Inspira enhances its Security-as-a-Service offerings with modernized SOC powered by IBM QRadar

May 15, 2023

Today, organizations need to detect and defend against cyberattacks around-the-clock to ensure their digital assets are protected from increasingly sophisticated and always on threat actors. If not done correctly, it could lead to significant losses and erosion of customer trust. In fact, IBM's 2022 Cost of a Data Breach report found the cost of a data breach averaged USD 4.35 million globally in 2022, a 2.6% increase from 2021.

"Cybercriminals are exploiting these circumstances to force organizations to pay increasingly higher ransoms. We have reached a point where cyberattacks are evolving into market stressors, hurting the economy," explains **Viswanath Ramaswamy, Vice President, Technology, IBM India and South Asia** . "Majority of businesses around the world have raised their prices because of data breaches, contributing to inflation, and inadvertently passing the cost on to customers," he added.

While many organizations are investing heavily in upgrading their security architectures and building internal security teams, yet these internal security teams often lack resources and expertise to be as effective as the current scenario demands. This is even more pronounced for small and medium sized enterprise who simply do not have the resources required to meet the rapidly evolving security challenges.

This is why, Inspira Enterprise India Limited (a global Cybersecurity Risk Management & Digital Transformation service provider) is modernizing their Security Operations Center (SOC) to provide Managed Security Services to small and medium enterprise customers across industries like BFSI, manufacturing, eGovernance, telecom, among others.

"Over the years, the kind of attacks and viruses have only increased in complexity. The good news however is that organizations can now deploy security operations-as-a-service that ensures improved 24×7 security while being cost-effective," says **Manoj Kanodia, Chief Executive Officer, Inspira Enterprise**. "Having access to our state-of-the-art SOCs significantly increases security effectiveness, operational efficiency and long-term business value with a proactive Incident Response, Breach Response, Managed Detection and Response

Services," he added.

As Inspira began work modernizing their SOC service, they did an extensive customer requirement analysis so that they could implement the right security products and tools that would meet those needs. Modernizing a state-of-the-art SOC can be technically challenging. It requires adequate tools for monitoring and management to keep up with the rapid shifts in the systems environment being monitored. Automation and integration are essential to avoid issues like repetitive tasks as they instantiate standard response workflows to security incidents, limiting incident response speed. Finally, clients across various industries are using different infrastructure platforms which often makes integration of multiple end devices challenging.

An IBM Ecosystem partner, Inspira focused on IBM technology, particularly the IBM Security QRadar XDR suite. They chose the QRadar SIEM solution to oversee the security information and event management (SIEM) needs of their managed security service. The QRadar technology offers Inspira a holistic view of the customer networks that it monitors alongside AI-backed threat detection and log analysis. This allows Inspira to rapidly detect advanced security threats in their customer's network with real-time analytics, changing their defense strategy from reactive to proactive by using accurate and contextual threat data.

According to **Viswanath Ramaswamy**, "A good SIEM architecture needs to be supported by AI to deliver prioritized, high-fidelity alerts so that security analysts can focus on alerts that matter. It also has to be quick to deploy because every second counts when responding to threats. Finally, it must be open to integrating existing tools and technologies. Therefore, IBM has invested heavily in these areas to ensure our security portfolio supports the entire SOC workflow — including visibility, detection, investigation and response — across multiple tools and data sets."

"QRadar was a logical choice for us because it allowed us to gain greater visibility into insider threats, uncover anomalous behavior, quickly identify risky users and generate meaningful insights for our teams to act upon. On top of that it comes with out-of-the-box use cases aligned to the MITRE ATT&CK framework. It also enabled us to quickly onboard custom log sources for analysis and create new log sources based on incoming threat event data," noted **Manoj Kanodia.**

He further adds, "We are a trusted cybersecurity solutions partner for Indian and global enterprises, and if we are going to offer world class service to our clients, then we need security products that match global standards. Hence having observed that QRadar SIEM in the Gartner Magic Quadrant since 13 years gave us great confidence."

With the help of its new/ modernized SOC service, Inspira is offering a comprehensive, robust security monitoring and management solutions at a price point of roughly <1.5 full-time equivalents (FTEs) whereas staffing an internal team would require 6-8 FTEs. This service is seeing strong demand and Inspira is already working with 30+ active clients across four countries.

Blog Categories

Secure