FOR589: **Cybercrime Intelligence**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Understand how traditional intelligence collection disciplines have adapted to today's modern cyber-centric landscape and differentiate what is actionable and what is noise
- Discover risks to your organization's assets and elements, mapped to threat actors and threat vectors as priority intelligence requirements
- Translate your organization's risk-guided intelligence requirements into threat-informed collection plans and operational tasks
- Address cybercrime risks with threat-informed decisions, enabling you to determine courses of action that are both defensive and responsive, whether to protect your organization or impose costs on criminals with counter-offensive measures
- Demystify the dark web and underground threat landscape, enabling you to traverse and surveil communities, marketplaces, ransom sites, data breaches, malware logs, and more
- Understand how the underground threat landscape has expanded and evolved, lowering the barrier to entry, allowing emerging actors to conduct perceivably advanced operations
- Create online personas and sock puppet safely to gain the placement and access needed for intelligence collection, whether to passively browse forums or actively elicit brokers
- Build credibility within underground networks to enable your sock puppet to infiltrate invite-only communities and adversarial infrastructure
- Vet sources by measuring their level of competence, access, and credibility
- Generate actionable cybercrime intelligence by delivering realistic solutions built upon tried-and-true intelligence requirements, collection plans, and operating procedures
- Apply practical victimology to map the adversary-target relationship observed in cyberattacks and cyber fraud incidents, useful for research and response purposes alike
- Speed up root cause analysis of cyberattacks with breach indicators and identifiers, reducing patient zero identification time from weeks/days to hours/minutes
- Develop threat intelligence platforms as early warning systems to detect all-source digital risk exposures within the Internet ecosystem, especially the deep and dark web
- Trace cryptocurrency payments using commercial and open-source tools to identify senders and receivers, and attribute them by using cluster analysis

Cybercrime intelligence can help organizations effectively anticipate, prevent, and mitigate potential cybercrime threats, while also helping law enforcement agencies and governments combat cybercrime and prosecute criminals. FOR589: Cybercrime Intelligence provides an in-depth understanding of the cybercrime underground and covers the wide variety of tactics and techniques used by cybercriminals to exploit organizations. By focusing on both conventional intelligence and contemporary cybersecurity methodologies, this course will help you augment any existing intelligence operations, proactively address risks, and enhance an overall cybersecurity posture. The course is ideal for security professionals, law enforcement officers, and anyone interested in the intricacies of the cybercrime underground, tracing cryptocurrency, intelligence and countermeasures.

The course covers how to map infrastructure, analyze capabilities, and uncover the victims of cybercrime, as well as attribute operations to the cybercriminal behind the keyboard. Students learn all about the dark web economy, tracing cryptocurrency, and money laundering schemes. This course also teaches students how to perform undercover operations safely, including how to create sock puppet accounts, interact with threat actors, and how to infiltrate underground communities. Participants will gain hands-on experience with various cybersecurity tools and work on real-life case studies to detect, analyze, and mitigate cyber threats as well as understand the scope, scale, and potential impact that organized cybercrime could have against their organizations.

Through practical exercises and real-life case studies, students in FOR589: Cybercrime Intelligence will gain hands-on experience and develop the skills to:

- Map cybercriminal infrastructure, analyze cybercriminal capabilities, uncover the victims of cybercrime, and attribute operations to the cybercriminals behind the keyboard
- Navigate the dark web, trace cryptocurrency transactions, and understand money-laundering schemes
- Perform undercover operations, including how to traverse the dark web safely, create sock puppet accounts with sound operational security (OPSEC), interact with threat actors, and infiltrate underground communities
- Work with various cybersecurity tools to detect, analyze, and mitigate cyber threats, as well as understand the scope, scale, and impact of organized cybercrime

Business Takeaways

- Close knowledge gaps between cybercrime and crypto crime
- Enhance Cyber Threat Intelligence (CTI) operations with cybercrime expertise
- Proactively discover and mitigate emerging cybercrime threats looming over the horizon
- Establish early warning systems to detect risks, threats, and fraud
- Identify access vectors and collect against cybercriminals exploring those vectors
- Focus investigative priorities with informed advice
- Profile cybercrime events using common intelligence frameworks and cyber kill chains
- Attribute threat actors behind cyberattacks and cyber fraud when needed
- Conduct blockchain forensics for attribution and fund recovery
- Create tailored intel products to supplement vendor offerings
- Support incident response teams with timely and relevant intelligence

Section Descriptions

SECTION 1: The Cybercriminal Intelligence Lifecycle

There are ways to stay ahead of the cybercrime economy - it starts with knowing the vast landscape you are up against and applying methodology to make sense of it all. Security professionals and law enforcement should be aware of the latest criminal trends. In scenarios where risk is high and room for error is low, peers and victims rely on us for help. To provide that help, our processes and methodology must be defensible. Using these standards for curating and handling cybercrime intelligence, FOR589 will be able to ensure that their selected courses of action are properly guided, decided, and applied. Section 1 introduces standards for intelligence requirements, collection plans, operating procedures, intelligence lifecycles, and knowledge frameworks that students will use to make intelligent decisions while also being mindful of operational security considerations. If we understand our elements and assets at risk, we can map them to our opposing threat actors and attack vectors. This approach allows us to repeatably anticipate emerging threats, stay ahead of cybercriminals, and mitigate risks to defend against threats.

