Program Catalog: Applied Cybersecurity for the AI Era (APCYBER)

SOC Operations, Incident Response & Digital Forensics

Program Overview

- **Program Name:** Applied Cybersecurity for the AI Era: SOC Operations, Incident Response & Digital Forensics
- **Program Code:** APCYBER
- **Program Length:** 28 Weeks (7 Months)
- **Total Contact Hours:** 336 Hours
- **Total Credit Hours:** 13.4 Credits
- **Delivery Method:** In-person Live Instructor-Led, Virtual Live Instructor-Led, or 1-on-1 Personalized Mentorship

Admissions Requirements

To ensure student success in this advanced technical program, applicants must meet the following criteria:

- High school diploma or GED equivalent.
- Minimum age of 18 years (Applicants under 18 require parental/legal guardian consent).
- Demonstrated basic computer literacy and foundational networking knowledge.
- Basic understanding of operating system concepts (Windows and Linux file structures).
- Successful completion of the NVIT Admissions Interview.

NVIT
IT Solutions, Consulting, & Training

Program Description

The **Applied Cybersecurity for the AI Era (APCYBER)** program is a specialized "Zero-to-Hero" vocational track designed to transform individuals into high-performance security professionals. Unlike traditional cybersecurity programs that focus solely on legacy defenses, this curriculum integrates **Artificial Intelligence (AI) and Machine Learning (ML)** into every stage of the cyber defense lifecycle.

Students begin with the **Digital Cybersecurity Literacy** foundation on the NVIT Learning platform and progress through a rigorous four-phase training structure. The program culminates in advanced **SOC Operations**, where students learn to defend against AI-driven threats, automate incident response, and conduct digital forensics.

Graduates will be able to:

- **Operationalize AI in Defense:** Monitor and analyze security events using AI-enhanced SIEM platforms (Splunk, Sentinel, QRadar).
- **Automate Threat Hunting:** Use Python and Generative AI APIs to write scripts that detect anomalies and parse logs faster than humanly possible.
- **Execute Offensive Maneuvers:** Conduct ethical hacking and penetration testing using Kali Linux to identify vulnerabilities before adversaries do.
- **Secure Cloud Infrastructure:** Architect and defend cloud-native environments (AWS/Azure) against identity theft and data breaches.
- **Manage Crisis Situations:** Lead incident response efforts using the NIST framework, containing threats and eradicating malware.

USA
NVIT Global Headquarters
6475 Preston Road, Suite 201
Frisco, TX 75034, USA
Phone: +1 (214) 407-7229
Email: info@nvit.tech

WEB
www.NVIT.tech

Career Pathways & Compensation

- **SOC Analyst (Tier 1) - AI Enhanced:** $58,000 - $75,000
- **Incident Response Specialist - AI Enhanced:** $85,000 - $110,000
- **Digital Forensics Analyst - AI Powered:** $90,000 - $115,000
- **AI/ML Security Engineer:** $95,000 - $140,000
- **Cloud Security Engineer - AI Native:** $95,000 - $125,000
- **GenAI Security Specialist:** $100,000 - $130,000

Instructional Components Breakdown

The program is divided into three primary learning modalities to ensure skill retention.

Instructional Component	Description	Hours
Live Lectures	Theory, concept introduction, and instructor demonstrations.	**63**
Labs & Projects	Hands-on practice in virtual environments	**189**
Capstone & OJT	Simulated real-world scenarios, reporting, and final defense exams.	**84**
TOTAL		**336**

Detailed Course Outline

Subject Code	Subject Title	Contact Hours	Credit Hours
APCYBER 100	Digital Cybersecurity Literacy	18	0.7
APCYBER 101	Cybersecurity Fundamentals	30	1.2
APCYBER 102	Network Security Fundamentals	36	1.5
APCYBER 103	Python Programming	36	1.5
APCYBER 201	Cybersecurity Linux Administration	36	1.5
APCYBER 202	Cryptography: Principles and Applications	18	0.7
APCYBER 203	Ethical Hacking and Penetration Testing	36	1.5

APCYBER 301	Cloud Security	36	1.5
APCYBER 302	Security Operations and Incident Response	54	2.1
APCYBER 401	Generative AI	36	1.5
TOTAL		**336**	**13.7**

Subject Descriptions & Learning Objectives

Phase 0: The Warm-Up

APCYBER 100: Digital Cybersecurity Literacy

18 Contact Hours | 0.7 Credits

This introductory module serves as the essential launchpad for your technical journey, utilizing the **Codio platform** to build a comprehensive digital skillset through a security-focused lens. The curriculum is built upon four critical pillars:

- **Device Navigation & Internet Basics:** Mastering the technical foundations and infrastructure of the digital world.
- **Digital Citizenship:** Learning to manage online identity and professional reputation with an ethical and secure framework.

