8 Steps to Create an Incident Response Plan

01

ESTABLISH AN INCIDENT RESPONSE TEAM

- Assign roles for detection, response, communication, and recovery.
- Ensure 24/7 availability and contact methods for critical members.

02

IDENTIFY POTENTIAL SECURITY INCIDENTS

- Define what constitutes an incident (e.g., malware, phishing, data breach).
- Classify incidents by severity to prioritize responses.

03

IMPLEMENT DETECTION AND REPORTING MECHANISMS

- Deploy monitoring tools like SIEM, IDS/IPS, and EDR.
- Establish clear reporting procedures for employees and third parties.

04

DEVELOP CONTAINMENT AND MITIGATION STRATEGIES

- Outline steps to isolate affected systems quickly.
- Minimize operational impact while stopping the spread.

05

PLAN FOR ERADICATION AND RECOVERY

- Remove the threat from all affected systems.
- Restore data from clean backups and verify system integrity.

06

LEARN FROM THE INCIDENT

- Document the timeline, root cause, and attacker behavior.
- Identify gaps in defenses and response processes.

07

CONDUCT POST-INCIDENT ANALYSIS AND IMPROVEMENT

- Host a "lessons learned" meeting with all stakeholders.
- Update policies, tools, and playbooks based on findings.

08

TRAIN AND TEST REGULARLY

- Run simulated incident drills and tabletop exercises.
- Keep your team sharp and your plan current.

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com