SOLUTION BRIEF

PRIORITIZATION WITH TENABLE CLOUD SECURITY

Introduction

The convergence of three key factors has created a challenging landscape for security teams tasked with managing and prioritizing cloud-related security exposure:

- Rapid migration to the cloud has resulted in a shift in spending from traditional IT infrastructure to cloud services. This transition brings about a shared responsibility model, where organizations struggle to determine their ownership of security risks versus the responsibility of the cloud service provider. This lack of clarity leads to unseen exposure and creates challenges in effectively managing security.
- Adoption of cloud-native architectures introduces a multitude of moving parts, such as containers, Kubernetes, and Infrastructure as Code (IaC). The modular and scalable nature of these architectures means that misconfigurations or vulnerabilities can be easily replicated at scale, generating a barrage of alerts that overwhelm limited security resources. The complexity of managing these components compounds the difficulty in scaling security operations.
- The need for speed and the increasing complexity of multi-cloud environments pose additional hurdles. More cloud workloads and a higher ratio of developers to security staff, often as high as 100:1, result in a strain on security resources. Developers prioritize fast time-to-market using DevOps practices, while security teams struggle to keep up with the rapid pace of deployment. Additionally, managing unique configuration requirements for each cloud provider adds further complexity to the security landscape.

These three trends collectively contribute to the difficulty of scaling cloud security staff and processes, necessitating innovative approaches, automation, and the use of preventative security to effectively address the evolving security challenges in cloud environments.

Two Main Varieties of Cloud Exposure

Before delving into the prioritization approaches used by Tenable Cloud Security, it is important to explore the two types of exposure it identifies, as different approaches will be needed to address each:

- Vulnerabilities (CVEs) represent one of the key types of cloud-related risks that organizations must address. Vulnerabilities can arise from flaws in software, operating systems, or other components used in cloud environments. Exploiting these vulnerabilities can allow attackers to gain unauthorized access, move laterally and escalate privileges.
- Misconfigurations constitute another critical type of risk in cloud environments. With extensive configuration options, risky defaults, specialized requirements by cloud provider, and increased multi-cloud adoption, misconfigurations have become the leading cause of cloud breaches. Misconfigurations can occur at various levels, such as network settings, access controls, excess privileges, storage permissions, or encryption settings. These misconfigurations can inadvertently expose sensitive data, create security gaps, or open avenues for unauthorized access.

The Need for Scalable Prioritization

Effective prioritization of vulnerabilities and misconfigurations in cloud environments is crucial for optimizing resources, reducing risks, ensuring business continuity, and meeting compliance requirements. It allows organizations to focus their efforts on the most critical security concerns, minimizing the chances of successful attacks, data breaches, or service disruptions.

By addressing high-risk areas first, organizations can protect essential systems, applications, and data, maintaining ongoing operations and customer trust. Additionally, prioritization aligns with compliance obligations, demonstrating due diligence and avoiding penalties or legal issues.

Risk Prioritization with Tenable Cloud Security

Whether prioritizing vulnerabilities or misconfigurations, there are several factors which are important in determining a priority score. They include an understanding of severity, exploitability, and potential consequences. As it relates to vulnerabilities, there are widely accepted approaches on how this can be done which lay the foundation. The most notable of these is the Common Vulnerability Scoring Systems (CVSS). In contrast, cloud misconfigurations currently lack broadly accepted standards for prioritization.

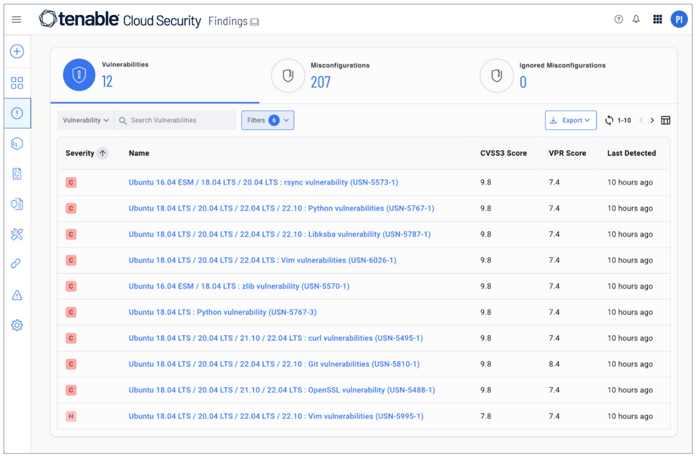
In this section we will explore the distinct approaches used by Tenable Cloud Security to enable effective prioritization of vulnerabilities and misconfigurations.

