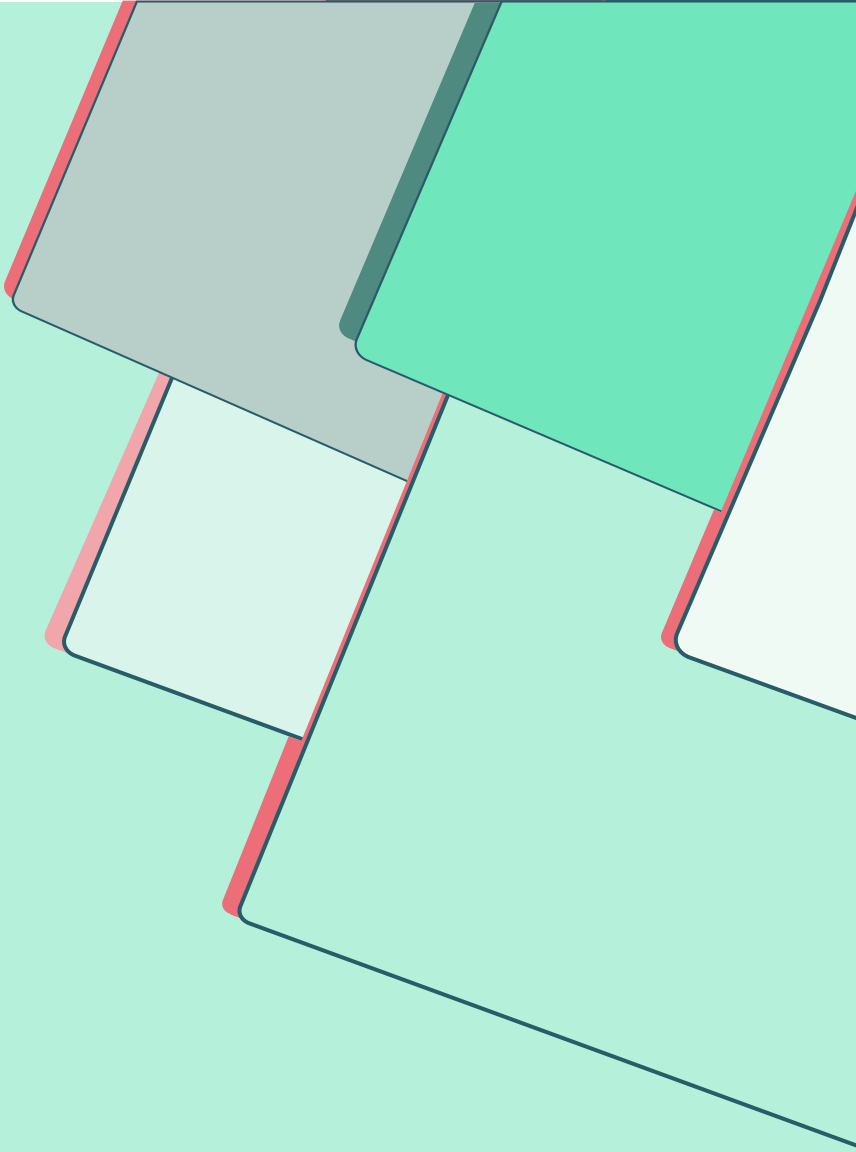
VULCAN.



White paper

# Exposure & vulnerability management metrics: A deeper dive

# Table of contents

# Introduction

By systematically identifying, prioritizing, and remediating vulnerabilities, organizations can significantly reduce their exposure to cyber threats and safeguard their critical assets. But without effective measurement and analysis, exposure management programs can lack direction and fail to demonstrate their true impact.

Key stat

**Only 3% of organizations globally have the "Mature" level of readiness to be resilient against cyber security risks[1]**

To this end, exposure management metrics provide a critical framework for assessing the effectiveness of exposure management programs and guiding informed decision-making. By tracking key indicators such as scan coverage, vulnerability age, and remediation time, organizations can gain valuable insights into their overall security posture and identify areas for improvement, prioritizing remediation efforts accordingly.

Below are 10 common exposure management metrics & KPIs, together with some suggested KPI dashboards to help teams make better sense of their cyber security programs.

# 10 key exposure & vulnerability management KPIs

There are a number of key metrics organizations can use to measure the impact of their exposure management programs and improve their security posture.

