Enhancing Cyber Resilience through the Azure Cloud Migration Environment

Objective

We consulted with one of the leading healthcare companies and the objective was to build a seamless cyber security operations center providing 24/7 incident response management that came as a business need out of the Azure Cloud Migration plan.

Result

The initial objective was to transfer workloads from on-premises to the Azure cloud, encompassing applications, AD infrastructure, and servers. The client also sought our expertise in Security Information and Event Management (SIEM). In a short timeframe, our cybersecurity technical consulting team swiftly provided visibility across their infrastructure and devised an improved Security Incident Response plan, along with migration strategies within a few weeks of onboarding. Furthermore, our extensive proficiency with tools such as Wireshark, Solarwinds, Azure Sentinel, CyberArk, IBM QRadar, Sailpoint, etc., proved instrumental. This not only enabled the establishment of a 24/7 Security Operations Center (SOC) but also empowered us to offer comprehensive expertise in the entire cybersecurity technology toolkit to the client—from Risk Awareness and Assessment to Design, Implementation, and the development ofPolicies and Frameworks.

Challenges

The challenge at hand involved constructing a 24/7 Security Operations Center with an incident response team to address threats and vulnerabilities, offering centralized support for approximately 10 client locations. This task was particularly demanding as our teams were concurrently engaged in the midst of an Azure cloud migration, requiring centralized technical expertise to meet the expanding needs. Additionally, there was a challenge in establishing a comprehensive response plan for various types of cyber threats.

Solution Highlights

Our expertise knowledge of security tools, processes know-how and more importantly, understanding the customer pain-points well in time.