Operational Threat Intelligence

Online Edition - Paralus LLC

paralus.co

Course Overview

When used properly, cyber threat intelligence allows an organization to leverage another's breach or incident to their own benefit. Yet while many cyber threat intelligence courses and guides exist, these are primarily designed for developing long-range, in-depth intelligence products for strategic or similar overview with an overemphasis on theory and little experience in practice. Operational threat intelligence instead supports a different audience: day to day security work and network defense. While cyber threat intelligence must always meet standards for accuracy, relevancy, and timeliness, SOC watch-standers and IR personnel need enriched information now in order to execute their jobs.

This course fills a critical role that other training does not address: how to successfully embed cyber threat intelligence operations into the daily rhythm of security to support everyday tasks, and extraordinary incidents. Toward that end, while this course will briefly touch on theoretical concepts such as analysis of competing hypotheses, kill chain methodology, and other ideas, the real focus will be on what efforts make operational threat intelligence possible and sustainable:

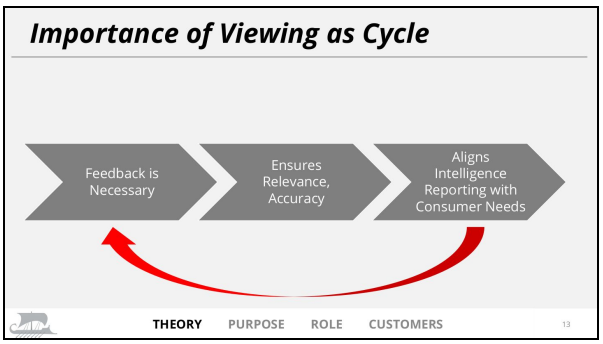
1. Establishing roles, responsibilities, and service agreements in advance.
2. Determining priorities, intelligence requirements, and customer threat landscape.
3. Molding threat intelligence information to security tools to make enriched information useful and actionable.
4. How to analyze internal and external data sources to extract actionable threat intelligence for operational defenders.
5. An extensive walk-through of IOC analysis, pivoting, and information enrichment to demonstrate how to better equip defenders to respond to emerging threats.
6. Discussions on reporting, feedback, and closing the intelligence loop to definitively show how threat intelligence operations link to SOC, IR, and security policy entities.

The course then concludes with the nature of pivoting, data and observable enrichment, and quick analysis reporting to close out instruction.

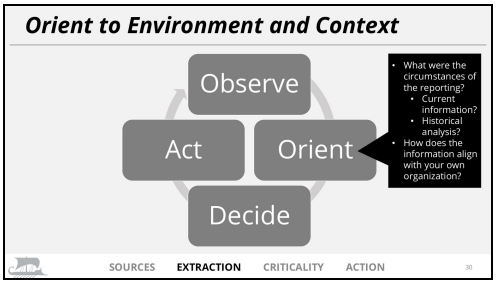
Attendees will receive a certificate of completion following the course to record for training and CPE purposes.

Course Syllabus

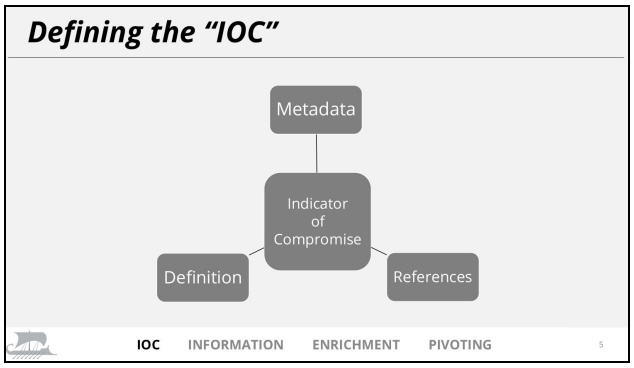
- Introduction and Overview of Threat Intelligence
  - Overview of Intelligence and the Intelligence Cycle
  - Differentiating Threat Intelligence from General Intelligence
  - Moving from Intelligence “Theory” to “Practice”
    - Overview of Kill Chain, Diamond Model, ACH
    - Putting Theory in Its Place
  - Threat Intelligence Value
    - Enable Operations
    - Assist Defense
    - Facilitate Recovery
  - Threat Intelligence Measures of Effectiveness
    - Actionability
    - Accuracy
    - Timeliness
    - Trade-Offs and Value Propositions for Operational Threat Intelligence
  - Organizational Value and Intelligence Needs
    - Differentiating “Strategic” from “Tactical”
    - Audience Identification and Audience Needs
    - Understanding and Orienting to Organizational Value
  - Threat Intelligence and Threat Hunting
    - Threat Intelligence is a Prerequisite for a Successful Hunting Program
    - Incorporating Threat Intelligence into Security Operations Enables Future Hunting Programs



