Security & Compliance Solutions

Proactive threat management that integrates defensive tactics and controls with real-world threats and vulnerabilities

emagine it

202.587.5607 | labs@eit2.com | www.eit2.com

Proactive (Attack)

Reactive (Defend)

Threat Emulation: Our Threat Emulation team works with your engineers to ensure that your defenses are properly tuned to match emerging and existing exploits being used by current threat actors.

Red Team: An offensive test for your organizations implemented defenses. This offering mimics an actual attacker attempting to infiltrate your organization to identify vulnerabilities that may lead to a data breach and/or complete system compromise. Multiple attack vectors are examined and will generally cover compliance-based penetration tests, while offering additional value to clients looking to further secure their organization.

Blue Team + Continuous Monitoring: After achieving compliance to a desired framework, our security professionals ensure that evolving security standards are adapted within your product and environment so that you're audit-ready 24/7.

Compliance + Penetration Test: A compliance-driven offering to identify and mitigate vulnerabilities. Performed in coordination with specific frameworks (e.g. PCI, SOC, FedRAMP, CMMC, HITRUST) that your organization is working toward. Offered for both initial compliance and continuous compliance. Can be performed on corporate, public facing, web, and mobile applications, and complemented with social engineering.

Key benefits to your business

+ Identify real-world threats to your business significantly mitigates risk to the enterprise
+ Turns compliance into a competitive advantage

EIT Security Professionals are certified and experienced.

	Threat Emulation	Red Team	Blue Team + ConMon	Compliance + Pen Test
Social Engineering	●	●		
Insider Threat	●			
Network Pen Test	●	●		●
Web App Pen Test	●	●		●
Mobile App Pen Test	●	●		●
Wireless Pen Test	○	○		
Continuous Monitoring	⊙		●	
AV Management	⊙		●	
Firewall Management	⊙		●	
Vulnerability Scanning	●	●	●	●

● Included in service ○ Optional service ⊙ Customer Optimization

FedRAMP | CMMC | HITRUST | SOC1 / SOC2 | NIST 800-171 | GDPR | CCPA | FISC | PCI
ISO 27001 / ISO 20000-1 / ISO 9001 | RMF / FISMA / NIST | CSA STAR | HIPAA / HITECH | ITAR

202.587.5607 | labs@eit2.com | www.eit2.com

Integrated Technical Security Solutions for the Enterprise

Employing The MITRE ATT&CK Framework

MITRE ATT&CK is based on actual threat-based intelligence and offers insights into how an organization's environment would respond to attacks that happen across the globe daily.

We employ the MITRE ATT&CK framework so that we can evaluate all applicable attack paths and assist your organization's security team to mitigate and/or to provide recommendations to identify security gaps.

Customized to fit your business

We work with a diverse group of industries that span healthcare, online merchants, software companies, and federal contractors. That means that every engagement is tailored to your specific security and organizational objectives. Whether its Ransomware, an insider threat, or other Advanced Persistent Threats, our Threat Emulation offering elevates your organizations defenses to ensure that all aspects of an attack have proper defense in depth in accordance with MITRE ATT&CK Framework recommendations.

Network Penetration Testing: Testing externally-facing servers is crucial, but so is looking for weaknesses within your firewall, where insiders (or bad actors with stolen credentials) can wreak havoc. We'll find the issues and help you seal the leaks.

Web Application Penetration Testing: Online applications can help drive greater user satisfaction, but they can also be entry points for attacks. We can ensure your web applications support your business and your customers without exposing your systems and customer data to threats.

Mobile Application Penetration Testing: Mobile applications are increasingly becoming paramount for companies expanding into technology to reach mobile users. This expansion can also serve as an entry point for attackers to gain a foothold within your network. EIT can perform mobile application penetration tests to ensure that your company provides safe and reliable mobile applications to your clients.

Social Engineering: Phishing attacks have become more prevalent and sophisticated, catching organizations of all sizes off guard. Test your employees' ability to identify social engineering threats from attack vectors such as email, telephone calls, and physical threats, such as cameras, USB drives, and "tailgating" into the environment.

Insider Threat: Does your organization know the risks of your own employees to sabotage your reputation, systems, and data? These attacks have increased 47% in the last 2 years alone. Insiders pose a substantial risk to organizations, as they inherently know the landscape and defensive measures of your organization. EIT will evaluate your defensive strategies against commonly used tactics to wreak havoc within your network.

Continuous Monitoring: Can your team adequately monitor ever-evolving security standards to maintain your certifications? We offer a forward-thinking approach and make it our mission to monitor changing compliance requirements that your customers demand so that your product and environment can adapt within your change management process.

Vulnerability Scanning: Do you have a clear understanding of the health and security of your IT assets? We help implement and manage scanners against your environment to alert on known vulnerabilities and provide monitoring so that vulnerabilities are immediately flagged and mitigated

CONTACT EIT to elevate your security posture through threat-based, quantifiable assessments.

Qualys. paloalto NETWORKS VERITONE. USDA

teradata. tenable tyler technologies

Accredited FedRAMP 3PAO, HITRUST CSF Assessor, CMMC Registered Provider Organization (RPO)
CAGE Code: 30NG5 | DUNS:165636205
NAICS:541519,541511,541512,541513,541611, 561410,541990,518210

FedRAMP | CMMC | HITRUST | SOC1 / SOC2 | NIST 800-171 | GDPR CCPA | FISC | PCI | ISO 27001 / ISO 20000-1 / ISO 9001 | RMF / FISMA / NIST | CSA STAR | HIPAA / HITECH | ITAR