Certified Cyber Forensics Threat Analyst

Description:

The **Certified Cyber Forensics Threat Analyst (C)CFTA)** is an advanced-level, practitioner-focused certification that trains cybersecurity professionals to collect, preserve, and analyze network-based digital evidence in support of cyber incident investigations and threat analysis. Aligned to DoD 8140 / DCWF Work Role 212 (Cyber Defense Forensics Analyst), the C)CFTA prepares candidates for the full lifecycle of a network forensics investigation: from physical and wireless evidence acquisition through protocol-level analysis, NSM toolchain operation, threat intelligence integration, timeline construction, anti-forensics detection, and cloud network forensics.

Annual Salary Potential $99,000 AVG/year

Course Information

Live Class Duration: 5 Days

CEUs: 40

Language: English

Class Formats Available:

- Instructor Led
- Self-Study
- Live Virtual Training

Suggested Prerequisites:

- 2 years networking experience
- 2 years in IT Secuirty
- Working knowledge of TCPIP

Modules/Lessons

Module 00: Course Introduction
Module 01: Network Forensics
Module 02: Digital Evidence
Module 03: Network Evidence
Module 04: Wireshark & Traffic
Module 05: Protocol Analysis
Module 06: Protocol Security
Module 07: NetFlow, IPFIX & Zeek
Module 08: NIDS/NIPS, Snort
Module 09: Network Log Forensics
Module 10: Wireless & Cloud
Module 11: Threat Investigation
Module 12: Anti-Forensics

Detailed Outline Below

Hands-On Labs

Lab 01: Network Evidence
Lab 02: Wireshark Fundamentals
Lab 03: Core Protocol Analysis
Lab 04: DNS, SMTP, FTP & Email
Lab 05: NetFlow / IPFIX / sFlow
Lab 06: Zeek (Bro) Log Analysis
Lab 07: Intrusion Detection
Lab 08: Proxy & Web Application
Lab 09: Wireless Network
Lab 10: Malware & C2 Analysis
Lab 11: Advanced Packet Carving
Lab 12: Network Timeline
Lab 13: Anti-Forensics & Evasion
Lab 14: Enterprise Triage with
Lab 15: Cloud Network Forensics

Detailed Outline Below

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Certified Cyber Forensics Threat Analyst

Accreditations

- ANAB (ANSI National Accreditation Board) ISO/IEC 17024 Aligned
- DoD 8140 / DCWF Work Role 212 — Cyber Defense Forensics Analyst
- NICE Cybersecurity Workforce Framework (NIST SP 800-181) Mapped
- Approved for DoD 8570 IA Workforce Improvement Program

Who Should Attend

- Forensic Examiners
- IS Managers
- Network Auditors
- IT Managers

Exam Information

The C)CFTA exam is taken online through Mile2's Assessment and Certification System ("MACS"), accessible from your mile2.com account. The exam consists of 100 multiple-choice questions with a 2-hour time limit.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

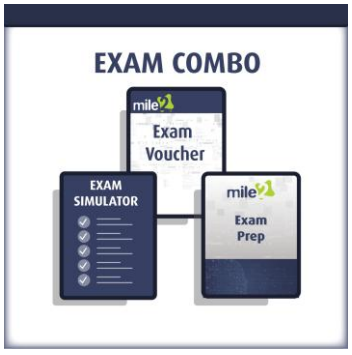
Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options



www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Upon Completion

Upon completion of the C)CFTA program, candidates will be equipped to sit for the C)CFTA certification exam and will possess the practical skills required to perform network-based forensic investigations in enterprise and government environments. Candidates will be able to:

- Acquire, preserve, and maintain chain of custody for network-based digital evidence including PCAPs, flow records, and log exports
- Apply the OSCAR investigative methodology to structure and document network forensics investigations from evidence collection through formal reporting
- Perform deep packet analysis using Wireshark, tshark, and tcpdump — including BPF filtering, protocol dissection, stream reassembly, and object extraction
- Analyze NetFlow, IPFIX, and sFlow records to detect lateral movement, exfiltration, and anomalous behavior
- Deploy and query the Zeek (Bro) NSM framework to produce structured logs for forensic investigation
- Configure and analyze Snort and Suricata for intrusion detection, alert triage, and custom rule development
- Correlate firewall logs, proxy logs, web server logs, and Windows Event Log data across multiple sources into a unified forensic timeline
- Identify and investigate C2 channels, covert tunneling (DNS, ICMP), malware beaconing, ransomware kill chain evidence, and phishing artifacts in packet captures
- Reconstruct network intrusion timelines using SOF-ELK and Timesketch, and detect anti-forensics evasion techniques on the wire
- Conduct enterprise-scale triage using RITA for automated beacon detection across distributed Zeek sensor logs
- Apply wireless network forensics techniques to 802.11 captures including attack detection, rogue AP identification, and WPA handshake analysis
- Analyze cloud network evidence sources including VPC flow logs, CloudTrail, Azure Activity Logs, GCP Audit Logs, and container/Kubernetes network forensics
- Map investigative findings to MITRE ATT&CK techniques and produce structured forensic reports for technical, executive, and legal audiences

