Whitepaper
Vulnerability Management

TFORM™

Discover.
Optimize.
Transform.

Despite the goal of simplifying infrastructure through the use of modern technology, the effort to secure the enterprise has become more complex. A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Vulnerability assessments are designed to uncover security gaps within computing systems and networks.

1. Understanding Enterprise Vulnerability Assessment
2. Network-based scans.
3. Host-based scans.
4. Wireless scans.
5. Database scans.
6. Application scans

What is a vulnerability assessment?

A vulnerability assessment is the process of defining, identifying, classifying, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures. Vulnerability assessments also provide an organization with the necessary knowledge, awareness, and risk backgrounds to understand and react to threats to its environment.

A vulnerability assessment process is intended to identify threats and the risks they pose. They typically involve the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report. Organizations of any size, or even individuals who face an increased risk of cyber attacks, can benefit from some form of vulnerability assessment, but large enterprises and other types of organizations that are subject to ongoing attacks will benefit most from vulnerability analysis. Because security vulnerabilities can enable hackers to access IT systems and applications, it is essential for enterprises to identify and remediate weaknesses before they can be exploited. A comprehensive vulnerability assessment, along with a management program, can help companies improve the security of their systems.

Importance of vulnerability assessments

A vulnerability assessment provides an organization with details on any security weaknesses in its environment. It also provides direction on how to assess the risks associated with those weaknesses. This process offers the organization a better understanding of its assets, security flaws and overall risk, reducing the likelihood that a cybercriminal will breach its systems and catch the business off guard.

Types of vulnerability assessments

Vulnerability assessments discover different types of system or network vulnerabilities. This means the assessment process includes using a variety of tools, scanners, and methodologies to identify vulnerabilities, threats, and risks.

Some of the different types of vulnerability assessment scans include the following:

- Network-based scans are used to identify possible network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks.
- Host-based scans are used to locate and identify vulnerabilities in servers, workstations, or other network hosts. This type of scan usually examines ports and services that may also be visible to network-based scans. However, it offers greater visibility into the configuration settings and patch history of scanned systems, even legacy systems.
- Wireless network scans of an organization's Wi-Fi networks usually focus on points of attack in the wireless network infrastructure. In addition to identifying rogue access points, a wireless network scan can also validate that a company's network is securely configured.
- Application scans test websites to detect known software vulnerabilities and incorrect configurations in network or web applications.
- Database scans can identify weak points in a database to prevent malicious attacks, such as SQL injection attacks.

Vulnerability assessments vs. penetration tests

A vulnerability assessment often includes a penetration testing component to identify vulnerabilities in an organization's personnel, procedures, or processes. These vulnerabilities might not normally be detectable with network or system scans. The process is sometimes referred to as vulnerability assessment/penetration testing, or VAPT.

TFORM Vulnerability and Threat Monitoring

Security and compliance have never been more important to the organization. TFORM offers a vulnerability management suite that utilizes a comprehensive and up to date vulnerability database. This database is consistently updated with the latest vulnerabilities identified in the NIST National Vulnerabilities Database (NVD). TFORM shows you the severity of each threat in a way that allows you to act, and it prioritizes the vulnerabilities requiring immediate remedial solutions. TFORM shows you the severity of each threat in a way that allows you to act, and it prioritizes the vulnerabilities requiring immediate remedial solutions.

TFORM scanning delivers results that allow our clients to remain compliant in even the most complex environments. Our algorithm is based on the NVD Common Vulnerability Scoring System (CVSS) and the Common Weakness Enumeration (CWE). Our algorithm uses these industry leading conventions to prioritize risks and to provide our customers with a remediation path in order to address vulnerability in a timely and effective manner.

We created TFORM to deliver real-time insights into the technical estate through deep data collection and versatile tools for reporting and dashboards. Unlike most industry leading tools, TFORM not only collects detailed information about technical assets, but it also possesses intelligence to offer actionable optimization.

TFORM integrates with common CMDB and ITSM systems to provide important data related to system capacities, device quantities and compliance against a library of known vulnerabilities. In addition to that real-time integration, TFORM can ingest data from common CMDB and ITSM systems for comparison to the monitored assets and to identify drift from known quantities and configurations