DARB. tech

CYBERSECURITY AND DIGITAL FORENSICS

PROGRAM BOOKLET

Supported By صندوق كفاءات المستقبل Future Skills Fund

Powered By استدامة للاستشارات Istidama Consulting

LevelUp Economy

Program Overview

Cybersecurity and digital forensics have moved from niche technical disciplines to critical national and enterprise capabilities. Organizations today face constant threats across networks, endpoints, cloud systems, and digital infrastructure, requiring professionals who can detect and respond to incidents, as well as investigate, document, and communicate findings in a legally defensible manner.

Modern cybersecurity roles demand more than theoretical knowledge or isolated tool usage.

Professionals must understand operating systems and networks, perform structured reconnaissance, analyze attacks, respond to incidents, preserve evidence, and produce clear technical reports aligned with industry frameworks such as MITRE ATT&CK.

To address this need, the program is designed with **two distinct technical tracks**: one focused on **Cybersecurity operations** and the other on **Digital Forensics & Incident Response**, enabling learners to develop deep, role-specific expertise.

Developed by LevelUp Economy and Istidama Consulting, the program is a 24-week practice-driven training program that prepares learners for real-world cybersecurity and digital forensics roles. The program emphasizes applied learning, professional discipline, and job-ready outputs over theoretical coverage or tool memorization.

The program integrates three strands: x

- A **Technical Track**: delivered through two specialized pathways: Cybersecurity and Digital Forensics & Incident Response (DFIR).
- **English for Technology**, focused on professional communication, technical reporting, and presentations within security contexts.
- A **Soft Skills Track** developing teamwork, analytical thinking, accountability, and workplace readiness in high-pressure technical environments.

The program follows a hybrid delivery model combining live online instruction, in-person labs, and scenario-based exercises. Learners progress is monitored continuously through structured labs, reports, and milestone-based assessments, culminating in a capstone project that simulates real-world cyber incidents.

Capstone-Driven Design

A defining feature of the program is its **capstone-driven design**.

Throughout the program, learners work togward a final capstone project in which they investigate, respond to, and document a realistic cybersecurity incident or forensic case. Capstone scenarios reflect real-world challenges such as network intrusions, phishing campaigns, compromised endpoints, malware infections, insider threats, and post-incident forensic investigations.

Learners operate under defined rules of engagement, apply structured workflows, preserve evidence and produce professional technical reports and presentations. Capstones may be completed by single-track teams or by mixed teams combining Cybersecurity and Digital Forensics learners, reflecting real-world collaboration between security operations and forensic response functions.

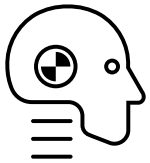
By the end of the program, learners graduate with a documented portfolio demonstrating their ability to operate effectively within professional cybersecurity and DFIR environments.

Program Highlights

The Cybersecurity and Digital Forensics program is designed around a deliberate set of features that distinguish it from fragmented, tool-centric, or purely theoretical trainings. These features work together to ensure depth, coherence, and real-world relevance across the entire learning journey.

Automated Pre-Testing and Baseline Mapping: All learners complete structured entry assessments covering technical foundations, analytical thinking, English communication, and professional readiness. These diagnostics establish baseline competencies and inform instructional support throughout the program.

Hybrid Delivery Model: combing synchronous online and in-person labs, workshops, and scenario-based exercises. This structure balances flexibility with accountability and ensures that complex technical aspects are reinforced through hands-on practice and guided collaboration.



Hands-On, Evidence-Safe Labs: Learners engage in controlled labs that emphasize structured workflows, documentation, validation, and ethical practice. Labs are designed to mirror real operational environments while maintaining safety and professional boundaries.

Programmatic Support via LMS: The program is delivered through a Learning Management System (LMS) that hosts are learning materials, assignments, communications, and assessments. Progress, attendance, and submissions are reviewed weekly to enable timely academic and technical support.

Employment & Career Support: The program includes structured **employment and career support** to help learners transition from training into professional opportunities. This includes networking events, exposure to industry practitioners, referrals to relevant opportunities, and guidance on professional positioning through portfolios, GitHub repositories, and LinkedIn profiles. Employment outcomes depend on individual performance and market conditions; however, the program actively supports learners in building connections and presenting their skills effectively to potential employers.

