Applied Cybersecurity for the AI Era

SOC Operations, Incident Response & Digital Forensics

From Zero to Cyber Hero in 7 months — a comprehensive masterclass in AI-enhanced threat defense, SIEM operations, and digital forensics.

28	336	56%	5:1	2
WEEKS	CONTACT HOURS	HANDS-ON LABS	LAB RATIO	EXAM VOUCHERS INCL.

WHY CYBERSECURITY? WHY NOW?

32% Projected growth in U.S. cybersecurity jobs 2022–2032 — more than 10× the average for all occupations (U.S. BLS).

470K Open cybersecurity positions across the United States (CompTIA, 2025) — nearly 4 million vacant globally.

$146K Top of the entry-level salary range in Dallas–Fort Worth ($80,000–$146,429); Texas medians run $72K–$125K.

AI AI will not replace security jobs — it will transform them. Professionals who master AI-augmented defense will lead the field.

THE PROGRAM AT A GLANCE

- **28 weeks | 336 contact hours | 13.4 credits** — a complete Zero-to-Hero vocational track.
- **56% hands-on labs** in a 24/7 simulated virtual SOC with real-time threat feeds, plus 25% capstone & on-the-job simulation.
- **Small classes:** 10:1 lectures, 5:1 labs, taught live by practicing industry professionals.
- **Three ways to learn:** In-Person (Frisco, TX), Virtual Live, or 1-on-1 Personalized Mentorship.
- **No degree or prior experience required** — high school diploma/GED plus drive.

CompTIA Security+ & CySA+ EXAM VOUCHERS INCLUDED

YOUR 28-WEEK ROADMAP

WEEKS 1–10
FOUNDATIONS
Digital cybersecurity literacy, security fundamentals, network security, and Python programming for security automation.

WEEKS 11–17
TOOLS & THE ATTACK
Linux administration, cryptography, and ethical hacking & penetration testing with Kali Linux and Metasploit.

WEEKS 18–24
SIEM & DEFENSE
Cloud security (AWS/Azure/GCP), SOC operations, incident response, and digital forensics with Splunk, Sentinel & QRadar.

WEEKS 25–28
AI & CAPSTONE
Generative & Agentic AI for cyber defense, capstone industry simulation, professional portfolio, and career preparation.

TOOLS YOU WILL MASTER

Splunk Enterprise Security • Microsoft Sentinel • IBM QRadar • Wireshark • Kali Linux • Metasploit • Burp Suite • Nessus • pfSense • Snort/Suricata • EnCase • FTK • Autopsy • Volatility • TheHive • MITRE ATT&CK • AWS / Azure / GCP Security Suites • Python • OpenAI API & LangChain

+1 (214) 407-7229 · info@nvit.tech · www.NVIT.tech

CAREERS & SALARIES THIS PROGRAM PREPARES YOU FOR

ROLE	LEVEL	SALARY RANGE
SOC Analyst (Tier 1) – AI Enhanced	Entry	**$58K – $75K**
AI-Powered Cybersecurity Analyst	Entry	**$70K – $90K**
Incident Response Specialist – AI Enhanced	Intermediate	**$85K – $110K**
Digital Forensics Analyst – AI Powered	Intermediate	**$90K – $115K**
Cloud Security Engineer – AI Native	Intermediate	**$95K – $125K**
AI/ML Security Engineer	Advanced	**$95K – $140K**
GenAI Security Specialist	Advanced	**$100K – $130K**

LEARN FROM INDUSTRY PRACTITIONERS

Sudha Malluru

LEAD INSTRUCTOR · CYBERSECURITY ENGINEERING & SOC OPERATIONS

12+ years securing Tier-1 global banks (Goldman Sachs, HSBC). Splunk SIEM management, Zero Trust architecture, automated incident response in Azure Sentinel & AWS Security Hub, threat hunting with MITRE ATT&CK, and enterprise AI/ML security aligned with NIST AI RMF.

