SERVICE DESCRIPTION

Cybersecurity Testing

Gigit's Cybersecurity Testing services are a portfolio of gigit delivered services designed to uncover cybersecurity risks within the Client's business environment.

Service Summary

The purpose of this testing is to identify the organization's vulnerabilities and weak spots from a 'hackers 'point of view. Gigit Security Testing service simulates threat behavior by utilizing standard and non-standard techniques that intruders may users to attempt to gain access, deface or bring down Client's IT services or information. The Client may combine these services with gigit's Compliance assessment services to provide a complete cybersecurity assessment and testing solution.

The following services and tests are available for purchase:

- Vulnerability Assessment
- Penetration Testing
- Wireless Penetration Testing
- Social Engineering Assessment

Gigit Responsibilities

- Develop a detailed Statement of Work with the Client that at a minimum specifies:
  - Scope of the work
  - Target testing locations and the associated IT Infrastructure
  - Delivery schedules
  - Service delivery price
  - Change management terms
  - Any client specific terms or conditions
- Deliver the Statement of Work specified services on time and within the agreed upon price.
- Assign a single point of contact for the project to manage gigit delivery resources, report project progress from start to finish, and act as the gigit representative for resolution of any client or questions.

AVAILABILITY

Gigit Services are available in the United States. If Client requests service outside of the United States, they may Contact gigit for a review of gigit's other delivery location options.

PRICING AND ORDERING

Gigit customizes service delivery pricing based upon the client's business needs and requirements. A Statement of Work provides the detailed pricing. The Client may purchase a single gigit service, bundle multiple services, or purchase a subscription agreement for a period of no less than 1 year. The subscription provides for recommended recurring service delivery throughout the life of the subscription.

FOR MORE INFORMATION

info@gigitsecurity.com

Client Responsibilities

- Sign a gigit Master Service Agreement
- Sign a gigit Security Services Statement of Work
- Provide written approval for access to project specific IT systems and personnel.
- Identify an individual within the Client team to act as a single point of contact to coordinate and work with the gigit service delivery team.

Methodology Overview

Gigit's Testing Service consists of six major phases, during which gigit's consultants use a range of tools and techniques, designed to highlight vulnerabilities and identify areas for further investigation. All of gigit's testing is preapproved by the Client.

Gigit's testing adheres to the following standards:

- ISO 27001
- LPT
- OSCP
- OWASP Top 10
- EC-Council
- SANS Top 25,
- PENTEST-STANDARD.ORG
- UK "Council of Registered Ethical Security Testers" (CREST)

NOTE: Gigit strongly recommends Clients experiencing frequent changes in their IT infrastructure, applications, and staff embed gigit testing in their change management policies and practice.

A vulnerability assessment performed 2-4 times per year is best practice.

Reconnaissance and Enumeration (Phase 1)

Gigit begins using foot-printing, a non-intrusive activity performed in order to get the maximum possible information about the Client's organization and their systems. Gigit's security consultant compiles and analyzes this information for further areas of investigation.

Mapping and Scanning identification (Phase 2)

Gigit sweeps the Client's environment. This sweep identifies network and system resources available within the environment. Following the initial service identification, gigit attempts to identify the application protocol that is in use, the vendor and version of the software supporting the application(s).

Vulnerability and Exposure Analysis (Phase 3)

The gigit consultant reviews each port, service and application identified for vulnerabilities. This assessment identifies known vulnerabilities in application code, as well as configuration and deployment vulnerabilities that the client may have introduced into their environment.

Service Exploitation (Phase 4)

Gigit attempts to exploit vulnerabilities and misconfigurations identified in Phase 3. In all instances, gigit discusses the options for exploitation with the client prior to the commencement of the test.

Pivoting (Phase 5)

Gigit consultant pivots through each exploited device and service and start enumerating other parts of the Client environment that might not be directly accessible. The aim of this phase is to gain access to as many devices as possible and identify as many security exposures as possible across the Client's IT environment.

Reporting (Phase 6)

Gigit's final report to the Client lists all assessed vulnerabilities, exposures, and points of exploitation. This risk report quantifies how and why the threats may impact the client's business. The report includes remediation advice and guidance for improving the Client's IT infrastructure, applications, and as appropriate social engineering elements.

