# Table of content

**CRASH COURSES**

- CNC1001 — Cyber security awareness
- CNC1002 — Crisis management strategies
- CNC1003 — Cyber security governance
- CNC1004 — OWASP top 10 vulnerabilities

**TRAININGS**

- CNT1101 — Cyber security fundamentals for IT
- CNT1102 — Cyber security threats and vulnerabilities
- CNT1201 — SIEM implementation
- CNT1202 — IDS / IPS deployment and operation
- CNT1203 — Cyber threat intelligence
- CNT1301 — Digital forensics and investigation
- CNT1302 — Advanced penetration testing
- CNT1303 — Introduction to malware analysis
- CNT1304 — Web security vulnerabilities analysis
- CNT1313 — Malware analysis and reverse engineering

**SCENARIOS**

- CNS1403 — Red team / Blue team exercise
- CNS1404 — Incident response management
- CNS1405 — CTF hacking

**PROGRAMS**

- CNP1601 — Certified CISO executive program
- CNP1008 – Bootcamp
CYBER NODE

Crash courses
CRASH COURSES

Code: CNC1001

Cyber security awareness

Introduction
This course aims to provide a high-level awareness on cyber security attacks, main concepts, regulations and protection. Participants will learn the key concepts and skills needed to understand security awareness and the cyber threat. The course is particularly suitable for individuals with limited cyber security experience wanting to understand how to protect themselves should an attacker or attackers target them.

Course content
• History of significant events in cyber security
• Definitions and standards of cyber security
• Network security, systems security and applications security
• The cyber kill chain and stages of a cyber-attack
• Differentiate between the different types of malicious software
• Vulnerability analysis and management
• Regulations and policies
• Several demonstrations of cyber-attacks
• Gain insight into legal issues and incident handling

Learning outcomes
• Demonstrate and understanding of cyber security concepts and the most effective way to manage your organizations awareness
• Demonstrate an understanding of the difference between awareness, education, and training
• Demonstrate an understanding of cyber threats and describe the most common techniques used for cyber-attacks

Prerequisites
• There are no prerequisites for this course; however, participants should have a basic understanding of computers and the internet

Duration
• One (1) day
Crisis management strategies

Introduction
This course aims to teach participants how an effective crisis management plan can protect enterprises from failure if a disaster occurs. Participants will explore the methods and tools used as the basis for crisis management. Participants will also learn the crisis management methodology, how to build an effective crisis management team, how to communicate when a crisis occurs and how to test the crisis management plan.

Course content
• Crisis management planning methodology
• Building an effective crisis management team
• Assessing threats and risks
• Setting up indicators and identifying incidents
• Prioritizing decisions and activities
• Communicating/coordinating with internal parties, external agencies and local authorities
• Testing and exercising the crisis management plan

Learning outcomes
• Demonstrate and understanding of dealing with emergencies that could lead to a variety of disruptive events or potential crisis within your environment
• Describe how to apply practical crisis management tools and techniques
• Determine best practices and processes to reduce cyber risks to enhance an organizations resilience

Prerequisites
• There are no prerequisites for this course

Duration
• One (1) day
Cyber security governance

Introduction
This course aims to introduce participants to risk management in concerning cyber security and teach attendees the necessary skills to perform a risk assessment. The course provides education on introductory concepts in concerning to Governance, Risk and Compliance (GRC) that the participants can then use, to improve their cyber security programs.

Course content
- Cyber security governance, risk management and compliance
- Cyber security management and maturity assessment
- Cyber security risk assessment, analysis, and treatment plans
- Cyber security incident management

Learning outcomes
- Describe the key concepts and importance of cyber security
- Present the fundamental processes that enable an organization at enterprise level to manage cyber security
- Demonstrate understanding of the critical concepts of Governance, Risk, Management and Compliance (GRC)
- Demonstrate an ability to define the elements of risk management and risk assessment

Prerequisites
- There are no prerequisites for this course

Duration
- One (1) day
Introduction
This course aims to improve the participants understanding of web application vulnerabilities and apply the most appropriate security measures to defend web assets. The course will cover the Top 10 most critical security risks to web applications, based on the 2021 Edition of the Open Web Application Security Projects (OWASP) Top 10 Standard.