1. Scan coverage
2. Time to detection
3. Vulnerability age
4. Time to remediation
5. Patching rate
6. Average vulnerabilities per asset over time
7. Remediation results against SLAs
8. Asset risks
9. Number of exceptions granted
10. Vulnerability reopen rate

[1]www.brightdefense.com/resources/cybersecurity-statistics/

# 1 Scan coverage

Scan coverage, a fundamental metric, measures the percentage of assets that have been successfully scanned for vulnerabilities. It provides a clear indication of the scope of an organization's exposure management program and helps to identify any areas where coverage may be lacking.

## The importance of scan coverage

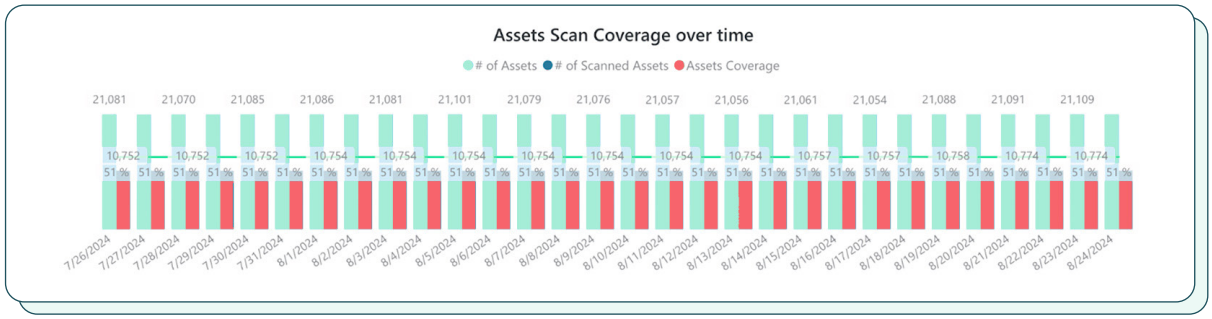
Comprehensive scan coverage is crucial for several reasons:

- **Clarifies risk scope:** By understanding the extent of assets that have been scanned, organizations can gain a clearer picture of the potential risks they face. This information is essential for prioritizing remediation efforts and ensuring that the most critical assets are protected.
- **Uncovers hidden vulnerabilities:** Assets that fall outside of the scan coverage scope may harbor undetected vulnerabilities, exposing the organization to potential breaches. Comprehensive scanning helps to identify these hidden risks and ensure that all assets are properly secured.
- **Demonstrates progress:** Tracking scan coverage over time provides a measurable indication of the progress of an organization's exposure management program. This data can be used to demonstrate the effectiveness of the program to stakeholders and to justify continued investment in security resources.

## Measuring scan coverage

There are several key factors to consider when measuring scan coverage:

- **Types of scanning conducted:** Organizations should employ a variety of scanning techniques to achieve comprehensive coverage. This includes network scanning, agent-based scanning, and application scanning.
- **Coverage analytics of business-critical assets:** Particular attention should be paid to business-critical assets, as these are often the most targeted by attackers. Scanning coverage for these assets should be prioritized and closely monitored.
- **Types of authentication offered:** The types of authentication offered by systems can also impact scan coverage. For instance, systems that require privileged access may not be scanned as frequently due to access restrictions. Organizations should consider alternative scanning methods for these systems.



## 2 Time to detection

Time to detection (TTD) measures the time it takes to identify a vulnerability following its introduction into an organization's IT environment. It provides valuable insights into the effectiveness of vulnerability scanning and assessment processes and helps organizations prioritize remediation efforts.

### The importance of rapid vulnerability detection

Swift vulnerability detection is essential for several reasons:

- **Timely risk mitigation:** Early detection allows organizations to assess the potential impact of a vulnerability and take appropriate mitigation measures before it can be exploited by attackers.
- **Prioritization of remediation efforts:** By identifying vulnerabilities promptly, organizations can prioritize remediation efforts based on the severity of the vulnerability and the potential impact on critical assets.
- **Reduced attack window:** Rapid detection narrows the window of opportunity for attackers to exploit a vulnerability, minimizing the potential damage that can be caused.

### Measuring time to detection

The most straightforward way to measure TTD is to calculate the time gap between when a vulnerability is first disclosed or publicly known and when it is identified within an organization's IT environment. This can be achieved by comparing vulnerability scanning results with vulnerability disclosure databases and tracking the time it takes to remediate the vulnerability.

