12 incident response metrics your business should be tracking

BY ANNA HAMMOND · OCTOBER 17, 2024 · LAST UPDATED ON NOVEMBER 13, 2025

If there's a vulnerability in your systems that cybercriminals could exploit, you'll want to know about it. Collaborating with people outside your organization to alert you to these issues can be extremely powerful because it allows your business to discover vulnerabilities before malicious hackers do. This approach, known as vulnerability disclosure, requires clear reporting channels and swift incident response.

Incident response metrics enable organization's to get an accurate picture of their ability to handle cybersecurity incidents. In this guide, we'll identify 12 data points that will help your security team identify bottlenecks, optimize workflow, and ensure continuous improvement.

Why use metrics to measure incident response?

Measuring the efficiency with which your security team responds and processes reported vulnerabilities is vital. The faster an incident is identified and mitigated, the less time attackers have to exploit vulnerabilities, exfiltrate data, or cause damage.

Metrics provide an objective insight into your team's performance, highlighting areas of strength and opportunities for improvement. Armed with this information, security leaders can make data-driven decisions on where and how to allocate resources and budget. Regularly reviewing these metrics allows security teams to track progress, celebrate successes, and adjust strategies as needed.

Incident response metrics are also essential for demonstrating the value of your team's work to senior leadership teams and other departments. They offer a clear and concise way to report on the team's activities and the organization's security posture. Security teams can build trust and secure buy-in for their initiatives by demonstrating improvements in response times and incident outcomes.

12 incident response metrics to monitor

Below, we've highlighted 12 incident response metrics that typically work well with security goals. Regularly tracking and improving upon these metrics helps organizations enhance their overall security posture and reduce the impact of incidents. While we've provided several options, select the metrics that fit best with your team's objectives, ensuring they plug into your organization's wider business goals, too.

1. Mean Time to Detect (MTTD)

Mean Time to Detect (MTTD) is the average time taken to identify a security incident or breach. It measures the efficiency of an organization's monitoring and detection capabilities. MTTD is crucial because the faster an incident is detected, the quicker the response can be initiated, minimizing potential damage.

- **What to aim for:** A lower MTTD indicates that the security team is effectively using tools and processes to identify threats as quickly as possible.
- **How to calculate MTTD:** This metric is typically calculated by averaging the detection times of all incidents over a specific period.

2. Mean Time to Acknowledge (MTTA)

Mean Time to Acknowledge (MTTA) is the average time a security team takes to confirm and respond to a detected incident. It measures the responsiveness and readiness of the team. MTTA is crucial because a swift acknowledgment enables a faster response, reducing the potential impact of an incident. Factors influencing MTTA include alerting mechanisms, team availability, and internal communication protocols.

- **What to aim for:** A lower MTTA indicates that the team is effectively managing alerts and prepared to handle incidents promptly.
- **How to calculate MTTA:** This metric is typically calculated by averaging the acknowledgment times of all incidents over a specific period.

3. Mean Time to Contain (MTTC)

Mean Time to Contain (MTTC) is the average time taken to isolate and prevent the spread of a security incident or threat after it has been detected. It measures the swiftness and effectiveness of an organization's incident response process. Prompt containment limits the potential damage and reduces the overall impact of an incident.

- **What to aim for:** A lower MTTC indicates that the response team is efficiently containing threats, minimizing the risk of further compromise.
- **How to calculate MTTC:** This metric is typically calculated by averaging the containment times of all incidents over a specific period.

4. Mean Time to Respond (MTTR)

Mean Time to Respond (MTTR) is the average time taken to contain and remediate a security incident after it has been detected. It measures the efficiency of an organization's incident response processes. Of course, a faster response time reduces potential downtime and the window of opportunity for hackers to exploit the vulnerability. Factors that might impact MTTR include the team's expertise, the availability of response tools and resources, and the complexity of the incidents.

- **What to aim for:** A lower MTTR indicates that the security team effectively manages incidents and minimizes their impact.
- **How to calculate MTTR:** This metric is typically calculated by averaging the response times of all incidents over a specific period.

5. Mean Time to Patch (MTTP)

Mean Time to Patch (MTTP) is the average time taken to apply a security patch or update after a vulnerability is identified. It measures the efficiency of an organization's patch management process. Prompt patching reduces the window of opportunity for attackers to exploit known vulnerabilities. How

quickly an incident is patched depends on the complexity of the process, the availability of patches, and the organization's policies and procedures.

- **What to aim for:** A lower MTTP indicates that the organization proactively manages vulnerabilities and minimizes risk.
- **How to calculate MTTP:** This metric is typically calculated by averaging the time taken to patch all identified vulnerabilities over a specific period.

6. Mean Time to Resolve (MTTR)

Mean Time to Resolve (MTTR) is the average time taken to fully address and close an incident, from detection to resolution—also known as Mean Time to Remediate. It measures the overall effectiveness of an organization's incident management process. MTTR is a vital metric because it encompasses the entire incident lifecycle, including detection, response, and recovery.

Factors influencing MTTR include the complexity of incidents, the team's expertise, the availability of resources, and the effectiveness of incident management policies and procedures.

