AFRICA | NIL | EC-Council Accredited Training Center

EC Council Course Catalogue

Advance your cybersecurity career with globally recognised EC-Council certifications.
Our EC-Council training programmes build hands-on offensive and defensive security skills, validate practical cyber expertise, and prepare professionals to detect, defend, and respond to evolving threats in today's digital environments.

Table Of Content

Explore Our Learning Collections

About NIL and EC Council

About NIL

NIL Africa is a leading IT skills development company and the exclusive delivery arm for NIL Learning in Sub-Saharan Africa. Since 2009, NIL Africa has been at the forefront of delivering comprehensive learning programmes across various tech verticals.

Committed to empowering IT professionals and organisations, our mission is to provide comprehensive learning programmes in Networking, Cybersecurity, IT Service Management, Data, Cloud, Data Centre, AI, Software, Automation, and Service Provider technologies across Africa.

Focused on advanced IT training, NIL Africa's Learning Division is dedicated to empowering IT professionals and organisations with cutting-edge skills and knowledge, aligning its offerings with the rapidly evolving digital landscape of Africa.

NIL Africa is proud to inform you that partnering with us means partnering with a proudly South African company which is recognised as a Level 1 B-BBEE contributor. We take pride in being 'ahead of the curve' in our commitment to engaging in direct empowerment initiatives in the Information Technology sector.

About EC Council

The International Council of E-Commerce Consultants (EC-Council) is a globally recognised leader in cybersecurity training and professional certification. Founded in 2001, EC-Council was established to address the growing demand for skilled cybersecurity professionals capable of defending organisations against evolving cyber threats. Its programs are trusted by organisations, governments, and professionals in over 150 countries.

EC-Council offers a comprehensive portfolio of certifications that validate practical skills and industry knowledge. Its flagship programs, including Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Certified Security Analyst (ECSA), and Certified Chief Information Security Officer (C|CISO), equip learners with hands-on experience and a deep understanding of cybersecurity principles.

EC-Council provides clear career pathways and certification roadmaps to help professionals progress from foundational knowledge to advanced cybersecurity expertise. Starting with entry-level programs, learners can build practical skills in ethical hacking, network security, and digital forensics, then advance to specialised and leadership certifications.

These structured roadmaps guide individuals through a logical progression of skills and credentials, enabling them to align their training with career goals, industry demands, and emerging threat landscapes. By following EC-Council's certification pathways, professionals can enhance employability, demonstrate verified expertise, and position themselves for roles ranging from security analysts and ethical hackers to cybersecurity managers and executives.

Essentials Series

Certified Security Specialist (ECSS)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	ECSS

Course Overview
This course provides foundational cybersecurity knowledge in information security, network defence, and digital forensics. Learners gain essential skills to understand threats, apply security controls, and start careers as security analysts, network defenders, or forensic support specialists.

Learning Objectives:
- Grasp core principles of information security: confidentiality, integrity, availability
- Understand network security, protocols, authentication, and access control
- Identify common threats and basic mitigation techniques
- Apply introductory ethical hacking concepts
- Learn essential cryptography and authentication methods
- Understand digital forensics fundamentals and evidence handling
- Utilise key security controls such as firewalls and intrusion detection systems

Who should enroll:
- Aspiring cybersecurity professionals

Certified Secure Computer User (CSCU)

Duration	2 Days
Delivery	ILT / VILT / Self-paced
Exam	CSCU

Course Overview
This course delivers essential cybersecurity awareness and practical skills for everyday computer users. It equips learners to recognise and respond to common cyber threats, secure their devices and online activities, and protect personal and professional information assets in both work and home environments.

Learning Objectives:
- Understand fundamental security principles and common cyber threats
- Secure operating systems and manage antivirus/antimalware tools
- Navigate the internet safely and recognize unsafe websites
- Protect email communications and social networking accounts
- Secure mobile devices and home network connections
- Implement basic data protection, backup, and recovery practices
- Apply safe practices for online transactions and digital interactions

Who should enroll:
- General computer users seeking foundational cybersecurity skills

Ethical Hacking Essentials (EHE)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	EHE

Course Overview
This introductory course builds foundational knowledge in ethical hacking and penetration testing. It equips learners with essential concepts in computer and network security, practical exposure to threats and vulnerabilities, and introductory hands-on experience, preparing them entry-level roles.

Learning Objectives:
- Understand fundamental ethical hacking concepts and the role of offensive security in defence
- Recognise common threats, vulnerabilities, and attack vectors across systems and networks
- Apply basic countermeasures for attacks against web, wireless, mobile, and IoT/OT platforms
- Explain techniques used in password cracking and social engineering
- Identify cloud security threats and related protection strategies
- Demonstrate basic penetration testing methodology and workflow
- Analyse security weaknesses and apply preliminary mitigation approaches

Who should enroll:
- Aspiring cybersecurity professionals

Security Operations Centre Essentials (SCE)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	SCE

Course Overview
This course is an introduction to SOC concepts, technologies, and workflows. Designed for beginners and career changers, this program builds essential skills in security monitoring, incident detection, threat analysis, and SOC architecture through hands-on labs and capstone challenges in simulated real-world environments.

