secpod

Mastering MTTR:

Reducing Mean Time to Remediate Risk

www.secpod.com

Introduction

How long is always a question that CISOs and security professionals around the world struggle to answer.

How long to patch that critical risk?
How long will it take to reduce your attack surface?
How long till the organization is fully compliant?

The Mean Time to Remediate (MTTR) Risks is another "how long" question that CISOs ask themselves. It's the time your organization takes to respond and remediate a security risk, and it is a critical metric that quantifies your ability to effectively combat cyber threats.

However, cybersecurity impacts your business, so MTTR is no longer a technical stat. It's a boardroom metric!

What Is Mean Time to Remediate (MTTR)?

Mean Time to Remediate measures the average time it takes from the moment a vulnerability or security issue is discovered to the point where it is fully resolved.

Formula:
MTTR = Total Time to Remediate Issues / Number of Issues Remediated

In here, the 'total time' metric includes:


Identification/Detection


Prioritization


Mitigation or remediation

The idea behind MTTR is to help you understand how long it takes you to respond to security risks and make sensible decisions to improve your security posture.

The Real Cost of Slow Remediation

$1.02 Million	56%	25%
Higher breach cost	Increase in exploited vulns	Increase in remediation cost

Here are three numbers that should jolt you right out of your chair. These are three real-life stats that help us visualize the impact of slow remediation.

Longer remediation -> Higher Breach Cost

According to IBM's 2023 Cost of a Data Breach report, organizations with longer remediation cycles experienced $1.02 million higher breach costs.

Longer remediation -> Higher Chance of Cyberattack

56% of exploited vulnerabilities are weaponized within 7 days of disclosure

Longer Remediation -> Higher Remediation Cost

Remediation delays of even 1 week can increase the work costs by 25%.

The bottom line of slow remediation is that it can be very, very costly! Every delay is an open door for attackers. The higher your MTTR, the bigger the blast radius.

Understanding MTTR & Other Lesser-Known Metrics

While MTTR is a critical metric that provides significant insights into your security and remediation process, here are a few more metrics that will provide additional insights, context, and feedback that'll drastically help you improve your remediation process and enhance your remediation strategy

METRIC	DEFINITION	WHY SHOULD YOU CARE?	WHAT SHOULD THE METRIC BE?
Mean Time to Patch (MTTP)	Time taken to identify a patchable vulnerability and deploy the respective patch	Lower MTTP means you're remediating risks faster with relevant patches.	**The lower the better.**
Remediation Success Rate (RSR)	The percentage of risks was remediated successfully from the total number assigned.	Higher RSR means your team is more effective in patching the newly detected risks.	**The higher the better.**

Why is your MTTR High? Key Factors Affecting MTTR

Your MTTR is most likely high, despite your best intentions and efforts. That's a problem, because every hour a vulnerability stays unaddressed is another hour of risk exposure.

So, what are the key factors that might be affecting your MTTR? Here are the top ones.

Volume of vulnerabilities

The number of vulnerabilities is just too high! In today's threat landscape, this is a totally valid reason: Most of us don't have enough manpower or the right tools to handle the backlog of vulnerabilities and the newly discovered ones. Security teams are buried in alerts, and without effective filtering or prioritization, everything starts looking urgent, even when it's not.

The result? Teams are overwhelmed, and truly critical issues can fall through the cracks or get delayed.

Unclear prioritization of threats

If you try to prioritize all the vulnerabilities, the problems become too difficult to handle and you'll be overwhelmed too easily.
Without proper prioritization, your team can waste precious time chasing low-impact issues while high-risk threats sit unpatched. Lack of a risk-based approach (like CVSS + asset context + threat intelligence) creates confusion and inefficiency and leads to higher MTTR.

Tool Sprawl & Lack of Effective Integration

The problem with tools is that they can become too much, especially when you try to solve each problem with a separate tool.
Most organizations have a mix of tools that were never designed to talk to each other, from scanners and patch managers to ticketing systems and SIEMs. That means your team is probably stuck jumping between dashboards, manually correlating data, or duplicating effort. When tools aren't integrated, the implementation is clunky and slow, causing friction that significantly extends MTTR.

Lack of automation

Manual patching, scanning, ticketing, and any activity in the risk remediation process can lead to lost valuable time and increased MTTR. But that doesn't mean automation is the solution. Controlled automation is. It doesn't just reduce manual efforts; it also ensures consistency, speed, and scalability.

Siloed Teams (IT vs. Security)

Security finds the problems. IT is expected to fix them. But do they talk?
Often, there's a communication gap between security and IT. Security teams detect and report vulnerabilities, but the remediation responsibility lies with IT, which might have different priorities or bandwidth constraints. If there's no shared visibility or workflow, issues bounce around between teams, leading to delays and, in worst-case scenarios, cyberattacks.

5 Golden Strategies to Reduce MTTR

You know 'the what' and you know 'the why'. So, how do you reduce your MTTR?

Build a Centralized Asset Inventory

You can't protect what you don't know exists. One of the biggest hindrances to fast remediation is poor asset visibility. If your security tools don't have a complete and up-to-date view of all endpoints, servers, and cloud workloads, vulnerabilities will slip through unnoticed or get flagged without context.
A centralized, real-time asset inventory with proper tagging (criticality, ownership, environment) allows for better prioritization and faster routing to the right team.

Prioritize by Risk, Not Volume

If you try to prioritize all the vulnerabilities, the problems become too difficult to handle and you'll be overwhelmed too easily.
Without proper prioritization, your team can waste precious time chasing low-impact issues while high-risk threats sit unpatched. Lack of a risk-based approach (like CVSS + asset context + threat intelligence) creates confusion and inefficiency and leads to higher MTTR.

