TECIS61031

Assisting with monitoring network activity for anomalous behaviour

Overview

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

In order to meet this standard, you are required to have the knowledge, skills and understanding necessary to undertake network monitoring processes, 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, follow instructions but you will 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 network security analyst work incorporating network monitoring for potential intrusion events e.g. Junior Analysts, Junior Network Analysts etc. 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 network communications / routing protocols and the principles involved in monitoring network / system activity for anomalous behaviour.

Performance criteria

You must be able to:

1. Assist in monitoring network and system activity in order to identify potential intrusion, malicious or other anomalous behaviour
2. Identify and validate issues reported by system alarms or problem notifications reported by end-users
3. Assist in providing incident response actions, including escalating to other support groups in line with organisational standards
4. Assist with providing reporting of possible intrusions, anomalous activities and misuse activities
5. Assist in evaluating the operational status of monitoring components, including network security sensors, network scanners and Security Information and Event Management (SIEM) systems tools, reporting and escalating outages
6. Assist with performing security event and incident correlation using information gathered from sources within the enterprise to identify trends
7. Follow organisational procedures to investigate possible security incidents

Knowledge and understanding

You need to know and understand:

1. The need for intrusion detection and analysis to maintain security of assets and systems
2. The difference between intrusion detection and intrusion prevention
3. The process for identifying, analysing and reporting potential intrusions
4. The principles involved in monitoring network and system activity for anomalous behaviour and utilisation of the results
5. The fundamentals of Network protocols and packet analysis tools
6. Industry standard network communications and routing protocols (TCP, UDP, ICMP, BGP, MPLS etc.) along with common internet applications and standards (SMTP, DNS, DHCP, SQL, HTTP, HTTPS etc.)
7. Operating systems (Windows, OS X, Linux, etc.) commonly deployed in enterprise networks
8. The importance of maintaining information related to security investigations and incidents in a format that supports analysis, situational awareness reporting and law enforcement investigation efforts
9. The organisational procedures relating to intrusion detection and analysis
10. 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)

TECIS61031

Assisting with monitoring network activity for anomalous behaviour

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	TECIS61031
Relevant Occupations	Information and Communication Technology Professionals
Suite	Information Security
Keywords	Cyber Security, information security, incident detection