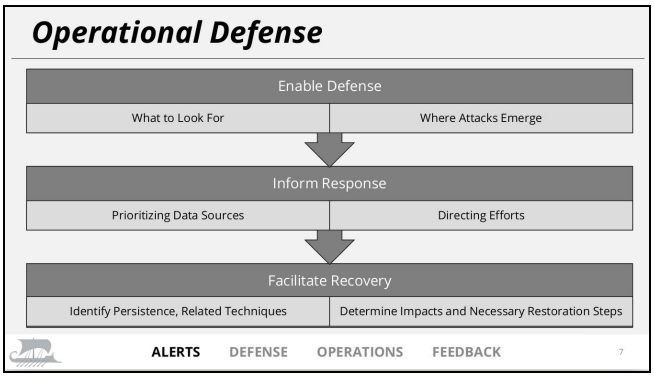
- Sources of Intelligence Information
  - External Sources of Intelligence
    - Paid Feeds, Blogs, Sharing Relationships
    - Benefits of External Reporting
    - Drawbacks of External Reporting
    - Differentiating “Good” from “Bad”
    - Special Case: Social Media
  - Internal Data Sources
    - Defining and Understanding
    - Realizing Capabilities and Limitations of Internal Sources
  - Intelligence Extraction from Sources
    - IOCs are Important - But Not the Focus of Extraction
    - OODA Loop for Critical Reading and Analysis
    - “Critical Information”
      - Relevant to the Organization
      - Related to Your Industry
      - Applicable to Your Technology
      - Actionable for Defensive Purposes
  - Orienting Information to Action



- IOCs & Enrichment
  - Defining the IOC
    - IOCs as Defined
    - IOCs as Implemented
    - Limitations of IOCs
  - IOCs, Information, and Behavioral Patterns
    - “Sustainable Intelligence”
    - Extracting Information from an IOC
  - Data Enrichment
    - Aligns with “Analysis and Production”
    - Key Concepts:
      - Context
      - Timing
      - Purpose

