FORENSICS 578

Hands On | Five Days | Laptop Required | 30 CPEs

FOR578: Cyber Threat Intelligence

Make no mistake: current computer network defense and incident response contain a strong element of intelligence and counterintelligence that analysts must understand and leverage in order to defend their computers, networks, and proprietary data.

FOR578: Cyber Threat Intelligence will help network defenders and incident responders:

- Construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organizations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions.

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology pre-supposes a successful intrusion. However, the evolving sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as **cyber threat intelligence** – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. **FOR578: Cyber Threat Intelligence** will train you and your team to determine, scope, and select resilient courses of action in response to such intrusions and data breaches.

THERE IS NO TEACHER BUT THE ENEMY!

Who Should Attend

- Incident response team members who regularly respond to complex security incidents/intrusions from APT adversaries and need to know how to detect, investigate, remediate, and recover from compromised systems across an enterprise
- Security operations center personnel and information security practitioners who support hunting operations that seek to identify attackers in their network environments
- Experienced digital forensic 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
- SANS FOR408, FOR572, FOR508, or FOR610 graduates looking to take their skills to the next level

> "Fantastic class! I love the way the terminology was covered. I will be making index cards to ensure I have them memorized."
>
> -Nate DeWitt, eBay, Inc.

DFIR
digital-forensics.sans.org

Course Day Descriptions

578.1 HANDS ON: Cyber Threat Intelligence for Intrusions

A key facilitator of cyber threat intelligence (CTI) is to use a common lexicon that defines its most basic elements and ideas. This section introduces students to fundamental CTI concepts and models, beginning with an understanding of broader intelligence analysis tradecraft. The section introduces and defines CTI through conventional lectures, class participation, and exercises from the students' lab book.

Topics: Course Introduction; Current Threat Landscape; Classic Intelligence Analysis; Intelligence in Computer Network Defense; Diamond Model; Kill Chain Introduction and Background; Kill Chain Phases in Detail; Analytical Aspects of the Kill Chain; Courses of Action Matrix; Indicator Lifecycle; Indicator Maturity Model; Decision-making in Intelligence Exploitation; Additional, Alternate, and Emergent Models

578.2 HANDS ON: Kill Chain for Computer Network Defense

One of the most commonly used and basic models covered in the first section is the "kill chain," which is the series of steps an adversary must accomplish to be successful. This section will use the kill chain as a guide to collect intelligence on the sophisticated adversary involved in a multi-phase intrusion, from initial discovery of command-and-control to completion of analysis of the event. The section also draws on other models introduced in Section 1, such as the Courses of Action Matrix, to show students their proper role in analyzing a successful intrusion as they methodically work their way toward being able to define a full campaign using the concepts introduced here.

Topics: Scenario-based Kill Chain Analysis: Web Drive-by; Application of Courses of Action for Computer Network Defense; Analytical Completeness Guided by Kill Chain Analysis; Multi-Stage Intrusions and Kill Chain Sequencing; Second Scenario-based Kill Chain Analysis: Webserver Intrusion; Historical Unsuccessful Intrusion Attempt: Phishing Attempt; Completing the Picture with Available Intelligence

FOR578 Training Formats

(subject to change)

Live Training
sans.org/security-training/by-location/all

Summit Events
sans.org/summit

Private Training
sans.org/onsite

Simulcast
sans.org/simulcast

SelStudy
sans.org/selfstudy

578.3 HANDS ON: Campaigns and Open-Source Pivoting

An intrusion is but a single attempt by an adversary to gain access to a system for some intended purpose. Dedicated adversaries, intent on exploiting systems that support specific organizations, people, or technologies, will not let one failed attempt deter them from their ultimate goal. Their sustained campaign will likely consist of multiple intrusions over an extended period of time, each with its individual kill chain, against organizations you monitor and defend as well as others beyond your visible spectrum. In this section, students learn what campaigns are, why they are important, and how to define them. From this baseline intelligence, gaps and collection opportunities are identified for fulfillment via open-source resources and methods. Common types and implementations of open-source data repositories, as well as their use, are explored in-depth through classroom discussion and exercises. These resources can produce an enormous volume of intelligence about intrusions, which may contain obscure patterns that further elucidate campaigns or actors. Tools and techniques to expose these patterns within the data through higher-order analysis will be demonstrated in narrative and exercise form. The application of the resulting intelligence will be articulated for correlation, courses of action, campaign assembly, and more.

Topics: Abbreviated History of Threats in Cyberspace; Cross-Incident Correlation; Campaign Definitions; Distinguishing Correlative and Actionable Intelligence Pitfalls in Correlating Intrusions Interpreting Campaign Intersections Pivoting, Hunting, and External Intelligence Exploitation; Exploratory Techniques for Campaign Analysis

578.4 HANDS ON: Organizations, Nation-States, and Higher-Order Analysis

Behind campaigns are people, and just like network defenders and intelligence analysts, these intruders have roles within organizations, employers, bosses, customers, and colleagues. This section will explore in more depth the characteristics of the organizational entities behind intrusions, and how these characteristics are projected through intrusions. Cognitive biases common in the cyber threat intelligence (CTI) domain are discussed. Analysis of Competing Hypotheses is then presented as a formal method for mitigating bias in intelligence assessments in general, then for nation-state and (separately) campaign attribution. Intent, opportunity, and capability are revisited from Section 1 in greater detail, particularly as they pertain to nation-state actors.The role and significance of nation-state attribution in CTI analysis is discussed as a general concept, with examples from contemporaneous nation-state threats. Finally, an abridged history of threats in cyberspace that marked inflection points particularly significant for the CTI domain is provided.

Topics: Formulating Conclusions; Cognitive Biases & Analysis of Competing Hypotheses (ACH); Nation-State Attribution; Understanding Threats and Their Actions at the Strategic and Operational Level; Abridged History of Threats in Cyberspace Influencing the CTI Domain

578.5 HANDS ON: Collecting, Sharing, and Actuating Intelligence

Intrusions consist of an enormous amount of information that, once refined, represents intelligence. In this section, students will learn effective ways to manage intelligence, collaborate with their peers, and empower their security teams. Campaigns consist of intrusions spanning months and sometimes even years, each with its own details linking its constituent intrusions. Collecting this intelligence is critical to making it actionable for defense, and appropriately sharing it with internal and peer organization security teams makes it possible to identify the resilient characteristics of adversaries and discover new campaigns. Intrusions will span organizations, and sometimes even spread across industries. External intelligence is key to keep up to date on the latest movements and tactics of adversaries, even if they are not (yet!) targeting you.

Topics: Intelligence-Sharing Purposes and Considerations; Extracting Tactical Threat Intelligence; Open-Source Intelligence Collection (OSINT); Commercial and Open-Source CTI Solutions; Intelligence Knowledge Management; Internal Threat Intel Sharing; Peer Collaboration; Report Writing