Intelligence-Driven Industrial Network Defense

Paralus LLC

paralus.co

Course Overview

Industrial network security is an increasingly popular (and important) topic, but precisely how to achieve this goal remains murky. This course teaches an intelligence-driven, threat-based approach to evaluating the threat landscape and developing countermeasures and defenses. As malicious entities increasingly target Operational Technology (OT) and Industrial Control System (ICS) networks, defenders - whether industrial operators new to security, or IT security personnel learning ICS - need to learn the basis and nature for these attacks.

This course begins with an overview of ICS networks and the OT landscape to ensure a common background in operational limitations and capabilities. With this in place, we then explore risk assessment, risk understanding, and threat modeling. Finally, we conclude with an overview of threat types, motivations, and capabilities as applied to ICS-specific values and defensive questions.

The online version of this course takes place over two, four hour sessions held over two days. Lessons and instruction divide between lecture, discussion, and group exploration of security incidents. Attendees will receive a certificate of completion following the course to record for training and CPE purposes.

Course Syllabus

- Defining Industrial Control Systems (ICS).
    - What does “ICS” mean?
    - IT-OT “Convergence” and its significance for ICS network operations.
    - Purdue Reference Architecture and dividing up the network.
        - The “IT Zone”.
        - IT-ICS Boundary Defense.
        - Physical Process Layer.
    - ICS Security Priorities
        - The fallacy of availability above all.
        - Integrity, security, and safety.
- Understanding intelligence and threat intelligence.
    - Intelligence as a process: refinement, and a cycle.
    - Theories of Threat Intelligence:
        - Cyber Kill Chain & ICS Cyber Kill Chain.
        - Diamond Model of Intrusion Analysis.
        - MITRE ATT&CK and ICS ATT&CK
    - Theory to practice in Threat Intelligence.
        - Enabling daily operations.
        - Assisting immediate defense.
        - Facilitating operational recovery.
    - Evaluating Threat Intelligence.
        - Values and trade-offs.
        - The importance of time and satisfying defensive needs.
        - ICS-specific trade-off considerations.
- Threat Modeling.
    - Combination of Self-Understanding and Adversary Knowledge builds risk perspective.
        - Understanding own environment:
            - Industry and vertical.
            - Geography and exposure.
            - Assets, technology, and attack surface.
        - Where are the threats?
        - Attribution and network defense.
        - Reviewing vulnerabilities and threat assessment.
    - Attack surface as a product of threats and opportunity.
- The ICS Threat Environment.
    - Threat as a composition of capability, intent, and vector.
        - Capabilities and tools.
        - Adversary intent and purpose.
        - Vectors and delivery opportunities.
    - Understanding Attacker Dependencies.
    - Adversary Objectives.
        - Deny/Degrade/Destroy/Disrupt = Attack.
        - Distinguishing “Attacks” from “Not Attacks”
        - Attacks compared to Attack Preparation.

- Mapping Adversary Operations to Impacts.
    - Availability impacts.
        - Indiscriminate or untargeted disruption.
        - Targeted disruption operations.
        - Monetization with disruptive consequences.
    - Integrity impacts.
        - Protection attacks in the Electric Sector.
        - Safety attacks in the Oil & Gas Sector.
        - Integrity attacks in Manufacturing.
    - Confidentiality impacts.
        - “Stealing the recipe.”
        - Possibilities of adversary mishaps and physical disruption.
- Risk evaluation and defensive planning.
    - Risk as a combination of attack surface, attacker capability, and attacker motivation.
    - Actualization of risk.
    - Identifying value centers for defensive planning.
    - Mapping value centers to impact scenarios.
- Implementing countermeasures and defense.
    - Moving from a “wall” to a “network” approach.
    - IT Controls & Defenses.
    - ICS Security Measures & Monitoring.
    - What to do when controls and defense fail.
        - Resilience and recovery planning.
        - ICS-specific incident response.
        - Engineering and control system failsafes.

Course Author & Instructor

Joe Slowik has emphasized the operational significance of threat intelligence through multiple roles: through leading intelligence and detection teams at Gigamon and Huntress; as an industrial control system (ICS) focused analyst for Dragos; leading the incident response team at Los Alamos National Laboratory; and serving as a Cryptologic Warfare Officer in the U.S. Navy. Ultimately Joe seeks to focus cyber threat intelligence as providing actionable, relevant guidance to day-to-day security operations to ensure robust, adaptable defense.

In addition to his work at Dragos and at Paralus, Joe also writes extensively on his website, Pylos. Joe is a frequent speaker and author of multiple papers covering threat intelligence and ICS concepts.