Cyber & Physical Security Focused Meetings

Security Meetings are held quarterly between the Cyber Monitor team and participating utilities to provide opportunities to discuss concerns, emerging threats, and trends facing Texas electric utilities. These meetings also include industry specific security briefings, peer sharing and training sessions, designed to inform and educate.

PURPOSE

Quarterly Security Meetings provide a secure environment for utilities to share information regarding threats and best practices.

PARTICIPANTS

Participants include a variety of technical and non-technical analysts and decision makers, e.g., CISOs, Cybersecurity Analysts, City Managers, General Managers.

TIME & PLACE

Security Meetings are held quarterly in March, June, September, and December. They are virtual meetings and participants are pre-screened prior to entry.

KEYNOTE SPEAKERS

Security Meetings are forums for expert speakers to communicate and explore valuable information and resources. Past speakers include:

- Amazon Web Services
  - BCSI Segmentation and Control Implementation
- ChaosTrack
  - AI-Based Incident Response Training & Tabletop Exercises

Cyber & Physical Security Focused Meetings

TOPICS COVERED:

2021

- Impact of IT breaches on OT Operations – Colonial Pipeline Ransomware Hack
- Presidential EO 14028 on Improving the Nation's Cybersecurity
- 2021 Massive Data Breach – The T-Mobile Hack
- Proliferation of Ransomware

2022

- Introduction to Counter Unmanned Aerial Systems (Leach Strategic Partners)
- The State of Utility Cybersecurity in Texas (Elizabeth Rogers, Michael Best LLP)
- Key Risk Mitigation Steps to Take for Breach Prevention
- 8 Key Questions to be Immediate Addressed When Faced with a Cyber Incident
- Top Ten Steps to Building a Cyber Incident Response Plan and Procedures

2023

- Managed Detection and Response (Texas A&M Security Operations Center)
- Emerging Social Media, Opportunities for Threat Intelligence (LifeRaft)
- Leveraging DIR Resources (Texas Department of Information Resources)
- Cyber Threat Intelligence (Joe Slowick, Paralus)
- Social Engineering Awareness (TNMP)
- Creating and Negotiating Service Level Agreements (Elizabeth Rogers, Michael Best LLP)
- CyberStrike Lights Out Training
- Artificial Intelligence - Usage, Risks, and Safeguards (Oncor)
- Cybersecurity Insurance – Best Practices (Elizabeth Rogers, Michael Best LLP)
- Workforce Development – Best Practices in the Muni Space (Bryan Texas Utilities)

2024

- GridEx In A Box: Exercise Deployment with Manageable Resources (E-ISAC)
- Procurement Best Practices & Navigating Cooperative Purchasing Challenges (Signature Advisory Partners)
- BCSI Cloud – Best Practices (Austin Energy)
- Global Security Risks in Cyber and Physical Security (SCIS)
- Navigating ERCOT Market Ruling NPRR 1199
- Artificial Intelligence: Opportunities & Threat (Austin Energy)

2025

- BCSI Segmentation and Control Implementation (Amazon Web Services)
- AI-Based Incident Response Training & Tabletop Exercises (ChaosTrack)
- Global Security Risks in Cyber and Physical Security (SCIS)
- Overview of the State Energy Security Plan (PUCT)
- Texas RSOCs: Available Resources, Ready to Serve
- Industry-Academia Collaboration (UT Austin, Texas A&M, Texas State)
- Alamo Regional Security Operations Center Overview (ARSOC)
- National Science Foundation FutureCoRe Program (Texas State University)
- Vulnerability of Integrated Security Analysis (E-ISAC)