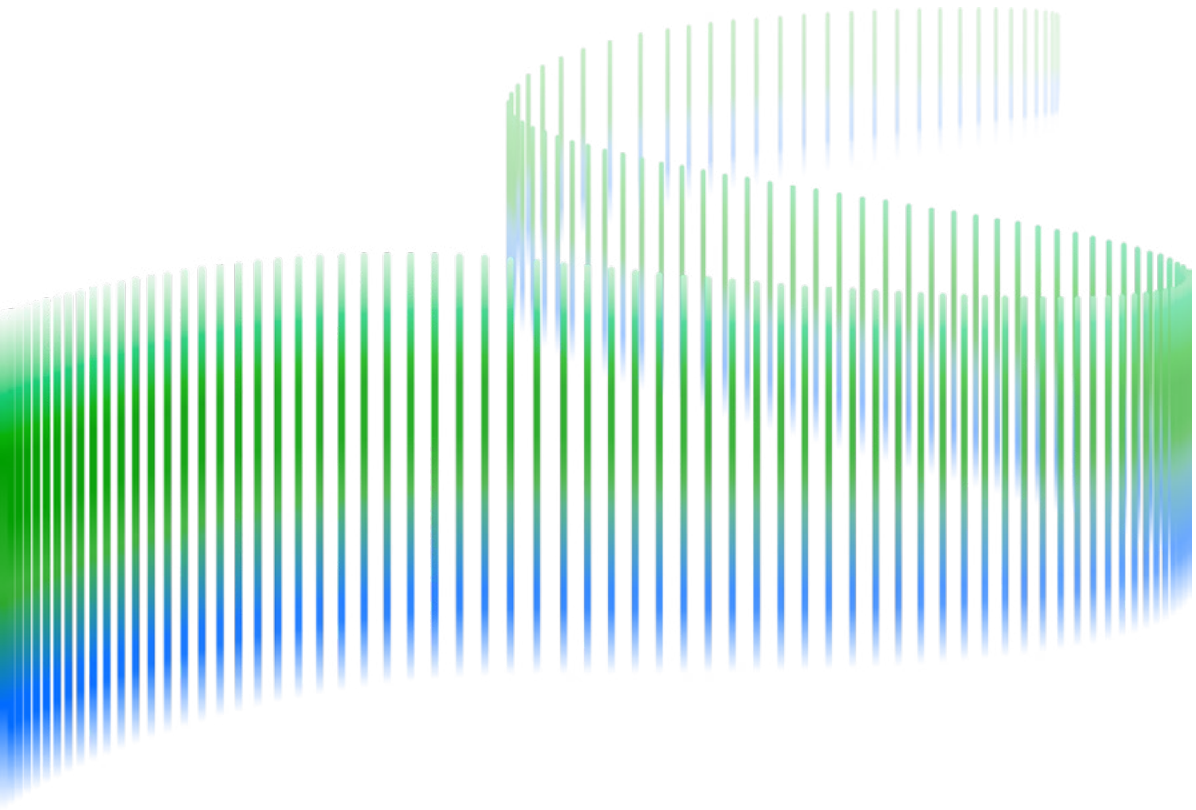
Security Operations Maturity Model

Assess and improve the maturity of your security operations



Introduction

As the threat landscape continues to evolve, your cybersecurity efforts must follow suit. With your security operations center (SOC) at the core of your defense against threats, you must ensure that it can handle anything that comes its way. To be effective, you need to continuously mature your SOC with the focus on stopping threats early — before damage occurs.

Whether your SOC is a virtual team of two to three or a 24x7 operation, maturing your security operations capabilities will help you achieve a faster mean time to detect (MTTD) and mean time to respond (MTTR) to cyberthreats.

This guide explores Exabeam's Security Operations Maturity Model (SOMM), which explains how to measure the effectiveness of your security operations. Through the model, you can assess how to improve your security operations capabilities and resilience to cyberthreats.

In this guide, you will learn how to:

- Measure the current capabilities of your SOC
- Evaluate your organization's maturity level
- Continuously improve your SOC maturity

Understanding and Measuring the Capabilities of a Security Operations Program

Enterprises should think of security operations as a critical business operation. It is important to measure the operational effectiveness of the SOC to identify whether they are realizing KPIs and SLAs. This will help you understand the current state of your program and identify any gaps in your security posture, so that you can improve your processes and maturity over time.

As organizations evolve to keep pace with digital transformation, implementing new processes and technology, or shifting to cloud or hybrid environments, security operations must align.

Continually monitoring and measuring primary metrics that indicate the maturity of a security operations program enables you to invest in the best solutions to move materially closer to the goal of reducing your organization's cyber-incident risk.

