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 it
- Validate information received externally to minimize the costs of bad intelligence
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
- Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats
- 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!

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: Cyber Threat Intelligence 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.

"I could take this course five times more and get something new each time! So much valuable info to take back to my organization."

—Charity Willhoite, **Armor Defense, Inc.**

"This course is terrific! Class discussion and relevant case studies are extremely helpful for better understanding the content."

—Larci Robertson, **Epsilon**

Section Descriptions

SECTION 1: Cyber Threat Intelligence and Requirements

Cyber threat intelligence is a rapidly growing field. However, intelligence was a profession long before the word "cyber" entered the lexicon. Understanding the key points regarding intelligence terminology, tradecraft, and impact is vital to understanding and using cyber threat intelligence. This section introduces students to the most important concepts of intelligence, analysis tradecraft, and levels of threat intelligence, and the value they can add to organizations. It also focuses on getting your intelligence program off to the right start with planning, direction, and the generation of intelligence requirements. As with all sections, the day includes immersive hands-on labs to ensure that students have the ability to turn theory into practice.

TOPICS: Case Study: MOONLIGHT MAZE; Understanding Intelligence; Case Study: Operation Aurora; Understanding Cyber Threat Intelligence; Threat Intelligence Consumption; Positioning the Team to Generate Intelligence; Planning and Direction (Developing Requirements)

SECTION 2: The Fundamental Skillset: Intrusion Analysis

Intrusion analysis is at the heart of threat intelligence. It is a fundamental skill set for any security practitioner who wants to use a more complete approach to addressing security. Two of the most commonly used models for assessing adversary intrusions are the "kill chain" and the "Diamond Model." These models serve as a framework and structured scheme for analyzing intrusions and extracting patterns such as adversary behaviors and malicious indicators. In this section students will participate in and be walked through 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: Primary Collection Source: Intrusion Analysis; Kill Chain Courses of Action; Kill Chain Deep Dive; Handling Multiple Kill Chains

SECTION 3: Collection Sources

Cyber threat intelligence analysts must be able to interrogate and fully understand their collection sources. Analysts do not have to be malware reverse engineers, as an example, but they must at least understand that work and know what data can be sought. This section continues from the previous one in identifying key collection sources for analysts. There is also a lot of available information on what is commonly referred to as open-source intelligence (OSINT). In this course section students will learn to seek and exploit information from Domains, External Datasets, Transport Layer Security/Secure Sockets Layer (TLS/SSL) Certificates, and more while also structuring the data to be exploited for purposes of sharing internally and externally.

TOPICS: Case Study: HEXANE; Collection Source: Malware; Collection Source: Domains; Case Study: GlassRAT; Collection Source: External Datasets; Collection Source: TLS Certificates; Case Study: Trickbots

SECTION 4: Analysis and Production of Intelligence

With great data comes great analysis expectations. Now that students are familiar with different sources of intrusions and collection, it is important to apply analytical rigor to how this information is used in order to satisfy intelligence requirements for long-term analysis. Taking a single intrusion and turning it into a group, and tracking the adversary's campaigns, are critical to staying ahead of adversaries. In this section students will learn how to structure and store their information over the long term using tools such as MISP; 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: Case Study: Human-Operated Ransomware; Exploitation: Storing and Structuring Data; Analysis: Logical Fallacies and Cognitive Biases; Analysis: Exploring Hypotheses; Analysis: Different Types of Analysis; ACH for Intrusions; Activity Groups and Diamond Model for Clusters

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. Labs will expose students to creating YARA rules, leveraging STIX/TAXII, building campaign heat maps for tracking adversaries over the long term, and analyzing intelligence reports. Students will also learn about state adversary attribution, including when it can be of value and when it is merely a distraction. We'll cover state-level attribution from previously identified campaigns, and students will take away a more holistic view of the Cyber Threat Intelligence industry to date. The section will finish with a discussion on consuming threat intelligence and actionable takeaways so that students will be able to make significant changes in their organizations once they complete the course.

TOPICS: Logical Fallacies and Cognitive Biases; Dissemination: Tactical; Dissemination: Operational; Dissemination: Strategic; Case Study: APT10 and Cloud Hopper; A Specific Intelligence Requirement: Attribution; Case Study: Lazarus Group

SECTION 6: 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. Students will get practical experience satisfying intelligence requirements ranging from helping the incident response team to satisfying state-level attribution goals. This analytical process will put the students' minds to the test instead of placing a heavy emphasis on using technical tools. At the end of the day the teams will present their analyses on the multi-campaign threat they have uncovered.

Who Should Attend

- Security practitioners, should attend. This course is perfect match to any security skill set from red teamers to incident responders. The course is focused on analysis skills.
- Incident response team members 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 Information Security 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)