EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

OFFENSIVE SECURITY SERVICES

"You saved our banking application from a critical vulnerability in licensed code that our vendor didn't catch when writing it!"

-Lead Developer

"The team was very responsive to keep me informed throughout the process!"

- Senior VP

RESHAPE THE EXPERIENCE

Expedient Technology Solutions' purpose is to reshape the experience for our clients and team members. Our Offensive Services Team strives to attain this goal by providing Vulnerability and Penetration Assessments customized to meet the client's business needs, performed by professional and qualified team members dedicated to enhancing security from a wholistic, risk-based approach.

Why are Offensive Services necessary?

Identify Risk to Assets

These services help clients to identify and better understand risk to their assets through the assessment of current security controls and policies using real-world attack techniques and methodologies. This enables clients to make informed decisions around risk management needs and where investment will be most effective.

Reduce Attack Surface

Regular assessments help clients determine and better understand avenues for attack and how they affect risk to the organization.

Compliance and Insurance

Many regulatory bodies and insurance policies have begun requiring regular penetration assessments, as well as contractual obligations from customers or business affiliations.

Peace of Mind

Offensive services can provide organizations with peace of mind that their security controls are effective in protecting critical data and minimizing the risk of costly incidents

What Offensive services are available through ETS?

Vulnerability Assessments:

We perform discovery on your network and assess any vulnerabilities we find for risk according to your business needs

- **Internal Network**
- **External Network**
- **Ongoing Web Application Pen Tests**

Penetration Assessments:

These are short-term engagements in which our team uses real-world attacks and methodologies to assess and demonstrate actualized risk to the systems and information you have determined are critical to your business. To determine which penetration assessments are right for you, we look at which avenues are available to access the critical assets of your business. It is common to string multiple assessments into one long assessment, using data from the earlier assessments to inform actions and techniques in the later ones.

Internal Network

- Initial access point is standard access to the internal network.
- Commonly assessed through simulated standard employee credentials or physical access to internal network ports/infrastructure.
- Best to assess internal security controls.

External Network

- Initial access point is from the internet.
- Best to assess external-facing security controls that protect exposed infrastructure, servers, or applications.

Wireless Network

- Initial access point is your wireless network infrastructure.
- Often paired with Internal Network assessment.
- Best to assess configuration and security controls on wireless technologies.

Web Application

- Initial access point is the internet anonymously and all authentication levels of the application.
- Best to assess misconfiguration, lack of secure development process, and security controls for web accessible applications.

Social Engineering

- The ETS team will attempt to gain information or passwords through phishing emails and vishing phone calls.
- Information gained from this assessment often leads to further access in other avenues.
- Best to assess security training and policies for employees.

Physical Security

- The ETS team will attempt to gain access to your physical systems and networks utilizing non-destructive methods to breach physical premises.
- Physical access often leads to access via other avenues and often rolls into internal and wireless assessments.
- Best to assess physical security controls and personnel training and policies.

Historical Expertise in Many Verticals

Our team of experts has a rich history of service in the cybersecurity industry across many verticals including Finance, Manufacturing, Healthcare, Technology, Aerospace, Public Service, AEC, Government Compliance, and XaaS. Our experts have honed the knowledge and expertise required to understand how diverse security events impact these verticals, including the unique idiosyncrasies highlighted in each. This expertise enables categorization and prioritization of client data that is most-at-risk, while simultaneously testing the attack vectors that most commonly lead to compromise and offering remediation options unique to the overall needs of each client.

Training and Certification

One of ETS' core values is Continued Growth. A way this is lived out is through our team's consistent training and certification. Our team holds numerous advanced cybersecurity certifications such as Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP), Certified Information Security Manager (CISM), and Certified Ethical Hacker (CEH).

Organization Certification | MSP Alliance Cyber Verify

A rigorous process is embraced in order to achieve the MSP Cyber Verify certification demonstrating our commitment to delivering services to ensure the integrity, safety, and security of client data, networks, and systems. Based upon the Unified Certification Standard (UCS) for Cloud and Managed Service Providers developed by the MSP Alliance, ETS is examined by a third-party public accounting firm to ensure adherence to all control objectives and requirements. This annual review produces a report that is available upon request.

937-535-4300

info@expedienttechnology.com

www.expedienttechnology.com