TECIS60931

Contribute to routine threat intelligence tasks

Overview

This standard covers the competences needed to contribute to routine threat intelligence and threat modelling tasks which are carried out by organisations to identify current and potential (electronic) threats to their business.

In order to meet this standard, you are required to; have the knowledge, skills and understanding necessary to contribute to threat intelligence and modelling 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 and to follow instructions, but you will take responsibility for the quality and accuracy of the threat intelligence work that you carry out.

This type and level of activity is likely to be undertaken by someone whose work role involves cyber security analyst work activities which incorporate threat analysis and modelling e.g. Junior Security Analysts, Junior Cyber Threat Intelligence Analysts etc. You will likely work within a team of analysts collecting and documenting information on cyber security threats to the organisation. You will be competent in assisting in sourcing information that identifies potential threats, analysing related trends and highlighting security issues relevant to the organisation.

Your underpinning knowledge of threat intelligence and modelling will enable you to apply the appropriate principles and practices and use these to inform on the potential threats to the systems and data in an organisation. Effective threat intelligence involves the comprehensive and continuous collection and analysis of information from the right data sources, originating from both inside and outside an organisation.

Performance criteria

You must be able to:

1. Collect information from defined sources of threat intelligence in order to inform organisational threat assessment
2. Analyse information collected to identify threats to information systems, networks and data
3. Respond to requests for threat information to meet any brief provided
4. Carry out routine security threat intelligence activities in support of the systems
5. Carry out routine threat modelling activities to identify / review threats and their potential impacts so that mitigations can be prioritised
6. Apply tools and techniques for threat intelligence and threat modelling in-line with organisational procedures
7. Assist in assessing network traffic using defined tools, to support organisational cyber intelligence analysis
8. Document threat results in accordance with organisational procedures
9. Assist in producing threat intelligence reports, indicators, tips, oral briefings and other associated guidance materials for the organisation
10. Assist in disseminating and communicating threat intelligence reports, indicators, tips, other materials and warnings to help harden and defend the organisations systems

Knowledge and understanding

You need to know and understand:

1. The nature, characteristics and risks of threats and vulnerabilities
2. The vulnerabilities of a system that may be open to threat actors, including people, devices, networks and databases
3. The role of threat agents in initiating deliberate or accidental threats
4. The successful exploitation of a vulnerability by a threat agent will result in the compromise of confidentiality, integrity or availability of an asset
5. The potential consequence and organisational impact of threats being realised
6. The importance of threat intelligence and threat modelling to protecting organisational security
7. That the threat environment is not static and requires continual monitoring
8. The approved threat modelling tools and how to apply them
9. The concepts and processes of threat intelligence and threat modelling and how to apply them
10. How to review threat intelligence information to determine insights
11. The scope of threat intelligence and modelling work to be carried out and the importance of keeping within these boundaries of responsibility
12. The organisational policies, procedures and priorities for carrying out threat intelligence and modelling activities
13. The relevant and applicable legislation, regulations and external standards relating to threat intelligence and modelling activities
14. The approval process for preparing and publishing the results of threat intelligence outcomes

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	TECIS60931
Relevant Occupations	Information and Communication Technology Professionals
Suite	Information Security
Keywords	Cyber Security, information security, threat analysis