Cybersecurity Testing Service Options

Vulnerability Assessment

The gigit vulnerability assessment attempts to find holes in the Client's security systems and practices. The assessment asks the question, "where can an intruder gain unauthorized access to IT infrastructure, databases, and applications". Gigit check network and Web Application Components. The checks include the search for known and unknown vulnerabilities including missing patch levels, out of date operating systems, out of date software revisions, open and exposed ports.

The assessment checks:

- Checks Network equipment (Servers, Routers etc.)
- Checks Web Applications (Websites, Portals etc.)

Penetration Testing

Gigit's Penetration Test evaluates computer and network security by simulating an attack on a computer system or network from external and internal threats. Gigit emulates the same tools, know-how and methodologies used by malicious hackers. The difference between a real attack and gigit testing, gigit teams with the client. The output produced is a comprehensive report that identifies where to close down security holes.

NOTE: To clarify a Vulnerability Assessment is part of a Penetration Test. It checks and advises on vulnerabilities.

It provides:

1. Reconnaissance and Enumeration,
2. Mapping and Scanning,
3. Vulnerability and Exposure Analysis

Penetration Testing Attempts a complete hack and then reports on vulnerabilities found through the hacking simulations.

Gigit Penetration Testing Areas

Internet of Things (IoT)

GigIT will analyze the security of the Client's IoT and supervisory control and data acquisition (SCADA) infrastructure. Due to the diversity and increase in the number of IoT devices in the market, gigit will customize the testing program with the Client and their teams.

Web Application

Gigit examines the Client's web applications for coding and implementation flaws. Gigit looks at issues like SQL injection and cross-site-scripting.

Mobile Application

Gigit strives to uncover flaws in traffic flows, coding vulnerabilities and other potential weaknesses. Gigit may test productivity, navigation, and gaming apps.

DoS and DDoS

Gigit performs extreme-scale load and performance testing on the Client's website or SOA services. Gigit may conduct a simulated distributed denial-of-service (DDoS) or cyber warfare testing.

Cloud Security

Gigit consultants validate whether your cloud deployment is secure. Gigit conducts pro-active, real-world security tests using the same techniques employed by attackers seeking to breach your AWS, Azure, and other like cloud-based systems and applications.

Wireless Penetration Testing

Gigit's Wireless Security evaluates the Client's Wi-Fi and Bluetooth security networks by simulating attacks against authentication, encryption or the "man-in-the-middle" attacks.

Gigit Wireless Testing Areas

Wireless Authentication & Encryption Attack

Gigit attempts to break into Wireless Access Points (AP) by performing "Ethical Hacking" against common security methods such as MAC authentication, WEP, WPA and WPA-2. The goal of this assessment is to break into a wireless network in order to gain access to the network.

Wireless Man-in-the Middle Attack

Gigit implements rogue and fake access points, waiting for users to connect in order to capture all activities they perform. Gigit employs Social Engineering techniques,

such as redirecting users to a fake webpage forcing them to re-enter the pre-shared key. Gigit may redirect users to capture online activities such as phone calls.

Wireless DDoS Attack

Gigit attempts to bring the Client wireless network to a complete hold by either jamming the wireless spectrum or overloading the Access Points.

Bluetooth Attack

Gigit evaluates every security aspect of Bluetooth Networking in order to gain control over blue-tooth devices, intercept calls (i.e. BT handset to BT earpiece) or temporarily disable Bluetooth functions.

Social Engineering Assessment

During gigit's Social Engineering Audit, gigit tests electronically (computer based) and phone based. The testing gathers open source information prior to the engagement through online information gathering. The testing impersonates sources of authority and use a variety of techniques such as:

- Spear Phishing in conjunction with the simulated exploitation of the endpoint
- Phone based social engineering including Caller ID and SMS spoofing along with Vishing exercises (Voice Phishing)
- Social engineering tasks by randomly distributing special USB devices with simulated malware
- Continuous e-learning user cybersecurity protection education

All services come with comprehensive reporting, user tracking and event classification.

Need more information? CONTACT US

www.gigitsecurity.com
4770 Baseline Rd., Suite 200
Boulder, CO 80303

Phone: +1-844-374-4448, +1-844-37GIGIT