CISSP · CISA · Azure Security Engineer Associate

Ola Ayeni

INSTRUCTOR & CURRICULUM VALIDATOR · GRC & AI SYSTEMS MANAGEMENT

Two decades across enterprise network & datacenter engineering, federal policy and compliance (NOAA), and AI governance. U.S. Dept. of State TechWomen Fellow at Symantec; translates NIST CSF 2.0, ISO 27001, and NIST AI RMF into real-world practice.

CISA · CISM · CRISC · AAISM (First Global Cohort)

TUITION & SCHEDULES

$8,500	$8,500	$8,500
IN-PERSON LIVE	**VIRTUAL LIVE**	**1-ON-1 MENTORSHIP**
Frisco, TX campus	Instructor-led online	Rolling admissions

Flexible shifts: Day, Afternoon & Evening (Mon–Wed) and Weekend (Thu–Sat) options. **Fall 2026 cohort: Orientation & first day of class Monday, August 3, 2026; graduation February 9, 2027. All-inclusive $8,500 total** — covers tuition, books & materials, registration, background check, and CompTIA Security+ & CySA+ exam vouchers · Single-subject enrollment available (~$21.45/hr). **WIOA / CareerSource funding accepted** — eligible students may qualify for full Individual Training Account (ITA) coverage.

CERTIFICATIONS YOU WILL BE PREPARED FOR

CompTIA Security+ & CySA+ (vouchers included) · CompTIA Network+ · CEH · GCIH · GCFA · GSEC · CISSP (Associate) · AWS / Azure / GCP cloud security certifications · CompTIA AI+ — plus an NVIT Certificate of Completion, a professional portfolio, and dedicated job placement support with resume & interview preparation.

Enroll Today — Ready for the AI Era?

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

APPLY NOW → www.NVIT.tech

PROGRAM CATALOG

Applied Cybersecurity for the AI Era

SOC Operations, Incident Response & Digital Forensics

Program Code: APCYBER

A 28-Week Comprehensive Masterclass in AI-Enhanced Threat Defense, SIEM Operations, and Digital Forensics

28 Weeks | 336 Contact Hours | 13.4 Credit Hours

In-Person Live • Virtual Live • 1-on-1 Personalized Mentorship

Fall 2026 Cohort: August 3, 2026 – February 9, 2027 | Orientation: Monday, August 3, 2026

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

1. Program Overview

Attribute	Detail
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
Student-to-Instructor Ratio	Lectures 10:1 | Labs 5:1
Credential Awarded	NVIT Certificate of Completion — Applied Cybersecurity for the AI Era

Mission & Program Objectives

The mission of the APCYBER program is to prepare students for entry-level to intermediate cybersecurity roles with hands-on experience in Security Operations Center (SOC) operations, incident response, digital forensics, and compliance management, directly addressing the critical skills shortage in the cybersecurity industry.

Course Objectives (CO):

- [CO1] Develop comprehensive knowledge of cybersecurity fundamentals, the modern threat landscape, and defense strategies.
- [CO2] Master SOC operations including SIEM management, threat detection, and security monitoring.
- [CO3] Acquire incident response and digital forensics skills following industry frameworks (NIST, NICE).
- [CO4] Understand compliance requirements and regulatory frameworks (GDPR, HIPAA, SOX, PCI-DSS).
- [CO5] Gain practical experience with industry-standard cybersecurity tools and technologies, enhanced by AI/ML.

Course Learning Outcomes (CLO):

- [CLO1] Demonstrate proficiency in cybersecurity fundamentals and risk management principles.
- [CLO2] Operate SIEM platforms and perform threat detection and analysis.
- [CLO3] Execute incident response procedures and conduct digital forensics investigations.
- [CLO4] Implement compliance controls and security frameworks.
- [CLO5] Apply ethical hacking and penetration testing methodologies.
- [CLO6] Design and implement cloud security solutions across AWS, Azure, and GCP.
- [CLO7] Integrate AI/ML technologies for enhanced cybersecurity operations.

