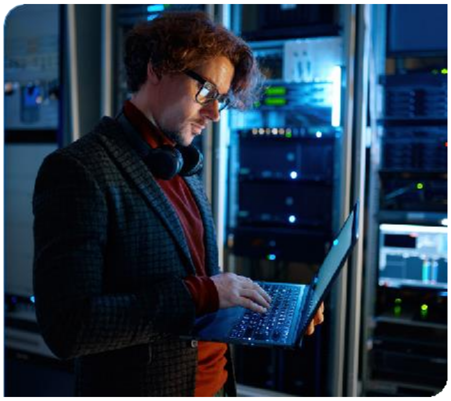
ThriveDX™

ThriveDX Digital Forensics and Incident Response

# TDXCS-1



ThriveDX Digital Forensics and Incident Response Course

Time Commitment	Skill Level	Format	Course Category
80 hours	Intermediate	Live Online, Instructor Led	Incident Response

Learn how to identify, respond to, and mitigate cyber threats with this in-depth course. Participants will delve into a variety of essential topics, from real incident response tactics and threat hunting to advanced techniques in malware analysis, credential theft prevention, and log analysis.

This advanced curriculum is for learners of diverse cybersecurity backgrounds, blending hands-on exercises with theoretical concepts to instill the skill set needed to succeed in the digital forensics field.

This course is designed for:

- System administrators
- Network engineers
- IT staff interested in cybersecurity and incident response
- Security analysts
- Incident responders
- Forensic investigators looking to deepen their expertise and stay current with industry

Prerequisites:

- Working experience with Windows and Linux operating systems
- Working experience with networking, infrastructure solutions, and cybersecurity principles
- Critical thinking ability for detailed examination of cyber threats and incidents

Relevant for the Following Work Roles:

- Security Analysts
- Incident Responders/Incident Response Analysts
- Forensic Investigators
- Digital Forensics Analyst
- Cyber Crime Investigator

Key Business Takeaways:

- **Enhanced Cybersecurity Posture:** Elevate organizational defenses with employees skilled in cutting-edge incident response and threat-hunting techniques
- **Reduced Incident Response Time:** Rapidly identify and mitigate threats, minimizing the impact on business operations.
- **Advanced Threat Detection and Analysis:** Equip professionals with the skills to detect and analyze sophisticated malware and advanced persistent threats (APTs)
- **Compliance and Risk Management:** Understand forensic methodologies and legal considerations for compliance with data protection and privacy laws, reducing legal and reputational risks.

Program Structure

Module 1

Introduction to Digital Forensics and Incident Response

- Overview of digital forensics
- Fundamentals of incident response
- Integration of real incident response tactics and preparation techniques
- Key procedures for proper intrusion response

Module 2

Identification and Scoping in Incident Response

- Incident response team's toolkit
- Techniques for detecting compromised systems
- Scoping of incidents in enterprise environments
- Identification of compromised systems and active/dormant malware

Module 3

Containment and Intelligence Development

- Restricting access and monitoring adversaries
- Forensic analysis and legal aspects of incident response
- Development of threat intelligence
- Building continuous incident response and threat-hunting capabilities

Module 4

Eradication, Remediation, and Recovery

- Steps for stopping and remedying incidents
- Recording and using threat intelligence for future incidents
- Avoiding ineffective incident response strategies

Module 5

Case Study | Credential Theft Prevention, Detection, and Mitigation

- Techniques for credential theft and countermeasures
- Analysis of common credential attacks and defenses

Module 6

Endpoint Detection and Response (EDR)

- EDR capabilities and integration with memory forensics
- YARA and other indicators of compromise
- Techniques for executable anomaly detection

Module 7

Advanced Evidence of Execution Detection

- Attacker tactics and process execution analysis
- Prefetch and registry examination
- Tools and techniques for memory acquisition and analysis
- Analysis of common anti-forensic techniques and countermeasures

Module 8

Lateral Movement and Log Analysis Techniques

- Lateral movement
- Log analysis for tracking and hunting movement
- Investigating PowerShell-based attacks

Module 9

Timeline Analysis and Volume Shadow Copy Examination

- Recovery of deleted or manipulated data
- Creation and analysis of filesystem timelines
- Super timeline creation and analysis techniques
- Volume shadow copy service and advanced NTFS filesystem tactics

Module 10

Capstone Project and Case Studies

- Real-world scenarios for applying learned techniques
- Case studies focusing on recent digital forensics challenges

Certification Readiness

All participants completing the course will receive a **ThriveDX Course Completion Certification**. Participants completing the final accreditation exam will receive a **ThriveDX Digital Forensics and Incident Response Practitioner Certification**.
This course also covers parts of the required knowledge expected for the GIAC Certified Forensic Examiner (GCFE) certification and the Computer Hacking Forensic Investigator (CHFI) certification.

Note: Specific materials and focus areas for the external certification exam are subject to change by the certifying organization and additional study and research may be necessary to meet certification requirements.

Embedded Labs and Challenges

The course includes our state-of-the-art proprietary cloud-based digital education platform, **TDX Arena**, in which real-life scenarios and advanced tech teaching meet in a gamified environment.