SecureBlu by new era.

Enhance Your Cybersecurity with SecureBlu's Penetration Testing Services

Identify Vulnerabilities, Strengthen Defenses, and Achieve Compliance with Expert Ethical Hacking

Penetration testing is a form of ethical hacking. It describes the intentional launching of simulated cyberattacks by SecureBlu, using strategies and tools designed to access or exploit computer systems, networks, websites, and applications.

Penetration testing is a proactive probing to find weaknesses before they can be exploited by an attacker.

Companies should perform penetration testing annually or after a significant change to their network, applications, or systems.

Best Practices Cybersecurity Hygiene
Penetration testing is a vital part of best practices cybersecurity hygiene. SecureBlu provides expertise for a wide range of security risk assessments and remediation including vulnerability, incident response, Microsoft 365 security, cloud platform security, and many others.

Ready to Learn More?

Get connected with an expert by visiting neweratech.com/us/security-services/ or neweratech.com/contact-us/

Penetration Testing Benefits:

- **Reduce organizational risk:** Penetration testing will identify vulnerabilities and exploits in customer's information technology assets. Testing analyzes operating systems, applications, and services for means that a malicious attacker may exploit to gain access to your critical systems, and data.
- **Evaluate and ultimately improve security effectiveness:** SecureBlu Cybersecurity Analysts will work with your team to evaluate effectiveness of your defensive controls.
- **Prioritize remediation efforts:** SecureBlu provides a clear roadmap for remediation using real-world results prioritized against business impact.
- **Ensure and improve regulatory compliance:** Penetration Testing helps ensure compliance with regulations such as HIPPA, PCI DSS, DFARS / NIST, GLBA, NYSFS, FTC 16 CFR, and others.