Brought to you by

tenable

RISK-BASED VULNERABILITY MANAGEMENT SOLUTION GUIDE

HOW TO EVOLVE YOUR LEGACY VM PRACTICE TO A RISK-BASED VM PROGRAM

STEP FIVE: MEASURE

Tenable Guide to Risk-Based VM

STEP FIVE: MEASURE

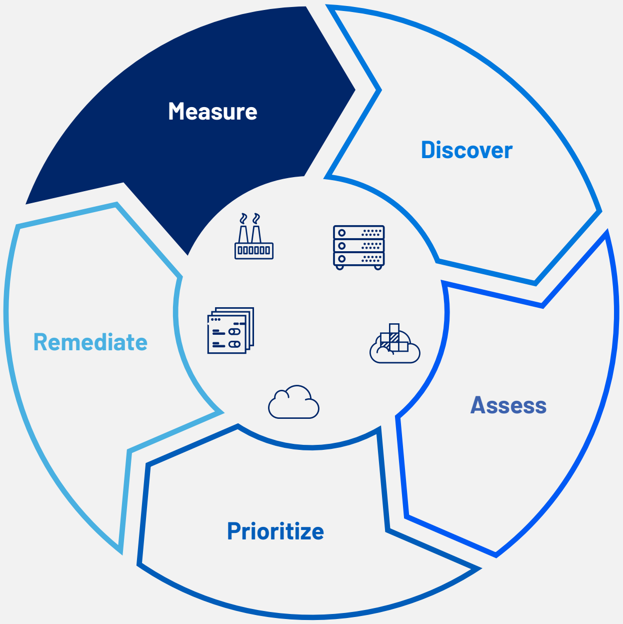
Comprehensive, real-time measurement empowers security leaders to communicate and benchmark the performance of their organization's security program to senior executives and the board. Robust reporting capabilities are key to making the right decisions – and standing by those decisions when questions are raised. By identifying metrics that align with business objectives, security leaders can gain and maintain the board's confidence in their abilities, and keep them out of "panic mode" during times of high-profile threats.

In the first four installments of our Risk-Based VM Solution Guide, we provided step-by-step instructions on how to discover, assess, prioritize and remediate the assets and vulnerabilities that pose the greatest risk to your organization. In this final installment of our five-part series, Measure, we'll explain how your security team can use key performance indicators (KPIs) to understand exactly how much cyber risk is in your environment, identify areas across your network most in need of improvement and effectively communicate the value of your risk-based VM program across the organization.

66%

Of business leaders are—at most—only somewhat confident in their security team's ability to quantify their organization's level of risk or security.[1]

Lifecycle for Risk-Based Vulnerability Management



Discover
Identify and map every asset for visibility across the organization's entire attack surface

Assess
Understand the state of all assets, including vulnerabilities, misconfigurations and other health indicators

Prioritize
Understand exposures in context, to prioritize which vulnerabilities to fix first based on asset criticality, threat context and vulnerability severity

Remediate
Apply the appropriate remediation or mitigation technique

Measure
Calculate, communicate and compare key maturity metrics to drive risk reduction

[1] Based on The Rise Of The Business-Aligned Security Executive, a commissioned study of 425 business executives conducted by Forrester Consulting on behalf of Tenable, April 2020.

Why Risk-Based VM?

Stop Being Reactive and Start Being Proactive

Play Offense

Continually assess all assets across your enterprise and address vulnerabilities that pose the greatest risk

Break Tradition

Go beyond traditional IT assets and analyze cloud, containers, web apps, mobile, operational technology and more

Dig Into Details

Use granular analytics to understand the context of each vulnerability, including severity, threat actor activity and asset criticality

Communicate Risk

Secure executive leadership and key stakeholder buy-in with business risk metrics they understand

Measure Up

Use your Cyber Exposure Score (CES) to understand how you're performing against industry peers

Keep Evolving

Identify where you have gaps and make plans to mature your program over time

Evaluate and Communicate the Effectiveness of Your Security Program

Once you've implemented your vulnerability management program, the final step is to understand and communicate the value of those security efforts.

For the Measure step, there are two core areas of focus:

5a. **Measure risk-based vulnerability management KPIs**

5b. **Evaluate and optimize your efficiency and effectiveness**

To be successful here, you'll need to work with the various security groups across the organization to determine what KPIs are most important, so each team can develop common dashboards to ensure consistent reporting. You'll also need to work with your management to decide when and how frequently reporting should occur.

