Security Assessment Guidebook

www.soteria.io | 843.501.0313

soteria

INTRODUCTION

Security assessments are valuable tools for determining the strengths and weaknesses of your organization's security. This guidebook is designed to provide an overview of the common types of security assessments and services, their intended goals, deliverables, as well as points to consider before pursuing any of them. By understanding the similarities among and differences between these common types of security assessments, you will be better able to select the services that best meet your organization's needs.

TABLE OF CONTENTS

KEY SECURITY AREAS

These five security assessments collectively address many factors that impact a business's comprehensive security posture. Key security areas that should be assessed are:

Commercial products and applications
The pieces of software your business develops and provides to customers

Internal networks
The components of your network that are only accessible from within your firm's private network

External networks
The components of your network that are accessible from the Internet

Employee training practices Define how your business educates your employees about common security risks

Corporate security policies
Define how your business will establish and maintain security in your firm

Physical security
Measures taken to ensure your physical office, facilities, and assets cannot be accessed by those unauthorized

Identity and Access Management
Processes and procedures in place to ensure proper authentication, authorization, and accounting

Application Hardening
Secure custom applications by protecting APIs, developing resilient application/ business logic, and using consistent secure coding practices

Security Program Procedures
Best practices for secure processes such as change management, logging, and monitoring programs

VULNERABILITY SCAN

WHAT IS A VULNERABILITY SCAN?

Vulnerability scans provide an assessment of your business's external and/or internal assets or web applications to determine if there are flaws in design or configuration that negatively affect their security.

AREAS OF FOCUS

- Commercial products and applications
- External networks
- Internal networks

OUTCOMES

Vulnerability scans provide a technical report that either confirms or denies the presence of vulnerabilities that the scanner is able to identify.

APPROPRIATE APPLICATION OF ASSESSMENT

Vulnerability scans provide value to businesses that have never completed a scan of their network or web applications and seek quick feedback on the state of their security. Businesses that are actively developing or changing the configurations of their networks or the designs of their web apps should consider running vulnerability scans before launching major changes or updates to their networks, software platforms, or web apps. If development is outsourced to a third-party, running a vulnerability scan is a good way to quickly check if the product was developed with security in mind. Running frequent vulnerability scans is considered good practice to ensure you have a clear picture into any exposure of your environment.

POINT OF CONSIDERATION BEFORE PURCHASE

Vulnerability scanners are tools that are only able to identify the vulnerabilities for which they have been programmed to detect. Before purchasing, do your homework on the type and number of vulnerabilities they are designed to identify. Inquire about the frequency with which the scanner tool is updated by the developer. Hackers are constantly adjusting their methods of attack and consequently finding new ways to exploit networks, software platforms, and web apps. For this reason, new vulnerabilities are always being discovered. It makes sense to ensure the vulnerability scanner you choose is searching for the latest known vulnerabilities.

The vulnerability scan reports are technical in nature, so it will be important that your business have access to a technical consultant who is qualified to interpret the report and understand how to make appropriate changes to your network or applications to improve security and lessen or remove the vulnerabilities identified. Additionally, having the technical expertise to prioritize mitigating vulnerabilities and understanding where your company's time and money would be best spent is critical to extracting the maximum value out of your vulnerability scan results.

VULNERABILITY ASSESSMENT

WHAT IS A VULNERABILITY ASSESSMENT?

Vulnerability assessments are vulnerability scans combined with a detailed analysis of the results with recommendations on how to fix the vulnerabilities and suggested priorities for addressing them

AREAS OF FOCUS

- Commercial products and applications
- External networks
- Internal networks

OUTCOMES

Vulnerability assessments include a report outlining the results of the vulnerability scan, the order in which the results should be addressed, and the recommended action that should be taken to address each identified.

