FIVE STEPS TO AN EFFECTIVE INCIDENT RESPONSE PROGRAM

What you need to know to prepare, protect, and mitigate against vulnerabilities and cyberattacks:

1 Develop a Prevention and Response Plan

- Prepare a plan in advance of an attack
- Find and address vulnerabilities
- Review and test your plan

2 Identify a Prevention and Response Team

- Choose an appropriate service level agreement
- Ensure the team possesses specialized expertise
- Vet and validate the team's claims

3 Perform a Compromise Assessment

- Run detection on current and previously compromised systems
- Collect evidence and investigate adversary tactics
- Remediate across the enterprise

4 Complete a Security Tools Assessment

- Evaluate existing security tools
- Execute a gap analysis
- Remediate findings and opportunities for improvement

5 Respond and Future-proof

- Contain discovered incidents immediately
- Perform complete remediation activities
- Carry out a sustainable prevention program

CYLANCE