Information Analytics

Homeland Security
Science and Technology

CHALLENGE: FILLING THE CYBER-PHYSICAL RISK/THREAT ANALYSIS GAP

Currently, there is no centralized source and capability for the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) operational units — the Integrated Operations Division and the National Risk Management Center — to query and correlate information related to cyber risk analysis, physical and infrastructure risk, and blended cyber-physical risk/threat. To close these operational gaps, the DHS Science and Technology Directorate's (S&T) Information Analytics Program seeks to enhance the ability of operational units to correlate threat intelligence and risk data. This includes analysis of risk elements, increasing automated tools, and providing situational awareness in risk factors.

SOLUTION: ADVANCED DATA ANALYTICS AND MACHINE LEARNING TECHNOLOGIES FOR CISA

This Program supports the improvement of computational analytics and information sharing to improve homeland security cyber-physical security risk analysis across government, the 16 Critical Infrastructure Sectors, and the 55 National Critical Functions. The work is driven by a vision for next generation CISA architectures, computation, and decision-making capabilities, and establishes the foundation for future artificial intelligence (AI) solutions. Activities will focus on maturing CISA data analytics efforts through the development of representative data sets, stand up of joint computational sandbox testing capabilities, assessment of emerging analytics tools, experimentation with a variety of analytics use cases, and establishment of strategic research capabilities for the development of secure multi-party computational capabilities. This will be accomplished through the following projects:

Cyber Analytics and Platform Capabilities (CAPC) – Tools to discover cyber threats and increase intelligence,

Artificial Intelligence and Machine Learning Pipeline (CyLab) – Develop a secure environment for strategic and critical cybersecurity problem solving.

Development of Joint Analytical Collaborative Environment (JACE) – Collaborate to advance governance of a common information architecture, tools, and techniques for improved effective information sharing.

PROJECTS' IMPACT

The projects will provide improved operational utilization of large and complex data, along with modern data analytics' techniques and enhanced tools and procedures. Enhanced risk anlysis, consequence analysis, and threat intelligence data capabilities will improve incident responses times and threat and mitigation correlation across federal, state, and local governments and the private sector.

UPCOMING MILESTONES

- Complete initial build for multi-cloud environment for next generation CISA architecture.
- Expand the advanced machine learning CISA environment to support additional infrastructure security use cases.
- Deliver capability advances to CISA that combat sophisticated, covert, and targeted malware developed by advanced threat adversaries.

PARTNERS AND PERFORMERS

- S&T's Data Analytics Technology Center, Washington D.C.
- Sandia National Laboratories, Albuquerque, NM
- CISA's Cybersecurity Division and National Risk Management Center, Washington, D.C.