

Curriculum

Cyber Security Expert Certificate Program



DACH
Dalilna Chools

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 1 TO 5

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 1	SAMA – Framework orientation version 1.0	• Introduction : • SAMA Framework 1.1 • Definition of Cyber security - SAMA definition 1.2 • SCOPE of SAMA framework in cyber security 1.3	Concepts	Y		Thesis- SAMA Framework – Part I
Day 2	SAMA – Framework orientation version 1.0	• Applicability- 1.4 • Responsibilities 1.5 of SAMA Framework in cyber security professionals,	Concepts	Y		
Day 3	SAMA – Framework structure & features 2.0	SAMA Interpretation 1.6 & target audience 1.7	Concepts	Y		
Day 4	SAMA – Control domain 3.0	SAMA Control domain 3.0	Concepts	Y		
Day 5	SAMA – Cyber security risk management & compliance 3.2	• Cyber security risk management • Compliance: • Cyber security risk management 3.2.1 • Regulatory compliance 3.2.2 • Compliance with international industry standards 3.2.3 • Cyber security review 3.2.4 • Cyber security audits 3.2.5	Concepts	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 6 TO 10

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 6	SAMA – Security operations & technology 3.3 - Part 1	- Cyber security human resources 3.3.1 - Cyber security - physical security 3.3.2 - Cyber security asset management 3.3.3 - Cyber security architecture 3.3.4	Concepts	Y		Thesis- SAMA Framework –Part 2
Day 7	SAMA – Security operations & technology 3.3 - Part 2	- Identity & access management 3.3.5 - Cyber security - application security 3.3.6 - Cyber security - change management 3.3.7 - Cyber security - infrastructure security 3.3.8	Concepts	Y		
Day 8	SAMA – Security operations & technology 3.3 - Part 2	- Cyber security cryptography - 3.3.9 - Bring Your Own Device (BOYD) - 3.3.10 - Secure disposal of information assets - 3.3.11 - Payment systems - 3.3.12 - Electronic banking services - 3.3.13	Concepts	Y		
Day 9	SAMA – Security operations & technology 3.3 - Part 3	- Cyber security event management 3.3.14 - Cyber security incident management 3.3.15 - Threat management 3.3.16 - Vulnerability management 3.3.17	Concepts	Y		
Day 10	SAMA – Third party cyber security 3.4	- Third party cyber security 3.4.0 - Contract & vendor management 3.4.1 - Outsourcing management 3.4.2 - Cyber security 3.4.3	Concepts	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 11 TO 15

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 11	Module 1 – Introduction to networking	- Types of network - Network topologies - Bus topology - Star topology - Mesh topology	Concepts	Y		Thesis- cyber-Security & Networking –Part 3
Day 12	Module 1 – Network devices	- Network devices, routers, - Switch : Different types of switching networks gateways - Hub / Access Point / Gateway / Bridge / Modem	Concepts	Y		
Day 13	Module 1 – OSI Model (Layered Model)	Open System Interconnection - application layer, presentation layer, session layer, Transport layers, network layer, data link layer, physical layer	Concepts	Y		
Day 14	Module 1 – TCP/IP MODEL	Structure, services & segment, connection establishment, timers OSI V's TCP/IP model	Concepts	Y		
Day 15	Module 2 – Introduction to servers and its types	Print Server / Application Server / Message Server / Database Server	Concepts	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 16 TO 20

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 16	Module 2 – PROTOCOLS	- TCP - UDP - ICP	Concepts	Y		Thesis- cyber-Security & Networking –Part 3
Day 17	Module 2 – Addressing in network	- Data transmission in networking - Physical layer implementation - Data link layer implementation - MAC Address	Concepts	Y		
Day 18	Module 2 – Network layer implementation	IPV4 / IPV6	Concepts	Y		
Day 19	Module 2 – Accessing the network	- Introduction to multiple access & ethernet - Introduction to internet - Firewalls	Concepts	Y		
Day 20	Module 2 – Advanced packet switching network	- Internal network operations in packet switching network - Routing in packet networks - Shortest path routing algorithm - Bellman-Ford algorithm - Dijkstra's algorithm - A* Search algorithm using heuristics approach	SQL	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 21 TO 25

