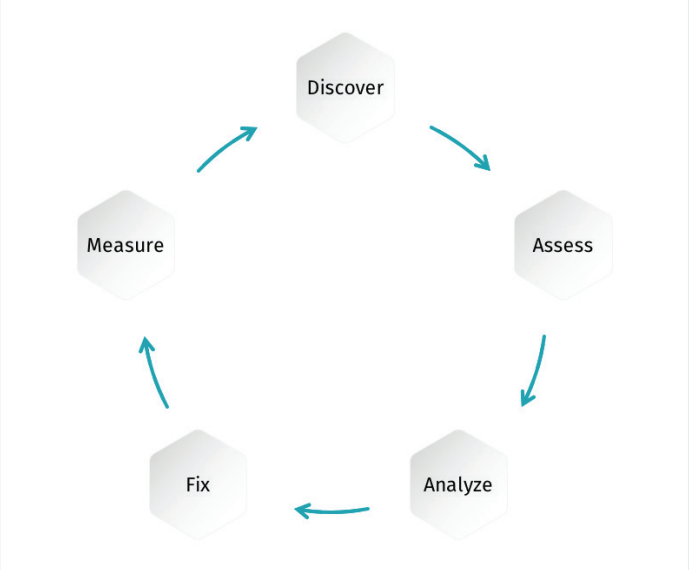
SOLUTION BRIEF

tenable

Vulnerability Management:
Asset Discovery

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 Discover, the first step of Cyber Exposure Lifecycle.

The Discover objective is for you to identify and map every hardware and software asset across all of your computing environments, including IT, mobile, cloud and operational technology. Asset discovery is an essential part of all information security frameworks, including the NIST Cyber Security Framework, ISO-IEC 27000, PCI and the CIS Controls (formerly the SANS Top 20). You must know all of the assets in your attack surface before you can adequately protect them.

Key Benefits

- **Understand your complete attack surface** so you can assess risk and adequately protect your organization.
- **Identify asset owners and/or administrators** who are responsible to define acceptable risk and take corrective action to reduce it, when needed.
- **Streamline IT asset management** processes and increase Configuration Management Database (CMDB) veracity.

Challenges

Inventorying all hardware and software assets in your entire attack surface is difficult for two primary reasons:

- Diverse asset types: Traditional IT, transitory, mobile, dynamic and operational technology assets often require different discovery technologies. Some organizations use different technologies from multiple vendors to discover the diverse asset types. This approach increases acquisition and management costs. Furthermore, multiple, disjointed discovery products results in asset inventory silos that make mapping diverse assets to business services difficult, if not impossible.
- Building mature discovery capabilities takes time: To start, you must understand your current capabilities, including identifying visibility gaps. Next, you must define the capabilities required to deliver complete visibility. Finally, you must plan and implement capabilities that will give you the complete visibility you need to understand your entire attack surface.

Solution

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

LEVEL 1. DISCOVER ON-PREMISES TRADITIONAL ASSETS

You should start discovery by identifying network infrastructure, servers and desktop PCs connected to your on-premises networks.

Tenable Cyber Exposure platforms include Nessus scanners that you can install throughout your networks to discover your assets. Nessus host discovery scans use ARP, TCP and ICMP pings to identify traditional hosts and common open ports within specified address ranges. Additionally, you can use a cloud-based Nessus scanner included with Tenable.io to scan your external- facing IP addresses and discover internet accessible hosts.

LEVEL 2. DISCOVER TRANSITORY, MOBILE, DYNAMIC AND OPERATIONAL TECHNOLOGY ASSETS

You must discover all modern assets to measure to manage your complete attack surface.

Transitory assets, such as laptops and virtual machines, are often disconnected from the network when Nessus host discovery scans run. Therefore, you should automatically include an agent in your standard laptop and virtual machine images. Then, when you deploy or instantiate a new asset, it will automatically report its presence to the Tenable Cyber Exposure platform.

Mobile assets include phones and tablets that connect to your network. You should ensure they adhere to corporate security policies by managing them with a mobile device management application. Tenable Cyber Exposure platforms connect to popular mobile device management applications to retrieve inventory information.

Dynamic assets include public cloud infrastructure, web applications and containers. They are challenging to discover and inventory because they are short-lived and/or may not be powered-on when active scans run. Tenable provides special software connectors to discover dynamic assets.

Operational technology (OT), if it exists in your organization, must be discovered because of its importance to your revenue stream and because a security incident involving OT could have significant safety and environmental impact. OT assets, such as PLCs and RTUs often cannot withstand active scanning. Nessus Network Monitor used in conjunction with Industrial Security passively discovers them without the risk of disruption.

LEVEL 3. ASSET CLASSIFICATION

After discovering all assets, you need to classify them.

Asset classification lays a foundation for risk-based vulnerability management. At a minimum, you should classify assets as high, medium, or low criticality based on business service criticality and regulatory and/or partner requirements. High criticality assets are those that would have high loss magnitude should a security incident occur. You will focus more thorough analysis, remediation and measurement on high criticality assets.

Tenable Cyber Exposure platforms let you tag assets with classification level and other attributes, such as asset owner and/or administrator to help you manage them.

LEVEL 4. CONTINUOUSLY DISCOVER ASSETS AND INTEGRATE WITH IT ASSET MANAGEMENT

You should broadly deploy passive monitoring throughout your network so you can quickly detect new/rogue devices. Additionally you should integrate your Tenable Cyber Exposure platform with your Configuration Management Database (CMDB).

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**.

Passive monitoring with Nessus Network Monitor shines light into the blind spots between active scans by immediately detecting new assets when they connect to the network. Additionally, passive monitoring sensors installed at network egress points will identify connections with external assets.

2-way CMDB integration improves Configuration Management Database (CMDB) data veracity by adding assets identified during the Discover step that may have been previously unrecorded in the CMDB. Asset attributes in the CMDB, such as asset owner, administrator, location and SLA will inform downstream VM phases. Additionally, rich CMDB data facilitates IT service management processes, including asset management and change management.

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