

MANAGE SECURITY OPERATIONS

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

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.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	These are assessable statements which specify the required level of performance for each of the elements. <i>(Bold and italicised terms are elaborated in the Range)</i>
1. Establish asset inventory risks	1.1 Organizational assets (hardware, software, data, users, cloud resources) are identified and inventoried. 1.2 Asset classification is performed based on criticality, sensitivity, and business value. 1.3 Potential risks and threats associated with each asset type are identified (e.g., data breaches, malware, unauthorized access, physical theft). 1.4 Asset vulnerabilities are documented through security assessments, audits, and monitoring tools. 1.5 Risk levels are analyzed considering likelihood, impact, and exposure of each asset. 1.6 Risk register is created to record identified risks, responsible parties, and mitigation strategies. 1.7 Asset inventory and associated risks are reviewed and updated regularly to reflect changes in the environment.
2. Assess threat risk factors	2.1 Potential internal and external threat sources (cybercriminals, insider threats, competitors, nation-state actors, natural disasters) are identified.

	2.2 Common attack vectors (phishing, malware, ransomware, denial-of-service, privilege escalation) are analyzed for likelihood of occurrence. 2.3 Emerging threats and vulnerabilities are monitored through threat intelligence feeds, advisories, and industry reports. 2.4 Organizational exposure to identified threats is evaluated based on existing security controls and infrastructure weaknesses. 2.5 Threat risk levels are determined using qualitative and quantitative risk assessment methods. 2.6 Threat modelling techniques are applied to simulate potential attack scenarios and impacts. 2.7 Assessment findings are documented and reported to stakeholders for informed decision-making.
3. Establish threats landscape	3.1 Global, regional, and industry-specific cyber threats are researched using threat intelligence sources, advisories, and reports. 3.2 Historical security incidents within the organization and sector are analyzed to identify recurring attack patterns. 3.3 Trends in attacker tactics, techniques, and procedures (TTPs) are reviewed to anticipate evolving threats. 3.4 Vulnerability data from scanning tools, penetration tests, and vendor disclosures are mapped to potential threats. 3.5 External factors such as regulatory changes, geopolitical issues, and emerging technologies are considered in defining the threat landscape. 3.6 Threat landscape is contextualized to the organization's environment, business processes, and critical assets. 3.7 Documented threat landscape is communicated to

	stakeholders for planning risk mitigation strategies. 3.8 Threat landscape is updated periodically to reflect new intelligence and changes in organizational operations.
4. Implement security management solutions	4.1 Security requirements are analyzed to determine appropriate security management solutions (SIEM, IAM, EDR, DLP). 4.2 Security tools and technologies are selected based on organizational policies, risk assessment, and compliance needs. 4.3 Security management solutions are installed, configured, and integrated with existing infrastructure. 4.4 Access controls and identity management solutions (role-based access, MFA, single sign-on) are implemented to regulate user privileges. 4.5 Network and endpoint monitoring systems are deployed to detect suspicious or malicious activities. 4.6 Incident response and alert mechanisms are configured to ensure timely detection and escalation of security events. 4.7 Logs and audit trails are enabled and maintained for accountability and forensic purposes. 4.8 Effectiveness of implemented solutions is tested, validated, and optimized for performance. 4.9 Documentation of configurations, procedures, and responsibilities is maintained for ongoing management.
5. Monitor security events	5.1 Security Information and Event Management (SIEM) systems and log management tools are configured to collect and correlate security events. 5.2 Network, server, application, and endpoint logs are continuously monitored for unusual or unauthorized

	activities. 5.3 Alerts are prioritized based on severity, impact, and relevance to organizational security policies. 5.4 False positives and false negatives are identified and tuned to improve detection accuracy. 5.5 Security dashboards and reports are reviewed to detect patterns, trends, and anomalies in real time. 5.6 Monitoring activities are aligned with compliance requirements, industry standards, and organizational policies. 5.7 Security events are escalated to the incident response team for further investigation and action. 5.8 Monitoring processes are reviewed and updated regularly to address emerging threats and technologies.
6. Update risk profile	6.1 Results from security monitoring, incident investigations, and audits are reviewed to identify changes in risk exposure. 6.2 New vulnerabilities, threats, and attack trends are analyzed and mapped to existing assets. 6.3 Impact and likelihood of identified risks are reassessed using established risk assessment methodologies. 6.4 Risk register is updated to reflect newly discovered risks, changes in asset value, and effectiveness of existing controls. 6.5 Residual risks are documented and communicated to management for decision-making. 6.6 Updated risk profile is aligned with organizational policies, compliance requirements, and business objectives. 6.7 Stakeholders are informed of significant risk changes to guide mitigation strategies and resource allocation.