Funding Options. The program is supported by funding from the **Future Skills Fund (FSF)** for learners who meet specific eligibility criteria, in line with FSF policies. For applicants who are not eligible for FSF funding, self-paid participation is an option. All applicants go through the same admissions and assessment process, regardless of the funding mechanism.

Program Structure

The program is structured as an integrated learning pathway in which technical, language, and professional skills develop in parallel and reinforce one another throughout the program.

The program runs over

The program is run over 24 weeks and combines three coordinated tracks:

1. Soft Skills: Professional Practice & Workplace Readiness

The soft skills component focuses on the professional behaviors required to function effectively in team-based, high-pressure technical environments. Soft skills sessions are delivered as workshops as well as being embedded in the daily practice across technical and English assignments.

Learners develop competencies in:

- Teamwork and collaboration
- Analytical thinking and structured problem-solving
- Time management and accountability
- Professional conduct and communication
- Receiving, processing, and acting on feedback

2. English for Technology

Running alongside the technical training, **English for Technology** develops learners' ability to communicate effectively within professional cybersecurity and DFIR contexts. Language instruction is embedded in technical content and real security scenarios. Learners practice:

- Writing technical and incident reports
- Documenting findings clearly and objectively
- Delivering briefings and presentations
- Participating in structured reviews and discussions
- Communicating technical information to both technical and non-technical stakeholders

3. Technical Tracks

Program Structure

Cybersecurity and Digital Forensics are run as two tracks over 24 weeks and consist of three main phases:

1. Shared Foundations
2. Specialized Technical Tracks
3. Capstone & Graduation Phase

1. Shared Foundations (All Learners)

All learners begin with a common technical and professional foundation designed to ensure a consistent baseline across both technical tracks. The shared foundations include:

- Operating system fundamentals (Windows and Linux)
- Networking basics (TCP/IP, DNS, HTTP/S)
- Virtualization and safe lab environments
- Command-line fluency (Bash and Powershell)
- Python scripting foundations for automation and analysis
- Logging, timelines, and basic correlation concepts
- Security ethics, professional conduct, and rules of engagement
- Documentation standards and professional reporting

This phase ensures that all learners develop disciplined technical habits and responsible security practices before specialization.

2. Specialized Technical Tracks

Cybersecurity

Focus: Applied cybersecurity operations, controlled offensive techniques, detection-aware workflows, and structured incident reporting.

Learners in this track develop the ability to:

- Perform reconnaissance, scanning, and enumeration
- Identify and exploit common vulnerabilities in controlled environments
- Analyze attack surfaces and privilege escalation paths
- Understand Active Directory attack chains and mitigation strategies
- Deploy command-and-control frameworks with operational security awareness
- Align offensive actions with detection and defensive visibility
- Produce professional reports aligned with industry frameworks such as MITRE ATT&CK

Graduate Profile: Cybersecurity Professional -*Specialization in Cybersecurity Operations*

Digital Forensics & Incident Response (DFIR)

Focus: Evidence acquisition, forensic analysis, incident response, and legally defensible reporting.

Learners in this track develop the ability to:

- Apply chain-of-custody principles and forensic imaging best practices
- Analyze Windows, Linux, and macOS forensic artifacts
- Construct unified timelines from multiple data sources
- Perform memory, malware, and mobile forensic analysis
- Analyze cloud and virtualized environment artifacts
- Design and document incident response playbooks
- Produce defensible forensic reports suitable for legal and organizational review

Graduate Profile: Cybersecurity Professional -*Specialization in DFIR*

3. Integrated Design and Capstone Convergence

In the final phase of the program, all learning strands converge in the capstone project.

Learners apply technical expertise, professional communication, and teamwork to investigate and respond to a realistic cybersecurity incident or forensic case. Cybersecurity and DFIR learners may work together, reflecting real-world collaboration between security operations and forensic response teams.