Prioritization of Vulnerabilities

In Tenable Cloud Security, the severity and exploitability of a given vulnerability is represented by its Vulnerability Priority Rating (VPR). VPR is calculated using a combination of drivers, including the widely accepted CVSS standard developed by a consortium of organizations known as the Forum of Incident Response and Security Teams (FIRST).

VPR extends the static measure of technical severity provided by the vulnerability's CVSS score, with dynamic variables that are continually updated to reflect the constantly changing threat environment. Tenable computes an initial VPR using a machine-learning algorithm that analyzes more than 150 different aspects of each vulnerability to determine its level of risk.

VPR is valuable, in that it does not rely on static CVSS alone, instead it leverages real world insights to continuously improve the accuracy of risk scoring and reduce noise.



Severity	Name	CVSS3 Score	VPR Score	Last Detected
C	Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : rsync vulnerability (USN-5573-1)	9.8	7.4	10 hours ago
C	Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 : Python vulnerabilities (USN-5767-1)	9.8	7.4	10 hours ago
C	Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 : Libksba vulnerability (USN-5787-1)	9.8	7.4	10 hours ago
C	Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6026-1)	9.8	7.4	10 hours ago
C	Ubuntu 16.04 ESM / 18.04 LTS : zlib vulnerability (USN-5570-1)	9.8	7.4	10 hours ago
C	Ubuntu 18.04 LTS : Python vulnerability (USN-5767-3)	9.8	7.4	10 hours ago
C	Ubuntu 18.04 LTS / 20.04 LTS / 21.10 / 22.04 LTS : curl vulnerabilities (USN-5495-1)	9.8	7.4	10 hours ago
C	Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 : Git vulnerabilities (USN-5810-1)	9.8	8.4	10 hours ago
C	Ubuntu 18.04 LTS / 20.04 LTS / 21.10 / 22.04 LTS : OpenSSL vulnerability (USN-5488-1)	9.8	7.4	10 hours ago
H	Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 : Vim vulnerabilities (USN-5995-1)	7.8	7.4	10 hours ago

As compared to CVSSv3, VPR can significantly reduce the number of critical and high severity findings, allowing prioritized remediation of vulnerabilities most likely to be exploited.

Key drivers that are used to calculate VPR include, but are not limited to, the following:

- Age of vulnerability, measured in days since publication in the National Vulnerability Database (NVD)
- CVSSv3 Impact Score, if available, or else a predicted impact score for vulnerabilities prior to NVD publication whereby the model analyzes the text from the security advisory as an input
- Exploit code maturity, based on the existence and sophistication of relevant exploit code
- Product coverage, in terms of the relative number of unique systems affected by the vulnerability
- Threat sources, such as social media channels and dark web forums where exploits are discussed
- Threat intensity, based on the number and frequency of recent threat events
- Threat recency, or the number of days since a threat event occurred

A vulnerability's VPR is expressed as a number from 0.1 to 10, with higher values corresponding to higher likelihood of the vulnerability leading to a compromise and a higher impact on the asset. Based on those values, vulnerabilities can be rated in terms of their severity levels, including Low (0.1-3.9), Medium (4.0-6.9), High (7.0-8.9), and Critical (9.0-10.0). The value is calculated within 24 hours of a vulnerability's initial disclosure on the National Vulnerability Database (NVD), providing security teams with early indicators of risk often days or weeks — and sometimes months — before a Common Vulnerability Scoring System (CVSS) value is assigned.

By integrating a broad range of dynamic risk factors, VPR is able to elevate the relatively few vulnerabilities that require immediate attention based on their actual — not theoretical — levels of risk. Vulnerability overload has long been a pitfall of prioritization based solely on CVSS, which rates as many as 56% of vulnerabilities as "High" or "Critical," muddying the real-world severity of a given vulnerability. VPR, by comparison, rates approximately 4% of all vulnerabilities as "High" and 1% as "Critical," respectively, providing a more actionable basis for remediation planning. In fact, VPR is 18 times more efficient than CVSS in spotting those vulnerabilities that end up being utilized by attackers; remediating the top 1,900 VPR scores is as efficacious as remediating the top 34,000 CVSSv3 scores.

