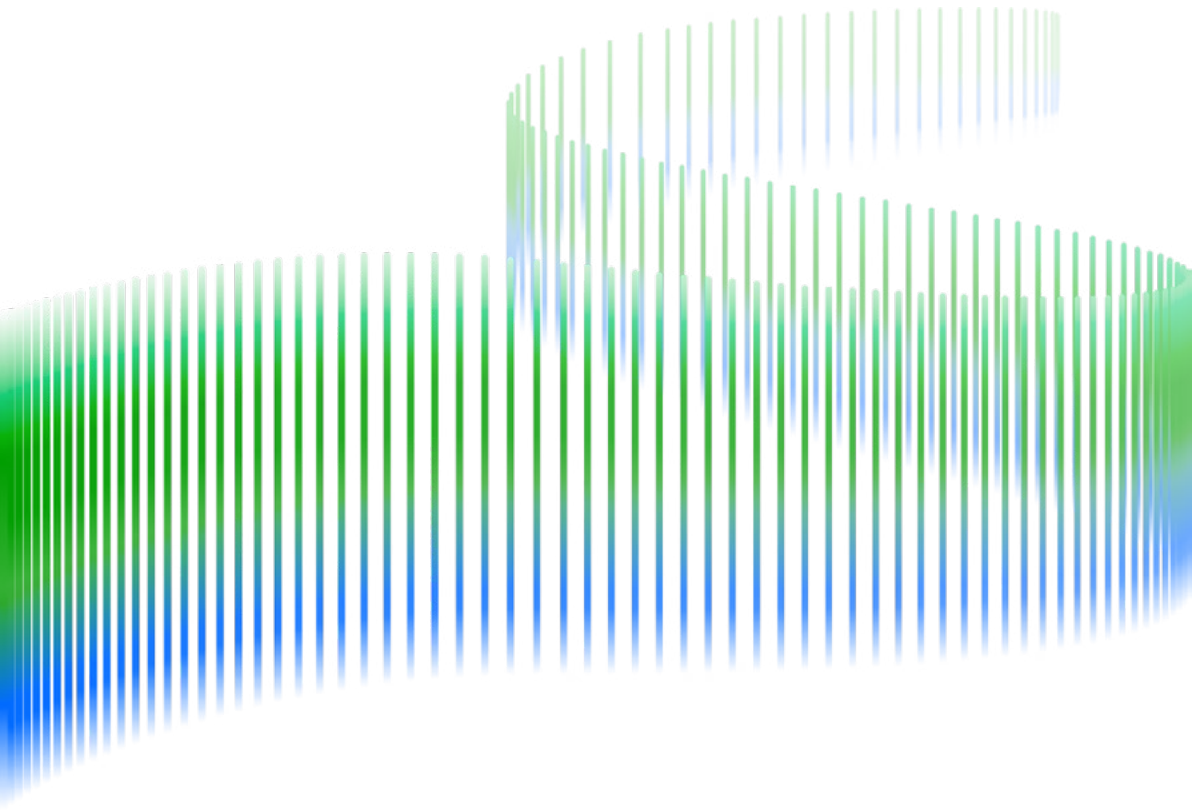
Seven Metrics to Measure the Effectiveness of Your Security Operations



Introduction

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

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

This eBook is designed to help you understand the key operational metrics you should use to measure and communicate your security operations effectiveness to detect and respond to cyber-related events.

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.

