APPLICATION ASSESSMENT

Well-informed organizations understand that their applications are more than just an information service; they also represent the corporate image to their customers and the public. If an application has to be disabled due to a security breach, this can result in the loss of information, reputation, trust, and revenue. Ensuring your applications can deter most threats means that you can continue serving your customers and not spend time and money reacting to a data loss or availability issue.

HITACHI SYSTEMS SECURITY'S APPLICATION ASSESSMENTS ARE DESIGNED TO

- **Identify vulnerabilities and the potential impact at the infrastructure, application, and operational levels**
- **Provide you with an accurate view of your security posture Provide recommendations on how to reduce risk to acceptable business levels**
- **Determine the level of real world business risk for your auditors, executive, security staff, and infrastructure professionals**
- **Ensure that you are compliant with requirements, regulations and standards**

WHAT IS AN APPLICATION ASSESSMENT?

A Hitachi Systems Security Application Assessment assists organizations in fully understanding the vulnerabilities in their applications, whether it's a public website serving customers, a third-party supplier interface into corporate CRM, or even stand-alone applications.

Through a **Web Application Vulnerability Assessment** or **Application Penetration Testing**, you will understand your corporate security posture as well as provide you with actionable recommendations on how to perform remediation of the vulnerabilities discovered in your environment, including potential required patches, code changes, access adjustments, etc.

SERVICE ELEMENTS

In conducting a complete Application Assessment, Hitachi Systems Security Inc. will:

- **Scope the Project** – Understand the business intent of the application(s), understand the potential threats, and define the testing approach and the environment to be assessed.
- **Perform Intelligence Gathering** – Determine what is known about the application(s) or company that can be used during testing.
- **Map the Application(s)** – Understand the application content and structure, naming conventions, application size, and type of technology used.
- **Analyze the Application(s) and Determine Vulnerabilities** –Understand security control points, user session management, data entry points, and error messages.
- **Test the Technical Vulnerabilities** – Test the application controls, authentication mechanisms, access controls, infrastructure weaknesses and application weaknesses.
- **Report Preparation –** Include identified vulnerabilities, prioritized according to their relative impact to your business with recommendations for remediation.

DELIVERABLES

Upon completion of an Application Assessment, you will be provided with a **detailed Application Assessment Report**, including:

- An executive summary indicating items that require immediate attention, with a focus on business impact or risk, rather than a detailed technical explanation of exact flaws
- A technical review section describing the activities performed to determine vulnerabilities
- A detailed list of vulnerabilities discovered, listed in order of criticality
- Recommendations to optimize protection of the assets identified by the vulnerability assessments, with consideration to the resulting costs in capital investment operation and maintenance, personnel, and time
- Appendices capturing tool outputs, screenshots, or other data that helps to give greater context or clarification to the vulnerabilities detected
- A tactical summary outlining possible next steps, including temporary workaround and/or long-term solutions that may need to be integrated into larger projects or investigated

OUTCOMES

✓ Fully understand your applications' security posture

✓ Identify the flaws, vulnerabilities and risks that your applications are subject to, based on their level of severity and their potential likelihood of occurrence

✓ Implement remediation activities to protect your applications

✓ Train your staff on how to remediate vulnerabilities to reduce overall risk