AppCode.

Coding • Cloud • Security • Data Analytics

ADVANCE CYBER SECURITY PROGRAM

Build cybersecurity skills to accelerate your career

Three months | **Live Mentorship with Experts** | **Lab Sessions for Hands-on Practice** | **Certificate of Completion**

A collaborative approach that goes beyond mandatory requirements is key to achieving true cyber resilience in the supply chain, says ClassNK.

Malicious hackers are becoming increasingly adept at exploiting software vulnerabilities, compelling organizations to build advanced cybersecurity measures or risk losing their reputation, billions of dollars and valuable data.

Organizations across the world are combating this challenge by upskilling their workforce, recruiting skilled cybersecurity professionals, and building robust cyber defense capabilities.

GLOBAL SKILLS SHORTAGE

93% of Business Leaders believe the global skills shortage is increasing every year.

- Information Systems Security Association, July 2020

3.5 MILLION JOBS

in cybersecurity to be available by 2025, according to the U.S. Bureau of Labor Statistics.

- Cybersecurity Ventures, 2022

$103,590

is the median average salary of cybersecurity professionals.

- Comptia.org, 2022

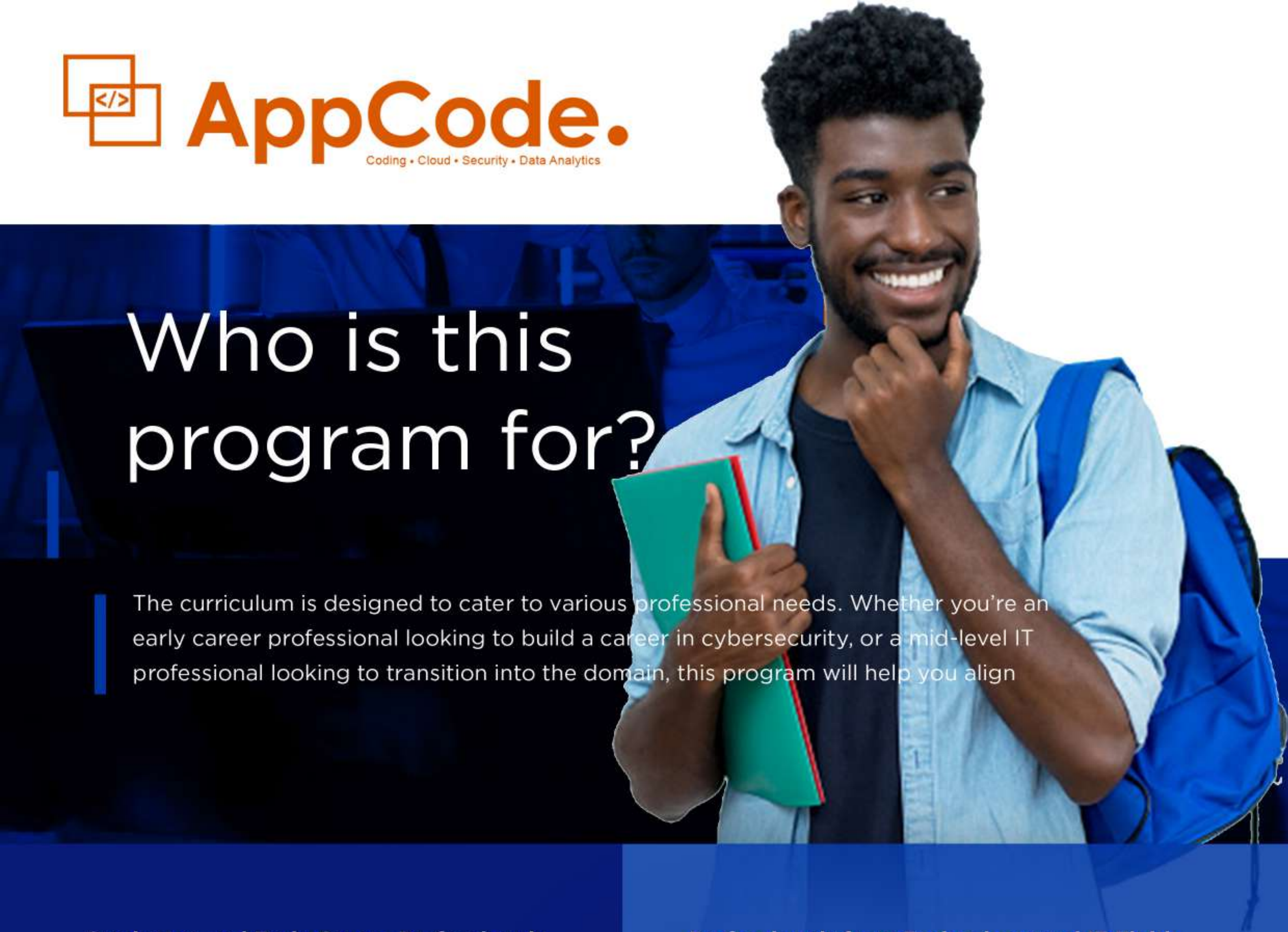
A cybersecurity professional is engaged in a strategic game of ever-changing defensive and offensive techniques and must know the ins-and-outs of the domain to protect IT infrastructures effectively.