Learning Objectives:
- Understand core SOC functions, architecture, and workflow
- Learn fundamentals of computer networks, TCP/IP and OSI models
- Identify cyber threats, vulnerabilities, and attack methods
- Explore security concepts across Windows, Linux, and Unix systems
- Gain insight into SIEM architecture, log management, and dashboard analysis
- Learn incident escalation and response lifecycle processes
- Examine threat intelligence sources, types, and basic threat hunting

Who should enroll:
- Aspiring cybersecurity professionals

AFRICA | NIL

Essentials Series

Digital Forensics Essentials (DFE)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	DFE

Course Overview
This entry-level course that introduces learners to the principles, methods, and practices of digital forensics investigation. Designed for beginners with no prior cybersecurity experience, DFE combines foundational theory with hands-on labs and simulated challenges to build competency in forensic analysis and evidence investigation.

Learning Objectives:
- Understand core digital forensics concepts, including investigation phases and methodologies
- Describe the computer forensics investigation process and evidence handling
- Analyse diverse data sources such as hard drives, file systems, and volatile memory
- Perform basic forensics tasks on Windows, Linux, and network environments
- Investigate web, email, and dark web activity
- Apply fundamental malware forensics techniques

Who should enroll:
- Aspiring cybersecurity professionals

Cloud Security Essentials (CSE)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	CSE

Course Overview
This course provides foundational training in cloud security, it provides core competencies in securing identities, data, applications, and hybrid cloud environments, with practical exposure through labs and capstone challenges.

Learning Objectives:
- Understand core cloud computing fundamentals, including service models and deployment types
- Explain cloud security principles, including data protection and encryption
- Apply identity and access management (IAM) techniques in cloud environments
- Recognize network and application security practices for cloud infrastructures
- Understand cloud monitoring, incident response, risk assessment, and governance
- Describe compliance, regulatory frameworks, and cloud security best practices

Who should enroll:
- Aspiring cybersecurity professionals
- Teams and organisations building baseline cloud security competencies

Network Defense Essentials (NDE)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	NDE

Course Overview
This course introduces core concepts of network defence, security controls, and practical threat identification, supplemented by interactive labs and real-world challenges to develop applied understanding in defending digital assets.

Learning Objectives:
- Understand foundational principles of network defence and information security
- Explain identification, authentication, and authorisation mechanisms
- Recognise essential security controls and protocols (firewalls, IDS/IPS, VPN)
- Gain awareness of wireless, mobile, and IoT network security
- Learn basic cryptography and data protection concepts
- Monitor network traffic for suspicious activity

Who should enroll:
- Aspiring cybersecurity professionals
- Teams and organisations building baseline network security competencies

DevSecOps Essentials (DSE)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	SCE

Course Overview
This course introduces secure application development across on-premises, cloud, and hybrid environments. Designed for beginners, it teaches how to identify development risks and implement security throughout the software lifecycle. Hands-on labs and capstone projects reinforce skills and prepare learners for careers in secure development and related roles.

Learning Objectives:
- Understand core principles of DevSecOps and its role in secure software development
- Identify common application development risks and vulnerabilities
- Apply basic security testing practices within continuous integration/continuous deployment (CI/CD) workflows
- Explain secure coding concepts and integration of security into development pipelines
- Recognise approaches for securing applications across on-premises, cloud, and hybrid environments
- Demonstrate skills through capstone projects with real-world challenges

Who should enroll:
- IT, development, and operations professionals building foundational security skills

AFRICA | NIL

Essentials Series

Internet of Things Security Essentials (ISE)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	ISE

Course Overview
This course provides foundational knowledge and practical skills for securing IoT environments. It covers fundamentals and networking protocols as well as threat identification, incident response, and security engineering. Hands-on labs and capstone projects prepare participants to design, deploy, and maintain secure IoT solutions across diverse systems and networks.

Learning Objectives:
- Understand core digital forensics concepts, incluUnderstand IoT fundamentals, including device characteristics and ecosystem architecture
- Explain IoT networking and communication protocols
- Identify common IoT threats, vulnerabilities, and attack vectors
- Apply basic security engineering principles to protect IoT systems
- Integrate cloud connectivity and security considerations for IoT deployments
- Learn incident response strategies tailored to IoT environments

Who should enroll:
- IT and technology teams building foundational IoT security competencies

Threat Intelligence Essentials (TIE)

Duration	3 Days
Delivery	ILT / VILT / Self-paced
Exam	TIE

Course Overview
This course course provides foundational knowledge in cyber threat intelligence, including the threat landscape, intelligence lifecycle, and analysis workflows. It teaches learners to collect and analyse threat data, understand threat types, and apply intelligence to real-world challenges through hands-on labs and capstone projects.

