

MTTD and MTTR

Two numbers decide how much a security incident costs you: how fast you spot it, and how fast you stop it. Here is what mean time to detect and mean time to respond mean, and the one habit that keeps both low.

WHAT IT IS

MTTD, mean time to detect, is the average time an incident runs before anyone notices it. MTTR, mean time to respond, is the average time from that moment to acting on it. The gap between them is where damage happens. An attacker who sits unseen for weeks has time to move between systems and copy data before a single control reacts, so slow detection and response is now a financial and legal exposure, not a technical footnote.

WHY IT MATTERS

241 days

The global average breach lifecycle in 2025, 181 days to detect and 60 to contain.

IBM Cost of a Data Breach, 2025

76 days

How long attackers sat inside Equifax unseen, because a monitoring certificate had quietly expired.

GAO, 2018

43 days

Median time to fix the internet-facing device flaws attackers exploit first.

Verizon DBIR, 2026

WHAT HAPPENED

In 2013 Target's security tools detected the malware stealing payment-card data and raised repeated high-priority alerts. No one acted on them. Target learned it had been breached about two weeks later, from the US Department of Justice, after roughly 40 million payment cards and the personal data of up to 70 million customers had been taken. Fast detection bought nothing because the response never started. (US Senate, 2014)

RED FLAGS TO WATCH FOR

You rarely have a slow-detection problem until an incident proves it. Watch for these signs first.

- You cannot say what your MTTD or MTTR is right now.
- Alerts pile up overnight with no one staffed to act on them.
- Your MTTR mixes respond, resolve and recover into one vague number.
- You report averages, so one long incident hides the typical case.
- No one checks that detection tooling is actually working.

THE ONE RULE THAT STOPS IT

Treat a detection as unfinished until someone has acted on it. Make sure every alert reaches a person who can respond, day and night.

THEN BUILD THE HABIT AROUND IT

- Centralise and continuously monitor your logs, so detection has something to see.
- Automate the first containment step for the clearest detections.
- Keep tested offline backups so recovery does not depend on luck.
- Track detection, response and recovery separately, by severity, using medians.

MYTHS AND FACTS

MYTH

MTTD and MTTR are the same thing.

FACT

MTTD measures time to detect an incident. MTTR measures time to respond or recover after it. They are tracked separately and both matter.

MYTH

A low MTTR means you are secure.

FACT

A fast MTTR that only means you close tickets quickly is a vanity metric. Speed without accuracy and containment can hide real risk.

MYTH

Detection tools alone shrink MTTD.

FACT

Target and Equifax both had detection tools. Tools only help when alerts are actioned and the tooling is actually working.

THE LEGAL DUTY

Under Cybersäkerhetslagen, in force since 15 January 2026, a significant incident must reach MCF (formerly MSB) as an early warning within 24 hours and a full notification within 72. You cannot report in hours what you detect in weeks, and boards are personally accountable under Article 20.

GET HELP

eBuilder Security provides managed detection and response and Sweden-based security awareness training to help your team keep MTTD and MTTR low. Read the full guide at the link below.

[Read the Full Article →](#)