The Security Operations Maturity Model Quick Reference Guide

Maturing security operations

Organisations should think of security operations as a critical business process. Effective security operations are the first line of defence when it comes to preventing cyberattacks. To accomplish this, organisations need mature programs that leverage people, process and technology to rapidly detect and respond to sophisticated attacks.

Yet some organisations struggle with the overall effectiveness of their security operations. They also lack the basis for measuring the effectiveness and maturing capabilities. A mature security operation enables organisations to detect threats earlier in the Cyberattack Lifecycle —a process that describes how the phases of an attack build toward a threat actor's goal.

The Security Operations Maturity Model

LogRhythm developed the Security Operations Maturity Model (SOMM) to assess an organisation's current maturity and plan for improved maturity across time. Organisations should use this model as a basis to evaluate their current security operations maturity and develop a roadmap to achieve the level that is appropriate in the light of their resources, budget and risk tolerance.

LogRhythm's model describes five levels of security operations maturity. Each level builds on the prior, adding additional technology and process improvements that strengthen the capabilities of an organisation's security operation toward mean time to detect (MTTD) and mean time to respond (MTTR) reductions. Organisations can achieve lower MTTD and MTTR by using LogRhythm's Threat Lifecycle Management (TLM) framework, a set of critical capabilities that align technology, people and process to support the principle programs of the security operations centre (SOC).

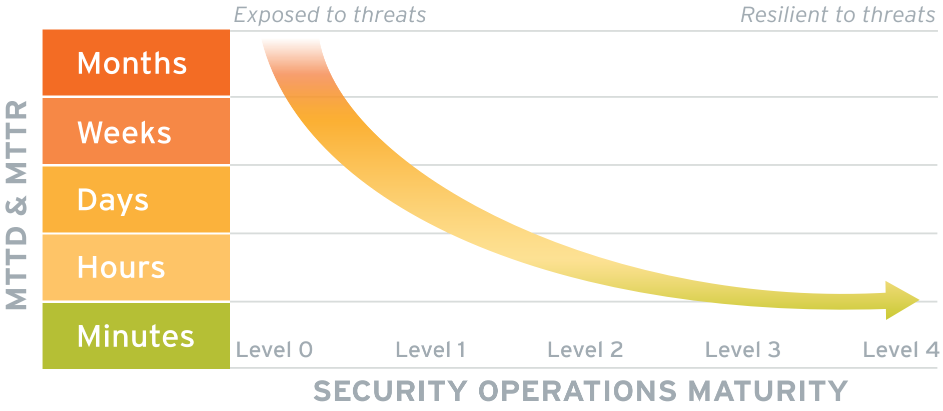
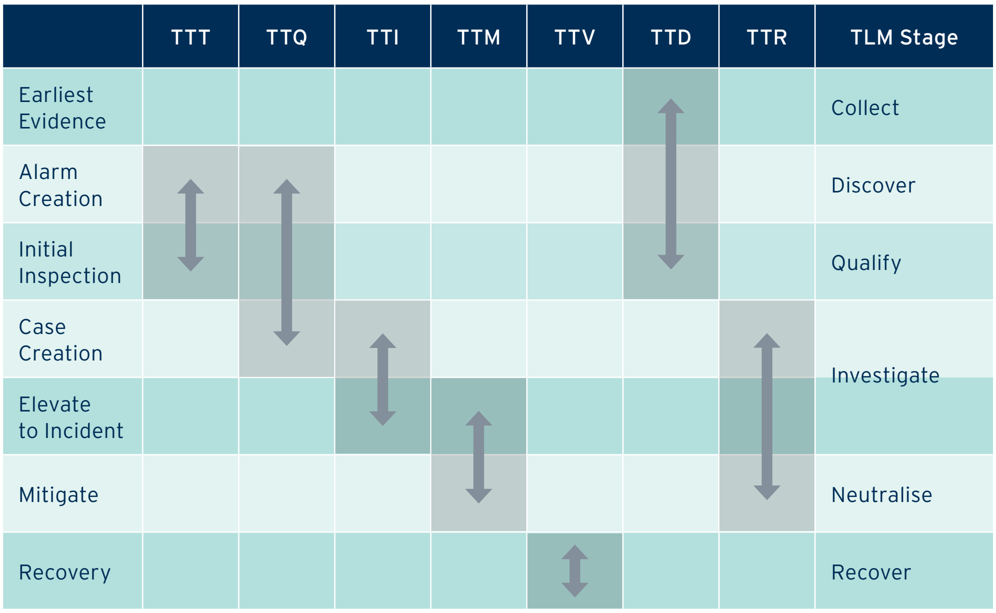