Automate patch management

Manual patching takes time and effort and doesn't scale well with your network. Automating your patching workflows removes unnecessary delays, reduces human error, and speeds up the entire remediation cycle. So, while looking for solutions, choose the ones that integrate scanning, patching, and rollback capabilities, so once a vulnerability is found, it can be fixed without much of a hassle.

Streamline collaboration between teams

Security and IT must work like one team, not two departments constantly fighting each other. However, a major source of friction in remediation is the disconnect between who detects the problem (security) and who fixes it (IT). Connecting your vulnerability management tools with ticketing and task assignment systems ensures that issues are tracked, prioritized, and routed correctly, with full visibility and accountability across both teams. So, teams working closely together.

Establish MTTR SLAs

When remediation timelines are not properly tracked, the team can easily slack off and lose control over the network. Defining clear MTTR SLAs (Service Level Agreements) for different classes of vulnerabilities based on severity or risk will help form a baseline for everyone involved and keep everyone on their toes. For example:

Critical vulns: fix within 24 hours

High: within 3 days

Medium/Low: within 5 days

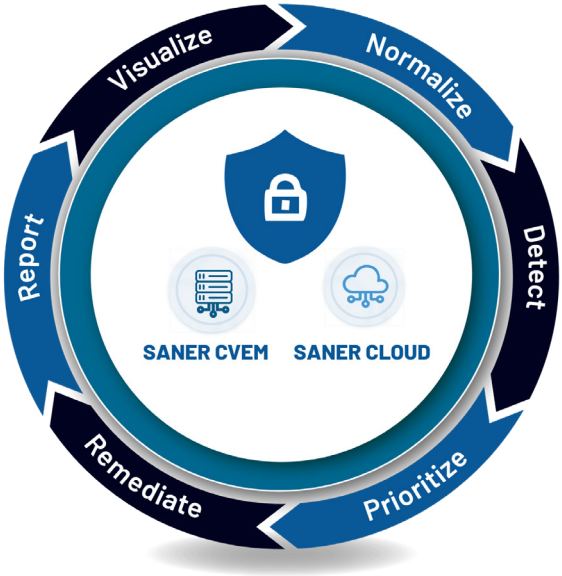
Pair these SLAs with regular reporting and dashboards to keep everyone aligned and accountable.

Enhancing Your Technology Stack for Lower MTTR

A key reason why your MTTR is high is the tools you use. Improving your MTTR begins by improving your technology stack and aiding your team in combating risks proactively before they turn into threats. Look for tools that provide:

- **Comprehensive visibility**
- **Real-time risk detection**
- **Automated remediation workflows**
- **Patch management integration**
- **Compliance alignment**
- **Customizable risk scoring and prioritization**

Tools like Saner Platform integrate risk detection, assessment, and remediation, automate the process, making the entire risk remediation process streamlined, effective and quick.



Business-Centric Approach to MTTR

Reducing Mean Time to Remediate (MTTR) isn't just about patching faster—it's about protecting the entire business from disruption, damage, and loss. Your upper management needs to understand MTTR as a security KPI and a business risk mitigation metric.
Here are five different ways MTTR can impact your business:

Reduced breach exposure

The longer a vulnerability stays unpatched, the greater the risk of exploitation. Reducing MTTR shrinks your attack surface and lowers the chances of breaches, ransomware, and costly compliance failures.

Improved customer trust

Customer trust depends on how quickly you respond to risks, and a low MTTR shows resilience and builds confidence with customers, partners, and stakeholders. It shows you care!

Regulatory compliance

Nobody likes compliance audits, but they matter a lot. Regulations like GDPR, HIPAA, and PCI-DSS demand timely remediation of security issues. A low MTTR supports compliance, while delays can lead to fines, audit failures, and reputational risk.

Lower remediation costs

Preventing a cyberattack is much cheaper than recovering from one. Money talks, and your management would rather save millions of dollars by investing in preventive security than spend time and money recovering from a cyberattack. By leveraging MTTR as a supporting metric, you can make remediation costs much lower.

Conclusion

MTTR matters. It could just be a simple number, but numbers never lie and can instantly unravel their impact.

With the world moving more and more towards an AI-driven era, threat actors have an edge over us, and they will take every advantage they get to breach organizations and create havoc. So, what do we all do?

Reacting to these threats hasn't worked so far. **So, prevention is the only way forward.**

Preventing cyberattacks begins with a change in the way we handle IT security. Preventing cyberattacks begins with you changing the way you approach risks.
So, will you prevent? Or react?

About SecPod

SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preemptively block cyber threats. The platform includes:
SANER CLOUD – An AI-fortified Cloud-Native Application Protection Platform (CNAPP) that delivers continuous visibility, security compliance, and risk mitigation for cloud environments.
SANER CVEM – A Continuous Vulnerability and Exposure Management (CVEM) solution that delivers continuous visibility, identifies, assesses, and remediates vulnerabilities across enterprise devices and network infrastructure.

With its suite of cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

FROST & SULLIVAN
GLOBAL VULNERABILITY MANAGEMENT
ENTREPRENEURIAL COMPANY OF THE YEAR AWARD
2023

GIGAOM RADAR REPORT
LEADER
2024
PATCH MANAGEMENT

G2 rating 4.5

Gartner Peer Insights
4.4

High Performer
Best Est. ROI
2024
High Performer
Easiest Setup
Users Most Likely To Recommend
Momentum Leader
2024

www.secpod.com | info@secpod.com