APPROPRIATE APPLICATION OF ASSESSMENT

Similar to vulnerability scans, vulnerability assessments should be conducted routinely. They provide value to businesses that have never completed a vulnerability scan or are actively undergoing major changes to their network or applications. Businesses that do not have easy access to a security expert on staff to interpret the scan results should consider a vulnerability assessment service to receive expert interpretation and analysis as well as guidance on how to implement findings. Vulnerability assessments by a third-party provider are often required or highly recommended by numerous compliance standards to ensure existing practices are in line with their security requirements. If you are subject to specific compliance standards, determine if a vulnerability assessment may be a required or recommended component.

POINT OF CONSIDERATION BEFORE PURCHASE

Because vulnerability assessments are highly service based, it is important to choose a qualified security partner you trust to provide honest and accurate feedback and recommendations. Understanding what vulnerability scanning tools your security consultant will use to identify the vulnerabilities is also a critical question that should be asked before choosing a consultant. As mentioned in the “vulnerability scan” section of this guidebook, the results of your vulnerability assessment will be strongly tied to the vulnerabilities detected by the scanning tool used. Request a sample report to review and understand what kind of report you would be receiving.

GAP ASSESSMENT

WHAT IS A GAP ASSESSMENT?

Gap assessments often start with an overview of the existing security related hardware and software, security policies and procedures, and employee workflows implemented by a firm. Once this security profile has been established, a consultant will provide recommendations for improving your security posture in accordance with industry best practices or compliance and regulatory requirements along with a roadmap to tailor your firm's timeline for making the improvements.

AREAS OF FOCUS

- Commercial products and applications
- Internal networks
- External networks
- Corporate security policies
- Employee training practices
- Physical office security
- Security program procedures

OUTCOMES

A detailed report providing an overview of your current security posture, a list of suggestions that your business should set to further strengthen your security posture, and recommended steps that can be taken for how to achieve these goals and properly prioritize them.

APPROPRIATE APPLICATION OF ASSESSMENT

Gap assessments are ideal for a wide range of businesses with varying levels of established security programs. These assessments provide businesses with valuable expert guidance on appropriate policies, training, asset and physical security measures that they should implement. Similar to vulnerability assessments, gap assessments conducted by a third-party are often required or highly suggested by compliance standards to ensure existing practices are in line with security requirements. Determine if a gap assessment may be a required or recommended component for meeting compliance.

POINT OF CONSIDERATION BEFORE PURCHASE

Before choosing a gap assessment provider, your business should ensure the provider will be mindful of and understands your business's existing operations and budget to implement the recommendations. Before purchasing a gap assessment, make sure your business is aware of security laws or compliance standards to which your business is subject. A gap assessment should be conducted with your requirements and regulatory mandates (if necessary) and ensure that the recommendations are tailored to your specific security requirements and goals.

PENETRATION TEST

WHAT IS A PENETRATION TEST?

Penetration tests expand on the work completed during the vulnerability assessment and provides additional insights into how the vulnerabilities identified in your network could be exploited. The tests provide a granular level of understanding on the amount and type of information a hacker could feasibly extract from your business as a result of exploiting the existing vulnerabilities in your network. Receive insight on the true level of risk your Internet-facing assets pose to your business, your vendors, and your customers.

AREAS OF FOCUS

- Commercial products and applications
- External networks
- Internal networks
- Physical office security
- Identity and Access Management

OUTCOMES

Detailed report outlining the vulnerabilities identified in your system, how hackers could feasibly exploit them, the specific information or assets hackers could gain access to as a result of a successful exploitation of these vulnerabilities, and how to remediate them.

APPROPRIATE APPLICATION OF ASSESSMENT

Penetration tests are best suited for businesses with sophisticated networks and/or are responsible for protecting sensitive data or large amounts of corporate assets. Often, penetration tests are required to meet regulations or compliance standards, many industry standards also support conducting a penetration test at least annually. These assessments are recommended for businesses that place a strong emphasis on security and want to measure their efforts to an attack by professional hackers.

POINT OF CONSIDERATION BEFORE PURCHASE

When you authorize a penetration test to be conducted on either your internal or external network, you are authorizing security professionals to attempt to hack into your business. Make sure you choose a provider you trust to conduct this work professionally and considerately. You do not want the penetration test to impact your business operations. Additionally, penetration tests are a highly sophisticated form of network security assessment. They are generally not recommended for businesses that have yet to conduct vulnerability assessments or gap assessments at their firm.

