THE CHALLENGE

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 For this India-based IT company with over 23,000 employees, an entire overhaul of its existing outdated SIEM was needed to achieve these goals. The company had several significant obstacles to overcome including an existing competitive SIEM (McAfee ESM) which was already in production. They were also facing operational capability gaps identified within the existing platform; both of which drove a desire to enhance security operations capabilities with a modern SIEM solution.

THE SOLUTION

Difenda was engaged by the Microsoft team to assist in replacing the company's existing SIEM with Microsoft Sentinel. By addressing clear internal capability gaps, outdated SIEM technology, and vastly improving visibility, Difenda was able to enhance this organization's response capabilities and greatly reduce operating costs across its platform. We focused on providing the customer with a best-practice design and deployment, log source integration and optimization, a custom Analytic Rule, Workbook, and Logic App development. These solutions decreased operational efforts and increased productivity for their team.

OUTCOMES

- INCREASED ENTERPRISE-WIDE VISIBILITY
- ENHANCED RESPONSE CAPABILITIES
- INCREASED TEAM PRODUCTIVITY
- INCREASED COST EFFECTIVENESS

CONCLUSION

The key to success here was Difenda streamlining the scoping process and prioritizing 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. Their new response playbook can also be easily leveraged in future use cases reducing the number of manual processes and new intellectual property required.