Training Course on Digital Forensics and Incident Response Workflow Automation with Low-Code/No-Code Platforms

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,100 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's hyper-connected world, cyber threats are escalating in sophistication and frequency, making robust **Digital Forensics and Incident Response (DFIR)** capabilities paramount for organizational resilience. Traditional DFIR processes are often manual, time-consuming, and resource-intensive, leading to delayed response times, increased financial implications, and potential data loss. This training course introduces a transformative approach by leveraging **Low-Code/No-Code (LCNC) platforms** to **automate DFIR workflows**, significantly enhancing efficiency, accuracy, and scalability in cybersecurity operations. Participants will gain practical skills to build customized automation solutions, bridging the critical gap between security expertise and rapid incident resolution.

Training Course on Digital Forensics and Incident Response Workflow Automation with Low-Code/No-Code Platforms empowers cybersecurity professionals to revolutionize their incident handling strategies. By integrating **workflow automation** with **digital forensics tools** and **incident response frameworks**, organizations can achieve accelerated threat detection, containment, eradication, and recovery. The focus on **LCNC development** democratizes automation, allowing security analysts and incident responders, even those with limited programming experience, to design and deploy powerful, tailored solutions. This course is essential for any organization seeking to bolster its **cybersecurity posture**, optimize **security operations center (SOC)** efficiency, and ensure **business continuity** in the face of evolving cyber threats.

Programme Curriculum

Training Course on Digital Forensics and Incident Response Workflow Automation with Low-Code/No-Code Platforms

Introduction

In today's hyper-connected world, cyber threats are escalating in sophistication and frequency, making robust **Digital Forensics and Incident Response (DFIR)** capabilities paramount for organizational resilience. Traditional DFIR processes are often manual, time-consuming, and resource-intensive, leading to delayed response times, increased financial implications, and potential data loss. This training course introduces a transformative approach by leveraging **Low-Code/No-Code (LCNC) platforms** to **automate DFIR workflows**, significantly enhancing efficiency, accuracy, and scalability in cybersecurity operations. Participants will gain practical skills to build customized automation solutions, bridging the critical gap between security expertise and rapid incident resolution.

Training Course on Digital Forensics and Incident Response Workflow Automation with Low-Code/No-Code Platforms empowers cybersecurity professionals to revolutionize their incident handling strategies. By integrating **workflow automation** with **digital forensics tools** and **incident response frameworks**, organizations can achieve accelerated threat detection, containment, eradication, and recovery. The focus on **LCNC development** democratizes automation, allowing security analysts and incident responders, even those with limited programming experience, to design and deploy powerful, tailored solutions. This course is essential for any organization seeking to bolster its **cybersecurity posture**, optimize **security operations center (SOC)** efficiency, and ensure **business continuity** in the face of evolving cyber threats.

Course Duration

5 days

Course Objectives

1. Comprehend core **digital forensics methodologies** and **incident response lifecycle** stages
2. Develop expertise in utilizing leading **low-code/no-code platforms** for **workflow automation design** and implementation.
3. Design and deploy automated scripts for **forensic data acquisition** from diverse sources like endpoints, networks, and cloud environments.
4. Implement **automated log correlation** and **SIEM integration** for rapid threat detection and alert enrichment.
5. Create automated playbooks for immediate **network isolation**, **endpoint quarantine**, and **malware eradication**.
6. Build and customize **automated incident response playbooks** to standardize actions and reduce manual intervention.
7. Ensure the integrity and **chain of custody** of digital evidence through automated hashing, logging, and secure storage.
8. Integrate **threat intelligence platforms** with DFIR workflows for automated indicator of compromise (IOC) lookups and enrichment.
9. Generate automated **incident reports** and **forensic dashboards** for clear communication and post-incident analysis.
10. Explore and implement **cloud security automation** techniques for incident response in AWS, Azure, and GCP environments.
11. Understand how to embed DFIR automation into **DevSecOps pipelines** for proactive security and continuous monitoring.
12. Explore the application of basic **AI and machine learning** capabilities within LCNC platforms to augment DFIR processes.

13. Empower participants to develop simple, custom **security applications** using LCNC principles to address unique organizational needs.

Organizational Benefits

- Significantly reduce the mean time to detect (MTTD) and mean time to respond (MTTR) to cyber incidents.
- Automate repetitive, labor-intensive tasks, freeing up valuable security analyst time for complex investigations.
- Minimize human error and ensure adherence to established DFIR protocols and best practices.
- Efficiently handle a growing volume of incidents without proportionally increasing headcount.
- Optimize resource allocation and potentially reduce the need for specialized, highly paid developers for certain automation tasks.
- Proactive and rapid response capabilities lead to better threat containment and prevention of widespread damage.
- Automated evidence collection and reporting simplify audit processes and regulatory compliance.
- Empower a broader range of security professionals to contribute to and implement automation solutions.

