USSF U.S. AIR FORCE

AFRL

SNICH

SENSOR NETWORK INTELLIGENT CORRUPTION HUNTER

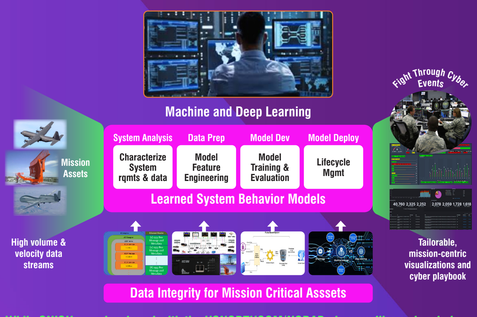
DEPLOYED AT EASTERN AIR DEFENSE SECTOR (EADS)

On 21 August 2020, Securboration Inc, with support from the Air Force Research Laboratory (AFRL) Rome Research Site, successfully deployed the Sensor Network Intelligent Corruption Hunter (SNICH) software at the North American Aerospace Defense Command's Eastern Air Defense Sector in Rome, New York. Installed on EADS' Battle Control Center operations floor, SNICH monitored select portions of the Federal Aviation Administration Telecommunications Infrastructure (FTI) and immediately detected anomalous data flowing through its complex network of equipment and sensors.

Since SNICH's initial deployment, EADS has received numerous enhancements and the software has been deployed to the Western Air Defense Sector (WADS) at Joint Base Lewis-McChord in Washington state. The technology has undergone numerous engineering tests and the Defense Accounting Office (DAO) has issued a Certificate to Field (CTF) for SNICH allowing government organizations to install the software on their network.

EADS and WADS are responsible for the air defense of the continental United States. The Sectors' Battle Control Centers take data from radars and sensors and use it to build and maintain a continuous air picture, which Airmen monitor in real-time for potential threats.

These Airmen receive vast amounts of data that must be quickly processed for identification, location, activity, and course-of-action decision-making. Securing these networks against traditional cyber-attacks is critical, as is ensuring the integrity of the data that feeds into the mission systems.



While SNICH was developed with the USNORTHCOM/NORAD air surveillance in mind, the technical concept is based on the development of an Extensible Architecture for Mission Data Resiliency to include components and processes for adversary counter deception.

Alex Sarnacki

Company:
Securboration Incorporated

Company POC:
Mr. Timothy Kesecker
Project Lead

Contract Number:
FA8750-19-C-0099

SBIR/STTR Topic Number:
AF17B-T004

Title of SBIR/STTR Topic:
Joint Collaborative Augmentation for Sense Making Environment (JCAUSE) / Sensor Network Intelligent Corruption Hunter (SNICH)

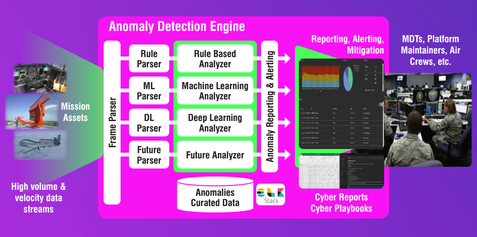
Air Force Technical POC:
Mr. Jason Bryant
Branch Chief
AFRL/RISA

Alex Sarnacki
Computer Scientist/COTR
AFRL/RISB

Sponsoring Organization:
Air Force Research Laboratory
Rome Research Site

SNICH is defensive cyber technology that assists Air surveillance operators with monitoring and understanding the data and behavior of their mission systems to verify that information from their sensors is consistent and reliable. The software passively monitors mission-critical sensor streams to counter adversarial deception, detect, and communicate the evidence of anomalies. SNICH combines advances in several fields of knowledge including machine learning, statistical algorithms, cyber security, and visualization with expertise from the command-and-control realm. SNICH is a new capability that will empower ultra-time-critical mission decisions and dramatically enhance the ability of mission defense teams, and their commanders. For the NORTHCOM mission, the projected cost savings of SNICH can be measured in terms of lives and resources saved resulting from reduced operator response times and circumvention of committing limited resources (manpower, equipment, money, etc.) to scramble aircraft against false targets.

SNICH is based on an open architecture and provides an extensible – modular design for adding new analyzers, data streams. A central piece of SNICH is to leverage Artificial Intelligence (AI) based machine learning (ML) computing techniques to identify nefarious behaviors and indicators of cyber influence. SNICH operates on models and formalisms that describe the various correct interactions by which mission-critical functionalities are achieved and uses these formalisms to identify emergent problematic behaviors and their potential impact on missions. The SNICH machine learning models (ML) have been extensively refined and test results show a high anomaly detection accuracy.



SNICH employs three methods in parallel to detect nefarious cyber influence: 1) Machine learning (ML) algorithms which identify individual frames of anomalous sensor network traffic 2) Rule-based analytics which ensure sensor traffic conforms to interface specifications and 3) Statistical algorithms which detect anomalies in a sequence of frames. The innovative combination of these three approaches ensures both simple and sophisticated cyber-attacks can be detected.

SNICH is being developed under the Joint Collaborative Augmentation for Sense Making Environment (JCAUSE) AFRL/RI sponsored SBIR/STTR program, contract number FA8750-19-C-0099.