Trusted CI Success Story
FABRIC

Trusted CI helps FABRIC build secure scientific infrastructure

The scientific community relies on high performance computing and networking to conduct experiments. FABRIC, a national-scale testbed funded by the NSF, is creating a new research infrastructure that enables scientists to experiment with novel ways to share the massive amounts of data generated by powerful new scientific instruments.

For example, FABRIC Across Borders (FAB) works with the high energy physics community that conducts experiments using the Large Hadron Collider (LHC) at CERN in Switzerland. Previously, scientists ran experiments, then sent the data elsewhere to do the analysis, requiring a larger and larger network pipe. By using FABRIC, LHC physicists are using machine learning and intelligent networking to process their data en route without having to increase the size of their internet connection to send larger amounts of data.

As FABRIC was being built in 2021, project leaders turned to Trusted CI, the NSF Cybersecurity Center of Excellence, to ensure they designed security into the project from the beginning. The collaborative cybersecurity engagement between Trusted CI and FABRIC included an inventory and threat assessment of system assets, development of a security monitoring architecture, and evaluation of software assurance practices.

As a national-scale research testbed with international connections through FAB and multiple connections to other research facilities, FABRIC faced the dual challenges of providing an open, well-connected environment that enabled research experimentation while maintaining a secure and reliable facility. The Trusted CI engagement, early in the FABRIC construction phase, helped to put the FABRIC project on a good trajectory to meet these challenges on the path to operations.

"The goal of FABRIC was to interconnect with the real internet, so we had to be very careful in regard to security," said Anita Nikolich, part of the leadership team at FABRIC and research scientist and director of Research and Technology Innovation at the University of Illinois Urbana Champaign.

Trusted CI identified more than 70 assets in the FABRIC system and documented threats, impacts, and controls for each asset. With a set of 20 concrete recommendations and a plan for next steps, the FABRIC project was well positioned to build and operate a secure facility.

"Trusted CI helped us redesign our architecture and helped us build security into our budget for the operations phase which began in 2023," said Nikolich. "To carry out the recommendations, we divided the findings into critical, optional, and nice to have, and put them into our project plan."

FABRIC continues its involvement with Trusted CI as a member of the Research Infrastructure Security Community (RISC) (formerly Framework Community of Practice). The cohort offers an opportunity to share challenges and solutions with others in the same research space.

"Our initial engagement with Trusted CI offered invaluable direction and guidance, especially in regard to security for FABRIC," said Nikolich. "And as a member of the RISC cohort, we can ask for advice from our peers on many topics, such as, 'Do you have a template for this situation, or what's the best way to talk with leadership about the budget?'"