CASE STUDY:

EMPOWERING IT CHAMPIONS: A SEAMLESS JOURNEY TO MICROSOFT SENTINEL DESIGN & IMPLEMENTATION

BUSINESS HISTORY

Any good cybersecurity program requires great visibility, future-ready architecture, and a knowledgeable team to back it up whether that's in-house or with an MSSP. For this India-based IT company with over 23,000 employees, an entire overhaul of its existing outdated SIEM was needed to achieve these goals.

Recognizing that its existing SIEM was outdated and unable to meet the demands of the modern cybersecurity landscape, the company embarked on a mission for an entire overhaul of its security infrastructure.

ABOUT DIFENDA

As the winner of Microsoft Canada's Security Impact Award, Difenda stands as the most trusted provider of Microsoft Security services. Difenda accelerates, performs, and validates your Microsoft Security technology, meeting you wherever you are on your cybersecurity journey to maximize your outcomes.

BUSINESS ROADBLOCKS

One of the primary challenges was the presence of an existing competitive SIEM solution (McAfee ESM) that was already in production. Despite its deployment, the current SIEM fell short in meeting the organization's evolving cybersecurity needs, leaving them vulnerable to potential threats. Furthermore, within the existing platform, operational capability gaps were identified, indicating a lack of adequate tools and resources to effectively manage and respond to security incidents.

"When we first considered Microsoft Sentinel for our cybersecurity needs, we were hesitant due to concerns about the cost. However, partnering with Difenda proved to be a game-changer. Their team of experts took the time to understand our specific technical and business requirements, ensuring a tailored solution that perfectly fits our needs. They provided us with an accurate quote and went above and beyond to optimize the implementation to reduce costs without compromising security."

CISO, IT Company

SOLUTION

Difenda was engaged by the Microsoft team to assist in replacing the company's existing SIEM with Microsoft Sentinel.Difenda initiated the engagement by conducting a comprehensive analysis of the IT environment and specific SIEM requirements. We collaborated on a detailed project plan to facilitate the seamless removal of the old SIEM and pave the way for the design, installation, and configuration of Microsoft Sentinel. Difenda's dedicated team meticulously validated custom log sources, analytic rules, and workbooks to ensure they were functioning optimally. With a focus on delivering a best-practice design and deployment, Difenda streamlined log source integration and optimization.

OUTCOME

By addressing clear internal capability gaps, outdated SIEM technology, and vastly improving visibility, the company experienced a significant reduction in operational efforts and an increase in overall team productivity. Difenda's expertise empowered the organization to transition smoothly to Microsoft Sentinel, providing them with unparalleled visibility and proactive threat detection. The optimized cybersecurity environment now keeps the company one step ahead of evolving cyber threats while efficiently managing security operations, ultimately fortifying their defence and achieving enhanced cybersecurity resilience.

- INCREASED ENTERPRISE-WIDE VISIBILITY
- ENHANCED RESPONSE CAPABILITIES
- INCREASED TEAM PRODUCTIVITY
- REDUCED COST OF LOG INGEST

CONTACT A MICROSOFT SECURITY EXPERT TODAY:

www.difenda.com | sales@difenda.com | 1-866-252-2103

Member of Microsoft Intelligent Security Association

Microsoft Intelligent Security Association

Microsoft Canada Impact Awards 2023 WINNER