Solution Brief

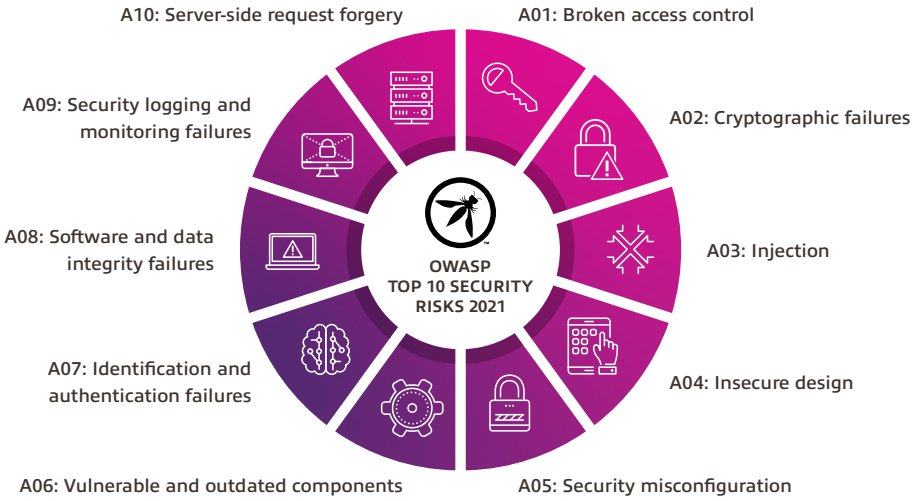
Technical Security Testing Services

Complete lifecycle services to keep your organization stable and secure

Nothing is quite as devastating to a business as a cybersecurity incident. The techniques and tactics of bad actors are evolving quickly, and today's business leaders are fortifying their approach to brace for impending attacks. Continual testing and assessments are helping to eliminate gaps in even the most well-thought-out systems. Performing tests and assessments can identify and remediate vulnerabilities in systems before those vulnerabilities are exploited.

Insight provides a full suite of consulting and professional security services to support you at any point:

- Proactive services to assess current environment for vulnerabilities and security gaps
- Reactive services to address post-incident testing and audit requirements
- Secondary testing to validate remediation
- Testing to validate employee training
- Testing of controls to measure level of adherence



Our Technical Security Testing Services are backed by years of expertise acquired as a trusted services provider — delivered via a globally coordinated team of certified security professionals.

We've built our services to align with regulatory compliance standards spanning PCI DSS, CMMC, HIPAA/HITRUST, GDPR and SOX, and are aligned with OWASP Top 10.

Why Insight

16 years
of incident and threat management experience

14 years
of penetration testing, vulnerability assessment and security management

1,500+
architects, engineers and subject matter experts in security and service delivery

168+
security products and software strategically delivered through Insight

A certified and award-winning partner
of major security solution vendors

Aligned to
industry-accepted and regulation-mandated frameworks

Work with Insight to:

- Identify and eliminate problem areas or weak points in your IT environment before they're exploited.
- Confirm all planned security control measures have been implemented and configured properly.
- Proactively avoid unexpected downtime and maintain business continuity.
- Gain a deeper understanding of what security controls may be needed across your unique IT architecture.
- Benefit from industry best practices and strategic guidance from seasoned security experts.
- Simplify a path to DevSecOps and GRC/regulatory program alignment through implementation, validation, maturation and managed services.

What we offer

External network vulnerability and penetration testing

Discovery of externally available devices, ports/services and vulnerabilities is performed from both manual and automated scanning. The addition of penetration testing allows Insight consultants to engage your infrastructure in a similar fashion as an adversary.

Application security testing

This testing is specifically focused on internally/externally facing web applications. Automated and manual vulnerability and penetration testing are performed on applications to ensure secure coding practices and web server configurations are utilized.

Internal network vulnerability, validation and penetration testing

Discovery of internal devices, ports/services and vulnerabilities is performed from both manual and automated scanning. Vulnerabilities are manually validated to provide evidence of potential results and removal of false positives. The addition of the penetration testing allows Insight consultants to engage client infrastructure in a similar fashion as an adversary.

Office 365 security controls assessment

Assessment is conducted to help plan a risk-driven Office 365® deployment strategy and adhere to industry security best practices. This service identifies gaps across the security architecture to uncover potential cybersecurity risks.

Wireless security testing

Wireless configuration and security review of implemented wireless access points and infrastructure give clients information-based insights to enhance security, drive optimization and maintain visibility across the entire wireless network.

Personnel security testing

Leverages various forms of social engineering testing to pinpoint gaps and training opportunities for employee security awareness. This includes phishing, vishing and smishing. Physical security testing attempts are performed to gain physical access to facilities, devices and data owned by the client.

Critical controls assessment

A thorough review of a prioritized set of actions can protect the organization and data from known cyberattack vectors. Critical controls are a recommended set of actions for cyber defense that provide specific, actionable ways to stop today's most pervasive and dangerous attacks. This assessment focuses on tools and techniques for effective cyber defense.

We also perform assessments against any framework to measure control implementation, to identify and articulate risk, and to measure the maturity of an organization's cyber defense posture.

Network threat assessment

An identification service is conducted to discover potential threat actors within the organization. Analysis of data collected during the engagement focuses on malicious activities performed within the organization, malicious outbound connections and malicious applications.

Insight.

Driving innovation with digital transformation

At Insight, we help clients enable innovation with an approach that spans people, processes and technologies. We believe the best path to digital transformation is integrative, responsive and proactively aligned to industry demands. Our client-focused approach delivers best-fit solutions across a scope of services, including the modern workplace, modern applications, modern infrastructures, the intelligent edge, cybersecurity, and data and AI.

Learn more at:

ca.insight.com/ransomware

Getting started is easy.

Visit ca.insight.com/ransomware to connect with our team.

ca.insight.com