The advance Program in Cybersecurity equips you with the skills needed to investigate attacks and build robust cybersecurity systems while giving your resume the University of Austin at Texas advantage. The program is ideal for cyber defense enthusiasts, enabling them to connect with thought leaders in the industry and understand the process of securing digital infrastructure.

Program Highlights

The new-age technological wave has come with its own set of threats, leading to a prominent demand for cybersecurity professionals. This program is crafted by experts to empower you with a skill set to analyze the threat landscape and build long-term cybersecurity strategies.

- A curriculum by the leading faculty
- Interactive live mentorship with industry experts
- Certificate of completion
- Lab sessions to gain hands-on experience
- A final 4-week capstone project (optional)
- Dedicated program support from



Who is this program for?

The curriculum is designed to cater to various professional needs. Whether you're an early career professional looking to build a career in cybersecurity, or a mid-level IT professional looking to transition into the domain, this program will help you align

Graduates and Early Career Professionals

Learn the core concepts of cybersecurity and build a solid foundation using in-demand market skills. You will benefit from this if you are:

- An early career professional looking to transition into a career in cybersecurity
- A fresh graduate wanting to break into the cybersecurity domain

Professionals from Technology and IT Fields

The program also gives you an overview of the best cyber defense practices, enabling you to analyze the threat landscape and upskill as a cybersecurity specialist. You will benefit from this if you are:

- An IT infrastructure manager who wants to upskill with cybersecurity
- An experienced professional looking to specialize in cybersecurity

Successful completion of the program may qualify you for various roles in cybersecurity, including:

- Cybersecurity Analyst
- Cyber Threat Intelligence Analyst
- Information Security Specialist
- SOC Specialist
- Incident Response Professional
- Cloud Security Analyst
- SOC Analyst

AppCode.

Coding • Cloud • Security • Data Analytics

Program Outcomes

Upon completion of the program, you would have developed the skill set needed to:

1. Develop the Security Mindset

2. Perform incident investigations to identify the source of the threat, assess the risk and respond, and write clear and world-class incident reports

3. Familiarize yourself with the Standards and Frameworks such as: National Institute of Standards and Technology (NIST), MITRE ATT&CK, Center for Internet Security (CIS) Benchmarks

4. Demonstrate the understanding of how to identify and defend against modern-day threats such as Ransomware

5. Comprehend the evolving threat landscape by understanding the biggest cyber attacks to-date

6. Build muscle memory for responding to cyber attacks by following Incident Response playbooks

The program also helps in preparing learners for the CompTIA Security+, CompTIA Cybersecurity Analyst (CySA+), and EC-Council Certified SOC Analyst (CSA) certifications.

AppCode.

Coding • Cloud • Security • Data Analytics

Curriculum

The program is designed with 4 milestones. Starting strong with the foundations of cybersecurity, you then deep dive into the different types of cyber attacks. As you understand the attacks, you will learn to design the security controls needed to build a resilient system. Finally, if an attack happens, you practice responding to these incidents by referring to Incident Response Playbooks given to you as part of the program. In this last section you will also learn how to investigate these attacks.

MODULE 1:
FOUNDATIONS OF INFORMATION SECURITY |

Learn the fundamentals of Risk Management, Cryptography, Network Security, and Cloud Security

MODULE 2:
UNDERSTANDING CYBER ATTACKS |

Learn about the latest advances in cybersecurity and how such attacks are managed at organizational levels

MODULE 3:
DESIGNING SECURITY CONTROLS |

Learn how to identify and implement the right cybersecurity control for various cyber attacks

MODULE 4:
SECURITY OPERATIONS & INCIDENT MANAGEMENT |

Learn to use Incident Response Playbook to defend against an ongoing cyber attack, and protect critical digital resources in this situation

MODULE 5:
CAPSTONE PROJECT (OPTIONAL) |

Demonstrate your learnings throughout the program with a comprehensive capstone project