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Detailed Course Outline

Module 00: Course Introduction

Module 01: Network Forensics Foundations

- Section 01: What Is Network Forensics?
- Section 02: The Threat Analyst Role & Adversary Landscape
- Section 03: Scope & Applicability
- Section 04: Tools Overview

Module 02: Digital Evidence & Investigative Methodology

- Section 01: Types of Digital Evidence
- Section 02: Network Evidence Challenges
- Section 03: Evidence Handling & Legal Authority
- Section 04: OSCAR Investigative Methodology

Module 03: Network Evidence Sources & Physical Interception

- Section 01: Sources of Network-Based Evidence
- Section 02: Physical Interception Methods
- Section 03: Tcpdump & Capture Management
- Section 04: Interception Hardware & Infrastructure
- Section 05: Live Acquisition & Chain of Custody

Module 04: Wireshark & Traffic Triage

- Section 01: Capture Libraries & BPF Filtering
- Section 02: Wireshark, Tshark & Capture Tools
- Section 03: Advanced Packet Analysis

Module 05: Protocol Analysis, Session Reconstruction & Packet Carving

- Section 01: Protocol Stack as Forensic Evidence
- Section 02: Transport, Address & Layer 2 Forensics
- Section 03: Session Reconstruction, Carving & TLS Decryption
- Section 04: Network Attack Forensics — PCAP-Level Indicators

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Module 06: Protocol Security & DNS/Email/FTP Forensics

Section 01: Protocol Security Fundamentals
Section 02: Protocol-Specific Vulnerability Forensics
Section 03: Phishing Investigation

Module 07: NetFlow, IPFIX & Zeek Forensics

Section 01: Flow Records & NetFlow Forensics
Section 02: Zeek (Bro) NSM Framework

Module 08: NIDS/NIPS, Snort & Suricata Forensics

Section 01: NIDS/NIPS Fundamentals & Forensic Context
Section 02: NIDS/NIPS Evidence Acquisition
Section 03: Snort — Architecture, Rules & Forensic Analysis
Section 04: Suricata — Rules, PCAP Analysis & eve.json
Section 05: Suricata vs. Zeek & Rule Tuning for Forensics

Module 09: Network Log Forensics & Proxy Analysis

Section 01: Log Forensics Foundations
Section 02: Firewall, IDS & System Logs
Section 03: Proxy & Web Server Log Analysis

Module 10: Wireless & Cloud Network Forensics

Section 01: Wireless Physical & Link-Layer Fundamentals
Section 02: WEP to WPA3 Evolution & 802.1X
Section 03: Wireless Infrastructure & Forensic Scope
Section 04: 802.11 Standards & Encryption
Section 05: Wireless Evidence Acquisition
Section 06: Wireless Traffic Analysis & Attack Detection
Section 07: Cloud Network Forensics

Module 11: Threat Investigation: C2 & Malware Analysis

Section 01: C2 Channels & Covert Tunneling
Section 02: Malware Network Traffic Analysis
Section 03: Threat Investigation Workflow

Module 12: Timeline, Anti-Forensics & Enterprise Triage

Section 01: Network Intrusion Investigation Framework
Section 02: IIS Log Forensics & Time Correlation
Section 03: Network Timeline Construction
Section 04: Anti-Forensics Detection on the Network
Section 05: Multi-Source Correlation & PCAP Matching
Section 06: Enterprise-Scale Network Triage

Detailed Labs Outline

The C)CFTA program includes 15 hands-on laboratory exercises covering the full investigation lifecycle. Labs are conducted in a preconfigured virtual environment with real-world evidence data including live PCAPs, flow records, Zeek logs, Suricata alerts, proxy logs, and cloud telemetry.