Metrics to measure the effectiveness of your SOC:

- Mean time to detect (MTTD)
- Mean time to respond (MTTR)
- Alarm time to triage (TTT)
- Alarm time to qualify (TTQ)
- Threat time to investigate (TTI)
- Time to mitigate (TTM)
- Time to recover (TTV)
- Incident time to detect (TTD)
- Incident time to response (TTR)

The Exabeam Security Operations Maturity Model

Exabeam developed the SOMM as a vendor-agnostic tool to help you assess your current maturity and plan to improve it over time. As your security operations capabilities grow, you will realize improved effectiveness, resulting in faster MTTD and MTTR. Material reductions in MTTD/MTTR will significantly reduce the risk of experiencing high-impact cybersecurity incidents.

The Exabeam model draws from over a decade of organizational experience serving enterprise SOCs around the globe. It features five levels of security operations maturity. Each level builds on the prior, resulting in reduced MTTD/MTTR by strengthening capabilities through people, processes, and technology. The following figure provides an illustrative example of MTTD/MTTR reductions as maturity improves.

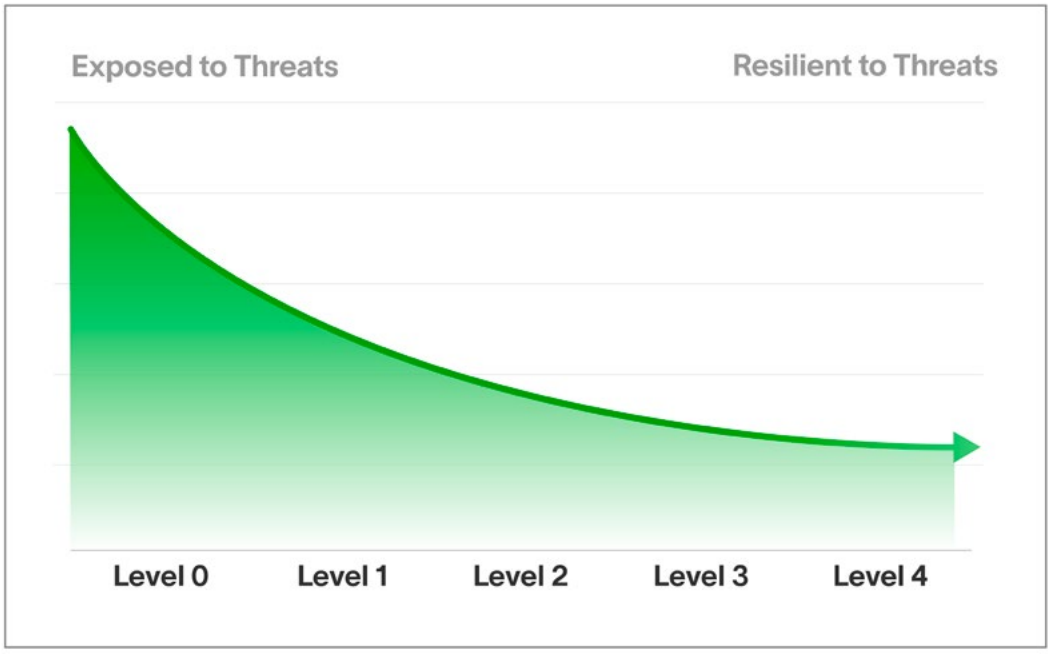


Table 1. Security Operations Maturity

Maturity Model Levels

The following table describes each Security Operations Maturity level in further detail, identifying the key technological and workflow capabilities that should be realized. The way you align with each capability will vary across your organization. The important thing is that you realize the intent of the capability. For each level, Exabeam has also described typical associated organizational characteristics and risk characteristics. This provides additional context to support security operations maturity assessment and planning.

Use this model to evaluate your organization's current security operations maturity and develop a roadmap to achieve the level of maturity that is appropriate considering available resources, budget, and risk tolerance.

Keep in mind, reaching Level 4 doesn't mean your organization's maturity has peaked. Security maturity is an evolution, and it requires ongoing evaluation to refine and continually improve your processes.

