

**CYBER SECURITY COURSE FOR**

 **CAMBODIA LEA OFFICERS**

# Training Duration: 10 Days

**Course Details:**

**Course Duration:** 10 days

**Start Date : 02-11-2021 (Tuesday)**

**End Date : 14-12-2021 (Tuesday)**

# Learning Objective and Outcomes

**Objectives:**

The purpose of this course is to provide understanding of the main issues related to Cyber Security in modern cyber environment and computer systems. This covers various concepts related to Cyber Crime, Cyber Security Fundamentals, Cyber attacks & Network Threats, introduction to Incident Handling, Digital Evidence handling and analysis, handling and responding to Malware Incidents, SOPs, Mobile Forensics, Cryptography, Latest technological advancements in cyber security, threat hunting, Website investigations, Cyber Laws, Information Security Management and to provide adequate practical hands on during the training programme.

**Learning Outcomes:**

On completion of this course, participants should have gained a good understanding of the concepts of Cyber Security.

**Note:** Time in both IST (Indian Standard Time) and Cambodia Time

**CYBER SECURITY COURSE FOR CAMBODIAN Ph.D POLICE STUDENTS – CDTI, HYDERABAD**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No.** | **SESSION TIME / DURATION (IST) & CAMBODIAN TIME** |  **TOPIC** | **DATE** | **TRAINER** |
| **DAY – 1 - 02-11-2021 (Tuesday)** |
| **1** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Introduction to Cyber Crimes and Security** | [Theory]**Introduction to Course Content and Modern-Day Cyber Crime*** Cyber Crime : Scope, characteristics and landscape over the years and present scenarios in cyber space
* Cyber Crime : Conventional and Emerging Crimes (with case studies/instances)
* Cyber Threats: Cyber Warfare, Cyber Crime, Cyber Terrorism, Cyber Espionage
* Sources of security threats, motives, target assets and vulnerabilities
* Consequences of threats, email threats, web threats, intruders and hackers, inside threats
 | 02-11-2021(Tuesday) | **Mr. Venkatesh Murthy, Director, Data Security Council of India (DSCI), Karnataka****Mob: 9880512125****Venkatesh.murthy@dsci.in** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **2.** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Theory]**Introduction to Cyber Security Fundamentals*** Introduction to OSI Model
* Understanding of Security Elements: CIA Triad
* Non-Repudiation
* Authorization
* Authentication – types, policies and techniques
 | 02-11-2021(Tuesday) | **Mr. Sai Satish, Cyber Security Expert****Mob: 9618222220****saisatish@indianservers.com** |
| **TEA BREAK -** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **3.** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Theory]**Understanding of Cyber Attacks & Network Threats: Active/Passive Interference*** Worms
* Virus
* Spams
* Adware
* Spyware
* Malwares-Ransomwares and APTs
* Trojans and covert channels
* Backdoors, Keyloggers
* Bots
* IP, Spoofing, ARP Spoofing, Session Hijacking
* Steganography
* Sabotage, Internal threats and Environmental threats
 |  | **Mr. Sai Satish, Cyber Security Expert****Mob: 961822220** |
| **04-11-2021 (Thursday) – Indian Holiday (Diwali)** |
| **09-11-2021 (Tuesday) – Cambodian Holiday** |
| **DAY – 2 – THURSDAY – 11-11-2021** |
| **4.** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Incident Handling** | Quiz for 15 minutes[Theory]**Introduction to Incident Handling*** Preparation
* Identification
* Containment
* Eradication
* Remediation
* Lessons Learnt
 | 11-11-2021(Thursday) | **Mr. Vinod Babu, Cyber Security Practitioner & Trainer****Mob: 8919782172****bsvsvinod@gmail.com** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **5** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Theory]**Introduction to Incident Handling** …..Continued. | 11-11-2021(Thursday) | **Mr. Vinod Babu, Cyber Security Practitioner & Trainer****Mob: 8919782172****bsvsvinod@gmail.com** |
| **TEA BREAK -** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |
| **6.** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Theory]* Handling and Responding to Malware Incidents
* Email Security Incidents
* Network Security Incidents
* Web Application Security Incidents
* Cloud Security Incidents
* Insider Threats
 |  | **-Do-** |
| **DAY – 3 – TUESDAY – 16-11-2021** |
| **7.** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Digital Evidence** | Quiz for 15 minutes[Theory]**Introduction to Digital Evidence Handling*** Digital Evidence – Definition, characteristics, types, source of digital evidence, etc.
* Classification of Digital evidence – User created, user protected and system created
* Difference between volatile and non-volatile memory
* Traditional forensic evidence Vs. digital evidence
* Cyber Forensics – Definition, classification
* Cyber Forensics Vs. Traditional forensics
* Understand pre-requisite for search & seizure and first responder kits

