FOR578: **Cyber Threat Intelligence™**

GCTI
Cyber Threat Intelligence
giac.org/gcti

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
- Identify and create intelligence requirements through practices such as threat modeling
- Understand and develop skills in tactical, operational, and strategic-level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
- Learn the different sources to collect adversary data and how to exploit and pivot off of those data
- Validate information received externally to minimize the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA and STIX/TAXII
- Understand and exploit adversary tactics, techniques, and procedures, and leverage frameworks such as the Kill Chain, Diamond Model, and MITRE ATT&CK
- Establish structured analytical techniques to be successful in any security role

GCTI
Cyber Threat Intelligence
giac.org/gcti

GIAC Cyber Threat Intelligence

The GCTI certification proves practitioners have mastered strategic, operational, and tactical cyber threat intelligence fundamentals and application.

- Strategic, operational, and tactical cyber threat intelligence application & fundamentals
- Open source intelligence and campaigns
- Intelligence applications and intrusion analysis
- Analysis of intelligence, attribution, collecting and storing data sets
- Kill chain, diamond model, and courses of action matrix
- Malware as a collection source, pivoting, and sharing intelligence

THERE IS NO TEACHER BUT THE ENEMY!

Cyber threat intelligence represents a force multiplier for organizations looking to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders. During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting, security operations, and incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. FOR578: Cyber Threat Intelligence will train you and your team in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

All security practitioners should attend FOR578: Cyber Threat Intelligence to sharpen their analytical skills. This course is unlike any other technical training you have ever experienced. It focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills. It is common for security practitioners to call themselves analysts. But how many of us have taken structured analysis training instead of simply attending technical training? Both are important, but very rarely do analysts focus on training on analytical ways of thinking. This course exposes analysts to new mindsets, methodologies, and techniques to complement their existing knowledge and help them establish new best practices for their security teams. Proper analysis skills are key to the complex world that defenders are exposed to on a daily basis.

The analysis of an adversary's intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that addresses an organization's key knowledge gaps, pain points, or requirements. This collection, classification, and exploitation of knowledge about adversaries gives defenders an upper hand against adversaries and forces defenders to learn and evolve with each subsequent intrusion they face.

Cyber threat intelligence thus represents a force multiplier for organizations looking to establish or update their response and detection programs to deal with increasingly sophisticated threats. Malware is an adversary's tool, but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

Knowledge about the adversary is core to all security teams. The red team needs to understand adversaries' methods in order to emulate their tradecraft. The Security Operations Center needs to know how to prioritize intrusions and quickly deal with those that need immediate attention. The incident response team needs actionable information on how to quickly scope and respond to targeted intrusions. The vulnerability management group needs to understand which vulnerabilities matter most for prioritization and the risk that each one presents. The threat hunting team needs to understand adversary behaviors to search out new threats.

In other words, cyber threat intelligence informs all security practices that deal with adversaries. FOR578 will equip you, your security team, and your organization with the level of tactical, operational, and strategic cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and accurately and effectively counter those threats.

Section Descriptions

SECTION 1: Cyber Threat Intelligence and Requirements

This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, as well as the value they can add to organizations.

TOPICS: Intelligence Cycle, Tradecraft, and Analytical Techniques; Cyber Threat Definitions, Risk, Actors, and Threat Models; Threat Intelligence Collection and Generation

SECTION 2: The Fundamental Skillset: Intrusion Analysis

In this section, students will be walked through and participate in multi-phase intrusions from initial notification of adversary activity to the completion of analysis of the event. The section also highlights the importance of this process in terms of structuring and defining adversary campaigns.

TOPICS: Intrusion Analysis; Kill Chain Deep Dive; Handling Multiple Kill Chains

SECTION 3: Collection Sources

In this section, students will learn to seek and exploit information from domains, external datasets, malware, Transport Layer Security/Secure Sockets Layer (TLS/SSL) Certificates, and more. Students will also structure the data to be exploited for purposes of sharing internally and externally.

TOPICS: Collection Sources; Different Styles of Analysis

SECTION 4: Analysis Production of Intelligence

In this section, students will learn how to structure and store their information; how to leverage analytical tools to identify logical fallacies and cognitive biases; how to perform structured analytic techniques in groups such as analysis of competing hypotheses; and how to cluster intrusions into threat groups.

TOPICS: Human-Operated Ransomware; Storing and Structuring Data; Logical Fallacies and Cognitive Biases; Clustering Intrusions and Creating Activity Groups

SECTION 5: Dissemination and Attribution

Intelligence is useless if not disseminated and made useful to the consumer. In this section students will learn about dissemination at the various tactical, operational, and strategic levels.

TOPICS: Tactical Dissemination; Operational Dissemination; Strategic Dissemination; Attribution

SECTION 6: Cyber Threat Intelligence Capstone

The FOR578 capstone focuses on analysis. Students will be placed on teams, given outputs of technical tools and cases, and work to piece together the relevant information from a single intrusion that enables them to unravel a broader campaign.

Authors' Statements

"When considering the value of threat intelligence, most individuals and organizations ask themselves three questions: What is threat intelligence? When am I ready for it? How do I use it? This class answers these questions and more at a critical point in the development of the field of threat intelligence in the wider community. The course will empower analysts of any technical background to think more critically and be prepared to face persistent and focused threats."

—Robert M. Lee

"Threat intelligence is a powerful tool in the hands of a trained analyst. It can provide insight to all levels of a security program, from security analysts responding to tactical threats against the network to executives reporting strategic-level threats to the Board of Directors. This course will give students an understanding of the role of threat intelligence in security operations and how it can be leveraged as a game-changing resource to combat an increasingly sophisticated adversary."

—Rebekah Brown

"Cyber Threat Intelligence is an entire discipline, not just a feed. This course will propel you along the path to understanding this rapidly maturing field of study."

—Bertha Marasky, **Verizon**

Who Should Attend

- Incident response team members
- Those who respond to complex security incidents/intrusions and need to know how to detect, investigate, remediate, and recover from compromised systems across an enterprise
- Threat hunters who are seeking to understand threats more fully and how to learn from them to be able to more effectively hunt threats and counter the tradecraft behind them
- Security Operations Center personnel and InfoSec practitioners who support hunting operations that seek to identify attackers in their network environments
- Digital forensic analysts and malware analysts who want to consolidate and expand their understanding of filesystem forensics, investigations of technically advanced adversaries, incident response tactics, and advanced intrusion investigations
- Federal agents and law enforcement officials who want to master advanced intrusion investigations and incident response, as well as expand their investigative skills beyond traditional host-based digital forensics
- Technical managers who are looking to build intelligence teams or leverage intelligence in their organizations building off of their technical skillsets
- SANS alumni looking to take their analytical skills to the next level

NICE Framework Work Roles

- Data Analyst (OPM 422)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Incident Responder (OPM 531)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Mission Assessment Specialist (OPM 112)
- Target Network Analyst (OPM 132)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Intel Planner (OPM 331)
- Partner Integration Planner (OPM 333)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)