	6.8 Risk profile is reviewed and updated periodically to remain current with evolving threat landscapes.
7. Respond to established threats	7.1 Security incidents are analyzed to confirm and validate established threats. 7.2 Incident response procedures are activated in line with organizational policies and response playbooks. 7.3 Containment strategies (e.g., isolating affected systems, disabling compromised accounts) are applied to prevent further damage. 7.4 Eradication measures such as malware removal, patching, or reconfiguration are performed to eliminate the threat. 7.5 Systems are restored and validated to ensure business operations return to normal securely. 7.6 Threat response effectiveness is evaluated and documented to identify strengths and areas for improvement. 7.7 Lessons learned are incorporated into updated security policies, procedures, and training programs. 7.8 Stakeholders and management are informed of the response outcomes, impact, and mitigation steps taken.
8. Generate security operations reports	8.1 Security events, incidents, and response activities are documented in line with organizational reporting standards. 8.2 Risk updates, threat trends, and monitoring results are consolidated into comprehensive reports. 8.3 Security Key Performance Indicators (KPIs) and metrics (e.g., incident response time, number of threats detected, patching status) are included for performance evaluation. 8.4 Reports are tailored to meet the needs of different stakeholders (technical teams, management, auditors,

	regulators). 8.5 Compliance requirements and industry standards are addressed in security reporting. 8.6 Visual dashboards, summaries, and detailed logs are prepared to support decision-making. 8.7 Reports are reviewed for accuracy, completeness, and clarity before distribution. 8.8 Security operations reports are shared with stakeholders at scheduled intervals or upon request. 8.9 Feedback from stakeholders is incorporated into future reporting to enhance effectiveness and relevance.
--	---

RANGE

This section provides work environments and conditions to which the performance criteria apply. It allows for different work environments and situations that will affect performance.

Variable	Range
Organizational assets may include but not limited to:	• Hardware • Software • Data • Users • Cloud resources
Asset classification may be based on but not limited to:	• Criticality • Sensitivity • Business value
Asset risks and threats may include but not limited to:	• Data breaches • Malware infections • Unauthorized access • Theft
Threat sources may include but not limited to:	• Cybercriminals • Malicious insiders • Competitors

Variable	Range
	• Nation-states • Natural disasters
Common attack vectors may include but not limited to:	• Phishing • Malware • Ransomware • Denial of Service (DoS) • Privilege escalation
Attacker Tactics, Techniques, and Procedures (TTPs) may include but not limited to:	• Reconnaissance • Initial access • Lateral movement • Persistence • Data exfiltration
Security management solutions may include but not limited to:	• SIEM (Security Information and Event Management) • IAM (Identity and Access Management) • EDR (Endpoint Detection and Response) • DLP (Data Loss Prevention)
Monitoring and event management may include but not limited to:	• SIEM configuration • Log collection • Event correlation
Security operations reporting may include: but not limited to:	• Scheduled reports • On-demand reports • Controlled distribution proced

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Hardware, software, data, users, and cloud resources as critical organizational assets requiring protection.
- Asset classification methods based on criticality, sensitivity, and business value to prioritize security measures.
- Risks and threats to assets, including data breaches, malware infections, unauthorized access, and theft.

- Potential threat sources such as cybercriminals, malicious insiders, competitors, nation-states, and natural disasters.
- Common attack vectors including phishing, malware, ransomware, denial-of-service (DoS), and privilege escalation.
- Security management solutions such as SIEM, IAM, EDR, and DLP, including their application in organizational defense.
- Configuring SIEM systems, collecting logs, and correlating events to detect and respond to security incidents.
- Security operations reporting practices, including scheduled reports, on-demand reports, and controlled distribution procedures.

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

- Communications (verbal and written);
- Proficient in Digital Literacy;
- Time management;
- Analytical
- Faults troubleshooting
- Problem solving;
- Planning; Decision making;
- Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Organizational assets (hardware, software, data, users, cloud resources) were identified and inventoried. 1.2 Asset classification was performed and documented based on criticality, sensitivity, and business value. 1.3 Potential risks and threats for each asset type (breaches, malware, unauthorized access, theft) were identified and documented.
-----------------------------------	---

	1.4 Internal and external threat sources (cybercriminals, insiders, competitors, nation-states, natural disasters) were identified and documented. 1.5 Common attack vectors (phishing, malware, ransomware, DoS, privilege escalation) were analyzed and documented. 1.6 Attacker tactics, techniques, and procedures (TTPs) were reviewed and documented to anticipate evolving threats. 1.7 Vulnerability data from scans, penetration tests, and vendor advisories were mapped and documented against threats. 1.8 Security requirements were analyzed and documented to determine suitable security management solutions (SIEM, IAM, EDR, DLP). 1.9 Security tools and technologies were selected and documented based on policies, risk assessments, and compliance needs. 1.10 SIEM and log management systems were configured and documented for collecting and correlating security events. 1.11 False positives/negatives were identified, tuned, and documented to improve accuracy. 1.12 Monitoring processes were regularly reviewed, updated, and documented to address evolving threats. 1.13 New vulnerabilities, threats, and trends were analyzed and mapped to existing assets, and documented. 1.14 Risk likelihood and impact were reassessed and documented using established methodologies. 1.15 Security incidents were analyzed, confirmed, and documented to validate threats. 1.16 Systems were restored, validated, and documented for secure business resumption. 1.17 Compliance requirements and standards were addressed and documented in reporting. 1.18 Security operations reports were distributed and documented at set intervals or on request.
--	---

2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	4.1 Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	5.1 Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.