**SOP on Scene of Crime Management*** Pre-search preparation and required forensic toolkit
* Procedure of digital evidence collection and preservation
* Chain of custody
* Seizure memos, preparing of legal documents, letters, etc.
 | 16-11-2021(Tuesday) | **Mr. Vishal Pawade, (MSc Phy.)**Assistant Director (Cyber Crime, Tape Authentication, and Speaker Identification Division)**FSL, Maharashtra****Mob: 9773183454****vishal.pawade24@gov.in** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **8.** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Throry] **Digital Forensic Analysis Methods*** Bit by Bit stream image analysis
* Hexadecimal Analysis
* Live Memory Analysis
* Triage Analysis
* Various open source tools such as Autopsy, FTK usage
* Various artefacts in Windows, Linux and Mac OS
 | 16-11-2021(Tuesday) | **Mr. Vishal Pawade, Assistant Director, FSL, Maharashtra****Mob: 9773183454****vishal.pawde24@gov.in** |
| **TEA BREAK -** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |
| **9.** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Practical Hands On]**Digital Evidence Analysis*** Forensic Imaging, hashing using FTK and Hardware Imaging Tools
* Forensic Analysis using Autopsy, Kape, SANS Sift, etc.
 | 16-11-2021(Tuesday) |  **Mr. Md. Nazim** **7207388016**mohdnazim282@gmail.com  |
| **DAY – 4 – TUESDAY – 23-11-2021** |
| **10** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Type of Digital Forensics** | Quiz for 15 minutes[Theory]**Mobile Forensics*** Mobile Devices related threats, vulnerabilities and countermeasures
* Mobile forensics – Mobile Forensics Definition, Information available in Mobile Phones, Memory Considerations in Mobiles, Subscriber Identity Module (SIM), IMEI, ICCID, IMSI, ESN, etc.
* SOP for handling of mobile devices, search and seizure of mobile devices
* Acquisition methods (physical, logical, file system, JTAG, Chip off),
* Analysis of mobile images, understanding a mobile forensic report
 | 23-11-2021(Tuesday) | **Mr. Chunduru Eswara Saiprasad, Assistant Director & Scientist C, Central Forensic Science Lab, Hyderabad****Mob:** 9441438917ch.e.saiprasad@gmail.com  |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **11** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [**Practical Hands On)****Mobile Forensics** | 23-11-2021(Tuesday) | **Mr. Chunduru Eswara Saiprasad, Assistant Director & Scientist C, Central Forensic Science Lab, Hyderabad****Mob:** 9441438917ch.e.saiprasad@gmail.com  |
| **TEA BREAK -** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |
| **12** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Theory]* Introduction to Cloud Forensics
* Blockchain Forensics
* IOt Forensics
* CCTV and DVR Forensics
 | 23-11-2021(Tuesday) | **Mr. Prasad Patibandla, Computer Hacking Forensic Investigator, Hyderabad** **Mr. Md. Nazim** **7207388016**mohdnazim282@gmail.com  |

|  |
| --- |
| **DAY – 5 – THURSDAY – 25-11-2021** |
| **13** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Cryptography and Layered Security Approach** | Quiz for 15 minutes[Theory]**Understanding of Cryptography*** Understanding of Cryptography and its components and types
* Fundamental Concepts of Encryption and Decryption
* Symmetric/Asymmetric Key Encryption
* Various Cryptographic algorithms
* Understanding of Digital Certificates

[**Practical Hands On]**Cyptographic Algorithms in Law Enforcement Perspectives | 25-11-2021(Thursday) | **Ms. Uma Rani Vanamala****Associate Professor, CSE School of IT, JNTU, Hyderabad****9440086956****umarani@jntuh.ac.in** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **14** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Theory]**Cyber Security as a layered approach*** OSI Model
* System/Information Security
* Application Security
* SSI/TLS

**Network Security*** Security certification – Security monitoring and Auditing – Security Requirements
* SIEM Tools
* IDS, IPS
* LOGS and LOG Sources
 | 25-11-2021(Thursday) | **Shri Kshitiz Kumar,** **State Bank of India****Mob: 8800688490****kshitiz003\_kumar@yahoo.com** |
| **TEA BREAK -** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **15.** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Theory]**System Security*** Application Security
* Endpoint detection and response
* Data Security
* Data Leak Prevention
 | 25-11-2021(Thursday) | **-Do-** |
| **DAY – 6 - TUESDAY – 30-11-2021** |
| **16.** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Vulnerability and Hardening Techniques** | Quiz for 15 minutes[Theory]**Introduction to Vulnerability /Threats Assessment*** Introduction to Kali NESSUS, OPENVAS, MISP
* Different exploits
* Obfuscation techniques
* Phishing Techniques
* SQL Injections

