SOLUTION BRIEF

PASSIVE NETWORK MONITORING

Discovering and assessing assets in modern IT and operational technology (OT) environments, requires multiple sensors; active scanners, agents, and passive network monitors. Each sensor has unique advantages, and many organizations rely on all three to maximize their ability to measure and manage cyber risk.

Tenable Nessus® Network Monitor (NNM), a passive monitoring sensor, continuously discovers active assets on the network and assesses them for vulnerabilities. NNM is based on patented network discovery and vulnerability analysis technology that continuously monitors and profiles non-intrusively. It monitors IPv4, IPv6 and mixed network traffic at the packet layer to determine topology, services and vulnerabilities. Nessus Network Monitor serves as an integrated component of Tenable.io™ VM, Industrial Security™ and Tenable.sc (formerly SecurityCenter), enabling full visibility into traditional and modern assets.

KEY CHALLENGES

Vetting newly connected assets. Security and operations staff must quickly determine if assets that have recently connected to their network are authorized so they can take corrective action, if needed.

Gaining visibility of vulnerabilities between active and agent scans. Depending on the scan frequency, organizations may require near real-time visibility of vulnerabilities on critical assets so they can mitigate them before an adversary exploits them.

Safely monitoring operational technology networks. Programmable Logic Controllers, Remote Terminal Units, and other OT devices cannot accept agents, and they may be disrupted by active scanning. Security staff needs a way to inventory and assess assets in OT environments, without the risk of causing an outage.

SOLUTION REQUIREMENTS

A number of commercial and open source organizations offer passive network monitoring products. However, the capabilities and maturity of these products vary widely, so it is important to define the most important requirements for your organization. Without defining your requirements, you could invest budget and time only to determine that the selected product cannot meet your needs.

Access to network traffic. Passive monitoring sensors must be able to "see" the network traffic that is to be monitored. The sensor must be able to connect to a physical TAP or SPAN port. Additionally, if you need to monitor virtual traffic in the cloud or in virtual infrastructure, the sensor must be able to run on a properly configured virtual machine.

Protocol support. In addition to TCP or UDP, you should ensure that the passive monitoring solution supports any other protocols you require. These might include SCTP, ICMP, IPIP and IDP; not to mention OT protocols. These may include BACnet, CIP, DNP3, Ethernet/IP, ICCP, IEC 60870-5-104, IEC 61850, IEEE C37.118, Modbus/TCP, OPC, PROFINET and Siemens S7.

Asset discovery and profiling. In addition to supporting protocols, a passive monitoring solution must recognize the assets that use the protocol. These will include IT assets, such as servers, desktops, laptops, network devices, web apps, virtual machines, mobile and cloud. They may also include OT assets, such as PLCs, RTUs, HMIs, communication adapters and more.

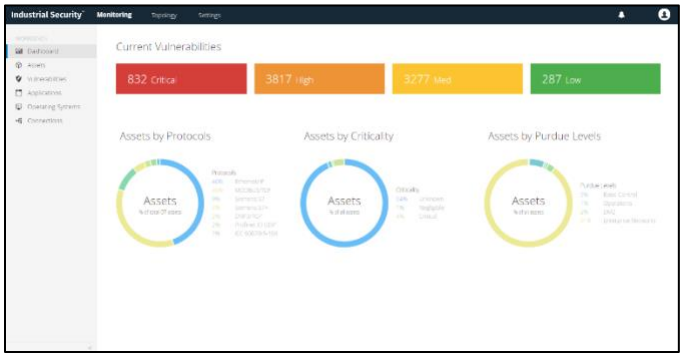
Vulnerability assessment. Building on asset discovery and profiling capabilities, a passive monitoring solution must also identify known vulnerabilities in the assets. These vulnerabilities may allow remote access, privilege escalation, buffer overflows and more.

Real-time notification. The passive monitoring solution should be capable of sending events to your SIEM when new assets are detected. This supports removing the asset from the network if it should not be on the network.

SOLUTION BRIEF

TENABLE NESSUS NETWORK MONITOR

Nessus® Network Monitor (NNM) meets all of the above passive monitoring requirements. NNM provides unmatched visibility of the systems and services running on your networks. From legacy assets to the latest technologies, it illuminates blind spots so you can see and protect your entire environment. Nessus Network Monitor detects new and unmanaged assets – spanning operating systems, network devices, hypervisors, databases, mobile devices, web servers, cloud applications, OT assets, and IoT devices. As part of Industrial Security, Nessus Network Monitor offers enhanced OT support – including asset discovery and protocol detection – for passively monitoring industrial control systems (ICS), SCADA systems and other operational technology. This gives security teams a safe and non-intrusive way to discover and monitor sensitive, critical infrastructure.



Industrial Security summarizes information gathered from an operational technology environment by NNM.

Patented NNM network discovery and vulnerability analysis technology delivers continuous monitoring and profiling non-intrusively. It monitors IPv4, IPv6 and mixed network traffic at the packet layer to determine topology, services and vulnerabilities. Nessus Network Monitor serves as an integrated component of Tenable.io, Industrial Security and Tenable.sc, enabling full visibility into traditional and modern assets.

KEY BENEFITS

Continuous Asset Discovery and Vulnerability Detection

Nessus Network Monitor continuously monitors network traffic for a variety of security-related information including:

- Detecting new assets added to a network
- Passively determining the operating system of each active host
- Applying more than 8,000 asset and vulnerability checks, covering a wide range of devices, communication protocols and asset categories – from IT to OT. As a part of Industrial Security, Nessus Network Monitor delivers
    - Coverage of more than 1,000 ICS and SCADA systems in industrial, manufacturing, energy and oil & gas companies
    - Support for systems from dozens of manufacturers are supported including ABB, Emerson, GE, Honeywell, Rockwell/Allen Bradley, Schneider Electric and Siemens
- Vulnerability Detection on communicating systems, protocols and applications

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 24,000 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 Tenable.io®, the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include 53 percent of the Fortune 500, 29 percent of the Global 2000 and large government agencies. Learn more at tenable.com.