You can't improve what you don't measure. To mature your security operations program, you need to evaluate its effectiveness. But this is a task many organizations still struggle with. If showing the effectiveness of your security operations is a challenge, it might be time to re-evaluate your KPIs and your ability to measure them.

Why Measure Your Security Operations Effectiveness?

Lack of clear KPIs has been a problem for many organizations. The fact is, you might not be doing as well as you'd like. But, if you reduce the dwell time of a cyberthreat, you could save the day.

A 2018 Mandiant report indicated threat actors are present on victims' networks for a median of 101 DAYS before being detected.1

77% of organizations were compromised during a 12-month period.2

When dwell time is confined to seven days, the impact is reduced by 77%.

3 If shortened to just one day, business impact is reduced by as much as 96%.3

7 Metrics to Improve Your Team's Effectiveness

You're likely already tracking mean time to detect (MTTD) and mean time to respond (MTTR). These are the critical indicators of your operational effectiveness. Reducing MTTD and MTTR is the primary goal of a resilient security operations program.

But are you measuring the effectiveness of your team through each stage of Threat Lifecycle Management?

By baselining your team's capabilities at this level, you can easily see how you can reduce your MTTD and MTTR.

Critical KPIs for Evaluating Security Operations Effectiveness

Like any core business operation, mature organizations will want to measure operational effectiveness to identify where KPIs can be improved or are not being measured. Following are some of the key operational metrics that allow enterprises to measure their operational effectiveness by process and by team:

- **Alarm Time to Qualify (TTQ)**
- **Alarm Time to Triage (TTT)**
- **Alarm Time to Mitigate (TTM)**
- **Time to Mitigate (TTM)**
- **Time to Recover (TTV)**
- **Incident Time to Detect (TTD)**
- **Incident Time to Response (TTR)**
- **Threat Time to Investigate (TTI)**
- **Workflow Metrics**

The following figure shows the key workflow metrics that should be measured to ultimately identify performance gaps and both maximize the operational efficiency of your teams and also increase the likelihood of the successful TLM technological solution.

Critical KPIs for Evaluating Security Operations Effectiveness

Learn How LogRhythm Can Help

With a simple definition of the workflow of your security operations program, the embedded metrics help teams uncover opportunities to improve operational efficiency, reduce risk exposure, and demonstrate the value of your security operations program. For more information, please contact us.

Want to see it in action? Schedule a demo today.