Course content
• History of major events in cyber security
• Definitions of cyber security
• Security of web architectures and web applications
• The stages of cyber-attack
• Web penetration-testing methodology
• Vulnerability analysis tools for web applications
• Demonstrations of cyber-attacks

Learning outcomes
• Gain an insight into web applications security
• Understand the OWASP projects and concepts
• Identify web penetration testing tools and methodology
• Gain skills in vulnerability assessment and analysis tools

Prerequisites
• Fundamental knowledge of web development and web server architecture

Duration
• One (1) day
Trainings
Introduction
The objective of the course is to enable participants to focus on the fundamental concepts of cyber security and raise the awareness of IT professionals. The course is particularly suitable for individuals who are part of an IT team. General security practitioners, system administrators, IT professionals and security architects will benefit by understanding how to design, build, and operate their systems to mitigate cyber-attacks.

Course content
Introduction to cyber security
• History of significant events in cyber security
• Definitions and references of cyber security
• Stages of a cyber-attack

Risks and threats management
• Ensures compliance with the changing laws and applicable regulations
• Constant updates on the cyber security strategy to leverage new technology and threat information
• Critical concepts of enterprise security
• Provides security policy to the relevant authority to ensure its enforcement
• CIA Triad, privacy, reliability, repudiation, and access control

Network security, systems security and applications security
• Hardening best practices
• Exchanges and data security
• Vulnerability analysis tools
• Product and technologies (AV, IDS, IPS, SIEM)

Crisis management
• Crisis management planning methodology
• Assessing threats and risks
• Prioritizing decisions and activities

Learning outcomes
• Define what cyber security is
• Gain awareness into network security
• Differentiate between different types of malware
• Gain an insight into the legal issues and incident handling
• Establish effective security metrics that the IT department can implement, auditors can validate, and executives can understand
• Describe information security topics, terms, technologies and concepts
• Assimilate and apply the Confidentiality, Integrity and Availability (CIA) for prioritization of critical security resources
• Describe system hardening
• Define system patching
• Determine the approach used by many computer attackers

Prerequisites
• Basic knowledge of cyber security
• Familiar with IT functions and IT organizations

Duration
• Four (4) days
Code: CNT1102

Cyber security threats and vulnerabilities

Introduction
The objective of the course is to enable participants to understand cyber threats, learn and use typical ethical hacking techniques to assess the impacts of hacking and ensure that systems are sufficiently protected to mitigate the impacts of a cyber-attack.

Course content
Risks and threats
- History
- Cyber security needs
- Legislation
- Audit methodologies

Reconnaissance
- Reconnaissance on the Internet
- Reconnaissance on files
- Reconnaissance on LAN
- Countermeasures

Scanning
- Port scanning using Nmap
- Packet forging using Scapy
- Vulnerability scanning using OpenVAS
- User enumeration
- Countermeasures

Exploitation techniques
- Exploitation fundamentals
- A focus on Metasploit Framework
- Countermeasures

Intrusion on Wi-Fi Networks
- Introduction to wireless networks
- Network discovery and sniffing
- Cryptographic attacks
- Other intrusion methods
- Countermeasures

Passwords Attacks
- Passwords and authentication
- Principles and techniques
- Putting these techniques into practice
- Countermeasures

Web Applications Vulnerabilities
- Vulnerability detection
- Common vulnerabilities
- Command injection
- Countermeasures

Learning outcomes
- Describe the legal aspects of cyber-attacks
- Apply networks penetration-testing methodology
- Explain network-scanning techniques
- Describe vulnerability assessment techniques
- Define intrusion and attack methods
- Apply network exploitation techniques
- Demonstrate understanding of password attack techniques
- Describe web and Wi-Fi attack techniques
- Apply common hardening rules to enhance security

Prerequisites
- Foundational knowledge of the Open Systems Interconnection (OSI) model
- Foundational knowledge of TCP/IP and networking protocols
Prerequisites continued

