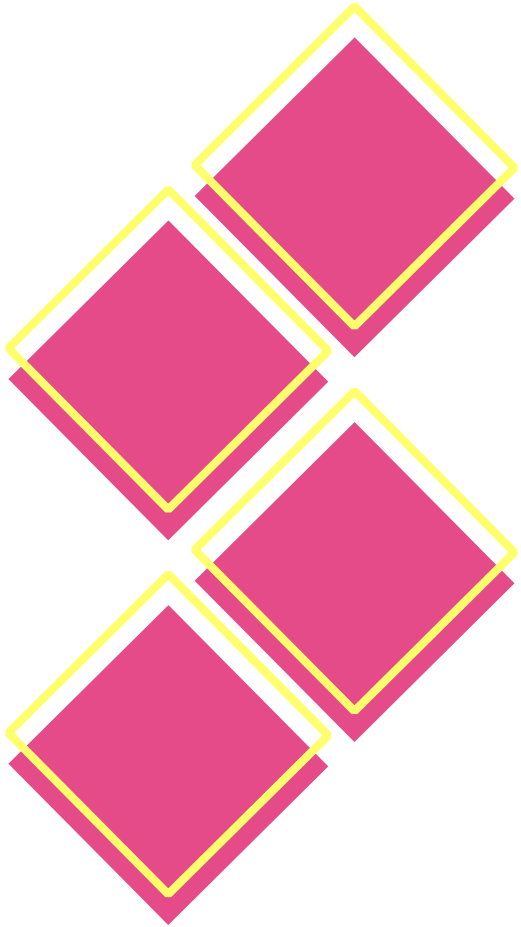
- Dedicated survivor computers
- Out-of-band communication
- Manual authentication for remote individuals

Prevent an Incident

- MFA
- Fixing bugs and misconfigurations
- MFA
- Let your proxy handle the malware

3

Detection & Analysis



Boom is coming…

- A third party tells you they spotted a ransomware gang on your network

Example

Friday

“[The AV Scan] went on, without any problems, and their IT Support Team reports no issues visible to them. We consider the source suspect and the case closed.”

Example

Friday

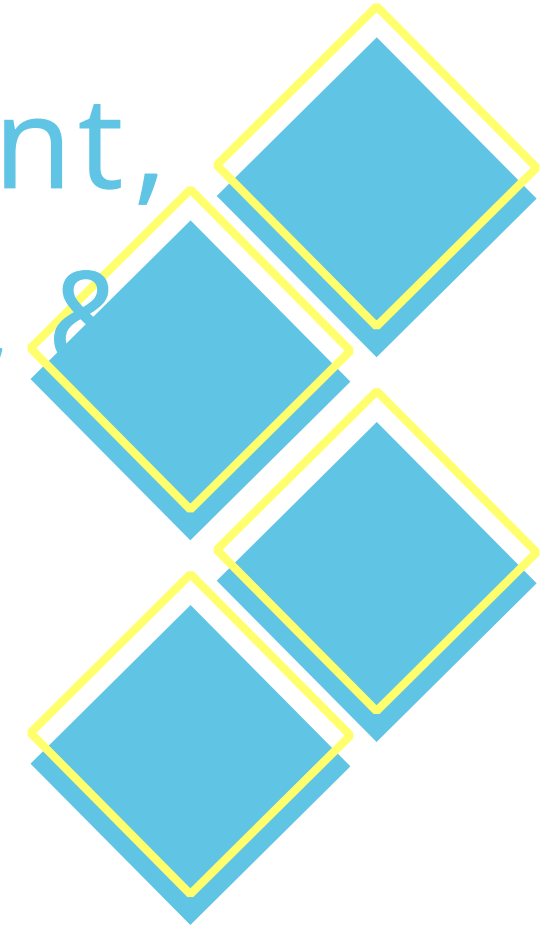
“[The AV Scan] went on, without any problems, and their IT Support Team reports no issues visible to them. We consider the source suspect and the case closed.”

Monday

“We are a victim of ransomware. Please advise how to proceed.”

4

Contiainment, Eradication, & Recovery

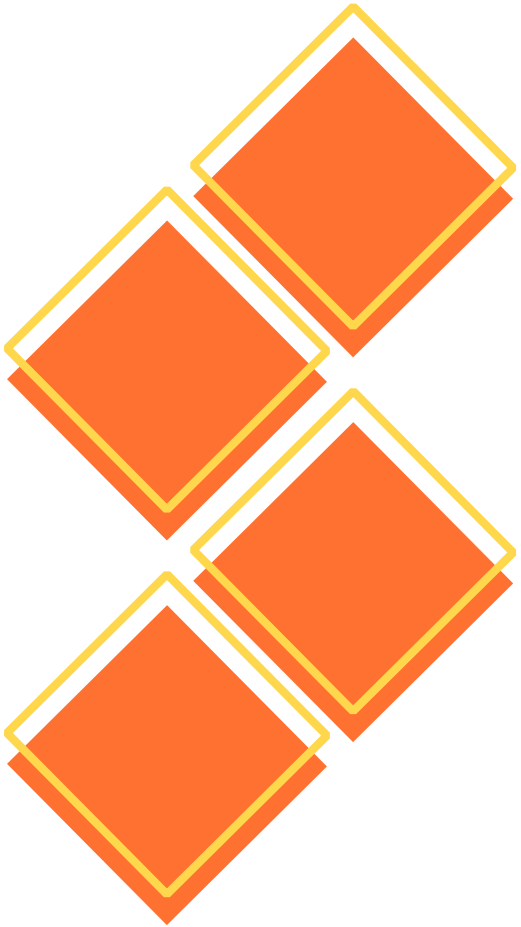


You told security to shove it…

- GeoBlocking will not solve your problem
- Turning off your internet for a day won’t make the issue go away

Lets NOT get Forensics

- A beacon was detected on the DC
- Firewall with default logging properties



5

Post-Incident Activities

That won’t happen again… right?

- Spend a lot of money without a plan
- Lightning was strike twice so why spend money?