Penetration Testing vs. LRS' Cyber-Risk Analysis

Understand the value of these important security assessments.

	PENETRATION TESTING	CYBER RISK ANALYSIS
PURPOSE	Identifies security vulnerabilities in a network, machine, or piece of software. Can be expanded to include human weaknesses, physical security controls or other targets.	Identifies errors, omissions, misconfigurations and vulnerabilities that are commonly exploited by bad actors to perpetrate cyber-attacks.
SCOPE	Dependent upon customer needs. Can incorporate all services at boundary layer, specific applications, social engineering, physical security, or other mutually agreed upon services.	Constrained to boundary firewalls, Active Directory configuration (including object-level reviews), and vulnerability analysis for all public-facing and internal IP-connected devices.
EXECUTION	Performed by one or more security experts who hold industry recognized certifications in penetration testing. Follows the Penetration Testing Execution Standard (PTES). Predominantly done remotely but may require on-site access depending upon requirements. Portions may require customer involvement.	Consists of a battery of proprietary health checks, performed by multiple security experts who hold industry recognized certifications in penetration testing and/or information security. Performed remotely, with little participation required from the customer.
BENEFITS	Identifies weaknesses in a broad range of security control mechanisms – including the human. Social engineering is often the simplest way to compromise an environment.	Identifies weaknesses that are most commonly exploited by bad actors and penetration testers, alike. Allows customers to prepare for a penetration test or reduce the amount of damage that a malicious entity could cause if security boundaries were compromised.
FREQUENCY	Generally, annual penetration tests are recommended. This cadence is required for compliance with several cyber security regulations and frameworks.	Semi-annual seems to provide a good timeframe for resolution of findings. It also allows for a clear measure of improved security controls from one assessment to the next. No commitment is required, however.
USE CASES	Compliance. Validation of security controls. Determining efficacy of training/education.	▪ Preparation for penetration testing. ▪ Establishing security baseline. ▪ Demonstrating improved security. ▪ Justification for additional security controls or programs.
VALUE	Provides technical insight into how current security controls may be compromised, or where gaps exist. May cover a broad range of technologies, infrastructure or people groups.	Can be used to establish KPIs and KRIs for tracking fundamental security health - providing alerts for commonly overlooked security risks. Educates customers on how to improve functional security.
DELIVERABLES	Reporting on vulnerabilities identified, exploits launched, and details regarding how the testers were able to dwell within the environment, move laterally and exfiltrate data.	Corrective Action Plan that provides prescriptive measures for addressing identified security weaknesses. These detailed plans can be performed by the customer, LRS or third party – there is no obligation for remediation.

LRS®
SECURITY SOLUTIONS

CALL US TODAY TO FIND OUT MORE.

2401 West Monroe Street, Springfield, IL | 217-793-3800
www.LRSsecuritysolutions.com | security@LRS.com

©2022 Levi, Ray & Shoup, Inc. All rights reserved. LRS is a registered trademark of Levi, Ray & Shoup, Inc.
LRS with the chevron logo is a trademark of Levi, Ray & Shoup, Inc.