Target Audience

1. Security Analysts
2. Incident Responders
3. Forensic Investigators.
4. SOC Team Members.
5. IT Administrators/Managers
6. Cybersecurity Consultants solutions.
7. Risk Management Professionals
8. Aspiring Cybersecurity Professionals.

Course Outline

Module 1: Foundations of Digital Forensics and Incident Response (DFIR)

- Introduction to DFIR: Definitions, importance, and the NIST Incident Response Framework.
- Key principles of digital forensics: Volatility, chain of custody, evidence acquisition.
- Overview of incident response stages: Preparation, identification, containment, eradication, recovery, lessons learned.
- Legal and ethical considerations in DFIR: Data privacy, compliance, reporting requirements.
- **Case Study:** Analyzing a simulated phishing attack and the initial steps of evidence preservation.

Module 2: Introduction to Low-Code/No-Code (LCNC) Platforms for Security

- Understanding LCNC: Concepts, benefits, and common platforms.
- Comparing LCNC with traditional coding for security automation.
- Identifying suitable DFIR processes for LCNC automation.
- Basic LCNC platform interface and component familiarization.
- **Case Study:** Automating a simple security alert notification workflow using a drag-and-drop interface.

Module 3: Automating Initial Incident Triage and Identification

- Automated alert correlation and enrichment from SIEM/EDR solutions.
- Building workflows for initial data collection: User information, device details, process lists.
- Implementing automated checks for known IOCs and threat intelligence lookups.
- Automated categorization and prioritization of security incidents.
- **Case Study:** Creating an automated workflow to collect initial triage data for a suspicious login alert.

Module 4: Low-Code/No-Code for Forensic Data Acquisition and Preservation

- Automating forensic image acquisition from endpoints
- Developing workflows for memory dump collection and analysis.
- Automated collection of network traffic logs and DNS queries.
- Ensuring data integrity and chain of custody through automated hashing and metadata recording.
- **Case Study:** Designing an LCNC workflow to remotely acquire a full disk image and memory dump from a suspected compromised workstation.

Module 5: Workflow Automation for Incident Containment and Eradication

- Automated endpoint isolation from the network.
- Building workflows for blocking malicious IPs/domains at firewalls and proxies.
- Automated removal of malware and malicious processes.
- Implementing automated password resets for compromised accounts.
- **Case Study:** Automating the containment of a ransomware outbreak by isolating affected systems and blocking C2 server communication.

Module 6: Recovery and Post-Incident Automation

- Automated system restoration from clean backups.
- Developing workflows for vulnerability patching and hardening.
- Automated verification of system integrity post-recovery.
- Automating the generation of lessons learned reports and action item tracking.
- **Case Study:** Creating an automated post-incident cleanup routine, including patch deployment and system health checks after a successful eradication.

Module 7: Advanced DFIR Automation and Integration

- Integrating LCNC platforms with various security tools (SOAR, EDR, SIEM, TIP).
- Building complex, multi-stage DFIR playbooks using conditional logic and loops.
- Leveraging APIs for custom integrations with unsupported security solutions.
- Implementing automated communication and collaboration within DFIR teams.
- **Case Study:** Developing an end-to-end automated playbook for a detected malware infection, from initial alert to final reporting, integrating multiple security tools.

Module 8: Cloud DFIR Automation and Future Trends

- DFIR automation in cloud environments (AWS, Azure, GCP): specific tools and challenges.
- Automating incident response for serverless functions and containerized applications.
- Exploring the role of AI and Machine Learning in next-generation DFIR automation.
- Best practices for scaling LCNC DFIR solutions and continuous improvement.

- **Case Study:** Automating a cloud security incident response, such as detecting and remediating a misconfigured S3 bucket or an exposed API key.

Training Methodology

This course employs a **blended learning approach** to maximize participant engagement and knowledge retention.

- **Instructor-Led Sessions:** Interactive lectures and discussions to cover theoretical concepts and best practices.
- **Hands-on Labs:** Extensive practical exercises using industry-standard LCNC platforms and simulated DFIR scenarios. Participants will build actual automation workflows.
- **Real-World Case Studies:** Analysis of past cyber incidents and their application to automated DFIR solutions.
- **Live Demonstrations:** Walkthroughs of complex automation builds and integrations.
- **Group Activities & Discussions:** Collaborative problem-solving and sharing of experiences.
- **Q&A Sessions:** Dedicated time for addressing specific participant queries and challenges.
- **Capstone Project:** A culminating project where participants design and implement an automated DFIR workflow for a complex scenario.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
03 Aug 2026	07 Aug 2026	Online	$1,100
10 Aug 2026	14 Aug 2026	Online	$1,100
17 Aug 2026	21 Aug 2026	Online	$1,100
24 Aug 2026	28 Aug 2026	Online	$1,100
31 Aug 2026	04 Sep 2026	Online	$1,100
07 Sep 2026	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskills.com | Website: www.fineskills.com