Managed Security Testing

Penetration Testing

A penetration test is a more in depth method of evaluating the security of a computer system, application or network by simulating an attack by a malicious user. SecuriCentrix Penetration Testing service provides an in-depth technical coverage of our client's systems by using proven methodologies to identify all technical weaknesses and vulnerabilities.

SecuriCentrix offers two types of Penetration Testing:

- Internal Penetration Testing
- External Penetration Testing

Benefits of a Penetration Test:

- Manage vulnerabilities intelligently
- Avoid the cost of network downtime
- Meet regulatory fines and avoid fines
- Preserve corporate image and customer loyalty
- Justify security investments
- Satisfy prerequisites for cyber security insurance

For further information please contact us at (antti.hyvarinen@adnet.fi)

Web Application and Application Testing

Our application security assessment offerings are designed to help organisations identify flaws in their custom and 3rd party applications that resist detection from traditional assessment techniques.

Our Application Security Assessments are highly customizable to meet our client's requirements and the scopes vary largely based on how much access to the target application and supporting environment is provided and targeted for analysis.

Our application security assessment services have the ability to analyze software security controls from logical process and procedures, to architecture and design flaws, to code level vulnerabilities that can compromise the integrity of the environment as a whole.

For further information please contact us at (antti.hyvarinen@adnet.fi).

Vulnerability Management

Vulnerabilities appear every day in applications, websites and within devices on the network. A vulnerability assessment is the process of identifying, quantifying and prioritizing the vulnerabilities in a given system.

A comprehensive vulnerability management program provides value not only in terms of identifying and addressing any potential vulnerability in a network but can also be leveraged to validate a number of information security practices.

SecuriCentrix offer two types of vulnerability scanning:

External Vulnerability Scanning – designed to detect and alert clients of security flaws at the network perimeter and provide guidance to address these exploits

Internal Vulnerability Scanning – is designed to verify systems on the internal network; are built, managed and maintained securely.

For further information please contact us at (antti.hyvarinen@adnet.fi)

PCI DSS

To protect and reduce the ever increasing amount of cardholder data breaches, the major credit card companies have collectively created the PCI DSS. The PCI standard specifies how merchants, service providers and financial institutions must secure systems and data to ensure confidential cardholder information is not compromised.

Any entity that stores, processes, and/or transmits payment card data, including online retailers (ecommerce) as well as brick-and-mortar businesses must be in compliance with the PCI Data Security Standard (PCI DSS).

SecuriCentrix is certified by the Payment Card Industry Security Standards Council (PCI SSC) to conduct assessments. We will assign a dedicated QSA (Qualified Security Assessor) to work with your team in a 'consultant' capacity to identify areas of non-compliance.

SecuriCentrix provide assistance in implementing controls and technologies required for PCI compliance or recommend solutions that can turn a project-driven approach into an internal process aligned with other compliance initiatives.

We have formulated a 4 step process that provides the overall framework for delivering Payment Card Industry Data Services. For further information please contact us at (antti.hyvarinen@adnet.fi).

PA DSS

The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

The Payment Application Data Security Standards have become an integral part of information security for organisations involved in payments. Software vendors have a requirement to become compliant with this mandated standard; with their aim to be a secure and compliant business application partner to organisations involved in card payment transactions.

Our consultative approach guides our clients through the intent of each requirement of the standard. For further information please contact us at (antti.hyvarinen@adnet.fi).

P2PE Fundamentals

A point to point encryption (P2PE) solution is provided by a third party solution provider to help reduce a merchants PCI DSS scope. It is a combination of secure devices, applications and processes that encrypt data from the point of interaction until the data reaches the solution providers secure decryption environment.

Our consultative approach provides guidance on the standard and identifies areas of compliance and non compliance in the form of an initial gap analysis. For further information please contact us at (antti.hyvarinen@adnet.fi)).

ISO 27001 implementation and analysis

ISO27001 is the stepping stone for information security management based on internationally recognized standards.

Many organisations are actively seeking to improve information security practices and establish formal programs for enterprise security. For some, the goal is to improve overall compliance with regulations and internal security requirements, while others seek to prove effective security and privacy practices to third-party partners, vendors and customers.

ISO 27001 defines a risk based approach to determining, evaluating, treating, and managing information and asset security risks. For further information please contact us at (antti.hyvarinen@adnet.fi).