Learning Objectives:
- Understand core threat intelligence concepts and terminology
- Explain the cyber threat landscape and threat actor categories
- Distinguish types of threat intelligence (strategic, operational, tactical, technical)
- Learn threat data collection methods and sources
- Apply basic threat analysis and interpretation techniques
- Explore the use of Threat Intelligence Platforms (TIPs) and threat hunting

Who should enroll:
- Aspiring cybersecurity professionals
- Teams and organisations building foundational threat intelligence capabilities

Certified Cybersecurity Technician (CCT)

Duration	5 Days
Delivery	ILT / VILT / Self-paced
Exam	CCT

Course Overview
This course prepares learners for technician-level roles by combining knowledge and practical application in network defence, ethical hacking, digital forensics, security operations, and related domains. Learners will solve practical challenges through hands-on labs and live cyber range exercises

Learning Objectives:
- Understand foundational cybersecurity principles, threats, and vulnerabilities
- Apply network defense techniques and core controls
- Demonstrate introductory ethical hacking and vulnerability identification
- Perform basic digital forensic tasks and security operations activities
- Analyse security events and support incident handling functions
- Utilise tools and techniques across security domains, including risk management and monitoring

Who should enroll:
- IT support and networking specialists seeking to transition into security roles

Core Series

Certified Network Defender (CND)

Duration	5 Days
Delivery	ILT / VILT
Exam	SC-900

Course Outline:
This vendor-neutral course is designed to equip learners with the skills to protect, detect, respond to, and predict network threats. Through a hands-on, lab-intensive curriculum, it develops expertise in defensive network operations, security controls, traffic monitoring, vulnerability management, and incident response, preparing participants to build and maintain resilient, secure network infrastructures that support organisational continuity.

Learning Objectives:
- Understand core network security principles and defense strategies
- Design, implement, and manage network security controls, including firewalls, IDS/IPS, and VPNs
- Monitor and analyse network traffic and logs to identify threats and anomalies
- Perform risk assessment and vulnerability management activities
- Apply defensive techniques for endpoint, wireless, and cloud network environments
- Respond to and recover from network security incidents
- Integrate threat intelligence and adaptive security practices into network defence

Who Should Enroll:
- Network administrators and engineers
- Security analysts and SOC personnel

Pre-requisites:
- Working knowledge of networking concepts (TCP/IP, routing, switching, OSI model)
- Familiarity with operating systems such as Windows and Linux
- Basic understanding of information security principles
- Prior experience in network administration or IT operations

Certified Ethical Hacker (CEH AI)

Duration	5 Days
Delivery	ILT / VILT
Exam	CEH AI

Course Outline:
This course equips learners with advanced ethical hacking skills enhanced by AI and automation. Participants develop a deep understanding of modern attack techniques, AI-driven reconnaissance, and intelligent exploitation methods. Through hands-on labs and real-world scenarios, learners assess, exploit, and secure systems, networks, applications, and cloud environments, applying offensive techniques efficiently and translating results into actionable defensive improvements.

Learning Objectives
- Apply the ethical hacking lifecycle using AI-assisted tools and techniques
- Leverage AI for reconnaissance, vulnerability discovery, and attack surface analysis
- Conduct network, application, cloud, and wireless penetration testing
- Identify and exploit modern threats while understanding associated countermeasures
- Analyse and bypass defensive controls using intelligent attack strategies
- Translate penetration testing results into risk-based remediation actions

Who Should Enroll:
- Ethical hackers and penetration testers
- Security analysts and SOC professionals
- Network and security engineers
- Incident response and threat hunting teams

Pre-requisites:
- Solid understanding of networking concepts and protocols
- Working knowledge of Windows and Linux operating systems
- Foundational understanding of information security principles
-

AFRICA | NIL

Specialisation Courses

Certified Security Operations Centre Analyst (CSA)

Duration	3 Days
Delivery	ILT / VILT
Exam	CSA

Course Outline:
This course prepares learners for roles within a SOC by building practical skills in security monitoring, threat detection, incident analysis, and response. It delivers comprehensive coverage of SOC workflows, SIEM technologies, log management, threat intelligence, and incident response, with a strong emphasis on hands-on labs and real-world scenarios. Participants also learn to leverage automation and AI-enhanced tools to improve detection and decision-making efficiency.

Learning Objectives:
- Understand SOC operations, workflows, and defensive responsibilities
- Monitor and analyse security events and alerts using SIEM tools
- Perform centralised log collection, normalisation, and correlation
- Identify threats, indicators of compromise, and attack vectors
- Apply threat intelligence to enhance detection and prioritisation
- Execute incident triage, response, escalation, and reporting
- Collaborate with incident response teams and support forensic analysis
- Adapt SOC practices to cloud environments and emerging technologies

Who Should Enroll:
- Tier I and Tier II SOC analysts
- Cybersecurity analysts

Pre-requisites:
- Basic understanding of networking concepts and security principles
- Familiarity with Windows and Linux operating systems
- Experience in network or security roles

Certified Encryption Specialist (ECES)

Duration	3 Days
Delivery	ILT / VILT
Exam	ECES

Course Outline:
This course provides foundational and practical knowledge of modern cryptography. Learners explore symmetric and asymmetric algorithms, hashing, steganography, and cryptanalysis. Hands-on exercises teach data encryption, secure communications, VPNs, and best practices, equipping participants to protect sensitive information and apply encryption effectively in real-world environments.

