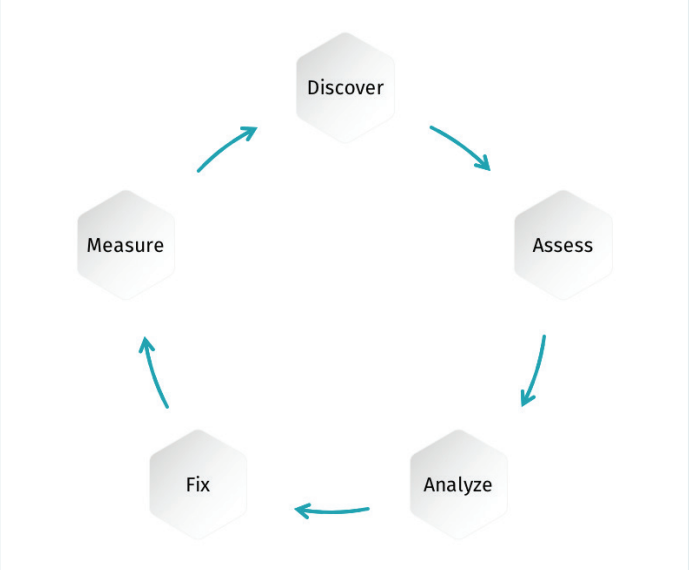
SOLUTION BRIEF

tenable

Vulnerability Management: Assess

Vulnerability management is an essential part of any organization's security program, and it is foundational to Cyber Exposure, an emerging discipline for managing and measuring cybersecurity risk in the digital era. A mature vulnerability management (VM) program includes all five steps in the Cyber Exposure Lifecycle shown below.



Cyber Exposure Lifecycle

This Solution Brief focuses on Assess, the second step of vulnerability management.

The Assess objective is for you to understand the cyber exposure of all assets, including their vulnerabilities, misconfigurations and other security health indicators.

Key Benefits

- **Assess your complete attack surface** so you can understand risk and adequately protect your organization.
- **Audit patching and configuration changes** to ensure that vulnerabilities and misconfigurations were remediated as expected.
- **Inform incident management** with vulnerability and misconfiguration information to help prioritize investigation.

Challenges

Assessing all assets is challenging for two primary reasons:

- Diverse asset types including traditional IT, transitory, mobile, dynamic and operational technology assets often require different assessment technologies. Active assessment scans are best suited to traditional IT assets. However, cloud, web apps, containers and operational technology (OT) require additional assessment methods. For example, you should use passive monitoring to assess OT assets, such as PLCs and RTUs. This will reduce the risk of active scanning disrupting their operation.
- Ensuring data veracity. Nothing undermines Security's credibility in the eyes of asset owners/administrators like inaccurate assessment data. One bad number and they may disregard all of your work. You need careful preparation to assess with the optimal breadth, depth and frequency. You need the right technologies to assess your full breadth of assets without double counting assets and/or vulnerabilities. You need current credentials for deep, authenticated assessments, and you need to run the right tests during the assessment. Finally, you need to provide timely information.

Solution

Building a mature Assess capability that identifies your organization's entire attack surface progresses through four levels, and Tenable can help you with each one.

LEVEL 1. ASSESS ON-PREMISES TRADITIONAL ASSETS

You should select the discovered hosts you want to assess and use the Nessus Basic Network Scan template to perform an internal vulnerability scan that is suitable for any host. Level 1 assessments assume that Nessus does not have the credentials required for authenticated scans. Therefore, Nessus will automatically skip the local security checks, which are included in the Basic Network Scan but require credentials.

LEVEL 2. INCREASE ASSESSMENT BREADTH, DEPTH AND FREQUENCY

You must expand assessment breadth to include all modern assets in order to measure to manage your complete attack surface. Tenable provides assessment capability optimized for laptops, mobile, virtual infrastructure, cloud, web apps, containers and operational technology. You may need to adopt a new mind-set, build new relationships with application development and find innovative ways to implement security while enabling fast-moving DevOps processes. One way is to integrate assessment into software build workflows in the development stage rather than waiting until software assets are deployed into production.

You increase depth by using authenticated scanning and agents. Authenticated scans, also called credentialed scans, use credentials to remotely login to devices and examine them from the inside out. Because authenticated scans interrogate devices from the inside out they can gather a wealth of security-related information about installed software and vulnerabilities. Agent-based scanning, performed by software installed on the target devices, sees devices from the inside-out and can provide detailed information similar to authenticated scanning. Agents solve two common problems for transitory assets. First, they remove the blind spot of not assessing assets which are disconnected from the network during scans. Second, they only report a given asset (and its vulnerabilities) once, even if its IP address changes with each reconnection.

You should include malware detection in your assessments, and authenticated scans can search file systems for known malware. Additionally, they can detect the presence, update status and operation of many anti-virus products.

You should increase assessment frequency from ad hoc to a regularly scheduled interval. The interval should be at least as frequent as your patching cycle, if not weekly.

LEVEL 3. ASSESS CONFIGURATIONS AND OPTIMIZE ASSESSMENT BY ASSET CLASS

Configuration assessment reduces an asset's attack surface by disabling unneeded services, such as FTP and RDP, enforcing strong authentication and generally hardening the asset. You can assess your servers, desktops, laptops, web services, databases, cloud infrastructure, network devices and more using standards from The Center for Internet Security, the Defense Information Systems Agency and from many vendors. Note: when you first assess your assets against one of these standards, you are likely to discover many more configuration issues than expected. Therefore, you may need to tailor the standards to initially reduce the requirements and then increase them gradually.

You will define assessment parameters based on the SLA for each asset class. Asset class SLAs fine-tune assessment depth, breadth and frequency to secure your attack surface based on the expected loss magnitude of your different business services. You will assess assets classified as "high" more thoroughly than other asset classes.

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 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 25 percent of the Global 2000 and large government agencies. Learn more at **www.tenable.com**.

LEVEL 4. CONTINUOUSLY ASSESS ASSETS AND INTEGRATE WITH PRIVILEGED ACCESS MANAGEMENT

At this level, you add near real-time assessment of new assets and periodic review of assessment SLAs. You can also integrate with Privileged Access Management systems, if applicable.

Real-time assessment evaluates newly discovered assets immediately. Passive monitoring continuously identifies many new vulnerabilities, and it can automatically trigger an active scan to more thoroughly assess the newly discovered asset. If the new asset included an agent in its build image, the agent will automatically assess the asset and report results.

SLA review ensures that assessment policies (depth, breadth and frequency) continue to suit each asset class. For example, if your application development team responsible for a revenue generating website has recently started using container technology or Azure, you need to work with them to update the appropriate assessment policy.

Privileged Access Management (PAM) integration is very helpful if you regularly change the credentials required for authenticated scanning. The integration automatically provides current credentials to the scanner to prevent failed scans.

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**