INSIGHTS | SOLUTION BRIEF

Proactive Insights:
WEI Cybersecurity Assessments

CORE SECURITY ASSESSMENTS

- **Network & Web Application Penetration Testing:** Our penetration testing services simulate cyberattacks, identifying security flaws in network configurations, web applications, APIs, and databases. We provide a detailed report with risk assessments, remediation steps, and recommendations.
- **Firewall Assessment:** This assessment reviews configuration settings, access controls, and rule sets to identify misconfigurations and security gaps. We ensure that firewalls are optimized to block unauthorized access.
- **Risk Assessment:** Identify and evaluate potential risks to the organization's information assets. This involves analyzing the likelihood and impact of various threats and vulnerabilities.
- **Cybersecurity Strategy:** Provide CISO-level guidance and strategic security planning to align cybersecurity initiatives with business objectives. This high-value assessment helps organizations take a proactive approach to risk management to help ensure long-term resilience.

INCIDENT PREPAREDNESS & RESPONSE

- **Tabletop Exercises:** Tabletop exercises provide a structured, discussion-based assessment where key stakeholders walk through real-world cyberattack scenarios. This helps organizations evaluate response plans, identify gaps, and improve communication between IT, security, legal, and executive teams.
- **Incident Response Retainers:** An Incident Response Retainer provides on-demand access to cybersecurity experts who assist in containing, investigating, and mitigating attacks. Organizations benefit from predefined response plans, faster recovery times, and expert guidance.
- **Detection Engineering Services:** Security tools must be configured effectively to detect and respond to cyber threats. Our experts review and optimize security monitoring systems, ensuring they detect relevant threats while reducing false positives. Organizations improve their ability to identify and respond to cyber incidents in real time.

The WEI Approach:

Practical, Proactive & Proven

WEI takes a holistic, risk-based approach to cybersecurity, integrating people, processes, and technology to build a defense strategy that addresses every layer of risk. Our methodology ensures proactive, adaptable security measures tailored to your organization's unique challenges.

STRATEGIC SECURITY SERVICES

- Strategy Development & Analysis
- Maturity Assessments

SECURITY COMPETENCIES

- Cyber Security Strategy
- Cloud Security
- SIEM & SOAR Orchestration
- Policy Framework
- Incident Response
- Vulnerability Management

Learn more about WEI Cybersecurity

WEI
CYBERSECURITY

SECURITY OPTIMIZATION & MATURITY

- **Security Gap Assessment & Tool Rationalization:** Our Security Gap Assessment evaluates existing security controls, identifies redundancies, and provides recommendations for optimizing security investments. This assessment also helps organizations align their security strategy with business objectives while eliminating unnecessary expenses.
- **Identity Access Management (IAM) Assessment:** Unauthorized access is a leading cause of data breaches. Our IAM Assessment evaluates authentication controls, role-based access, and privilege management to ensure secure identity governance. Organizations gain insights into access control weaknesses and receive recommendations to enhance identity security.
- **Microsoft Security Assessment:** Many organizations rely on Microsoft environments for business operations, but misconfigurations can leave critical systems exposed. This assessment evaluates security settings, access controls, and compliance measures within Microsoft environments.

FORWARD-THINKING SECURITY STRATEGY

- **Cybersecurity Readiness Assessment:** This assessment provides a high-level evaluation of cybersecurity maturity, policies, and processes. It helps organizations identify vulnerabilities, prioritize security initiatives, and develop a roadmap for strengthening cyber resilience.
- **Zero Trust Assessment:** We evaluates an organization's current security posture, access controls, and authentication mechanisms. We provide a roadmap for implementing Zero Trust principles, ensuring least-privilege access and continuous verification across users, devices, and applications.
- **Red Team Assessment:** A Red Team engagement simulates real-world cyberattacks to test an organization's detection and response capabilities. Unlike standard penetration tests, this exercise takes an adversarial approach, using covert attack techniques to bypass defenses and access critical systems. The goal is to uncover security gaps and evaluate incident response effectiveness.

Talk to WEI Today

Protecting your organization from cyber threats requires a proactive approach and the right expertise.

Led by WEI's cybersecurity experts and partnering with industry leaders, these assessments provide the insights needed to strengthen your defenses, optimize security investments, and ensure compliance. Whether you need to identify vulnerabilities, test your incident response capabilities, or develop a long-term security strategy, our team is here to help.

Contact WEI's cybersecurity experts today to learn more about our assessments and discover how we can support your security goals.