

(P) Preparation	(I) Identification	(C) Containment
<div>1. Patch asset vulnerabilities</div> <div>2. Perform routine inspections of controls/weapons</div> <div>3. Maintain Antivirus/EDR application updates</div> <div>4. Create network segmentation</div> <div>5. Log traffic between network segments</div> <div>6. Incorporate threat intelligence</div> <div>7. Perform routine inspections of asset backups</div> <div>8. Conduct phishing simulations</div> <div>9. Conduct user security awareness training</div> <div>10. Conduct response training (this PBC)</div>	<div>1. Monitor:</div> <div> a. Email mirroring services that scan copies of emails for malicious content ^[1]</div> <div> b. Traffic patterns and packet contents, specifically looking for unusual uses of protocols internally ^[1]</div> <div> c. Network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. ^[1]</div> <div>2. Investigate and clear ALL alerts associated with the impacted assets or accounts</div> <div>3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity</div>	<div>1. Inventory (enumerate & assess)</div> <div>2. Detect Deny Disrupt Degrade Deceive Destroy</div> <div>3. Observe -> Orient -> Decide -> Act</div> <div>4. Issue perimeter enforcement for known threat actor locations</div> <div>5. Archive scanning related artifacts such as IP addresses, user agents, and requests</div> <div>6. Determine the source and pathway of the attack</div> <div>7. Fortify non-impacted critical assets</div>
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<div>1. Close the attack vector by applying the Preparation steps listed above</div> <div>2. Perform endpoint/AV scans on targeted systems</div> <div>3. Reset any compromised passwords</div> <div>4. Inspect ALL assets and user activity for IOC consistent with the attack profile</div> <div>5. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery</div> <div>6. Patch asset vulnerabilities</div>	<div>1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)</div> <div>2. Address any collateral damage by assessing exposed technologies</div> <div>3. Resolve any related security incidents</div> <div>4. Restore affected systems to their last clean backup</div>	<div>1. Perform routine cyber hygiene due diligence</div> <div>2. Engage external cybersecurity-as-a-service providers and response professionals</div> <div>3. Implement policy changes to reduce future risk</div> <div>4. Utilize newly obtained threat signatures</div> <div>5. Avoid opening email and attachments from unfamiliar senders</div> <div>6. Avoid opening email attachments from senders that do not normally include attachments</div> <div>7. Pay attention to unusual behavior exhibited by trusted parties</div> <div>8. Remember that data and events should not be viewed in isolation but as part of a chain of behavior that could lead to other activities</div>

References:

1. MITRE ATT&CK Technique T1534:
<https://attack.mitre.org/techniques/T1534/>

Resources:

→ GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan

→ IT Disaster Recovery Planning: <https://www.ready.gov/it-disaster-recovery-plan>

→ Report Cybercrime: <https://www.ic3.gov/Home/FAQ>