Web Application Penetration Test

WHAT IS A WEB APPLICATION PENETRATION TEST?

A web application penetration test is a specialized exercise in which the security of a single website or application is deeply assessed. This test can uncover previously unknown application security flaws and provide you with a detailed snapshot of the security posture of your web products and services. If applications or websites are an integral part of your mission, a web application penetration test is one step toward understanding how hackers might attack them and how to reduce the risks applications pose to your organization and your customers.

AREAS OF FOCUS

- Application hardening
- Commercial products and applications

OUTCOMES

A report outlining what vulnerabilities were identified in your application and explaining how attackers could feasibly exploit them, what specific impact attackers could have as a result of successfully exploiting these vulnerabilities, and how to remediate them.

APPROPRIATE APPLICATION OF ASSESSMENT

Web application penetration tests are intended for organizations who present custom web applications and services to their customers, employees, or to the internet. In some cases these tests may be required to meet compliance regulations. Web application tests provide the most value to those who have already completed a vulnerability assessment of their application or have mature application security practices. This type of test is a logical next step and utilizes experienced ethical hackers in a controlled examination of your application to uncover the type of vulnerabilities a skilled, motivated attacker might exploit. Web application penetration test should be conducted at least annually as applications frequently change with updates and new versions.

POINT OF CONSIDERATION BEFORE PURCHASE

When you permit security professionals to conduct a web application penetration test, you are permitting them to attempt to hack into that application. Be sure to choose a trustworthy security services provider who can conduct this work without negatively impacting your organization's mission. Additionally, web application penetration tests are sophisticated exercises which provide the most benefit for organizations who already engage in vulnerability assessments or have some level of application security controls.

Mobile Application Penetration Test

WHAT IS A MOBILE APPLICATION PENETRATION TEST?

Similar to a web application penetration test, a mobile application penetration test is an extended assessment of the security posture of a specific mobile application. This type of test can uncover hidden risks in the design and configuration of your apps. Many organizations use custom-made mobile applications as a key product offering for branding, or as an internal productivity tool. Mobile application penetration tests demonstrate how real attackers can use your application as a springboard to attack your mission, and how to stop them.

AREAS OF FOCUS

- Application hardening
- Commercial products and applications

OUTCOMES

A report outlining what vulnerabilities were identified in your application and explaining how attackers could feasibly exploit them, what specific impact attackers could have as a result of successfully exploiting these vulnerabilities, and how to remediate them.

APPROPRIATE APPLICATION OF ASSESSMENT

Mobile application penetration tests are best utilized by organizations who create or use custom mobile applications for the Android or iOS platforms. This type of test is part of the application security lifecycle and utilizes experienced ethical hackers in a controlled examination of your app to uncover the type of vulnerabilities a skilled, motivated attacker might exploit. Similarly to web application tests, scheduled testing is recommended as the application changes with updates and new versions.

POINT OF CONSIDERATION BEFORE PURCHASE

A thorough mobile application test encompasses both the application itself along with the supporting web services and infrastructure which the application interacts with. When you permit security professionals to conduct a mobile application penetration test, you are permitting them to hack into these design components. Be sure to choose a trustworthy security services provider who can conduct this work without negatively impacting your organization's mission.

Secure Source Code Review

WHAT IS A SECURE SOURCE CODE REVIEW?

A secure source code review is an examination of your application source code for prevalent application security issues and unsafe practices. In a code review, security experts will utilize both automated tools and manual review methods to discover what classes of security issues exist and present a clear picture of areas where the source code could be hardened against attack. Code reviews by trusted parties are an efficient and valuable means of discovering issues in applications.

AREAS OF FOCUS

- Application hardening
- Commercial products and applications

OUTCOMES

A report outlining the vulnerabilities or insecure coding practices discovered, how hackers could feasibly exploit them, what the impact of a successful attack could mean, and how to remediate the discovered issues and establish secure coding practices.