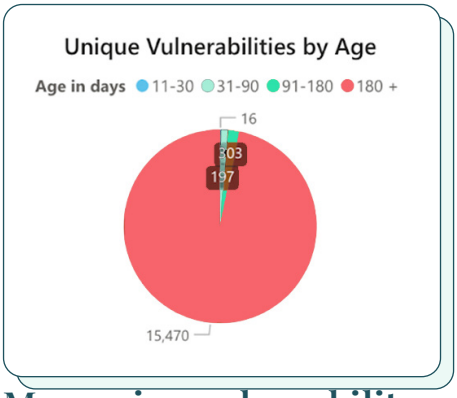
## 3 Vulnerability age

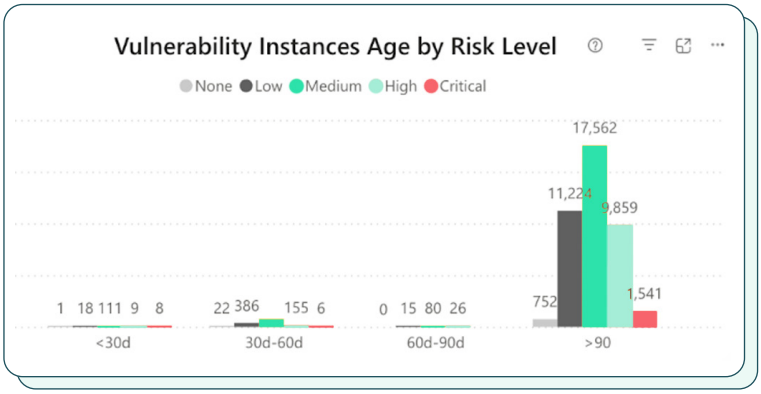
Vulnerability age measures the length of time a vulnerability remains unpatched or unmitigated within an organization's IT environment. It provides valuable insights into the effectiveness of exposure management processes and helps organizations prioritize remediation efforts.

### The risk of aged vulnerabilities

Unpatched vulnerabilities pose a significant risk to organizations, as they become increasingly attractive targets for attackers. The longer a vulnerability remains unaddressed, the higher the likelihood of it being exploited, which could result in data breaches, financial losses, and reputational damage.

Vulnerability age is calculated by determining the time gap between when a vulnerability is first disclosed or publicly known and when it is remediated within an organization's IT environment.




## Measuring vulnerability age

Vulnerability age is typically measured in days or weeks and is calculated by determining the time gap between when a vulnerability is first disclosed or publicly known and when it is remediated within an organization's IT environment. This information can be tracked using exposure management tools and by referencing vulnerability disclosure databases.

# 4 Time to remediation

Time to remediation (TTR) measures the average time it takes for an organization's security team to remediate a vulnerability after it has been identified. It provides valuable insights into the effectiveness of exposure management processes and helps organizations prioritize remediation efforts based on their vulnerability appetite.

## The importance of rapid vulnerability remediation

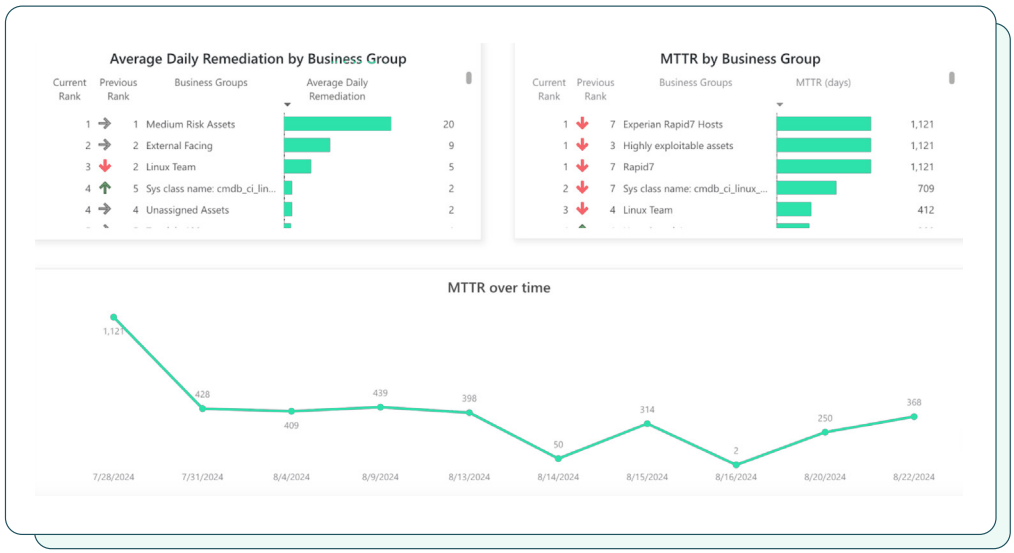
Rapid vulnerability remediation is essential for several reasons:

- **Reduced attack window:** Prompt remediation narrows the window of opportunity for attackers to exploit a vulnerability, minimizing the scale of potential damage that can be caused by the exploit.
- **Effective risk mitigation:** Timely remediation ensures that potential risks posed by vulnerabilities are addressed before they can be exploited, minimizing the likelihood of data breaches or other security incidents.

