FOR478: **Cyber Threat Intelligence Foundations™**

2 Day Course	12 CPEs	Laptop Required

You Will Be Able To

- Architect an effective CTI program that aligns service support to organizational needs
- Manage requirements and build an actionable ICP that maps telemetry to stakeholder needs
- Baseline threat actor history to contextualize evolving adversary goals and tactics
- Analyze how geopolitical drivers and past adversary operations shape your threat landscape
- Produce finished intelligence products that meet the standards employers and stakeholders expect
- Apply intelligence tradecraft, CTI frameworks, and AI-assisted workflows used by working analysts
- Map your professional skills to a career plan aligned with current industry needs

Business Takeaways

- Return to work with a library of production-ready CTI program templates for immediate use
- Reduce onboarding time for new CTI hires by grounding them in operational realities
- Contextualize cyber news by identifying commonalities with past adversary operations
- Anticipate stakeholder needs by mapping their workflows to drive high-impact CTI support
- Confidently conduct stakeholder interviews to align CTI outputs with common pain points
- Improved threat research workflows through AI integration and intelligence tradecraft best practices during 8 hands-on labs
- Extract insights from malware and logs to predict adversary actions and mitigate risk

Who Should Attend

- Aspirant or current CTI analysts who want to understand industry state of play, how CTI programs are structured, and how to shore up foundational practices, methodologies, or tool use
- Incident responders who want to understand how CTI can assist their hunt efforts and work better with CTI peers
- SOC analysts who want to understand how geopolitical dynamics impact cyber threat activities and explore natural career pathways into CTI
- Military, civilian intelligence, and law enforcement agents who require a baseline understanding of working cyber threats in public or private sector roles
- Business, systems, and risk (GRC) analysts who want to expand their job prospects in CTI and understand which skills are transferable
- Data scientists and intelligence engineers who need to understand CTI data, tooling, and which workflow elements can be automated

FOR478 is an immersive, two-day course designed to explore the Cyber Threat Intelligence (CTI) discipline and its application across enterprise, government, and vendor environments. Engineered for both aspirant and seasoned CTI practitioners, the course demystifies CTI program structure, stakeholder support, and common threat research and analysis workflows. Instruction and hands-on labs are uniquely augmented with expert panel discussions, providing direct exposure to industry thought leaders, prevailing discourse, evolving best practices, and institutional lessons learned.

Day 1 establishes CTI as a customer-centric service designed to drive organizational decision-making against cyber security and business objectives, moving beyond the reductive notion that threat intelligence is solely a data feed. The material then grounds CTI research and analytic production in core frameworks including the Intelligence Lifecycle and the OODA loop before deconstructing CTI program elements, the evolution of the discipline, and the analyst's operational workbench.

The course exposes students to the operational expectations and frequent pain points when supporting cybersecurity and risk stakeholder teams. By analyzing common stakeholder objectives, workflows, and vernacular, students gain the critical framing necessary to anticipate customer needs. This alignment empowers analysts, and the broader intelligence program, to develop strategic partnerships and deliver high-impact support across the organization.

On Day 2, students develop a baseline for analyzing threat actor activity while learning about the risks and rewards of publicly publishing threat research. This includes understanding personal security considerations with potential societal impact. This section also covers effective approaches for collaborating with journalists to amplify research, build personal brand, and drive thought leadership. The course concludes with a deep dive into the specific roles and responsibilities of security and risk teams that comprise strategic, operational, and tactical stakeholder audiences.

Section Descriptions

SECTION 1: Foundational Elements of a CTI Program

Section 1 builds the foundational elements of a CTI program, covering the evolution of the CTI discipline, program structure, analyst KSA development and career planning, stakeholder analysis, collection management, and the CTI analyst workbench. The day features four hands-on labs.

TOPICS: Introduction to Cyber Threat Intelligence; The Evolution of the CTI Field and the Defining Characteristics of CTI; CTI Program Structure, Stakeholder Analysis, Intelligence Requirements, and Collection Management; The Intelligence Collection Plan, Collection Management, and Supporting CTI Data Sets; CTI Mechanics and Analytic Approaches

SECTION 2: Cyber Threats and Stakeholder Workflows

Day 2 deconstructs the anatomy of cyber operations, tracing how state and non-state actor tradecraft evolves during geopolitical tensions and conflict. After baselining adversary behavior, students navigate the professional perils of threat research and media engagement. The day concludes by mapping workflows to various stakeholder audiences.

TOPICS: The Evolution of Cyber Operations; The Ethics and Perils of Threat Research; The Role of the Media and Journalists in CTI; Supporting Stakeholders by Audience Type: Strategic, Operational, and Tactical