2. 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 and a Capstone industry simulation, 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 Enterprise Security, Microsoft Sentinel, IBM 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/GCP) against identity theft and data breaches.
- **Manage Crisis Situations:** Lead incident response efforts using the NIST framework, containing threats and eradicating malware.
- **Conduct Digital Forensics:** Preserve evidence, maintain chain of custody, and analyze malware artifacts using AI-assisted forensic platforms.

Why This Program — The Market Opportunity

The U.S. Bureau of Labor Statistics projects a 32% increase in cybersecurity jobs from 2022 to 2032 — more than ten times the average growth rate for all occupations. Nearly 470,000 cybersecurity job openings exist in the United States (CompTIA, 2025), with over 225,000 skilled professionals needed as of Q2 2024 and nearly 4 million positions vacant globally.

Texas is one of the strongest cybersecurity markets in the nation. Median cybersecurity salaries in Texas range from $72,490 to $124,970, and the Dallas–Fort Worth market — NVIT's home region — offers $80,000 to $146,429 for entry-level positions. Employers consistently demand the exact skills this program teaches: SIEM operations (Splunk, Sentinel, QRadar), AI-enhanced threat detection, incident response, cloud security, Python scripting, and compliance frameworks.

Industry analysts agree: AI will not replace cybersecurity jobs, but it will transform them. Professionals who master AI-augmented security operations will lead the field. APCYBER is purpose-built for this AI Era.

3. 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 (TCP/IP, DNS, DHCP).
- Basic understanding of operating system concepts (Windows and Linux file structures).
- Successful completion of the NVIT Admissions Interview and technical aptitude assessment.
- Background check (required for certain career paths).

Basic programming knowledge (Python preferred) is helpful but not required.

4. Career Pathways & Compensation

The program prepares graduates for high-demand roles across the cybersecurity career ladder, with salary ranges validated against 2024–2025 Texas and national market research.

Career Stage	Role	Salary Range (USD)
Entry-Level (0–2 yrs)	SOC Analyst (Tier 1) – AI	$58,000 – $75,000

	Enhanced	
Entry-Level (0–2 yrs)	AI-Powered Cybersecurity Analyst	$70,000 – $90,000
Entry-Level (0–2 yrs)	IT Security Specialist	$60,000 – $80,000
Entry-Level (0–2 yrs)	Compliance Analyst	$55,000 – $75,000
Intermediate (2–5 yrs)	Incident Response Specialist – AI Enhanced	$85,000 – $110,000
Intermediate (2–5 yrs)	Digital Forensics Analyst – AI Powered	$90,000 – $115,000
Intermediate (2–5 yrs)	Cloud Security Engineer – AI Native	$95,000 – $125,000
Advanced (5+ yrs)	AI/ML Security Engineer	$95,000 – $140,000
Advanced (5+ yrs)	GenAI Security Specialist	$100,000 – $130,000
Advanced (5+ yrs)	AI Security Consultant	$120,000 – $160,000

5. Instructional Components Breakdown

The program is divided into three primary learning modalities to ensure skill retention. More than half of all program time is dedicated to hands-on labs and projects.

Instructional Component	Description	Hours	Share
Live Lectures (LIT)	Theory, concept introduction, and instructor demonstrations (2.25 hrs/week).	63	18.75%
Labs & Projects (LLP)	Hands-on practice in virtual environments (6.75 hrs/week).	189	56.25%
Capstone (CAP) & OJT	Simulated real-world scenarios, reporting, and final defense exams	84	25%

	(42 hrs CAP + 42 hrs OJT).		
TOTAL		**336**	**100%**

Learning modalities include interactive lectures with real-world case studies, hands-on labs with industry-standard tools, team-based and individual cybersecurity challenges, a 24/7 simulated virtual SOC environment with real-time threat feeds, and practical assessments aligned to certification preparation.

