

“Why are they asking me to do this?”

or Adventures in IR Land



@GyledC

whoami

- Melbourne-based Sr. Security Consultant – IR for IBM X-Force IR
- Shifted to tech in the early part of this century
- Received her Graduate Certificate in Incident Response from the SANS Institute and Master in Cyber Security – Digital Forensics from UNSW Canberra (ADFA)
- Volunteers for different organisations (Defcon BTV, TL, KSD)
- Mentor: Defcon Blue Team, UNSW alumni and AWSN
- Twitter: @GyledC

Agenda

- Why?
- Incident Response Lifecycle
- Typical Activities/Questions

Why?

X-Force Threat Intelligence Index 2021

“the proliferation of malware targeting Linux was the dominant trend of 2020”

<https://www.ibm.com/au-en/security/data-breach/threat-intelligence>



Photo by Ibrahim Boran on Unsplash

Why?

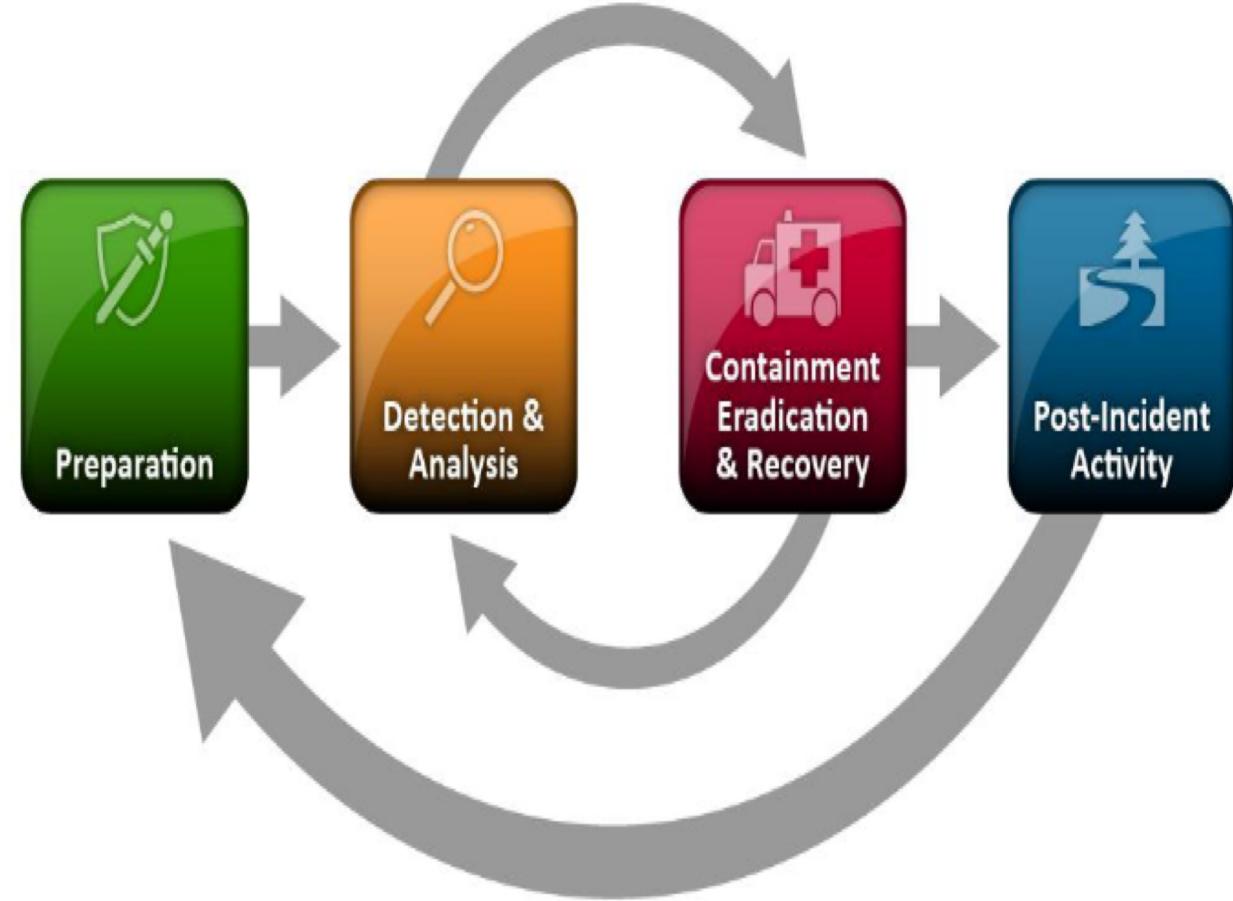
- Sys Admins as security incident first responders
- Walkthrough the IR process



Photo by Headway on Unsplash

IR Lifecycle

- Each phase has its own activities
- Source: NIST Computer Security Incident Handling Guide



Preparation

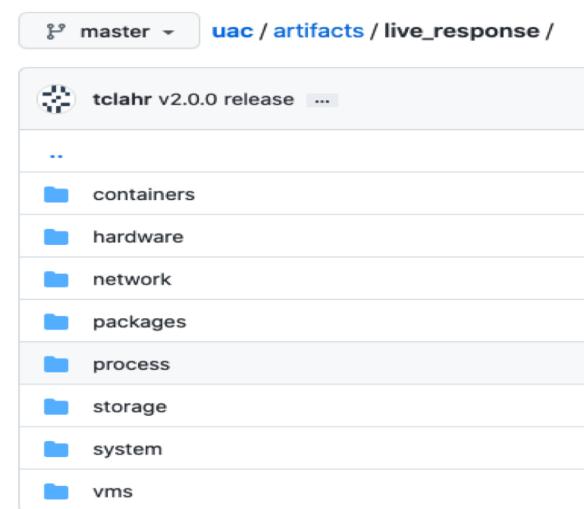
- Could you attend the TTX?
- Could you check this playbook?
- Could you check the log retention period?