- **Online Privacy & Security:** Moving beyond the basics to protect sensitive data and cultivate advanced cybersecurity awareness.
- **Critical Thinking:** Developing the analytical skills to identify social engineering, evaluate credibility, and detect bias in digital information.

Hands-On Foundations Using **Virtual Machine (VM) environments**, you will complete hands-on labs in every section. This ensures you are technically, ethically, and strategically prepared for the specialized cybersecurity challenges that follow in the program.

Learning Objectives: Upon successful completion of this module, students will be equipped to:

- **Master Virtualized Environments:** Confidently navigate and operate within virtualized operating systems and cloud-based Integrated Development Environments (IDEs).
- **Govern Digital Presence:** Strategically manage online identity, professional reputation, and the long-term impact of their digital footprint.
- **Execute Critical Information Analysis:** Systematically evaluate digital content for source credibility, inherent bias, and underlying security risks or social engineering tactics.

Technical Ecosystem (Tools)

To simulate real-world cybersecurity scenarios, students will gain proficiency in the following:

- **NVIT Learning Platform:** The primary hub for curriculum delivery and progress tracking.
- **Virtual Machines (VMs):** Isolated environments used to safely practice technical skills and OS navigation.
- **Modern Web Browsers:** Tools for internet navigation, security configuration, and digital research.

Phase 1: The Foundation

APCYBER 101 – Cybersecurity Fundamentals

(30 Contact Hours | 1.2 Credits)

An immersion into the history, theory, and language of cybersecurity. Students explore the Confidentiality, Integrity, and Availability (CIA) triad and the modern threat landscape.

- **Learning Objectives:**
  - Analyze the contemporary threat landscape (Malware, Phishing, Social Engineering).
  - Apply risk management frameworks (NIST RMF, ISO 27001).
  - Understand Access Control models (DAC, MAC, RBAC).
- **Prerequisite:** APCYBER 100

APCYBER 102 – Network Security Fundamentals

(36 Contact Hours | 1.5 Credits)

The backbone of the SOC. This course covers TCP/IP, the OSI model, and packet analysis. Students learn to secure the network edge.

- **Learning Objectives:**
  - Analyze network traffic for security threats using packet sniffers.
  - Configure firewalls, VPNs, and IDS/IPS systems.
  - Implement network segmentation and secure wireless protocols.
- **Tools:** Wireshark, pfSense, Snort, Suricata, Nmap.

APCYBER 103 – Python Programming

(36 Contact Hours | 1.5 Credits)

Students transition from users to developers, learning Python specifically for security automation and data analysis.

- **Learning Objectives:**
  - Write scripts to automate file handling and log parsing.
  - Develop tools to interact with security APIs and web scrapers.
  - Create basic port scanners and automation bots.
- **Tools:** Python 3, Jupyter Notebooks, Requests Library, Socket Library.

Phase 2: The Tools & The Attack

APCYBER 201 – Cybersecurity Linux Administration

(36 Contact Hours | 1.5 Credits)

Mastery of the Command Line Interface (CLI). Students learn to manage and secure Linux servers, the industry standard for security tools.

- **Learning Objectives:**

- Manage users, permissions, and file systems via bash.
- Secure Linux servers using SSH hardening and IPTables.
- Automate system administration tasks with bash scripting.

- **Tools:** Ubuntu, CentOS, Bash, SSH, VIM.

APCYBER 202 – Cryptography: Principles and Applications

(18 Contact Hours | 0.7 Credits)

A deep dive into the math that protects data. Students learn how encryption works and how it is implemented in the real world.

- **Learning Objectives:**
  - Differentiate between Symmetric and Asymmetric encryption.
  - Implement Hashing, Digital Signatures, and PKI certificates.
  - Analyze SSL/TLS handshakes and troubleshoot certificate errors.
- **Tools:** OpenSSL, GPG, Hashcat.

APCYBER 203 – Ethical Hacking and Penetration Testing

(36 Contact Hours | 1.5 Credits)

Students adopt the offensive mindset ("Red Teaming") to find and fix vulnerabilities before attackers exploit them.

