TECIS609301

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 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. 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 identify 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. use defined external threat intelligence sources to collect data in order to inform organisational threat assessment activities
2. carry out threat hunting within internal computer networks using approved procedures to locate undetected threats
3. develop threat assessments by following threat intelligence workflows
4. identify threats to information systems, networks and data
5. respond to requests for threat information required by stakeholders in the required timescales
6. perform packet capture analysis to intercept and log network communications to identify new threats
7. assist with threat modelling assessments to identify the potential business impacts of new threats to prioritise mitigations
8. apply tools and techniques for threat intelligence and threat modelling in line with organisational procedures
9. produce required threat intelligence reports, indicators and other associated guidance materials in the required timescales
10. assist in disseminating and communicating threat intelligence reports and awareness and warning materials

Knowledge and understanding

You need to know and understand:

1. the nature, characteristics and risks of threats
2. the industry standard workflow for intelligence gathering that starts with Human Intelligence (HUMINT), utilises Open Source Intelligence (OSINT), and provides leads for Signals Intelligence (SIGINT)
3. the vulnerabilities of a system that may be open to threat actors, including people, devices, networks and databases
4. how to identify compromises of confidentiality, integrity or availability of data that result from the successful exploitation of a vulnerability by a threat agent
5. the current cyber threats, attack methodologies and threat detection techniques using a wide variety of sources
6. why the threat environment requires continual monitoring
7. the cyber threat intelligence sources that are available
8. how to determine the impact of different threats being realised
9. the role of threat agents in initiating deliberate or accidental threats
10. the importance of threat intelligence and threat modelling to protecting organisational security
11. the required threat modelling tools and how to apply them
12. the concepts and processes of threat intelligence and threat modelling and how to apply them
13. the steps involved in reviewing and correlating threat intelligence information to determine insights
14. the regulatory and legislative requirements, organisational policies and procedures for carrying out threat intelligence and modelling activities
15. the approval process for preparing and publishing the results of threat intelligence outcomes

TECIS609301

Contribute to routine threat intelligence tasks

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	TECIS609301
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Cyber Security, information security, threat analysis