8 ways to reduce your Mean Time to Remediate (MTTR)

BY ANNA HAMMOND · JULY 10, 2024 · LAST UPDATED ON MARCH 6, 2025

When a potential threat emerges, organizations must act quickly. Yet despite this urgency, response times often lag, leaving systems vulnerable to attacks. Globally, 75% of organizations take longer than 24 hours to respond to a vulnerability disclosure, according to Intigriti research. The consequences of slow responses can be severe, ranging from data breaches to significant financial losses and damage to an organization's reputation.

To mitigate security breaches, it is imperative for organizations to adopt a proactive stance in securing their IT environments. For Managed Service Providers (MSPs) and IT professionals, this means implementing best practices for vulnerability remediation timelines. These practices are crucial not only for the timely remediation of vulnerabilities but also for protecting IT assets and the data they hold. By establishing practical time frames for addressing these vulnerabilities, businesses can enhance their responsiveness and resilience against threats. Ultimately, a swift Mean Time to Resolution (MTTR) is not just a target; it's a necessity in ensuring the security and continuity of business operations.

In this guide, we'll cover the meaning of MTTR in security operations and give ten easy-to-apply tips for speeding up incident response, mitigation and remediation.

What is vulnerability remediation?

Vulnerability remediation is a critical component of cybersecurity, focusing on safeguarding the integrity and security of digital environments. This process involves several key steps: identifying vulnerabilities, repairing them, and ensuring they are patched to prevent future exploits. By understanding the scope and definition of vulnerability remediation, organizations can better protect themselves against potential cyber threats.

Vulnerability remediation scope

Vulnerabilities can exist in various forms across all digital assets, including software applications, operating systems, networks, and hardware devices. Vulnerability remediation extends beyond just fixing software bugs. It also covers securing network configurations, strengthening user authentication processes, and ensuring that all digital assets are compliant with current security standards and practices. This holistic approach ensures that potential entry points for hackers are minimized.

Detection and correction

The first step in vulnerability remediation is detection. This involves using automated tools and manual techniques to scan systems for known vulnerabilities. These tools compare current system configurations and software versions against a database of known issues and alert administrators to any matches.

Popular scanning tools include Nessus, known for its comprehensive network scans, and Qualys, which offers cloud-based global asset visibility. OpenVAS provides free, open-source scanning, while Burp Suite focuses on web application testing. Metasploit allows for penetration testing by simulating attacks, and Acunetix specializes in detecting web application vulnerabilities. Wireshark analyzes network traffic for unusual activity, and Nmap is used for network mapping and security scanning.

Patching and prevention

Once vulnerabilities are identified, the next step is correction. This may involve applying patches provided by software vendors, making configuration changes, or even replacing outdated or unsupported hardware and software. Each remediation action depends on the severity of the vulnerability and the potential impact of an exploit on the organization.

After addressing the immediate vulnerabilities, the focus shifts to prevention through regular updates and patches. Patch management is a critical aspect of vulnerability remediation that involves keeping all software and systems up to date with the latest security patches. This not only fixes known vulnerabilities but also helps to protect against new threats and recently discovered vulnerabilities.

Mean Time to Remediation (MTTR) meaning

Mean Time to Remediation (MTTR) is a key performance indicator in IT and cybersecurity, and relevant to multiple industries. It measures the average time required to resolve an issue from the moment it is reported until the problem is completely resolved. MTTR is crucial for assessing the efficiency of service and support teams in managing and rectifying issues, directly impacting system reliability and customer satisfaction.

Broader interpretations of MTTR

MTTR can be interpreted in several ways, depending on the context:

1. **Mean Time to Respond:** This variation of MTTR measures the time it takes for a team to initially respond to an issue. It is crucial in customer service and IT support roles, where a quick response can significantly impact the perception of service quality.

2. **Mean Time to Recover:** Often used in the context of IT and network operations, this metric focuses on the time it takes to recover from hardware or software failures that lead to downtime. Reducing MTTR in this context is vital for minimizing disruptions and maintaining operational continuity.

3. **Mean Time to Resolve:** This is the traditional interpretation of MTTR, encompassing the complete cycle from the identification of an issue to its final resolution. It includes diagnosis, intervention, testing, and confirmation that the problem has been fully resolved.

