TECIS609401

Carry out threat intelligence assessments

Overview

This standard covers the competences needed to carry out threat intelligence and threat modelling assessments to identify current and potential threats to business data and systems.

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

This type and level of activity is likely to be undertaken by someone whose work role involves cyber security threat analyst work which incorporates threat analysis and modelling e.g. Security Analysts, Cyber Threat Intelligence Analysts. You will likely work within a team of analysts collating, analysing and reporting upon information relating to cyber security activities and threats as well as assessing their origin and potential impact to the organisation. You will be competent 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 comprehensive, continuous collection and analysis of the right data sources, from both inside and outside an organisation.

Performance criteria

You must be able to:

1. research and collect information from a range of threat intelligence sources (including threat intelligence databases, Open Source Intelligence [OSINT] and Warning, Advice and Reporting Point communities [WARP]) to identify new threats and threat actors
2. identify new threat tactics, techniques and procedures used by cyber threat actors
3. develop tactical and strategic cyber intelligence from acquired threat intelligence and technical indicators from external and internal sources
4. proactively engage in threat hunting activities for threats in the enterprise environment
5. deliver cyber threat intelligence services and material to information technology and business leaders
6. publish actionable threat intelligence for business and technology management
7. review and disseminate known trends and countermeasures for potential threats to the organisation
8. assess and validate threat information and exploits data in order to determine the relevance and reliability in line with organisational requirements
9. use threat intelligence in order to develop attack trees that show how an asset can be attacked
10. investigate and analyse threat information to track threat propagation and produce actionable threat intelligence reports and briefings to the organisations teams
11. collaborate with other cyber security teams (network security, security testing, vulnerability detection, incident management) to help guide organisational cyber security strategy
12. identify irregular patterns in network and system activity using log correlation
13. analyse the significance of processed intelligence to identify significant trends, potential threat agents and their capabilities
14. carry out threat modelling to examine the impact of threats on infrastructure and key assets
15. document new threats and trends identified and make recommendations on how to mitigate these in line with organisational requirements

16. select and apply threat analysis tools in line with organisational procedures
17. comply with organisational policies, procedures, guidelines and regulatory requirements when carrying out threat analysis and modelling activities

Knowledge and understanding

You need to know and understand:

1. the steps involved in threat intelligence, modelling and assessment
2. how to identify internal and external data sources and plan and conduct comprehensive, continuous collection and analysis of threat intelligence from them
3. the processes, procedures and methods to research, analyse and disseminate threat intelligence information
4. the systems for automated threat intelligence sharing using the industry standard protocols for Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indication Information (TAXII)
5. how to identify new threat actors, tactics and methods
6. how to identify threat scenarios that are attributed to a specific threat source or multiple threat sources
7. how to perform packet capture analysis
8. the open and closed-sources of threat intelligence information available, including Open Source Intelligence (OSINT) and Warning, Advice and Reporting Point communities (WARP), and how to access and evaluate these
9. the organisational policies and procedures for carrying out threat intelligence and threat modelling
10. the industry standard threat modelling tools and techniques and how to apply them
11. the steps involved in kill chain threat modelling
12. the network activity characteristics that indicate new threats
13. how to analyse and review threat intelligence information to identify patters and trends
14. how to prepare threat intelligence reports
15. how to apply attack trees using a methodical analysis of a security system
16. how to implement the regulatory, legislative and organisational policies and procedures for carrying out threat intelligence and modelling activities

Carry out threat intelligence assessments

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	TECIS609401
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Cyber Security, information security, threat analysis