LogRhythm

Security Operations Maturity Model

A Practical Guide to Assessing and Improving the Maturity of Your Security Operations

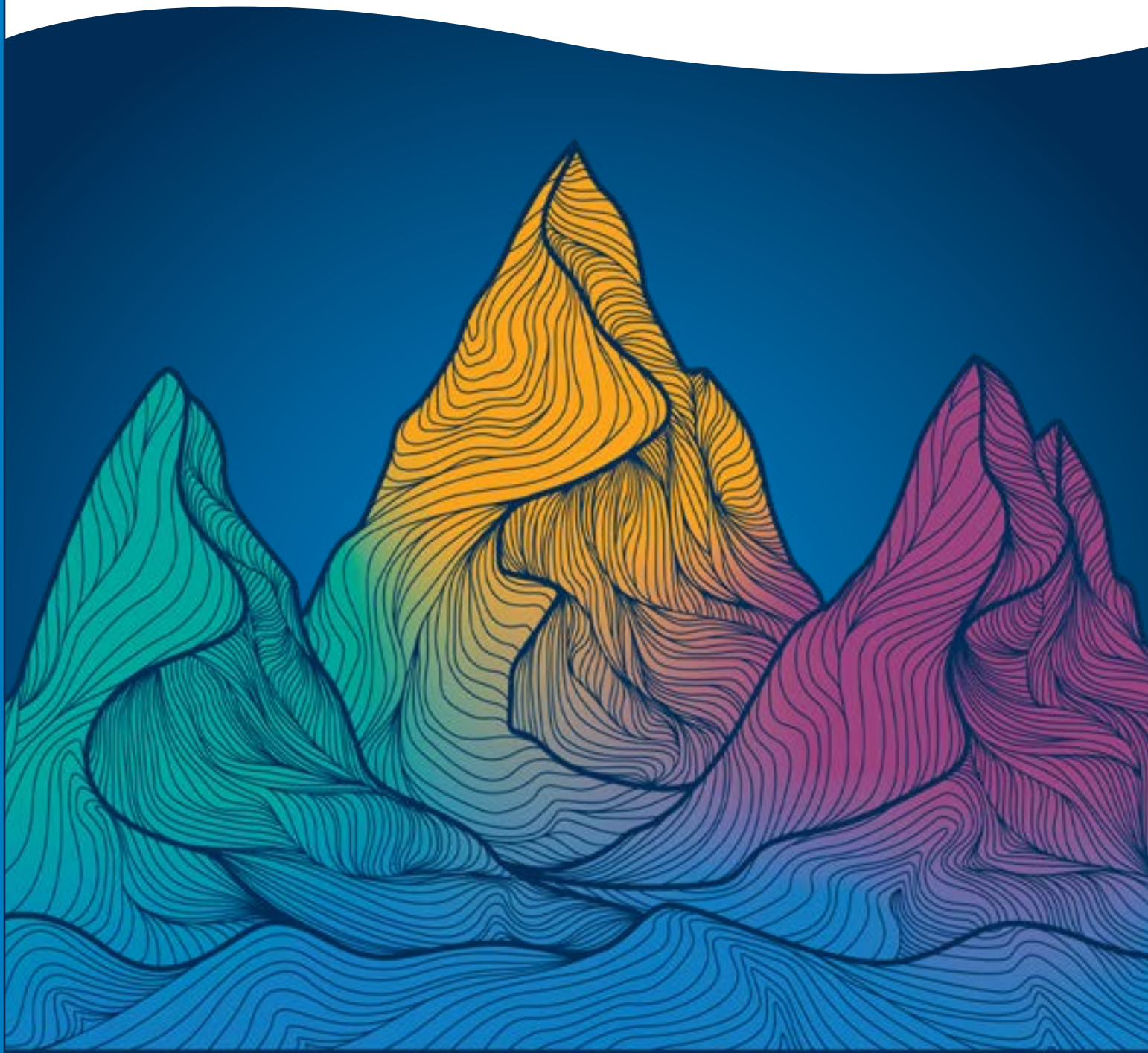


TABLE OF CONTENTS

Security Operations Maturity Model

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 offense against threats, you must ensure that it can handle anything that comes its way. To be effective, you need to mature your SOC to stop 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 cyber-threats. This white paper explores LogRhythm's Security Operations Maturity Model (SOMM), which explains how to measure the effectiveness of your security operations. Through the model, you can learn how to mature your security operations capabilities, improving your resilience to cyberthreats.

In this white paper, you will learn:

- How to understand and measure the capabilities of your SOC
- Details about the LogRhythm Security Operations Maturity Model
- LogRhythm's five levels of security operations maturity
- How to evaluate your organization's maturity level

Understanding and Measuring the Capabilities of a Security Operations Program

Enterprises should think of security operations as a critical business operation. Like any core business operation, organizations should want to measure operational effectiveness to identify whether they are realizing KPIs and SLAs and to help baseline and mature the function. That's why understanding the current status of your security posture is critical. It not only helps you understand your organization's security posture, but it enables you to improve your cybersecurity efforts over the long term.