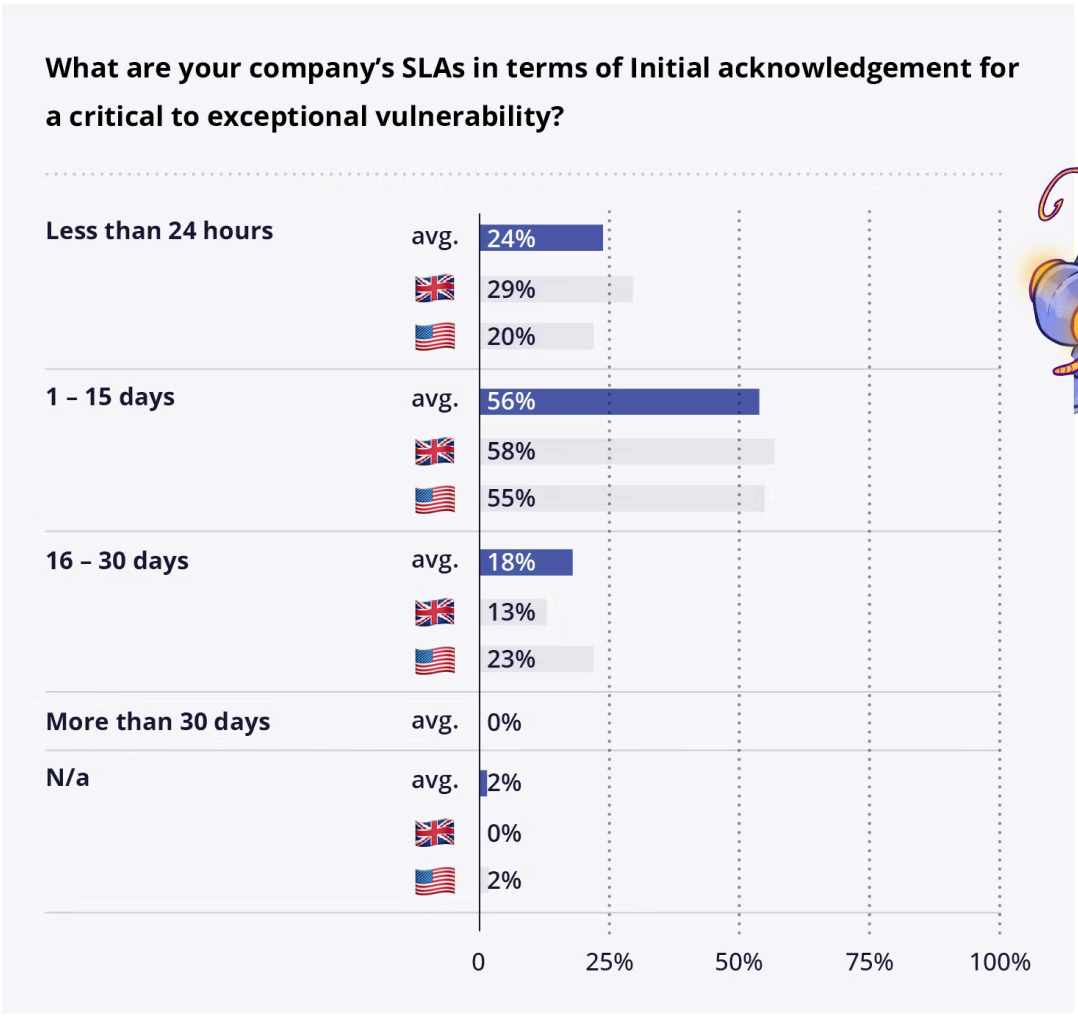
In practice, MTTR helps organizations identify areas needing improvement in their response processes and service delivery. By analyzing MTTR, companies can better understand their operational effectiveness, pinpoint bottlenecks, and implement strategies to enhance their service levels. Whether it's speeding up responses, reducing recovery times, or streamlining resolutions, improving MTTR can lead to more efficient operations and higher customer satisfaction.

MTTR industry standards and benchmarks

A lower MTTR is generally preferred, with benchmarks often set by regulatory requirements or best-practice frameworks. For instance, critical IT systems might aim for an MTTR of a few hours, while less critical systems could tolerate longer downtimes.