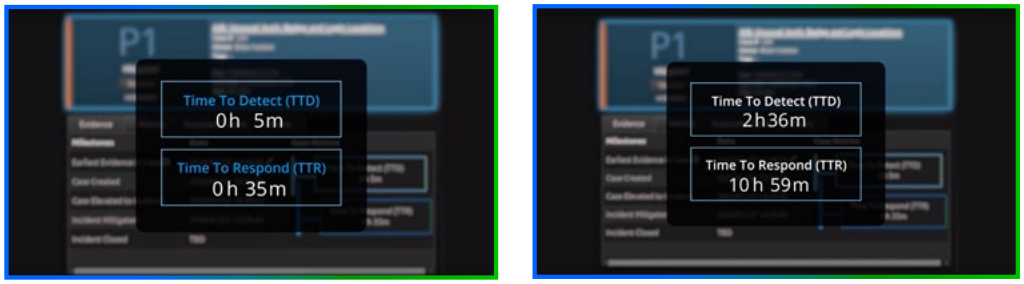
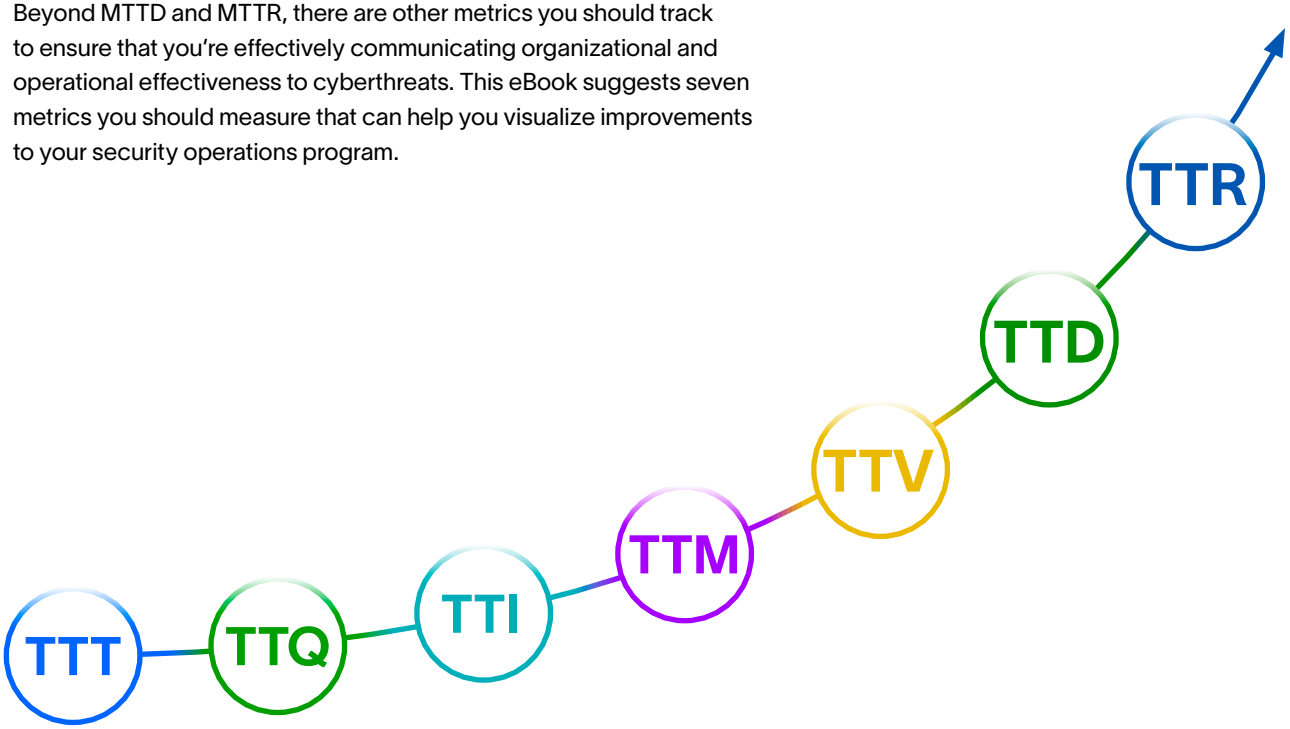


Figure 1. By understanding your MTTD and MTTR, you can lower your risk of cyber incidents and improve your security effectiveness.

Seven 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 eBook suggests seven metrics you should measure that can help you visualize improvements to your security operations program.



1. Alarm Time to Triage

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 (for example, high/medium/low, risk score bands, etc.)
- Might indicate the team can take on additional monitoring load (for example, monitoring another area of the IT infrastructure)
- Might indicate a need for increased staff, or for the team to narrow its monitoring focus (for example, 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

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 (for example, high/medium/ low, risk score bands, etc.)
- Should be measurable/reportable within alarm outcome (for example, false positive, benign issue, incident, etc.)
- Might indicate weakness in the echnological 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

3. Threat Time to Investigate

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 (for example, 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

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 (for example, via the 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

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 (for example, via the 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

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

Incident Time to Detect (TTD) = Date/Time Threat Qualified for Investigation/Case Creation - Date/Time of Initial Indicator of Threatof Case Creation

7. Incident Time to Response

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 (for example, via the ATT&CK categories)
- Might indicate slowness/weakness in the technology solution in the areas supporting threat discovery (for example, threat investigation (for example, search) and mitigation (for example, automation)

Incident Time to Response (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 Exabeam, measuring the effectiveness of your security operations center (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.

Want to see Exabeam in Action?

Schedule a Demo

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam

Learn more at
www.exabeam.com →