Security Operations Maturity Model

A practical guide to assessing and improving the maturity of your security operations through Threat Lifecycle Management

LogRhythm®
The Security Intelligence Company

TABLE OF CONTENTS

Security Operations Maturity Model

This white paper explores how to assess and evolve the principle programs of the security operations center (SOC): threat monitoring, threat hunting, threat investigation, and incident response. LogRhythm developed the Threat Lifecycle Management (TLM) framework to help organizations ideally align technology, people, and process in support of these programs. The TLM framework defines the critical security operations technological capabilities and workflow processes that are vital to realize an efficient and effective SOC. LogRhythm's Security Operations Maturity Model (SOMM) helps organizations measure the effectiveness of their security operations, and to mature their security operations capabilities. Using our TLM framework, the SOMM provides a practical guide for organizations that wish to optimally reduce their mean time to detect (MTTD) and mean time to respond (MTTR) — thereby dramatically improving their resilience to cyberthreats.

Of course, TLM doesn't describe every program a SOC might encompass. For instance, a SOC might also be responsible for other programs, such as an organization's vulnerability management program or a security awareness program. LogRhythm recognizes the importance of other programs that run out of the SOC. However, when evaluating the fundamental maturity of security operations, LogRhythm believes TLM and the programs delivered thereby, serve as the foundation of the SOC and are where organizations should place highest emphasis from a maturity modeling perspective.

Whether a SOC is a virtual team of three or a 24x7 operation, improvements in TLM will result in faster mean time to detect (MTTD) and mean time to respond (MTTR) to cyberthreats. Reduction of MTTD and MTTR should be a primary goal for every organization desiring to materially reduce cyber-incident risk.

In this white paper, organizations will learn about:

- The importance of focusing on threat detection and response
- How attacks typically unfold, and why threats need to be mitigated early
- LogRhythm's Threat Lifecycle Management (TLM) framework for security operations
- The key metrics to measure and evaluate an organization's security operations TLM effectiveness
- A model for assessing security operations maturity based on LogRhythm's TLM framework

Introduction

The Necessity of a Balanced Security Approach

Organizations globally are being compromised by sophisticated cyberattacks at an unprecedented rate and with devastating and costly consequences. A 2018 CyberEdge survey of 1,200 global IT security professionals representing organizations with 500 or more employees indicates that 77 percent of surveyed organizations were compromised during the 12 months preceding the study.[1] Modern threat actors include criminal organizations motivated by financial gain, ideologically driven groups that seek to disrupt or discredit their targets, malicious insiders driven by profit or revenge, and nation-states and state-sponsored organizations engaged in covert operations and industrial espionage targeting both public and private interests.

77 percent of surveyed organizations were compromised during the 12 months preceding the study.

These threat actors are highly motivated and well-funded. They often have software development capabilities that rival those of mainstream technology innovators and will go to extreme lengths to achieve their objectives. The emergence of an increasingly mature cybercrime supply chain and underground economy that support these threat actors serves to heighten their capabilities and increase their ranks. In fact, Cybercrime-as-a-Service (CaaS) is estimated to generate more than $1 trillion in annual revenue.[2] The nature of a cyber-incident, meanwhile, is such that the cost is significant and increases as an attack's lifecycle progresses. A 2018 Mandiant report indicates that threat actors were present on victims' networks for a median of 101 days before being detected.[3] The longer an attacker can remain undetected within an organization, the more data of value they can exfiltrate, the more pervasive the effort required to neutralize and recover from the threat and, consequently, the more damaging and expensive the incident.

Meanwhile, organizations worldwide face other significant challenges in securing their IT and operational environments. Often, they encounter new and evolving regulations and compliance standards for cybersecurity, data protection, privacy and internal IT controls, including such mandates as the Payment Card Industry (PCI) Data Security Standard, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the General Data Protection Regulation (GDPR).

1. 2018 CyberEdge Defense Report, CyberEdge Group, March 2018
2. Cybercrime-as-a-Service: No End in Sight, Dark Reading, Oct. 17, 2018 // 3. M-Trends 2018, FireEye Inc., April 2018

In addition, many of these organizations are rapidly adopting or being impacted by new technology paradigms, including public and private cloud infrastructure, software as a service (SaaS), mobile computing, bring your own device, and the Internet of Things (IoT). This ongoing digital transformation further expands the complexity and size of the attack surface that organizations must protect and increases the difficulty of that challenge. These factors, and the growing volume, variety, and sophistication of threats, are increasingly overwhelming security teams and inhibiting them from identifying threats that could lead to a damaging cyber-incident or data breach.

A 2018 Mandiant report indicates that threat actors were present on victims' networks for a median of 101 days before being detected.

The traditional approach to addressing the cybersecurity challenge has been prevention-centric, focused on access control and blocking known threats. While prevention-centric approaches are important and necessary for thwarting traditional known attacks, they are ineffective at preventing emerging and advanced threats, stopping socially engineered attacks, and containing insider threats. Consequently, organizations are increasingly shifting their resources and focus to strategies centered on rapid threat detection and response. In 2022, worldwide spending on security-related hardware, software, and services is forecast to reach $133.7 billion, according to International Data Corporation (IDC).[4] Security spending in 2022 will be 45 percent greater than the $92.1 billion forecast for 2018.[5] Consistent with this rebalancing of security investment priorities, many organizations are now investing in the build-out or refurbishment of a SOC, whether physical or virtual, with rapid threat detection and response as core missions.

4. Worldwide Semiannual Security Spending Guide, International Data Corporation, Oct. 2018 // 5. IBID

Obstacles to Faster Threat Detection and Response

Even as security budgets rise, and organizations place increasing emphasis on a more balanced cybersecurity strategy that focuses on detection and response, along with prevention, significant reductions in MTTD and MTTR have been difficult to realize due to six common obstacles.

1. Information Overload and Alarm Fatigue

Many security solutions cannot accurately differentiate among high-risk threats, low-risk threats, false positives, and benign anomalies, resulting in large numbers of unqualified security alerts. This high alert volume often obscures legitimate threats, overwhelms security teams, and erodes the ability to identify, prioritize, and respond to critical threats.

