TECIS610501

Manage intrusion detection and analysis

Overview

This standard covers the competences you need to manage intrusion detection and analysis operations and teams.

In order to meet this standard, you are required to have the knowledge, skills and understanding necessary to manage intrusion and analysis within an organisation. You will be required to manage intrusion and analysis teams and take responsibility for selecting and implementing appropriate responses.

This will include defining roles and responsibilities and supporting the development and enhancement of organisational incident response capabilities.

This activity is likely to be undertaken by someone whose work role involves leading and being responsible for intrusion monitoring and detection e.g. people working as lead or principal Intrusion Analysts. You will lead teams of analysts to establish intrusion detection and prevention systems and tools, fine tuning these to improve the validity of alarms and notifications.

You will be competent in monitoring network and system activity, identifying and validating issues reported by system alarms and user generated notifications as well as tuning systems to provide valid alarms. You will utilise file integrity monitoring to validate the integrity of operating systems and application software files.

Your underpinning knowledge will provide an understanding of the application of intrusion detection and intrusion prevention systems, and in monitoring intrusion detection systems for anomalous behaviour.

Performance criteria

You must be able to:

1. create the intrusion detection policy that identifies key stakeholders and their responsibilities in maintaining organisational governance for intrusion detection
2. develop, review and maintain intrusion detection procedures that define the step-by-step sequence of activities required
3. promote wide awareness and understanding of intrusion detection and incidents across the organisation
4. manage the intrusion detection and analysis function within an organisation in order to deliver the required intrusion detection capabilities
5. lead and oversee intrusion detection activities ensuring intrusion detection and analysis teams deliver intrusion management objectives
6. review and identify gaps in intrusion detection capabilities in order to continuously improve intrusion monitoring and detection and plan resource and training needs
7. create new signatures and rules to improve detection of malicious activity
8. define and implement base metrics to review and measure the intrusion detection process
9. coordinate the delivery of intrusion detection and 24/7 protective monitoring
10. advise senior business management on intrusion detection and analysis capabilities and resource requirements
11. communicate intrusion incidents, trends and recommendations for improving intrusion detection capabilities
12. escalate declared incidents with incident management and forensic teams
13. define and document intrusion detection and analysis team roles and responsibilities to meet organisational requirements
14. promote wide awareness and understanding of what's involved in intrusion detection and the implications in different areas of the organisation

Knowledge and understanding

You need to know and understand:

1. the regulatory and operational requirements relating to the management of intrusion detection
2. how to create, update and maintain intrusion detection policies and procedures for enterprise computer networks
3. how to research industry best practices to ensure appropriate technologies, processes and standards are implemented to protect from latest threats
4. the organisational systems and procedures for intrusion detection
5. the roles and responsibilities for delivering intrusion detection and analysis capabilities
6. what the requirements are for enterprise, multi-server intrusion detection and intrusion prevention systems
7. how to plan and manage intrusion detection and analysis activities
8. the reasons for cyber security attacks including attacker motivation, tactics, techniques and procedures
9. the required specification of the intrusion monitoring, detection and analysis infrastructure to inform organisational policies, procedures and resource needs
10. the importance of aggregating intrusion trend analysis and reporting to inform the strategy, policies and procedures of the organisation
11. how to report and make recommendations resulting from fault diagnosis
12. advise the Chief Information Officer (CIO) and senior leadership on all intrusion detection issues, vulnerabilities and overall security strategies of the organisation
13. how to raise awareness of the intrusions that can occur and the role of intrusion detection to detect them, tailored for different audiences

Manage intrusion detection and analysis

Developed by	ODAG
Version Number	1
Date Approved	April 2020
Indicative Review Date	March 2023
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd
Original URN	TECIS610501
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Cyber Security, information security, intrusion detection