- Foundational knowledge of Windows operating systems
- Foundational knowledge of UNIX / Linux operating systems
- Foundational knowledge of cyber security threats and attack methods
- Further to the above knowledge, a recommended pre-requisite is to attend the (CNT1101) cyber security fundamentals for IT course before this course

Duration

- Five (5) days

---

1 As of January 2022, all 5-day courses have been adjusted to comply with the new 4.5 day working week, as per UAE regulations.
SIEM implementation

Introduction
The objective of the course is to highlight the benefits of deploying a Security Incident and Event Management (SIEM) within an IT environment. The course will provide participants with the knowledge, methodology and processes to solve logging problems and monitor cyber threats and attacks via SIEM infrastructure.

Course content
Introduction to SIEM
• Definition and concepts
• Design
• Components and architecture

SIEM Architecture
• Log definition and concepts
• Types of logs and agents
• Log aggregation
• Log broker
• Log storage
• Log visualisation, search and alert

Tactical analysis
• Service profiling
• Endpoints analytics
• Baselining and user behaviour

Learning outcomes
• Analyze standard alerts and prioritization
• Determine the log data necessary to establish security control effectiveness

Prerequisites
• Foundational knowledge of the Open Systems Interconnection (OSI) model
• Foundational knowledge of TCP / IP and networking protocols
• Foundational knowledge of Windows operating systems
• Foundational knowledge of UNIX / Linux operating systems
• Foundational knowledge of cyber security threats and attack methods
• Foundational knowledge of digital forensic concepts

Duration
• Four (4) days
IDS / IPS deployment and operation

Introduction

The objective of the course is to deliver technical knowledge, awareness and hands-on Intrusion Detection and Prevention Systems (IDS/IPS). The course will provide clear understanding of how to instrument your network and enable participants to perform detailed incident analysis and reconstruction.

Course content

Introduction to IDS/IPS
• What is an IDS / IPS
• Types of IDS / IPS
• Alert classification

IDS/IPS deployment
• Deployment strategy
• Suricata introduction
• Wazuh introduction

Configuration and administration
• Detection strategy and rule writing
• NIDS (Suricata)
• HIDS (Wazuh)

Limitations and bypass techniques
• Sensor and ruleset management
• Adversary techniques

Learning outcomes
• Understand and analyze IDS/IPS traffic to mitigate threats
• Identify potentially malicious activities
• Hands-on practice on detection and analysis

Prerequisites
• Foundational knowledge of the Open Systems Interconnection (OSI) model
• Foundational knowledge of TCP / IP and networking protocols
• Foundational knowledge of Windows operating systems
• Foundational knowledge of UNIX / Linux operating systems
• Foundational knowledge of cyber security threats and attack methods
• Foundational knowledge of Security Information and Event Management (SIEM) systems
• Foundational knowledge of digital forensic concepts

Duration
• Three (3) days
Cyber threat intelligence

Introduction
This course aims to provide participants with the knowledge and techniques to understand and counter cyber security threats and attacks effectively. Furthermore, this course allows participants to understand the critical cognitive processes that govern investigatory tasks, the technologies and the platforms, to perform cyber threat intelligence.

Course content
Introduction to cyber threat
- Cyber threats critical review
- Cyber threat Intelligence
- Indicators and their life cycle
- Threat profiling through their TTP

Collecting evidence, share and produce intelligence
- The investigation process and principles
- Rate sources and collect observables
- The STIX and TAXII models

Cyber threat platform
- How to use a cyber-threat intelligence platform
- Best practice for cyber-threat platform in intelligence
- Use of Open CTI (gathering and feeding)

Reasoning behind successful investigations
- Make inferences and reasoning modes
- Avoid cognitive biases

Cyber threat intelligence in action
- Report findings and reporting
- Relate geopolitical context with cyber security events
- Use indicators for network detection
- Match malware samples with YARA

Learning outcomes
- Understand the definition and usage of cyber threat intelligence
- Understand the differences between threat data and threat intelligence
- Design a cyber-threat intelligence platform
- Create structured analytical techniques, perform detection, respond and defeat targeted threats
- Validate information received to minimize the costs of bad intelligence

