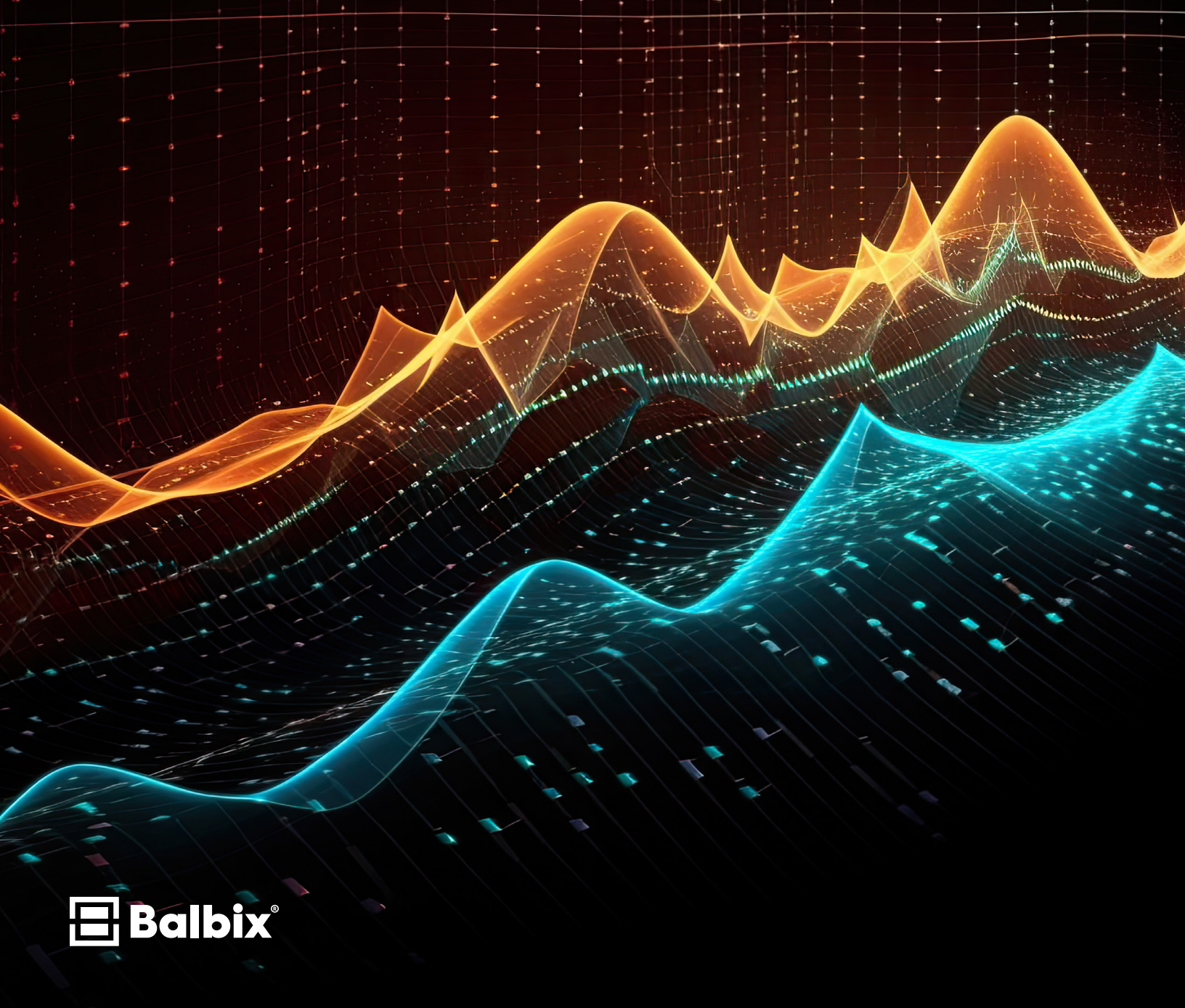
Top 11 Metrics for Building an Effective Vulnerability Management Program



Balbix®

Introduction

Building an effective vulnerability management (VM) program is paramount for safeguarding organizational assets against rapidly evolving threats. Clearly reporting the success of that program to executive staff, meanwhile, ensures the program is recognized as a business enabler, not just another cost center–thereby justifying adequate cybersecurity budget and resources.

