Consequence-driven
Cyber-informed
Engineering

PARTNER TRAINING

Partner Training is designed to provide an in-depth,team-based training for select individuals who will participate in the execution of a Tier 1 engagement. It includes 16 hours of training on the CCE methodology, plus a detailed student guide and templates particpants can reference throughout the engagement.

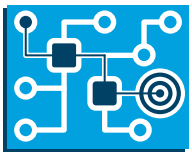
WHAT IS CCE?

CCE is a methodology developed by Idaho National Laboratory (INL) that aims to reduce the impact of an advanced, targeted cyber sabotage campaign on an organization's most critical operations.

Assuming an aggressor mindset, CCE examines how an adversary might target the most critical operations, focusing on entire systems and processes, not individual technologies.

Even strong cyber hygiene may not withstand a targeted attack campaign intent on catastrophic damage. Rather than focusing on perimeter defenses that reduce attacker access, CCE results in engineering changes and process improvements that limit the damage an attacker can do once inside.

CCE is a structured process to determine High Consequence Events—catastrophic disruptions to critical functions.



Map how an adversary could achieve them using cyber means

Identify engineering solutions or tripwires that would eliminate or significantly block those events

This focuses limited resources on high-impact investments.

WHAT DOES PARTNER TRAINING OFFER?

This 16-hour training (either in-person or a virtual format) offers participants the following:

- **A fundamental overview of CCE concepts,** shifting how participants approach risk decisions
- **A structured set of process steps to implement the methodology**, including checklists and templates to facilitate a self-guided CCE evaluation, plus a detailed **student guide**
- **A combination of trainer instruction and group exercises** that use realistic case studies to practice implementing each phase of the CCE process

In-person format

2 days/ 8 hrs. per day

Virtual format

16 hours (~4 hours/day) training with a series of prerequisite online modules

WHO SHOULD ATTEND?

A CCE effort requires a diverse mix of expertise that crosses business and functional units. The following key personnel are encouraged to attend:

- Asset and system operators
- Control systems engineers
- Process experts
- Functional and operational managers
- Cybersecurity analysts (both IT and OT)
- Risk management analysts
- Emergency management system (EMS) support

Companies that train multiple staff will be better equipped to conduct a coordinated CCE effort.

PREREQUISITES:

Training is focused on preventing the sabotage of critical infrastructure functions. Participants should have applied experience in or responsibility for the following areas:

- Engineering
- Operations
- Industrial control systems
- Cybersecurity

Idaho National Laboratory INL