2. Lack of Centralized Forensic Visibility

Many organizations lack broad and deep centralized visibility into activity across the extended IT and operational environments. While organizations may have invested in products designed to provide this visibility, such as basic log management and first-generation SIEM tools, these technologies generally cannot sufficiently ingest or contextualize the growing number of evolving machine data types present in an organization, particularly from cloud applications and infrastructure.

3. Swivel-Chair Analysis

Because of its investment in multiple point security products, an organization's security team must triage and investigate threats by moving back and forth among numerous product user interfaces to develop a complete picture of a cyberthreat and assess its risk. This inefficient and disjointed process — often referred to as "swivel-chair analysis" — is time-consuming, does not scale, and is prone to errors and inconsistent results.

4. Ineffective Holistic Threat Detection

One of the most common obstacles in detecting and remediating threats is the failure to realize central and holistic visibility into threats across the extended IT landscape. First-generation SIEMs, and other point analytics solutions, have tried to serve this need, but they lack the depth and breadth of centralized forensic data, business, and operational risk context. Furthermore they lack the ability to perform analytics across all attack surfaces — whether user, network, or endpoint — and consequently cannot corroborate activity across those attack surfaces to detect advanced threats. Products focused on performing point analytics from specific attack surfaces are vulnerable to both higher numbers of false negatives without visibility to the full scope of threat indicators, as well as false positives where potential threat activity could be ruled out with additional context.

5. Fragmented Workflow

To facilitate collaboration across members of the threat detection, threat investigation, and incident response teams, security teams likely utilize multiple disjointed communications tools and techniques, including point security products, IT ticketing systems, email, spreadsheets, and shared online document stores. The disparate nature of these approaches prevents alignment of people and processes in the security operation and introduces inefficient workflow, inability to create consistent, repeatable processes, and extends ramp time of new team members.

6. Lack of Automation

Organizations must perform numerous tasks to effectively triage, investigate, neutralize, and recover from a threat. Many of these tasks are routine, repetitive, and time-consuming. Automation allows analysts to focus on higher-value activities. It becomes increasingly more difficult to implement automation solutions when leveraging multiple point security tools with independent data silos. Without automation of preapproved actions, security teams cannot act to immediately neutralize threats, and system changes can often sit in IT ticketing queues for hours or days.

Materially reducing cyberthreat MTTD and MTTR is only possible when these traditional obstacles are overcome. This allows organizations to detect and neutralize threats early in the Cyberattack Lifecycle, thereby avoiding damaging cyber-incidents.

Understanding the Cyberattack Lifecycle

When a threat actor targets an organization's environment, a process unfolds from initial intrusion through eventual data breach. Whether the attacker is a lone actor, a criminal group, or a nation-state operations unit, if they are detected and neutralized quickly, damage is more likely to be negligible. Conversely, if an attacker is allowed to dwell for weeks or months, a data breach is much more likely and the threat may have compromised hundreds of systems and/or user accounts as they work toward their goal. In its *Quantifying the Value of Time in Cyber-Threat Detection and Response* report, Aberdeen Group determined that limiting dwell time to 30 days results in a reduction of the impact on business by 23 percent.[6] In addition, compression of dwell time delivers even stronger results for business. When dwell time is confined to seven days, the impact is reduced by 77 percent. If shortened to just one day, business impact is reduced by as much as 96 percent.

When dwell time is confined to seven days, the impact is reduced by 77 percent. If shortened to just one day, business impact is reduced by as much as 96 percent.

Threat actors may adopt many different strategies to achieve their goals. The Cyberattack Lifecycle provides a useful framework to understand how the phases of an attack build toward that ultimate goal. Some of the phases may be merged in certain types of attacks, and in other cases, phases may be skipped altogether. However, while attack types vary, the overall pattern remains consistent. Mature security operations teams kill threats early through technology-enabled threat management processes that drive down MTTD and MTTR — rapidly detecting and neutralizing threats before real damage occurs.

The following graphic illustrates the Cyberattack Lifecycle and the typical steps involved in a cyber-incident such as a data breach:

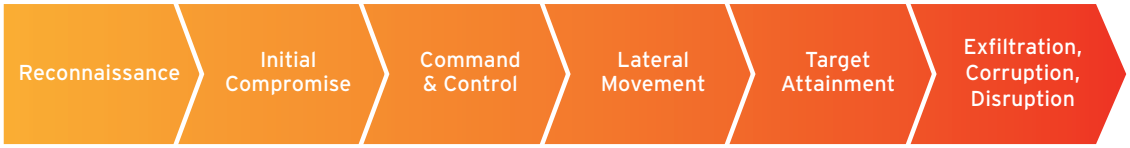


Figure 1. The Cyberattack Lifecycle

6. Quantifying the Value of Time in Cyber-Threat Detection and Response, Aberdeen Group, February 2016

Phase 1: Reconnaissance

The first stage in reconnaissance is identifying potential targets (companies or individuals) that satisfy the mission of the attacker (e.g., financial gain, targeted access to sensitive information, brand damage, etc.). Once the target or targets are identified, the attacker determines the best mode of entry.

The attacker further determines what defenses organizations have in place, what web applications or other internet-accessible systems are in place, how to compromise external systems, and how to gain an initial foothold on an internal device. They choose the initial weapon based on what they discover during their reconnaissance, whether it is a zero-day exploit, a spear phishing campaign, physical compromise, bribing an employee, or some other means of launching their initial attack.

Phase 2: Initial Compromise

The initial compromise usually involves an attacker bypassing an organization's perimeter defenses and, in one way or another, gaining access to an internal network through a compromised system or user account. Compromised systems might include externally facing servers or end-user devices, such as laptops or desktops. Recent breaches have also included systems that were never traditionally considered as intrusion entry points, such as point-of-sale (POS) systems, medical devices, personal consumer devices, networked printers, and IoT devices.

Phase 3: Command & Control

The compromised device is used as a beachhead into an organization. Typically, this involves the attacker surreptitiously downloading and installing a remote-access Trojan (RAT) so they can establish persistent, long-term, remote access to an environment. Once the RAT is in place, the attacker can carefully plan and execute the next move using covert connections from attacker-controlled systems on the internet.