Prerequisites
- Foundational knowledge of IP network and TCP/IP protocols
- Foundational knowledge of Windows operating systems
- Foundational knowledge of UNIX/Linux operating systems
- Foundational knowledge of security Information and Event Management (SIEM) Systems
- Foundational knowledge of forensics incident response and digital concepts
- Further to the above knowledge, recommended pre-requisites are to attend the (CNT1201) SIEM implementation & deployment and the (CNT1202) IDS/IPS deployment and operations courses before this course

Duration
- Four (4) days
Introduction

This course provides participants with the necessary skills and knowledge to understand digital forensic and related incident response and investigation methodologies. This course enable participants to carry out essential actions to recover exploitable information, collect clues, complete practical analysis and respond effectively to incidents.

Course content

Introduction to digital forensics
- Digital forensics in today’s world
- Digital investigation process
- Best practices

Malwares awareness
- Malware and infections
- Digital forensics in a compromised environment

Data structuring and acquisition
- Overview of storage media
- Data acquisition
- Static data acquisition
- Volatile data acquisition
- Acquisition in virtual environments

Data structuring and acquisition
- Data recovery from deleted partitions
- Analysis of volatile evidence
- Analysis of non-volatile evidence
- Log analysis
- Network capture and forensics

Anti-forensic methods
- Techniques, attacks and countermeasures

Digital forensics global best practices
- Data structuring and acquisitions overview of storage media

Learning outcomes
- Describe the legal aspects and forensic investigation rules, standard forensic investigation methods and information analysis techniques
- Discover information recovery techniques
- Demonstrate an understanding of investigation techniques, recovery and analysis tools, incident response processes and procedures
- Discover best practices to interact with qualified organizations, digital forensics principles and processes

Prerequisites
- Foundational knowledge of TCP / IP and networking protocols
- Foundational knowledge of Windows operating systems
- Foundational knowledge of UNIX / Linux operating systems
- Foundational knowledge of cyber security threats and attack methods
- Foundational knowledge of Security Information and Event Management (SIEM) systems
- Foundational knowledge of malware analysis and reverse engineering
- Foundational knowledge of incident response and digital forensic concepts
Prerequisites continued

• Further to the above knowledge, a recommended pre-requisite is to attend the (CNT1203) cyber threat intelligence course before this course.

Duration

• Four (4) days
Introduction
This course aims to provide participants with the necessary skills and knowledge to obtain the ethical hacking and penetration testing techniques, specifically targeting those with prior experience in this field of cyber security. This course provides advanced in-depth knowledge of attacks, coupled with hands-on scenarios and practical exercises.

Course content
Cyber security basics
• Penetration testing concepts and tools

Network vulnerabilities
• Idle host scanning
• Network sniffing and spoofing
• Hijacking

Attacks on secured protocols
• DOS / DDOS
• HeartBleed / SSL Strip
• Firewalls
• Port scan
• Antivirus and IDS bypass techniques

Client vulnerabilities
• Intrusion signs
• Malware
• RAM analysis

System vulnerabilities
• Persistence / backdoor
• Privilege escalation
• Windows / Linux passwords
• Web vulnerabilities
• Integrity controls / Intrusion detection

Learning outcomes
• Gain skills on network advanced scanning techniques, network exploitation, intrusion and attack methods, network devices, assess network application protocols and the standard hardening rules to apply
• Apply the required techniques to assess new vulnerabilities and the applications running on Linux and Windows systems
• Model the techniques used by attackers to perform attacks
• Develop advanced quantitative and qualitative risk assessments through validation

Prerequisites
• Intermediate knowledge of TCP / IP and networking protocols
• Intermediate knowledge of Windows operating systems
• Intermediate knowledge of UNIX / Linux operating system
• Intermediate knowledge of cyber security threats and attack methods
• At least two (2) years experience in penetration testing
• Further to the above knowledge, a recommended pre-requisite is to attend the (CNT1203) cyber threat intelligence course before this course

Duration
• Five (5) days

---

1 As of January 2022, all 5-day courses have been adjusted to comply with the new 4.5 day working week, as per UAE regulations.
Introduction to malware analysis

Introduction
This course aims to build a strong foundation for participants to understand malicious software behaviours, analysis methods, signatures, foundational malware reverse engineering, and detect and protecting environments from malwares. Furthermore, the course examines malicious software, concepts, and threat intelligence and teaching participants how to respond to cyber security incidents, to ensure systems have improved protection from and against cyber attacks and threats.

