Stock Group Analytics BEP Operation's Modernization

The Customer

The Bureau of Engraving and Printing (BEP), under the U.S. Department of the Treasury, designs and produces the nation's paper currency and other secure documents. With mission-critical operations spanning cybersecurity, IT modernization, and physical production oversight, BEP's Office of Critical Infrastructure and Information Technology Security (OCIITS) plays a pivotal role in safeguarding sensitive data and ensuring operational continuity. Within OCIITS, the Security Operations Center (SOC) manages BEP's cybersecurity monitoring and response initiatives. The Cyber Data Analytics Program (CDAP), a specialized function within the SOC, utilizes data analytics to strengthen cyber visibility, optimize workforce allocation, and enhance strategic planning. CDAP is a newly established initiative, launched only one year ago, and SGA has supported its development since inception—building the foundational data analytics capabilities using diverse streams of cyber data across BEP's security ecosystem.

The Challenge

To maintain its security posture and modernize operations across geographically distributed facilities, BEP needed:

- Real-time visibility into workforce distribution and SOC resource capacity.

- Centralized dashboards to replace fragmented reporting across Qlik, Tableau, and Power BI.

- Predictive insights to assess cybersecurity posture and operational performance.

- Compliance-aligned solutions to meet mandates under Executive Orders, FISMA, **Zero Trust, and FedRAMP.**

Stock Group Analytics's Solution

SGA supported the Office of Critical Infrastructure and Information Technology Security (OCIITS) by delivering advanced data analytics, AI/ML integration, and cybersecurity insights that enhance operational resilience, security posture, and executive decision-making across the agency.

- **Governance and Strategy Support:** Provided strategic advising to help CDAP define and document data governance, Data and AI strategies, and program chartering aligned with Treasury-wide modernization objectives

- **SOC Workforce Analytics:** Built visual tools to monitor SOC staffing, track day-to-day coverage, and support workforce realignment during reduction in force (RIF).

- **Cyber Operations Monitoring:** Designed and implemented comprehensive analytics pipelines and monitoring tools that ingest, normalize, and visualize large volumes of cyber event data from a variety of sources.

- **AI/ML Integration:** Developed anomaly detection models and early warning indicators to flag deviations in user behavior, system access, and threat intelligence feeds.

- **Leadership Dashboards:** Created SharePoint-integrated dashboards and situational awareness modules tailored to executive decision-making needs.

- **Compliance Mapping:** Built data models and reporting templates aligned with Treasury cybersecurity standards and federal mandates such as FISMA, Zero Trust, and Executive Order 13960.

Benefits

SGA's solutions revolutionized BEP's operations, delivering measurable impacts:

- **Cost Savings**: Saved hundreds of thousands of dollars by retiring legacy visualization tools and consolidating reporting in Power BI.

- **Strategic Insights:** Equipped leadership with real-time visual tools to monitor cybersecurity posture and SOC performance.

- **Mandate Alignment:** Delivering analytics frameworks aligned with Zero Trust, FISMA, and Executive Order 13960.

- **Data-Driven Security:** Enabling proactive cyber monitoring through anomaly detection and workforce coverage metrics.