DIFENDA

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

Member of
Microsoft Intelligent Security Association
Microsoft

BILLION-DOLLAR COMPANY ACHIEVES SEAMLESS SIEM OVERHAUL WITH MICROSOFT SENTINEL

Key Drivers & Business Outcomes

Any good cybersecurity program requires good visibility, future-ready architecture, and a knowledgeable team to back it up, whether that's in-house or handled externally by an MSSP. For one India-based IT company, an entire overhaul of their existing outdated SIEM was needed to achieve these goals.

By addressing clear internal capability gaps, outdated SIEMs, and vastly improving visibility, Difenda was able to enhance their response capabilities and greatly reduce operating costs across their platform.

Most importantly, this company needed to vastly improve their security operations visibility. To do so, they required a modern platform with future supportability (Microsoft Sentinel). We deployed the cloud-native platform with broad integration support following industry best practices to give the customer confidence for future growth and advancing technology with a use-based pricing model, resulting in improved total cost of ownership (TCO)

At-A-Glance

Customer
Billion-Dollar Multinational Company

Country:
India

Industry:
IT

Products and Services
Microsoft Sentinel, Azure Active Directory, Azure AD Identity Protection, Azure Security Center, Defender for Endpoint, Defender for M365, Microsoft Cloud App Security, Intune

See The Difference A Personalized Approach To Cybersecurity Makes

CONTACT US TO REQUEST A DEMO: www.difenda.com | sales@difenda.com | 1-866-252-2103

Value Provided & Business Outcomes

The customer now possesses greatly increased enterprise-wide security visibility and enhanced response capabilities. This solution also decreased all operational efforts to maintain the platform. Decreased operational efforts of our new solution came from time saved integrating new log sources, maintaining detection capabilities, agent patching/management, and platform maintenance. Now, around 15 SOC users leverage the solution; plus additional IT operational users.

What was once a challenging daily operational support of a legacy SIEM platform which kept teams busy and bogged down, was transformed greatly by increasing productivity and cost effectiveness. Through using existing capabilities augmented by modern, future-proof capabilities of the cloud native Microsoft Sentinel platform, while also reducing operational overhead freeing up time for higher value work, the desired outcomes were realized.

Customer Situation

For this multinational company with over 23,000 employees, it became clear that their existing security tools were failing to keep up, and as they continued to grow this issue only compounded. An update was needed to get them back on track for present and potential future cybersecurity requirements.

This company had several significant obstacles to overcome in order to reach their desired security outcome. These challenges included an existing, competitive SIEM (McAfee ESM) which was already deployed and in production, as well as operational capability gaps identified with the existing platform, both of which drove a desire to enhance security operations capabilities with a modern SIEM solution.

Partner Solution: Services & Microsoft Technology

Difenda was engaged by Microsoft India to assist the customer with replacing their existing SIEM with Microsoft Sentinel. We focused on providing the customer with a best-practices design and deployment, log source integration and optimization, a Custom Analytic Rule, Workbook, and Logic App development.

The deal was secured with a professional services Proof of Concept ("POC") to demonstrate the integration skills and experience of our team at Difenda. We successfully provided them with a full production implementation, playbook development, integration of custom sources, product and operational training. We also planned and implemented a detailed hand-off to their customer's operations team so that they could retain full ownership of the program, with our assistance when required.

Win Insights

- Integration with enterprise-grade ITSM platform
- Microsoft-led McAfee ESM migration capabilities.

See The Difference A Personalized Approach To Cybersecurity Makes

CONTACT US TO REQUEST A DEMO: www.difenda.com | sales@difenda.com | 1-866-252-2103

Lessons Learned

What worked best here was Difenda streamlining the scoping process and highlighting the communication of success factors to ensure future projects with this company and others are a success.

The ITSM platform integration we developed for this project can be reused for other customers in similar circumstances. Our new response playbook can also be easily leveraged in future use cases reducing the amount of manual processes and new intellectual property required.

DIFENDA

Connect with Us Today

www.difenda.com
1 (877) 555-1234 | sales@difenda.com

See The Difference A Personalized Approach To Cybersecurity Makes

CONTACT US TO REQUEST A DEMO: www.difenda.com | sales@difenda.com | 1-866-252-2103