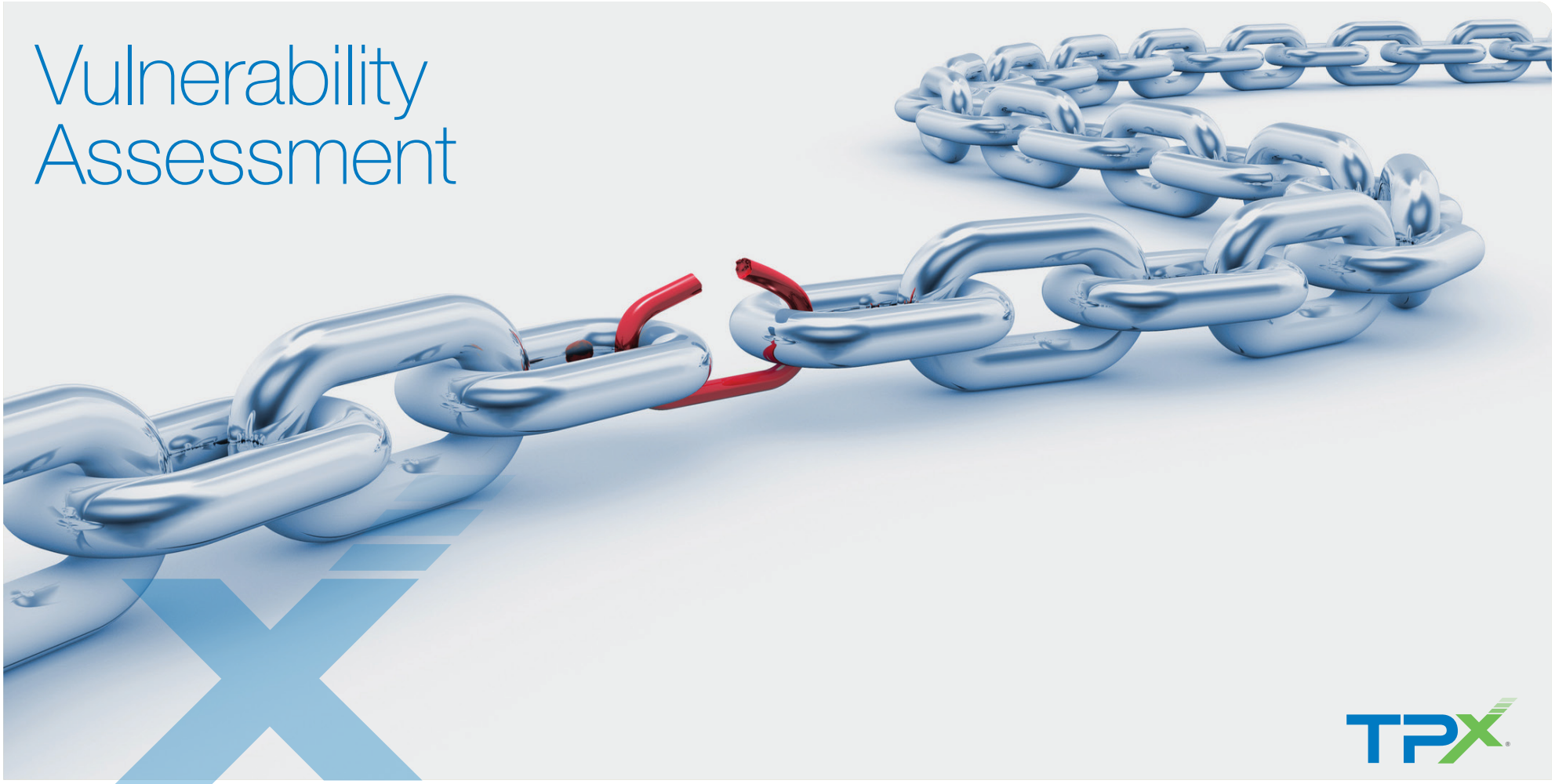
Vulnerability Assessment



TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our depth of expertise enables us to offer standards-based security consulting services developed from our experiences in solving strategic and operational challenges for customers.

TPx consultants are subject matter experts in their field and thought leaders in security. All of our offerings are based on best practices derived from Information Security Standards (CISSP Domains, NIST, ISO 27000 series, etc.) and our extensive experience deploying, architecting, operating, and securing environments nationwide.