Average response time for critical vulnerabilities

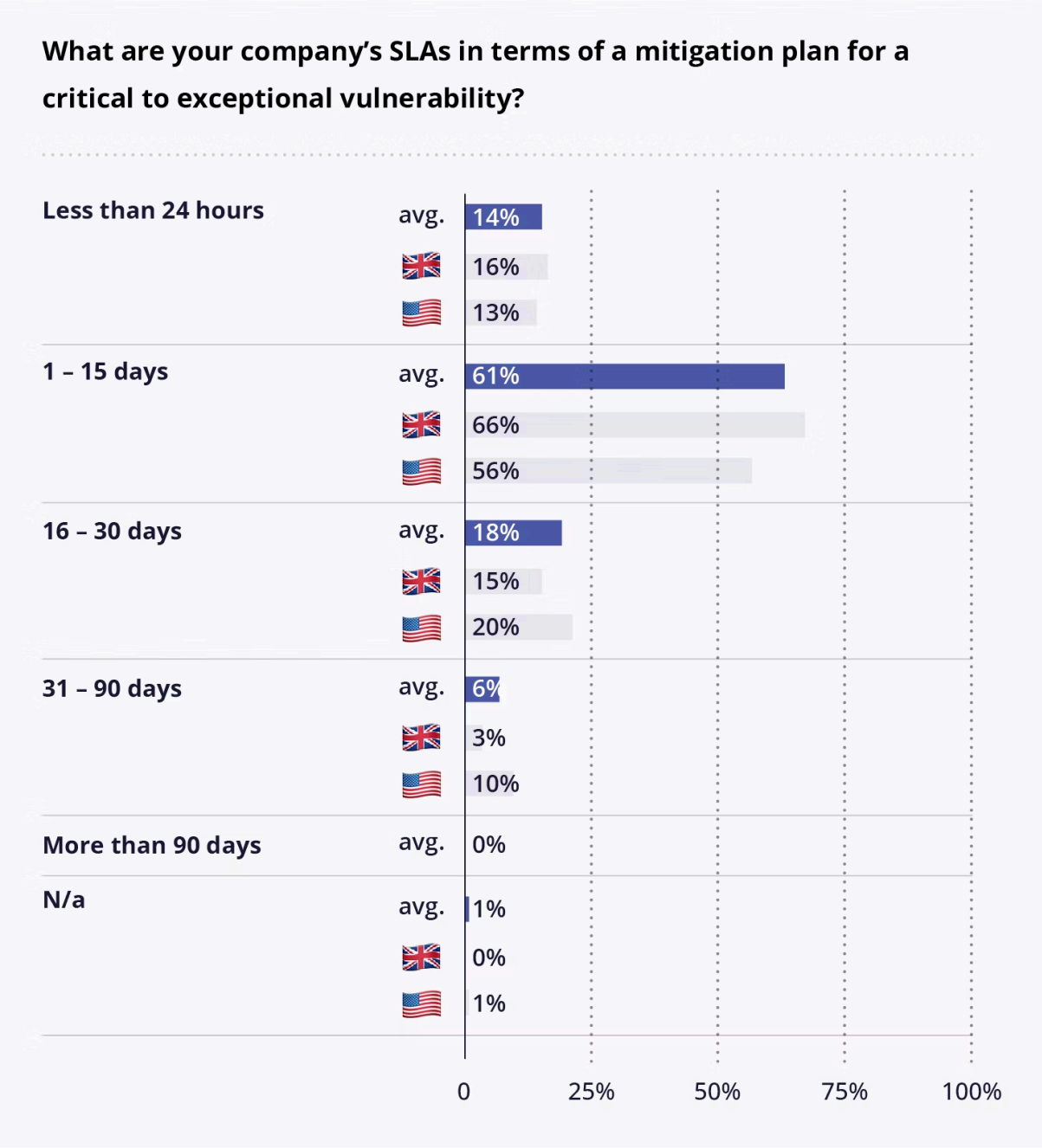
Despite this need for urgency, globally, 75% of businesses fail to respond to critical vulnerabilities within 24 hours—consequences could include customer dissatisfaction, loss of business, and reputational damage. In the UK, 29% respond within 24 hours, compared to 20% in the US.



