TECIS609501

Manage threat intelligence activities

Overview

This standard covers the competences needed to manage threat intelligence activities to identify, model and assess current and potential threats to an organisation.

In order to meet this standard, you are required to have the knowledge, skills and understanding necessary to undertake threat intelligence and modelling processes, ensuring that your work complies with all legal, statutory, industrial, organisational requirements, and to follow applicable industry codes of practice. You will be required to lead on threat related activities, take responsibility for the quality and accuracy of threat intelligence and modelling activities and communicate these with senior organisational representatives.

This activity is likely to be undertaken by someone involved with advanced cyber security threat analyst work which incorporates threat analysis / modelling and assessment e.g. Security Analysts, Cyber Threat Intelligence Analysts. You will likely lead a team of threat analysts who analyse and report on new threats, their origins and potential impact to the organisation. You will be competent in sourcing information that identifies potential threats, analysing trends and highlighting security issues relevant to the organisation. You will link the threats identified to vulnerabilities in order to close gaps.

Your underpinning knowledge will provide an understanding of your threat intelligence and modelling work, in order to apply the appropriate principles and practices and use this 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. lead and direct the strategic and operational threat intelligence function, managing threat hunting activities, threat correlation and raising qualified threats with vulnerability management
2. manage threat intelligence teams, reviewing their performance in order to deliver the required threat detection capabilities
3. set the organisational cyber security threat intelligence framework, policies and procedures
4. prepare assessments and cyber threat profiles of current events based on the collection, research, and analysis of cyber threat intelligence
5. develop processes and techniques for analysis of malware and detection of threats to the organisation
6. manage the performance of the threat intelligence team (including setting objectives, planning training and development and ensuring all team members follow organisational processes)
7. implement and lead delivery and operation of the organisations threat intelligence infrastructure, platform and tools
8. review threat intelligence processes in order to recommend improvements and drive process enhancements
9. collaborate across threat analysis and modelling teams to resolve complex threat scenarios
10. align threat intelligence activities to organisational assets in order to close control gaps and reduce organisational risk
11. direct the production of threat intelligence reports on the current threat landscape for technical and non-technical audiences
12. work alongside other cyber security management teams including vulnerability management, intrusion detection and incident response to ensure that threat intelligence information is presented and acted upon to mitigate threats

Knowledge and understanding

You need to know and understand:

1. the scope, purpose and requirements of the threat intelligence work which is being managed
2. legal and organisational requirements on threat intelligence activities
3. how to select and implement relevant threat assessment tools and infrastructure
4. the range of problems and challenges that may arise during threat assessment activities
5. how to critically evaluate and take informed action on threat intelligence assessments
6. how to communicate effectively with senior stakeholders and to gain support for threat intelligence strategy
7. the policies, regulations, legislation and external standards that apply to threat intelligence activities
8. the factors involved in researching threat intelligence sources and databases to seek evidence of new threats and threat actors
9. the characteristics of threat intelligence in providing evidence-based knowledge about threats to assets that can be used to inform decisions on cyber security resilience
10. how to confirm the roles and capabilities of threat intelligence team members
11. how and why to negotiate a clear and accurate brief on the purpose, process and intended results of threat intelligence team activities
12. the threat modelling actions to be taken where potential threats can be identified, enumerated, and prioritised
13. the requirements of threat intelligence to provide indicators of threat and compromise scenarios in a timely manner
14. the importance of ensuring the delivery of threat intelligence resources matches organisational requirements and budgets
15. how to prepare and complete threat intelligence reports and who they should be provided to

TECIS609501

Manage threat intelligence activities

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	TECIS609501
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Cyber Security, information security, threat analysis