Before delving into the top metrics driving VM success, however, it's imperative to note the importance of establishing a solid program foundation rooted in Cyber Risk Quantification (CRQ). Transitioning from the Common Vulnerability Scoring System (CVSS) to CRQ serves as a linchpin in ensuring both cyber resilience and that the metrics we employ accurately reflect the health and efficacy of our vulnerability management initiatives. While CVSS offers insights into vulnerability severity, its limitations in capturing the holistic risk landscape necessitate a shift towards prioritized remediation through CRQ. By factoring in not only the severity of risks but also the potential impact on critical assets, business operations, and financial risk, CRQ empowers organizations to channel resources toward mitigating vulnerabilities that pose the greatest threat.

This strategic alignment not only fortifies overall security posture but also enhances synergy with business objectives, steering organizations towards proactive risk mitigation and resilience in the face of cyber threats. It also enables CISOs to confidently report risk management program success in financial terms that non-technical executive staff can easily understand. Now, let's explore the pivotal metrics that drive success in a CRQ-driven vulnerability management program.

Cyber Risk Management vs. Vulnerability Management

Cyber risk management and VM often get used interchangeably. Cyber risk management encompasses a broad spectrum of activities aimed at identifying, assessing and mitigating risks associated with both cyber threats and vulnerabilities. It involves strategic planning, policy development and implementation of controls to manage and reduce risks across an organization's entire digital ecosystem. Risk management metrics assess the overall effectiveness of an organization's approach to managing cyber risks, which includes vulnerabilities but also encompasses a broader range of factors such as threats, compliance requirements and business impacts. These metrics may include:

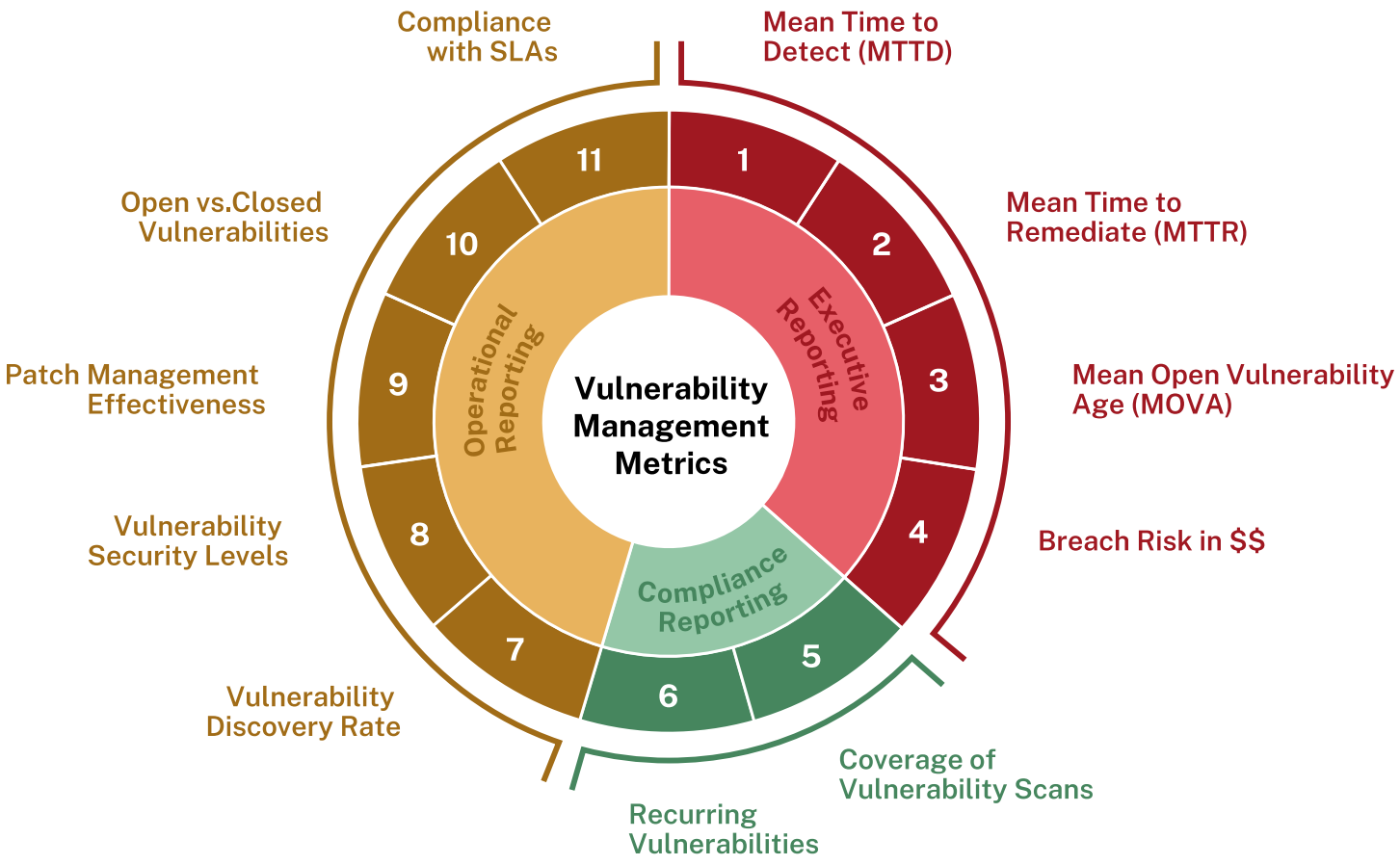
- **Overall Cyber Risk Exposure:** A comprehensive assessment of the organization's exposure to cyber risks, considering vulnerabilities, threats and potential business impacts.
- **Risk Reduction Effectiveness:** The degree to which risk management activities, including vulnerability management, have reduced overall cyber risk over time.
- **Compliance Adherence:** The organization's level of compliance with relevant regulations, standards, and industry best practices related to cybersecurity.
- **Business Impact Analysis:** An evaluation of the potential financial and operational consequences of cyber incidents on the organization's core business functions.