Through constant monitoring and measuring mean time to detect (MTTD) and the mean time to respond (MTTR)—the primary metrics that indicate the maturity of a security operations program—you will be materially closer to your goal to reduce your organization's cyber-incident risk.

Enterprises should think of security operations as a critical business operation.

Like any core business operation, organizations should want to measure operational effectiveness to identify whether they are realizing KPIs and SLAs and to help baseline and mature the function.

The LogRhythm Security Operations Maturity Model

LogRhythm developed the Security Operations Maturity Model (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 profoundly decrease the risk of experiencing high-impact cybersecurity incidents.

LogRhythm's model draws on a decade of organizational experience serving enterprise SOCs across 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 process and technology improvements. The following figure provides an illustrative example of MTTD/MTTR reductions as maturity improves.

Figure 1. Reduced Time to Detect and Respond to Cyberthreats is Directly Tied to Security Operations Maturity

Score Your Security Maturity

See how the maturity of your security operations ranks. Take LogRhythm's free self-assessment quiz to learn where your organization's capabilities stand.

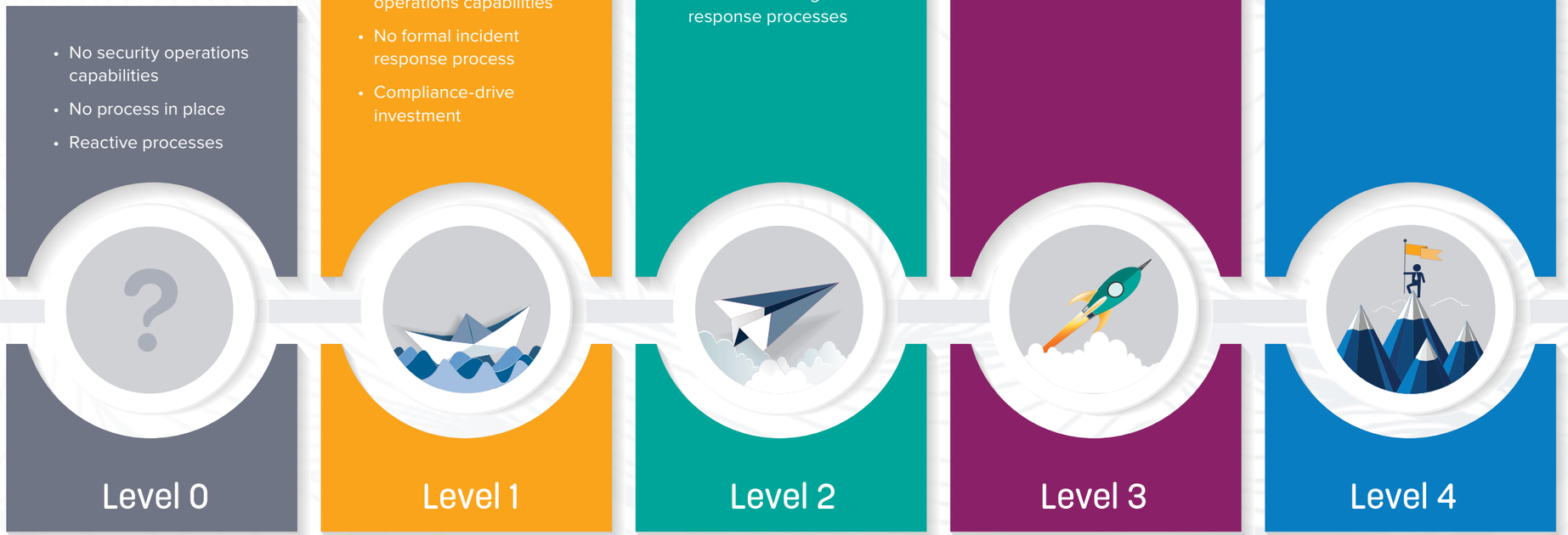
https://logrhythm.com/security-operations-maturity-quiz/

