IDAHO NATIONAL LABORATORY INNOVATION SHEET

Cyber Strike Workshop

Translating Real-world cybersecurity events to protect US utilities

The Cybercore Integration Center at Idaho National Laboratory (INL) is focused on the protection of the grid and energy infrastructure from cyberattack. This is one of the nation's most difficult technical and operational challenges, and requires capabilities of the national laboratories in partnership with government and industry.

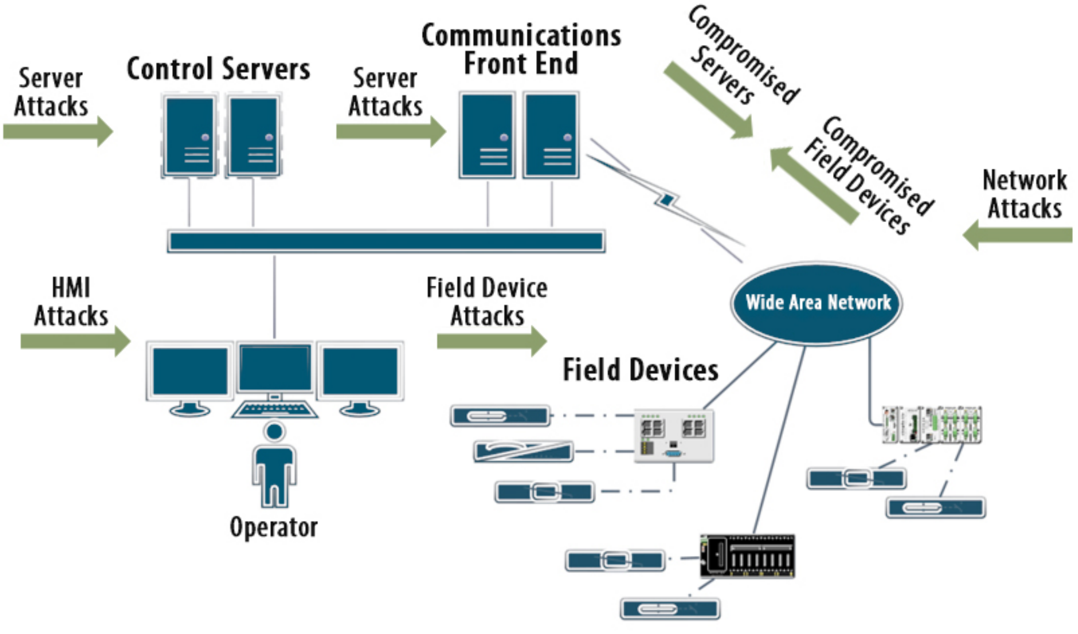
The cyberattacks on the Ukraine power grid demonstrated how quickly cybersecurity attacks can move and impact a wide variety of interdependent systems across a region. In the U.S., high-profile events like Nuclear 17 and Palmetto Fusion illustrate why utilities and regulators are concerned with increasing burdens due to more sophisticated and frequent cyber events. It is crucial for industry to have advanced capabilities and cyber skills to not only detect, but also respond to these events before there is an unacceptable impact.

The Cyber Strike workshop is an example of Cybercore Integration Center actively enabling research and development of cybersecurity solutions to:

- Understand and manage the multifaceted interdependencies between the grid and other critical infrastructure
- Detect and respond within compressed timelines to prevent highly impactful consequences
- Develop top-tier defenders to mitigate sophisticated threat actors

The U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE-OE), in collaboration with the Electricity Information Sharing and Analysis Center and INL, continues to host Cyber Strike workshops for electricity subsector owners and operators in the U.S. to enhance their preparedness against a cyber incident impacting industrial control systems.

In response to a DOE-OE request for INL to provide critical knowledge transfer to utility operators related to the Ukraine power grid cyberattack, INL researchers designed, developed, and prototyped unique hands-on training devices. These Cyber Strike instruction platforms are designed to challenge course participants to defend against cyberattack on the equipment



https://ics.sans.org/blog/2016/12/21/pictures-and-theories-may-help-but-data-will-set-us-free

UNCLASSIFIED

U.S. DEPARTMENT OF ENERGY Infrastructure Security & Energy Restoration

Idaho National Laboratory

they routinely encounter within their power generation systems and power distribution substations. INL is exploring opportunities to make these training systems readily available for university engineering laboratories and industrial control room simulators.

The training offers attendees a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine. Workshop attendees are guided through a series of exercises/labs in groups of five or six operators. Other topics referenced include the North American Electric Reliability Corporation (NERC) alert related to the 2015 Ukraine cyber incident and the applicability of NERC Critical Infrastructure Protection (CIP) reliability standards for such an incident. However, the primary focus is not standards, but rather understanding the Ukraine cyber incident from a technical perspective to enhance cyber preparedness.

INL experts seek novel approaches to improve the effectiveness of knowledge transfer and information sharing by developing singular immersive learning environment methods and tools. Within our program portfolios for DOE, Department of Homeland Security (DHS), and other federal organizations, INL experts are in high demand nationally and internationally to provide education and training to elevate cyber skills and provide cyber awareness through sharing real-world knowledge and experiences. Examples are focused on demonstrating the progress in advancing the Cybercore Integration Center's objective for developing highly skilled, multidisciplinary cyber defenders and researchers.

The development of strategic partnerships, innovative technology, and next-generation workforce are priorities within INL's strategic initiative, the Cybercore Integration Center. This initiative seeks to create and align national science and engineering resources, technical expertise, and collaborative partnerships to focus on scalable and sustainable control system cybersecurity solutions – solutions that protect the U.S. grid, other critical infrastructure, and military systems.

Target Audience

The Cyber Strike workshop is tailored to U.S. utility operations staff in the following areas:

- Control room operational technology personnel
- Critical infrastructure protection-focused technical staff
- Energy Management System (EMS) support
- Operating personnel
- Cybersecurity staff

For more information

Daniel Noyes
208-526- 0516
Daniel.noyes@inl.gov

Misty Benjamin
208-526- 5940
misty.benjamin@inl.gov

www.inl.gov

A U.S. Department of Energy
National Laboratory