Incident Response TTX Workshop

Terin D. Williams
Cybersecurity Advisor, Ohio
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency
Resilience Defined

“… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…”

- Presidential Policy Directive 21
  February 12, 2013

<table>
<thead>
<tr>
<th>Protect (Security)</th>
<th>Sustain (Continuity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform (Capability)</td>
<td>Repeat (Maturity)</td>
</tr>
</tbody>
</table>
# CTTX Format

<table>
<thead>
<tr>
<th>Duration:</th>
<th>4-8 hours (minimum of 4 hours usually unless you do them often)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participants:</td>
<td>Facilitator; Notetaker; Decision maker; IT team; cybersecurity team; legal, HR, PR/marketing, CFO/procurement person; operations and more!</td>
</tr>
<tr>
<td>Type:</td>
<td>TTX only; Functional; Hybrid</td>
</tr>
</tbody>
</table>
CISA CTTX Resources

Planning Assistance: Exercise Team or Cybersecurity Advisor (CSA)

CISA Cybersecurity TTX templates

https://www.cisa.gov/publication/cybersecurity-scenarios

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework
IR Agenda

1. Preparation/Identification
2. Containment
3. Eradication
4. Recovery
5. Lessons Learned
Preparation
1. Logging the RIGHT things
2. Backups (3-2-1 rule)
3. MFA (multi-factor authentication)
4. Canaries/honey elements
5. Data exfiltration prevention tools
6. TTX muscle memory (and hard copy of incident response plan)/incident playbook
7. Hard copy of network diagram (within last six months)
8. Hard copy of asset inventory (within last six months)
9. Centralized logging solution
10. Cybersecurity aware employees (trained)
Resources & Links (Adversary)

Shodan
https://www.shodan.io

Censys
https://censys.io

Compromised Accounts
https://haveibeenpwned.com

MitreAtt&ck Framework
https://attack.mitre.org

Hackmageddon
https://www.hackmageddon.com

Train your IT(Sec+ or equivalent)/cybersecurity(CE|H or equivalent) employees in offense to make better defenders!!!
Containment
Eradication
Recovery
Lessons Learned
Range of Cybersecurity Assessments (NO COST)

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Phishing Campaign Assessment (PCA)
- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (VSS)
- Web Application Scanning (WAS)
- Remote Penetration Test (RPT)
- Risk & Vulnerability Assessment (RVA)
- Red Team Assessment (RTA)
CISA Resources & Links

CISA Shields Up

https://www.cisa.gov/shields-up

CISA Cyber Essentials

https://www.cisa.gov/cyber-essentials

CSET Ransomware Readiness Assessment

https://github.com/cisagov/cset/releases/tag/v10.3.0.0

Other CISA Cyber Resources

https://www.cisa.gov/cyber-resource-hub
CISA Contact Information

Terin D. Williams
Cyber Security Advisor, Ohio
Cybersecurity & Infrastructure Security Agency

Email: terin.williams@cisa.dhs.gov
Mobile: 614.314.7793