Course content
Malwares concept
• Module objectives
• Definitions of malware and malware analysis
• Types, evolution and popular examples of malware
• Malware attack type statistics and objectives and goals of malware attacks
• Types of malicious attackers and malware analysis
• Infection vectors and symptoms of infected systems
• Preventing malware infections
• Malware indicators

Malware analysis
• Malware analysis process
• Anti-virus vs. anti-malware
• Technical analysis types and evasion techniques
• Identifying malware
• Intelligence & resource databases and malware analyst toolboxes

Malware eradication and remediation
• Incident handling, preparation, detection and analysis, containment, eradication & recovery, documentation and lessons learned

Learning outcomes
• Create and analyze different types of malwares
• Demonstrate understanding of how to detect and react to malware infection
• Gain a foundational understanding of malware analysis and reverse engineering
• Gain an understanding of identifying and detecting malicious software

Prerequisites
• Foundational knowledge of TCP / IP and networking protocols
• Foundational knowledge of Windows operating systems
• Foundational knowledge of UNIX / Linux operating systems
• Foundational knowledge of cyber security threats and attack methods
• Foundational knowledge of development and programming
• Foundational knowledge of digital forensic and incident response concepts

Duration
• Two (2) days
Web security vulnerabilities analysis

Introduction
This course is designed to improve participants' understanding of web application vulnerabilities and providing education on how to apply the correct security measures to defend web assets. The course will raise awareness of web attacks and cover the most critical vulnerabilities, based on the top 10 most critical security risks to web applications per the Open Web Application Security Projects (OWASP) standard.

Course content
Risks and threats
- International legislation
- Types of attacks according to web architectures

Analysis and research of vulnerabilities
- Methods to obtain information
- Using the ethical hacker toolkit
- Authentication
- Session mechanism
- Access control
- Injection (SQL, OS command)
- Encryption
- Attack by injection of XSS and CSRF code
- Best practices on the use of framework and libraries

Security rules
- Protection of architectures and operating systems
- Strengthen authentication, session mechanisms and access control
- Apply security on databases
- Apply encryption protocols (SSL/TLS)

- Define an input validation strategy to fight against injections
- Define a secure environment

Learning outcomes
- Demonstrate an in-depth understanding of the OWASP standard, its concepts and defined critical security risks
- Gain an understanding of web penetration testing tools, methodology, web applications security, vulnerability assessment and analysis

Prerequisites
- Foundational knowledge of TCP/IP and networking protocols
- Foundational knowledge of Windows operating systems
- Foundational knowledge of UNIX/Linux operating systems
- Foundational knowledge of web application and database programming languages
- Foundational knowledge of cyber security threats and attack methods

Duration
- Four (4) days
Code: CNT1313

Malware analysis and reverse engineering

Introduction
This course builds a strong foundation for participants who want to learn how malware analysis and reverse engineering of software occurs. This advanced course improves the skills and knowledge of participants focusing on the inner in-depth working of malware, tools used by malware analysts, processes for reversing different types of malware and how to detect and protect from malwares.

