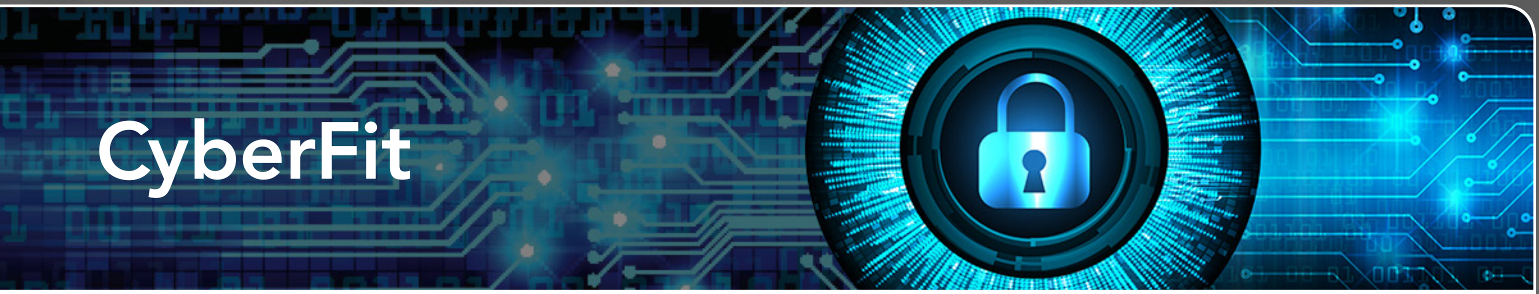
ASYMMETRIC RESILIENT CYBERSECURITY

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*



CyberFit

CHALLENGE

While there has long been a positive attitude between cyber operations, researchers, and software engineers, the culture gap and lack of interaction between these groups has been problematic. Researchers are often unfamiliar with real world cyber defense practices and their research is typically done on synthetic data that is not realistic. Furthermore, they do not have the time or expertise to engineer their ideas into production ready solutions. All three groups strive to put the best and brightest to work, but there is a need to merge these cultures to inspire innovation, drive requirements, and produce tested solutions, all within a cohesive, productive environment.

CyberFit lays the groundwork for cyber operations, cyber research, and cyber engineering to team up and create a culture of Cyber Fitness, enabling us to better stand up against our adversaries

CURRENT PRACTICE

Researchers are embedded in cyber operations teams for a period of time to let them learn the way of cyber analysis and defense. Capture The Flag (CTF) events expose many people to cyber defense practices. These approaches are valuable, but are not ongoing efforts that actually blend the cultures into an effective environment for growing cyber operations, research, and engineering efforts in a cohesive way. Research efforts typically start out as exploratory prototypes, show significant promise, and are thrust untested into production environments. This either increases risk due to lack of engineering or causes undeserving criticism of the research. This is problematic in both cases.

U.S. DEPARTMENT OF
ENERGY

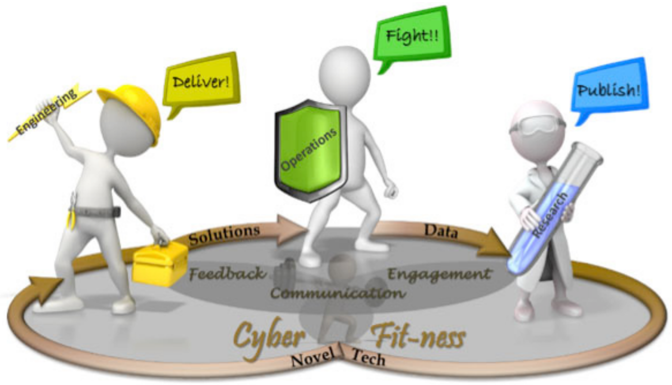
APPROACH

The CyberFit approach to removing this culture gap is to lay a foundation of teamwork and technology. CyberFit Trench Talks provide the communication, feedback, and engagement foundation for teamwork, while the CyberFit Data Warehouse is the technology that delivers data, novel technology, and solutions to problems.

Trench Talks bring cyber operations, cyber researchers, and software engineers together using one of three formats:

1. ***Briefing*** – a cyber operations person describes daily activities to provide insight into daily defense life
2. ***Challenge*** – a cyber operations person explains the hard problems too big for current time and resources
3. ***Checkpoint*** – a cyber researcher pitches progress to operations people for feedback

The Data Warehouse provides de-identified realworld data to cyber researchers, enabling novel technology to be engineered and deployed as realworld solutions for cyber operations. Combining forces with Pacific Northwest National Laboratory's (PNNL) Unclassified Cyber Security team (UCS – our network defenders), CyberFit works in conjunction with PNNL's Data Stewardship Board to establish usage policies, Memoranda of Understanding, and procedures for managing cyber data. The Board approves de-identification methods and storage practices for both static data sets and streaming data from UCS. The CyberFit StudyMaker captures interesting data as a basis for ground truth determination.



Together, the Data Warehouse and the Trench Talks provide the teamwork and technology foundation for a blended culture of CyberFit-ness.

IMPACT

Here at PNNL, we are blessed with an abundance of cyber researchers, software engineers, and an enterprise cyber defense operations team (UCS) critical to our survival as a national labratory. By creating the culture of CyberFit-ness, all of these groups will benefit from each other, and from the environment they create. With CyberFit-ness, the real world drives cyber research, and the cyber research directly serves the enterprise. The mutual ownership benefits the entire cyber community, which in turn benefits all of PNNL as we become more secure. The benefit does not stop with PNNL. We are not the only organization with researchers, engineers, and operations teams. PNNL's success can be spread through communication and exchange with other organizations, benefiting all involved in cyber defense, and thus all who benefit from better cybersecurity.

Contact

Chance Younkin
Principal Investigator
(509) 375-5957
chance.younkin@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*