- **Enhanced security posture:** By promptly addressing vulnerabilities, organizations can maintain a strong security posture rating and reduce their overall exposure to cyber threats.

## Measuring time to remediation

TTR for an identified vulnerability is calculated by determining the time difference between when a vulnerability is identified within an organization's IT environment and when it is successfully remediated. This information can be tracked using exposure management tools and by maintaining records of remediation activities.




Mean TTR (MTTR) for the organization's security team is computed by determining the sum of TTRs divided by the number of identified vulnerabilities that have been successfully remediated over a specific timeframe.

To put things in perspective using a case study, the average MTTR in the travel service industry is around 60-150 days while the time to exploit for critical vulnerabilities could be within minutes. A reduction in MTTR by over 75% significantly reduces the window of attack for exploits.

## 5 Patching rate

Patching rate measures the total number of security patches that have been applied within a specified timeframe. It provides valuable insights into the effectiveness of an organization's exposure management program and helps identify areas where patching efforts may be lacking.

## The importance of patching rate

Patching is a process of addressing known vulnerabilities in software that have not yet been detected within an organization's IT environment. It is essential for organizations to apply security patches on a regular basis to keep on top of software security updates and safeguard their critical assets.

## Measuring patching rate

Patching rate is typically measured by calculating the number of vulnerabilities that have been remediated through patching divided by the total number of vulnerabilities within an organization's IT environment. This information can be tracked using exposure management tools and by maintaining records of patch deployment activities.

A high patching rate indicates that an organization is effectively addressing vulnerabilities and reducing its overall security risk. However, it is important to note that other factors such as the severity of unpatched vulnerabilities and the timeliness of patch application should also be considered when evaluating patching effectiveness.


# Average vulnerabilities per asset over time

While traditional vulnerability scanning provides valuable insights on vulnerability remediation and patching effectiveness, it can sometimes overlook certain assets or fail to capture the full extent of an organization's vulnerability exposure. To address these limitations, tracking the average number of vulnerabilities per asset over time offers a more comprehensive and holistic measure of security posture.

## The importance of average number of vulnerabilities per asset

Monitoring the average number of vulnerabilities per asset over time provides several critical benefits:

- **Comprehensive security assessment:** Unlike scan results, which may not encompass the entire IT environment, tracking vulnerabilities per asset provides a more comprehensive assessment of an organization's security posture.
- **Trend analysis:** By analyzing trends in vulnerability counts over time, organizations can identify areas of improvement or potential deterioration in their exposure management efforts.

- **Resource allocation optimization:** Understanding the vulnerability distribution across different asset groups can guide resource allocation decisions, ensuring that critical assets receive adequate attention.

### Calculating the average number of vulnerabilities per asset

To determine the average number of vulnerabilities per asset, organizations should consider the following factors:

- **Critical risk vulnerabilities:** Focus on vulnerabilities with critical severity levels, as these pose the most significant risk to the organization.
- **Distinct asset groups:** Categorize assets based on their function, criticality, and risk profile. This allows for a more granular assessment of vulnerability distribution.
- **Exposure duration:** Consider the time period each asset has been exposed to the vulnerability. This provides context for the vulnerability count.

## 7 Remediation results against SLAs

Service level agreements (SLAs) provide a framework for organizations to prioritize and manage vulnerabilities effectively by establishing clear expectations and performance benchmarks for exposure management. Tracking remediation results against SLAs offers valuable insights into the performance of exposure management programs and helps organizations identify areas for improvement in terms of maintaining SLA compliance.

