Overview

This standard is about undertaking cyber threat hunting assignments.

Cyber threat hunting is a complementary approach to cyber threat detection. Whilst threat detection identifies an incoming or ongoing attack and then prevents or remediates it, threat hunting involves proactively searching for unknown vulnerabilities and undetected attacks within an organisation's digital environment. Cyber threat hunters need to know how to develop and test hypotheses about potential new and sophisticated threats to the organisation that can evade automated cyber security controls.

Cyber threat hunting includes gathering cyber threat intelligence, identifying known attack techniques and developing and testing hypotheses about potential new threats by analysing data from sources inside and outside of the organisation. This improves the security posture and resilience of the organisation and provides more comprehensive protection against sophisticated cyber threats. It also includes analysing, exploring, and reporting findings on cyber security threats discovered.

This standard is for those who need to undertake cyber threat hunting assignments as part of their duties.

Performance criteria

You must be able to:

1.
Define threat hunting requirements to narrow the scope of detections
2.
Select and apply threat hunting methodologies to plan the threat hunting strategy in line with organisational procedures
3.
Respond
to triggers from advanced detection tools that identify malicious activity to
plan detailed investigation for advanced threats
4.
Develop hypothesis about potential risks to the organisation
5. Identify data sources to contribute to proving or disproving the hypothesis
6. Develop an approach for collecting and analysing that data
7. Collect and analyse the data required to prove or disprove their hypothesis
8. Validate whether the suspected threat is present in line with hypothesis
9.
Perform an in-depth investigation to identify potential malicious compromise of a system
10.
Identify compromised systems to determine details about how the attack was performed and its impacts to the organisation
11. Produce an account of how the attack was carried out, its objectives, and the impacts on the organisation and its system to inform the remediation actions
12.
Determine what steps are necessary to respond to and mitigate identified threats
13.
Investigate dark web marketplaces to identify evidence of new threat intelligence to inform threat hunting
14.
Develop mitigation and countermeasures tools to remediate attacks and restore systems to normal operation
15. Produce a threat hunt report to document and explain evidence detected of

cyberattacks or new threats identified

Knowledge and understanding

You need to know and understand:

1. How to define a threat hunt assignment scope
2. Industry standard and organisational frameworks used to plan threat hunting exercises
3. The basic principles of threat hunting and its use to improve cyber resilience
4. The benefits of threat hunting including detecting intrusions, identifying vulnerabilities, quantifying risks, improving defences and streamlining threat detection
5. The industry standard types of threat hunting methodologies including adversary hunting, hypothesis-based hunting, indicators of attack and hybrid hunting
6. The steps involved in researching Tactics, Techniques, and Procedures (TTPs) of known threat actors
7. How to develop hypotheses to perform a threat hunt
8. The approaches used for collecting and analysing threat hunting data and how to apply them
9. The data sources used to collect and analyse hypothesis testing data
10. The industry standard tools used to collect threat data including Security Information and Event Management (SIEM) and dark web monitoring solutions
11. How to access to high-quality data and threat intelligence
12. The steps involved in collecting and processing threat intelligence data
13. How to collect and analyse hypothesis testing data
14. Industry standard specialised and custom-built threat hunting tools and how to apply them
15. The types of tools used for threat hunting including threat intelligence sources, telemetry-based technologies, and automation solutions
16. How to validate threats in line with hypothesis
17. The steps involved in remediating a verified attack
18. How to access dark web marketplaces
19. How to automate threat hunting including the use of artificial intelligence (AI) and user and entity behaviour analytics (UEBA)
20. How to develop a detailed account of an attack

21. How to develop mitigation and countermeasures tools
22. How to document the results of threat hunting exercises

TECIS60942

Undertake cyber threat hunting assignments

Developed by	e-skills
Version Number	1
Date Approved	30 Mar 2023
Indicative Review Date	30 Mar 2026
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd.
Original URN	TECIS60942
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Cyber threat hunting, threat intelligence, cyber resilience