Photo by Michèle Eckert on Unsplash

Detection and Analysis

- (if not previous done) Could you install this EDR agent?
 - Could you run these scripts to collect a triage package?
 - Could you collect these artefacts?
 - /etc – system-wide config files
 - /home - user
 - /var – logs
 - wtmp – successful logins & logouts
 - btmp – failed login
 - lastlog – most recent user logins
- Tools
 - Velociraptor - offline triage collector
 - UAC - Unix-like Artifacts Collector



Containment, Eradication and Recovery

- Could you quarantine/contain this server?
- Could you do a fresh re-install?
- Could you use the back-ups?
- Are our back-ups clean? Usable?

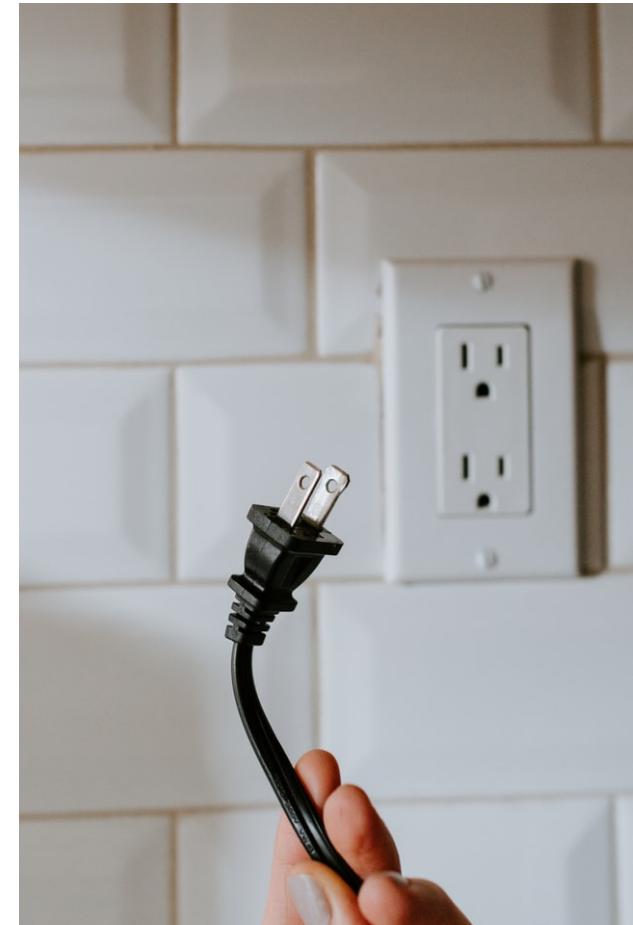


Photo by Kelly Sikkema on Unsplash

Post-incident Activity (lessons learned)

- What can we improve?
- What did we learn from this?
- What improvements do we need to make?
- How can we do better next time?

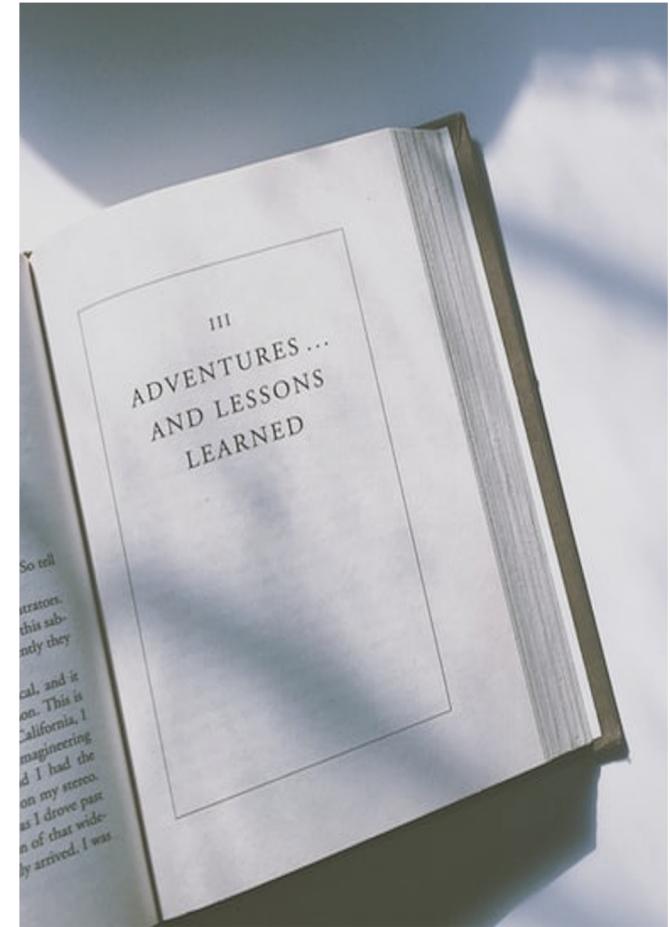


Photo by Ryan Graybill on Unsplash

References

- IBM X-Force Threat Intelligence Index:
<https://www.ibm.com/security/data-breach/threat-intelligence>
- NIST Computer Security Incident Handling Guide:
<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>
- Practical Linux Forensics: <https://nostarch.com/practical-linux-forensics>
- UAC: <https://github.com/tclahr/uac>
- Velociraptor: <https://github.com/Velocidex/velociraptor>
- If there are other questions after this conference, please feel free to send me a DM in Twitter: @GyledC