Learning Objectives
- Understand core cryptography principles and algorithms
- Apply symmetric and asymmetric encryption techniques
- Implement hashing and steganography for data protection
- Configure secure VPNs and encrypted storage
- Analyze cryptanalysis and emerging encryption trends
- Evaluate and apply best practices for encryption in real-world scenarios

Who Should Enroll:
- Cybersecurity professionals and ethical hackers
- Network and security engineers
- IT professionals responsible for data protection

Pre-requisites:
- Basic knowledge of networking and information security
- Familiarity with operating systems and IT fundamentals
- Understanding of security and encryption concepts

Computer Hacking Forensic Investigator (CHFI)

Duration	5 Days
Delivery	ILT / VILT
Exam	CHFI

Course Overview
This course provides comprehensive training in digital forensics investigation methodologies and tools. Learners gain practical skills for identifying, collecting, preserving, analysing, and reporting digital evidence in support of cybersecurity incidents, internal investigations, and legal requirements. The curriculum covers forensic techniques across systems, networks, mobile devices, cloud services, and emerging technologies.

Learning Objectives
- Understand digital forensics principles, lifecycle, and legal considerations
- Identify and preserve digital evidence from systems, networks, and storage devices
- Conduct forensic analysis on Windows, Linux, and mobile platforms
- Apply forensic techniques to memory, disk, and cloud data sources
- Perform email, web, and network traffic forensics
- Document findings and produce professional forensic reports
- Support incident response and litigation readiness with forensic evidence

Who Should Enroll
- Digital forensic examiners and investigators
- Incident response and SOC professionals
- Security analysts and cybercrime responders
- Law enforcement and legal professionals involved in cybercrime

Pre-requisites
- Foundational understanding of networking and operating systems
- Basic knowledge of information security principles

AFRICA | NIL

Specialisation Courses

Certified Incident Handler (ECIH)

Duration	3 Days
Delivery	ILT / VILT
Exam	ECIH

Course Outline:
This course equips learners with the skills and methodologies to prepare for, identify, respond to, and recover from cybersecurity incidents. It covers incident lifecycle management, response frameworks, forensics integration, communication strategies, and post-incident analysis. Participants gain hands-on experience with real-world scenarios to build confidence in managing incidents across enterprise environments.

Learning Objectives:
- Understand the full incident response lifecycle from preparation through recovery
- Identify and classify security incidents using structured frameworks
- Implement effective detection and escalation mechanisms
- Apply best practices for containment, eradication, and recovery
- Integrate forensic evidence handling into incident workflows
- Communicate with stakeholders during an incident
- Conduct post-incident analysis and lessons-learned processes

Who Should Enroll:
- Incident response team members and SOC personnel
- Network and security operations professionals
- IT managers responsible for incident readiness and response
- Cybersecurity practitioners advancing toward leadership roles

Pre-requisites:
- Basic understanding of information security concepts
- Familiarity with networking and operating systems
- Understanding of security operations and incident processes

Certified Threat Intelligence Analyst (CTIA)

Duration	5 Days
Delivery	ILT / VILT
Exam	CTIA

Course Outline:
This course develops advanced skills in collecting, analysing, and operationalising cyber threat intelligence to inform security decision-making. Participants learn structured methodologies for building intelligence reports, understanding threat actor behaviours, and applying intelligence across defensive operations. The curriculum bridges technical and analytical frameworks that enable security teams to anticipate, detect, and mitigate threats more effectively.

Learning Objectives
- Understand the threat intelligence lifecycle and its role in cybersecurity strategy
- Identify and profile threat actors, tactics, techniques, and procedures (TTPs)
- Collect and validate data from diverse intelligence sources
- Analyse threat data to produce actionable intelligence products
- Integrate intelligence into detection, response, and risk prioritisation
- Apply frameworks for strategic, operational, and tactical intelligence
- Communicate threat insights to technical and executive stakeholders

Who Should Enroll:
- Security operations and incident response professionals
- Security analysts and risk teams
- Cybersecurity managers and strategic planners

Pre-requisites:
- Foundational cybersecurity knowledge (networking, security principles)
- Familiarity with security operations and threat detection concepts
- Experience in security analysis or SOC environments

Disaster Recovery Professional (DRP)

Duration	3 Days
Delivery	ILT / VILT
Exam	DRP

Course Overview
This course equips learners with the strategies, frameworks, and practical skills necessary to ensure operational resilience in the face of disruptions. Participants learn how to develop, implement, test, and maintain business continuity and disaster recovery plans that protect critical systems, data, and services against cyber incidents, natural disasters, and other operational disruptions.

Learning Objectives
- Understand the fundamentals of business continuity planning and disaster recovery
- Conduct business impact analysis to identify critical functions and dependencies
- Develop effective continuity strategies and recovery objectives
- Design, document, and implement BCP and DR plans
- Perform plan testing, validation, and refinement exercises
- Integrate risk assessment and mitigation into continuity planning
- Coordinate cross-functional teams and stakeholder communication during disruptions

Who Should Enroll
- Business Continuity / Disaster Recovery Manager
- IT Infrastructure / Operations Manager
- Governance, Risk, and Compliance (GRC) Analyst / Manager
- Security Operations Manager

Pre-requisites
- Basic understanding of organisational operations, risk, and IT systems
- Familiarity with information security and risk management fundamentals
- Experience in planning, operations, IT, or security functions

AFRICA | NIL

Specialisation Courses

Certified Penetration Tester (CPENT AI)

Duration	5 Days
Delivery	ILT / VILT
Exam	CPENT AI

Course Outline:
This is an advanced, hands-on program designed to build AI-enabled penetration testing capability. The course delivers a complete end-to-end penetration testing methodology, integrating AI techniques across every phase of the attack lifecycle. Learners gain real-world experience through extensive labs, cyber ranges, and multi-disciplinary environments, enabling them to conduct complex enterprise-grade penetration tests and translate findings into actionable security outcomes.

