

(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. Regularly update virus definitions and signatures</div> <div>5. Conduct employee security awareness training</div> <div>6. Ensure all software is kept up to date</div> <div>7. Audit for permission weaknesses that could be used to escalate privileges <sup>[4]</sup></div> <div>8. Leverage GPO to force tasks to run under an authenticated account <sup>[2]</sup></div> <div>9. Restrict scheduled tasks to a defined group of administrators <sup>[3]</sup></div>	<div>1. Monitor for:<div>a. Existing commands that may abuse task scheduling functionality to execute malicious code <sup>[1]</sup></div><div>b. Newly constructed containers or files that may abuse task scheduling to execute malicious code <sup>[1]</sup></div><div>c. Newly created scheduled jobs for initial indicators of malicious activity <sup>[1]</sup></div></div> <div>2. Investigate and clear ALL alerts</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. Utilize EDR hunter/killer agents to terminate offending processes</div> <div>5. Remove the affected system from the network</div> <div>6. Determine the source and pathway of the attack</div> <div>7. Issue a perimeter enforcement for known threat actor locations</div>
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<div>1. Close the attack vector</div> <div>2. Create forensic backups of affected systems</div> <div>3. Perform endpoint/AV scans on targeted systems</div> <div>4. Reset any compromised passwords</div> <div>5. Inspect ALL assets and user activity for IOC consistent with the attack profile</div> <div>6. Inspect backups for IOC consistent with the attack profile PRIOR to system recovery</div> <div>7. Patch asset vulnerabilities</div> <div>8. Reset the passwords of any compromised accounts</div>	<div>1. Restore to the RPO (Recovery Point Objective) within the RTO (Recovery Time Objective)</div> <div>2. Assess and address collateral damage</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>References:<div>1. <a href="https://attack.mitre.org/techniques/T1053/">https://attack.mitre.org/techniques/T1053/</a></div><div>2. <a href="https://attack.mitre.org/mitigations/M1028/">https://attack.mitre.org/mitigations/M1028/</a></div><div>3. <a href="https://attack.mitre.org/mitigations/M1026/">https://attack.mitre.org/mitigations/M1026/</a></div><div>4. <a href="https://attack.mitre.org/mitigations/M1047/">https://attack.mitre.org/mitigations/M1047/</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>