Cybersecurity Services

blue-star-cyber.com

Table of Contents

Overview

The Cyber team at Blue Star Software is managed and staffed by former Department of Defense (DoD) security experts who draw on years of experience in all facets of information security. This experience includes comprehensive penetration tests of extremely complex enterprise networks, source code analysis of critical applications, reverse engineering, vulnerability assessment, and exploit development against sophisticated, nation-state level malware. The Cyber team combines this experience with cutting edge security assessment tools to eliminate false positives/negatives and provide comprehensive, reliable results.

The Cyber team at Blue Star stays abreast of the latest security breaches to truly understand modern adversarial intrusion techniques. We go above and beyond by delivering concise and relevant reports so our clients can make swift, educated decisions. We use industry standard best practices, including the OWASP framework, DISA STIGs, NIST Special Publications, ISO/IEC 27000 series, and NSA's IA Security Configuration Guidance documents.

It can be a tedious process finding an information security service provider that meets industry requirements in terms of certifications and credentials. In addition to real-world hands-on experience, the Cyber team at Blue Star is highly credentialed by the information security industry's most trusted sources, including: $(ISC)^2$; the International Council of Electronic Commerce Consultants (EC-Council); Offensive Security; and, the SANS Institute.

Penetration Testing

Penetration Testing is the ultimate way to determine if a client's systems are vulnerable. In a penetration test, the Cyber team will assume the role of adversary intent on gaining access to the client's network. There are several different models and formats of Penetration Tests that Blue Star offers:

Models:

Black Box:

This type of penetration test most resembles a real-life cyber attack. In this type of penetration test, Blue Star's Cyber team has no prior knowledge of the network architecture, applications, or security infrastructure of the target. The Cyber team will follow hacker methodology starting with open source information gathering and reconnaissance, deliver a successful attack, pivot within the network, perform privilege escalation, and attempt to maintain access within the network.

White Box:

A white box penetration test is one in which the Cyber team has prior knowledge of the target. This prior knowledge often includes the logical diagrams of the networks, infrastructure layouts, and currently active credentials. This type of test is focused on the internals of the enterprise, and less focused on network border defenses. By skipping some portions of the hacker methodology, the Cyber team is able to focus its efforts on the security posture of the client's internal network.

Formats:

External:

This type of penetration test is performed remotely (off-premises) and is designed to resemble an attack from the internet. The Cyber team performs a comprehensive test against all public facing internet assets to include email servers, VPNs, web servers, firewalls, etc.

Internal:

This type of penetration test is performed from the client site and is designed to resemble an insider threat. Insider threats include employees with malicious intent, adversaries who have breached the physical perimeter, and cyber adversaries who have penetrated the digital perimeter.

Blue Star penetration tests are comprised of model/format pairings depending on the needs of the client. For example, in an internal white box penetration test, Blue Star security experts would be on-site for the duration of the test and be given prior knowledge of the target. Blue Star's penetration testing service can also be used to test a client's incident response procedure.

Web Application Security Testing

Web applications often serve as the public face of most companies. Services such as online shopping, banking, email, and streaming entertainment are provided instantaneously from any internet connected device. The availability and convenience provided by web applications provide a large target for adversaries.

Blue Star offers two services in our Web Application Security Testing area:

Static Web Application Source Code Analysis:

The Cyber team performs a comprehensive review of a web application's source code looking for vulnerabilities that may be exploitable by potential adversaries. This service allows the Cyber team to provide a snapshot in time of the web application's current security state.

Web Application Penetration Testing:

The Cyber team imitates a cyber adversary seeking to infiltrate a web application. A combination of red team experience and state of the art penetration testing knowledge will be used to discover exploitable vulnerabilities.

These two services can be conducted separately but are usually requested as part of a combined package. The Cyber team uses the Open Web Application Security Project (OWASP), an industry recognized web application security framework, as a baseline to inform the testing. Special attention is given to SQL-injection or command-injection vulnerabilities that may compromise back end databases, as well as vulnerabilities that lead to escalation of privileges, information leakage, or unauthorized access to critical IT resources.

Wireless Network Assessment

Many organizations are eager to offer wireless access as a form of convenience to their customers and employees. Everyone from a potential customer who connects to the guest network in the lobby, to a long-time employee utilizing the company's new Bring Your Own Device program, are expecting a seamless wireless experience. However, where does the wireless signal end? Is it possible for a passerby on the street to pick up this signal? Is it possible for a hacker to broadcast a stronger wireless signal and trick all devices in the organization into connecting to their system? With Blue Star's wireless network assessment, our clients will finally know the answer.

Blue Star security experts will perform a comprehensive review of all wireless network diagrams to ensure no vulnerabilities exist in the network configuration. Once completed, identification and penetration testing of all wireless access points will be conducted. Blue Star will use the same tools that malicious actors use in order to determine the security state of a wireless network, but we don't stop there. If the Cyber team gains access to the wireless network, we will attempt to pivot inside the network to determine potential data leakage opportunities from the vulnerable wireless network.

Network Security Assessment

Organizations tend to relax security controls once a user has been authenticated and is inside the internal network with an understanding that "if you've reached this point, you must be trusted." Because of this approach, many vulnerabilities are often found on the internal network. Device settings that a network administrator would not allow if accessible from the internet, such as unrestricted access to a share drive, are common on internal networks.

Blue Star's network security assessment differs from a penetration test in that it's designed to be conducted on-site, with administrator level credentials, with access to internal IT resources, diagrams, and configuration files. The Cyber team will review the entire enterprise network from the inside. Processes such as patch management and data backup will be scrutinized heavily. Ports and services accessible from within the network such as FTP, DNS, WWW, and SMTP will be reviewed. The Cyber team will also review firewalls, encryption, and authentication methodologies. Furthermore, if any vulnerabilities are discovered during the network security assessment, the Cyber team will review the viability and severity by attempting to exploit them. The Cyber team will leave no endpoint un-scanned, no firewall un-probed, and no patch un-implemented.

Source Code Analysis

It is important to conduct an in-depth review of an application's source code because most vulnerabilities are introduced during software development and have the potential to go undiscovered for a long period of time. The Cyber team's source code analysis service goes beyond the use of automated tools, as these tend to result in high levels of false positives/negatives. Instead, we combine these tools with our years of experience in reverse engineering and source code audits to provide the most accurate results possible. Some items of particular scrutiny include input validation, authentication mechanisms, API use, and memory management.

As enterprise software often contains millions of lines of code, the Cyber team begins its source code analysis by reviewing the logical flow and understanding the functionality from a high level. This allows the team to focus on suspected vulnerable areas of code. Depending on the size of the application, a comprehensive source code analysis can take up to several months to complete.

Exploit Development

Blue Star security experts have many years of experience developing exploits against previously disclosed (n-day) vulnerabilities. On occasion, Blue Star's Cyber team is called upon to assist in developing exploits against certain applications, architectures, or environments. This is a specialty service requiring an extremely high level of skill and time, and therefore is considered on a case-by-case basis.

Reverse Engineering

The Cyber team is proficient in the use of many industry standard debuggers/disassemblers/decompilers and other tools required for successful reverse engineering. On occasion, Blue Star's Cyber team is called upon to reverse engineer certain applications, architectures, or environments. This is a specialty service requiring an extremely high level of skill and time, and therefore is considered on a case-by-case basis.