[Theory]**Hardening Techniques*** OS related
* Authentication techniques
* Two Factor Authentication
 | 30-11-2021(Tuesday) | **Mr. Yasir Shaikh****Mob: 9930824239****yasir@macksofy.com** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **17.** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Practical Hands On]**Hands on on Previous Techniques*** IPS/IDS
* Endpoint Security
* Firewall
* Data Loss Protection
 | 30-11-2021(Tuesday) | **-Do-** |
| **TEA BREAK -** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |
| **18** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Theory]**Latest Technological advancements in Cyber Security*** Artificial Intelligence and Cyber Security
* Attacks
* Counter Measures
* Block Chain
* IOT, SCADA
* Use Cases
 | 30-11-2021(Tuesday) | **Mr. Deepak Kumar****Cyber Threat Intelligence****I4C, BPR&D, New Delhi****Mob: 9560348444****D3pak@protonmail.com** |

|  |
| --- |
| **DAY – 7 – THURSDAY – 02-12-2021** |
| **19** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Threat Hunting Policing Techniques** | Quiz for 15 minutes[Theory]**Cyber Crime Prevention Techniques*** Proactive approaches
* Surveillance
* Preventive Approaches
 | 02-12-2021(Thursday) | **Mr. Anup Girdhar****Data Security Expert** **anup@sedulitygroups.com** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **20** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Theory]**Proactive Cyber Threat Hunting*** OSINT Techniques
* Predictive Policing
* MITRE Attack Metrix
* Cyber Kill Chain – Lockheed Martin
 | 02-12-2021(Thursday) | **-Do-** |
| **TEA BREAK -** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |
| **21** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Practical Hands On]**Hands on of Previous Session** | 02-12-2021(Thursday) | **-Do-** |

|  |
| --- |
| **DAY – 8 – TUESDAY - 07-12-2021**  |
| **22** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Investigation** | Quiz for 15 minutes**Investigation of Common Cyber Crimes*** Phishing, Vishing, Smishing, Identify Theft, DDOS
* Ransomware
* Financial Frauds
* Data Theft
* Extortion
 | 07-12-2021(Tuesday) | **Mr. Deepak Kumar, BPR&D****9560348444** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **23** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Theory]**Introduction to Website Investigation, Electronic Mail & Investigation related to it*** Business/Personal Emails
* Investigation of Virtual Machines, Databases and Server OS used for website hosting
 | 07-12-2021(Tuesday) |  **Mr. Md. Nazim** **7207388016**mohdnazim282@gmail.com |
|  **TEA BREAK –** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |
| **24** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Practical Hands On]**Hands on Session on Email Investigation & Website Investigation** | 07-12-2021(Tuesday) | **-Do-** |
| **DAY – 9 – THURSDAY – 09-12-2021** |
| **25** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Cyber Laws** | Quiz for 15 minutes**Cyber Laws*** **Discuss Best Practices pertaining to Cyber Law in International Community**
 | 09-12-2021(Thursday) | **Advocate (Dr.) Prashant Mali, Ph.D****Mumbai****Mob: 9821763157****cyberlawconsulting@gmail.com****prashant.mali@cyberlawconsulting.com** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **26** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Theory]**Roles of International Law*** **Introduction to Cyber Laws/Practices**
* **MLAT/LR Processes**
 | 09-12-2021(Thursday) | **-Do-** |
| **TEA BREAK –** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |
| **27** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | [Case Studies]To be discussed with reference to India and Rest of world | 09-12-2021(Thursday) | **-DO-** |
| **DAY – 10 - TUESDAY – 14-12-2021** |
| **28** | 0900-1030 hrs (IST)1030-1200 hrs. (Cambodian Time)**Information Security Management** | Quiz for 15 minutes[Theory]**Cyber Security Policies*** Introduction, Cyber Security Regulations
 | 14-12-2021(Tuesday) | **Mr. Robin Desouza****Information Security Expert****9964203651****robsouz19@gmail.com** |
|  | **LUNCH**1030-1130 hrs (IST) - 1200-1300 hrs (Cambodian Time) |
| **29** | 1130-1300 Hrs. (IST)1300-1430 (Cambodian Time) | [Theory]* The State and Private Sector in Cyberspace, Cyber Security Standards
* Role of ISO/IEC standards in Cyber Security and auditing compliance
* Cyber Security Insurance
* Compliances – GDPR
* HIPAA, ISO:27001
 | 14-12-2021(Tuesday) | **-Do-** |
| **TEA BREAK –** 1300-1315 (IST) - 1430-1445 (Cambodian Time) |
| **30** | 1315-1445 hrs. (IST)1445-1615 hrs. (Cambodian Time) | 1315-1430 hrs. (IST)1445-1600 hrs. (Camb. Time)[Theory]**Information Security Management – Roles and Responsibilities*** CISO/CRO
* System Admin, Network Admin
* Database Admin
* Privileges, Access Controls
* Policies Authentication

Quiz for 15 minutes | 14-12-2021(Tuesday) | **Mr. Venkatesh Murthy, Director, Data Security Council of India (DSCI), Karnataka****Mob: 9880512125** |
| **31** | 1445-1500(IST)1615-1630 (Cambodian Time) | **‘Closing Ceremony’** | 14-12-2021TUESDAY |  |