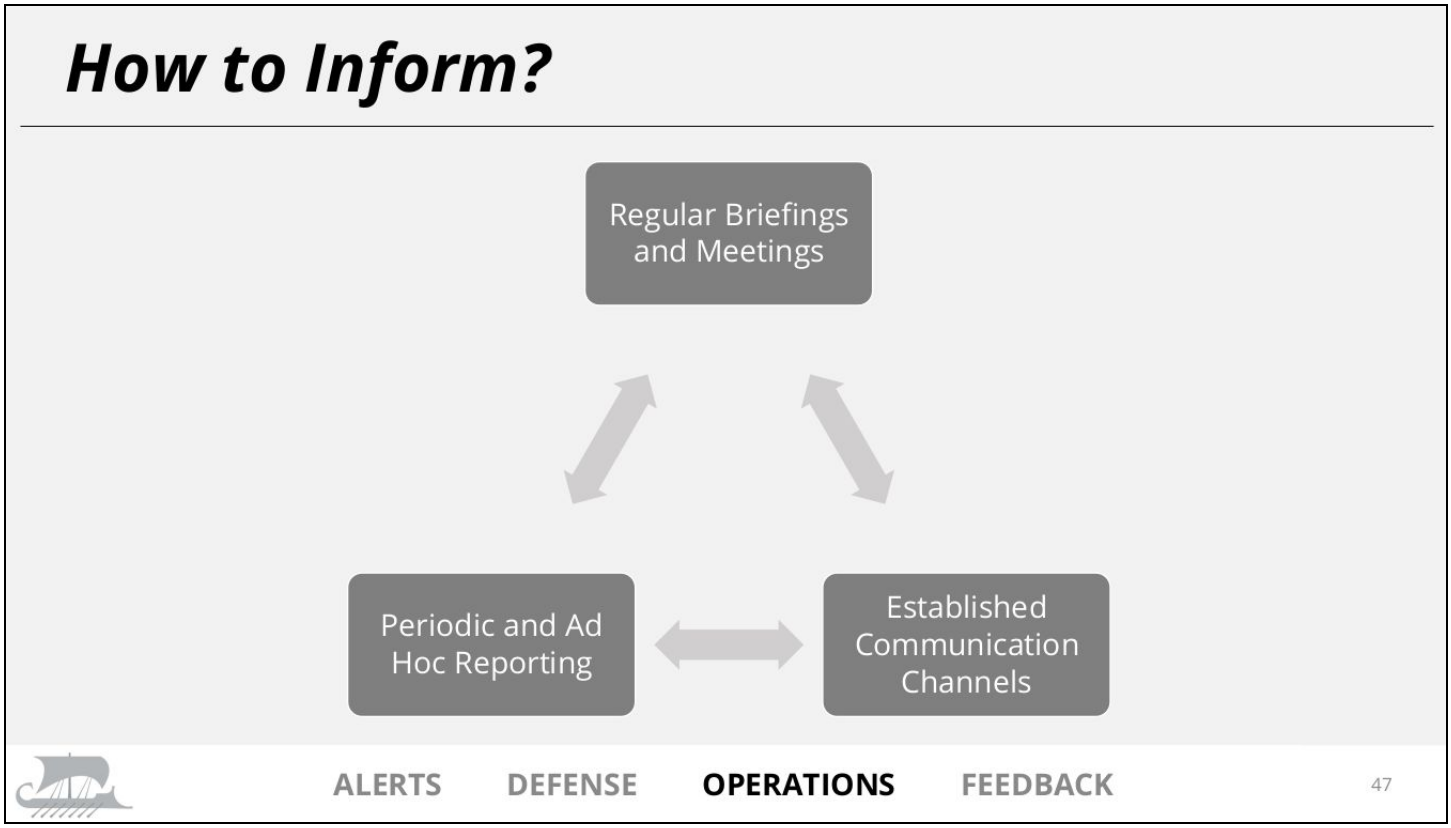


  - Enrichment Enables Pivoting
    - Pivoting is Not Simply Collecting More IOCs
    - Understanding Existing IOCs and Behaviors Yields Tendencies
    - Tendencies and Patterns allow for Identification of New Observables for Analysis
  - Adversary Operational Profiles
    - Fundamental Understanding of Adversary Tools, Actions, and Infrastructure
    - A Clear Understanding of an Adversary’s Operational Profile Enables Accurate Pivoting
- IOC Extraction, Data Sources, and Pivoting
  - IOC Composition and Data Extraction
    - Host-Based IOC Elements
    - Network-Based IOC Elements
  - Sources for Enrichment and Refinement
    - Overview of Paid versus Free Feeds
    - Examples of Host-Centric Feeds and Sources
    - Examples of Network-Centric Feeds and Sources
  - Pivoting
    - Pivoting and Operational Profiles
    - Pivoting as an Iterative Process
    - Guided Pivoting Example
- Closing the Intelligence-Operations Loop
  - Intelligence and Operational Defense
    - Enable Defense
    - Inform Response
    - Facilitate Recovery
  - Intelligence-Informed Alerting
    - Classic Alerting and Its Failures
    - Alerting with Context and Behavioral Understanding



  - Intelligence Support to Operations
    - Classic Understanding: Support SOC, Incident Response
    - Expanded View:
      - IT Operations
      - Network Engineering

        - Policy & Governance
    - Informing Operations
        - Typical View: Security Alert
        - Available Options:
            - Regular Briefings and Meetings
            - Periodic and Ad Hoc Reporting
            - Irregular but Familiar Communication
        - Key Requirement: Adopt Whatever Ensures Organization Listens to Intelligence
        - Nature and Importance of Feedback



Course Author & Instructor

Joe Slowik has emphasized the operational significance of threat intelligence through multiple roles: 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.