LogRhythm | SEDARA

Case Study

How Sedara and LogRhythm Helped Secure a Local Government 911 Center

With LogRhythm's advanced security information and event management (SIEM) capabilities and Sedara's expert managed detection and response (MDR) services, organizations gain real-time threat detection, seamless integration, and proactive protection. In this case study, learn how Sedara worked with a local government to identify and remediate gaps in its cybersecurity posture and reduced risk using LogRhythm SIEM.

Background

A medium-sized local government was in the midst of a push to improve cybersecurity. They had made various infrastructure and cybersecurity investments over the months prior. Their focus shifted to a critical department that they felt needed some attention, the 911 center. Their IT systems and processes were managed by the government's central IT team rather than having completely dedicated technical personnel. They also relied heavily on key vendors for the 911 center and wanted to ensure those vendors were performing as expected.

Challenge

Given the high-level of risk that is inherent to 911 centers, it is imperative to have clearly defined policies, procedures, and responsibilities. A GAP assessment needed to be performed in areas including IT systems, process, policy and procedures, and identifying ownership. This includes major vendors that are critical to the functionality of the 911 center. The local government was looking to obtain better insight into the assets, services, and applications within the environment. Not having a clear picture of all assets, the scope of service contracts and responsibility for assets and services, posed an overwhelming task for the already overextended IT staff. They approached Sedara as a trusted cybersecurity advisor to help accomplish this goal.

ORGANIZATION
County 911 Center

INDUSTRY
Local Government

COUNTY SIZE
70,000

RESULTS

- Reduced overall risk to 911 center
- Identified and documented 911 center assets by location
- Identified and documented 911 center service contracts and the status of third-party services
- Created a prioritized list of actions to remediate risks
- Determined ownership and accountability of identified risks, including third-party vendors

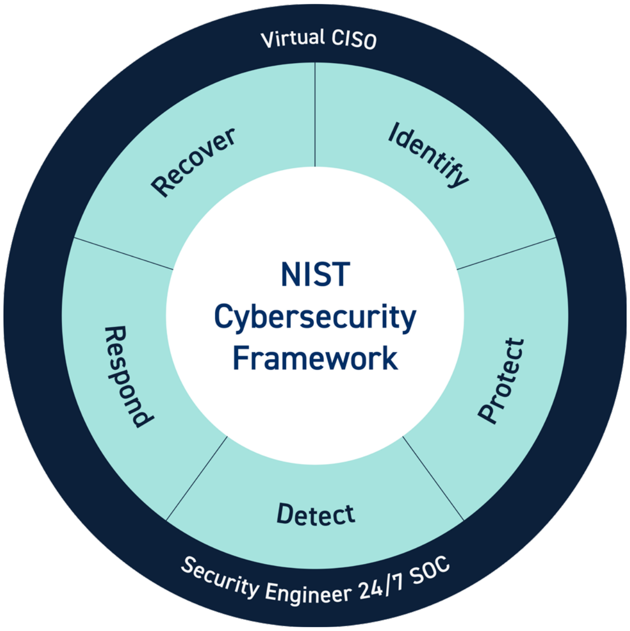
Solution

The GAP assessment created a Plan of Action with Milestones (POAM) to deliver a roadmap for the local government to reduce overall risk, and identify roles and responsibilities. This removed assumptions and clearly defined all components that support the 911 systems.

Sedara selected the National Institute of Standards and Technology Cybersecurity Framework to carry out the solution in three phases.

The NIST Framework

NIST CSF 1.1 focuses on using business drivers to guide cybersecurity activities and cybersecurity risk considerations as part of the organization's risk management processes. The framework enables organizations to apply the principles and best practices of risk management to improve security and resilience. By assembling standards, guidelines, and practices that are currently working, the framework creates a common organizational structure for multiple approaches to cybersecurity. The assessment was carried out in three phases.



Phase 1: Discover and Document

Outlined in the Identify Function of NIST CSF 1.1, you must identify people, processes, and technology involved with relevant assets, business environment, governance, and strategy, and include vendors. Sedara helped with these steps in the following ways:

- Questionnaire: To collect relevant information, Sedara developed a questionnaire concerning the management and operational controls. Questionnaires were also used during interviews.
- Interviews: Interviews with IT support and management personnel enabled Sedara to collect useful information about how systems are managed, and who is in charge of managing them.

Phase 2: Audit and Review Data

In this phase, Sedara worked with the client to discern and differentiate what was important from what wasn't based on interpreting and validating data. This is the last attempt to find any missing data, and to produce supporting artifacts. Sedara helped to:

- Quantify GAPs in people, processes, and technology.
- Review all policy, directives, system, and IT documentation that existed within the organization.

Phase 3: Summarize and Deliver Results

Upon completing the assessment, Sedara provided a detailed Plan of Action and Milestones document to provide actionable next steps. This is the document that identifies tasks needing to be accomplished. It details resources required to accomplish the plan's elements, any milestones for meeting the tasks, and recommended completion dates for the milestones. In this phase, Sedara helped to:

- Prioritize the roadmap to close gaps.
- Create long-term strategy to maintain closed gaps.

Summary of POAM Main Points

Finding	Recommendation
No Disaster [redacted] plan, and an untested failover with limited capacity that may not suffice.	Create and document a disaster [redacted] plan.
C[redacted] System is antiquated, insecure, and has poor vendor support.	Procure and implement a new C[redacted] system with proper documentation surrounding support.
Identified gaps in third-party vendor SLA coverage for processes and procedures that everyone thought were covered.	Identify ownership of all assets, applications, processes, and procedures whether the owner is an internal or a third-party vendor.
Identified multiple critical single points of failure.	Address all critical single points of failure that could lead to downtime.
Lack of visibility into network activity and management.	Implement a long management solution with monitoring to align to NIST best practices.

Conclusion

Through the gap assessment, it became clear that the County 911 center needed to improve observability of all their data and critical assets. Sedara turned to LogRhythm SIEM to reduce risk and give the client one user interface to manage all their data in one place.

Allied together, LogRhythm and Sedara form a powerful cybersecurity force. With LogRhythm's advanced SIEM capabilities and Sedara's expert MDR services, organizations gain real-time threat detection, enhanced visibility, seamless integration, and proactive protection. Unlock the advantages of dedicated support and robust defense strategies, by aligning with a team that helps you implement the critical components of a comprehensive cybersecurity program.

Get in touch with a member of the Sedara team!

www.sedarasecurity.com // info@sedarasecurity.com // +1 (844) 473-3272

Request a demo today! www.logrhythm.com/schedule-online-demo

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 300 // +65 6222 8110 // +61 2 8019 7185 // +97155 642 2224

www.logrhythm.com