

(P) Preparation	(I) Identification	(C) Containment
<div>1. Patch asset vulnerabilities</div> <div>2. Ensure antivirus/endpoint protection software is installed on workstations and laptops</div> <div>3. Confirm that servers and workstations are logging to a central location</div> <div>4. Review firewall, IDS, and IPS rules routinely and update based on the needs of the environment</div> <div>5. Restrict access to critical assets as needed</div> <div>6. Conduct employee security awareness training</div> <div>7. Restrict users to the least privileges required</div> <div>8. Audit system controls, features, and programs that may indirectly use the command line or a terminal and restrict such features to only those necessary ^[1]</div>	<div>1. Monitor for:<div>a. Social media activity for unusual body posts or inconsistent server requests</div><div>b. Suspicious emails and attachments coming into your organization</div></div> <div>2. Routinely check firewall, IDS, IPS, and SIEM logs for any unusual behavior</div> <div>3. Analyze web application metadata for suspicious user-agent strings and other artifacts</div> <div>4. Investigate and clear ALL alerts</div> <div>5. Monitor and analyze logs from host-based detection mechanisms, such as Sysmon, for events such as process creations that include or are resulting from parameters associated with invoking programs/commands/files and/or spawning child processes/network connections Social media activity related to your organization ^[1]</div>	<div>1. Inventory (enumerate & assess) environment technologies</div> <div>2. Detect Deny Disrupt Degrade Deceive Destroy</div> <div>3. Observe -> Orient -> Decide -> Act</div> <div>4. Archive scanning related artifacts such as IP addresses, user agents, and requests</div> <div>5. Determine the source and pathway of the attack</div> <div>6. Issue a perimeter enforcement for known threatactor locations</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 within the RTO</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><div>References:</div><div>1. MITRE ATT&CK Technique T1202: https://attack.mitre.org/techniques/T1202/</div></div>

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>