

A background image showing a person in profile, wearing a headset, looking at multiple computer monitors displaying data and charts. The scene is dimly lit with a blue color cast.

DEMONSTRATED PERFORMANCE

NEXTGEN SIEM IMPLEMENTATION

Federal Regulatory Agency

THE CHALLENGE

EFFICIENT, EFFECTIVE NETWORK SECURITY

Indigo IT provides full-spectrum IT support, which includes cybersecurity and IT Security Program services, to a Federal Regulatory Agency. To ensure the protection of sensitive data as it traverses the IT Infrastructure, we address security controls at the program level, in addition to securing the general support systems, applications, resources, and data.

The Agency lacked a comprehensive understanding of security events happening on their network and required a solution that provided visibility, event data consolidation, correlation, and logging controls to secure the network and remain compliant with increasingly stringent FISMA requirements.

THE SOLUTION

NEXTGEN SIEM IMPLEMENTATION

Indigo IT worked with the Agency to prioritize business, FISMA, and cyber response requirements to guide our analysis of existing Security Information and Event Management (SIEM) tools. During our analysis, we evaluated ingestion capabilities, alerting functionality, customization options, breadth of device support, environment logging requirements, and cost. Understanding the extent of the surface to be monitored and the large volume of data to be evaluated, we also took into consideration the balance of data ingestion and processing needs with cost and capabilities for the environment. Following our evaluation, we implemented a NextGen SIEM platform within the Agency that fulfills all of these requirements. This platform enables logging, monitoring, and event management from a single dashboard, allowing security engineers to triage data and respond to network events more efficiently and at mission speed.

THE INDIGO IT DIFFERENCE

COLLABORATIVE SECURITY

Indigo IT was able to understand and respond to the customer technical requirements, unique operational needs, required customizations, response capabilities and expectations. Due to our long established relationship with the Agency, we also collaborated with the IT Security Team to craft executive messaging during the evaluation and implementation of the SIEM solution.

Due to the full-spectrum nature of our program, we were able to implement a constant feedback loop that includes not just the IT Security Team, but also our engineering and helpdesk staff. This collaborative process allows us to share data and associated correlations, which assists in troubleshooting, and improves customer support from Tier 1, through engineering.