- **Learning Objectives:**
  - Conduct reconnaissance and vulnerability scanning.
  - Execute exploitation attacks (SQL Injection, XSS, Buffer Overflow).
  - Perform post-exploitation and privilege escalation.
- **Tools:** Kali Linux, Metasploit Framework, Burp Suite, Nessus.

Phase 3: The Defense & The Future

APCYBER 301 – Cloud Security

(36 Contact Hours | 1.5 Credits)

Focuses on securing virtualized infrastructure in AWS and Azure, addressing the "Shared Responsibility Model."

- **Learning Objectives:**
  - Configure Identity and Access Management (IAM) policies.
  - Secure S3 buckets and cloud storage against data leaks.
  - Audit cloud environments for compliance (GDPR/HIPAA).
- **Tools:** AWS Console, Azure Portal, CloudWatch.

APCYBER 302 – Security Operations and Incident Response

(54 Contact Hours | 2.1 Credits)

The Capstone Course. Students synthesize all previous skills to operate as a SOC Analyst, detecting and responding to active threats.

- **Learning Objectives:**
  - Monitor SIEM logs to detect behavioral anomalies.
  - Execute the NIST Incident Response lifecycle (Preparation to Recovery).
  - Conduct Digital Forensics to preserve evidence and analyze malware artifacts.
- **Tools:** Splunk, IBM QRadar, TheHive, Autopsy, Volatility.

APCYBER 401 – Generative AI

(36 Contact Hours | 1.5 Credits)

The cutting edge of cyber defense. Students learn to use AI as a force multiplier for security operations.

- **Learning Objectives:**
  - Leverage LLMs to automate incident report writing and code generation.
  - Identify AI-generated phishing and "Deepfake" social engineering.
  - Integrate AI APIs into Python scripts for automated threat analysis.
- **Tools:** OpenAI API, LangChain, AI-enhanced Security Plugins.

Tuition and Fees

Fee Type	Cost
Registration Fee	$50.00
Books and Supplies (estimated)	$500.00
Background Check (if applicable)	$150.00
Tuition (In-person Live Instruction)	**$12,199.00**
Tuition (Virtual Live Instruction)	**$12,199.00**
Tuition (1-on-1 Virtual Mentorship)	**$13,199.00**

Note: *Registration Fee, Books/Supplies, and Background Check are included in the total program cost but apply separately for single-subject enrollment.*

Cost per Single Subject

Costs are calculated based on the standardized hourly tuition rate of approx. ***$36.31/hour****.*

Subject Code	Subject Title	Contact Hours	Standard Tuition (In-Person & Virtual)
APCYBER 100	Digital Cybersecurity Literacy	18	$653.58
APCYBER 101	Cybersecurity Fundamentals	30	$1,089.30
APCYBER 102	Network Security Fundamentals	36	$1,307.16
APCYBER 103	Python Programming	36	$1,307.16

USA
NVIT Global Headquarters
6475 Preston Road, Suite 201
Frisco, TX 75034, USA
Phone: +1 (214) 407-7229
Email: info@nvit.tech

WEB
www.NVIT.tech

APCYBER 201	Cybersecurity Linux Administration	36	$1,307.16
APCYBER 202	Cryptography	18	$653.58
APCYBER 203	Ethical Hacking & Pen Testing	36	$1,307.16
APCYBER 301	Cloud Security	36	$1,307.16
APCYBER 302	Security Ops & Incident Response	54	$1,960.74
APCYBER 401	Generative AI and Agentic AI	36	$1,307.16
APCYBER 402	Capstone Project and Industry Simulation		

Class Schedule

- **Classes Begin: May 26, 2025** (Rolling admissions for Virtual Mentorship).
- **Day Shift:** Mon–Wed, 9:30 AM – 12:30 PM

- **Afternoon Shift:** Mon–Wed, 1:30 PM – 4:30 PM
- **Evening Shift:** Mon–Wed, 6:00 PM – 9:00 PM
- **Weekend Shift:** Thu–Sat (Morning, Afternoon, and Evening slots available).

School Closure Dates:

New Year's Day, Martin Luther King Day, Presidents' Day, Good Friday, Memorial Day, Independence Day, LBJ's Birthday, Labor Day, Veteran's Day, Thanksgiving Day, Day After Thanksgiving, Christmas Eve, Christmas Day, Day After Christmas.