Phase 4: Lateral Movement

Once the attacker has an established (persistent) connection to an internal network, they seek to compromise additional systems and user accounts. First, the attacker will take over the user account on the compromised system. This account allows the attacker to scan, discover, and compromise additional systems from which additional user accounts can, in turn, be compromised. Because the attacker is often impersonating authorized users, evidence of their existence can be hard to recognize.

Phase 5: Target Attainment

At this stage in the lifecycle, the attacker typically has multiple remote access entry points and may have compromised hundreds (or even thousands) of an organization's internal systems and user accounts. They have mapped out and deeply understand the aspects of the IT environment of highest interest to them. Ultimately, the attacker is within reach of the desired target(s), and is comfortable with completing their ultimate mission at the time of their choosing.

Phase 6: Exfiltration, Corruption, and Disruption

The final stage of the Cyberattack Lifecycle is where cost to the business rises exponentially if the attack is not defeated. This is the stage where the attacker executes the final aspects of the mission, stealing intellectual property or other sensitive data, corrupting mission-critical systems, or generally disrupting an organization's business operations. In the event of data theft, data is often transmitted via covert network communications across days, weeks, or even months. The attacker may also hide activity by using seemingly legitimate cloud-storage applications, such as Dropbox and Google Drive, to steal data.

The LogRhythm Threat Lifecycle Management Framework

Organizations that strive to reduce their cybersecurity risk through significant reductions in MTTD and MTTR must realize an enterprise capability for detecting and responding to threats across the holistic physical, virtual, and cloud-based information technology (IT) environment. Industries such as critical infrastructure and manufacturing, or industries being impacted by the rise of IoT, should realize the same enterprise threat detection and response capability across the operational technology (OT) environment as well.

LogRhythm developed the Threat Lifecycle Management (TLM) framework to define the critical security operations technological capabilities and workflow processes that are vital to realize organizationally efficient and optimal MTTD/MTTR reductions. MTTD and MTTR are the key measurable indicators of security operations maturity. TLM, when done well, empowers teams, whether they are a three-person virtual SOC or a globally distributed 24x7 SOC, to more effectively realize the following foundational workflows that ultimately determine organizational MTTD/MTTR.

LogRhythm considers a **virtual SOC** to be one in which a dedicated collection of individuals, that might span security, IT, and OT roles, executes their defined operational mission through software, collaboration, and communication tools versus doing so in a physical room.

PRINCIPLE PROGRAMS OF A SOC

Threat monitoring consists of evaluating alarms and events that might indicate the presence of a cyberthreat, and quickly triaging them to determine if further investigation is required.

Threat hunting consists of proactively searching for threats in the environment based on threat intelligence, analyst instinct, and behavioral anomaly cues.

Threat investigation consists of deeply analyzing a suspected threat until it can be assessed as benign or it can be determined an incident has occurred or is imminent.

Incident response consists of taking actions to mitigate an active cyberthreat risk until the threat is fully neutralized and the organization has fully recovered from the incident.

Breaking Down TLM

Collaboration across security and IT/OT teams is critical to realizing rapid and effective results. Each stage of the TLM framework is highly interrelated, enabled by intelligence gathered and work performed in the preceding stage.

Optimal TLM aligns people, process, and technology to realize high-efficiency workflows, enabled through analytics and automation, with the goal of reducing MTTD and MTTR within existing staffing levels. The following diagram depicts the TLM framework with each stage.

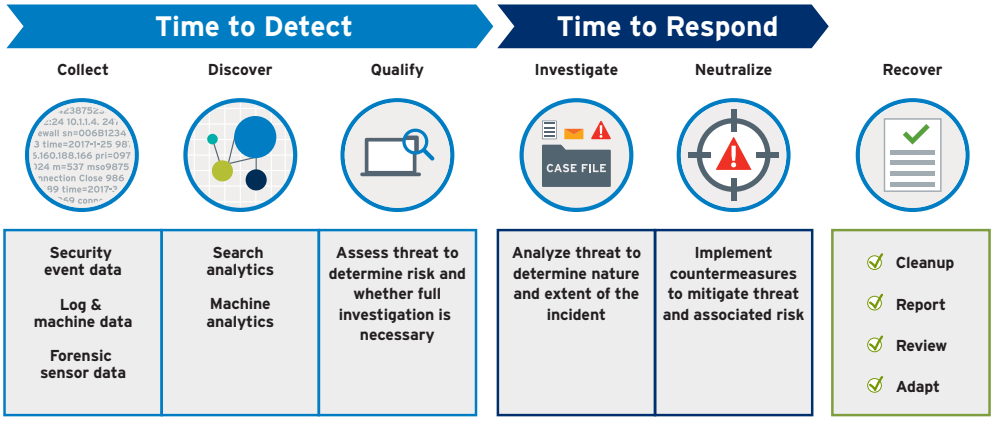


Figure 2. The Threat Lifecycle Management Framework

Stage 1: Centralize Event and Forensic Data

Before detecting any threat, organizations must be able to see evidence of the attack within the IT/OT environment. Because threats target all aspects of the IT/OT infrastructure, the more organizations can see, the more ably they can detect. There are three principle types of data enterprises should focus on, generally in the following priority:

Security Event and Alarm Data

Most organizations have an array of security products to prevent a wide range of attacks from being successful. However, in some cases, these technologies can only warn that an attack may be in process or has already occurred. In these cases, events and alarms are generated. Organizations may also be investing in more network-, system-, and application-level intrusion and threat detection systems. The challenge enterprises may be dealing with is the ability to rapidly identify which events or alarms to focus on, as tens of thousands may be generated on a daily basis. At the same time, this is typically the most valuable source of data a security team has for finding evidence of a successful attack.

Log and Machine Data

Log data can provide deeper visibility into an IT environment — recording on a per user, per system, per application basis — who did what, when, and where. This rich set of data can support more effective and rapid investigations of suspected attacks. The ability to comprehend what is normal within the IT environment is also within this dataset — enabling automated machine analytics to detect behavioral anomalies that might indicate a more advanced attack is in progress.

