# 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. Lead on intrusion detection and analysis within an organisation
2. Create, update and implement unambiguous intrusion detection and analysis policies, process documentation and procedures in line with organisational requirements.
3. Review and continuously improve monitoring, detection and mitigation capabilities
4. Design the infrastructure for intrusion detection and analysis to deliver organisational objectives
5. Set up and configure the intrusion detection environment in accordance with organisational requirements
6. Design and specify Network Intrusion Detection System (NIDS), Network Intrusion Prevention System (NIPS), Host Intrusion Detection System (HIDS) and Host Intrusion Prevention System (HIPS)
7. Advise senior business management on intrusion detection and analysis issues
8. Liaise effectively with internal and external stakeholders to report intrusion incidents, trends and recommendations for mitigation
9. Manage relationships with sponsors and external providers at all levels to set the priority of intrusion detection and analysis in organisational cyber security resilience
10. Plan, organise and monitor intrusion detection and analysis teams to deliver intrusion management objectives
11. Define and document intrusion detection and analysis team roles and responsibilities to meet organisational requirements

## Knowledge and understanding

*You need to know and understand:*

1. How to plan and manage intrusion detection and analysis activities
2. The importance of clearly specifying organisational requirements for intrusion detection and analysis
3. How to create, configure and maintain multi-server intrusion detection and intrusion prevention systems
4. Maintain an awareness of informational security news and trends
5. The implications of emerging technological developments, economic and industry trends on intrusion detection and analysis within an organisation
6. The correct placement of sensors in designing NIDS/NIPS products in enterprise architectures and networks
7. The need to clearly define roles and responsibilities for intrusion detection and analysis
8. How to review the structure of the intrusion detection and analysis specification to inform organisational policies, and procedures
9. The relevance of intrusion incident trend analysis and reporting
10. The process of creating warning material and how it should be tailored for the target audience
11. The importance of communicating intrusion detection activities clearly and assertively
12. The methods of raising awareness of incident detection

# Manage 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** | TECIS61051 |
| **Relevant Occupations** | Information and Communication Technology Professionals |
| **Suite** | Information Security |
| **Keywords** | Cyber Security, information security, intrusion detection |