CTI + DE&TH Workshop

Paralus LLC

paralus.co

Course Overview

The Paralus Technical Cyber Threat Intelligence (CTI) plus Detection Engineering and Threat Hunting (DE&TH) workshop is designed to be an intensive and technical introduction to these security concepts. By working through topics in a rapid, focused nature, students will quickly gain familiarity with core principles behind CTI work and how this applies to and informs subsequent DE&TH operations. This workshop is designed to be highly interactive and conversational, with opportunities to test out and explore concepts within the material to ensure the greatest possible immersion into critical CTI and DE&TH ideas.

Course Schedule

The Workshop is broken into four, two-hour sessions covering the following topics:

- Session One: Intelligence Fundamentals
    - Meaning & Purpose of Intelligence
    - CTI & Outcomes
- Session Two: Technical Intelligence & Operational Applications
    - Understanding Intelligence Artifacts & Observables
    - Indicators & Indicators of Compromise
    - CTI Purpose & Alignment with Operations
- Session Three: Intelligence-Driven Detection Engineering
    - Understanding Detection Engineering
    - Intelligence Support to Detection Engineering Functions
    - Evaluating Efficacy, Coverage, & Gaps
- Session Four: Intelligence-Driven Threat Hunting
    - Understanding Threat Hunting
    - Threat Hunting Hypothesis Formulation & Development
    - Internal & External Threat Hunting
    - Threat Hunting Outcomes & Deliverables

Course Technical Requirements

- Computer for following along with materials and taking notes is preferable.
- Computer with capability of running virtualized environments for sample analysis is possible, but not necessary.
- Access to any of the following tools is preferable, but not necessary:
    - VirusTotal Intelligence

- DomainTools Iris
- Censys.io
- Urlscan.io

Course Author & Instructor

Joe Slowik currently leads cyber threat intelligence (CTI) functions for the MITRE ATT&CK project while also conducting extensive critical infrastructure cyber security work for the MITRE corporation. Joe 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 the MITRE Corporation 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.