Maturity Model Levels

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

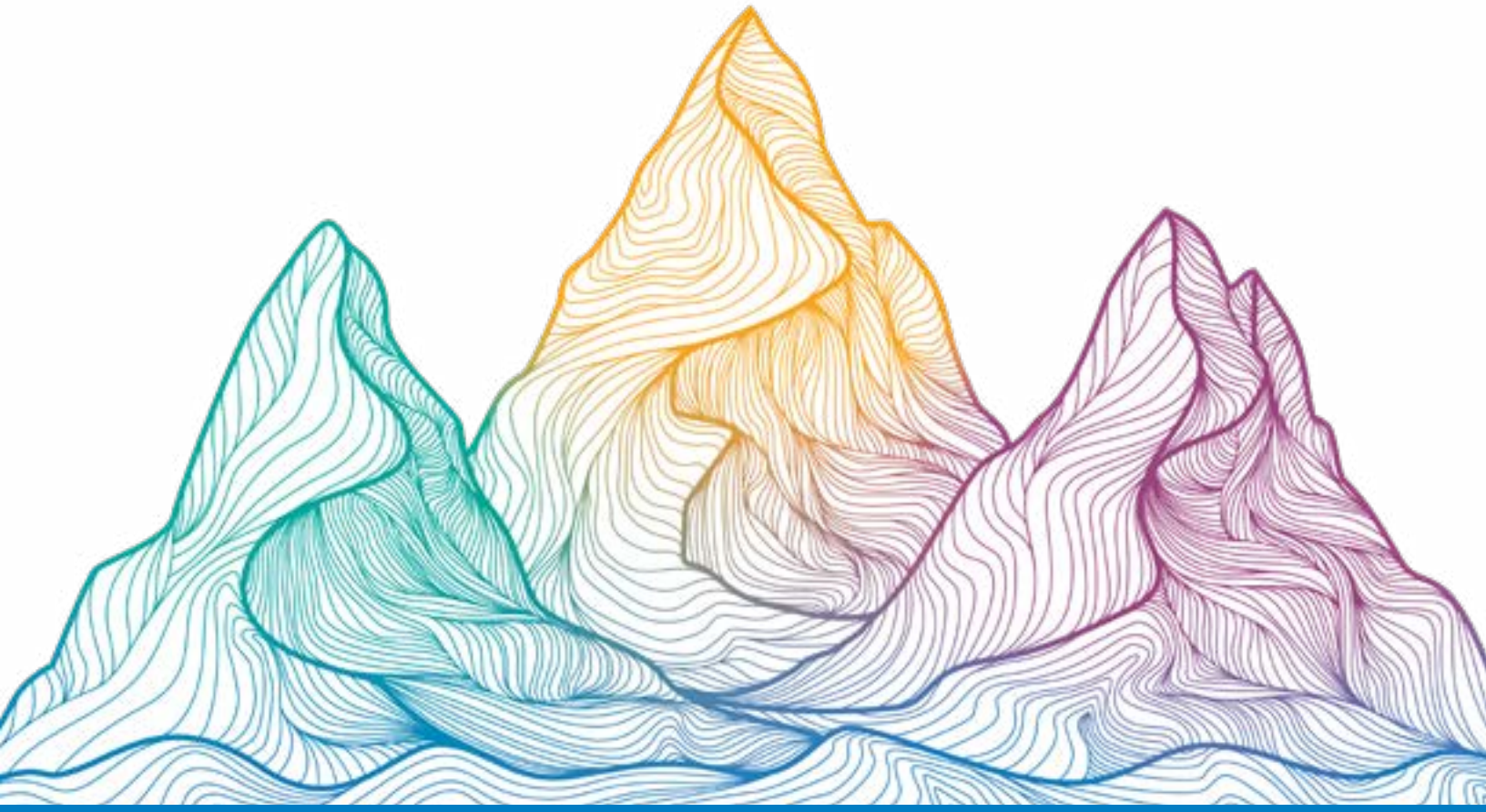
You should use this model to evaluate your organization's current security operations maturity and develop a roadmap to achieve the level of maturity that is appropriate in light of available resources, budget, and risk tolerance.

Reaching Level 4 doesn't mean your organization's maturity has peaked. Security maturity is an evolution and it requires ongoing monitoring to refine your processes.



	Security Operations Capabilities	Organizational Characteristics	Risk Characteristics
LEVEL 0 Initial	• 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 • 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 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) • 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 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 unaware of 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 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 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 unaware of 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 can strategically manage their activities • Extremely resilient to all class of cybercriminals • Can withstand and defend against the most extreme nation-state-level adversary



CONCLUSION

Knowing your organization's current maturity will help you grow and prove the value of your security program.

Threats will continue to target data, and threat actors will be 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.

LogRhythm's Security Operations Maturity Model 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. Whether you partner with LogRhythm, or go a different route, this model will enable you to plan for the future and realize continuous improvement of your security operations maturity.

Expert Tip:

Determine your organization's current level of security operations maturity. Complete the self-assessment and learn how to build a use case for a stronger investment.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering thousands of enterprises on six continents to successfully reduce cyber and operational risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm NextGen SIEM Platform combines advanced security analytics; 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. LogRhythm's technology serves as the foundation for the world's most modern enterprise security operations centers (SOCs), helping 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 countless customer and industry accolades. For more information, visit logrhythm.com

LogRhythm®

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