FORGE

FREE Community Membership for Electric Utilities

Cyber Awareness • ICS SOC Training • Threat Intelligence Briefing • Workforce Planning
Threat Intelligence Sharing • Annual Exercise Discussion • Keynotes

TRAINING
APR 9-11, 2024

EXERCISE
APR 25, 2024

The Emerging Threat Center (ETC), powered by Forge Institute, invites you to join our FREE community membership. The ETC is a cross-sector fusion center dedicated to uniting private and public sectors to identify threats against critical infrastructure and develop comprehensive risk-mitigation strategies. Our approach integrates bi-directional information sharing, joint analytical efforts, strategic insights, and more, fostering an environment of effective collective defense.

Information Sharing | Analytic Collaborations | Strategic Briefings

By joining, you'll gain access to the Emerging Threat Information Sharing & Analysis Center (ET-ISAC or Community Membership). The ET-ISAC extends the ETC and provides additional threat intelligence, awareness training, and collaborative opportunities, specifically designed to bolster the security posture of electric sector entities against both cyber and physical threats.

Why join the ETC as a Free Community Member

- **Collective Defense Strategy:** Leverages insights from a network of utilities, cybersecurity experts, and regulatory bodies to bolster sector-wide resilience.
- **Fulfillment of RUS Program Requirements:** Supports adherence to Rural Utilities Service funding conditions by promoting sector-wide cybersecurity awareness and preparedness.
- **Regulatory Body Collaboration:** Encourages alignment with regulatory expectations from entities like FERC and the Department of Energy, ensuring utilities are well-prepared against evolving cyber threats.
- **Better Secure your Critical Infrastructure:** Help enhance your cybersecurity posture through community-shared insights.

Register Now:

forge.institute/etc

ETC Community Level Membership (ET-ISAC)
Services are free through the end of the Grant period.

Email **etc@forge.institute** or call **501-500-0812 ext. 816** with questions.

 The Forge Institute is funded, in part, through a Cooperative Agreement with the U.S. Department of Energy. All opinions, and/or recommendations expressed herein are those of the author(s) and do not necessarily reflect the views of the DOE.

COLLABORATION PARTNERS

UA Little Rock | University of Arkansas | Arkansas Municipal League | Electric Cooperatives of Arkansas | National Energy Technology Laboratory | INL Idaho National Laboratory | Pacific Northwest National Laboratory

ET-ISAC Development Opportunities

The ET-ISAC project fosters collective cybersecurity defense by uniting electric utilities and energy entities in the mid-South U.S. It harnesses student research, real-time threat platforms, and innovative technologies like distributed ledgers to enhance threat sharing. This collaboration strengthens both individual entities and the entire region against cyber threats, underscoring the vital importance of shared intelligence and a collective defense.

Key Learning Objectives

- Gain an understanding of the fundamentals of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA), including their significance, basic components, and architecture.
- Gain introductory knowledge of Cyber Threat Intelligence (CTI) and its critical role in enhancing the security of ICS/SCADA systems.
- Understand common cybersecurity failure scenarios for ICS and SCADA systems in the electric sector and the consequences of failure.
- Learn about basic cybersecurity principles for ICS/SCADA, including common threats, vulnerabilities, and the importance of securing these systems.
- Acquire basic skills in using tools and techniques for cyber threat detection and analysis, including simple reconnaissance methods and network traffic analysis.
- Learn to understand commonly used cybersecurity controls to protect, detect, respond, and recover from a cyberattack.

Why Register for Training and Exercise Workshops

- **Meets Regulatory Training Requirements:** Helps utilities comply with regulatory mandates from NERC and FERC by providing comprehensive cybersecurity training.
- **Supports RUS Compliance:** Ensures utilities meet Rural Utilities Service funding requirements related to workforce development and cybersecurity competencies.
- **Enhanced Regulatory Compliance and Readiness:** Prepares utilities to exceed cybersecurity benchmarks set by authoritative bodies, fostering a proactive security culture.
- **Sector-Specific Skill Development:** Focuses on the unique cybersecurity challenges faced by the energy sector, aligning with the strategic priorities of regulatory authorities to safeguard critical infrastructure.

Key Dates

April 9-11th - 3 Day Awareness & Threat Hunting Training

April 25th - 1 Day Regional Cyber Simulated Attack Exercise

Learn more & register:
www.forge.institute/etc

INSTRUCTORS

Dr. Philip Huff is an Assistant Professor of Computer Science at the University of Arkansas in Little Rock, where he directs Cybersecurity Research at the Emerging Analytics Center. A pioneer in the field, he co-founded Bastazo, a company at the forefront of Cybersecurity AI, contributing his significant expertise to advance industry innovation. Dr. Huff spearheads the National Cyber Teaching Academy and the Department of Energy's Emerging Threat Information Sharing and Analysis Center (ET-ISAC), offering innovative strategies for developing the cybersecurity workforce. Additionally, he holds a CISSP certification, underscoring his expertise in the field.

Becky Passmore holds the position of Senior Vice President in Kroll's Cyber Risk practice and is also an Assistant Professor at the University of Arkansas at Little Rock Cybersecurity Department. She worked as a Senior Digital Forensic Examiner at the FBI until joining Kroll in November 2020. Becky has conducted complex digital investigations involving technical analysis for various issues including national security, insider threats, internet fraud, child exploitation, terrorism, and public corruption. Ms. Passmore has a Bachelor of Science in Information Technology and a Master of Science in Digital Forensics and Cyber Investigation. Ms. Passmore possesses multiple industry certifications.

Dr. Chris Farnell serves as an Assistant Professor in the Electrical Engineering and Computer Science (EECS) Department at the University of Arkansas. He earned his Ph.D. in Electrical Engineering from the same university in 2020 and is distinguished as an IEEE Senior Member. Chris's research spans Cybersecurity for Critical Infrastructure, Embedded System Design, FPGA Design, Advanced Control Algorithms, and Power Electronics. He holds the position of Associate Director at the National Center for Reliable Electric Power Transmission (NCREPT), a 12,000 ft² laboratory at the University of Arkansas that specializes in testing and evaluating power electronic systems. Beyond his research, Chris chairs the IEEE Ozark Section, serves as the treasurer for the IEEE Computer Society Chapter, mentors the CyberHogs Registered Student Organization (RSO), and is actively involved in K-12 outreach programs.

Dugan Stem, the Interim Managing Director of Forge Institute's Emerging Threat Center, brings his experience as a former Army Intelligence Analyst to the Forge team. Before joining Forge Institute through its Fellowship program, Dugan has played a pivotal role as a manager and senior threat intelligence analyst. His work focuses on mentoring transitioning service members and developing strategies to counter emerging threats to Arkansans and the surrounding region.