Forensic Sensor Data

Once an organization is effectively collecting its security and log data, forensic sensors can provide even deeper and broader visibility. Forensic sensors can fill visibility gaps when logs aren't available or where the level of forensic detail is insufficient. There are two primary types of forensic sensors that might be employed:

- Network forensic sensors that capture packets and flows
- Endpoint forensic sensors that can record with high fidelity all activity occurring on the monitored system.

Investment in forensic sensors can provide additional gains in investigative and incident-response effectiveness. This data also enables more powerful and capable machine analytics-driven approaches for detecting the most sophisticated attacks.

Stage 2: Discover

Once organizations establish visibility, they now stand a chance at detecting and responding to threats. Discovery of potential threats is accomplished through a blend of search and machine analytics.

Search Analytics

This type of analytics is performed by people and enabled by software. It includes things such as targeted hunting of threats by monitoring dashboards and leveraging search capabilities. It also includes reviewing reports to identify known exceptions. Search analytics is people intensive. Thus, while effective, it cannot be the sole (or even primary) method of analytics most organizations should employ.

Machine Analytics

This type of analytics is performed by software using machine learning (ML) and other automated analysis techniques where outputs can be efficiently leveraged by people. Machine analytics is the future of a modern and efficient threat discovery capability. The goal of using machine analytics should be to help organizations realize a "risk-based monitoring" strategy through the automatic identification and prioritization of attacks and threats. This is critical for both detecting advanced threats via data science-driven approaches, as well as helping organizations orient precious human cognitive cycles to the areas of highest risk to the business.

Risk-Based Monitoring is automatic identification and prioritization of attacks and threats. LogRhythm enables risk-based monitoring through its patented Risk-Based Prioritized Alarms, which helps a SOC reduce alarm fatigue and effectively focus time on what is most likely a true risk to the enterprise. Adopting a risk-based monitoring strategy improves operational efficiency and materially reduces the risk of experiencing a data breach or other damaging cyber-incident.

Stage 3: Qualify

Threats must be rapidly qualified to assess the potential impact to the business and the urgency of additional investigation and response efforts. The qualification process is manual and time intensive, while also being very time sensitive. An inefficient qualification process increases the level of human investment needed to evaluate all threat indicators (e.g., alarms), but an efficient process allows organizations to analyze more indicators with less staff.

False positives will happen. Organizations need the tools to identify them quickly and accurately. Inefficient qualification could mean a true threat (aka "true positive") has been ignored for hours or days. Incorrect qualification could mean that organizations miss a critical threat and let it go unattended. Philosophically and practically, it is important to note that only qualified threats can truly be considered detected, otherwise it's simply noise — an alarm bell going off that nobody really hears.

Stage 4: Investigate

Once threats have been qualified, they need to be fully investigated to conclusively determine whether a security incident has occurred or is in progress. This begins with conducting a deep investigation using all the collected evidence to understand the risk presented by the threat and its scope. Rapid access to forensic data and intelligence on the threat is paramount. Automation of routine investigatory tasks and tools that facilitate cross-organizational collaboration is ideal for optimally reducing MTTR.

Ideally, a secure facility for keeping track of all active and past investigations is available. This can help ensure that forensic evidence is well-organized and is available to collaborators. It can also provide an account of who did what in support of investigation and response activities to measure organizational effectiveness and hold parties responsible for the tasks they own in the investigation.

Stage 5: Neutralize

When an incident is qualified, organizations must implement mitigations to reduce and eventually eliminate risk to the business. For some threats, such as ransomware or compromised privileged users, every second counts. To maximally reduce MTTR, easily accessible and updated incident response processes and playbooks, coupled with automation, are critically important. Similar to the Investigate stage, facilities that enable cross-organizational (e.g., IT, legal, HR) information sharing and collaboration are also important.

Stage 6: Recover

Once the incident has been neutralized and risk to the business is under control, full recovery efforts can commence. These efforts are less time critical, and they can take days or weeks depending on the scope of the incident. To recover effectively and on a timely basis, it is imperative that an organization's security team has access to all forensic information surrounding the investigation and incident-response process. This includes ensuring that any changes made during incident response are tracked, audit trail information is captured, and the affected systems are updated and brought back online. Many recovery-related processes can benefit from automation. In addition, the recovery process should ideally include putting measures in place that leverage the gathered threat intelligence to detect if the threat returns or left behind a back door.

Improving Security Operations Maturity by Aligning TLM with the Cyberattack Lifecycle

The goal of efficient TLM is to detect and respond to cyberthreats as early in the attack lifecycle as possible to prevent the attacker from reaching the ultimate goal — exfiltration, corruption, or disruption. The Cyberattack Lifecycle provides multiple opportunities to neutralize the attack, and as the maturity of security operations improves, the organization is able to detect and neutralize attacks earlier in the attack lifecycle.

The Cyberattack Lifecycle provides multiple opportunities to neutralize the cyberattack, and as security operations maturity improves, the organization can detect and respond to attacks earlier.

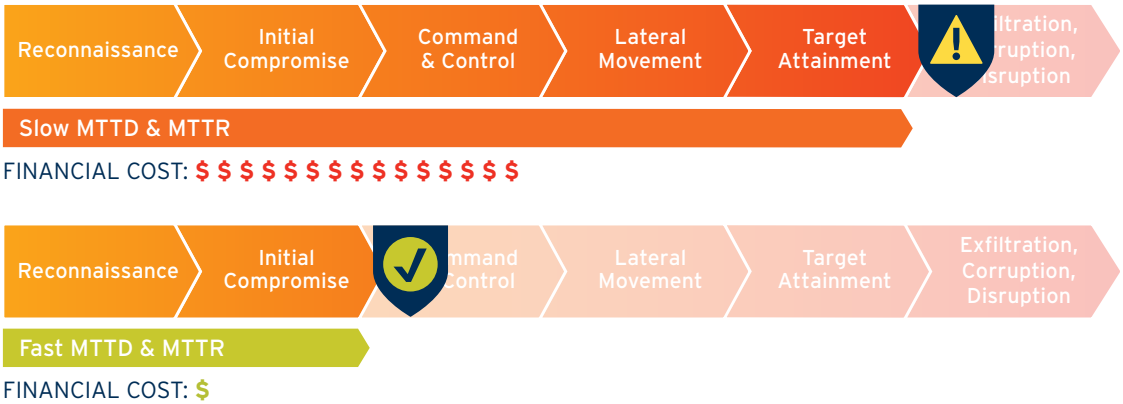


Figure 3. Neutralizing an Attack Earlier in the Lifecycle Results in a Drastic Reduction in Financial Cost to the Company and Damage to its Reputation

