TECIS610401

Carry out intrusion detection and analysis

Overview

This standard covers the competences needed to carry out intrusion detection and analysis.

In order to meet this standard, you are required to have the knowledge, skills and understanding necessary to carry out tasks associated with intrusion detection monitoring, ensuring that your work complies with all legal, statutory, industrial, organisational requirements whilst following applicable industry codes of practice.

This activity is likely to be undertaken by someone whose work involves implementing and monitoring intrusion detection and prevention systems and monitoring these for potential intrusion events e.g. Intrusion Analysts. You will likely work as a member of a team responsible for managing the implementation of intrusion detection and intrusion prevention systems, collecting and documenting information on anomalous network events. 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. install, operate and maintain network and host-based intrusion detection and prevention systems, including 24x7 protective monitoring
2. test and tune current intrusion detection signatures and rules in order to ensure low rates of false positives and negatives
3. perform comprehensive computer network surveillance and monitoring to detect potential intrusions and attacks
4. schedule vulnerability scans using Security Information and Event Management (SIEM) SIEM tools in required timescales
5. implement policies to maintain organisational governance of intrusion detection
6. use the results of vulnerability scans to develop plans to remediate or mitigate vulnerabilities as they are discovered
7. perform audits of network security monitoring infrastructure in order to maintain network security infrastructure
8. analyse and characterise network traffic data in order to identify anomalous activity and potential threats to network resources
9. use the outputs from threat intelligence analysis to search for and detect potential breaches
10. perform incident correlation to identify trends and patterns that threaten organisational security
11. establish effective intrusion messaging for the respective teams to understand and consume
12. carry out file integrity monitoring to validate the integrity of operating system and application software files
13. collaborate with technical teams to resolve and mitigate information security intrusion events in line with organisational policies and procedures
14. observe internal system behaviours for anomalous activity to recommend new use cases for insider monitoring
15. produce incident reports, awareness and warning materials to stakeholders inside the organisation in the required timescales
16. implement disclosure processes to restrict the knowledge of new vulnerabilities and incidents until appropriate remediation or mitigation is available

Knowledge and understanding

You need to know and understand:

1. the current organisational policies and procedures for Intrusion Response (IR) and where to locate them
2. the roles, responsibilities and authorities of those involved in intrusion detection and prevention
3. the industry standard intrusion detection and prevention tools and how to install, operate and maintain them
4. how to detect anomalous network or system activity using protective monitoring
5. the identifying characteristics of anomalous behaviour
6. the capabilities and limitations of intrusion detection and prevention systems
7. the need to maintain and tune of intrusion detection systems
8. how to conduct vulnerability scans using SIEM tools
9. how to perform network security infrastructure monitoring
10. the required steps involved in incident correlation to identify incident trends and patterns
11. how to identify that an intrusion has been attempted, is occurring, or has occurred
12. the insider threat to security and the need to identify and monitor suspicious behaviours
13. how to install, configure and maintain Intrusion Detection System (NIDS), Network Intrusion Prevention System (NIPS), Host Intrusion Detection System (HIDS) and Host Intrusion Prevention System (HIPS)
14. the required documentation for intrusion detection reporting
15. the tools and methods used for file integrity monitoring and how these are applied
16. the importance of managing information of new vulnerabilities to maintain its confidentiality until known vulnerabilities have been resolved
17. the correct placement of sensors in designing NIDS/NIPS products in enterprise architectures and networks

Carry out 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	TECIS610401
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Cyber Security, information security, intrusion detection