6. Detailed Course Outline

Subject Code	Subject Title	Weeks	Contact Hours	Credit Hours
APCYBER 100	Digital Cybersecurity Literacy	1–2	18	0.7
APCYBER 101	Cybersecurity Fundamentals	2–4	30	1.2
APCYBER 102	Network Security Fundamentals	5–7	36	1.5
APCYBER 103	Python Programming for Security	8–10	36	1.5
APCYBER 201	Cybersecurity Linux Administration	11–13	36	1.5
APCYBER 202	Cryptography: Principles and Applications	14	18	0.7
APCYBER 203	Ethical Hacking and Penetration Testing	15–17	36	1.4
APCYBER 301	Cloud Security	18–20	36	1.4
APCYBER 302	Security Operations and	21–24	54	2.1

	Incident Response			
APCYBER 401	Generative AI and Agentic AI for Cyber Defense	25–26	24	0.9
APCYBER 402	Capstone Project and Industry Simulation	27–28	12	0.5
TOTAL		**28**	**336**	**13.4**

7. Subject Descriptions & Learning Objectives

Phase 0: The Warm-Up

APCYBER 100 — Digital Cybersecurity Literacy

18 Contact Hours | 0.7 Credits | Prerequisite: None

This introductory module serves as the essential launchpad for the technical journey, utilizing the Codio platform to build a comprehensive digital skillset through a security-focused lens. The curriculum rests on four pillars: Device Navigation & Internet Basics, Digital Citizenship, Online Privacy & Security, and Critical Thinking. Using Virtual Machine (VM) environments, students complete hands-on labs in every section, ensuring they are technically, ethically, and strategically prepared for the specialized cybersecurity challenges that follow.

Learning Objectives:

- Master virtualized environments: confidently navigate and operate within virtualized operating systems and cloud-based IDEs.
- Govern digital presence: strategically manage online identity, professional reputation, and long-term digital footprint.
- Execute critical information analysis: systematically evaluate digital content for source credibility, bias, and social engineering tactics.

Tools: NVIT Learning Platform, Virtual Machines (VMs), modern web browsers.

Grading: Laboratory Exercises 50% | Module Assessments 35% | Class Participation 15%.

Phase 1: The Foundation

APCYBER 101 — Cybersecurity Fundamentals

30 Contact Hours | 1.2 Credits | Prerequisite: APCYBER 100

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

Learning Objectives:

- Analyze the contemporary threat landscape (malware, phishing, social engineering, AI-generated attacks).

- Apply risk management frameworks (NIST RMF, ISO 27001) with AI-assisted continuous risk assessment.
- Understand access control models (DAC, MAC, RBAC) and AI-powered incident classification.

Tools: NIST RMF templates, Nessus, OpenVAS, risk assessment software, AI-enhanced threat intelligence platforms.

Grading: Laboratory Exercises 40% | Risk Assessment Project 35% | Class Participation 15% | Final Portfolio 10%.

APCYBER 102 — Network Security Fundamentals

36 Contact Hours | 1.5 Credits | Prerequisite: APCYBER 101

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

Learning Objectives:

- Analyze network traffic for security threats using packet sniffers.
- Configure firewalls, VPNs, and IDS/IPS systems with machine learning capabilities.
- Implement network segmentation and secure wireless protocols with AI-powered threat detection.

Tools: Wireshark, pfSense, Snort, Suricata, Nmap, AI-enhanced network monitoring tools.

Grading: Laboratory Exercises 45% | Network Security Projects 30% | Technical Documentation 15% | Class Participation 10%.

APCYBER 103 — Python Programming for Security

36 Contact Hours | 1.5 Credits | Prerequisite: APCYBER 102

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.

Grading: Laboratory Exercises 45% | Scripting Projects 35% | Code Documentation 10% | Class Participation 10%.

Phase 2: The Tools & The Attack

APCYBER 201 — Cybersecurity Linux Administration

36 Contact Hours | 1.5 Credits | Prerequisite: APCYBER 103

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

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.

Grading: Laboratory Exercises 45% | Administration Projects 35% | Technical Documentation 10% | Class Participation 10%.

APCYBER 202 — Cryptography: Principles and Applications

18 Contact Hours | 0.7 Credits | Prerequisite: APCYBER 201

A deep dive into the mathematics that protect data. Students learn how encryption works, how it is implemented in the real world, and how hashing preserves forensic chain of custody.

