TECIS60941

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 (information and cyber security) threats to their business.

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 etc. 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. Review and disseminate known trends and countermeasures for vulnerabilities, exploits, and potential threats to the organisation
3. Assess and validate threat information and exploits data, taking into account its relevance and reliability, to develop and maintain 'situational awareness' on threats to the organisation
4. Use threat intelligence to develop attack trees that show how an asset might be attacked
5. Investigate and analyse threat information to track threat propagation and produce actionable threat intelligence reports and briefings to the organisation’s teams
6. Explore patterns in network and system activity through log correlation to identify and report anomalies
7. Analyse the significance of processed intelligence to identify significant trends, potential threat agents and their capabilities
8. Document clearly threat modelling outcomes and, threat trends relevant to the organisation
9. Carry out threat modelling, in order to examine the impact of threats on infrastructure and key assets
10. Examine the impact of a threat taking place on each of the key assets identified
11. Use threat analysis tools as appropriate to meet analysis requirements
12. Provide prioritised recommendations to mitigate identified or detected threat issues
13. Escalate any threats identified that are outside level of responsibility to resolve.
14. Comply with organisational policies, procedures and guidelines when carrying out threat analysis and modelling activities

Knowledge and understanding

You need to know and understand:

1. The principles of threat intelligence, modelling and assessment
2. The role of threat intelligence and threat modelling in performing risk assessments
3. That a threat scenario is a set of discrete threat events, attributed to a specific threat source or multiple threat sources, ordered in time, that result in adverse effects
4. The different types of threat models that can exist and how to respond to them
5. That effective threat intelligence involves comprehensive, continuous collection and analysis of the right data sources, from both inside and outside an organisation
6. The different sources of information available for threat intelligence and how to access and evaluate these
7. The organisational policies and procedures for carrying out threat intelligence and threat modelling
8. The industry standard threat modelling tools and techniques and how to apply them
9. The different methodologies used in threat analysis and threat modelling
10. How to analyse threat information and prepare threat intelligence reports
11. When and who to refer any problems that fall outside the limits of authority
12. The role of attack trees in elaborating threats
13. How to apply attack trees using methodical analysis of a security system

Carry out threat intelligence assessments

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	TECIS60941
Relevant Occupations	Information and Communication Technology Professionals
Suite	Information Security
Keywords	Cyber Security, information security, threat analysis