Figure 1. Reduced time to detect and respond to cyberthreats is directly tied to security operations maturity

	TLM capabilities	Organisational characteristics	Risk characteristics
LEVEL 0 Blind	• None	• Prevention-oriented (e.g. firewalls, antivirus, etc. 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; response due to individual heroic efforts	• Non-compliance • Blind to insider threats • Blind to external threats • Blind to advanced persistent threats (APTs) • Potentially stolen IP (if of interest to nation-states or cybercriminals)
LEVEL 1 Minimally compliant	• Mandated log data and security event centralisation • 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 prioritisation • No formal incident response process; response due to individual heroic efforts	• Significantly reduced compliance risk (depending on depth of audit) • Blind to most insider threats • Blind to most external threats • Blind to APTs • Potentially stolen IP (if of interest to nation-states or cybercriminals)
LEVEL 2 Securely compliant	• Targeted log data and security event centralisation • Targeted server and endpoint forensics • Targeted environmental risk characterisation • Reactive and manual vulnerability intelligence workflow • Reactive and manual threat intelligence workflow • Basic machine analytics for correlation and alarm prioritisation • Basic monitoring and response processes established	• Moving beyond minimal, "check box" compliance, seeking efficiencies and improved assurance • Have recognised organisation is effectively blind to most threats; striving toward a material improvement that works to detect and respond to potential high-impact threats, focused on areas of highest risk • Have established formal processes and assigned responsibilities for monitoring and high-risk alarms • Have established basic, yet formal process for incident response	• Extremely resilient and highly effective compliance posture • Good visibility to insider threats, with some blind spots • Good visibility to external threats, with some blind spots • Mostly blind to 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
LEVEL 3 Vigilant	• Holistic log data and security event centralisation • 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 behavioural 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	• Have recognised organisation is blind to many high-impact threats • Have invested in the organisational 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 centre (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	• Extremely resilient and 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
LEVEL 4 Resilient	• Holistic log data and security event centralisation • 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 behavioural 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-organisational case management collaboration and automation • Extensive automation of investigation and mitigation workflow • Fully autonomous 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 organised crime • Are continuously being attacked across all potential vectors: physical, logical, social • A disruption of service or breach is intolerable and represents organisational 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 organisational 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	• Extremely resilient and highly efficient compliance posture • Seeing and quickly responding to all classes of threats • Seeing evidence of APTs early in the Cyberattack Lifecycle and are able to strategically manage their activities • Extremely resilient to all class of cybercriminals • Can withstand and defend against the most extreme nation-state-level adversary

7 significant metrics to measure in your SOC

To determine TLM operational effectiveness, organisations should measure the following:



	TTT	TTQ	TTI	TTM	TTV	TTD	TTR	TLM Stage
Earliest Evidence						↕		Collect
Alarm Creation	↕	↕				↕		Discover
Initial Inspection	↕	↕				↕		Qualify
Case Creation		↕	↕				↕	Investigate
Elevate to Incident			↕	↕			↕	
Mitigate				↕			↕	Neutralise
Recovery					↕			Recover

Figure 2. 7 Key metrics for measuring the effectiveness of TLM

- **Alarm Time to Triage (TTT):** Measures latency in your team's ability to inspect an alarm
- **Alarm Time to Qualify (TTQ):** Measures the amount of time it takes your team to fully inspect and qualify an alarm
- **Threat Time to Investigate (TTI):** Measures the amount of time it takes your team to investigate a qualified threat
- **Time to Mitigate (TTM):** Measures the amount of time it takes your team to mitigate an incident and eliminate immediate risk to your business
- **Time to Recover (TTV):** Measures the amount of time it takes your team to complete full recovery of an incident
- **Incident Time to Detect (TTD):** Measures the amount of time it takes your team to confirm and qualify an incident
- **Incident Time to Response (TTR):** Measures the amount of time it took a confirmed incident to have been investigated and mitigated

Conclusion

To reduce cyber-incident risk and improve security posture, organisations must invest in realising more mature levels of Threat Lifecyle Management—across the holistic IT and OT infrastructure. The LogRhythm Security Operations Maturity Model provides a roadmap for success by helping organisations make material reductions in MTTD/MTTR to profoundly decrease the risk of experiencing high-impact cybersecurity incidents.

To learn more, read the Security Operations Maturity Model white paper: www.logrhythm.com/somm.