

Cyber Threat Intelligence: Building and Running an Intel Function Course

Run a cyber threat intelligence function end to end, from collection priorities to intelligence that drives decisions.

Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: <https://www.graduateschool.edu/courses/cyber-threat-intelligence-course>



support@graduateschool.edu • [\(888\) 744-4723](tel:(888)744-4723)

Course Outline

Module 1: Foundations of Cyber Threat Intelligence

- Lessons:
 - What Cyber Threat Intelligence Is and Is Not
 - The Four Levels of Intelligence: Strategic, Operational, Tactical, Technical
 - Threat Intelligence and Threat Hunting: Parent and Consumer
 - The Intelligence Lifecycle at a Glance
- Applied activity: Learners sort a set of sample intelligence products, such as an executive briefing, a SOC alert, an indicator feed, and a hunting hypothesis, by intelligence level and justify each placement.

Module 2: Planning and Collection

- Lessons:
 - Setting Intelligence Requirements
 - Open Source and Technical Collection
 - Closed Source and Commercial Feeds
 - Evaluating Collection Sources
- Applied activity: Learners draft a set of priority intelligence requirements for a hypothetical organization and select which collection sources would satisfy each requirement.

Module 3: Processing and Analysis

- Lessons:
 - Structured Analytic Techniques
 - The Diamond Model of Intrusion Analysis
 - Mapping Adversary Behavior to MITRE ATT&CK
 - Confidence Levels and Analytic Bias
- Applied activity: Learners take a short incident narrative, plot it on the Diamond Model, map the observed behavior to MITRE ATT&CK,

and assign a confidence level to their conclusion.

Module 4: Dissemination and Sharing

- Lessons:
 - Writing Intelligence Products for Different Audiences
 - The Traffic Light Protocol
 - Information Sharing Organizations and Mechanisms
 - Handling Sensitive and Shared Intelligence
- Applied activity: Learners take one analytic finding from Module 3 and produce two versions of it, an executive summary and a technical bulletin, each correctly labeled with a Traffic Light Protocol marking.

Module 5: Building and Running the Intel Function

- Lessons:
 - Team Structure and Roles
 - Threat Intelligence Platforms and Tooling
 - Integrating Intelligence with the Security Program
 - Measuring Program Value
- Applied activity: Learners sketch a staffing and workflow plan for a small intelligence function supporting a stated organization, including how intelligence reaches the security operations center.

Module 6: From Intelligence to Action

- Lessons:
 - Handing Intelligence to Threat Hunting
 - Handing Intelligence to Incident Response
 - The Hunting Ladder as One Consumer of Intelligence
 - Closing the Feedback Loop and Maturing the Function
- Applied activity: Learners take the finished intelligence product from Module 4 and draft one hunting hypothesis and one incident response question it should answer, then propose a feedback update to the original intelligence requirement.