INTRODUCTION TO MTTD: MEAN TIME TO DETECT

DevOps teams rely on data-driven insights to establish and maintain an efficient SDLC pipeline. A variety of IT incident metrics support evaluating the performance evaluation of your IT infrastructure overall as well as individual IT incidents. The challenge for ITOps and service desks centers around identifying the most meaningful metrics, especially those that contribute to minimizing the impact of IT incidents on end users.

In this article, we will discuss mean time to detect, a metric focused on finding IT incidents faster, regardless of the issue resolution capacity and performance. Both DevOps and ITOps teams can utilize MTTD.

What is mean time to detect?

A key performance indicator (KPI) within IT incident management, mean time to detect (MTTD) refers to the average time passed between the onset of an IT incident and its discovery.

MTTD can be calculated mathematically with the following formula:

$$MTTD = \frac{Sum\ of\ Incident\ Detection\ Times}{Number\ of\ Incidents}$$

Though calculating the MTTD mathematically is simple, it does require an accurate knowledge of the start time of IT incidents. This may require an evaluation of historical infrastructure KPI data. Take the average of time passed between the start and actual discovery of multiple IT incidents. These calculations can be performed across different periods

(e.g., daily, weekly, or quarterly) to evaluate changes in MTTD performance over time.

Mean time to detect is one of several metrics that support system reliability and availability

MTTD for effective incident management

Incident management comes down not merely to detecting incidents, but to determining what incidents may impact end-user performance or your revenue stream. Incidents that do not affect performance and revenue earning are likely prioritized. MTTD can help you track both:

- Numerous infrastructure metrics, not a single one, should report **revenue-impacting incidents**. That's a good thing, but it has some failings: the vast volume of log metrics generated at every IT means there's a lot of noise. IT teams using traditional ITSM tooling may struggle to identify IT issues proactively.
- End users also help identify IT incidents when they report **performance-impacting incidents** such as service outages, disruptions, or other performance issues. If the underlying incidents are not already known or visible to your team, the types and scale of end-user reports might indicate a discrepancy around your incident management methods and/or an inadequacy of your monitoring solutions to recognize the issues proactively.

Addressing these two MTTD-related issues can be both technical and strategic in nature:

- DevOps may need reevaluate how they define the impact tolerance of an incident.
- IT may need to invest in technology solutions capable of producing granular insights using the log metrics big data. Some ITSM event tools are capable of correlating information from multiple sources of IT incident information in order to identify hidden patterns of insights.

Uncovering these can help you identify a significant IT incident *before* it makes its impact on performance and revenue. Once an IT incident is recognized as higher priority, DevOps teams can follow pre-designed issue resolution protocols to address issues based on priority and impact on SDLC performance.

MTTD best practices

Improving MTTD offers DevOps teams the opportunity to address IT incidents before the impact reaches end users or slows down the SDLC process. Even for lower-priority incidents that may not require immediate resolution, ITOps can gather accurate incident-related information.

Many service disruptions trigger a chain of IT incidents across multiple infrastructure nodes. At each node, an individual IT incident may not present sufficient risk to warrant corrective measures. By improving the MTTD, however, ITOps can expand its scope of evaluating of IT incidents and infrastructure nodes to a proactive measure that reduces large-scale service disruptions.

In this context—proactive, preventative incident management—the following MTTD best practices can be useful:

Strategize

Like any single metric, MTTD alone will not provide an adequate picture of infrastructure performance. Similarly, not all incidents are the same: you must account for the varied nature of IT

incidents when evaluating MTTD performance. Being strategic allows DevOps teams to better invest in resources that enhance incident monitoring and management.

In a DevOps environment, strategy also requires a lean approach to ITSM. Instead of following a fixed set of protocols to account for IT incident management relative to MTTD, you'll need a broader ITSM perspective. ITOps must observe the cause and effect of IT changes *before* targeting improved or relaxed MTTD targets across the spectrum of IT incidents.

Skill your people

Despite the complex nature of IT infrastructure and the sophistication of IT incident monitoring solutions, human error continues to play a significant role in inaccurate MTTD metrics.

- Considering the vast insights drawn from the monitoring tools, **your ITOps team** requires deep understanding of the technologies and ITSM processes related to the variety of IT incidents that occur. Your ITSM tooling may flag incidents—often overwhelmingly—therefore your ITOps team should be equipped with the human knowledge, expertise, and skills to extract the right information about incidents that may result to impactful service disruptions.
- Human errors or lack of awareness may also account for inaccurate or insufficient MTTD information. Especially when measurements must be taken manually, **your service technician** must act diligently to log the necessary measurements periodically.
- Finally, **your IT service desk** must also respond proactively to incident reports and end user complaints. A streamlined service desk process is critical for ITOps to discover IT incidents reported by end users that may have otherwise gone under the radar.

Automate and codify

Though automation is the heart of DevOps, it should just as critically be applied to the IT incident management process, particularly around incident detection and resolution. (If automation isn't possible or able to offer full visibility, your ITOps team must develop and utilize a systematic approach for incident detection.)

The clarity that results from automating incident detection and management offers several benefits:

- Makes it easier for ITOps to codify appropriate ITSM processes.
- Helps ITOps maintain an accurate documentation of the incident logs and the actions taken at various value thresholds of the KPI metrics.
- Promotes flexible, agile environments. When the issue detection and resolution processes fall out of alignment with strategic ITSM and DevOps objectives, ITOps can simply adjust the coded parameters.
- Keeps consistent data collection and reporting even as the requirements of IT teams changes.

Detection first, resolution next

The next step of improving the ITSM process is resolving issues using the service desk metric mean time to resolve (MTTR).

BMC Blogs has many resources on IT metrics. Browse our Enterprise IT Glossary or see these articles:

- Mean Time to Resolve (MTTR) as a Service Desk Metric
- MTTR Explained: Repair vs Recovery in a Digitized Environment
- MTBF vs. MTTF vs. MTTR: Defining Failure for IT and Data Center Environments