VM, on the other hand, is a subset of cyber risk management focused specifically on identifying and addressing vulnerabilities in an organization's systems, applications, and networks. It involves activities such as vulnerability scanning, assessment, prioritization and remediation to reduce the likelihood and impact of security incidents caused by exploitable weaknesses.

Top 11 Vulnerability Management Metrics

Important metrics to report should ultimately focus on the effectiveness of vulnerability remediation, which is achieved through effective prioritization of vulnerabilities based on their potential financial impact on the business. These can be broken down into key metrics that should be reported to executives, secondary ones to compliance authorities and performance metrics that should be tracked internally by the security team to optimize program success.

These metrics include:



4 Key VM Metrics for Executive Reporting

These are the 3 key success metrics that should be communicated to executive staff to facilitate VM program planning.

1	**Mean Time to Detect (MTTD)**	This metric measures the average time to identify vulnerabilities after their initial discovery or reporting. Rapid detection is crucial for minimizing exposure and mitigating potential risks promptly. MTTD ensures organizations can respond swiftly to emerging threats.
2	**Mean Time to Remediate (MTTR)**	MTTR calculates the average time taken to remediate vulnerabilities after identification. It reflects the agility and effectiveness of the organization's response to vulnerabilities, which is essential for reducing attackers' window of opportunity.
3	**Mean Open Vulnerability Age (MOVA)**	MOVA tracks the age of open vulnerabilities, providing insights into the rate of incoming vulnerabilities and their resolution. This metric enables organizations to prioritize remediation efforts based on the urgency of vulnerabilities, minimizing their exposure to potential exploits.
4	**Breach Risk in $$**	Leveraging Cyber Risk Quantification (CRQ), you should report the potential financial impact of a breach across the entire organization, assess the financial risk for each department or business unit and track the reduction in financial risk over time.