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.

Grading: Laboratory Exercises 45% | Applied Cryptography Project 35% | Quizzes 10% | Class Participation 10%.

APCYBER 203 — Ethical Hacking and Penetration Testing

36 Contact Hours | 1.4 Credits | Prerequisite: APCYBER 202

Students adopt the offensive mindset ("Red Teaming") to find and fix vulnerabilities before attackers exploit them, augmented with AI-enhanced testing methodologies and automated vulnerability assessment.

Learning Objectives:

- Conduct reconnaissance and vulnerability scanning.
- Execute exploitation attacks (SQL Injection, XSS, Buffer Overflow).
- Perform post-exploitation, privilege escalation, and professional penetration test reporting.

Tools: Kali Linux, Metasploit Framework, Burp Suite, Nessus, AI-enhanced penetration testing tools.

Grading: Laboratory Exercises 35% | Security Assessment Projects 50% | Reporting Quality 10% | Class Participation 5%.

Phase 3: The Defense & The Future

APCYBER 301 — Cloud Security

36 Contact Hours | 1.4 Credits | Prerequisite: APCYBER 203

Focuses on securing virtualized infrastructure in AWS, Azure, and GCP, addressing the "Shared Responsibility Model" and cloud-native SIEM operations.

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) and operate cloud-native security services.

Tools: AWS Console (Security Hub, GuardDuty, CloudTrail), Azure Portal (Security Center, Sentinel, Key Vault), GCP Security Command Center, CloudWatch.

Grading: Laboratory Exercises 40% | Cloud Security Projects 35% | Compliance Audit Report 15% | Class Participation 10%.

APCYBER 302 — Security Operations and Incident Response

54 Contact Hours | 2.1 Credits | Prerequisite: APCYBER 301

The core SOC course. Students synthesize all previous skills to operate as SOC Analysts, detecting and responding to active threats, then conduct digital forensics investigations following the NIST incident response lifecycle.

Learning Objectives:

- Monitor SIEM logs to detect behavioral anomalies with UEBA and machine learning.

- Execute the NIST Incident Response lifecycle: Preparation → Detection & Analysis → Containment, Eradication & Recovery → Post-Incident Activity.
- Conduct threat hunting campaigns using MITRE ATT&CK and AI-powered hypothesis generation.
- Perform digital forensics to preserve evidence, maintain chain of custody, and analyze malware artifacts.
- Prepare professional investigation reports and expert testimony.

Tools: Splunk Enterprise Security, Microsoft Sentinel, IBM QRadar, TheHive, SOAR platforms, MITRE ATT&CK Navigator, EnCase, FTK, Autopsy, Volatility.

Grading: Laboratory Exercises 30% | Simulation Exercises 45% | Documentation & Reports 15% | Class Participation 10%.

APCYBER 401 — Generative AI and Agentic AI for Cyber Defense

24 Contact Hours | 0.9 Credits | Prerequisite: APCYBER 302

The cutting edge of cyber defense. Students learn to use Generative and Agentic AI as force multipliers for security operations — and to defend against AI-powered attacks.

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.
- Assess AI/ML model security, including adversarial attacks and model defense.
- Apply AI governance frameworks (NIST AI RMF) and ethical AI implementation.

Tools: OpenAI API, LangChain, AI-enhanced security plugins, SOAR/agentic automation platforms.

Grading: Laboratory Exercises 40% | AI Automation Projects 40% | Documentation 10% | Class Participation 10%.

APCYBER 402 — Capstone Project and Industry Simulation

12 Contact Hours (plus 84 hours integrated CAP/OJT) | 0.5 Credits | Prerequisite: APCYBER 401

The professional culmination. Students demonstrate comprehensive cybersecurity expertise through real-world projects and AI-enhanced security operations in a full cyber range environment.

Learning Objectives:

- Design a comprehensive cybersecurity program with AI integration.
- Execute an advanced incident response simulation using AI-powered tools.
- Develop a professional portfolio and AI Era career plan.
- Present and defend findings before an industry panel.

