PRACTICE OVERVIEW

CYBERSECURITY: Technical Security Services

Your organization faces threats associated with newly deployed technologies, personnel changes, increasing malware sophistication, and ever more knowledgeable attackers.

online
business systems

Online's Technical Security Services (TSS) team helps organizations address their technical security requirements and ensure that all layered security controls are designed to be efficient and effective.

Through security testing, we verify your organization's defense-in-depth strategy, including overlapping security controls. We can test your networks, web applications, APIs, mobile devices, and even your people and processes to determine vulnerabilities, weaknesses, and gaps within your security program, and provide you with viable solutions to improve the strength of your security posture.

Online's TSS team offers a suite of security services:

- > Penetration Testing
- > Red Teaming
- > Social Engineering
- > Physical Site Security Assessment
- > Secure Software Development Lifecycle
- > Secure Code Review
- > Dark Web Monitoring
- > Technical Security Assessments

Penetration Testing

Penetration Testing helps detect and analyze vulnerabilities. It's designed to assess how your organization can hold up against an attack and detect where the weak points are in your security controls.

Our Penetration Testing services provide your business with an in-depth technical review of your current security posture by providing a comprehensive analysis of vulnerabilities, their exploitability, associated business risk and most importantly, how to fix them. Organizations often have different Penetration Testing requirements depending on what they are trying to achieve. Some need to assess how an attacker, with little to no information about your environment, may be able to circumvent controls or otherwise gain unauthorized access. Others want to better understand insider threat – an employee or contractor – and how they may use additional information to gain unauthorized access.

Our team has experience across an array of environments including internal and external networks, wireless networks, applications, application programming interfaces (APIs), mobile apps, and cloud environments.

Red Teaming

Online's Red Teaming services are focused on helping clients identify security weaknesses and expose potential attacks scenarios made by skilled hackers and sophisticated criminal organizations. By embodying the attacker viewpoint of a cybercriminal, Red Teaming provides valuable security insights that are often not identified by Penetration Testing efforts alone. A Red Teaming engagement tests the effectiveness of an organization's security technology, and their people and processes by emulating real-world threats and attack vectors, to provide a thorough and realistic understanding of exposed vulnerabilities and risks.

Online's Red Team service focuses on executing a longer-term strategy to identify gaps in an organization's defenses using Open Source Intelligence (OSINT) gathering, along with any number of attack methods including, but not limited to, Penetration Testing, Social Engineering (Phishing/Vishing), and Physical Penetration Testing.

Social Engineering

Social Engineering is the practice of obtaining confidential information or access to assets by manipulating legitimate users. Often executed through social networking, phishing and vishing, Online's Social Engineering service is designed to proactively test the client's security posture, employee adherence to established security policies, and create organizational awareness around tactics malicious actors are actively using on a daily basis to infiltrate your organization.

Social Engineering testing provides an objective metric to determine if employees understand and incorporate internal security policies into their daily routine. It is not designed to target a specific user, but rather targets the corporate culture.

Physical Site Security Assessment

Organizations must have physical security to maintain the safety of information assets. Many network and application controls can be bypassed if physical access to systems or networks can be obtained. A physical security assessment provides a clear understanding of areas that may be vulnerable.

Online's Physical Site Security Assessment can include social engineering attacks to test personnel security training.

Secure Software Development Lifecycle

Online's Secure Software Development Lifecycle (SSDLC) service helps to ensure that software is securely developed on time and on budget by integrating security into the client's software development process.

Our security specialists work with development teams starting with the planning and design phase to review software requirements and constraints to ensure that secure software solutions are built into each of the development stages. Using OWASP's Software Assurance Maturity Model (SAMM), we help identify potential issues with architecture, integration, and user requirements early in the process, so your software is built and implemented securely from the start.

We work with the organization's architects, designers, developers and quality assurance team to ensure that security processes and gates are inserted throughout the process to adequately defend against inevitable malicious attacks.

Secure Code Review

For organizations using software solutions that were developed without using a secure software development lifecycle (SSDLC), or were developed by a third party, a Secure Code Review is the most thorough way to determine if the software has any security vulnerabilities.

Our software security specialists complete an application security architecture review and then analyze the application's source code to search for design flaws, programming flaws, the use of unsafe functions, and the improper use of cryptography. The service utilizes advanced Secure Code Analysis tools to scan the software and identify potential vulnerabilities. Our specialists will review all the possible issues identified and validate those that are a risk to the developed application.

Online will manually review code that is associated with critical security features such as authentication, access control, input validation and event logging to ensure that they are free from vulnerabilities. Once complete, a detailed report is delivered that outlines all the vulnerabilities identified, along with specific guidance on how to modify the software to fix the issues.

Dark Web Monitoring

It's no secret that cybercriminals mine and sell personal and organizational data on the dark web; what is surprising is how it often happens without the organization's knowledge. Dark Web Monitoring provides critical information to help organizations protect themselves against evolving threats that target the exploitation of stolen credentials and highly confidential business data on the dark web.

Online's Dark Web Monitoring is an ongoing service identifying risks to your organization that lurk in the dark web. Our security analysts search through the depths of the dark web to identify information that is related to your organization, notifying you of their findngs, and providing you with as much information as possible about threat actors and motives.

Technical Security Assessments

Technical Security Assessments quickly identify potential gaps in an organization's security controls that may be exploited by attackers. Many compliance regulations and security standards mandate that a Technical Security Assessment be conducted to meet specific certification and remediation requirements.

These Assessments require resources with specialized training and experience that is not easy to obtain. Online's team of highly trained, certified, and experienced consultants helps organizations execute on their Technical Security Assessment requirements and provides a detailed findings report with remediation and maturity recommendations.

Why Online Business Systems

Our Risk, Security and Privacy team takes a collaborative approach to security by working closely with our clients to gain a strong understanding of their business model, critical data flows and repositories, network architecture, and systems/applications that support their business.

> *We help organizations execute on their technical security assessment requirements with a team of highly trained, certified, and experienced consultants.*

> *We help enterprise customers enhance their competitive advantage by designing improved business processes enabled with robust and secure information systems*

Contact:
Online Business Systems
1.800.668.7722
rsp@obsglobal.com

About Online Business Systems

Online is a leading Digital Transformation and Cybersecurity consultancy.
Businesses today are under pressure to transform to remain relevant – at the same time, there is unprecedented opportunity to innovate and achieve incredible things never seen before – securely. We combine the best technology, business, and security practices, and lead Clients through the transformation process.