2 Additional VM Metrics for Compliance Reporting

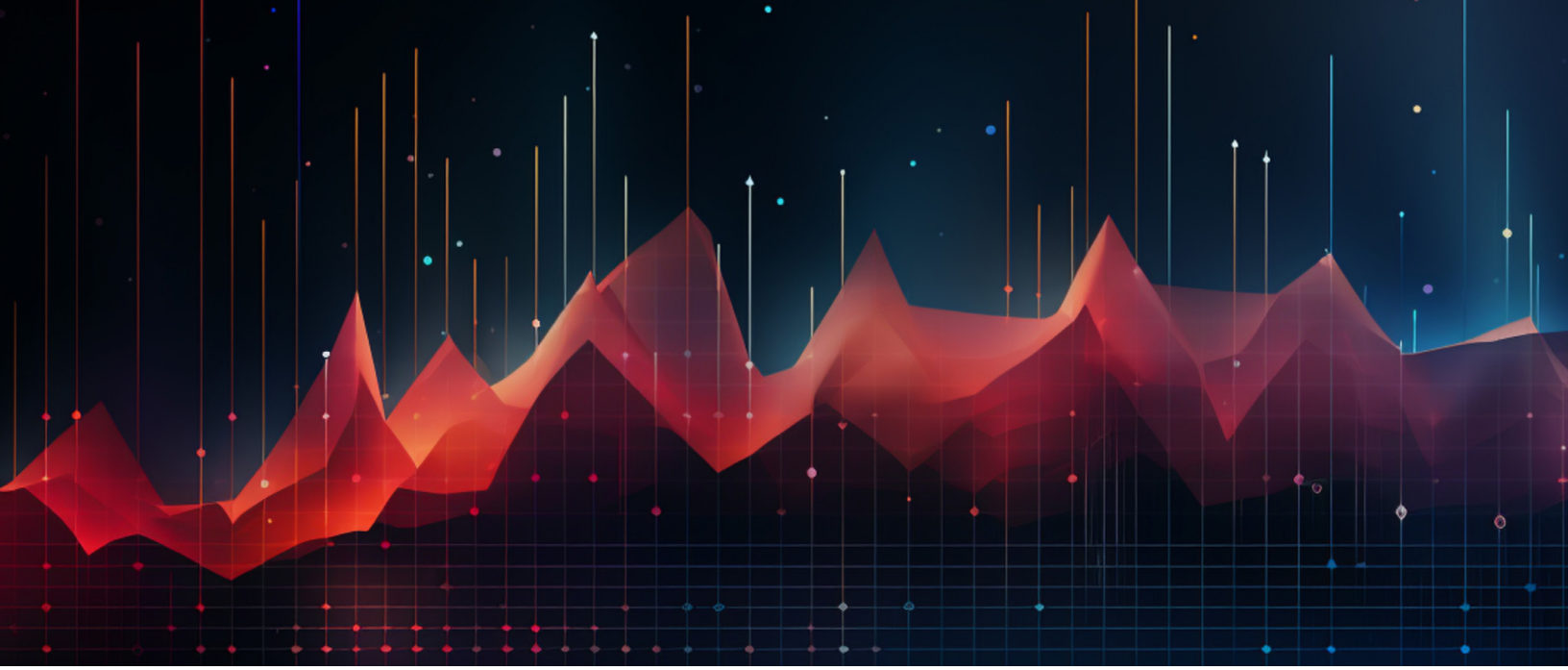
In addition to the 4 metrics presented to executives, the following 2 metrics should be regularly can be used in communications with compliance authorities.

5	**Coverage of Vulnerability Scans**	Assessing the percentage of organizational assets regularly scanned for vulnerabilities ensures comprehensive risk management. High coverage indicates proactive monitoring of the attack surface, reducing the likelihood of overlooking critical vulnerabilities.
6	**Recurring Vulnerabilities**	Identifying and tracking the number of vulnerabilities that reappear after remediation highlights potential issues with patch management or security configurations. Addressing recurring vulnerabilities is crucial for maintaining a resilient security posture and preventing persistent threats.

5 Internal Security Team Metrics to Track

The following 5 metrics are internal to the security team and should be tracked to continuously diagnose problem areas in the VM program.

7 Vulnerability Discovery Rate	Tracking the rate at which new vulnerabilities are discovered provides insights into the VM program's responsiveness. It helps organizations stay proactive in identifying emerging threats and adapting their security measures accordingly.
8 Vulnerability Severity Levels	Monitoring the severity classification of identified vulnerabilities allows for prioritized remediation efforts based on potential impact. However, it's essential to complement severity scores with contextual factors such as asset criticality and threat intelligence feeds to accurately assess the associated risks.
9 Patch Management Effectiveness	Assessing the success rate of patch deployments and timely remediation of vulnerabilities ensures proactive risk mitigation. Effective patch management is critical for addressing known vulnerabilities promptly and reducing the organization's exposure to potential exploits.
10 Open vs. Closed Vulnerabilities	The ratio of open vulnerabilities to resolved ones indicates progress in vulnerability management over time. It reflects the organization's ability to address and remediate vulnerabilities effectively, reducing the overall risk posture.
11 Compliance with SLAs	Monitoring compliance with cybersecurity SLAs ensures timely response to identified risks, reflecting the effectiveness of IT and security teams. High compliance rates indicate prompt vulnerability remediation, enhancing security posture and reducing the window of opportunity for exploitation. It also helps identify resource constraints, enabling proactive optimization of cybersecurity operations to mitigate risks effectively.