Learning Objectives
- Execute a complete penetration testing engagement from scoping to reporting
- Apply AI-driven techniques across reconnaissance, exploitation, and post-exploitation
- Conduct advanced attacks across Active Directory, web, API, IoT, binaries, and cloud environments
- Leverage AI tools and automation, develop custom scripts and offensive tooling, to improve efficiency and accuracy
- Perform advanced privilege escalation, lateral movement, and pivoting
- Exploit modern enterprise defences, segmented networks, and filtered environments

Who Should Enroll:
- Application security and advanced security engineers
- Ethical hackers and penetration testers

Pre-requisites:
- Strong understanding of networking, operating systems, and security fundamentals
- Proficiency with Windows and Linux environments
- Ethical hacking or penetration testing experience

Certified Responsible AI Governance & Ethics (C|RAGE)

Duration	5 Days
Delivery	ILT / VILT
Exam	CRAGE

Course Outline:
The Certified Responsible AI Governance & Ethics (C|RAGE) course equips professionals to govern AI responsibly. Learners gain practical skills in ethical AI deployment, risk management, compliance, and audit-ready processes, applying global standards such as NIST AI RMF, ISO/IEC 42001, and the EU AI Act across the AI lifecycle.

Learning Objectives
- Understand AI concepts, lifecycles, and operations.
- Apply ethical and responsible AI principles.
- Implement AI governance frameworks aligned with global standards.
- Ensure regulatory compliance and audit readiness.
- Assess and mitigate AI risks and vulnerabilities.
- Embed privacy, trust, and safety controls.
- Lead AI incident response and business continuity.
- Conduct assurance, testing, and auditing of AI systems.

Who Should Enroll:
- GRC managers, AI program managers, Chief AI Officers
- Compliance and privacy officers
- Internal auditors and ethics advisors
- AI risk managers and security architects

Pre-requisites:
- Basic understanding of AI concepts and data/technology principles.
- Experience in governance, compliance, risk, or AI program management.
- Familiarity with regulatory frameworks is beneficial.

Web Application Hacking and Security (WAHS)

Duration	3 Days
Delivery	ILT / VILT
Exam	WAHS

Course Outline:
This course provides practical training in testing the security of web applications. Learners gain hands-on experience identifying vulnerabilities, analysing risks, and applying mitigation strategies based on real-world scenarios. The course emphasises the OWASP Top Ten and common web threats, equipping participants with the skills to assess application security, perform professional testing, and contribute to secure development lifecycles.

Learning Objectives:
- Understand web application architecture and security principles
- Identify and exploit common web vulnerabilities, including OWASP Top Ten risks
- Perform manual and automated testing techniques
- Analyze application logic flaws and insecure coding practices
- Apply secure coding recommendations and remediation guidance
- Use industry-standard tools for web application testing
- Document findings and produce actionable security reports

Who Should Enroll:
- Penetration Testers
- Application Developers

Pre-requisites:
- Basic understanding of web technologies (HTTP, HTML, JavaScript)
- Familiarity with networking and operating systems
- Security fundamentals
- Experience with testing concepts

Specialisation Courses

Certified Blockchain Developer (BDC)

Duration	5 Days
Delivery	ILT / VILT
Exam	BDC

Course Outline:
This course equips learners with core and advanced skills in blockchain technology fundamentals, development practices, and applied implementation. The curriculum balances conceptual foundations (e.g., cryptography, network consensus) with hands-on labs and project work on real blockchain platforms (e.g., Ethereum, smart contracts). Practical exercises include setting up private networks, cryptomining, use of code IDEs, and developing decentralised applications.

Learning Objectives
- Understand the architecture of blockchain networks and decentralisation principles.
- Explain hashing, consensus mechanisms, and scalability challenges.
- Distinguish key blockchain use cases, business impact, and deployment criteria.
- Describe leading cryptocurrency structures and tokenisation processes.
- Apply cryptography basics and cryptomining tools in private networks.
- Use Python, JavaScript, and Java for blockchain programming tasks.
- Work with Ethereum tools and construct secure smart contracts.
- Integrate blockchain solutions with emerging technologies (AI, IoT).

Who Should Enroll:
- Software engineers and developers
- Full-stack and web developers
- System architects

Pre-requisites:
- Basic programming knowledge (object-oriented concepts)
- Familiarity with JavaScript and full-stack web development
- General computing skills with access to a Linux environment for labs

Blockchain Fintech Certification (BFC)

Duration	5 Days
Delivery	ILT / VILT
Exam	BFC

Course Outline:
This course equips finance and fintech professionals with an understanding of blockchain technology and its strategic application in financial services and insurance. The program blends conceptual foundations (e.g., decentralisation, consensus mechanisms) with real-world insights into cryptocurrencies, financial use cases, regulatory considerations, and blockchain project implementation.