### The importance of remediation results against SLAs

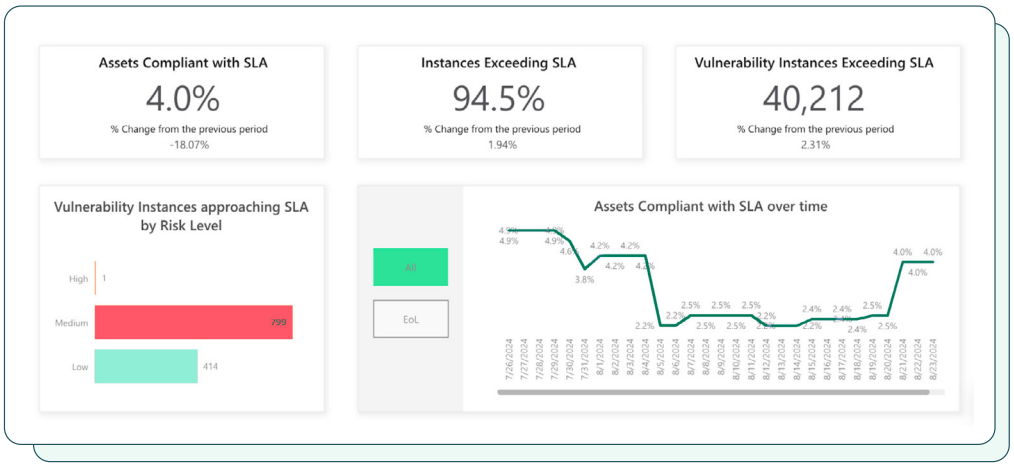
Monitoring remediation results against SLAs provides several critical benefits:

- **Performance benchmark:** SLAs serve as a performance benchmark, allowing organizations to track their progress in remediating vulnerabilities within the agreed-upon timeframes.
- **Prioritization guidance:** By identifying vulnerabilities that are close to breaching or have already breached SLAs, organizations can prioritize remediation efforts accordingly, ensuring that the most critical risks are addressed promptly.
- **SLA compliance monitoring:** Tracking SLA compliance helps organizations maintain adherence to contractual obligations and avoid potential penalties or legal ramifications.

## Measuring remediation results against SLAs

To effectively measure remediation results against SLAs, organizations should track the following metrics:

- **SLA compliance:** Count the number of instances where vulnerabilities were remediated within the specified SLA timeframe.
- **SLA near-breaches:** Identify the number of instances where vulnerabilities were close to breaching the SLA timeframe but were remediated just in time.
- **SLA breaches:** Count the number of instances where vulnerabilities were not remediated within the agreed upon timeframe, indicating a breach of the SLA.




# 8 Asset risks

Exposure management extends beyond simply identifying and remediating vulnerabilities. It encompasses a comprehensive approach to understanding and managing asset-level risks to safeguard an organization's critical infrastructure while optimizing resource allocation in exposure management.

## The importance of asset risk assessment

Asset risk assessment plays a pivotal role in exposure management for several reasons:

- **Prioritization of risk mitigation efforts:** By understanding the potential impact and likelihood of exploitation of vulnerabilities across different assets, organizations can prioritize risk mitigation efforts, ensuring that the most critical assets receive the necessary attention.

- **Resource allocation optimization:** Asset risk assessment guides resource allocation decisions, ensuring that security teams are equipped with the necessary tools and expertise to address the most pressing risks effectively.
- **Informed decision-making:** Asset risk insights help with strategic decision-making, enabling organizations to make informed choices regarding asset acquisition, deployment, and retirement.

## Measuring asset risks

To effectively measure asset risks, organizations should consider the following factors:

- **Custom risk weighting:** Assign custom risk weights to assets based on their business impact, criticality, and sensitivity. This ensures that the most critical assets are prioritized.
- **Admin access control:** Identify the number of users with admin access to each asset. Excessive admin access privileges increase the attack surface and exacerbate risks.
- **Exploit probability inventory:** Maintain an inventory of assets with high exploit probability based on vulnerability scanning results and threat intelligence. This allows for proactive mitigation.

# 9 Number of exceptions granted

Exposure management also includes a strategic approach to evaluating and accepting residual risks based on organizational priorities and resource constraints. Tracking the number of exceptions granted provides valuable insights into an organization's risk tolerance and helps ensure informed decisions are made regarding risk acceptance.

## The importance of monitoring exception granting

Quantifying the number of exceptions granted offers several critical benefits:

- **Risk auditing:** Monitoring exceptions helps audit the potential impact of accepted risks, ensuring that organizations are fully aware of the potential consequences of not remediating certain vulnerabilities.
- **Risk tolerance assessment:** Tracking the frequency of exceptions provides insights into an organization's overall risk tolerance, allowing for a more informed assessment of risk management practices.

- **Resource optimization:** Understanding the rationale behind exceptions granted helps optimize resource allocation, ensuring that security teams are not overburdened with remediating vulnerabilities that pose minimal risks.