Table 2. Security Operations Maturity Model

	Security Operations Capabilities	Organizational Characteristics	Risk Characteristics
Level 0	• None	• Prevention-oriented (e.g., firewalls and antivirus in place) • Isolated logging based on technology and functional silos; no central logging visibility • Indicators of threat and compromise exist, they are not visible and threat hunting is not occurring to surface them • No formal incident response process; any response is dependent on individual heroic efforts	• Non-compliance • Unaware of insider threats • Unaware of external threats • Unaware of advanced persistent threats (APTs) • Potentially stolen IP (if of interest to nation-states or cybercriminals)
Level 1	• Mandated log data and security event centralization • Mandated compliance-centric server forensics, such as file integrity monitoring and endpoint detection response (EDR) • Minimal compliance-mandated monitoring and response	• Compliance-driven investment or have identified a specific area of environment requiring protection • Compliance risks identified via report review; process to manage violations may or may not exist • Improved visibility into threats targeting the protected domain, but lacks people and process for effective threat evaluation and prioritization • No formal incident response process; any response is dependent on individual heroic efforts	• Reduced compliance risk (depending on depth of audit) • Unaware of most insider threats • Unaware of most external threats • Unaware of APTs • Potentially stolen IP (if of interest to nation-states or cybercriminals)
Level 2	• Targeted log data and security event centralization • Targeted server and endpoint forensics • Targeted environmental risk characterization • Reactive and manual vulnerability intelligence workflow • Reactive and manual threat intelligence workflow • Basic machine analytics for correlation and alarm prioritization • Basic monitoring and response processes established	• Moved beyond minimal “check box” compliance, seeking efficiencies and improved assurance • Recognizes the organization may be at risk of high-impact threats, and is striving towards improvements with detection and response • Have established formal processes and assigned responsibilities for monitoring and high-risk alarms • Have established basic, yet formal process for incident response	• Effective compliance posture • Good visibility to insider threats, with some blind spots • Good visibility to external threats, with some blind spots • Mostly unaware of APTs, but more likely to detect indicators and evidence of APTs • More resilient to cybercriminals, except those leveraging APT-type attacks or targeting blind spots • Highly vulnerable to nation-states

	Security Operations Capabilities	Organizational Characteristics	Risk Characteristics
Level 3	• Holistic log data and security event centralization • Holistic server and endpoint forensics • Targeted network forensics • IoC-based threat intelligence integrated into analytics and workflow • Holistic vulnerability integration with basic correlation and workflow integration • Advanced machine analytics for IoC- and TTP-based scenario analytics for known threat detection • Targeted machine analytics for anomaly detection (e.g., via behavioral analytics) • Formal and mature monitoring and response process with standard playbooks for most common threats • Functional physical or virtual SOC • Case management for threat investigation workflow • Targeted automation of investigation and mitigation workflow • Basic MTTD/MTTR operational metrics	• Recognizes the organization may be a target for high-impact threats • Have invested in the organizational processes and headcount to significantly improve ability to detect and respond to all classes of threats • Have invested in and established a formal security operations and incident response center (SOC) that is running effectively with trained staff • Are effectively monitoring alarms and have progressed into proactive threat hunting • Are leveraging automation to improve the efficiency and speed of threat investigation and incident response processes	• Highly effective compliance posture • Great visibility into, and quickly responding to insider threats • Great visibility into, and quickly responding to external threats • Good visibility to APTs, but have blind spots • Very resilient to cybercriminals, except those leveraging APT-type attacks that target blind spots • Still vulnerable to nation-states, but much more likely to detect early and respond quickly

	Security Operations Capabilities	Organizational Characteristics	Risk Characteristics
Level 4	• Holistic log data and security event centralization • Holistic server and endpoint forensics • Holistic network forensics • Industry specific IoC- and TTP-based threat intelligence integrated into analytics and workflows • Holistic vulnerability intelligence with advanced correlation and automation workflow integration • Advanced IoC- and TTP-based scenario machine analytics for known threat detection • Advanced machine analytics for holistic anomaly detection (e.g., via multi-vector AI/ML-based behavioral analytics) • Established, documented, and mature response processes with standard playbooks for advanced threats (e.g., APTs) • Established, functional 24/7 physical or virtual SOC • Cross-organizational case management collaboration and automation • Extensive automation of investigation and mitigation workflow • Full automation, from qualification to mitigation, for common threats • Advanced MTTD/MTTR operational metrics and historical trending	• Are a high-value target for nation-states, cyber terrorists, and organized crime • Are continuously being attacked across all potential vectors: physical, logical, social • A disruption of service or breach is intolerable and represents organizational failure at the highest level • Takes a proactive stance toward threat management and security in general • Invests in best-in-class people, technology, and processes • Have 24/7 alarm monitoring with organizational and operational redundancies in place • Have extensive proactive capabilities for threat prediction and threat hunting • Have automated threat qualification, investigation, and response processes wherever possible	• Highly effective compliance posture • Seeing and quickly responding to all classes of threats • Seeing evidence of APTs early in the Cyberattack Lifecycle and can strategically manage their activities • Extremely resilient to all classes of cybercriminals • Can withstand and defend against the most extreme nation-state-level adversary

Next Steps

Security operations are critical business operations. Understanding your current maturity will provide a baseline for how to mature your posture, and help you demonstrate the value of your security program to business stakeholders.

Threats continue to target data, and threat actors are persistent and creative in their efforts. To improve your security posture, you need to understand your SOC's strengths and weaknesses. Being able to monitor, measure, and communicate the state of your security capabilities is powerful. Measuring metrics such as MTTD and MTTR plays a pivotal role in maturing your SOC. Not only will you understand where growth opportunities exist, but you'll be more effective and will further reduce your risk to threats.

Exabeam's SOMM gives you a roadmap to achieve success. With this insight, you can present hard evidence that you're improving your organization's security stance and garner additional support from your board.

Contact Us

If you're ready to take the next steps in your security journey, **contact Exabeam** to learn how we can help you reduce risk.

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 →