Technology Enablement

Each of the TLM phases is critically dependent on technology. The right technological approach and strategy will significantly influence the organizational capability and cost when it comes to realizing TLM and resulting levels of MTTD/MTTR. The same three-person virtual SOC, leveraging a more optimal technology approach, might have twice as much capacity and realize two times the reduction in MTTD/MTTR versus a team relying on outdated or poorly integrated technologies. While there are a variety of strategies and approaches to realizing technologically enabled TLM, security operations teams ideally have a modern and highly integrated technological platform that delivers all of the following:

- **Centralized Security Intelligence:** Centralized visibility into all security alerts and alarms generated across the distributed IT/OT infrastructure, including visibility into the current status of active threat investigations and incidents with real-time situational awareness
- **Centralized Forensic Visibility and Search:** Centralized search into all forensic data from across the distributed IT/OT environment, including immediate access to complete, full-fidelity forensic data to accelerate threat investigation and incident response
- **Holistic Threat Analytics:** The application of artificial intelligence, TTP/IOC-based scenario analytics and deep contextual analytics across a 360-degree view of forensic data to detect advanced threats and accurately prioritize all threats across the holistic attack surface
- **Case Management:** Capabilities enabling security teams to engage in highly confidential, collaborative, and efficient workflows with a centralized and secure case management facility for managing and accelerating threat investigation and incident response efforts
- **Task Automation:** The automation of routine and time-consuming tasks performed in support of threat investigation and incident response, including automated execution of mitigations and countermeasures for threat containment and neutralization
- **Operational Metrics:** The ability to easily capture metrics and effectively report on the business key performance indicators (KPIs), service-level agreements (SLAs), and operating-level agreements (OLAs)
- **High-Speed Integrated User Experience:** A highly integrated user experience that spans the end-to-end TLM workflow, from initial threat discovery to full incident recovery; the user experience should support high-speed workflows where UI latency is minimized to ensure the pace of people is not impeded by the responsiveness of the UI and the underlying technology

Understanding and Measuring the Capabilities of a Security Operations Program

Enterprises should think of TLM as a critical business operation. 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.

Enterprises should think of TLM as a critical business operation. Like any core business operation, mature organizations will want to measure operational effectiveness to identify whether KPIs and SLAs are being realized.

Visibility and Analytics Metrics

Centralized Forensic Visibility (CFV)

This measures the estimated percent of the IT/OT infrastructure across which a reasonable level of centralized forensic visibility exists and search and machine-based analytics can be applied. This metric can be broken down into further sub-metrics that evaluate the type of central visibility currently realized. For instance:

- **Enterprise Security Event Visibility:** the percentage of security event-generating devices that can be centrally searched and forensically analyzed
- **Enterprise Log Visibility:** the percentage of log-generating devices and servers that can be centrally searched and forensically analyzed
- **Enterprise Network Forensic Visibility:** the percentage of the infrastructure that is being independently monitored by a network forensics (e.g., full packet capture) technology

- **Enterprise Endpoint Forensic Visibility:** the percentage of the infrastructure that is being independently monitored by an endpoint forensics (e.g., EDR) technology

These metrics:

- Should be measurable/reportable by business unit, compliance domains, and data risk domains
- Can be separately measured across the IT and OT infrastructure
- Will indicate inherent threat detection risk when forensic visibility is low
- Will indicate inherent threat response and recovery risk when forensic visibility is low
- Can support the business case for realizing expanded visibility

CFV Calculation: This metric and related sub-metrics are difficult to empirically measure. An organizational method for estimating visibility should be formalized and then consistently applied. Organizations should consider establishing target visibility for each type (e.g., enterprise log visibility target = 100 percent of production servers in data domains A, B, and C; 50 percent for data domains X, Y, and Z). Organizations can then measure their current visibility against targets, as well as against the whole environment.

Centralized Machine Analytics Visibility (CMAV)

This metric measures the estimated percent of the IT/OT infrastructure across which machine analytics is being actively applied for threat discovery and alarm prioritization. CMAV is closely related to CFV as the ability to apply centralized machine analytics is dependent on centralized forensic visibility. This metric can be broken down into sub-metrics based on the analytics method type.

- **Centralized Security Event Prioritization:** the percentage of security event generating devices, across which automated correlation and prioritization is being performed to risk score and prioritize related alarms
- **Centralized Scenario Analytics:** the percentage of log-generating devices across which automated TTP- or IOC-based scenario analytics is being applied to detect applicable threats and further risk score and prioritize related alarms
- **Centralized User Behavior Analytics:** the percentage of enterprise users across which behavioral analytics is being applied to detect behavioral shifts that might indicate a user-borne threat is present

- **Centralized Network Behavior Analytics:** the percentage of enterprise network infrastructure across which behaviorial analytics is being applied to detect behavioral shifts that might indicate a network-borne threat is present

These metrics:

- Should be measurable/reportable by business unit, compliance domains, and data risk domains
- Can be separately measured across the IT and OT infrastructure
- Will indicate inherent false positive risk and related operational efficiency risk when machine analytics is low
- Will indicate inherent false negative risk and related threat detection risk when machine analytics is low
- Can support the business case for realizing expanded machine analytics

CMAV Calculation: This metric and related sub-metrics are difficult to empirically measure. An organizational method for estimating machine analytics visibility should be formalized and then consistently applied. Organizations should consider establishing target machine analytics visibility for each type (e.g., Centralized User Behavior Analytics target = 100 percent of IT workers and execs; 50 percent for all other users). Organizations can then measure their current visibility against targets, as well as against the distributed IT/OT environment.