Proactively maintaining and protecting a computing network requires continuous effort. Vendors are continually releasing patches and updates, access and permissions requirements are always evolving, and most importantly, the threat landscape is continuously expanding and becoming more dangerous.

Cybercriminals have turned malware and hacking into a robust, money-driven industry complete with commercial-grade exploit kits widely available to those who seek them. A haphazard approach to identifying and mitigating vulnerabilities in your network cannot hope to keep up. TPx can give you the information you need to ensure your vulnerability program is methodical, thorough, and continuous.

Get answers to these questions…

- What vulnerabilities currently exist in my network? How do I know which ones pose the greatest threat?
- How do I best prioritize my patching and updating activities?
- Am I susceptible to attack from employees and others inside my organization?
- Based on my network infrastructure, are there threats that I do not need to worry about?
- How do I stay current on the threat landscape and defend my organization against emerging threats?

57% of data breaches are attributed to poor patch management. The average time to apply, test, and fully deploy a patch is 102 days.

Ponemon Institute

Overview

TPx's Vulnerability Assessment methodology is founded on industry standards such as ISO 27001, CIS "Top Twenty" (Control 3) and current best practices. It is designed to evaluate your organization's posture and capabilities as they pertain to securing the attack surface. The approach for the assessment is to evaluate your organization's current exposure to threats through a vulnerability scan, and also your ability to limit future exposure through an effective vulnerability management program. The assessment will be divided into two components:

- **Vulnerability Scan** TPx will perform an active scan of the defined platforms within your environment. The resulting output will be a summary of identified vulnerabilities, their risk to your environment, and recommended actions to remediate or reduce the risk for identified vulnerabilities.
- **Program Review** TPx will assess the quality of your Vulnerability Management program as it relates to industry best practices and risk to your organization. Patching processes and policies, the use of threat intelligence sources, license management, and technical security measures implemented within your network infrastructure will be evaluated.

Vulnerability Assessment Activities

TPx will perform a vulnerability scan of your network to provide a prioritized list of risks to your organization. TPx will provide a report with business priorities based on the exposure of the organization and the operational risk to business sustainability. We will also review your organization through interviews, policy review, validation and investigation of processes to generate an assessment of your VM program. TPx will detail the results of each best practice assessed, the validation method and risk level to the business. The aspects of your current program that will be evaluated are:

Automated Vulnerability Scanning Tools Evaluates for SCAP compliance, completeness of output reports, prioritization of findings, and subsequent actions

Scheduled Process for Performing Scans & Patches Vendors typically release patches and updates according to a specific schedule (e.g. Patch Tuesday); organizations should align with those schedules

Compare Back-to-Back Vulnerability Scans Tracking of mitigation efforts, as well as establishing and track KPIs such as Mean Time to Remediate, which are essential for evaluating the performance of the VM program

Accounts with Elevated Privileges Prevents unintended access to protected systems and enforces policy of least privilege

Automated Software Patch Management Tools In addition to automated tools, processes must exist to track down and remediate platforms that are missed (especially workstations and other wireless devices). With work-from- home becoming increasingly common and in many cases the norm, new policies and procedures need to be implemented to address the issues this raises.

Risk-Rating Process Prioritizes identified vulnerabilities using CVSS or other scoring method enables highest-risk vulnerabilities to be mitigated first. This must take into account the threat level and the cost to your organization if exploited.

Risk Acceptance Process Standardizes the method for accepting risk where patches cannot be applied

License Administration Tracks EOL/EOS dates for relevant vendors to enable advanced notice of end-of-support dates. Helps prioritize tech refresh activities

Reporting

The results of the Assessment will speak to two different levels of resources: the leadership and the security practitioner. TPx will deliver the results of the vulnerability scan, annotated to highlight the most important findings and recommend how to mitigate those vulnerabilities. An additional Best Practices report presents the VM program assessment results and observations related to your organization's current level of exposure.

TPx will also generate an executive-level document containing a summary of the engagement's activities & findings. From TPx's insights, you will be able to build or enhance a VM program based on controls with the greatest impact to your risk posture, and ensure that you utilize your limited resources most effectively.