TOPICS

- CIA Triad
- Cybersecurity Risk Management
- Need for Security
  IAAA – Identity Authentication
- Authorization Auditing
- Cryptography
- Enterprise Applications
- Network Security
- OSI and TCP/IP Model
- Wireshark
- Zero Trust
- Securing the Cloud
- Security Compliance & Frameworks
- Application Security (Nessus, Metasploit)

KEY TAKEAWAYS

- Understand the ‘why’ behind cybersecurity
- Learn the principles of Risk Management
- Gain an understanding of how enterprise applications work
- Understand the concepts behind network design & network security
- Understand how cryptography works & what it protects
- Get a flavor of perimeter-less security, also called as Zero Trust Network Architecture
- Demonstrate your understanding by completing labs that simulate real-life scenarios

MODULE 2: UNDERSTANDING CYBER ATTACKS

TOPICS

- MITRE ATT&CK Framework
- Threat Tactics
- Malware
- Attack Kill Chain
- Attack Vectors
- Deep Dive Into the Dark Web
- Physical Attacks
- Indicators of Compromise
- Tactics Techniques and Procedures
- Case Study: Not Petya Solarwinds, Colonial Pipeline, Olympic games
- Attack Groups - Unit 8200, Nobelium, APT 29

KEY TAKEAWAYS

- Understand the different types of cyber attacks and the risks they pose
- Familiarize yourself with the types of threats and the threat actors
- Delve deeper into the Tactics, Techniques and Procedures used by the adversaries with insights
- Understand the structure of an attack- Kill chain methodology
- Apply the concepts of cyber attacks and threat to discern the Solarwinds and Colonial Pipeline attacks

TOPICS

- Firewalls
- Web Application Firewalls
- IDS/IPS
- Antivirus & EDR
- Email Protection
- Data Loss Prevention
- Vulnerability Management
- Zero-Day Vulnerability
- Patching
- System Audit
- Maintenance, Monitoring, and Analysis of Audit Logs
- SIEM (Security Information and Event Management)
- Incident Investigation
- Threat Intelligence

KEY TAKEAWAYS

- Understand the controls that help in detecting security threats
- Develop a deeper understanding of SIEM and its purpose
- Familiarize yourself with the reviewing, interpreting, and understanding of computer-generated logs
- Learn how cyber threat intelligence helps in assessing security threats
- Gain knowledge on network firewalls and web application firewalls
- Familiarize yourself with antivirus and its applications
- Understand and practice shell scripting

MODULE 4: SECURITY OPERATIONS & INCIDENT MANAGEMENT

TOPICS

- Incident Response and Playbooks
- NIST Framework
- The Golden Hour
- Log and Email Analysis
- Writing Incident Reports
- Security Operations Centre – A Deep dive
- SLAs KRIs, KPI
- Maintenance, Monitoring, and Analysis of Audit Logs
- Recovery from an Incident
- Forensics

KEY TAKEAWAYS

- Learn how to read, write and examine incident reports
- Learn about the Incident Response Lifecycle of NIST
- Familiarize yourself with the concept of the golden hour
- Understand how to examine incident data in order secure from cyber threats using forensics
- Gain knowledge on the tasks performed at a Security Operations Center (SOC)
- Learn to form a recovery strategy from a cyber attack

Testimonials

I enrolled in the advance cybersecurity program on May 22 and it's been an interesting journey so far.The payment option was friendly and flexible. The recorded and hands on project have been engaging and impactful - Perri Daniels (0 Breach)

professional, I realized that the world was soon moving towards the "Internet of Things" direction, with digital platforms leading the way. As a 21st century lawyer, enrolling for a cybersecurity program was the best option for me. This program is by far, the most useful in the cyber world. It has noticeably improved my understanding of how cyber criminals plan and execute their malicious activities.

This program is a must-have for every professional. The recent election in Kenya and the technical and detailed evidence gathered is enough proof that all professionals - lawyers, judges, accountants and politicians - need to understand the basics of cybersecurity. As world dynamics change with the influence of IoT, we need to keep up with this change.

This program gives people a thorough understanding of the tools. Unlike a lot of other programs, which only focus on memorizing facts and concepts, this one teaches you cyber skills that you can apply in any area of work. I would recommend this program to anyone who wants to learn more about cybersecurity."
Kelvin Selorm - Upcode

AppCode.

Coding • Cloud • Security • Data Analytics

Ready to become a cybersecurity expert?

APPLY NOW

appcodeglobal.org

Contact Us

☎ 059 804 4825 | ✉ appcodeglobal.org | 🌐 www.appcodeglobal.org