The program concludes with capstone presentations and a graduation showcase, where learners present their work, reflect on their learning journey, and prepare for entry into the professional workforce.

Program Experience

16 core technical lectures
(online, synchronous)
with the Program Lead

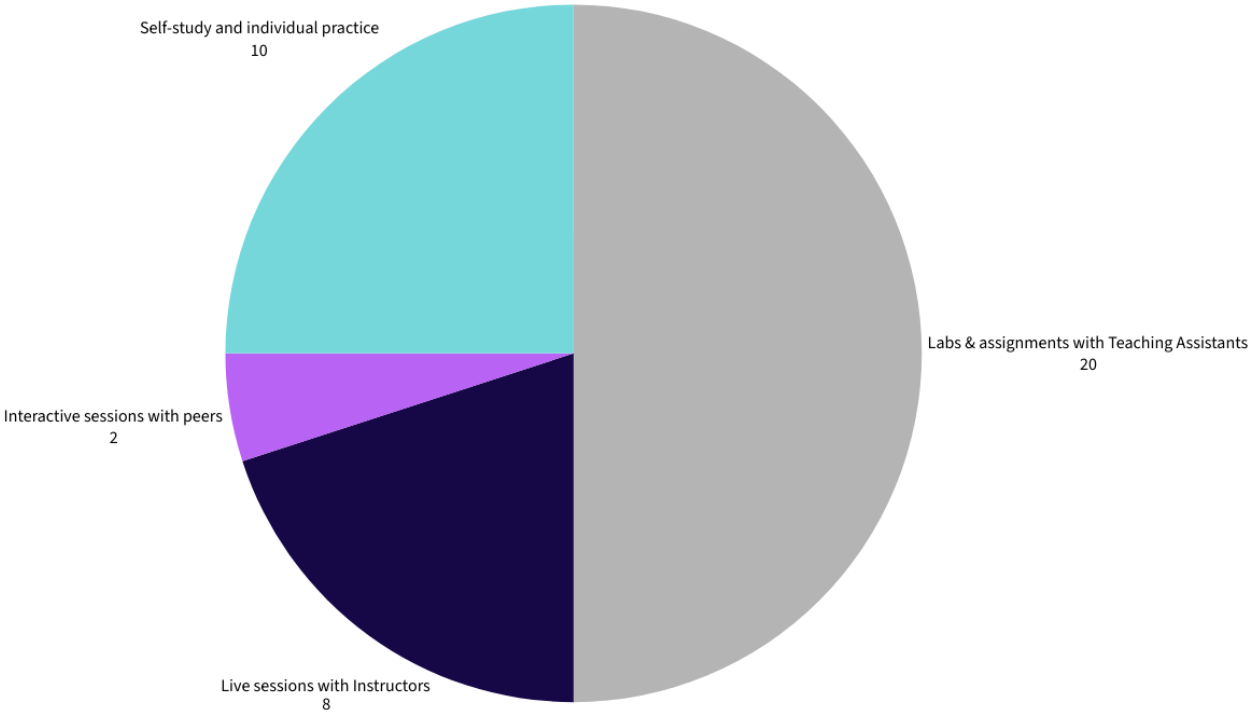
2 applied labs every week
(in-person)
with Technical Instructor

80 hours
(online)
English language learning

10 sessions
(in-person)
Soft Skills training

Sample Weekly Program Planner

Learners should expect to dedicate a minimum of 30-40 hours per week to the program.



Who is the Program For?

The Cybersecurity and Digital Forensics program is designed for motivated learners who are ready to commit to an intensive, applied learning experience in cybersecurity and digital forensics. This program is suited for:

