Security Fundamentals

Session No#	Session mode	Topic	Week -Day No	Duration Hrs
1	EL-Async	IU 1: Introduction to Cybersecurity • Understanding cybersecurity concepts, importance, and key terminologies • Types of cyber threats (malware, phishing, social engineering, ransomware, etc.) • Overview of cybersecurity frameworks and compliance standards (ISO 27001, NIST, GDPR) • Roles and responsibilities of cybersecurity professionals IU 2: Network Security Fundamentals • Network architectures, protocols (TCP/IP, HTTP, DNS), and communication models • Common network vulnerabilities and attack vectors (MITM, DoS/DDoS, packet sniffing) • Network security devices and configurations (firewalls, IDS/IPS, VPNs) • Securing wireless and cloud networks	Before Sync Session	4
2	FC -Sync	IU 1: Introduction to Cybersecurity IU 2: Network Security Fundamentals Discussion on the assignments	1-1	3
3	AS -Sync	Assignment 1 – Identify and assess cybersecurity threats using industry-standard threat intelligence frameworks. Assignment 2: Configure firewalls, intrusion detection/prevention systems (IDS/IPS), and implement secure network configurations.	1-2	3
4	MS-Async	Assignment 1 & 2 Submission	Before next Assignment session	1
5	EL-Async	IU 3: Ethical Hacking Principles • Ethical hacking process: Reconnaissance, scanning, exploitation, post-exploitation • Common attack techniques (brute force, SQL injection, cross-site scripting) • Overview of penetration testing tools (Nmap, Metasploit, Wireshark) • Ethical considerations and legal aspects of penetration testing.	Before Sync Session	2
6	FC -Sync	IU 3: Ethical Hacking Principles Discussion on the assignments	1-3	3
7	AS -Sync	Assignment 3: Conduct basic vulnerability scanning and penetration testing using ethical hacking tools like Nmap and Metasploit.	2-4	3
8	MS-Async	Assignment 3 Submission	Before next Assignment session	1
9	EL-Async	IU 4: Digital Forensics Essentials • Fundamentals of digital forensics and types of forensic investigations	Before Sync Session	2

		• Evidence collection, preservation, and chain of custody • Analyzing system logs, recovering deleted files, and extracting metadata • Tools for forensic investigations (Autopsy, FTK, EnCase)		
10	FC -Sync	IU 4: Digital Forensics Essentials Discussion on the assignments	2-5	3
11	AS -Sync	Assignment 4: Perform forensic data collection, analyze logs, and recover deleted files from compromised systems.	2-6	3
12	MS-Async	Assignment 4 Submission	Before next Assignment session	2
13	EL-Async	IU 5: Security Operations and Monitoring • Understanding Security Information and Event Management (SIEM) • Monitoring security logs and detecting anomalies • Incident response lifecycle and handling security breaches • Cyber Threat Intelligence (CTI) and proactive threat hunting	Before Sync Session	2
14	FC -Sync	IU 5: Security Operations and Monitoring Discussion on the assignments	3-7	3
15	AS -Sync	Assignment 5: Monitor network traffic, analyze security logs, and respond to simulated cyber incidents.	3-8	3
16	MS-Async	Assignment 5 Submission	Before next Assignment session	2
17	EL-Async	IU 6: Cryptography and Data Protection • Basics of cryptography: Symmetric vs. asymmetric encryption • Common cryptographic algorithms (AES, RSA, SHA) • Implementing encryption for data-at-rest and data-in-transit • Digital signatures, certificates, and Public Key Infrastructure (PKI) IU 7: Business Continuity and Disaster Recovery • Importance of Business Continuity Planning (BCP) and Disaster Recovery (DR) • Identifying risks, conducting impact assessments, and developing response strategies • Incident response planning and execution (tabletop exercises, simulations) • Backup and recovery techniques for data protection	Before Sync Session	4
18	FC -Sync	IU 6: Cryptography and Data Protection Discussion on the assignments IU 7: Business Continuity and Disaster Recovery	3-9	3
19	AS -Sync	Assignment 6: Implement encryption techniques to secure files, emails, and communication channels.	4-10	3
20	MS-Async	Assignment 6 Submission	Before next Assignment session	2

21	AS -Sync	Assignment 7: Develop and test a cybersecurity incident response plan to mitigate the impact of security breaches	4-11	3
22	PM-Sync	Explain the project which the learners need to submit for the summative assessment	4-12	3
23	MS-Async	Project Report Submission for the Summative assessment	Before Assessment	2
24	SA-Sync	Summative Assessment (Per learner)	4-13	30 min

Copyright Disclaimer

All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author or publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator,” at the address below.