CAP-M: CISA Advanced Analytics Platform for Machine Learning

Science and Technology

ADDRESSING THE THREAT ENVIRONMENT

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from evolving threats and nefarious actors. Sophisticated state and non-state cyber actors exploit vulnerabilities to steal information and threaten the safety and well-being of the American public. These actors are constantly changing their tools, techniques, and procedures to wreak havoc. The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and Cybersecurity and Infrastructure Security Agency (CISA) are partnering to counter these evolving threats, to defend against cyberattacks, and to foster more secure and resilient infrastructure for the future.

APPROACH: RESEARCH PLAN

The S&T-led project, the CISA Advanced Analytics Platform for Machine Learning (CAP-M) (formerly known as CyLab), is chartered to develop a next-generation analytics ecosystem for strategic and critical cybersecurity problem-solving that incorporates on-premises and virtual computing environments. CAP-M is a secure, multi-cloud collaborative research environment that will enable CISA users to apply advanced analytic techniques across a variety of cyber data sources. CAP-M's capabilities will make previously out of reach use cases and experiments possible. It will host experimentation in analyzing, correlating, and enriching data to prepare for and respond to threats. Lessons learned will be shared with partners in government, academia, and industry.

S&T's research plan, which takes into account privacy concerns, consists of:

1) **Ecosystem.** Prototyping a multi-cloud "sandbox" environment that will be the next-generation training environment for CISA end-users, with advanced capabilities for enabling active experimentation.
2) **Tools and Tradecraft.** Researching advanced data analytic methods and tools, particularly artificial intelligence/machine learning (AI/ML) capabilities.
3) **Automating the Machine Learning Loop.** CAP-M will build and automate the ML solution loop and then automate the workflows (e.g., exporting, tuning data) through the loop.

FUTURE: BEYOND CYBERSECURITY

Fully realized, CAP-M will feature a multi-cloud environment and multiple data structures, a logical data warehouse to facilitate access across CISA data sets, and a production-like environment to enable realistic testing of vendor solutions. While initially supporting cyber missions, this environment will be flexible and extensible to support data sets, tools, and collaboration for other infrastructure security missions.

IMPACT: CONTINUOUS INNOVATION

The goal of this project is to enhance situational awareness and decision-making capabilities for cyber and infrastructure security missions.

Although threats and hazards continue to evolve, CAP-M will provide CISA with the capabilities to continually innovate to prepare for and respond to them.

ABOUT S&T AND CISA

S&T serves as the research and development arm of DHS. S&T does the science that strengthens the nation's overall security and develops and transitions the technologies that allow those on the front lines to effectively and safely complete their missions.

CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. For more information about CISA, visit www.cisa.gov.

Science and Technology CISA

Contact Us: Cyber-MB@hq.dhs.gov