

CASE STUDY

How a Hospital Found Relief with Redlegg's MDR



INTRODUCTION

In data security, few sectors face challenges as complex and critical as the healthcare industry.

Hospitals are a goldmine of interconnective systems with highly valuable personal data. Their dependence on technology to deliver services makes them an attractive target for identity thieves and ransomware attacks.

According to HHS, large breaches in healthcare organizations have risen 93% between 2018-2023. A modern cybersecurity approach is necessary to protect patient data and achieve compliance with government regulations and insurance requirements.

For this hospital, maintaining security coverage was especially challenging. With a small internal IT team, limited resources, and responsibility for daily hospital operations, the Director of IT & Security needed additional support to strengthen the organization's security program.

THE PROBLEM

Upon becoming the Director of IT & Security, our client was able to see the full picture of the hospital's security infrastructure.

He found himself in the all-too-familiar predicament of being understaffed, with a limited budget. He lacked the necessary tools to provide 24-hour security. In the early days of his role that meant sacrificing sleep:

"I only have two people, and this is a basically impossible task by ourselves. We needed some help."

To balance the daily IT demands of the hospital and enhance their security operations, the team needed support.

LIMITED STAFF	LIMITED BUDGET	NEED FOR 24/7 SECURITY COVERAGE
ONLY TWO PEOPLE WERE AVAILABLE TO MANAGE THE HOSPITAL'S IT AND SECURITY DEMANDS.	THE HOSPITAL NEEDED TO STRENGTHEN SECURITY OPERATIONS WITHIN A LIMITED BUDGET.	THE INTERNAL TEAM LACKED THE TOOLS AND STAFFING NEEDED TO PROVIDE 24-HOUR SECURITY.

Operational Security challenges

The hospital's internal team was responsible for balancing day-to-day IT operations with ongoing security demands. Limited staffing and resources made it difficult to maintain continuous monitoring while addressing the technical needs of the organization.

The Director needed additional security expertise and around-the-clock coverage that could operate alongside the existing team, allowing internal resources to remain focused on hospital operations.

"Agility is so important because we don't have time, and we don't have the staff or a team to deal with every individual issue. A vendor needs to be extremely quick, and I appreciate that from RedLegg."

WHY REDLEGG

The Director was looking for an agile cybersecurity partner with a personal touch one that he wasn't finding with larger providers.

The director found it difficult to get in touch with the right person to resolve issues quickly.

Unlike those larger corporations, RedLegg offered the availability and dedication essential for addressing the hospital's security concerns and came recommended via a trusted partner.

"The fit was made evident after having our first meeting with RedLegg: I was impressed with the personal nature of the service."

SOLUTION

RedLegg's Managed Detection and Response (MDR) was precisely what the hospital needed. He chose to build this around a managed EDR platform.

Together, RedLegg and the hospital have developed predefined remediation and quarantine playbooks. This allows RedLegg to execute MDR response actions, like host isolation, to prevent lateral movement within the network.

All the above gives the small in-house team the flexibility to tackle other necessary projects and ensure the hospital IT systems are running as efficiently as possible.

REAL-TIME MONITORING

Provides the hospital with 24/7 real-time monitoring by a dedicated team of expert analysts and engineers.

DETECTION LOGIC

The hospital and RedLegg engage in regular status calls to evaluate and refine detection logic.

ANALYSIS & ESCALATION

Analysis and escalation procedures ensure potential security risks are quickly identified and addressed.

RESPONSE ACTIONS

Predefined remediation and quarantine playbooks allow RedLegg to execute MDR response actions, like host isolation.

ONGOING REFINEMENT

Regular status calls support continued evaluation and refinement of detection logic.

IMPLEMENTATION

Deployment of the EDR tool on the hospital's endpoints was quick and painless for The Director and his team.

After the initial setup, and preliminary false positive tuning, the hospital was live with monitoring around the clock.

RedLegg MDR has been non-intrusive for the hospital staff with no impact on their daily tasks.

THE BENEFITS

Backed by RedLegg's detection analysts and platform engineers, The Director has a much larger team supporting him. The hospital's endpoints are under constant monitoring for unauthorized activity, allowing for rapid response to potential threats. According to the Director, RedLegg provides "sleep-as-a-service."



"Threats don't stop at 4:00 or 5:00 when we take off, so having that agent keep an eye out for us has been invaluable and very comforting."

The small IT team also has more flexibility to allocate resources to other projects around the hospital and even grow their team.

Having RedLegg's MDR demonstrates the hospital's proactive approach to security, ensuring that they meet their cyber insurance requirements: and saving money down the road in the event of an attack. The Director is hypervigilant about breaches and attacks happening in the healthcare industry.

He collects "horror stories" from across the country to help. When confronted with their own scare, The Director quoted the COO saying, "thank God you had an MDR in place."

HOW IT WAS DELIVERED

24/7 REAL-TIME MONITORING

Dedicated expert analysts and engineers provide around-the-clock monitoring.



PREDEFINED RESPONSE PLAYBOOKS

Remediation and quarantine playbooks enable response actions such as host isolation.



DETECTION MANAGEMENT

Regular status calls support the evaluation and refinement of detection logic.

CONCLUSION

The Director's decision to partner with RedLegg for Managed EDR has been a major step forward for the hospital.

In healthcare proactive security is a must. The hospital benefits from round-the-clock monitoring, expert analysis, and rapid response capabilities.

This proactive approach not only safeguards patient data but also ensures compliance with regulatory requirements and cyber insurance mandates.

As the healthcare industry grapples with escalating cyber threats, the Director stands confident, knowing that RedLegg is there every step of the way, ensuring the hospital remains resilient.

RedLegg's partnership continues to play a role in the growing security program at the hospital, providing a collaborative and responsive alliance, and helping them achieve their goals.

“**Too much to do, too little staff and trying to keep up is very difficult. That's one of the reasons why I appreciate RedLegg for the service they provide.**”
-Director of IT & Security

IMPACT

- A dedicated team with regular status calls and detection management.
- 24/7 real time monitoring, including event analysis and escalation.
- Light remediation and host isolation.
- Continuous centralized recording, with automated and on-demand reporting.
- Integrated threat intelligence.

FOR MORE INFORMATION REACH OUT:



312.757.4941



dotell@redlegg.com



redlegg.com