# 7 Metrics of Security Operations Effectiveness

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?

**The fact is, you might not be doing as well as you'd like.**

*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]

**But, if you reduce the dwell time of a cyberthreat, you could save the day.**

*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]

And, measuring the effectiveness of your SOC will help you focus your efforts on the areas where improvements will provide the highest gains.

Last but not least, visualizing your progress can help you prove the value of your program to your board.

## 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 whether KPIs and SLAs are being realized. Following are some of the key operational metrics that allow enterprises to measure and communicate to the business current organizational and operational effectiveness when it comes to being able to detect and respond to cyber-related threats.

### Alarm Time to Triage (TTT)

**= Date/Time Alarm Inspection - Date/Time of Alarm Creation**

Measures latency in your team's ability to inspect an alarm

### Alarm Time to Qualify (TTQ)

**= Date/Time of Alarm Closure or Addition to Case - Date/Time of Alarm Creation**

Measures the time it takes your team to fully inspect and qualify an alarm

### Threat Time to Investigate (TTI)

**= Date/Time of Case Closed or Elevated to Incident - Date/Time of Case Creation**

Measures the time it takes your team to investigate a qualified threat

### Time to Mitigate (TTM)

**= Date/Time Incident Mitigated - Date/Time Incident Determination**

Measures the time it takes your team to mitigate an incident and eliminate immediate risk to your business

### Time to Recover (TTV)

**= Date/Time of Recovery from Incident - Date/Time of Incident Mitigation**

Measures the time it takes your team to complete full recovery of an incident

### Incident Time to Detect (TTD)

**= Date/Time Threat Qualified for Investigation/Case Creation - Date/Time of Initial Indicator of Threat**

Measures the time it takes your team to confirm and qualify an incident

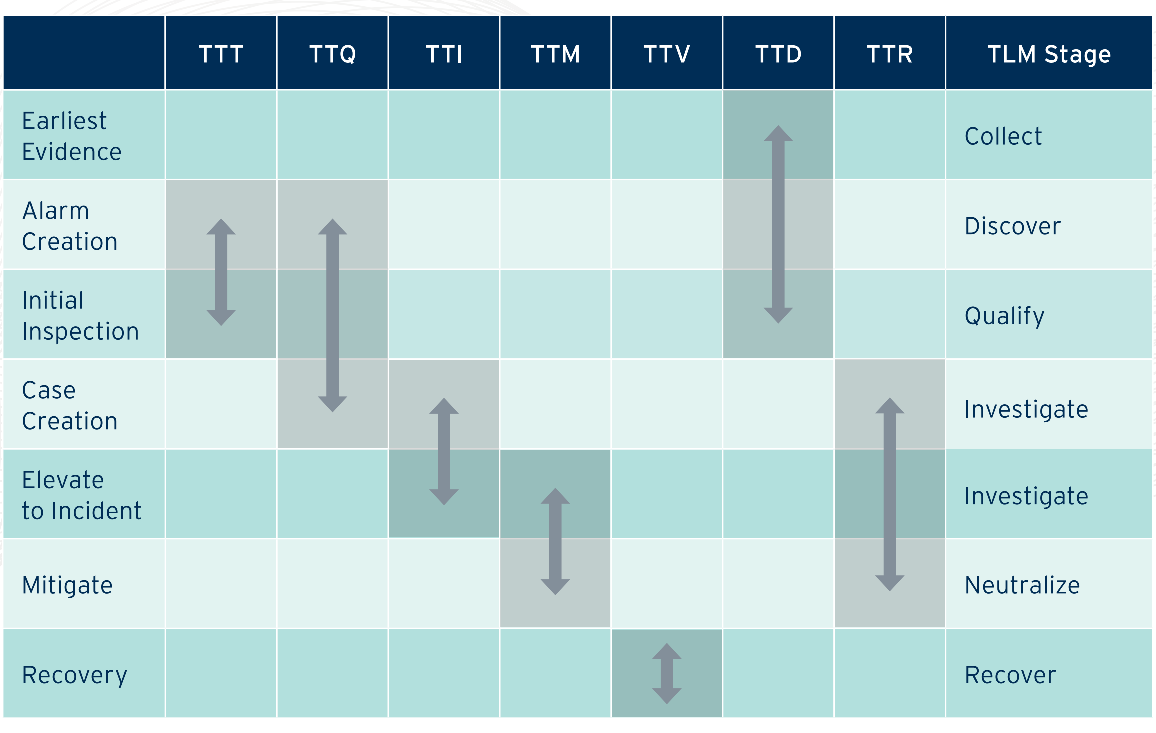
### Incident Time to Response (TTR)

**= Date/Time of Incident Mitigation - Date/Time Initiation of Investigation**

Measures the time it takes your team to investigate and mitigate a confirmed incident

## Workflow Metrics

The following figure shows the key workflow metrics that should be measured to ultimately determine TLM operational effectiveness, and effectiveness of the supporting TLM technological solution.



|  | TTT | TTQ | TTI | TTM | TTV | TTD | TTR | TLM Stage |
|---|---|---|---|---|---|---|---|---|
| Earliest Evidence |  |  |  |  |  | ↑ |  | Collect |
| Alarm Creation | ↑ | ↑ |  |  |  | │ |  | Discover |
| Initial Inspection | ↓ | │ |  |  |  | ↓ |  | Qualify |
| Case Creation |  | ↓ | ↑ |  |  |  | ↑ | Investigate |
| Elevate to Incident |  |  | ↓ | ↑ |  |  | │ | Investigate |
| Mitigate |  |  |  | ↓ |  |  | ↓ | Neutralize |
| Recovery |  |  |  |  | ↕ |  |  | Recover |

## Ready to experience the MRK difference?

MRK provides traditional MSSP services for monitors and alerts by utilizing the industry-leading LogRhythm cybersecurity suite. However, our efforts extend well beyond the typical "copy and paste" generic approach of other providers. MRK is committed to providing best in class results by fully running out an alert - correlating all available log sources and investigating and running to ground every available detail.

This differentiator provides actionable alerts with details on remediation, containment and response. We provide detailed communication that minimizes your internal team's effort and provides an expedited path to resolution - no copy and paste tickets, no alerts without context.

Want to see it in action?

Schedule a demo today

[1] M-Trends 2018, FireEye Inc., April 2018 // [2] 2018 CyberEdge Defense Report, CyberEdge Group, March 2018
[3] Quantifying the Value of Time in Cyber-Threat Detection and Response, Aberdeen Group, February 2016