Security Operation Analysis

Session No#	Session mode	Topic	Week -Day No	Duration Hrs
1	EL-Async	IU 1: Introduction to Security Operations Centers (SOCs): • Roles and responsibilities within a SOC • SOC architectures and models • Key technologies and tools used in SOCs • Metrics and performance indicators for SOC effectiveness IU 2: Understanding Cyber Threats and Attack Vectors • Classification of cyber threats (e.g., malware, phishing, DDoS) • Stages of the cyber kill chainaccumentum.net • Common attack vectors and exploitation techniques • Indicators of Compromise (IoCs) and their identification	Before Sync Session	4
2	FC -Sync	IU 1: Introduction to Security Operations Centers (SOCs): IU 2: Understanding Cyber Threats and Attack Vectors Discussion on the assignments	1-1	3
3	AS -Sync	Assignment 1: Navigate and utilize SOC tools and platforms for monitoring and analysis. Assignment 2: Analyze network traffic and system logs to identify signs of potential threats or breaches.	1-2	3
4	MS-Async	Assignment 1 & 2 Submission	Before next Assignment session	1
5	EL-Async	IU 3: Log Management and Correlation Techniques • Sources and types of logs (e.g., system, application, network) • Log collection, storage, and retention policies • Log analysis and correlation methodologies • Use of log management tools (e.g., Splunk, ELK Stack, Graylog)	Before Sync Session	2
6	FC -Sync	IU 3: Log Management and Correlation Techniques Discussion on the assignments	1-3	3
7	AS -Sync	Assignment 3: Implement log collection, normalization, and correlation processes to detect anomalous activities.	2-4	3
8	MS-Async	Assignment 3 Submission	Before next Assignment session	1
9	EL-Async	IU 4: Deployment and Utilization of SIEM Solutions • SIEM architecture and deployment models • Data ingestion, normalization, and correlation in SIEM • Creating and fine-tuning SIEM alerts and rules • Automating threat detection and incident response with SIEM	Before Sync Session	2
10	FC -Sync	IU 4: Deployment and Utilization of SIEM Solutions Discussion on the assignments	2-5	3

11	AS -Sync	Assignment 4: Configure and operate SIEM tools to aggregate data, create dashboards, and generate alerts for suspicious events.	2-6	3
12	MS-Async	Assignment 4 Submission	Before next Assignment session	2
13	EL-Async	IU 5: Leveraging Threat Intelligence for Incident Detection • Threat intelligence sources (OSINT, commercial, ISACs) • Analyzing Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs) • Threat hunting techniques using threat intelligence • Integration of threat intelligence with SIEM and security workflows	Before Sync Session	2
14	FC -Sync	IU 5: Leveraging Threat Intelligence for Incident Detection Discussion on the assignments	3-7	3
15	AS -Sync	Assignment 5: Integrate external threat intelligence feeds into SOC workflows to enhance detection capabilities.	3-8	3
16	MS-Async	Assignment 5 Submission	Before next Assignment session	2
17	EL-Async	IU 6: Incident Response Procedures and Best Practices • Phases of incident response (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) • Investigating security incidents and gathering forensic evidence • Incident response playbooks and case management • Utilizing automation and orchestration (SOAR) in incident response IU 7: Collaborative Operations with CSIRT and Stakeholders • Structure and role of CSIRT in incident handling • Coordinating incident response across teams and stakeholders • Reporting and communication protocols during security incidents • Compliance considerations in security operations and incident response	Before Sync Session	2
18	FC -Sync	IU 6: Incident Response Procedures and Best Practices IU 7: Collaborative Operations with CSIRT and Stakeholders Discussion on the assignments	3-9	3
19	AS -Sync	Assignment 6: Execute incident response playbooks, conduct root cause analyses, and document findings systematically.	4-10	3
20	MS-Async	Assignment 6 Submission	Before next Assignment session	2

21	AS -Sync	Assignment 7: Coordinate communication and information sharing with CSIRTs and relevant stakeholders during incident handling.	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	Assignment 7 Submission 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.