Prioritization of Misconfigurations

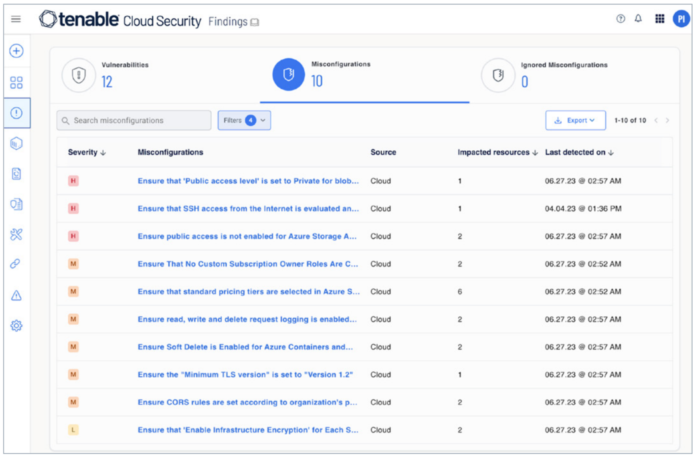
Tenable Cloud Security offers two methods of prioritization specific to cloud misconfigurations - risk based scoring and compliance posture scoring. These methods are designed to compliment each other. Additional prioritization methods for misconfigurations and vulnerabilities are also available from the Tenable One platform. They are introduced later in this brief, and covered in a separate paper.

Risk Based Scoring

Tenable Cloud Security provides a comprehensive collection of 1500+ policies that align with industry best practices for configuration. The risk-based approach leverages expert knowledge from Tenable Research and evaluates each security policy based on various risk variables. This assessment enables the calculation of a prioritization score, categorizing policies as high, medium, or low priority based on their potential risk level.

When calculating a risk-based score for a given policy, several variables are evaluated by Tenable Research, including but not limited to the following:

- **Impact:** The potential impact, including potential for data breaches, unauthorized access, or service disruptions.
- **Exploitability:** The ease and expertise required to exploit by an attacker including the availability of known exploits, and the level of technical expertise required for exploitation.
- **Visibility:** The likelihood of the misconfiguration being discovered by external security assessments, or malicious actors.
- **Reach:** The number of resources, users or systems impacted that rely on the affected components, and the potential for lateral movement.



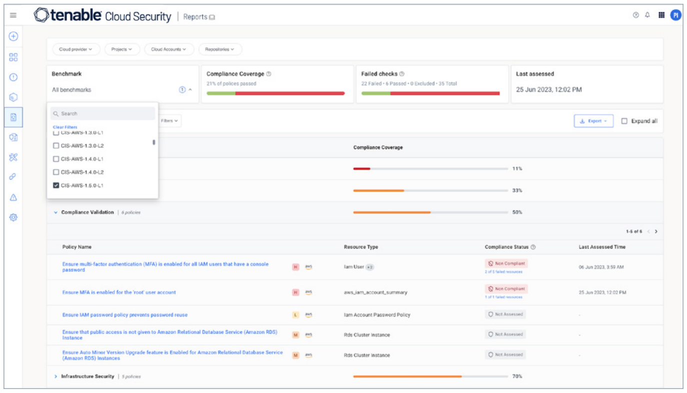
Severity ↓	Misconfigurations	Source	Impacted resources ↓	Last detected on ↓
H	Ensure that 'Public access level' is set to Private for blob...	Cloud	1	06.27.23 @ 02:57 AM
H	Ensure that SSH access from the Internet is evaluated an...	Cloud	1	04.04.23 @ 01:36 PM
H	Ensure public access is not enabled for Azure Storage A...	Cloud	2	06.27.23 @ 02:57 AM
M	Ensure That No Custom Subscription Owner Roles Are C...	Cloud	2	06.27.23 @ 02:52 AM
M	Ensure that standard pricing tiers are selected in Azure S...	Cloud	6	06.27.23 @ 02:52 AM
M	Ensure read, write and delete request logging is enabled...	Cloud	2	06.27.23 @ 02:57 AM
M	Ensure Soft Delete is Enabled for Azure Containers and...	Cloud	2	06.27.23 @ 02:57 AM
M	Ensure the "Minimum TLS version" is set to "Version 1.2"	Cloud	1	06.27.23 @ 02:57 AM
M	Ensure CORS rules are set according to organization's p...	Cloud	2	06.27.23 @ 02:57 AM
L	Ensure that 'Enable Infrastructure Encryption' for Each S...	Cloud	2	06.27.23 @ 02:57 AM

Risk based prioritization uses multiple variables to prioritize misconfigurations including impact, exploitability, visibility, and reach.

Compliance Posture Scoring

Tenable Cloud Security offers pre-built policies that align with over 20 different industry benchmarks and frameworks. These include popular benchmarks for cloud such as those from the Center for Internet Security (CIS). CIS Benchmarks are widely accepted as the best practice configurations for specific environments and products, including AWS, Azure and Google Cloud, and Kubernetes. Control framework support includes NIST, CSA and others, as well as those mandated by regulations or governing bodies, such as HIPAA, GDPR, and PCI DSS.