Learning Objectives
- Explain blockchain architecture, decentralisation, and core components
- Assess blockchain applications in financial services and insurance
- Understand DeFi, crypto exchanges, digital currencies, and tokenisation
- Apply regulations and compliance considerations in financial blockchain use
- Build and analyse private blockchain networks (e.g., Ethereum)
- Compare PoW and PoS consensus mechanisms and their financial implications
- Understand smart contracts, security, and permissioned vs. permissionless models
- Explore blockchain-as-a-service, DAOs, and emerging financial frameworks

Who Should Enroll:
- Finance / Fintech professionals
- Banking and insurance practitioners
- Technical consultants in financial services
- Business analysts focused on financial systems

Pre-requisites:
- General awareness of business management processes
- Basic computing knowledge
- General computing skills with access to a Linux environment for labs

Blockchain Business Leader Certification (BBLC)

Duration	3 Days
Delivery	ILT / VILT
Exam	BBLC

Course Outline:
This course prepares business leaders to leverage blockchain technology strategically across industries. It blends foundational blockchain concepts with applied business use cases, covering decentralization, consensus mechanisms, digital assets, smart contracts, and real-world applications (e.g., supply chain, finance, healthcare). The curriculum includes both conceptual learning and hands-on blockchain exposure

Learning Objectives:
- Explain blockchain fundamentals and network elements
- Articulate how and when blockchain adds business value
- Analyze digital currencies, tokenization, and cryptocurrency assets
- Understand blockchain implementation models, including BaaS
- Evaluate permissioned vs. permissionless networks and governance
- Describe enterprise use cases across industry domains
- Understand basics of Ethereum, Bitcoin, and smart contracts
- Address security considerations and scalability challenges

Who Should Enroll:
- Mid- to senior-level business managers and executives
- Strategic planners and business transformation leaders
- Technical project leads
- Professionals responsible for digital innovation adoption

Pre-requisites:
- General awareness of business operations and management principles
- Basic computing knowledge
- General computing skills with access to a Linux environment for labs

AFRICA | NIL

Specialisation Courses

Certified Application Security Engineer (CASE .NET)

Duration	3 Days
Delivery	ILT / VILT
Exam	CASE.NET

Course Outline:
This course develops advanced application security expertise across the full Software Development Lifecycle (SDLC) with a focus on secure design, coding, testing, and deployment. Unlike secure-coding-only trainings, the program covers security requirements gathering, architecture, secure coding patterns, threat analysis, and both static and dynamic testing practices.

Learning Objectives
- Understand application security threats and the role of secure SDLC practices
- Gather and define security requirements for software projects
- Design secure application architectures and components
- Apply secure coding practices for input validation, authentication, authorization, and cryptography
- Manage secure session handling and error management
- Perform static and dynamic application security testing
- Implement secure deployment and maintenance processes
- Reinforce security across all SDLC phases

Who Should Enroll:
- Intermediate .NET developers
- Application security engineers, analysts, and testers
- Application developers / testers

Pre-requisites:
- Experience with .NET development
- Understanding of software development and programming fundamentals

Certified Application Security Engineer (CASE Java)

Duration	3 Days
Delivery	ILT / VILT
Exam	CASEJAVA

Course Outline:
This course prepares software professionals to embed security throughout the Software Development Lifecycle (SDLC) with a specific focus on the Java platform. It emphasizes secure requirement gathering, design, secure coding practices, security testing, and secure deployment. The curriculum goes beyond secure coding to include comprehensive security considerations from planning through post-deployment.

Learning Objectives
- Understand application security threats and SDLC security needs
- Gather and define security requirements for software projects
- Design secure application architectures and components
- Apply secure coding practices for input validation, authentication, authorization, cryptography, session management, and error handling
- Perform static and dynamic application security testing (SAST & DAST)
- Secure application deployment and maintenance
- Recognise common Java-specific security issues and mitigation techniques
- Incorporate security throughout the application lifecycle

Who Should Enroll:
- Intermediate Java developers
- Application security engineers, analysts, and testers
- Application developers / testers

Pre-requisites:
- General awareness of business management processes
- Basic computing knowledge
- General computing skills with access to a Linux environment for labs

Industrial Cybersecurity (ICS/SCADA)

Duration	4 Days
Delivery	ILT / VILT
Exam	ICS/SCADA

Course Outline:
This training prepares participants to defend Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) environments against cyber threats. It emphasizes both strategic understanding and practical skills to analyze risk, defend OT networks, and counter attacks in industrial contexts. The course includes labs and exercises that simulate real-world attack and defense scenarios, teaching attendees to think like attackers to better protect critical infrastructure.

Learning Objectives:
- Explain ICS/SCADA architecture, risk elements, and security challenges
- Analyse and model risk in ICS/SCADA environments
- Understand TCP/IP fundamentals and industrial protocol vulnerabilities
- Simulate common attack methodologies and intrusion tactics
- Manage vulnerability assessments specific to ICS/SCADA systems
- Apply relevant standards and regulatory frameworks (e.g., IEC 62443, NIST SP 800-82)
- Design and secure ICS networks and OT defences
- Implement intrusion detection and prevention strategies

Who Should Enroll:
- Professionals responsible for securing or managing industrial networks and operational technology (OT)

Pre-requisites:
- Basic cybersecurity awareness
- Familiarity with IT infrastructure concepts
- Practical IT networking knowledge

AFRICA | NIL

AI Certifications

Certified AI Program Manager (CAIPM)

Duration	3 Days
Delivery	ILT / VILT
Exam	CAIPM

Course Outline:
This course is designed for professionals who need to lead, govern, and operationalise AI initiatives, it is a business-focused programme that bridges the gap between AI technology and organisational execution, equipping learners to align AI adoption with strategy, governance, risk management, change management, and measurable business outcomes while driving innovation, operational efficiency, and ROI.