TOPICS: Intelligence Fundamentals; Intelligence Operations; Planning Collections; Curating Collections; Cyberattack Forecasting; Cyberattack Profiling; Operational Security 101

SECTION 2: The Cybercriminal Underground

Within the cybercriminal ecosystem, there are adversaries/criminals, victims/targets, methods/services, and infrastructure/finances, so demystifying that ecosystem has never been so clear. As an intelligence professional, understanding the cybercrime underground is vital to knowing the landscape and economy that you are up against. From attackers to targets, people to communities, currencies to technologies, and capabilities to infrastructure, we must have the know-how to access and traverse it all. With a solid mapping of the cybercrime underground, we meet the adversaries on their own playgrounds to gather underground intelligence at its source. This section will provide students with the resources necessary to find the "known" and explore the "unknown." By demystifying the cybercriminal underground, we can find both, which is fundamental to take on emerging risks and threats with identification, protection, detection, response, and recovery. This is also needed to prepare a counter-offensive response. By the end of this section you will be able to see eye-to-eye with cybercriminals on their own playing field, opening possibilities for a strong defense or a knock-out offense.

TOPICS: Tracking Cybercriminal Ecosystems with Underground Intelligence; Cybercrime Discovery: Services and Infrastructure; Cybercrime Discovery: Actors and Adversaries; Cybercrime Discovery: Methods and Capabilities; Cybercrime Discovery: Targets and Victims; Tools of the Tradecraft: Threat Intelligence Platforms

SECTION 3: Cryptocurrency Investigations

Cryptocurrencies are often thought to be anonymous, but they are pseudonymous at best. Since criminals deal heavily in these virtual assets, we can exploit this to unmask them! The prevalence of cryptocurrency in the criminal economy can neither be overstated nor overlooked. In this section, students will learn to trace through cryptocurrency, understand its underlying blockchain technology, and demystify the money laundering schemes layered atop. In addition, we translate these concepts to practical intelligence applications, such as criminal attribution. While these virtual assets have certainly played a prolific role in the funding of services within the cybercriminal underground, they are not bulletproof! Mistakes are made during transactions, creating opportunities to map out criminal counterparties and their affiliated real-life identities. This section teaches empowering cluster-analysis skills that are useful to differentiate senders from receivers, separate services from people, and demystify money-laundering schemes. Finally, we explore the practical use of "Know-Your-Customer" requests for unmasking criminals.

TOPICS: Tracking Financial Crimes with Financial Intelligence; Tracing Cryptocurrency Crimes with Blockchain Intelligence; Cryptocurrency Tracing: Basic Clustering; Cryptocurrency Tracing: Advanced Clustering; Cybercriminal Profiling with Cryptocurrency Attribution

SECTION 4: Undercover Operations and Countermeasures

We've assessed the cybercriminal ecosystem. Now let's infiltrate deeper to facilitate the use of countermeasures. Criminals can be disrupted using social deceit, campaign mapping, and planned takedowns. People, systems, and money possess exploitable characteristics that can be recognized by investigators with the correct access and skills. These characteristics can be collected to inform a variety of countermeasures. This section teaches you how to spot these characteristics, collect them both manually and automatically, and leverage them for criminal investigation and disruption. This section will teach students how to use a combination of rapport and elicitation techniques that exploit core characteristics of a human intelligence source. Through this process, the intelligence collector will maintain covertly structured control of the conversation to ensure that each cybercriminal source reveals topics that are relevant to the collector's intelligence requirements. Once cybercriminals and their infrastructure are attributed, a new realm of possibility to enforce countermeasures presents itself, with opportunities ranging from forensic seizures to coordinated takedowns.

TOPICS: Undercover Preparation: Case Management; Undercover Preparation: Personas and Accounts; Undercover Engagements: Infiltration and Deception; Undercover Engagements: Automating Data Collections; Undercover Countermeasures: Responsive Disruption

SECTION 5: Capstone

Put everything you learned to the test by investigating the cybercriminal underground and unraveling who is behind a new kind of cyber extortion campaign. The final day of FOR589 is a capstone challenge that focuses on launching an investigation. Students engage in a fun and meaningful exercise that brings together various components of the entire course. The capstone will reinforce the principles taught via a simulated scenario that enables students to practice implementing their newly learned skills. Students will be presented with a fictional scenario and then given a list of items to investigate and analyze. These will include posts, threads, and profiles from cybercriminal underground forums, markets, and leak sites, as well as leaked private chat logs, databases, and threat actor infrastructure. There will also be a fictional blockchain ledger that students will use to trace transactions and track threat actors and various types of activities. Students will have to think about how to fulfil intelligence requirements from a law enforcement perspective, using the data sets provided that emulate real-world scenarios investigated by intelligence analysts. Students will be placed on teams and at day's end make presentations to instructors and the class to showcase what they found in their investigations, including the steps taken during the intelligence life cycle showing what they collected, processed, analyzed, and exploited.

TOPICS: What You Will Learn; What You Will Need; What You Will Do

Who Should Attend

- Cyber threat intelligence analysts
- Cyber intelligence professionals
- Criminal actor investigators
- Financial crime investigators
- Threat hunters
- Incident responders
- Forensic analysts
- Information security professionals
- Federal agents and law enforcement professionals
- SANS alumni looking to take their skills to the next level

NICE Framework Work Roles

- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- All-Source Analyst (OPM 111)
- Cyber Crime Investigator (OPM 221)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Forensics Analyst (OPM 212)
- Cyber Defense Incident Responder (OPM 531)
- Cyber Intel Planner (OPM 331)
- Cyber Operator (OPM 331)
- Cyber Ops Planner (OPM 332)
- Cyber Policy and Strategy Planner (OPM 752)
- Data Analyst (OPM 422)
- Exploitation Analyst (OPM 121)
- Law Enforcement/Counterintelligence Forensics Analyst (OPM 211)
- Mission Assessment Specialist (OPM 112)
- Partner Integration Planner (OPM 333)
- Research & Development Specialist (OPM 661)
- Target Developer (OPM 131)
- Target Network Analyst (OPM 132)
- Threat/Warning Analyst (OPM 141)