- **What to aim for:** A lower MTTR indicates that the team efficiently handles incidents, minimizing downtime and potential damage.
- **How to calculate MTTR:** This metric is typically calculated by averaging the total resolution times of all incidents over a specific period.

7. Mean Time to Recovery (MTTR)

Mean Time to Recovery (MTTR) is the average time taken to restore a system or service to full functionality after an incident or failure. It measures the efficiency of an organization's recovery processes. MTTR helps organizations understand the impact of downtime and the effectiveness of recovery strategies.

- **What to aim for:** A lower MTTR indicates that the organization is quickly restoring services, minimizing disruptions and potential losses.
- **How to calculate MTTR:** It is typically calculated by averaging the recovery times of all incidents over a specific period.

8. System availability

System availability is a metric that measures the percentage of time a system or service is operational and accessible to users within a given timeframe. It indicates the reliability and uptime of a system, reflecting its ability to perform its intended function when needed.

Regularly monitoring and optimizing system availability helps organizations proactively identify and address potential issues, ensuring consistent and dependable service delivery.

- **What to aim for:** System availability is typically expressed as a percentage, with 100% signifying that the system is always available.
- **How to calculate system availability:** It is calculated using the formula: (Total Time - Downtime) / Total Time * 100.

9. Mean Time Between Failures (MTBF)

Mean Time Between Failures (MTBF) is another metric that measures the average time a system or component operates without failing. It is a key indicator of a system's reliability and stability. This metric helps predict system downtime, plan maintenance activities, and assess the system's overall health.

- **What to aim for:** A higher MTBF indicates that the system is more reliable and experiences fewer failures.
- **How to calculate MTBF:** MTBF is calculated by dividing the total operational time by the number of failures within a specific period.

10. Service-level agreement (SLA) compliance

Service-level agreement (SLA) compliance measures how well an organization meets the agreed-upon service standards with its customers or users. Alternatively, it can be used in the context of third parties. It indicates the percentage of time services are delivered within the promised parameters, such as availability, response time, and resolution time.

Regularly monitoring and reporting SLA compliance helps identify areas for improvement, optimize resource allocation, and drive operational excellence. Failure to meet SLAs can result in penalties, damaged reputation, and lost business.

- **What to aim for:** Organizations should aim for high SLA compliance rates above 95% to ensure customer satisfaction and maintain trust.
- **How to calculate SLA compliance:** To calculate SLA compliance, divide the number of incidents resolved within the agreed SLA timeframes by the total number of incidents, then multiply by 100 to get a percentage. For example, if 95 out of 100 incidents are resolved within the SLA, the compliance rate is 95%.

11. Incidents over time

Incidents over time is a metric that tracks the number of incidents occurring within specific time intervals, providing a historical perspective on operational performance. It helps organizations identify trends, peak periods, and recurring issues, enabling proactive incident management.

By analyzing incidents over time, teams can better allocate resources, plan for future demand, and measure the impact of improvement initiatives. Regular review of this metric supports continuous service enhancement and improved overall operational stability.

- **What to aim for:** Organizations should aim to see a decreasing or stable trend in this metric, as an increasing trend may indicate underlying systemic issues or ineffective incident management processes.
- **How to measure incidents over time:** To calculate incidents over time, count the number of incidents within a defined time frame (e.g., daily, weekly, monthly) and plot these counts over time.

12. Issue classification analysis

Issue classification is more of an analysis than a metric— it is a process that categorizes incidents based on their type, impact, or other relevant criteria to facilitate efficient response and resolution. Regular

tracking of this data point can reveal trends, identify recurring problems, and highlight areas that need attention or investment.

Common classification criteria include the affected service or system, the severity of the impact, the urgency of resolution, and the underlying cause of the issue. By understanding the distribution of incident types, teams can prioritize resources, refine response strategies, and drive targeted improvements to enhance overall service reliability.

- **What to aim for:** Organizations should have a comprehensive and consistent classification scheme covering all potential incident types.
- **How to measure issue classification:** To calculate issue classification, incidents are tagged or labeled according to categories such as hardware failure, software bug, user error, or network outage. The number of incidents in each category is then tracked over time.

How Intigriti can help speed up these metrics

Intigriti empowers global organizations to proactively identify and address vulnerabilities through crowdsourced security, preventing costly security breaches. Together with our ethical hacking community, we help organizations like Coca-Cola, Microsoft, and Intel to pinpoint unknown vulnerabilities in their systems, speeding up remediation and reducing risk. Through the platform, organizations are better able to:

- **Discover:** Organizations mitigate missing an unknown vulnerability through crowdsourced security testing, preventing potentially devastating breaches.
- **Verify:** Our triaging process alleviates the burden of validating submissions from security teams, allowing them to focus on essential issues and assess severity more quickly.
- **Optimize:** Integrate with Intigriti's API for seamless data exchange, connect with Jira for issue tracking, and set up real-time alerts in Slack to accelerate remediation.
- **Assess:** Leverage platform statistics to monitor key metrics and trends such as MTTA, incidents over time and issue classification, showcasing the impact of your team's efforts.

To find out how Intigriti's platform can help improve your organization's incident response performance, speak with one of our advisors today.