Novatech

www.novatech-global.com

How to Protect Your Company from Cyberattacks in 5 Steps

Identify and Assess Risks

1

- **Conduct a Risk Assessment:** Evaluate your organization's data, systems, and applications to identify potential threats and vulnerabilities. This includes understanding the types of data you store and the consequences of a breach.

- **Map Out Assets:** Catalog critical assets (e.g., customer databases, financial records) and prioritize their protection.

- **Example:** Use tools like vulnerability scanners to detect weaknesses in your network.

Implement Technical Controls

2

- **Firewalls and Antivirus:** Deploy firewalls to block unauthorized access and use antivirus software to detect/remove malware.

- **Encryption:** Secure data in transit (e.g., via HTTPS) and at rest (e.g., encrypted databases).

- **Multi-Factor Authentication (MFA):** Require MFA for all accounts to add an extra layer of security.

- **Patch Management:** Regularly update software to fix known vulnerabilities.

Educate and Train Employees

3

- **Cybersecurity Awareness Training:** Teach staff to recognize phishing emails, avoid suspicious links, and use strong passwords.
- **Phishing Simulations:** Conduct regular tests to evaluate employees' ability to spot fake emails.
- **Password Policies:** Enforce complex, unique passwords and password managers.

Novatech

www.novatech-global.com

Develop an Incident Response Plan

4

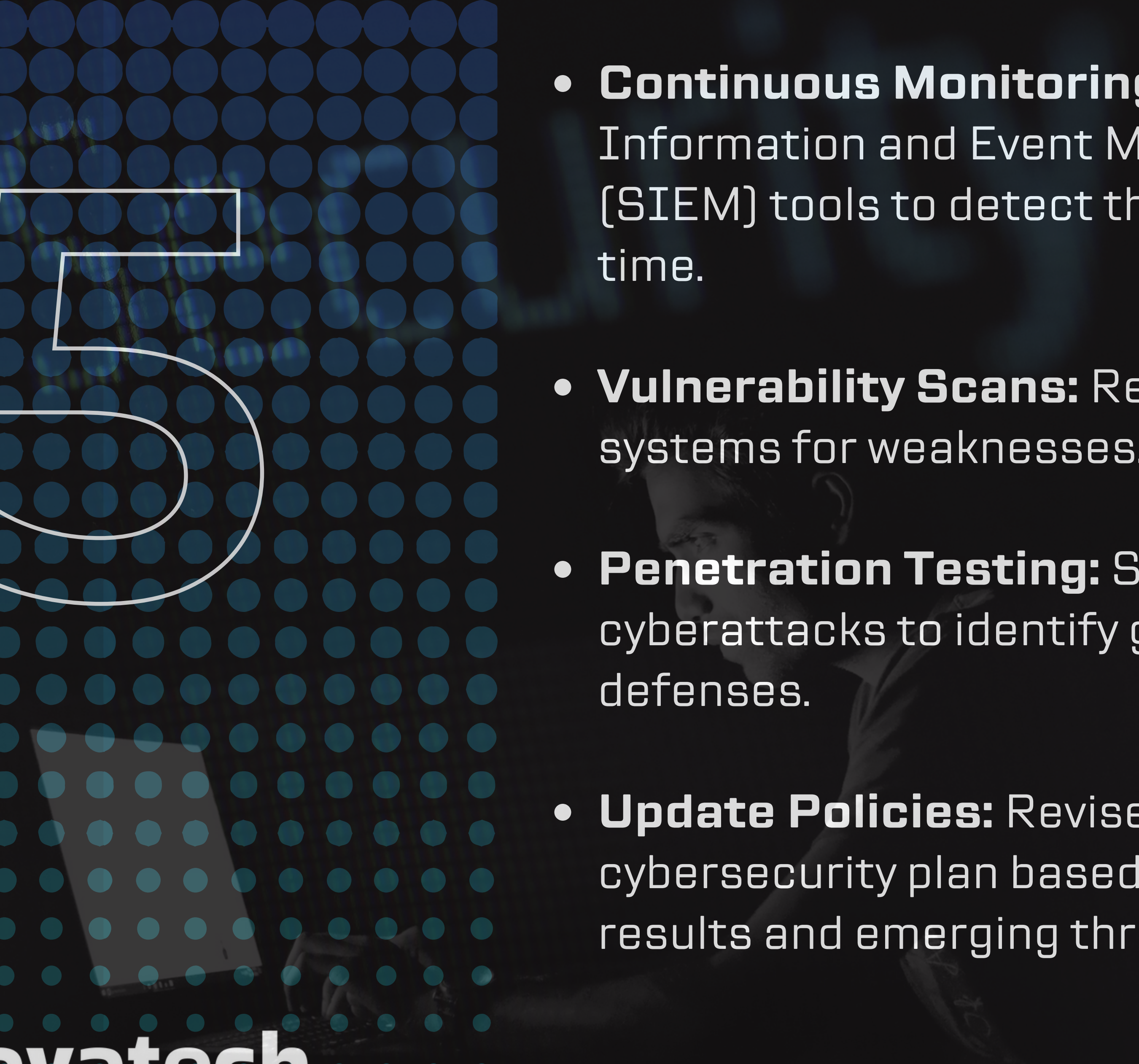
- **Create a Response Team:** Assign roles and responsibilities for handling cyberattacks.
- **Containment and Remediation:** Outline steps to isolate affected systems and remove threats (e.g., malware).
- **Communication Plan:** Define how to notify stakeholders (e.g., customers, regulators) in case of a breach.

Novatech

www.novatech-global.com

Monitor, Test, and Update

5



- **Continuous Monitoring:** Use Security Information and Event Management (SIEM) tools to detect threats in real time.
- **Vulnerability Scans:** Regularly scan systems for weaknesses.
- **Penetration Testing:** Simulate cyberattacks to identify gaps in your defenses.
- **Update Policies:** Revise your cybersecurity plan based on test results and emerging threats.

Novatech

www.novatech-global.com

KEY TAKEAWAYS

- Cyberattacks follow a lifecycle (reconnaissance, weaponization, delivery, exploitation, installation), so **prevention** must address each stage.
- **Employee training** and **technical controls** are equally critical.
- **Regular updates** and **testing** ensure long-term security.

Novatech

www.novatech-global.com