Cyber Attacks Are Evolving—Is Your Security Ready?

1

Identifying Security Gaps

- Have you conducted a full-scale attack simulation on your organization in the last 12 months?
- Are your cyber defense teams prepared to detect and respond to sophisticated threats?
- Do you test for both internal and external vulnerabilities, including insider threats?

2

Evaluating Threat Readiness

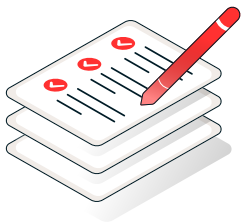
- Do you have real-world attack scenarios tested against your systems?
- Have you simulated social engineering attacks, such as phishing or pretexting?
- Are your incident response teams trained and ready to handle breaches?

3

Assessing AI-Powered Threat Detection

- Have you tested how AI-based security tools perform against adversarial AI techniques?
- Do your AI systems adapt to evolving cyber threats, or are they vulnerable to bypass strategies?
- Have you considered Red Teaming AI models to assess safety, privacy and quality.

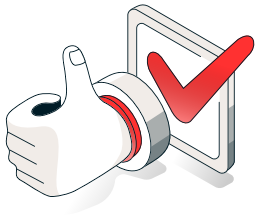
4



Compliance & Risk Mitigation

- Does your security strategy align with industry regulations and compliance standards (e.g., NIST, ISO 27001, GDPR)?
- Have you assessed third-party vendor risks using Red Teaming exercises?
- Do you have a clear post-Red Teaming remediation plan to address weaknesses?

5



Enhancing Organizational Security Culture

- Is your security awareness training effective against evolving attack methods?
- Have you conducted live attack simulations for executives and employees?
- Do you perform continuous Red Teaming rather than one-off assessments?

admin@isadviceandconsulting.com 571-564-1351 www.isadviceandconsulting.com