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 21	Module 2 – Advanced TCP/IP	Multicast routing, DHCP, NAT, Mobile IP, multimedia networking	Concepts	Y		Research Paper – Cyber Security – Network Security
Day 22	Module 3 – Introduction to network security	• Methods adapted in network security • Introduction to encryption • Encryption methodologies • Secret key encryption ○ DES (Data Encryption Standard) ○ 3DES (Triple Strength Data Encryption Standard) ○ RC 2 (Rivest Cipher 2) ○ RC 4 (Rivest Cipher 4) • Public key encryption ○ RSA (Rivest–Shamir–Adleman)	Concepts	Y		
Day 23	Module 3 – Sensor networks	• Overview of quality of services in a network • Integrated QoS • Differentiated QoS	Concepts	Y		
Day 24	Module 3 – Network security and standards	• Various network security terminologies • Security standards : ISO / NIST / GDPR / PCI DSS • Various approaches of network security • Guiding principles of network security • Laws for network Security	Concepts	Y		
Day 25	Module 3 – Network security and standards	• Network security controls • Administrative controls, • Technical controls • Network security protocols • Network segmentation, • Firewall • IDS/IPS,	Concepts	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 26 TO 30

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 26	Module 3 – Network security and standards	- Honeypot, - Proxy server. - Virtual private network, - UBA, NAC, UTM, SIEM, SOAR	Concepts	Y		Case Study I – Network Security & Standards
Day 27	Module 3 – Network security and standards	- Load balancer - Anti malware tools - Network assessment technique - Threat hunting, threat intelligence - Vulnerability assessment & configuration management	Concepts	Y		
Day 28	Module 4 – Introduction to various cyber attacks	- Denial of service attack - Buffer overflow attack - IP spoofing - Session hijacking	BrupSuit	Y		
Day 29	Module 4 – Firewalls	- What is a firewall? Types of firewall - Firewall implementation & proxy servers - Windows and Linux firewalls	Tufin	Y		
Day 30	Module 4 – Encryption	- Modern encryption methods - Windows and Linux encryption - Hashing - Virtual private network (Advanced)	BitLocker TrendMicro	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 31 TO 35

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 31	Module 4 – Virus	- Types of Virus / detecting viruses / antivirus - Trojan horse the most common virus	McAfee	Y		Case Study 2 : Access Control and Recovery
Day 32	Module 4 – Access control and recovery	- Access control and security policies - System security analysis - System recovery - Physical recovery - Disaster recovery - Fault tolerance	Concepts	Y		
Day 33	Module 5 – Cryptography	- Cipher texts and elementary substitution ciphers - Elementary transport ciphers & other cipher properties - Public key cryptography - RSA CryptoSystem - Introduction to RSA - Performance calculation of a RSA CryptoSystem - Applications of RSA CryptoSystem	BitLocker TrendMicro	Y		
Day 34	Module 5 – Cryptography	- PKCS - Cryptographic hash - Introduction to RSA - Properties of a RSA CryptoSystem - Applications of RSA CryptoSystem	Concepts	Y		
Day 35	Module 5 – Cryptography	- Birthday attack - Diffi-Hellmen key exchange algorithm - Secret Key Cryptography - Product Ciphers - DES construction.	Concepts	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 36 TO 40

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 36	Module 5 – Cryptography	- Mathematical aspect of cryptography - Modulo Arithmetic's - The Greatest Comma Divisor - Useful algebraic structures - Chinese Remainder Theorem - Public key infrastructure - Identity-based encryption	Concepts	Y	Capstone Project - I - Cryptography	
Day 37	Module 6 – Authentication	- One way authentication - Mutual authentication - Dictionary attacks - Centralised authentication - The Needham-Schroeder protocol - Kerberos - Biometrics	Concepts	Y		
Day 38	Module 7 – Introduction to ethical hacking	- Fundamentals of key issues in the information security world - Basics of ethical hacking - Information security controls relevant laws & standard procedures.	Concepts	Y		
Day 39	Module 8- Foot Printing and reconnaissance	- The latest techniques and tools to perform foot printing and reconnaissance - Critical pre-attack phase of the ethical - Hacking process	Netifera	Y		
Day 40	Module 8 – Scanning networks	- Network scanning techniques - Countermeasures	NMAP	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 41 TO 45

