

(P) Preparation	(I) Identification	(C) Containment
<div>1. Patch asset vulnerabilities</div> <div>2. Perform routine inspections of controls/weapons</div> <div>3. Ensure antivirus/endpoint protection software is installed on workstations and laptops</div> <div>4. Confirm that servers and workstations are logging to a central location</div> <div>5. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment</div> <div>6. Conduct employee security awareness training</div> <div>7. Restrict users to the least privileges required</div> <div>8. Ensure permissions are in place to restrict unauthorized users from interfering with security services <sup>[1]</sup></div>	<div>1. Monitor for:<div>a. Unauthorized modifications to the Windows Registry <sup>[2]</sup></div><div>b. Unauthorized modifications to the firewall</div><div>c. Unauthorized command or script execution <sup>[3]</sup> <sup>[4]</sup></div><div>d. Unauthorized process creation or termination <sup>[5]</sup></div><div>e. Unauthorized access or modification to security tools/weapons</div></div> <div>2. Investigate and clear ALL alerts associated with the impacted assets</div> <div>3. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual activity</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>
(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>7. Reset accounts that have been breached immediately</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. 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>References:</div><div>1. MITRE ATT&amp;CK Technique T1562: <a href="https://attack.mitre.org/techniques/T1562/">https://attack.mitre.org/techniques/T1562/</a></div><div>2. MITRE ATT&amp;CK Datasource DS0024: <a href="https://attack.mitre.org/datasources/DS0024/">https://attack.mitre.org/datasources/DS0024/</a></div><div>3. MITRE ATT&amp;CK Datasource DS0017: <a href="https://attack.mitre.org/datasources/DS0017/">https://attack.mitre.org/datasources/DS0017/</a></div><div>4. MITRE ATT&amp;CK Datasource DS0012: <a href="https://attack.mitre.org/datasources/DS0012/">https://attack.mitre.org/datasources/DS0012/</a></div><div>5. MITRE ATT&amp;CK Datasource DS0009: <a href="https://attack.mitre.org/datasources/DS0009/">https://attack.mitre.org/datasources/DS0009/</a></div></div>

**Resources:**

→ GuardSight GSVSOC Incident Response Plan: [https://github.com/guardsight/gsvsoc\\_cybersecurity-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>