How e360 Provided Hybrid Managed Security Services for a Not-For-Profit Health Care Organization

CASE STUDY

ABOUT THIS CASE STUDY:

Our client is a US based large Health Care provider. We have happily accommodated their request to remain anonymous.

HIGHLIGHTS

CHALLENGES

- Lacked cybersecurity expertise
- Inadequate 24/7 monitoring capability
- Missing incident response aligned with MITRE ATT&CK

SOLUTIONS

- Implemented SIEM, SOAR, EDR solutions
- Developed incident response procedures
- Partnered for 24/7 support with expert analysts

RESULTS

- Enhanced security environment and budget management
- Multi-layered security approach with improved visibility
- Reduced overhead costs, optimized resource allocation
- Faster threat detection and response times

CHALLENGES

A prominent health care provider faced significant cybersecurity challenges within its multi-vendor security platform architecture. They struggled with a lack of cybersecurity expertise across the organization, leading to insufficient defenses and suboptimal operational performance.

The limited size of their team hindered continuous monitoring and rapid threat identification, leaving them unable to conduct proactive threat hunting.

Furthermore, the absence of incident response triage protocols and procedures, particularly those aligned with the MITRE ATT&CK framework, raised concerns among the leadership about the organization's ability to respond to incidents effectively.

SOLUTION

To tackle the client's cybersecurity challenges, e360 implemented a tailored solution that integrated Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR), and Endpoint Detection and Response (EDR) technologies.

This was complemented by providing incident response support and developing procedures aligned with the MITRE ATT&CK framework. Collaborating with a remote Managed Services Partner, e360 assigned a Sr. Security lead to provide client focused oversight to a team of highly trained security analysts and engineers, offering 24/7 support and efficient security solutions to meet the client’s needs without the overhead of an in-house team.

RESULTS

The engagement with e360 yielded substantial benefits for the client's security stance, visibility, and financial planning. By employing a layered security strategy that utilized SIEM, SOAR, and EDR technologies, e360 enhanced visibility across the client's environment. This strategy centralized monitoring, automated incident response, and strengthened endpoint security.

Assigning an e360 expert to act as the 'client's voice' creates a more effective impact compared to traditional managed security operations. This method offers dedicated supervision that eliminates the requirement for clients to directly engage in security operations to initiate response actions, pinpoint improvement opportunities, or perform quality assessments on related outcomes.

Additionally, fine-tuning the SIEM and aligning analyst tactics, techniques, and procedures with the MITRE ATT&CK framework facilitated standardized threat detection methodologies, enriched data sets, and decreased the mean time to detection, response, and resolution.

KEY TAKEAWAYS

- The tuning of the SIEM and training of the team were critical to achieving operational speed and efficiency.
- Leveraging external expertise significantly improved resource allocation, enhancing the organization's detection and response capabilities and minimizing the impact of potential attacks.
- The development of incident response playbooks and alignment with the MITRE ATT&CK framework enabled the team to seamlessly integrate with the client's operations, providing 24/7 support and delivering a consistent, repeatable outcome.
- Having multiple security experts on staff added value by enhancing the clients organizational security posture through expert insights, proactive threat management, and tailored security strategies.