Tools: Comprehensive cyber range platforms, AI-enhanced security tools, project management platforms, professional portfolio systems.

Grading: Capstone Project 60% | Professional Portfolio 25% | Presentation & Communication 10% | Class Participation 5%.

8. AI Era Cybersecurity Focus

This program is uniquely designed for the AI Era of cybersecurity, integrating artificial intelligence and machine learning technologies throughout all courses.

AI-Enhanced Security Operations: machine learning-powered SIEM platforms and automated correlation; behavioral analytics using AI for anomaly detection and insider threat identification; automated threat hunting with AI-powered hypothesis generation; AI-assisted incident response and automated orchestration (SOAR).

AI Security Specializations: AI/ML model security and vulnerability assessment; GenAI security including large language model protection; AI governance frameworks and ethical AI implementation; adversarial attack detection and AI model defense.

Emerging AI Threats and Defenses: AI-powered attack techniques and automated exploitation; deepfake and synthetic media threat detection; AI-generated malware analysis and defense; machine learning-enhanced social engineering detection.

9. Technology Stack and Tools

Category	Tools & Platforms
SIEM & Security Platforms	Splunk Enterprise Security, Microsoft Sentinel, IBM QRadar, Rapid7 InsightIDR
Digital Forensics	EnCase, FTK (Forensic Toolkit), Autopsy, Volatility, Wireshark
Penetration Testing	Kali Linux, Metasploit, Nmap, Burp Suite, Nessus
Cloud Security	AWS Security Hub, Azure Security Center/Sentinel,

	GCP Security Command Center
Network Security	pfSense, Snort, Suricata, Wireshark
Programming & Scripting	Python, PowerShell, Bash
AI & Automation	OpenAI API, LangChain, SOAR platforms, MITRE ATT&CK Navigator, AI-enhanced security platforms
Incident Response	TheHive, NIST SP 800-61 framework, CSIRP playbooks

Recommended texts: NIST Special Publication 800-61: Computer Security Incident Handling Guide; Digital Forensics and Incident Response (Gerard Johansen); Network Security Essentials (William Stallings).

10. Certification Preparation

Students are prepared for industry-standard certifications throughout the program, with exam vouchers included for CompTIA Security+ and CompTIA CySA+.

Level	Certifications
Entry-Level	CompTIA Security+ (voucher included), CompTIA CySA+ (voucher included), CompTIA Network+
Intermediate	CISSP (Associate), CEH (Certified Ethical Hacker), GCIH (GIAC Certified Incident Handler)
Specialized	GCFA (GIAC Certified Forensic Analyst), GSEC (GIAC Security Essentials), AWS/Azure/GCP cloud security certifications
AI-Focused	CompTIA AI+, Certified AI Security Professional (emerging)

11. Assessment, Grading & Completion Requirements

Assessment combines three components:

Component	Weight	Includes
Continuous Assessment	60%	Weekly lab exercises, practical

		assignments, tool demonstrations, team project contributions, peer evaluations
Formal Assessments	25%	Module examinations, practical skill demonstrations, certification practice tests
Capstone Project	15%	Comprehensive cybersecurity project, industry simulation, professional presentation, portfolio development

Students must successfully complete all course requirements with a minimum grade of 70% in each course and demonstrate proficiency in all major program learning objectives through the capstone project and portfolio assessment. Upon successful completion, students receive the NVIT Certificate of Completion and are prepared for entry-level to intermediate cybersecurity positions, with a foundation for advanced certifications and AI-enhanced security career advancement.

12. Meet Your Instructors

NVIT instructors are practicing industry professionals who bring current, real-world expertise into every classroom session.