Learning Objectives
- Explain core AI, machine learning, and generative AI
- Assess organisational readiness and maturity for AI
- Identify and prioritise AI use cases aligned to business goals
- Develop AI strategies, governance models, and roadmaps
- Apply change management principles
- Evaluate AI platforms, tools, vendors, and integration needs
- Implement AI governance, risk, ethics, and compliance
- Measure AI programme success using KPIs and ROI frameworks

Who Should Enroll:
- Programme and project managers leading AI initiatives
- Digital transformation and innovation leaders
- IT managers and technology strategists
- Business and operations managers driving AI adoption

Pre-requisites:
- General business, IT, or project management experience
- Basic understanding of digital transformation concepts
- Familiarity with AI or generative AI terminology and workflows
- Interest in enterprise AI governance, strategy, and operationalisation

Certified Offensive AI Security Professional (COASP)

Duration	3 Days
Delivery	ILT / VILT
Exam	COASP

Course Outline:
This course equips cybersecurity professionals with the skills to identify, exploit, test, and defend vulnerabilities in AI systems, large language models (LLMs), and agentic AI environments. The programme focuses on offensive AI security methodologies including prompt injection, adversarial machine learning, AI reconnaissance, model exploitation, and AI infrastructure hardening.

Learning Objectives
- Explain AI attack surfaces, threat models, and offensive AI security methodologies
- Perform AI reconnaissance and map AI system attack surfaces using OSINT techniques
- Identify and exploit vulnerabilities in LLMs, AI agents, APIs, and AI pipelines
- Conduct prompt injection, jailbreaking, and output manipulation attacks
- Apply adversarial machine learning and model extraction techniques
- Assess AI infrastructure for security risks
- Implement AI red teaming methodologies

Who Should Enroll:
- Penetration Testers and Ethical Hackers
- AI/ML Engineers and GenAI Developers
- AI Security Architects and Security Engineers

Pre-requisites:
- Foundational cybersecurity knowledge and security operations experience
- Basic understanding of penetration testing or ethical hacking concepts
- Familiarity with AI, machine learning, or LLM technologies

Certified Responsible AI Governance & Ethics (CRAGE)

Duration	3 Days
Delivery	ILT / VILT
Exam	CRAGE

Course Outline:
This training equips professionals to design, implement, and manage enterprise AI governance frameworks that align with global regulations, ethical standards, and organisational risk management requirements. The course focuses on responsible AI practices across the full AI lifecycle, enabling organisations to operationalise AI with accountability, transparency, compliance, and stakeholder trust.

Learning Objectives:
- Explain core principles of responsible AI governance, ethics, and accountability
- Develop AI governance frameworks aligned to enterprise and regulatory requirements
- Conduct AI risk assessments, impact analysis, and governance evaluations
- Identify and mitigate AI bias, transparency, privacy, and compliance risks
- Apply global AI governance standards including NIST AI RMF and ISO/IEC 42001
- Design AI policies, controls, audit mechanisms, and oversight processes
- Implement AI incident response, monitoring, and continuous governance practices
- Align AI initiatives with organisational strategy, stakeholder trust, and regulatory readiness

Who Should Enroll:
- Chief Privacy Officers and Data Protection Officers
- AI Programme Managers and Transformation leaders
- Legal, policy, and ethics advisors involved in AI oversight

Pre-requisites:
- General understanding of governance & compliance functions
- Familiarity with data governance concepts
- Interest in AI, ethics, governance, and regulatory frameworks

Executive Courses

Associate CISO Certification

Duration	5 Days
Delivery	ILT / VILT
Exam	CCISO

Course Outline:
This executive-level certification is designed to prepare senior cybersecurity professionals for C-suite leadership roles. It focuses on integrating the Certified Chief Information Security Officer (CCISO) Body of Knowledge across the five principal domains:

- Governance and Risk Management
- Information Security Controls and Audit Management
- Security Program Management and Operations
- Information Security Core Competencies
- Strategic Planning, Finance, Procurement, and Vendor Management

It blends information security governance, risk management, controls, audit, operational leadership, strategic planning, and financial management into a cohesive executive skill set. Unlike purely technical certifications, CCISO emphasises the application of security principles from a business and management perspective, equipping participants to align information security strategy with overarching organisational objectives, communicate effectively with executives and boards, and lead complex security portfolios.

The curriculum was developed by experienced CISOs to bridge the gap between technical competence and executive leadership, enabling practitioners to transition from operational or mid-management roles to strategic decision-making positions at the highest organisational levels.

Pre-requisites:

- Five years of experience in each of the five CCISO domains, verified via application: or
- Five years of experience in at least three of the domains combined with authorised training; or
- Progress through the Associate CCISO pathway if foundational experience is still being accumulated.

