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. Identify potential attacks and misuse activities using approved intrusion detection tools
2. Implement internal and external intrusion detection systems in order to establish 24x7 protective monitoring
3. Analyse and characterise network traffic data in order to identify anomalous activity and potential threats to network resources
4. Use the outputs from intelligence analysis and predictive research in order to search for and detect potential breaches
5. Perform incident correlation in order to identify patterns that threaten organisational security
6. Carry out file integrity monitoring to validate the integrity of operating system and application software files
7. Tune intrusion detection systems to reduce the number of false positives and false negatives
8. Monitor and analyse alerts from security tools, including; Intrusion Detection And Prevention Systems (IDPS), Security Information and Event Management (SIEM), anomaly detection systems, firewalls, antivirus systems, user behaviour analytics, endpoint inspection, and proxy devices
9. Implement and monitor Network Intrusion Detection System (NIDS), Network Intrusion Prevention System (NIPS), Host Intrusion Detection System (HIDS) and Host Intrusion Prevention System (HIPS)
10. Recommend and review new use cases for insider monitoring
11. Collaborate with technical teams to, resolve and mitigate information security intrusion events
12. Produce reports and warning materials in a manner that is both timely and intelligible to the target audience
13. Implement disclosure processes in order 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 need for intrusion detection and analysis to maintain information security
2. The organisational requirements for intrusion detection and analysis
3. The nature and characteristics of Intrusion prevention and intrusion detection tools and how to apply them
4. How anomalous network or system activity can be detected using protective monitoring
5. The constraints of intrusion detection and prevention systems
6. The requirements of maintaining tuning of intrusion detection systems
7. Where to find sources of external vulnerability reports relevant to an organisation
8. The role of protective monitoring in maintaining information security
9. How to identify that an intrusion has been attempted, is occurring, or has occurred and how to respond
10. The requirements of relevant industry standards and codes of practice
11. The roles, responsibilities and authorities of those involved in intrusion detection and prevention
12. How to configure Intrusion Detection System (NIDS), Network Intrusion Prevention System (NIPS), Host Intrusion Detection System (HIDS) and Host Intrusion Prevention System (HIPS)
13. The relevant industry standards and codes of practice
14. Industry standard intrusion detection alert messaging formats
15. The characteristics of the detection performed by sensors
16. How to implement automated mitigation in Intrusion Prevention Systems and in particular for large-scale Distributed Denial of Service (DDoS) attacks
17. How to maintain an awareness of intrusion detection and analysis news and trends

Carry out intrusion detection and analysis

Developed by	ODAG
Version Number	1
Date Approved	March 2020
Indicative Review Date	March 2023
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd
Original URN	TECIS61041
Relevant Occupations	Information and Communication Technology Professionals
Suite	Information Security
Keywords	Cyber Security, information security, intrusion detection