Lab 01: Network Evidence Acquisition

- Capture live network traffic in a controlled investigation environment
- Acquire PCAPs using tcpdump, Wireshark, and Velociraptor
- Handle large captures using file splitting, ring buffers, and capture-time filtering

Lab 02: Wireshark Fundamentals & Traffic Triage

- Navigate Wireshark: IO Graphs, Conversations, Endpoints, and Expert Info panels
- Apply display filters and BPF capture filters for targeted analysis
- Identify normal vs. anomalous traffic patterns in real-world PCAPs
- Export objects (files, images, executables) from packet captures

Lab 03: Core Protocol Analysis — TCP/IP, HTTP/HTTPS

- Deep dive into TCP handshake mechanics, flag anomalies, and session reconstruction
- HTTP request/response analysis for C2 detection and data exfiltration identification
- TLS decryption using session key logs and certificate analysis

Lab 04: DNS, SMTP, FTP & Email Forensics on the Wire

- Detect DNS tunneling, fast-flux, and resolution anomalies in packet captures
- Analyze SMTP traffic for phishing and spam campaign identification
- Investigate FTP/SFTP sessions for credential harvesting and file transfer evidence
- Reassemble and carve files transferred over DNS, SMTP, and FTP protocols

Lab 05: NetFlow / IPFIX / sFlow Analysis

- Generate and analyze flow records using nfdump, SiLK, and Elastic
- Detect scanning, lateral movement, and data exfiltration using flow data
- Compare full packet capture vs. flow data — trade-offs, storage efficiency, and forensic gaps

www.mile2.com 10213 Wilsky Blvd, Tampa, FL 33625 813-920-6779

Lab 06: Zeek (Bro) Log Analysis

- Deploy and run Zeek against PCAP evidence files
- Analyze core logs: conn.log, http.log, dns.log, files.log, notice.log
- Use zeek-cut and scripting basics for targeted threat hunting
- Extract and correlate files carved by Zeek across log sources

Lab 07: Intrusion Detection with Suricata

- Configure Suricata rules and run against PCAP evidence files
- Analyze alerts, eve.json logs, and extracted files
- Compare Suricata vs. Zeek outputs on identical traffic — identifying complementary strengths
- Tune rules to reduce false positives in a forensic investigation context

Lab 08: Proxy & Web Application Forensics

- Analyze Squid, BlueCoat, and Zscaler proxy logs for investigative value
- Reconstruct user web activity and detect web-based C2 or exfiltration channels
- Correlate proxy log sessions with PCAPs to confirm and extend findings

Lab 09: Wireless Network Forensics

- Analyze 802.11 frame captures in Wireshark
- Detect rogue APs, deauth attacks, evil twin attacks, and WPA cracking attempts
- Extract WPA handshakes and analyze weak or compromised wireless encryption

Lab 10: Malware & C2 Communication Analysis

- Identify common C2 protocols and beacon patterns in network traffic
- Analyze encoded and obfuscated C2 traffic (Base64, XOR, DGA)
- Carve and analyze malware payloads from reconstructed network streams

Lab 11: Advanced Packet Carving & Session Reconstruction

- Use tcpflow, foremost, and Wireshark to carve files from packet captures
- Reassemble fragmented TCP streams and incomplete file transfers
- Address encrypted traffic challenges in carving and reconstruction workflows

Lab 12: Network Timeline Construction & Correlation

- Build unified investigation timelines combining PCAP timestamps, Zeek logs, NetFlow, and host artifacts
- Use SOF-ELK and Timesketch for multi-source timeline visualization and analysis
- Identify temporal gaps caused by anti-forensics activity on the wire

Lab 13: Anti-Forensics & Evasion Techniques on the Network

- Detect timestomping in flow records, fragmented packets, and protocol tunneling
- Identify traffic obfuscation, fast-flux DNS, and encryption-based evasion
- Recognize living-off-the-land (LOLbins) network activity in enterprise traffic

Lab 14: Enterprise Triage with Network Tools

- Use RITA combined with Zeek and Suricata for remote network artifact collection and beacon detection
- Scale analysis across multiple PCAPs and distributed sensor logs

Lab 15: Cloud Network Forensics

- Analyze VPC Flow Logs from AWS, Azure NSG flows, and Google Cloud network logs
- Correlate cloud network telemetry with on-premises PCAP and NIDS data
- Address challenges of ephemeral cloud infrastructure and shared responsibility model