Who Should Enroll:

- Senior cybersecurity managers and directors
- Security architects and senior practitioners
- IT and leaders in digital transformation

Learning Objectives

Domain 1: Governance and Risk Management

- Establish and oversee enterprise information security governance structures
- Define, assess, and manage cybersecurity risk in alignment with business objectives and risk appetite
- Integrate regulatory, legal, and compliance requirements into security strategy
- Develop risk metrics and dashboards for executive and board-level reporting
- Enable informed executive decision-making through structured risk analysis

Domain 2: Information Security Controls, Compliance, and Audit Management

- Design and evaluate administrative, technical, and physical security controls
- Align control frameworks with industry standards and regulatory expectations
- Lead internal and external audit initiatives and remediation programs
- Oversee compliance management and continuous control improvement
- Communicate control effectiveness and audit outcomes to senior leadership

Domain 3: Security Program Management and Operations

- Lead enterprise-wide security programs and operational security functions
- Direct incident response, crisis management, and business continuity efforts
- Develop and enforce security policies, standards, and operating procedures
- Measure security program performance using KPIs and maturity models
- Coordinate security operations across IT, business units, and third-party providers

Domain 4: Information Security Core Competencies

- Apply foundational security principles across infrastructure, applications, data, and cloud environments
- Interpret threat intelligence, vulnerability trends, and attack methodologies at an executive level
- Guide secure architecture and design decisions without deep technical dependency
- Translate technical risk into business impact for non-technical stakeholders
- Ensure security is embedded across digital transformation initiatives

Domain 5: Strategic Planning, Finance, Procurement, and Vendor Management

- Align information security strategy with organisational vision and long-term goals
- Develop and manage security budgets, cost models, and investment justifications
- Integrate security requirements into procurement and contract negotiations
- Assess and manage third-party and supply-chain cybersecurity risk
- Build multi-year security roadmaps that support business growth and resilience

Upon completion, participants will be prepared to:

- Operate effectively at the C-suite and board level
- Lead enterprise cybersecurity strategy and governance
- Balance risk, compliance, cost, and operational effectiveness
- Fulfill the responsibilities of a Chief Information Security Officer

Executive Courses

CISO Certification

Duration	5 Days
Delivery	ILT / VILT
Exam	CCISO

Course Outline:
This executive-level certification is designed to prepare senior cybersecurity professionals for C-suite leadership roles. It focuses on integrating the Certified Chief Information Security Officer (CCISO) Body of Knowledge across the five principal domains:

- Governance and Risk Management
- Information Security Controls and Audit Management
- Security Program Management and Operations
- Information Security Core Competencies
- Strategic Planning, Finance, Procurement, and Vendor Management

It blends information security governance, risk management, controls, audit, operational leadership, strategic planning, and financial management into a cohesive executive skill set. Unlike purely technical certifications, CCISO emphasises the application of security principles from a business and management perspective, equipping participants to align information security strategy with overarching organisational objectives, communicate effectively with executives and boards, and lead complex security portfolios.

The curriculum was developed by experienced CISOs to bridge the gap between technical competence and executive leadership, enabling practitioners to transition from operational or mid-management roles to strategic decision-making positions at the highest organisational levels.

Pre-requisites:

- Five years of experience in each of the five CCISO domains, verified via application: or
- Five years of experience in at least three of the domains combined with authorised training; or
- Progress through the Associate CCISO pathway if foundational experience is still being accumulated.

Who Should Enroll:

- Senior cybersecurity managers and directors
- Security architects and senior practitioners
- IT and leaders in digital transformation

Learning Objectives

Learning Objectives:

Domain 1: Governance and Risk Management

- Explain the role of governance frameworks in establishing effective information security oversight
- Identify and assess enterprise cybersecurity risks aligned to business objectives and risk appetite
- Apply risk management methodologies to prioritise security initiatives and investments
- Interpret legal, regulatory, and compliance requirements affecting information security programs
- Support executive-level risk reporting and decision-making

Domain 2: Information Security Controls and Audit Management

- Evaluate the effectiveness of administrative, technical, and physical security controls
- Align security controls with recognised standards and frameworks
- Understand internal and external audit processes and their impact on security posture
- Support audit planning, evidence collection, and remediation tracking
- Communicate audit findings and control gaps to executive stakeholders

Domain 3: Security Program Management and Operations

- Understand how enterprise security programs are structured, governed, and managed
- Contribute to the development and execution of security policies, standards, and procedures
- Support incident response, business continuity, and crisis management activities
- Measure and report security program performance using metrics and KPIs
- Coordinate operational security activities across IT, business units, and third parties

Domain 4: Information Security Core Competencies

- Understand foundational security concepts including threat landscapes, vulnerabilities, and attack vectors
- Apply security principles across network, application, data, and endpoint domains
- Support secure architecture and design decisions from a leadership perspective
- Interpret technical security information for non-technical executives
- Bridge the gap between technical teams and executive leadership

Domain 5: Strategic Planning, Finance, Procurement, and Vendor Management

- Align information security strategy with organisational goals and digital transformation initiatives
- Participate in security budgeting, cost justification, and return-on-investment discussions
- Understand procurement processes and integrate security requirements into vendor selection
- Assess third-party and supply-chain security risks
- Support long-term security roadmaps and executive-level strategic planning

AFRICA | NIL

OUR CONTACT INFO

+27 (0)87 086 3550

www.nil.co.za

salesadmin@nil.co.za

NIL Data, Ground Floor, Building 2, The Ingress,
23 Magwa Crescent, Waterfall City, Midrand