# Intelligence-Driven Threat Hunting

Online Edition - Paralus LLC

*paralus.co*

---

## Course Overview

Designed as a follow-on to the Paralus Operational Threat Intelligence Course, organizations that have already incorporated cyber threat intelligence (CTI) into security operations can move from a reactive posture to an active hunt stance against attackers. With the foundations of CTI in place, organizations can work to train, engage, and empower security personnel to leverage knowledge and adversary operational profiles to build robust, intelligence-driven hunt programs.

This course addresses the following items:

- The fundamentals of threat hunting within security operations.
- Hypothesis development, testing, and evaluation as part of a knowledge and intelligence-driven hunting program.
- Differentiating between internal and external hunting operations, including production of internal threat intelligence for operational consumption.
- Reporting and recording fundamentals and the critical aspect of knowledge maintenance and longevity for sustainable hunting activity.
- Building threat hunt teams within the context of classical security operations center (SOC) and incident response (IR) roles.

Attendees will receive a certificate of completion following the course to record for training and CPE purposes.

# Course Syllabus

- Introducing Threat Hunting
    - Differentiating Reactive Security Operations from Active Threat Hunting
    - Requirements and Pre-requisites
    - Expectation Setting
- Intelligence-Driven Threat Identification and Analysis
    - Building Adversary Operational Profiles
    - Moving from IOCs to Behaviors
        - Differentiating Indicators, IOCs, and Behaviors
        - Identifying  the Characteristics of IOCs to Reveal Behaviors
    - Tradecraft Analysis and Behavioral Mapping
- Hypothesis Development, Testing, and Analysis
    - The Scientific Method of Threat Hunting
    - Key Threat Hunting Hypothesis Requirements:
        - Documented
        - Repeatable
        - Testable
    - Hypothesis Testing Methodology
        - Formulating Hypothesis
        - Developing a Test Plan
        - Recording Results
- Internal and External Hunting Activities
    - Differentiating Internal from External
        - Internal: Hunting in Your Network
        - External: Hunting in Data Sets, the Internet, etc.
    - Internal Hunting Methodologies
        - Know Thyself
            - Understand Information and Data Sources
            - Know the Fidelity of Logs and Other Records
            - What Are Your Visibility Gaps
        - Know Your Threats
            - Leveraging Intelligence, Understand the Threat Landscape
            - Mapping Adversary Development to Threat Landscape:
                - General Tradecraft Evolution
                - Specific Tradecraft and Impacts for Your Threat Model
            - Threat-Driven Gap Analysis
                - Based on Self-Knowledge, Relate Threat Landscape to Visibility Gaps
                - Identify Critical Gaps, Potential Mechanisms for Addressing Gaps
        - Know Your Resources
            - Who Are Your Hunters
            - Building Awareness and Capability through Teams
                - Knowing the Security Team
                - Incorporating IT Teams for Institutional Knowledge and Operational Awareness
    - External Hunting Methodologies

        - Moving Threat Intelligence from Passive Consumption to Active Searching
            - Defining “Active” Threat Intelligence
            - Sustainable Collection, Ingestion, and Action
        - Operational Profiles, Behaviors, and Pivoting
        - Pivoting Resources and Methodologies
        - Differentiating IOC Discovery from Tracking Behavioral Evolution
- Reporting, Documentation, and Institutionalizing Results
    - Hunting as an Iterative, Developmental Process
        - Results Not Recorded are Lost
        - Develop and Maintain a Mechanism to Capture Institutional Knowledge and Hunting Results
        - Standardization, Formats, and Repeatable Processes
    - Output of a Threat Hunt
        - Successful Hunts Should be Developed into New Alerts
        - Failed Hunts Should be Used as the Basis for Future Hypothesis Development
    - Implementing Strategies to Retain and Store Knowledge
        - Documentation Standards and Formatting
            - Capturing the Hypothesis
            - Documenting Testing and Evaluation
            - Recording Results
        - A Discussion on Metrics and Proving the Value of Threat Hunting
- Building and Maintaining Threat Hunting Teams
    - Likelihood of Expanding Head Count to Build a Dedicated Hunt Team is Small
    - Using Existing Resources to Build a Hunting Program
        - IR Analysts can become Full Time Hunters when not Responding to an Incident
        - SOC Analysts are Ideally placed to Enabled Hypothesis Evaluation and Testing
        - Visibility and Gap Analysis is Facilitated by Working with Existing IT and Infrastructure Teams
    - Making the Case for Hunting Investment
        - Metrics and Showing Value
        - Capturing Success and Wins

# 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.