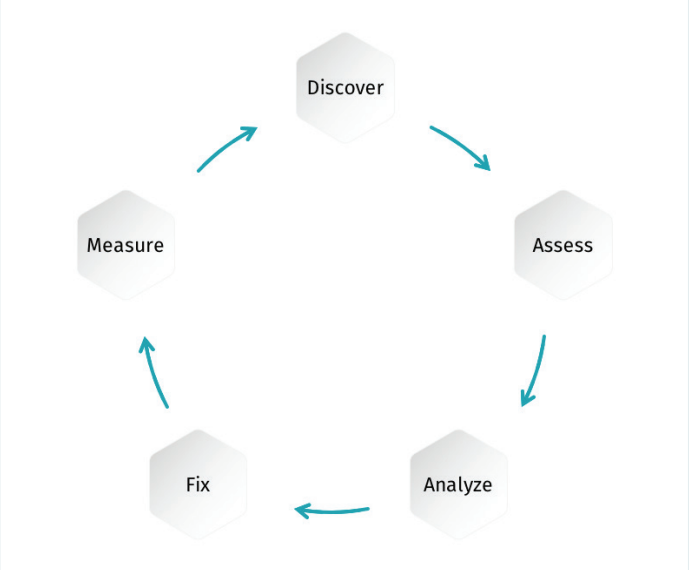
SOLUTION BRIEF

tenable

Vulnerability Management:
Analyze

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 Analyze, the third step of vulnerability management.

The Analyze objective is to help you answer two questions so you can deal with the onslaught of vulnerabilities and other exposures identified earlier in the Assess phase:

1. How should my organization prioritize the exposures?
2. What action should we take to mitigate the exposures?

Key Benefits

- **Prioritize vulnerabilities** based on a combination of threat intelligence, exploit availability and vulnerability metadata.
- **Focus remediation resources** on the vulnerabilities having the highest potential impact to your organization.
- **Inform incident management** with prioritized vulnerability and misconfiguration information to help prioritize investigations.

Challenges

Many organizations rely solely on CVSS scores to prioritize vulnerabilities and endeavor to remediate those rated high and critical. However, CVSS scores are only one of many prioritization factors you should consider. You need to quickly identify a manageable number of vulnerabilities that present the highest risk to your organization; the ones you need to fix first and fix fast. In addition to CVSS scores, your prioritization should include threat intelligence about past, active, expected exploits and vulnerability metadata. Automation is required to process this information and keep it current.

Next, you need to determine what action you should take and how quickly you need to take it. Should you do nothing and accept the risk? Should you patch immediately or wait until the next scheduled patch cycle? Should you mitigate with compensating controls?

Solution

Building a mature Analyze capability that helps you prioritize your vulnerability response progresses through four levels, and Tenable can help you with each one.

LEVEL 1. USE CVSS SCORES TO PRIORITIZE VULNERABILITIES

Most organizations initially rely on the Common Vulnerability Scoring System (CVSS) to prioritize vulnerabilities. CVSS assigns a score between 0.1 – 10.0 to each vulnerability and then adds a corresponding rating (low, medium, high and critical) depending on the score. CVSS-based prioritization is simple because virtually all vulnerability assessment tools report CVSS scores and allow users to filter vulnerabilities based on ratings. For example, you could filter only the high and critical vulnerabilities and endeavor to fix them.

The problem is that your organization is likely to face many more vulnerabilities than it can mitigate. More than 16,500 new vulnerabilities were discovered in 2018, and 59% were rated high or critical. That works out to nearly 200 new high/critical vulnerabilities each week. Of course, your organization will not have them all. However, if you have a given vulnerability you are likely to have multiple instances of it — each potentially needing mitigation.

A better approach is to prioritize based on underlying CVSS metrics that make up the overall score. The metrics fall into three groups; Base, Temporal and Environmental. The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics. The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. The Impact metrics reflect the direct consequence of a successful exploit in terms of confidentiality, integrity and availability.

The Temporal metric group reflects the characteristics of a vulnerability that may change over time. For example, the presence of a simple-to-use exploit kit would increase the CVSS score.

The Environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment. Realistically, few organizations modify the Environments metrics.

Tenable vulnerability scanners allow you to use custom filters based on CVSS metrics to prioritize vulnerabilities. Using the metrics is better than using only the rating. However, even using the metrics omits important factors, such as asset criticality and whether or not the vulnerability is being actively exploited in the wild.

LEVEL 2. MOVE BEYOND CVSS SCORES, AND ANALYZE ALTERNATIVES TO PATCHING

Effective prioritization analyzes many factors in order to winnow vulnerabilities down to the highest priority ones that must be fixed first. These factors include CVSS score, ease of exploit, exploit activity, threat vector and threat sources. Analyzing these factors on a daily basis requires automation, and it requires a machine-learning model that rates each vulnerability to determine its likelihood of being exploited in the near future. Tenable calls this rating the vulnerability's Vulnerability Priority Rating (VPR). VPR scores help you reduce the number of CVSS high and critical vulnerabilities by as much as 97%.

The likelihood of a vulnerability being exploited in the near future evolves as factors, such as exploit activity, change. Therefore, the model must continually update ratings. Tenable updates VPR scores daily.

Vulnerability-patching alternatives are appropriate when patches are not available and when availability requirements preclude patching and associated reboots. In some cases, you will accept the risk associated with the vulnerability. In other cases, you will apply compensating controls instead of patching. In either case, you need to document your response, who authorized it, any compensating controls and any expiration date.

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 3. INCORPORATE ASSET CRITICALITY INTO PRIORITIZATION

A more mature Analyze capability incorporates the concept of expected loss impact into vulnerability prioritization by combining an Asset Criticality Rating (ACR) with the VPR. The Tenable Lumin Cyber Exposure Score (CES) is the result of this combination, and the CES provides risk-based guidance about what to focus on. You can calculate the CES for any asset, asset group (such as business process or business unit) or for the entire organization. This provides you with a Cyber Exposure score for each user-defined group and provides useful metrics for you to improve your cyber exposure program. These metrics include vulnerability age, scan type, and scan frequency. Additionally, it provides recommendations to improve the Cyber Exposure Score.

You can also analyze configuration assessment results to inform your response. This is especially important for high criticality assets. IT operations should not remediate misconfigurations without first testing each change to ensure that it does not disrupt operation of the business service. If you decide not to reconfigure the asset to eliminate the finding, you must either modify the standard or grant and document an exception to the standard. If you decide to reconfigure the asset, you must also reconfigure backups and golden images to prevent the misconfiguration from being reintroduced.

LEVEL 4. INFORM SECURITY MONITOR WITH VULNERABILITY AND MISCONFIGURATION DATA

You can use vulnerability and configuration assessment data to inform security monitoring. Integrating Tenable Cyber Exposure platforms with your SIEM application allows analysts to quickly scan a host and/or view the latest vulnerability and configuration summary for a host during an investigation.

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