__CFV__ indicates inherent threat detection, response, and recovery risk when forensic visibility is low. __CMAV__ indicates inherent false positive and false negative risk, with associated operational and threat detection risks when machine analytics visibility is low.

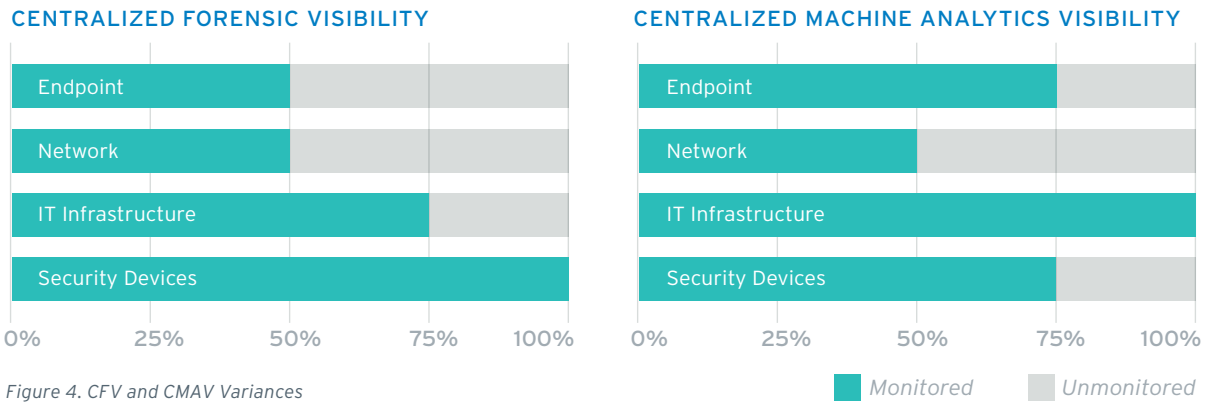


Figure 4. CFV and CMAV Variances

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. Each metric is then described in further detail.

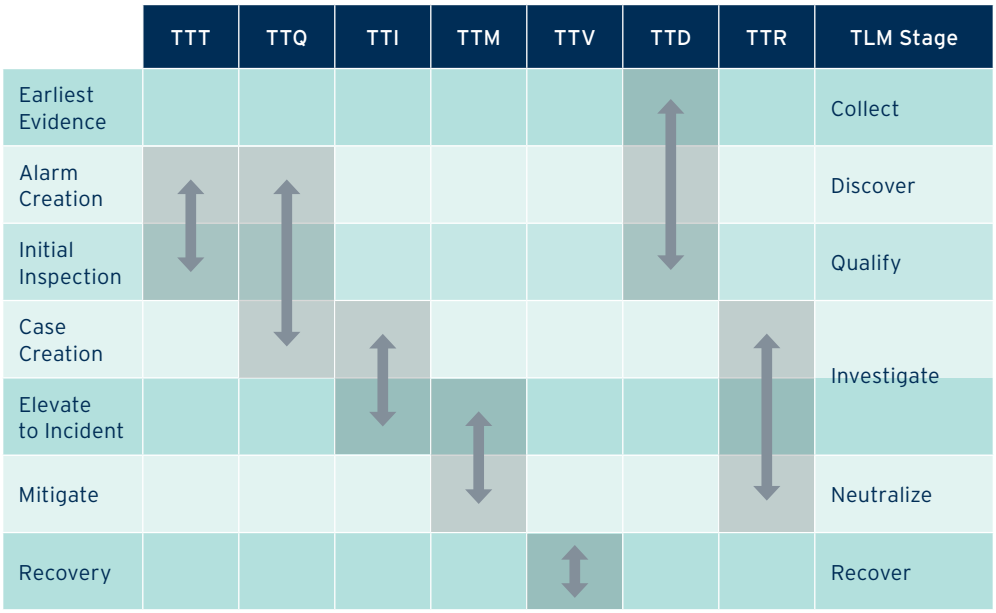


Figure 5. Seven Key Metrics for Measuring the Effectiveness of TLM

Alarm Time to Triage (TTT)

TTT measures latency in the team's ability to immediately inspect an alarm. It helps organizations understand the level of real-time responsiveness to threats. This metric:

- Should be measurable/reportable within alarm priority bands (e.g., high/medium/low, risk score bands, etc.)
- Measures operational effectiveness and capacity of the front-line (i.e., security analyst) team
- 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)

TTT Calculation: The date/time difference between alarm creation and the initial inspection of the alarm

Alarm Time to Qualify (TTQ):

TTQ measures the amount of time it took an alarm to be fully inspected and qualified. It helps organizations identify bottlenecks and understand the 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.)
- Measures operational effectiveness and capacity of the front-line (i.e., security analyst) team
- Might indicate weakness in the technological TLM solution in the area of alarm drill down, search, data analysis, and contextual analysis

TTQ Calculation: The date/time difference between alarm creation and the alarm either being closed or added to a case

Threat Time to Investigate (TTI)

TTI measures the amount of time it took a qualified threat to be fully investigated. It helps organizations 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)
- Measures operational effectiveness and capacity of the second-line (i.e., threat investigation) team
- Might indicate slowness in the technology TLM solution in the area of search, data analysis, contextual analysis, and collaboration

TTI Calculation: The date/time difference between the case being created and the case either being closed or elevated to an incident

Time to Mitigate (TTM)

TTM measures the amount of time it took an incident to be mitigated and immediate risk to the business to be eliminated. This metric helps organizations understand how quickly the team is able to implement mitigations that 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)
- Measures operational effectiveness and capacity of the third-line (i.e., incident response) team

- Might indicate slowness in the technology TLM solution in the area of evidence capture and use, standard playbooks, automation, and collaboration

TTM Calculation: The date/time difference between incident determination (e.g., case being elevated to an incident) and the incident being considered mitigated

Many organizations are adopting the **MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)** framework for assessing their overall maturity in being able to respond to threats across the Cyberattack Lifecycle. TLM can help organizations empirically measure MTTD and MTTR across MITRE tactics.

