Industrial Cyber Threat Intelligence Theory and Practice

Paralus LLC

paralus.co

Course Overview

The field of cyber threat intelligence (CTI) is increasingly popular in both presentations and vendor offerings, but rarely includes an industrial-specific focus of interest to industrial control system (ICS) functions and operational technology (OT) environments. Yet digital convergence, rapid adoption of distributed or cloud capabilities, and increased adversary interest in ICS environments combine to make ICS-specific CTI a relevant topic for industrial asset owners, operators, and defenders.

This course provides a roadmap to educate asset owners and operators, or traditional information technology (IT) personnel, in the specific requirements and concerns of ICS-related CTI. While traditional IT concepts are addressed, overall this training seeks to build an ICS-specific understanding of threat intelligence to enable stakeholders to better understand their operational environments, the current threat landscape, and how the interaction between these two views influences operational security and resiliency.

Course Syllabus

- Understanding Intelligence and “Threat Intelligence”
    - Defining Intelligence
        - Intelligence Process
        - Overview of the Intelligence Cycle
    - Differentiating Threat Intelligence from General Intelligence Production
        - Incorporating Adversaries and Risk
        - Considerations of Timeliness, Accuracy, and Actionability
- Industrial-Focused Threat Intelligence
    - CTI in General Focuses on IT-Specific Observations
        - Network Indicators - IP Addresses, Domains
        - Host Indicators - File Hashes, Host Observables
    - Industrial Operations Require Industrial-Specific Observations
        - Process-Centric Understanding
            - Example: Stuxnet
            - Example: Ukraine Events
        - How Cyber Capabilities may Interact with or Alter Processes
        - Understanding Operational Integrity and Adversary Operations
- Orienting Intelligence to the Enterprise
    - Understanding Organizational Values and Mission
    - Identifying Critical Processes and Critical Path Nodes

            - Example: Norsk Hydro
            - Example: Abqaiq Attacks
        - Mission- and Process-Focused Understanding and Intelligence
- IT Observables and Industrial Defense
    - Overview of the Cyber Kill Chain
    - Overview of MITRE ATT&CK and ICS ATT&CK
    - Understanding the Lifecycle of an ICS Attack
        - Access and Control are Critical:
            - Adversaries Maintain Interactive Control over Capabilities (Ukraine, Saudi)
            - Adversaries Can Pre-Program Effects for Autonomous Action (Stuxnet)
        - Effects and Implications
            - IT-Focused Wipe or Lock can Have Significant Effects, but not Process-Focused
                - Example: Shamoon
                - Example: Norsk Hydro
            - Process-Specific Attacks Enable Destructive Scenarios
                - Example: 2016 Ukraine
                - Example: 2017 Saudi
        - When are Effects Desirable?
            - Orienting Industrial Attacks to Policy and Inter-State Relations
            - Understanding “Operational Preparation of the Environment”
                - Example: Energetic Bear
                - Example: Nitro Zeus
            - Distinguishing between Attack Enablement and Imminent Attack
    - How do IT-Specific Observables Help ICS-Centric Defense?
        - Understand Adversary Targeting and Motivations
            - Example: Dragonfly
            - Example: Palmetto Fusion
        - Insight into Adversary Behaviors
            - Example: 2016 Ukraine
            - Example: PoetRAT Campaign
    - Network Observables
        - Identify Communication Infrastructure
        - Identify Communication Methodology
    - Host Observables
        - Identify Initial Access Mechanisms
        - Identify Persistence Mechanisms
        - Identify Lateral Movement Techniques
    - The Value of IT Observables in Industrial Defense
        - Only Valuable as Far as You Can See
        - Identifying Attack Paths and Possible Intentions is Significant - but Hard!
- Industrial Intelligence and Visibility
    - ICS CTI is Only Valuable to the Extent Visibility Exists into the Industrial Network
    - Visibility Types:
        - Network Traffic and Observables
        - Host Behaviors and Artifacts
        - Process-Centric Visibility and Monitoring
            - Frequently Deployed in Industrial Environments

            - Rarely Used for Security Purposes
    - Understanding Possibilities and Limitations is Critical
        - Layer 3.5-2 Visibility May be Quite Easy!
        - Layer 1-0 Visibility Nearly Impossible - But Does This Matter?
        - Determining What Adversary Artifacts are Observable and Where Can Focus Detection and Analysis Efforts
        - Additionally, Knowing “What You Can See” allows You to Prioritize CTI Information
    - Supply Chain Considerations
        - Understanding what a Supply Chain Attack Means
        - Adversary Obstacles and Limitations
        - Actionable Information for Supply Chain Defense
    - Vulnerability Reporting and Significance
        - ICS Software is Frequently Vulnerable and Insecure - But to What Extent Does this Matter?
        - Understanding Scope, Implications, and Impacts of ICS-Related Software Vulnerabilities is Critical for Reporting to OT Personnel
        - Windows and Other IT Software/Hardware Vulnerabilities are Also Potentially Significant, and Cannot be Ignored
- Reporting, Communication, and Action
    - CTI is Only Valuable if You can Act on It
        - “Inactionable” CTI Exists
            - Example: Black Hat Talks
        - Goal: CTI that is Not Just “Informative”, but Discretely Actionable
    - How to Communicate with Defenders and Operators?
        - IT-OT Communication
            - IT Security Concerns Transmitted to OT Personnel
            - OT-Specific Worries Communicated to IT Security
        - Knowing Organizational Maturity and Capability
            - Reporting “Too Much” in Immature Environments can be Overwhelming
            - Knowing Organizational Capability and Ability to Use CTI is Vital in Designing Meaningful CTI
        - Adapting Information to Environments
            - ICS Environments are Highly Customized Cyber-Physical Systems
            - Understanding the Environment is Critical to Adapting CTI
                - Knowing Vulnerability Applicability and Significance
                - Understanding Process-Specific Implications of Cyber Activity
    - Communication and Reporting Types
        - Indicator Feeds: They Exist, They are Nearly Useless in OT
        - Narrative Reports: Helpful and Contextual, but Likely Too Great an Investment for OT Personnel
        - Threat Summary Reporting: Short (1-3 Pages), Concise Reporting Highlighting Specific Threat and Impact Scenarios to the Organization’s Operational Environment
    - Feedback and Intelligence Iteration
        - ICS-Specific CTI Requires Frequent Contact and Communication with Operational Personnel
            - Determine How Effective CTI Reporting is for OT Personnel
            - Identify Where CTI Work needs to Improve or Shift

- Facilitating Feedback and Communication is Necessary to Enable Good CTI
    - Regular Meetings or Threat Briefings can Build Familiarity and Awareness
    - Connections and Regular Communications Between Teams enables Real-Time Information Sharing and Feedback
    - Operational Rotations or “Ride Alongs” Can Facilitate Knowledge Transfer and Environment Awareness

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 DomainTools, 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.