Measure: Identifying KPIs

Business Risk: Tracking the organization's overall Cyber Exposure Score (CES) can help you clearly see the team's progress over time. Maintaining separate measurements for each region, office, business unit or asset group helps identify potential weak areas that need to be addressed.

Process Maturity: If you're not scanning frequently enough, your authenticated scan coverage is inadequate or you're not remediating critical vulnerabilities quickly enough, you may not be maximizing risk reduction. Understanding the maturity of your assessment and remediation processes can help you find and fix critical gaps in your VM program.

Industry Benchmarks: In addition to understanding how much risk you have across your attack surface, comparing that exposure to the rest of your industry, as well as the global population, delivers a degree of context that can help both technical and business leaders better understand the effectiveness of your security program.

Core Focus Area: 5a.

Measure Risk-Based Vulnerability Management KPIs

Before you can optimize your risk-based program, you'll first need to establish your organization's KPIs.

What's the Objective?

Align security and business leaders with common metrics to measure and manage cyber risk across your organization.

Steps

1. Identify a common set of metrics required to monitor process integrity (e.g., asset scan coverage, asset scan frequency, scan depth, mean time to assess, mean time to remediate).

2. Determine overall risk metrics based on the predicted severity of open vulnerabilities, as well as the business criticality of affected assets, so you can report risk trends by business service.

3. Design common dashboard templates for deployment across the organization.

4. Determine required reporting frequency.

5. Scope dashboards by business system for each business owner.

Did You Know?

Only 5% of enterprises display a highly mature approach to vulnerability assessment. This means they frequently scan the majority of their assets, using local credentials and targeted vulnerability plugins. To make sure your team has the visibility they need, Tenable Lumin recommends personalized actions that can boost your organization's assessment maturity and ultimately lower your cyber exposure.[2]

Why is This Important?

Measuring your risk-based vulnerability management processes is the only way to track and communicate your team's progress. You'll need these metrics to optimize the integrity of your enterprise-level and department-specific risk metrics and ultimately drive your assessment or remediation efforts to help reduce cyber risk.

[2] Tenable Research, "Cyber Defender Strategies," July 2018.

Core Focus Area: 5b.

Evaluate and Optimize

Once you've identified your KPIs and collected initial measurements, follow these steps to evaluate and optimize your risk-based vulnerability management program.

What's the Objective?

Apprise business, security and IT leaders on the status of your security program and create agreed-upon action plans.

Suggested Steps

1. Compare actual results against service-level agreements (SLAs).

2. Identify SLA performance gaps.

3. Document SLA attainment status.

4. Plan corrective actions, which may include revising SLAs upward or downward.

5. Assign corrective action to responsible parties.

6. Implement corrective action.

Why is This Important?

Evaluating your risk-based vulnerability management program can help security leaders, IT operations staff and business executives better collaborate and understand business risk, including identifying areas for improvement and actions that can make your program stronger.

Did You Know?

Tenable can help you determine your Cyber Exposure Score for a single asset, a group of assets or your entire organization, so you can better manage business risk and plot trends.

Recommended Products

Platform

Tenable.ep (for comprehensive risk-based VM)

Tenable.io (for cloud environments)

Tenable.sc (for on-premises environments)

Tenable.ot (for OT environments)

Analytics

Tenable.ep (for assessing all assets in a unified view)

Tenable Lumin

Reduce the Greatest Amount of Risk With the Least Amount of Effort

Now that you've completed the Measure step, you're able to determine the effectiveness of your risk-based vulnerability management program, including what's working well and where there are areas for improvement. This knowledge will help you communicate the value of your security program to senior management and other key stakeholders, so you can effectively build their confidence in your capabilities, request additional resources and manage expectations when high-profile cyberattacks draw media attention.

With a specific, quantifiable understanding of how your program has performed, you'll also know exactly what adjustments to make to optimize your team's effectiveness and efficiency, as you continue to evolve your VM practices to align with a risk-based strategy.

Are you ready to get started? See how Tenable Lumin can help you gain the upper hand on cyber risk by signing up for a free demo today.

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.

070121 v2

tenable