Sudha Malluru — Lead Instructor, Cybersecurity Engineering & SOC Operations

Sudha Malluru is a cybersecurity engineer with over 12 years of hands-on experience designing, implementing, and optimizing security architectures for complex enterprise environments at global financial institutions. She currently serves as a Cybersecurity Engineer at Goldman Sachs (USA), where she designs enterprise security controls across networks, endpoints, and critical systems; administers IAM, MFA, and SSO; manages Forcepoint DLP and cloud security services across AWS and Azure; and implements end-to-end AI/ML security across data pipelines and model lifecycles — including adversarial testing with frameworks such as CleverHans and the Adversarial Robustness Toolbox, and zero-trust controls for AI environments aligned with NIST AI RMF.

Previously, Sudha spent more than 11 years at HSBC as a Cyber Security Engineer and Analyst, where she implemented Zero Trust Architecture that reduced insider threat risk by 25%, managed the Splunk SIEM environment with custom correlation rules and dashboards, built automated incident response playbooks in Azure Sentinel and AWS Security Hub that cut mean time to detect and respond by 35%, remediated 90+ high and critical vulnerabilities in a single quarter, and performed 24/7 SOC alert triage, EDR response, threat hunting with MITRE ATT&CK and IOCs, and penetration testing.

Credential Area	Details
Certifications	CISSP, CISA, Microsoft Certified: Azure Security Engineer Associate
Education	M.S. Computer Science, Southern Arkansas University (2023, GPA 3.90); B.S., Osmania University
Specialties	SOC Operations & SIEM (Splunk, Sentinel, QRadar), Threat & Vulnerability Management, Cloud Security (Azure/AWS/GCP), Zero Trust & IAM, DLP, Incident Response (CSIRP), AI/ML Security, Compliance (NIST, ISO 27001, HIPAA, PCI-DSS, FedRAMP, RMF)

Teaching Focus	APCYBER 101–103, 201–203, 301, and 302 (SOC/SIEM/IR core), 401

Why students benefit: Sudha brings authentic case studies from Tier-1 global banks, current knowledge of the threat landscape, and deep technical fluency across the exact SIEM, cloud, and AI-security toolchain taught in this program.

Ola Ayeni — Instructor & Curriculum Validator, GRC, Infrastructure & AI Systems Management

Ola Ayeni is an industry practitioner and subject matter expert whose teaching draws from two decades of real-world delivery across enterprise network and datacenter engineering, technology-driven organizational leadership, and risk governance and compliance. She holds a Master of Engineering Management (Michigan Technological University, GPA 3.85) and a distinguished portfolio of certifications including CISA, CISM, CRISC, and AAISM (Advanced AI Security Management — among the first cohort issued globally), plus ISC2 CC, Fortinet Certified Fundamentals in Cybersecurity, and Cisco CCNA/CCDA foundations.

Ola currently serves as a Policy & Reporting Specialist at NOAA (National Sea Grant College Program), translating complex federal regulatory and policy frameworks into board-level guidance across 34 federal offices and 200+ stakeholders, and designing audit-ready compliance documentation and evidence management systems. Her earlier career spans founding and leading a technology-driven organization to 5,000+ returning customers with U.S. Embassy contract delivery; a TechWomen Fellowship at Symantec Corporation (U.S. Department of State program) supporting incident response and forensic documentation workflows at one of the world's leading endpoint protection firms; delivering enterprise network and AV infrastructure across West Africa including a $500K+ NIGCOMSAT videoconferencing contract; and designing multi-state Cisco-based enterprise datacenter security architectures.

Credential Area	Details
Certifications	CISA, CISM, CRISC, AAISM (ISACA), ISC2 CC, Fortinet Certified Fundamentals Cybersecurity, CCNA/CCDA (foundational)
Education	Master of Engineering Management, Michigan Technological University (GPA 3.85); B.Tech Computer Engineering, Ladoke Akintola University of Technology

Specialties	Governance, Risk & Compliance (NIST CSF 2.0, ISO 27001, SOC 2, FISMA, HIPAA, GDPR), IT General Controls & Audit Readiness, Network Infrastructure & Secure System Architecture, AI Systems Management & AI Risk Frameworks (NIST AI RMF), Agentic & Edge AI Governance, Program Delivery
Teaching Focus	APCYBER 100, 102, compliance modules within 301–302, 401 (AI governance), 402 (Capstone advisory)
Recognition	NOAA Knauss Marine Policy Fellow (2025); U.S. Dept. of State TechWomen Fellow; Nasdaq Entrepreneurial Center Times Square Billboard honoree; Social Impact Award (Michigan Tech); Member, ISACA & ISC2; Mentor, Society of Women Engineers

Why students benefit: Ola bridges how systems are built, how organizations govern them, and how both must evolve as AI moves from software into physical, embedded environments — translating complex regulatory subject matter into practical, outcome-oriented learning that prepares students for real roles, not just exams.

