Trellix

DATA SHEET

Internal Security Assessment

From the Inside Out: Uncover Hidden Risks, Strengthen Your Core

Benefits

This comprehensive assessment enables organizations to fine-tune their security measures, ensuring sensitive data remains protected against both external and internal threats.

The process fosters a culture of continuous improvement in cybersecurity practices, making it an invaluable tool in any organization's security arsenal.

Gives you a comprehensive list of all security vulnerabilities.

Provides an "Anatomy of an Attack" to show exactly how root or Active Directory access can be gained.

Our Trellix Guardians performing penetration testing for our clients, is a proactive and critical measure for safeguarding an organization's IT infrastructure. This simulated cyber attack against one's network identifies vulnerabilities from an insider's perspective or someone who has breached the perimeter defenses.

The primary benefit is the early detection of security weaknesses that could be exploited by malicious insiders or hackers who have bypassed external safeguards.

By uncovering these vulnerabilities, organizations can prioritize and remediate them before they are exploited, significantly reducing the risk of data breaches, financial loss, and reputational damage. Moreover, internal penetration testing helps in compliance with various regulatory requirements, ensuring that security controls are effective and up to date, i.e. PCI DSS, HIPPA, GDPR, FFIEC, SOX, ISO/IEC 27001.

Guardians methodology typically follows several phases: planning (defining scope and goals), reconnaissance (gathering information about the target system), vulnerability assessment (identifying potential points of entry), exploitation (attempting to breach the system), post-exploitation (determining the value of the compromised system), and reporting (providing detailed findings and recommendations for remediation).

Guardians Methodology

A typical internal security assessment consists of the following phases:

- Host Discovery
- Service Enumeration
- Operating System Identification
- Vulnerability Scanning
- Vulnerability Testing
- Manual Verification
- Manual Penetration Testing

If root or Domain Admin access is achieved a detailed "Anatomy of an Attack" is provided, including step-by-step compromise with screen shots.

Discounted Retesting

Our Guardians consultant's partner with your organization in attaining its strategic security goals. At the conclusion of this engagement, we list all discovered vulnerabilities upon a ranking of high, medium, and low. At a discounted rate, we perform a retest of each of the
discovered vulnerabilities within three months of the completion of your engagement. This allows you to validated that your security remediation efforts resolved all discovered vulnerabilities.

For more information or to schedule a consultation, please contact us at Guardians@Trellix.com