

| (P) Preparation   | (I) Identification   | (C) Containment   |
|---|--|---|
| <div><div><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 user security awareness training</div><div>9. Conduct response training (this PBC)</div><div>10. Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic [2]</div><div>11. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level [3]</div></div></div> | <div><div><div>1. Monitor for:<div><div>a. newly constructed network connections that are sent or received by untrusted hosts [4]</div><div>b. network data exhibiting uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious [4]</div></div></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>4. Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows [4]</div></div></div> | <div><div><div>1. Inventory (enumerate &amp; assess)</div><div>2. Detect   Deny   Disrupt   Degrade   Deceive   Destroy</div><div>3. Observe -&gt; Orient -&gt; Decide -&gt; 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></div></div>  |
| (E) Eradication   | (R) Recovery   | (L) Lessons/Opportunities   |
| <div><div><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></div>   | <div><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></div>   | <div><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. 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></div></div> <div><div>References:<div><div>1. <a href="https://attack.mitre.org/techniques/T1572/">https://attack.mitre.org/techniques/T1572/</a></div><div>2. <a href="https://attack.mitre.org/mitigations/M1037/">https://attack.mitre.org/mitigations/M1037/</a></div><div>3. <a href="https://attack.mitre.org/mitigations/M1031/">https://attack.mitre.org/mitigations/M1031/</a></div><div>4. <a href="https://attack.mitre.org/datasources/DS0029/">https://attack.mitre.org/datasources/DS0029/</a></div></div></div></div> |