RAPID7

Defining KPIs for Security Operations

What metrics support your story and drive decisions? You need to develop and maintain a starting set of metrics and/or key performance indicators (KPIs) that can be evaluated along a maturity scale, even as your tools may evolve. You'll establish targets, follow trends, and measure progress. In general, three consecutive reporting periods in the wrong direction – or one trend the business considers "significant" in just one reporting period – should lead to corrective action.

But which KPIs are the right ones to measure? You'll want to focus on those aspects of your security program that the business can provide the resources, time, and money to improve. Here's a range of choices to keep in mind when you're reporting on performance:

Number and disposition of security incidents Gives stakeholders insight into the risk they face. You have no direct control of this but it may help explain life in your security operation.

Incidents detected vs. reported Reveals the health of your security culture. If there are a large number of attempts (successful or not) and few reports, that would signify an issue.

Mean time-to-detect (MTTD) Gives insight into both efficacy of tools and coverage of data (is the detection coming from a reported incident vs. a tool, etc.). It goes hand-in-hand with MTTA (mean time-to-acknowledge), which is a good indicator of how well your processes are working and the workload of your team.

Mean time-to-acknowledge (MTTA) Tells how long it takes for someone to look at an alert and begin the process of triage and investigation. Your argument for resources often starts here.

Mean time-to-respond (MTTR) Similar to MTTD above, this also gives insight into your ability to respond, and whether your tools and processes meet your threats and use cases.

Mean time-to-remediate (MTTR) Pertains to vulnerability management and can be a measure of the time it takes to resolve or patch a vulnerability or misconfiguration. Measurement can start from the time a report or request is sent to a remediation team and end when the successive/next scan comes back clean.

The 1/10/60 rule A cybersecurity standard for minimizing damage: 1 minute to detect, 10 to acknowledge, 60 to investigate. How often are you meeting this standard?

Cost-per-incident Gives insight into efficiency of process, tooling, and also potential staffing shortcomings (like the number of people or specific skills).

Number of tools required to detect and respond This is a data quality metric: Does your tooling produce a high number of alerts which have low fidelity? Require a lot of investigation? Produce a lot of false positives? The results of this metric may suggest a need for consolidation.

Employee turnover Are you losing key talent to burnout, and having to spend extra budget and time hiring and training? Is turnover trending the right or wrong way?

Mean time-between-failures (MTBF) A good metric, but more IT-related than security-focused, unless those failures are related to security incidents (DDoS or other resource exhaustion attacks), in which case they may be important to track.

Want more? Check out how you can measure and report on security KPIs with Rapid7 Managed Threat Complete and Cloud Risk Complete.