

MANAGE SECURITY OPERATIONS

ISCED UNIT CODE: 0612554 11A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/02/6/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Manage security operations

Duration of Unit: 160 hours

Unit Description

This unit covers the competencies required to manage security operations and risks related to cybersecurity. It comprises establishing asset inventory risks, assessing threat risk factors and implementing a security management solution. It entails monitoring security events, updating risk profile, responding to established threats and generating security operation reports.

Summary of Learning Outcomes

Learning Outcomes	Durations (Hours)
1. Establish asset inventory risks	20
2. Assess threat risk factors	20
3. Establish threats landscape	10
4. Implement security management solutions	30
5. Monitor security events	30
6. Update risk profile	20
7. Respond to established threats	20
8. Generate security operations reports	10
Total Hours	160

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Establish asset inventory risks	1.1 Identify and classify assets based on business value and criticality. 1.2 Analyse potential vulnerabilities associated with hardware, software, and data. 1.3 Evaluate exposure to environmental, operational, and cyber threats.	• Observation • Oral questioning • Practical tests • Written tests
2. Assess threat risk factors	2.1 Identify potential threat actors, including internal and external sources. 2.2 Analyse likelihood and impact of threats using qualitative and quantitative methods. 2.3 Utilize threat intelligence to enhance risk assessment accuracy.	• Observation • Oral questioning • Practical tests • Written tests
3. Establish threats landscape	3.1 Meaning of terms 3.2 Threats identification and modelling 3.3 Threat mitigation measures	• Observation • Oral questioning • Practical tests • Written tests
4. Implement security management solutions	4.1 Deploy access controls, encryption, and endpoint security measures. 4.2 Apply security policies, standards, and frameworks for risk mitigation. 4.3 Utilize automation tools for threat detection and response.	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
5. Monitor security events	5.1 Deploy real-time monitoring tools such as SIEM, IDS/IPS, and endpoint detection. 5.2 Analyze security logs, alerts, and anomalies for potential threats. 5.3 Establish baselines for normal system behaviour to detect deviations. 5.4 Automate correlation of security events to identify attack patterns. 5.5 Continuously assess network traffic and user activity for suspicious behaviour.	• Observation • Oral questioning • Practical tests • Written tests
6. Update risk profile	6.1 Review risk levels based on emerging threats and vulnerabilities. 6.2 Integrate threat intelligence feeds to enhance risk awareness. 6.3 Update asset classification and security controls to align with changing risks. 6.4 Conduct periodic security audits and vulnerability assessments.	• Observation • Oral questioning • Practical tests • Written tests
7. Respond to established threats.	7.1 Initiate incident response plans and containment procedures. 7.2 Conduct forensic investigations to determine root causes. 7.3 Apply remediation measures and update security policies.	• Observation • Oral questioning • Practical tests • Written tests
8. Generate Security Operations Reports	8.1 Document security incidents, trends, and response actions. 8.2 Use dashboards and metrics to communicate security posture	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
	effectively. 8.3 Provide compliance reports for regulatory and organizational requirements. 8.4 Communicate risk adjustments to stakeholders.	

Suggested Delivery Methods

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended resources for 25 trainees

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	Learning Materials			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	Learning Facilities & infrastructure			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	Consumable materials			

8	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard markers			
D	Tools and Equipment			
11.	Computers		25 pcs	1:1
12.	Projector		1 pc	25:1
13.	Wireshark 32/64-bit Latest version		25 pc	1:1
14.	VMware/Oracle virtual box		25 pc	1:1
15.	Kali Linux or Parrot OS		25pc	1:1