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 41	Module 9 – Enumeration	- Various enumeration techniques - Border gateway - Protocol (BGP) - Network File Sharing (NFS)	Concepts	Y	Capstone Project 2: VAPI – Penetration testing – Vulnerable Adversely Programmed Interface (vAPI)	
Day 42	Module 10 – Vulnerability analysis	- Identify security loopholes in a target organization's network - Communication infrastructure and end systems - Different types of vulnerability assessment and vulnerability assessment tools	Concepts	Y		
Day 43	Module 11 – System hacking	- Various system hacking methodologies - Steganography - Steganalysis attacks - Covering track used to discover system and network vulnerabilities	Concepts	Y		
Day 44	Module 12 – Malware threat	Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware counter measures	Concepts	Y		
Day 45	Module 13 – Sniffing	- Packet-sniffing techniques - Discover network vulnerabilities - Countermeasures to defend against sniffing attacks.	WireShark	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 46 TO 50

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 46	Module 14 – Social engineering	- Social engineering concepts and techniques - Identify theft attempts - Audit human-level vulnerabilities - Suggest social engineering countermeasures	Kali Linux OS	Y	Capstone Project 2: VAPI – Penetration testing – Vulnerable Adversely Programmed Interface (vAPI)	
Day 47	Module 15 – Denial-of-Service	- Different Denial of Service (DoS) - Distributed DoS (DDoS) attack techniques - Audit a target - Devise DoS and DDoS countermeasures and protections	Kali Linux OS	Y		
Day 48	Module 16 – Session hijacking	- Session hijacking techniques used to discover - Network-level session management	Kali Linux OS VM Different OS's	Y		
Day 49	Module 16 – Session hijacking	- Authentication - Authorization - Cryptographic weaknesses and associated countermeasures	DNS Server	Y		
Day 50	Module 17 – Evading IDS, firewalls, and honeypots	- Intrusion detection system (IDS) - Honeypot evasion techniques - The tools used to audit a network perimeter for weaknesses	Kali Linux Windows Server	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 51 TO 55

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 51	Module 17 – Hacking web servers	- Web server attacks - Including a comprehensive attack	Kali Linux	Y		Research Papers – Ethical Hacking
Day 52	Module 17 – Hacking web servers	Methodology used to audit vulnerabilities in web server infrastructures and countermeasures	Nessus	Y		
Day 53	Module 18 – Hacking web applications	- Web application attacks - Including a comprehensive web - Application hacking methodology used to audit vulnerabilities in web - Applications and countermeasures	Nessus	Y		
Day 54	Module 18 – Hacking web applications	- Web application attacks - Including a comprehensive web - Application hacking methodology used to audit vulnerabilities in web - Applications and countermeasures	Kali Linux	Y		
Day 55	Module 19 – SQL Injection	Basic of SQL	Mysql Server	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 56 TO 60

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 56	Module 19 – SQL Injection	- SQL injection attacks - Evasion techniques - SQL injection countermeasures	SQL Map	Y	Capstone Project 3 : Ethical Hacking	
Day 57	Module 20 – Hacking wireless networks	- Understand different types of wireless technologies encryption - Threats - Hacking methodologies	Kali Linux	Y		
Day 58	Module 20 – Hacking wireless networks	- Hacking tools - Wi-Fi - Security tools - Countermeasures	Kali Linux	Y		
Day 59	Module 20 – Hacking mobile platforms	- Mobile platform attack vector - Android - IOS hacking	Kali Linux	Y		
Day 60	Module 20 – Hacking mobile platforms	- Mobile device management - Mobile security guidelines - Security tools	Kali Linux	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 61 TO 65