Course content
x86 system architecture
- Assembler (x86)
- Reverse engineering basics
- How to build your own toolbox
- OSINT malware detection and rules

Reverse engineering and how to proceed
- Disassembler
- User and kernel mode debuggers
- Common binary file formats
- Dynamic analysis tools
- Network analysis tools
- Static and dynamic analysis
- Packers
- Cryptography
- Anti-debugger / Anti VM
- Command and Control (C&C)

Learning outcomes
- Demonstrate the ability to analyze malware, how it works and create rules for detection
- Demonstrate the ability to analyze shellcode
- Describe software exploits and threat
- Demonstrate the ability to analyze packed and obfuscated code
- Demonstrate the ability to be able to apply the reverse engineering skills necessary to dissect and analyze malware

Prerequisites
- Intermediate knowledge of assembly language
- Intermediate knowledge of networking protocols
- Intermediate of operating systems
- Intermediate knowledge development and programming
- Intermediate knowledge of x86 and x64 system architecture
- Intermediate knowledge of cyber security and digital forensics
- Intermediate knowledge of threat analysis
- Further to the above knowledge, a recommended pre-requisite is to attend the (CNT1303) introduction to malware analysis course before this course

Duration
- Three (3) days
Red team / Blue team exercise

Introduction
To keep business processes secure, operators need to know how to anticipate, prevent and defend against threats to their systems. In this team-based workshop, participants will form two teams of five (5) participants, experiencing what it is like to be, a Red team and a Blue team. For the first half of the course, and as a member of the Red Team, participants will attack a specifically designed simulated real-world infrastructure, attempting to breach the environment while capturing “flags”. Subsequently, in the second half of the course, while a member of the Blue team, participants will use their skills to investigate a previously occurred attack, investigate and document it, and learn to protect it from future attacks.

Workshop content
- Scenario explanation
- Infrastructure recognition
- Vulnerabilities
- Scanning detection
- Debriefing and pooling
- Security, detection, protection and monitoring
- Attack scenario from the inside for example, phishing, USB key
- Forensic analysis and C&C identification
- Exchange between Red/Blue team, general debriefing
- Explanation of expected attacks from Red team
- Explanation of security and detection expected from Red/Blue team

Learning outcomes
- Demonstrate an enhancement to leadership and team playing skills while developing new and improving existing communication, offensive and defensive techniques
- Explain the importance and form a greater understanding of the risks associated with cyber-attacks on IT and OT systems, all while under pressure from a series of increasingly complex scenarios

Prerequisites
- Intermediate knowledge of TCP / IP and networking protocols
- Intermediate knowledge of Windows operating systems
- Intermediate knowledge of UNIX / Linux operating systems
- Intermediate knowledge of cyber security threats and attack methods
- Intermediate knowledge of system architectures and enterprise environments
- Intermediate knowledge of malware and threat analysis
- Intermediate knowledge of digital forensics and incident investigations
- At least four (4) years experience in penetration testing

Duration
- Three (3) days
Incident response management

Introduction
This scenario-based learning approach aims to enhance participant skills; in hunting, identifying, handling and recovering from threats within an enterprise. This scenario is highly interactive and structured. Participants will also learn how to detect an attack in progress, perform threat hunting and acquire skills specific to incident handling, detection and analysis, containment, eradication & recovery, and post-incident activity processes.

Course content
• Multiple incident response scenarios
• Policy and processes
• Incident handling and response
• Analysis of the attacks carried out by SME trainers

Learning outcomes
• Gain skills to detect breaches, incident handling and recovery
• Ability to identify and analyze affected systems, perform incident assessments, determine modifications to systems to handle and mitigate incidents

Prerequisites
• Intermediate knowledge of cyber and information security
• Intermediate knowledge of digital forensics and incident response concepts and techniques
• Intermediate knowledge of Security Incident and Event Management (SIEM) systems and infrastructure

Duration
• Four (4) days
Introduction
Capture-the-flag (CTF) is a team-based competition in which participants use their advanced knowledge, skillsets, cyber security tools and techniques to find hidden clues or "flags". Each team attacks the other team's system while defending their own during these exercises. Participants will engage in challenges related to hacking techniques and penetration testing.

