white paper

7 Metrics to Measure the Effectiveness of Your Security Operations

LogRhythm

Introduction

You can't improve what you don't measure. To mature your security operations center (SOC) and security operations program, you need to evaluate its effectiveness. But measuring your security operations program effectiveness isn't an easy task.

If showing the effectiveness of your security operations (SecOps) is a challenge, it might be time to re-evaluate your KPIs and your ability to measure them.

Why Measure Your Security Operations Effectiveness?

If you apply security metrics to your security program, you will enable your organization to make wiser decisions and demonstrate value to the board and other stakeholders.

The problem is that the most companies aren't far along in their security maturity. In a survey of more than 250 security operations practitioners, one in five respondents claimed they had mature security operations.[1]

The remaining 80 percent said they were just starting their journey or were only halfway through it.[2]

Where do you stand with your security operations capabilities?

It's can be difficult to know the state of your security operations without having measurable goals. If you start by reducing your dwell time of a cyberthreat, you may very well save the day.

A 2020 Mandiant report indicated that the median amount of time an attacker was present in a victim's network was **56 DAYS** before being detected.[3]

This represents a **28% DECREASE** in dwell time from 2018.[4]

While dwell time measurements improved, you still must be vigilant with your cybersecurity and security maturity efforts.

[1] *The Road to Security Operations Maturity: A Cyentia Institute Research Report, Siemplify, June 2019*

[2] *IBID*

[3] *M-Trends 2020, FireEye Mandiant Services Special Report, FireEye, Feb. 20, 2020*

[4] *IBID*

stc

Improve Your Team's Effectiveness

How do you get started? If you aren't already, the first set of metrics you should be tracking is mean time to detect (MTTD) and mean time to respond (MTTR). These are the critical indicators of your operational effectiveness. These metrics support the success of your security operations program.

Reducing MTTD and MTTR is the primary goal of a resilient security operations program. MTTD allows you to track the time it takes to discover a possible threat. This metric helps you understand the effectiveness of your organization's security tools and your team's speed to detect a threat. The goal is to keep this metric as low as possible to minimize the impact on your organization.

Meanwhile, MTTR helps you measure the time it takes to remediate and respond to a threat. The higher your response time, the greater your chances are for a costly breach or damage. As with MTTD, the goals are to reduce your response time and lower your risk.

While MTTD and MTTR are important metrics to measure to baseline your team's capabilities, it's crucial to track the effectiveness of your team as your organization's maturity increases.

Like any core business operation, if you're interested in maturing your organization, you should measure operational effectiveness to identify whether your organization is realizing its KPIs and SLAs.

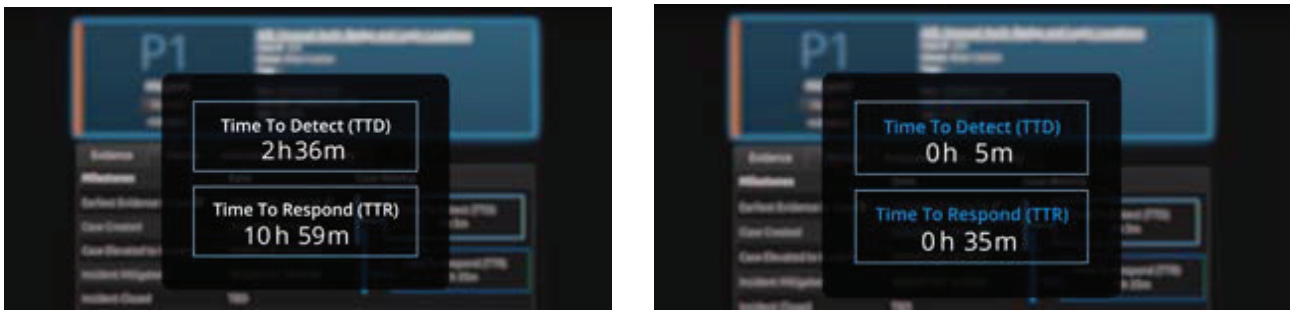

Figure 1: By understanding your MTTD and MTTR, you can lower your risk to cyberthreats and improve your security effectiveness

white paper

7 key metrics for security operations success

Beyond MTTD and MTTR, there are other metrics you should track to ensure that you're effectively communicating organizational and operational effectiveness to cyberthreats. This e-Book suggests seven metrics you should measure that can help you visualize improvements to your security operations program.

1. Alarm Time to Triage (TTT)

Alarm Time to Triage (TTT) measures latency in the team's ability to immediately inspect an alarm. It helps you understand the level of real-time responsiveness to threats.