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 61	Module 21 – IoT and OT hacking	Different types of IoT and OT attacks	Kali Linux	Y	Capstone Project 3 : Ethical Hacking	
Day 62	Module 22 – Cloud computing	Introduction to cloud computing	Kali Linux	Y		
Day 63	Module 22 – Cloud computing	- Different cloud computing concepts - Container technologies and server less computing - Various cloud computing threats	Kali Linux	Y		
Day 64	Module 22 – Cloud computing	- Attacks - Hacking methodology - Cloud security techniques & tools	Kali Linux	Y		
Day 65	Module 23 – Advanced cryptography	- Disk encryption - Cryptography - Attacks - Cryptanalysis tools	Kali Linux	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 66 TO 70

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 66	Module 24 – Cyber forensics	• Introduction to digital /cyber forensics using Sthe leuth Kit, FTK images, Xplico • Identification process • Preservation process • Analysis process • Documentation process • Presentation process	Using Sthe leuth Kit, FTK images, Xplico	Y		Case studies 3 – Cyber Forensics
Day 67	Module 24 – Cyber forensics	• Introduction to digital /cyber forensics using Sthe leuth Kit, FTK images, Xplico • Identification process • Preservation process • Analysis process, • Documentation process • Presentation process	Using Sthe leuth Kit, FTK images, Xplico	Y		
Day 68	Module 24 – Cyber forensics	• Developing indigenous cyber forensics tools. • Providing training on cyber forensics to Law Enforcement Agencies (LEAs)	Using Sthe leuth Kit, FTK images, Xplico	Y		
Day 69	Module 24 – Cyber forensics	• Providing technical support to LEAs for cybercrime investigation and analysis • Supporting LEAs for setting up of cyber forensics Laboratories	Using Sthe leuth Kit, FTK images, Xplico	Y		
Day 70	Module 24 – Cyber forensics	• Disk Forensics • Network forensics • Mobile device forensics	Using Sthe leuth Kit, FTK images, Xplico	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 71 TO 75

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 71	Module 24 – Cyber Forensics	• Live Forensics. • Memory Forensics	Using Sthe leuth Kit, FTK images, Xplico	Y	Capstone Project 4 – Cyber Forensics	
Day 72	Module 24 – Cyber Forensics	• Multimedia Forensics • Internet Forensics	Using Sthe leuth Kit, FTK images, Xplico	Y		
Day 73	Module 24 – Cyber Forensics	• Database forensics: retrieval and analysis of data or metadata found in databases • Malware forensics: analysis of code to identify malicious programs like viruses, ransomware, or trojan horses	Using Sthe leuth Kit, FTK images, Xplico	Y		
Day 74	Module 24 – Cyber Forensics	• Defeating Anti - forensic techniques • Understanding hard disks & file system • Operating system forensics • Cloud forensic in a cloud environments • Investigating email crimes • Developing forensic skills - email phishing, vishing, smishing	Using Sthe leuth Kit, FTK images, Xplico	Y		
Day 75	Module 24 – Real Time Work on Cryptography	Real time work on cryptography	Kali Linux	Y		

TRAINING MODULES- ADVANCED CYBER SECURITY PROGRAM – DAY 76 TO 80

Days	Main Topics	Subtopic	Tools – Software's or Templates	Assignment (Y/N)	Capstone Project (Y/N)	Research / Case Studies
Day 76	Module 24 – Real Time Work on Cryptography	Real time work on cryptography	Kali Linux	Y		Case Stud 4 – Cryptography
Day 77	Module 24 – Real Time Work on Cryptography	Real time work on cryptography	Kali Linux	Y		
Day 78	Module 24 – Cyber Forensics	• Live forensics • Memory forensics	Using The sleuth Kit, FTK images, Xplico	Y		
Day 79	Module 24 – Cyber Forensics	• Multimedia forensics • Internet forensics	Using The sleuth Kit, FTK images, Xplico	Y		
Day 80	Module 24 – Cyber Forensics	• Database forensics: Retrieval and analysis of data or metadata found in databases. • Malware forensics: Analysis of code to identify malicious programs like viruses, ransomware, or Trojan horses	Using The sleuth Kit, FTK images, Xplico	Y		

Thank You

Sathish Narayanan – Chief Growth Officer – DACH Group

Sathish@dachksa.com

Mobile : +966559087967

Global Whatsapp : +917406733363

www.dachksa.com

Office No. 36, Orchid Center,
Al-Thumama Road, Riyadh, KSA



DACH
Dalilna Chools