TECIS610301

Assisting with monitoring network and systems activity for anomalous behaviour

Overview

This standard covers the competences needed to assist with monitoring computer network and system activity for anomalous behaviour in the network and endpoints.

In order to meet this standard, you are required to have the knowledge, skills and understanding necessary to undertake network monitoring processes. You will ensure that your work complies with all legal, statutory, industrial and organisational requirements, and follow applicable industry codes of practice. You will be required to work under close supervision and take responsibility for the quality and accuracy of the network monitoring work that you carry out.

This activity is likely to be undertaken by someone whose work role involves computer network security analyst work incorporating network monitoring for potential intrusion events e.g. Junior Analysts, Junior Network Analysts. You will work within a team of analysts to collect and document 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.

Your underpinning knowledge will encompass; an understanding of the difference between intrusion detection and intrusion prevention, the fundamentals of computer network communications and routing protocols and the steps involved in monitoring computer networks and systems, including endpoints for irregular behaviour.

Performance criteria

You must be able to:

1. monitor computer network and endpoint activity for anomalies and suspicious activities in order to detect potential intrusions
2. troubleshoot and validate security issues reported by system alarms or end-users in the required timescales
3. respond to intrusion incidents and alert the team in line with organisational standards
4. assist in maintaining, tuning and testing Security Information and Event Management (SIEM) software to maintain their effectiveness
5. assist in evaluating the operational status of network security monitoring components (including network security sensors, network scanners and tools) to identify and resolve issues
6. report and document intrusions and irregular activities in line with organisational standards
7. validate intrusion incidents and escalate them to the team lead
8. locate and follow organisational policies and procedures to investigate and resolve possible security incidents

Knowledge and understanding

You need to know and understand:

1. the difference between intrusion detection and intrusion prevention
2. what is meant by Network Intrusion Detection System (NIDS), Network Intrusion Prevention System (NIPS), Host Intrusion Detection System (HIDS) and Host Intrusion Prevention System (HIPS)
3. how to monitor computer network activity for anomalies
4. the typical features of a network security incident response policy
5. how to respond to computer network security incidents
6. the need for intrusion detection and analysis
7. how to convey the relevant information surrounding the specific intrusion incident
8. to maintain security of assets and systems
9. the role and features of Security Information and Event Management (SIEM) software in relation to identifying possible computer network intrusions
10. how to test and tune SIEM software
11. the industry standard computer network monitoring approaches and how to apply them
12. the characteristics of irregular behaviours in computer networks
13. that whitelisting is the practice of explicitly allowing approved users access to a particular privilege or service
14. the fundamentals of Network protocols and packet analysis tools
15. the industry standard network communications and routing protocols (including TCP, UDP, ICMP, BGP, MPLS)
16. the standard security profiles and security administration features of networks and operating systems
17. the importance of maintaining accurate records of security incidents in order to identify trends
18. the organisational procedures relating to intrusion detection and analysis
19. how to validate intrusion incidents

TECIS610301

Assisting with monitoring network and systems activity for anomalous behaviour

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	TECIS610301
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Cyber Security, information security, incident detection