Early-Career Graduates

In computer science, IT, engineering, or related technical fields

Professionals Seeking to Upskill or Pivot

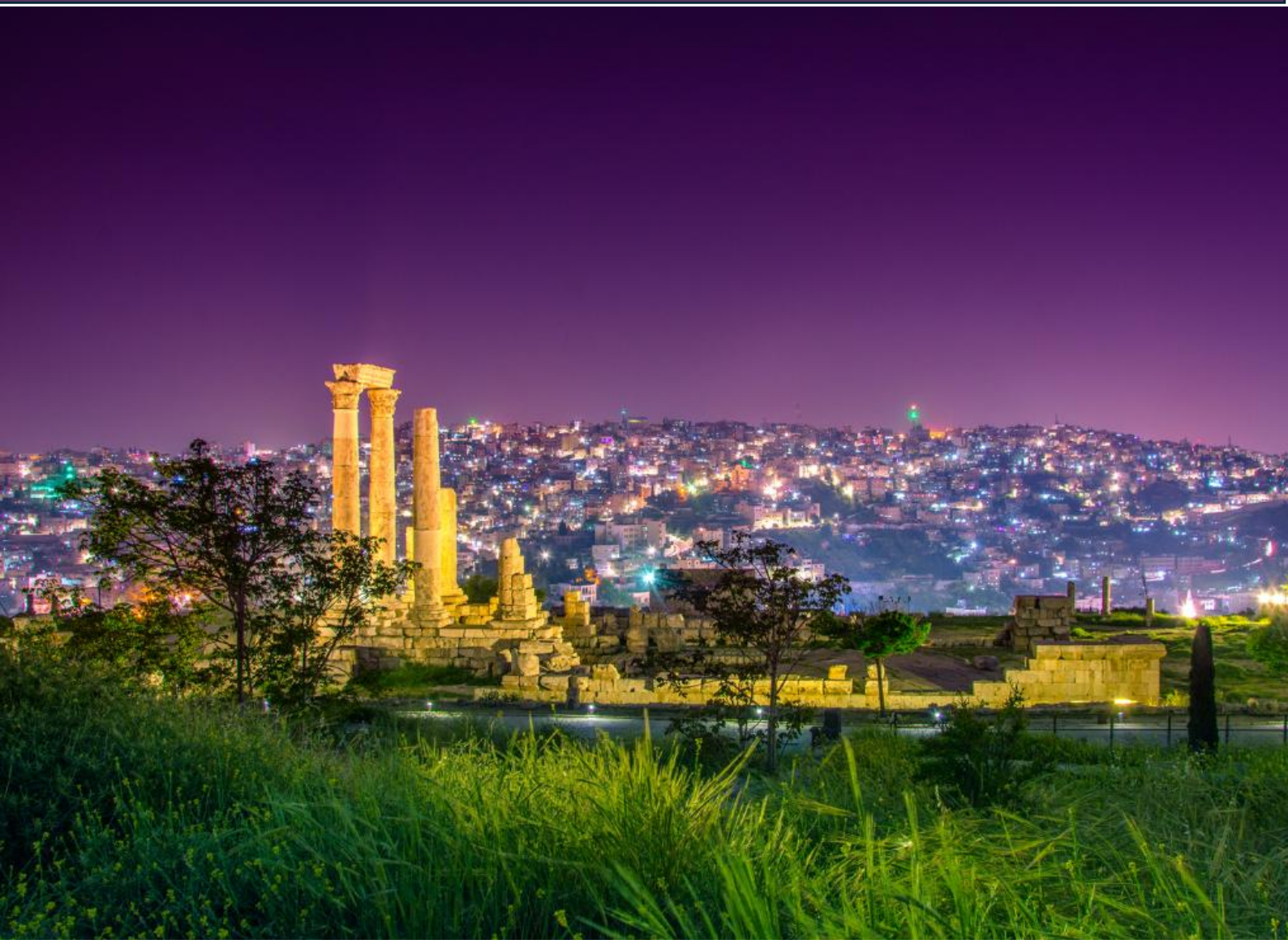
Into cybersecurity, SOC, or DFIR roles

Learners with Foundational Technical Experience

Who are comfortable with structured problem-solving and ready for advanced applied training.

Applicants are placed in one technical track during onboarding based on their interests, assessments results, and the decision of the education team.

CYBERSECURITY AND DIGITAL FORENSICS



You can apply for the program here:

APPLY

Connect with a program advisor:

CONNECT

Supported By صندوق كفاءات المستقبل Future Skills Fund

Powered By استدامة للاستشارات Istidama Consulting

LevelUp Economy