Course content
Presentation of the challenge and the platform
• Challenges in relation to different areas
• Penetration testing benefits
• Types
• Methodology
• Forensics
• Network
• Cryptography
• Web client and server
• Steganography
• Reverse engineering

Learning outcomes
• Gain and improve skills in ethical hacking techniques
• Improve and enhance their problem-solving skills
• Undertake knowledge sharing on each aspect of the challenge
• Gain much-needed hands-on experience and practice of advanced penetration testing techniques

Prerequisites
• Advanced knowledge of cyber security
• Advanced knowledge of penetration testing
• Advanced knowledge of digital forensics and incident response
• Intermediate knowledge of software and system development and programming

Duration
• Three (3) days
Programs

CYBER NODE
Certified CISO executive program

**Introduction**
The certified CISO executive program helps candidates better understand the CISO’s role and its challenges within the field. Students will be given the chance to engage with CISO experts and learn skills required to be an effective CISO professional in real life settings. Students will also have the opportunity to form relationships with peers in similar positions and build their networks during the cohort. The program is co-administrated by Thales, CINI, and CCSIRS.

**Course content**

- **Week 1**
  - Day 1 – CISO’s role
  - Day 2 – ISR implementation process
  - Day 3 – Information assurance and risk management

- **Virtual week**
  - Day 1 – Artificial intelligence and emerging technologies
  - Day 2 – Cybersecurity for ICS, OT & IOT systems
  - Day 3 – Cloud security

- **Week 3**
  - Day 1 – Enterprise cybersecurity strategy
  - Day 2 – Cyber threat intelligence
  - Day 3 – Digital transformation security challenges

- **Week 4**
  - Day 1 – Cyber resilience, business continuity and readiness
  - Day 2 – Crisis management and incident handling
  - Day 3 – Tabletop exercise

- **Week 5 - Executive week**
  - Day 1 – Strategic planning, finance, procurement, and third-party management
  - Day 2 – Building a culture of cybersecurity
  - Day 3 to 5 – Use cases workshop

**Prerequisites**
- All candidates qualified to the certified CISO executive program must have at least five years of relevant managerial experience and be C-level or above to be considered

**Selection process**

- **Phase 1: Candidates submit interest & CV**
  - The CISO jury committee will evaluate candidates’ profile/CV and short-list selected candidates for interview

- **Phase 2: Interview**
  - The short-listed candidates are invited to complete a face-to-face interview on-site with jury members

- **Phase 3: Pre-assessment**
  - Following the interview, candidates will need to complete a self-evaluation via 30 multiple choice questions

**Duration**
- 5 months (only 1 week, per month)
- Course timings: 8:00am - 3:30pm
Bootcamp

Introduction
This program offers recent graduates a way to advance their knowledge within the field of cyber security. As well as, market themselves as desirable candidates for recruitment into government roles. The program provides guidance for further upskilling within the domain of cybersecurity.

Course content
- Welcome, introduction and motivation
- So, you want to be a hacker...
- Networking fundamentals and secure networking
- Vulnerability and risk management
- Hacking the planet; well, not quite...
- Cryptography – Part 1 and access control
- Cryptography – Part 2, PKI, certificates and secure mail
- Threat and open-source intelligence
- Application and website security
- Programming fundamentals for cyber
- Securing the enterprise
- Securing the cloud
- Securing the endpoint and human
- Dashboarding and reporting
- Legal and ethical issues
- Legislation, regulations, standards and frameworks
- Incident response and digital forensics
- Understand the governance perspective and how security frameworks and controls are applied
- Apply networks attack methodologies and conduct network exploitation, while understanding common vulnerabilities within web applications and the fundamentals of WAF
- Gain an understanding on security challenges within cloud environments, as well as understand the requirements to secure them
- Understand and write code following cyber security best practices and apply codes in various languages, while ensuring they are written securely
- Define intrusion and attack methods and conduct network exploitation
- Understand the definition of forensics, threat hunting and incident response. While analysing standard alerts and prioritization based on significance
- Understand SOC & SIEM and apply certain forensic techniques, as well as certain SOC related scenarios
- Understand encryption and obfuscation, as well as understanding its significance in cyber security
- Understand how to generate reports for various levels of management

Duration
- 4–6 weeks

Learning outcomes
- Define cyber security, network security, vulnerability assessment, intrusion, and attack methodologies