HACKTHEBOX

Security Incident Report

CDSA Exam Report

HTB Certified Defensive Security Analyst (HTB CDSA) Exam Report

Candidate Name: TODO Candidate Name

Version: TODO 1.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

Contacts		
Primary Contact	**Title**	**Contact Email**
TODO Candidate Name	TODO Candidate Title	TODO Candidate Email

3 Exam Objectives (Read Carefully)

To be awarded the HTB Certified Defensive Security Analyst (CDSA) certification, you must:

- Obtain a minimum of 85 points while investigating **Incident 1** by submitting 17 out of the 20 flags listed below **AND**
- Compose and submit a commercial-grade security incident report **for both incidents** that encompasses an **Executive Summary** and **Technical Analysis** sections **for each incident**, adhering strictly to the format and content outlined in the **Security Incident Reporting** module.
  - While the Impact Analysis and the Response and Recovery Analysis, including diagrams, can be excluded, the Technical Analysis for both incidents must be exceptionally thorough.
  - Each stage of the cyber kill chain needs to be addressed, and any activities related to process injection should be scrutinized thoroughly, considering aspects like the origin, destination, and whether a process was sacrificial.
  - Each detection should be elucidated step by step, inclusive of the associated data sources, SIEM queries, and tool commands.

4 Executive Summary

TODO Customer Ltd. engaged TODO Candidate Name to investigate two (2) independent security incidents across two of TODO Customer Ltd.' separate networks. The objective is to identify the root causes and the full extent of these incidents and to meticulously document the findings in an understandable, technically robust, and reproducible way.

TODO INCIDENT TITLE

Incident ID: TODO TO BE FILLED BY THE SECURITY ANALYST

Incident Severity: TODO: TO BE FILLED BY THE SECURITY ANALYST

Incident Status:

Incident Overview:

TODO TO BE FILLED BY THE SECURITY ANALYST

Key Findings:

TODO TO BE FILLED BY THE SECURITY ANALYST

Immediate Actions:

TODO TO BE FILLED BY THE SECURITY ANALYST

Stakeholder Impact:

TODO TO BE FILLED BY THE SECURITY ANALYST

5 Technical Analysis

TODO INCIDENT TITLE

Affected Systems & Data

Highlight all systems and data that were either potentially accessed or definitively compromised during the incident. If data was exfiltrated, specify the volume or quantity, if ascertainable.

TODO TO BE FILLED BY THE SECURITY ANALYST

Evidence Sources & Analysis

Emphasize the evidence scrutinized, the results, and the analytical methodology employed. Each detection should be elucidated step by step, inclusive of the associated data sources, SIEM queries, and tool commands.

TODO TO BE FILLED BY THE SECURITY ANALYST

Indicators of Compromise (IoCs)

IoCs are instrumental for hunting potential compromises across our broader environment or even among partner organizations. These can range from abnormal outbound traffic to unfamiliar processes and scheduled tasks initiated by the attacker.

TODO TO BE FILLED BY THE SECURITY ANALYST

Root Cause Analysis

Within this section, detail the root cause analysis conducted and elaborate on the underlying cause of the security incident (vulnerabilities exploited, failure points, etc.).

TODO TO BE FILLED BY THE SECURITY ANALYST

Technical Timeline

This is a pivotal component for comprehending the incident's sequence of events. The timeline should include:

- Reconnaissance
- Initial Compromise
- C2 Communications
- Enumeration
- Lateral Movement
- Data Access & Exfiltration
- Malware Deployment or Activity (including Process Injection and Persistence)
- Containment Times (can be excluded)
- Eradication Times (can be excluded)

- Recovery Times (can be excluded)

TODO TO BE FILLED BY THE SECURITY ANALYST

Nature of the Attack

Deep-dive into the type of attack, as well as the tactics, techniques, and procedures (TTPs) employed by the attacker.

TODO TO BE FILLED BY THE SECURITY ANALYST

A Appendix

A.1 Technical Timeline

Time	Activity
TODO	TODO
…	…
…	…
…	…
…	…

End of Report

This report was rendered
by SysReptor with
♥