This metric:

- Measures within alarm priority bands (e.g., high/medium/low, risk score bands, etc.)
- Might indicate the team can take on additional monitoring load (e.g., monitoring another area of the IT infrastructure)
- Might indicate a need for increased staff, or for the team to narrow its monitoring focus (e.g., focusing only on highest- risk areas of the IT infrastructure and ignoring others)

Alarm Time to Triage (TTT)

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

2. Alarm Time to Qualify (TTQ)

Alarm Time to Qualify (TTQ) measures the amount of time it took an alarm to be fully inspected and qualified. TTQ helps you identify bottlenecks and understand your team's capacity for qualifying threats.

This metric:

- Should be measurable/reportable within alarm priority bands (e.g., high/medium/low, risk score bands, etc.)
- Should be measurable/reportable within alarm outcome (e.g., false positive, benign issue, incident, etc.)
- Might indicate weakness in the technological security operations solution in the area of alarm drill down, search, data analysis, and contextual analysis

Alarm Time to Qualify (TTQ)

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

LogRhythm®

3. Threat Time to Investigate (TTI)

Threat Time to Investigate (TTI) measures the amount of time it took to fully investigate a qualified threat. It helps you identify bottlenecks and understand the team's capacity for investigating threats.

This metric:

- Should be measurable/reportable based on threat/incident types (e.g., via the MITRE ATT&CK® categories)
- Might indicate slowness in the technology security operations solution in the area of search, data analysis, contextual analysis, and collaboration

Threat Time to Investigate (TTI)

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

4. Time to Mitigate (TTM)

Time to Mitigate (TTM) measures the amount of time it took to mitigate an incident and remove the immediate risk to the business. TTM helps you understand how quickly your team can mitigate the issue to stop or slow down an active threat.

This metric:

- Should be measurable/reportable based on threat/incident types (e.g., via the MITRE ATT&CK categories)
- Might indicate slowness in the technology solution in the area of evidence capture and use, standard playbooks, automation, and collaboration

Time to Mitigate (TTM)

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

5. Time to Recover (TTV)

Time to Recover (TTV) measures the amount of time it took to recover fully from an incident. Measuring TTV helps you understand how quickly your security team and other involved groups can completely recover from an incident. It can identify operational and collaboration bottlenecks.

This metric:

- Should be measurable/reportable based on threat/incident types (e.g., via the MITRE ATT&CK categories)
- Might indicate slowness/weakness in the technology security operations solution in evidence capture and use, standard playbooks, automation, and collaboration

Time to Recover (TTV)

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

6. Incident Time to Detect (TTD)

Incident Time to Detect (TTD) measures the amount of time it took to confirm an incident was initially detected and ultimately qualified. TTD is a key measure of security operations effectiveness that shows the amount of time it took to identify threats that actually resulted in an incident.

This metric:

- Should be measurable/reportable based on threat/incident types (e.g., via the MITRE ATT&CK categories)
- Should be measurable/reportable based on threat detection method (e.g., hunting, behavioral analytics, scenario analytics, specific threat detection technology, etc.)
- Might indicate slowness/weakness in the technology solution in the areas supporting threat discovery (e.g., threat hunting, behavioral anomaly detection) and workflow capabilities supporting threat qualification (e.g., search, data analysis)

Threat Time to Investigate (TTI)

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

7. Incident Time to Response(TTR)

Incident Time to Response (TTR) measures the amount of time it took to investigate and mitigate a confirmed incident. TTR is a key measure of security operations effectiveness that shows the amount of time it took to analyze and mitigate threats that actually resulted in an incident.

This metric:

- Should be measurable/reportable based on threat/incident types (e.g., via the MITRE ATT&CK categories)
- Might indicate slowness/weakness in the technology solution in the areas supporting threat investigation (e.g., search) and mitigation (e.g., automation)

Incident Time to Recover (TTR)

= Date/Time of Incident Mitigation - Date/Time Initiated of Investigation

Conclusion

To show the value of your security program, you need to set a baseline and then track your progress in improving your efficiency over time. That's where measurement comes in. The first step is to determine which metrics you should track and measure. As your organization matures, metrics will help you better understand how your security operations program is performing and where you can improve. Metrics can also help you prove the program's value to the board.

With LogRhythm, measuring the effectiveness of your SOC is easy. Our embedded SOC metrics can help your team uncover opportunities to improve operational efficiency, including identifying tasks better suited for automation, and enable you to measure and report on the effectiveness of your security program.

About LogRhythm

LogRhythm empowers more than 4,000 customers across the globe to measurably mature their security operations program. LogRhythm's award-winning NextGen SIEM Platform delivers comprehensive security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralization of threats.

Built by security professionals for security professionals, LogRhythm enables security professionals at leading organizations like Cargill, NASA, and XcelEnergy to promote visibility for their cybersecurity program and reduce risk to their organization each and every day. LogRhythm is the only provider to earn the Gartner Peer Insights' Customer Choice for SIEM designation three years in a row. To learn more, please visit logrhythm.com.