DIFENDA

Microsoft Partner
Microsoft
Gold Security
Gold Cloud Platform
Gold Application Development
Advanced Specialization - Threat Protection

Member of
Microsoft Intelligent Security Association
Microsoft

A sizable SaaS firm eliminates operational challenges from their legacy security stack by implimenting a new SIEM solution without hiring additional security staff.

At-A-Glance

Customer: Large SaaS based Technology Firm

Country: Canada

Industry: Technology

Products and Services: Microsoft Sentinel

Key Drivers & Business Outcomes

The goal of any modern cybersecurity program is to streamline the people, processes, and technology that drive an organization forward. Complex operational requirements, poor visibility into security processes, legacy infrastructure, and increasing demand meant internal teams were stretched too thin to prioritize security. The added challenge of hiring, training, and retaining security staff only compounded that problem.
The need for a solution that leveraged the latest in cloud technology, automation, and machine learning was clear.

This company needed streamlined security technology and specific controls to increase their visibility into the SIEM log and alert configuration. The solution would be to leverage a future-proofed platform to continuously tackle the ever-advancing technology, while consolidating their investments and partnerships.

Our solution: all core security technologies seamlessly integrated with the Microsoft Sentinel SIEM, including enhanced detections from native Microsoft security technologies.

Customer Situation

Overrun by operational challenges created by running their legacy, open source SIEM stack was taking its toll on the IT and security teams. Implementing a new SIEM can be a difficult process which could be a distraction to other critical projects, so waiting for the right time was key.

They had completed a proof of concept (POC) and decided to outsource the heavy lifting to accelerate their implementation timeline to migrate to the modern solution and freeing up more operational resources to work on other priorities.

Solution

Difenda was contracted to provide a managed SIEM threat detection solution.

The scope of the project included a hybrid environment where on-premise and cloud resources were leveraged for maximum visibility. Difenda provided a best-practices design and deployment, log source integration and optimisation, as well as use case, dashboard, and automation development. As part of the detection strategy, Difenda was also able to leverage Azure AD, Microsoft Information Protection, Microsoft Defender for Cloud and Microsoft Defender for Cloud Apps. Simultaneously, the customer initiated a project to migrate from a competing EDR vendor to Microsoft Defender for Endpoint, that was also integrated with our solution.

Win Insights

Customized infrastructure and threat intelligence to meet customer needs

Hybrid security environment promoting further cloud adoption

Leveraging Microsoft security technologies for visibility

Migration to Microsoft from leading competitive solution