CASE STUDY:

ENHANCING OPERATIONAL TECHNOLOGY SECURITY WITH DEFENDER FOR IOT PROFESSIONAL SECURITY SERVICES

BUSINESS HISTORY

The Pharmaceutical Organization, a prominent player in the healthcare sector, had recently undergone a period of rapid expansion, significantly increasing its attack surface. However, this growth inadvertently led to a surge in cyber threats and vulnerabilities. Despite their investment in Microsoft Security E5 licenses, the organization needed assistance in fully harnessing the potential of these tools. As a result, they were in urgent need of a Managed Security Services Provider (MSSP) that could swiftly replace their bespoke tools, enhancing their security posture.

ABOUT DIFENDA

Named Microsoft's 2023 Security Impact Award Winner for delivering excellence and innovative end-to-end security solutions. Difenda is proud to be a long-standing Microsoft Partner, an early achiever of MXDR verified status, a member of the Microsoft Intelligent Security Association (MISA), and a holder of the Microsoft Threat Protection Advanced Specialization and Cloud Security.

BUSINESS ROADBLOCKS

The Pharmaceutical Organization faced several significant challenges that impeded its cybersecurity endeavors. he organization was reliant on a multitude of custom security tools, and they lacked comprehensive awareness of the technologies operating within their Operational Technology (OT) environment. This led to a lack of visibility into their Operational Technology (OT) environment and hindered their capacity to efficiently address security incidents and vulnerabilities. On top of that the organization was constrained by a lean in-house security team, they struggled to cope with the extensive demands of monitoring, threat detection, and incident response.

"Our work with Difenda is part of an ongoing effort to maintain operational safety and resilience, including the reduction of cybersecurity risks. The team helped us understand the security of our OT environments without disrupting our daily operations."

- Principal IT Security Engineer

SOLUTION

Difenda collaborated with the Pharmaceutical Organization to implement a Microsoft Defender for IoT Professional Services solution. Leveraging the existing Microsoft Security E5 tools, Difenda deployed Microsoft Defender for Endpoint and Sentinel to establish a robust security foundation. Deploying Microsoft Defender for IoT at a key facility to improve OT/ICS asset visibility. Asset classification through a High Consequence Event Assessment further strengthened their cybersecurity readiness, ensuring effective protection of their OT environment. This focused approach fortified their defenses against potential threats in this critical operational area.

OUTCOMES

A key achievement was the implementation of a layer-on approach to OT security, which prioritized minimal disruption to the organization's critical OT processes. This allowed for the successful deployment of Microsoft Defender for IoT and MXDR for OT, significantly improving visibility in the OT environment while maintaining the operational continuity of vital processes. Moreover, the reduction in reliance on custom security tools streamlined security operations, enhancing efficiency and incident response capabilities without causing disruptions to core operational activities. Additionally, asset classification and business impact context enhanced risk management, enabling informed decisions and the development of tailored security strategies for heightened cybersecurity readiness.

- INCREASED VISIBILITY INTO OT ASSETS AND OPERATIONS
- SIMPLIFIED SECURITY OPERATIONS, REDUCING SECURITY ENVIRONMENT COMPLEXITY
- ENHANCED UTILIZATION OF MICROSOFT SECURITY INVESTMENT
- ENHANCED SECURITY POSTURE IN THE OT ENVIRONMENT

CONTACT A MICROSOFT SECURITY EXPERT TODAY:

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

Microsoft Solutions Partner Security Specialist Cloud Security Threat Protection

Microsoft Intelligent Security Association Microsoft

Microsoft Canada Impact Awards 2023 WINNER