Time to Recover (TTV)

TTV measures the amount of time it took for the full recovery around an incident to be complete. Measuring this helps organizations understand how quickly the security team and other involved groups are able to 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)
- Measures operational effectiveness and capacity of third-line (i.e., incident response) teams and other supporting teams (e.g., IT, Legal, HR)
- Might indicate slowness/weakness in the technology TLM solution in the area of evidence capture and use, standard playbooks, automation, and collaboration

TTV Calculation: The date/time difference between incident mitigation and the incident being considered fully recovered from and closed

Incident Time to Detect (TTD)

TTD measures the amount of time it took a confirmed incident to have been initially detected and ultimately qualified. This 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.)

- Measures operational effectiveness and capacity of the first- and second-line teams
- Might indicate slowness/weakness in the technology TLM 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)

TTD Calculation: For a determined incident, the date/time difference between initial indicator of the threat (e.g., earliest evidence of) and the threat being qualified for full investigation (date case was created)

Incident Time to Response (TTR)

TTR measures the amount of time it took a confirmed incident to have been investigated and mitigated. This 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)
- Measures operational effectiveness and capacity of the second-line (e.g., threat investigation) and third-line (e.g., incident response) teams
- Might indicate slowness/weakness in the technology TLM solution in the areas supporting threat investigation (e.g., search) and mitigation (e.g., automation)

TTR Calculation: For a determined incident, the date/time difference between investigation initiation (e.g., date case was created) and the incident being considered mitigated

As an organization's TLM maturity improves, it will realize improved effectiveness of its security operations resulting in faster MTTD and MTTR. Material reductions in MTTD/MTTR will profoundly decrease the risk of experiencing high-impact cybersecurity incidents.

The LogRhythm Security Operations Maturity Model

LogRhythm has developed a Security Operations Maturity Model (SOMM) — based on LogRhythm's Threat Lifecycle Management (TLM) framework — that can be used to assess an organization's current maturity, and plan for improved maturity across time. As an organization's TLM capability matures, it will realize improved effectiveness of its security operations resulting in faster MTTD and MTTR. Material reductions in MTTD/MTTR will profoundly decrease the risk of experiencing high-impact cybersecurity incidents.

Maturity Model Levels

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 organization's security operation toward MTTD/MTTR reductions. The following figure provides an illustrative example of MTTD/MTTR reductions as TLM maturity improves.

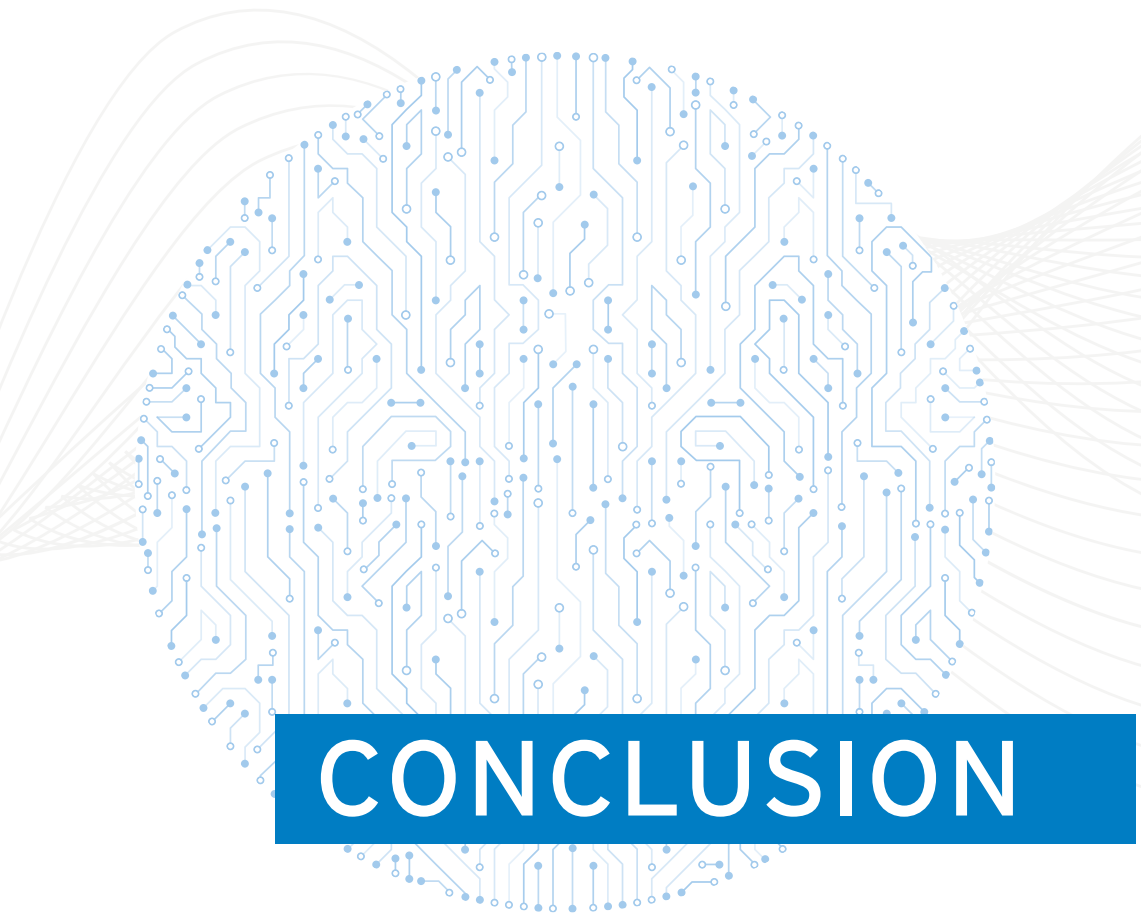
Figure 6. Reduced Time to Detect and Respond to Cyberthreats is Directly Tied to Security Operations Maturity

The following table describes each level in further detail, identifying the key TLM technological and workflow/process capabilities that should be realized. These capabilities are described at a high level with the intent of serving as a guidepost for enterprises. The manner in which each capability is realized will vary from organization to organization. The important thing is that the intent of the capability is realized. For each level, LogRhythm has also described typical associated organizational characteristics and risk characteristics. This is to provide additional context in support of security operations maturity assessment and planning.