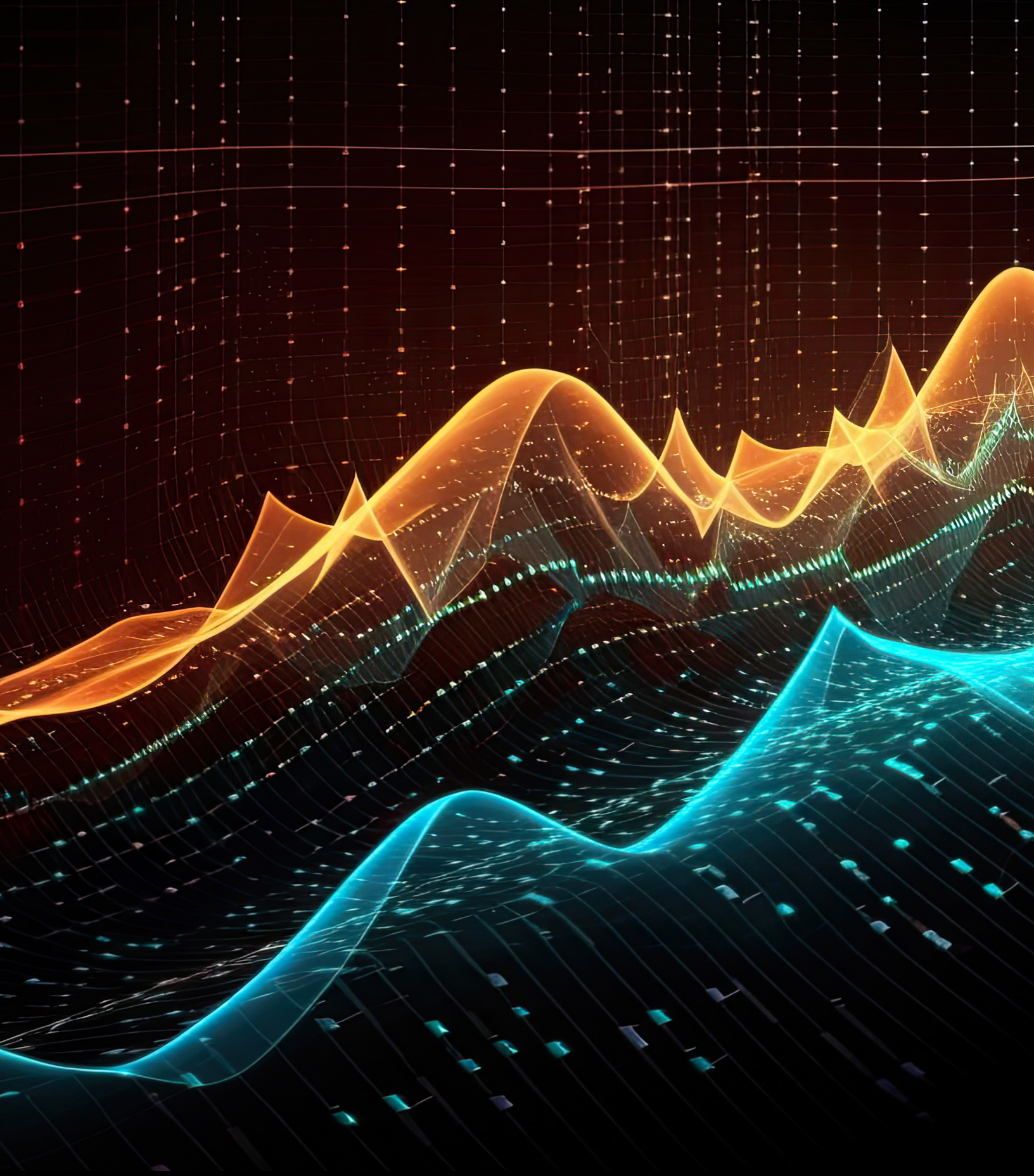
Why These Metrics Matter

Each of these metrics plays a crucial role in assessing and enhancing the effectiveness of a vulnerability management program. TTD and MTTR measure the organization's ability to detect and remediate vulnerabilities promptly, reducing the window of exposure to potential exploits. MOVA helps prioritize remediation efforts based on vulnerability urgency, minimizing risks to the organization's assets.

Coverage of vulnerability scans ensures comprehensive monitoring of the attack surface while tracking recurring vulnerabilities addresses persistent threats. Monitoring the vulnerability discovery rate and severity levels helps organizations stay proactive in identifying and addressing emerging risks.

Effective patch management and compliance with SLAs are essential for proactive risk mitigation and regulatory compliance. Finally, tracking the cost of vulnerability management ensures cost-effective resource allocation and justifies security investments.

In summary, by monitoring these key metrics and embracing comprehensive cyber risk management practices, organizations can strengthen their security posture and mitigate potential threats effectively.



Request a demo to learn more about how Balbix can help you improve your security.

Balbix®