Initial acknowledgement response rates

Average mitigation timeline for critical vulnerabilities

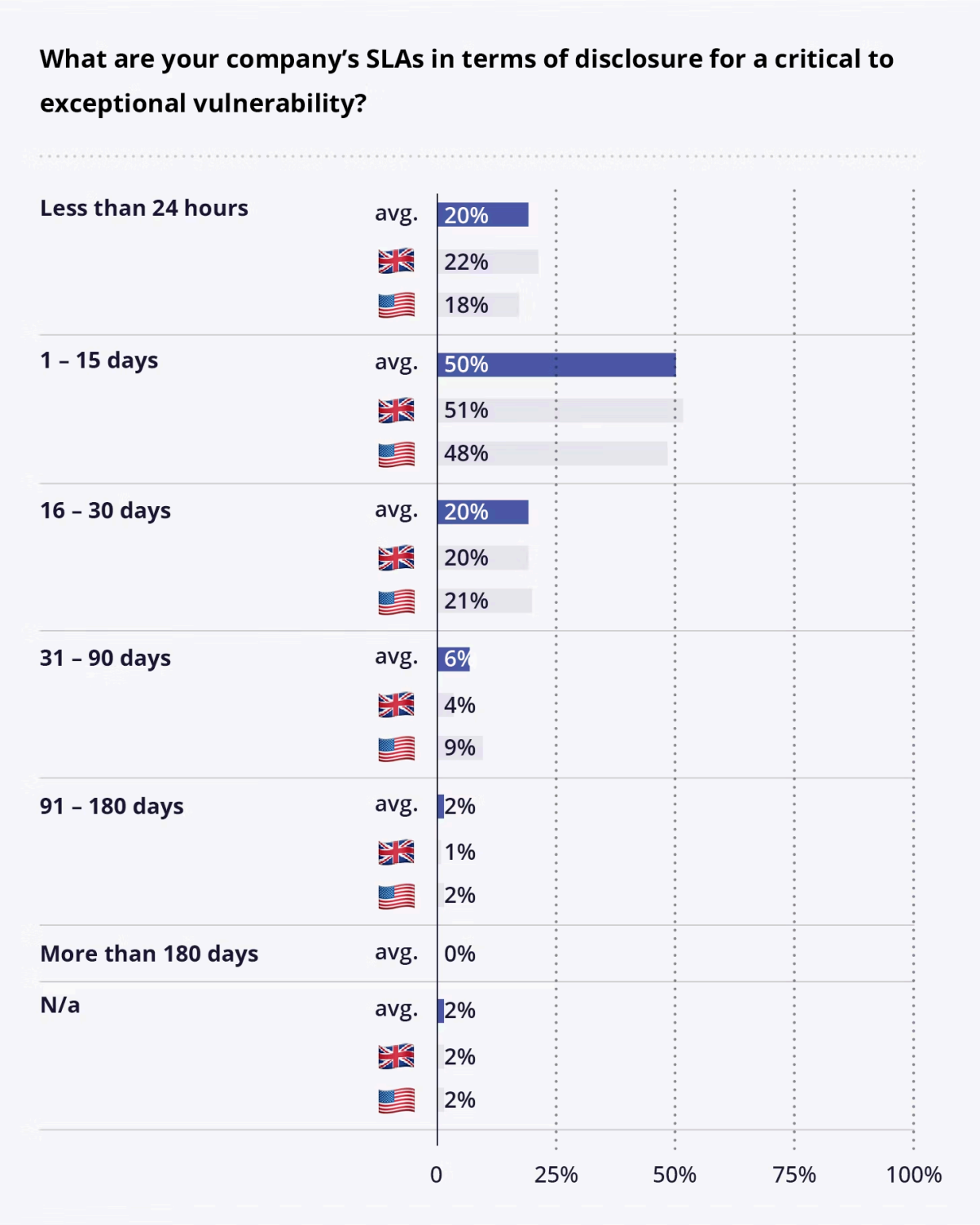
More UK respondents (82%) aim to resolve a critical to exceptional vulnerability within 15 days (about 2 weeks) compared to the US (69%).



Average mitigation timelines

Average vulnerability disclosure timeline for critical vulnerabilities

The UK is faster at vulnerability disclosure, with 73% disclosing a vulnerability within 15 days (about 2 weeks) versus 66% in the US.



Average disclosure timelines

How to speed up mean time to remediation

Speeding up the Mean Time to Remediation (MTTR) not only enhances security but also boosts customer trust and compliance with industry standards. Here are 10 effective strategies to accelerate MTTR in your organization.