Organizations can apply filters for specific benchmarks and frameworks and instantly see what assets are non-compliant, and the specific policies that have been violated along with their risk based prioritization score. They also see an overall compliance score for the benchmark or frameworks, and individual scores for compliance associated with specific control categories. This comprehensive view empowers organizations to assess their compliance posture efficiently and take targeted actions to address any areas of concern.



Benchmark: All benchmarks

Compliance Coverage: 21% of polices passed

Failed checks: 22 Failed • 6 Passed • 0 Excluded • 35 Total

Last assessed: 25 Jun 2023, 12:02 PM

□ CIS-AWS-1.3.0-L1
□ CIS-AWS-1.3.0-L2
□ CIS-AWS-1.4.0-L1
□ CIS-AWS-1.4.0-L2
☑ CIS-AWS-1.5.0-L1

	Compliance Coverage
	11%
	33%
Compliance Validation | *6 policies*	50%

Policy Name		Resource Type	Compliance Status	Last Assessed Time
Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	H aws	Iam User +2	Non Compliant 2 of 5 failed resources	06 Jun 2023, 3:59 AM
Ensure MFA is enabled for the 'root' user account	H aws	aws_iam_account_summary	Non Compliant 1 of 1 failed resources	25 Jun 2023, 12:02 PM
Ensure IAM password policy prevents password reuse	L aws	Iam Account Password Policy	Not Assessed	-
Ensure that public access is not given to Amazon Relational Database Service (Amazon RDS) Instance	M aws	Rds Cluster Instance	Not Assessed	-
Ensure Auto Minor Version Upgrade feature is Enabled for Amazon Relational Database Service (Amazon RDS) Instances	M aws	Rds Cluster Instance	Not Assessed	-

Infrastructure Security | *5 policies* 70%

Organizations can select specific benchmarks and regulations and see an overall compliance score, including severity of individual policy violations for prioritized remediation.

IaC Security Testing and Artifact Scanning

One of the key benefits of the cloud is the modular and reusable nature of images and infrastructure as code (IaC). This also means that vulnerabilities and misconfigurations can be replicated at scale in runtime environments, generating large volumes of alerts. Scanning images and Infrastructure-as-Code (IaC) as part of automated DevOps workflows for vulnerabilities and misconfigurations is a highly effective approach to reduce alert noise and scale cloud security. Tenable Cloud Security offers comprehensive scanning capabilities for container registries, IaC code repositories, and as part of automated pipelines.

By conducting scans before deployment and automating the generation of pull requests for remediation, Tenable Cloud Security helps not only prevent the overwhelming volume of alerts during runtime, alleviating the burden on security staff, but also reduce costly rework needed by Dev teams. Ultimately, the combination of pre-deployment scanning and developer-initiated remediation empowers organizations to leverage automation and preventative measures, maximizing limited security resources and expertise, while minimizing runtime alerts and prioritization demands.

About Tenable

Tenable® is the Exposure Management company. More than 40,000 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 approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

Prioritization with the Tenable One platform

As a robust exposure management platform, Tenable One enriches the prioritization provided by Tenable Cloud Security and extends it across the end-to-end attack surface. Key prioritization capabilities within Tenable One include:

- **Vulnerability Priority Rating (VPR) for Misconfigurations:** Similar to VPR for vulnerabilities within Tenable Cloud Security, Tenable One calculates a VPR score for misconfigurations based on unique variables for exploitability and impact.
- **Asset Criticality Rating (ACR):** ACR assesses the type of asset and its unique capabilities to calculate an asset's relative criticality to the business. ACR can be individually tailored by users to address an organization's unique criteria and requirements.
- **Asset Exposure Score (AES):** AES is an aggregate score which combines the VPR and ACR for a given asset into an overall Asset Exposure Score which can be used to prioritize remediation according to total asset risk.
- **Cyber Exposure Scoring (CES):** CES aggregates AES values to produce an overall exposure score across a group of assets in a targeted exposure card. Exposure cards can be customized to reflect critical applications, processes or business units providing insight into Cyber Exposure in business context.
- **Attack Path Analysis (APA):** APA assesses asset relationship and exposure data to identify attack paths and potential impact enabling prioritized remediation.

Streamline Prioritization with Tenable Cloud Security

With security resources in short supply, effective prioritization is a necessity to scale cloud security and control risk. Tenable Cloud Security offers organizations a scalable solution to address the complex challenge of managing and prioritizing security risk from misconfigurations and vulnerabilities – which are the leading cause of cloud breaches. Combining risk-based and compliance posture scoring, along with shift left scanning that detects misconfigurations and vulnerabilities before they are deployed, organizations can effectively prioritize remediation and make better use of existing talent. Further, prioritization can be extended across the full hybrid attack surface using AES, CES, and attack path analysis provided by the Tenable One platform.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact