Threat and Vulnerability Assessments

Uncovering threats, reducing your risk

How vulnerable is your organization to malicious hackers and criminals? How secure are your systems, your applications and hardware, your people? The only way you can know for sure is by testing for every possible vulnerability. TELUS Security Solutions offers a comprehensive range of assessments to help you identify weaknesses, the first step in strengthening your defenses.

Vulnerability Assessments

TELUS Vulnerability Assessments provide a comprehensive examination of a specific system, service or IT structure. You will receive an evaluation of any weaknesses or vulnerabilities that can expose your organization's systems and information to malicious exploit. You will also be provided with recommendations for remediation. Assessments are available for:

- IT infrastructure and associated services
- Web, desktop and mobile applications
- End-point communication protocols and service

Penetration Testing

TELUS Penetration Testing or offensive security is a pro-active attempt to exploit a target environment, its users and data in order to evaluate all the components of its infrastructure, systems, services and applications. It delivers a multi-stage evaluation of your organization's security practices by attempting to exploit your environment, occupy it and create a presence in the same way a malicious attacker would do. It includes:

- Passive & active reconnaissance
- IP discovery
- Threat modelling
- Vulnerability analysis and exploitation
- Device jail-breaking & mobile penetration testing
- Wireless access point scanning and exploitation

Social Engineering

TELUS Social Engineering is the social and psychological manipulation of individuals in order to gain proprietary information. It combines physical and digital methods to gain confidential information and/or access. In this way, TELUS will assess your key personnel and identify any potential weaknesses. It may include:

- Digital social engineering, including phishing campaigns
- Fraud replication
- Physical engineering with pre-texting, baiting, and tailgating

Secure Code Analysis

TELUS Secure Code Analysis is a critical and effective technique for identifying security flaws in an application's underlying source code and configuration files. Also known as static code analysis, it provides insight into the "real risk" associated with insecure code in any of your Web, desktop and mobile applications/services. It includes:

- Analysis of source code and configuration files
- Review against platform secure-coding practices

Security Requirements Review

An extension of Secure Code Analysis, a TELUS Security Requirements Review analyzes the requirements of an application and its related systems. This allows us to define additional security features and options required to meet the business needs of the system, while simultaneously validating the existing security rules against best practices and their implementation. Performed by a security specialist, the review focuses on practical security measures that best meet the needs of the application, its user-base, and security requirements. It includes:

- Requirement review from a security audit perspective
- Platform specific, channel direction, application scoped
- Integration as part of your business lifecycle

Stolen Laptop Assessment

The TELUS Stolen Laptop Assessment will detail all risks associated with the potential theft of an employee laptop, one of the largest sources of data breaches. It will help you identify the true cost of a theft, including data lost to criminals, over and above the pure monetary value of the stolen device. This assessment includes:

- Authentication bypass review, including encryption
- User and password review
- Review of remote connections available
- Examination against security hardening guidelines

Discover how TELUS can enable your business.

Contact your TELUS Account Executive, call **1-877-710-0404**
or visit **telus.com/businesssecurity**.

TELUS