tenable®

Top 5 Reasons to Evolve to Risk-Based Vulnerability Management

Legacy vulnerability management solutions weren't designed to handle the modern attack surface and the growing number of threats that come with it. They're also limited to a theoretical view of the risk a vulnerability could potentially introduce – causing security teams to waste the majority of their time chasing after the wrong issues while missing many of the most critical vulnerabilities that pose the greatest risk to the business.

In contrast, taking a risk-based approach to vulnerability management enables security teams to focus on the vulnerabilities and assets that matter most while deprioritizing the vulnerabilities that are unlikely to ever be exploited.

1. Make full-context decisions.

Correlate and analyze dozens of essential vulnerability characteristics along with other key contextual elements, including the criticality of the asset(s) affected, threat and exploit intelligence and an assessment of current and likely future attacker activity – so you can understand the true risk posed by each vulnerability.

2. Focus on what matters most.

Understand all vulnerabilities in the context of business risk, so you can use that data to prioritize your remediation efforts. This empowers you to move beyond the inherent problems of using CVSS in isolation. Instead, you can address true business risk instead of wasting valuable time on vulnerabilities that have a low likelihood of being exploited. As a result, you can maximize your team's efficiency by proactively reducing the greatest amount of risk with the least amount of effort.

3. Eliminate blind spots.

Assess modern assets as well as traditional on-premises IT environments to eliminate the blind spots that plague legacy tools. This enables you to gain visibility into your entire attack surface, so you can determine which vulnerabilities to prioritize for remediation based on risk – regardless of where they reside in your network.

4.Be purposeful and strategic.

Continuously discover and assess the risk associated with all business-critical assets across your attack surface and employ analytics that dynamically assess changes in vulnerability, threat and asset criticality data. Limiting assessments to assets that fall within audit scope can cause critical systems to be ignored. And, static, point-in-time analyses often lead to late and incomplete remediations – or meaningless work that doesn't reduce risk.

5. Minimize disruptive events.

Leverage machine learning models to automatically and continuously combine vulnerability data with threat and exploit intelligence as well as asset criticality to accurately measure risk. These insights empower you to adjust your remediation strategy in near real time. Proactively address the vulnerabilities that pose the most risk to the organization while minimizing disruptions from new vulnerabilities and zero-day exploits that gain media attention.

Taking a risk-based approach enables you to maximize the efficiency and effectiveness of your remediation efforts, so you can make the best use of your limited security resources.

Learn more about **Risk-Based Vulnerability Management**.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies.

Learn more at **www.tenable.com**.