APPROPRIATE APPLICATION OF ASSESSMENT

Code reviews are primarily intended for organizations who rely on custom-built websites and applications as an everyday part of their operations. They may sometimes be required to fulfill regulatory requirements. Code reviews result in a clear overarching picture of whether an application was designed with security in mind because they provide complete transparency into the workings of an application. They are often utilized to augment security efforts at key junctures in the application's lifecycle, such as in advance of a major release or after code has been inherited through an acquisition or merger.

POINT OF CONSIDERATION BEFORE PURCHASE

Since your organization's code is part of your mission, a secure code review requires a trusted security partner. Consider also that while a code review provides security benefits on its own, it can be combined with an application penetration test to achieve maximum effect. Finally, while organizations can use some automated tools to perform code reviews, it should be noted that these tools often need to be configured by a security professional to match a particular application or source code type.

Social Engineering Simulation

WHAT IS A SOCIAL ENGINEERING SIMULATION?

In many cyber attacks, hackers gain access to your organization's proprietary data by sending employees a crafted email that entices them to visit a malicious site, download spyware, or provide credentials to the attacker. The most effective way to assess your organization's preparedness for attacks like these is to conduct a simulation in which ethical hackers send realistic phishing emails to a targeted group of employees and monitor which employees fall victim to the social engineering attack.

AREAS OF FOCUS

- Employee training practices

OUTCOMES

A report outlining which employees opened the phishing email, visited the phishing URL, or provided their credentials upon receiving the phishing email. The report provides suggestions for remediation or training and gives a general sense of how well your employees and organization would withstand a targeted phishing attack.

APPROPRIATE APPLICATION OF ASSESSMENT

Social engineering simulations are most effective when they are followed shortly by phishing awareness training. They can also be applied multiple times after the initial simulation to gauge the effectiveness of awareness training or remediation actions. Other variations of social engineering simulations are additionally available including vishing, smishing, and in person social engineering for a physical penetration test. Employees should be regularly tested to keep them vigilant to these types of attacks.

POINT OF CONSIDERATION BEFORE PURCHASE

A social engineering simulation conducted by a trusted security partner is an excellent initial assessment of an organization's phishing resistance and offers the organization more hands-on guidance from security experts. For repeated phishing simulations over a long period of time, mature organizations that have in-house IT and security experts may find it more beneficial to use a reputable phishing-as-a-service software that partially or fully automates the process of conducting a phishing simulation.

Cloud Configuration Review

WHAT IS A CLOUD CONFIGURATION REVIEW?

A cloud configuration review examines the settings, policies, permissions, and setup of the cloud computing resources a firm is using. A detailed analysis is produced that provides recommendations on configuration changes based on security best practices.

AREAS OF FOCUS

- Identity and access management
- Security program practices

OUTCOMES

A report detailing recommended configuration changes, and security best practices a firm should follow to secure its cloud infrastructure and assets. The guidance is specific to the products, tools, and settings provided by the individual cloud provider.

APPROPRIATE APPLICATION OF ASSESSMENT

Cloud configuration reviews are helpful to any company, business, or state entity that has moved their assets or infrastructure to a cloud based solution, or if they are already actively using cloud based services. It is also beneficial to any firm that has made changes to their current cloud setup and need to confirm they are still secure.

POINT OF CONSIDERATION BEFORE PURCHASE

It is important to have knowledgeable staff to manage a cloud solution and configuration changes that should be reviewed before implementation. The selection of a trusted security partner is critical because each individual cloud solution has several services, areas to input settings, and specific configuration decisions that need to be made. The recommendations provided should be detailed and specific enough to secure your cloud setup and follow the security best practices that will yield the best results.

Navigating security can seem like a complicated process. The right security partner can make the difference in your firm eliminating compliance headaches, avoiding penalties, and unlocking new business potential.

Contact Soteria to learn how we can assist your business in creating a strategic plan for establishing and growing your security program.

soteria

Tailored Cyber Security Solutions

soteria.io
843.501.0313
contact@soteria.io