



## FEDERAL BUREAU OF INVESTIGATION VIOLENT CRIMINAL APPREHENSION PROGRAM (VICAP)

### TECHNICA SOLUTION:

Technica recommended open source Elasticsearch technology enhanced through Technica's internal research and development efforts. The prototype was built using an Elasticsearch instance created in AWS GovCloud. It ingests data by pulling from the database using a four-step interrelated process:

- 1 Data is reshaped for analysis
- 2 Data is extracted from the database in JSON format
- 3 Extracted documents are transformed for compatibility with Elasticsearch
- 4 Data is formatted and then loaded into Elasticsearch for querying, reporting and visualization

### BENEFIT TO THE FBI:

Technica's prototype incorporated state of the art data analytics technologies such as Elasticsearch, Kibana and Logstash, which enabled a host of additional program capabilities including inclusion/exclusion queries, multiple query dimensions being returned in a single list, and customizable/interactive searches that allow agents to see previously uncorrelated results in a variety of different displays such as tables, graphic charts and geospatial views.

### MISSION CHALLENGE:

The FBI needed a virtualized & analytical-based database to replace their legacy technology used to execute search queries against multiple databases.

The FBI ViCAP team was designated a 2018 Public Sector Innovation Winner by 1105 Media.



## U.S. ARMY RESEARCH LAB SMARTFOG COMPUTING PLATFORM

### TECHNICA SOLUTION:

In conjunction with the ARL's Computational and Information Sciences Directorate (CISD), Technica has developed an architecture-agnostic microservice framework incorporating load distribution algorithms with data localization as well as best practices for heterogeneous tactical High-Powered Computing (HPC) transactions.

### BENEFIT TO ARL AND THE WARFIGHTER:

This innovative program will result in software prototypes, algorithms, computational frameworks and models to substantiate a SmartFog Computing Platform. When production ready, this capability will improve the distribution and assimilation of digital battlespace information.

### MISSION CHALLENGE:

The U.S. Army Research Lab (ARL) desired a Fog Computing Platform (FCP) that supports state-of-the-art capabilities in the distribution and/or assimilation of real or simulated digitized battlespace information.



## U.S. AIR FORCE COMBINED AIR OPERATIONS CENTER-EXPERIMENTAL (CAOC-X)



### MISSION CHALLENGE:

The U.S. Air Force Air Combat Command needed a capability to rapidly scan large amounts of data throughout the environment when certain predetermined events occurred that changed the baseline or security posture such as configuration changes, firewall changes or unauthorized logon attempts & then report in near real time.

### TECHNICA SOLUTION:

Technica merged its big data analytics and cybersecurity capabilities developed through its internal Research & Development Lab initiatives to deliver a zero-cost solution that scanned, reported, and created NIPR and SIPR email alerts for predefined incidents which provided CAOC-X with the desired visibility and situational awareness.

### BENEFIT TO CAOC-X:

By incorporating Technica's best-in-class analytic insight and in-depth knowledge of cyber defense, CAOC-X achieved a 3-Year ATO for the AOC WS, improved situational awareness and Cybersecurity, while gaining numerous accolades for an outstanding RMF package across the Weapon System.

**“Technica’s approach was the most forward-thinking solution they have seen implemented to date.”**

- Colonel William Dayton  
ACC A5



## U.S. ARMY LOWER ECHELON ANALYTIC PLATFORM (LEAP)

### MISSION CHALLENGE:

U. S. Army desired a Lower Echelon Analytic Platform for incorporation into their Big Data Platform (BDP) for processing large raw data sets on limited compute & storage platforms.

### TECHNICA SOLUTION:

Through an OTA, Technica prototyped and integrated into the Army's BDP two separate data analytic capabilities to solution data processing on limited platforms – Anomaly Detection and Time Series. Additionally, Technica integrated Federated Learning into the anomaly detection service. The Anomaly Detection prototype used an auto-encoder neural network to detect anomalies. The Time Series prototype uses a long-short term memory (LSTM) neural network for time series prediction. Both analytics used Keras API for building neural networks, incorporated TensorFlow for machine and deep learning capabilities, and used PyInstaller to package the analytics. A front-end UI monitors and displays the results of both prototypes.

### BENEFIT TO U.S. ARMY:

The incorporation of Technica's machine learning prototype capabilities into the Army's BDP allows for enhanced capabilities such as unsupervised learning opposed to signature-based network monitoring in detecting anomalies and defending against zero-day attacks.

Technica™ is a trademark of Technica Corporation. 121721

**Technica™**