TECIS60951

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, manage associated staff/teams and take responsibility for the quality and accuracy of threat intelligence / modelling and assessment activities of the organisation and to communicate these activities with senior organisational representatives.

This activity is likely to be undertaken by someone whose work role involves leadership and cyber security threat analyst work which incorporates threat analysis / modelling and assessment e.g. Security Analysts, Cyber Threat Intelligence Analysts etc. You will likely lead 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 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 threat intelligence teams to deliver proactive threat reporting and mitigation in order to improve organisational defensive resilience
2. Provide leadership across threat intelligence and assessment functions, managing threat hunting activities and threat correlation
3. Plan day to day operations and work allocation and management to maintain operational services
4. Create unambiguous operating instructions and related threat intelligence and modelling process documentation for use by teams
5. Act as a single point of contact for threat intelligence and modelling activities
6. Plan mentoring, training, and development of staff skills to maintain effective threat intelligence and modelling capabilities
7. Prepare assessments and cyber threat profiles of current events based on the collection, research, and analysis of cyber threat intelligence
8. Collaborate across threat analysis and modelling teams to resolve complex threat scenarios
9. Review processes, procedures, and approved tools and techniques to ensure continuous improvements to monitor, detect and mitigate threats
10. Collaborate with cyber security, IT and business stakeholders to ensure that threat intelligence analysis outcomes are mapped to s organisational assets in order to close control gaps and reduce organisational risk
11. Conduct periodic capability and performance reviews with teams to identify skills and training development needs
12. Provide weekly and monthly status reports to higher management
13. Maintain adherence to organisational quality and security standards
14. Lead production and editing of threat intelligence reports that enhance the intelligence production workflow

Knowledge and understanding

You need to know and understand:

1. How to select and acquire relevant threat assessment tools
2. The range of problems and challenges that may arise during threat assessment activities
3. How to select threat intelligence professionals to manage and take responsibility for specific threat assessment tasks
4. How to establish escalation, communication processes and lines of authority for threat intelligence
5. What are the internal and external factors that may impact on threat intelligence activities?
6. The policies, regulations, legislation and external standards that apply to threat intelligence activities
7. The need to conduct research to keep up to date with threats and threat actors
8. The factors involved in researching Internet sources and threat intelligence databases to seek evidence of new threats and threat actors
9. The characteristics of threat intelligence in providing evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard
10. The threat modelling actions to be taken where potential threats can be identified, enumerated, and prioritised
11. The factors involved in using threat intelligence to establish new vulnerabilities
12. The requirements of threat intelligence to provide the ability to recognise and act upon indicators of attack and compromise scenarios in a timely manner
13. That effective threat intelligence involves comprehensive, continuous collection and analysis of the right data sources, from both inside and outside an organisation

TECIS60951

Manage threat intelligence activities

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	TECIS60951
Relevant Occupations	Information and Communication Technology Professionals
Suite	Information Security
Keywords	Cyber Security, information security, threat analysis