Organizations should use this model as a basis to evaluate their current security operations maturity and develop a roadmap to achieve the level of maturity that is appropriate in light of their resources, budget, and risk tolerance.

	TLM Capabilities	Organizational 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 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; 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 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	• Moving beyond minimal, "check box" compliance, seeking efficiencies and improved assurance • Have recognized organization 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

	TLM Capabilities	Organizational Characteristics	Risk Characteristics
LEVEL 3 Vigilant	• 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	• Have recognized organization is blind to many 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	• 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 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 • 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 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	• 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



CONCLUSION

The world will continue to be hostile.

Threats will continue to target data, and threat actors will be persistent and creative in their efforts. There is no silver bullet on the horizon — no magic AI that will easily solve the problem. To realize an improved security posture and reduce cyber-incident risk, organizations must invest in realizing more mature levels of Threat Lifecycle Management — at an enterprise level across the holistic IT and OT infrastructure.

LogRhythm's Security Operations Maturity Model provides organizations with a roadmap for success. As a leading innovator in cybersecurity, LogRhythm has built a platform that is uniquely capable of helping organizations lower their risk through realizing optimal TLM at lowest organizational TCO. Whether organizations partner with LogRhythm, or go a different route, LogRhythm hopes this model will enable enterprises to plan for the future and realize continuous improvement of their security operations maturity.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organizations on six continents to successfully reduce risk by rapidly detecting, responding to, and neutralizing damaging cyberthreats. The LogRhythm NextGen SIEM Platform combines enterprise log management, user and entity behavior analytics (UEBA), network detection and response (NDR) and security orchestration, automation, and response (SOAR) in a single end-to-end solution. The LogRhythm platform is powered by AI and our patented Machine Data Intelligence Fabric. Its seamlessly integrated solution set is designed to deliver enterprises highest-efficacy Threat Lifecycle Management (TLM) at lowest total cost of ownership (TCO). A LogRhythm-powered security operations center (SOC) helps customers measurably secure their cloud, physical, and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm NextGen SIEM Platform has won many **accolades**, including being positioned as a Leader in Gartner's SIEM Magic Quadrant. **www.logrhythm.com**

About the Authors

Chris Petersen

Chief Product & Technology Officer, Co-Founder

Chris Petersen co-founded LogRhythm in March 2003 and has served as a member of LogRhythm's board of directors and chief technology officer (CTO) since its inception. Mr. Petersen currently serves as LogRhythm's chief product and technology officer (CPO/CTO). In his current role, Mr. Petersen is responsible for product from concept to delivery as the executive leader for product management, engineering, and LogRhythm Labs. Mr. Petersen has served in a variety of other executive roles at LogRhythm including SVP of products, SVP of research & development, and SVP of customer care.

Immediately before co-founding LogRhythm, he led product marketing for the Dragon Intrusion Detection product line as part of Enterasys Networks. He was also a faculty member at the Institute for Applied Network Security, providing expert advice on intrusion detection and security information and event management (SIEM) to Fortune 500 clients across North America.

Mr. Petersen's 20 years of cybersecurity experience began at Price Waterhouse, serving as a senior consultant and developing a proprietary governance risk & compliance (GRC) solution. Mr. Petersen later joined Ernst & Young's National Information Security & Risk Management practice where he held a management role and was responsible for leading the development of software solutions, including eSecurityOnline.com, an internet information security portal and managed vulnerability service. In 1999, Mr. Petersen was an early employee at Counterpane Internet Security, a pioneering managed security service provider (MSSP). At Counterpane, he served as an engineering manager leading

threat intelligence research and supporting the development of SOCRATES, its back-end SIEM technology. Mr. Petersen is a sought-after expert in cybersecurity and is often quoted in media publications. He holds a B.S. in Accounting from Colorado State University.

Andrew Hollister

Chief Architect & Product Manager, LogRhythm Labs

Andrew Hollister brings 20 years of experience in corporate and central government IT and security consulting. In his current role, Mr. Hollister is responsible for ensuring a cohesive architecture for the Machine Data Intelligence, threat, and compliance content delivered through the LogRhythm Knowledge Base. He owns the overall LogRhythm Labs content delivery strategy and related feature areas. He is a platform subject matter expert, having held a variety of other roles at LogRhythm, including director of sales engineering and director of customer success.

Prior to joining LogRhythm, Mr. Hollister was a consultant with engagements encompassing technologies such as Data Loss Prevention, Application Whitelisting, and NG Firewalls.

James Carder

Chief Information Security Officer & Vice President, LogRhythm Labs

James Carder brings more than 21 years of experience working in corporate IT security and consulting for the Fortune 500 and U.S. Government. At LogRhythm, he develops and maintains the company's security governance model and risk strategies, protects the confidentiality, integrity, and availability of information assets, leads the security awareness program, and oversees both threat and vulnerability management as well as the security operations center (SOC). He also directs the mission and strategic vision for the LogRhythm Labs, Machine Data Intelligence, strategic integrations, threat research, and compliance research teams.

Prior to joining LogRhythm, Mr. Carder was the director of Security Informatics at Mayo Clinic where he oversaw Threat Intelligence, Incident Response, Security Operations, and the Offensive Security groups. Prior to Mayo, he served as a Senior Manager at MANDIANT, where he led professional services and incident response engagements. He led criminal and national security-related investigations at the city, state and federal levels, including those involving the theft of credit card information and advanced persistent threats (APTs).

Mr. Carder is a sought-after and frequent speaker at cybersecurity events and is a noted author of several cybersecurity publications. He holds a Bachelor of Science degree in Computer Information Systems from Walden University, an MBA from the University of Minnesota's Carlson School of Management, is an Advisory Board member for Colorado University (Boulder and Denver), member of the Forbes Technology Council, and is a Certified Information Systems Security Professional (CISSP).

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301