1. Keep track of IT assets

An accurate inventory of all IT assets is crucial for effective vulnerability management. Knowing what assets you have and their security status helps in prioritizing actions during a security incident. This comprehensive visibility is key to reducing MTTR as it allows for quicker identification and resolution of vulnerabilities.

2. Establish a structured vulnerability management process

A structured vulnerability management process is essential for efficiently dealing with security threats. The four key steps include:

- **Locate and identify vulnerabilities:** Use automated tools and regular assessments to continuously identify vulnerabilities across all IT assets.
- **Evaluate, monitor, and remediate:** Assess the risk associated with each vulnerability, apply necessary patches or fixes, and monitor the environment to ensure that the remediation is effective.
- **Confirm and communicate:** Once a vulnerability is remediated, verify the resolution and communicate the outcome to relevant stakeholders to maintain transparency and accountability.
- **Prioritize vulnerabilities:** Not all vulnerabilities pose the same risk. Prioritizing them based on their severity and exploitability helps in allocating resources where they are needed most, thus reducing the window of opportunity for attackers.

3. Shift relevant security responsibilities to your developers

Empowering development teams by shifting certain security responsibilities to them can significantly reduce MTTR. Training developers to recognize and remediate the most common vulnerabilities in their projects ensures that many security issues are resolved at the development stage itself. This not only speeds up the resolution process but also embeds security into the product lifecycle from the outset.

4. Create a vulnerability disclosure policy

A well-defined Vulnerability Disclosure Policy (VDP) encourages ethical reporting of potential security issues. By clearly stating how to report vulnerabilities, what response reporters can expect, and the legal protections provided, organizations can foster a cooperative relationship with the security research community, leading to faster and more effective resolutions.

5. Leverage automation

Implementing automation for routine and time-consuming tasks can free up valuable time for security teams to focus on more critical issues. Automated tools can handle tasks such as vulnerability scanning and patch management efficiently. According to an IBM report, companies that have deployed security AI and automation incur significantly lower costs from breaches compared to those without—an average of nearly $1.8 million lower in fact.

6. Perform regular audits and assessments of security vulnerabilities

Conducting regular audits and assessments is fundamental in identifying and addressing security vulnerabilities before they can be exploited. These proactive measures help organizations understand their current security posture and implement timely improvements. Regular vulnerability assessments enable teams to detect new threats and update their security measures accordingly.

7. Implement proactive testing solutions

Engaging in proactive security testing through bug bounty programs, penetration testing, and hybrid approaches can identify and mitigate vulnerabilities before they are exploited in the wild. These programs simulate real-world attacks and provide valuable insights into the effectiveness of the current security measures, allowing for timely improvements.

8. Focus on vulnerability remediation, reporting, and evaluation

Maintaining detailed reports on how vulnerabilities were handled and evaluating the effectiveness of the remediation process is important for continuous improvement. These reports should include timelines, actions taken, and parties involved. This documentation is vital for auditing purposes and for refining the vulnerability management strategy.

Reducing your MTTR—and how Intigriti can help

Reducing MTTR is a multifaceted approach that involves enhancing the capabilities of development teams, leveraging automation, establishing robust vulnerability management processes, and maintaining clear communication and documentation. By implementing these strategies, organizations can not only speed up their response to security incidents but also improve their overall security posture, ultimately leading to reduced costs and enhanced trust among customers and stakeholders.

Intigriti is the trusted leader in crowdsourced security and bug bounty programs. Established in 2016, we enable major global entities like Coca-Cola, Microsoft, and Intel to proactively pinpoint and tackle security vulnerabilities before they're exploited by cybercriminals. Through our platform, security teams are better able to:

- **Identify:** With a robust network of over 100,000 researchers, organizations can quickly surface security weaknesses, preventing potentially damaging breaches.
- **Validate:** Through our triaging process, we remove the burden of validating submissions from security teams so that they can stay focused on essential issues and assess severity faster.
- **Streamline:** Integrate with Intigriti's API for seamless data exchange, link with Jira for issue tracking, and set up real-time alerts in Slack to speed up remediation.
- **Evaluate:** Utilize platform statistics to track key metrics like the number of submissions and identified vulnerabilities, demonstrating the value of your team's work.

To learn more about how Intigriti's platform can help speed up your MTTR, speak to one of our advisors today.

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com