Instructor Standards

All NVIT Applied Cybersecurity instructors meet or exceed program requirements: relevant industry certifications (CISSP, CISM, CISA, CRISC, GCIH, GCFA, or equivalent), a minimum of five years of hands-on cybersecurity experience, direct experience in SOC operations, incident response, digital forensics, GRC, or related fields, and ongoing professional development with active participation in cybersecurity communities.

13. Industry Partnerships & Job Placement Support

NVIT maintains partnerships with leading cybersecurity employers in Texas and across the United States. Students benefit from a 24/7 simulated Virtual SOC environment with real-time threat feeds and industry-standard workflows, guest speakers and mentors from Texas companies and government cybersecurity agencies, and comprehensive career services including job placement assistance and career counseling, resume and interview preparation with industry professionals,

professional networking opportunities, internship and apprenticeship program connections, and continuing education pathways for career advancement.

14. Tuition and Fees

Fee Type	Cost
Tuition (all delivery modes)	$7,206.00
Books and Course Materials	$500.00
Registration Fee	$50.00
Background Check	$150.00
Professional Exam Vouchers (CompTIA Security+ & CySA+)	$594.00
TOTAL PROGRAM COST	**$8,500.00**

Note: The total program cost of $8,500.00 applies to all delivery modes — In-Person Live, Virtual Live, and 1-on-1 Virtual Mentorship. Books, registration, background check, and CompTIA Security+ and CySA+ exam vouchers are all included in the total. For single-subject enrollment, fees apply separately.

Cost per Single Subject

Costs are calculated based on the standardized hourly tuition rate of approximately $21.45/hour.

Subject Code	Subject Title	Contact Hours	Standard Tuition (In-Person & Virtual)
APCYBER 100	Digital Cybersecurity Literacy	18	$386.04
APCYBER 101	Cybersecurity Fundamentals	30	$643.39
APCYBER 102	Network Security Fundamentals	36	$772.07
APCYBER 103	Python Programming for Security	36	$772.07
APCYBER 201	Cybersecurity Linux Administration	36	$772.07

APCYBER 202	Cryptography: Principles and Applications	18	$386.04
APCYBER 203	Ethical Hacking & Pen Testing	36	$772.07
APCYBER 301	Cloud Security	36	$772.07
APCYBER 302	Security Ops & Incident Response	54	$1,158.11
APCYBER 401	Generative AI and Agentic AI	24	$514.71
APCYBER 402	Capstone Project and Industry Simulation	12	$257.36
TOTAL		**336**	**$7,206.00**

15. Class Schedule

Orientation & Start Date: New Student Orientation is held Monday, August 3, 2026. Classes for the Fall 2026 cohort run August 3, 2026 through February 9, 2027 (28 weeks). Rolling admissions remain available for the 1-on-1 Virtual Mentorship track.

Milestone	Date
New Student Orientation	Monday, August 3, 2026
First Day of Class (Fall 2026 Cohort)	Monday, August 3, 2026
Program Completion / Graduation	February 9, 2027

Shift	Days	Time
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.

Funding & Workforce Partnerships

NVIT is an approved training provider for Workforce Innovation and Opportunity Act (WIOA) funding through workforce development boards, including CareerSource. Eligible students may qualify for Individual Training Account (ITA) funding covering tuition, books and course materials, registration, background check, and professional exam voucher fees. Contact your local career center or NVIT admissions at info@nvit.tech to determine eligibility and begin the funding approval process.