## Measuring number of exceptions granted

To effectively measure the number of exceptions granted, organizations should track the following:

- **Exception requests:** Identify and track all instances where exceptions are requested for vulnerability remediation.
- **Exception approvals:** Document and record all instances where exception requests are approved, providing context for risk acceptance decisions.
- **Vulnerability details:** Capture details of the vulnerabilities for which exceptions are granted, including severity, exploitability, and potential impact.


# 10 Vulnerability reopen rate

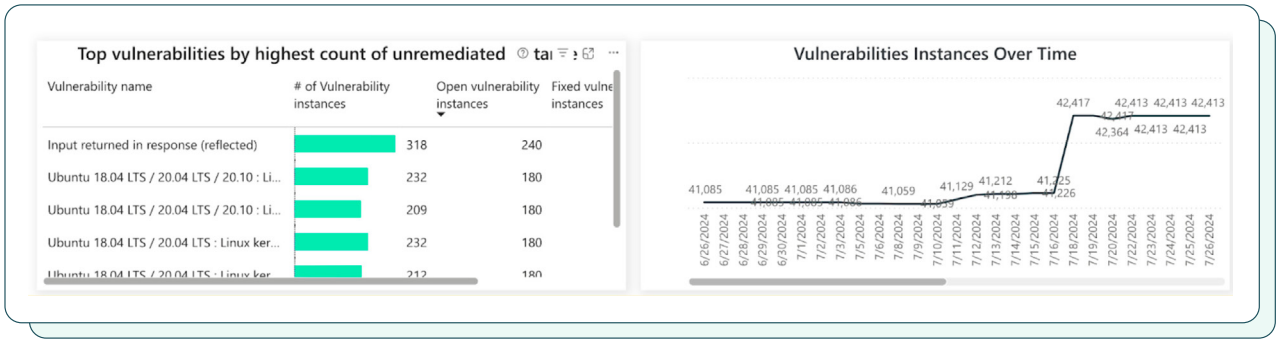
exposure management should also incorporate a holistic approach in ensuring that vulnerabilities are effectively addressed and do not recur. Tracking the vulnerability reopen rate provides valuable insights into the effectiveness of remediation processes on addressing vulnerabilities.

## The importance of reopen rate monitoring

Monitoring the vulnerability reopen rate offers several critical benefits:

- **Remediation effectiveness assessment:** The reopen rate serves as a measure of remediation effectiveness, indicating whether vulnerabilities are being adequately addressed or are recurring due to underlying systemic issues.

- **Root cause analysis:** Analyzing the frequency and patterns of vulnerability reopens can help identify root causes (e.g., configuration flaws or incomplete patching), allowing for targeted remediation efforts.
- **Continuous improvement:** Tracking the reopen rate over time enables organizations to continuously monitor the effectiveness of their remediation processes and make data-driven adjustments to optimize security outcomes.




## Measuring vulnerability reopen rate

To effectively measure the vulnerability reopen rate, organizations should consider the following:

- **Vulnerability reopen tracking:** Identify and track all instances where previously remediated vulnerabilities reappear.
- **Reopening time frame:** Look at the timeframe within which vulnerabilities are considered reopens, ensuring consistency and avoiding misinterpretations.
- **Remediation details:** Document the remediation actions taken for each vulnerability, providing context for reopen occurrences.

# The bottom line: Exposure & vulnerability management metrics

Exposure and vulnerability management metrics are essential for organizations to gauge the effectiveness of their security programs. By systematically tracking key indicators such as scan coverage, time to detection, and vulnerability age, organizations can identify areas for improvement and prioritize their remediation efforts effectively.

This data-driven approach not only strengthens overall security posture but also ensures that critical vulnerabilities are addressed promptly, reducing the risk of cyber threats and safeguarding valuable assets.

# About Vulcan Cyber

The Vulcan Cyber ExposureOS is the one platform for managing exposure risk across IT and cloud-native surfaces. At its core, the platform aggregates and correlates security findings from your infrastructure, code, application, and cloud environments into the exposure data lake. Vulcan Cyber then provides asset risk context, recommendations for the best fixes, and automated remediation workflows to streamline tedious mitigation tasks. Our commitment to innovation has earned recognition as a 2023 Forrester Wave Leader and Omdia RBVM leader. Prominent security teams, such as those at Mandiant and Snowflake, trust Vulcan Cyber to help them own their risk.

**Try Vulcan Free >>**

**Read our blog >>**

**Start owning your risk. See Vulcan Cyber in action >>**