



HACKTHEBOX

Detection Engineering Report

**Paradox Development
Corporation**

HTB Certified Detection Engineering Principal (HTB CDEP) Exam
Report

Candidate Name: TODO CANDIDATE NAME

September 30, 2026

Version: 1.0

Table of Contents

1	Statement of Confidentiality	3
2	Engagement Contacts	4
3	Executive Summary	5
4	Detection Engineering Methodology	6
5	Identified Techniques Overview	7
6	Scope and Data Availability	8
6.1	Scope	8
6.2	Telemetry and Data Sources Used	8
7	Per-Host Behavior Analysis and Detection Engineering Workflow	9
7.1	PD-WS-1	9
7.1.1	Detection Engineering Synthesis (ATT&CK-mapped)	9
7.1.2	Tactics, Techniques, and Procedures (TTP-by-TTP "Detection Decomposition")	9
7.1.3	Tool / Tradecraft Analysis	10
7.1.4	Artifact Analysis	10
7.1.5	Detection Engineering Deliverables	10
7.1.6	Proposed Detection Rules & Correlations	12
7.1.7	Additional Telemetry Sources and Detection Opportunities to Consider	12
8	Cross-Host Detection Storyline	13
9	MITRE ATT&CK® Navigator - Attack Chain Mapping	14

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 is 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's external or internal infrastructure.

2 Engagement Contacts

Contacts		
Primary Contact	Title	Contact Email
Andy Lewis	SecOps Manager	a.lewis@paradox.local
David Maron	SecOps Manager	d.maron@paradox.local
TODO CANDIDATE NAME	Detection Engineer	TODO CANDIDATE MAIL

3 Executive Summary

Paradox Development Corporation Ltd. was breached in a full-chain intrusion spanning a user workstation, the domain controller, a Linux build server, and additional workstations. In total, five machines were involved: one Domain Controller, three Windows workstations, and one Linux server. Incident response is complete: containment and eradication are done. During the intrusion, the SOC captured a comprehensive telemetry corpus (Sysmon, multiple ETW providers, ETW-TI, Windows Security, and Linux auditd) and preserved the recovered adversary tooling in an analysis store.

TODO CANDIDATE NAME joined Paradox as a Detection Engineer. The mandate is not to re-investigate the incident. It is to build the detection content that would have caught each stage of this intrusion, and to validate every analytic against the captured corpus so that only rules proven to fire are shipped. The captured telemetry is the validation dataset; the recovered samples are the reference for designing behavior-based detections that survive a rebuild, rather than brittle IOC rules.

Each analytic, together with its validation evidence, must be documented in this report in an understandable, technically robust, and reproducible way.

4 Detection Engineering Methodology

For every task in this engagement, the same five-step detection-engineering loop is applied:

1. **Characterize the behavior:** from the recovered sample (capability analysis) and/or telemetry, understand how the technique works, so that the detection targets behavior rather than a hash or filename.
2. **Map to ATT&CK:** identify the technique / sub-technique the analytic covers.
3. **Author the analytic:** write the detection over the correct data source (Sysmon, the relevant ETW provider, ETW-TI, Security, or auditd).
4. **Validate:** run it against the captured corpus and confirm it fires on the true positive.
5. **Submit proof-of-detection:** the field value the validated analytic returns is the evidence that the rule works. That value is the flag.

5 Identified Techniques Overview

Reference for Detection Coverage:

- **High:** Detection is based on hard-to-change behaviors or strong telemetry, and is resilient to simple evasion.
- **Medium:** Detection is useful but can be bypassed with moderate effort, or is sensitive to environmental variance.
- **Low:** Detection is fragile or noisy. It relies mostly on easy-to-change indicators.

Finding ID	Host(s)	ATT&CK Technique	Time Window (UTC)	Detection Coverage
F-001	Machine Name	TXXXX(.XXX)	YYYY-MM-DD hh:mm:ss to YYYY-MM-DD hh:mm:ss	High / Medium / Low

TODO TO BE FILLED BY THE DETECTION ENGINEER

6 Scope and Data Availability

6.1 Scope

Here, the Detection Engineer is expected to clearly define the boundaries of the technical analysis and detection engineering work so the reader can interpret the results accurately. This includes explicitly listing the assets in scope, such as the relevant domain, hosts, subnets, and user accounts that were examined, and clarifying whether any systems or accounts were out of scope.

The Detection Engineer is also expected to specify the exact time window analyzed, including the start and end timestamps and the timezone used, since event sequencing, correlation logic, and conclusions depend on consistent time interpretation and log availability within that period.

TODO TO BE FILLED BY THE DETECTION ENGINEER

6.2 Telemetry and Data Sources Used

In this section, the Detection Engineer lists the exact telemetry sources used to author and validate each detection, so the work is transparent and reproducible. It should state which available data sources each analytic relies on, where they are queried in Splunk (indexes and source types), which key fields are relied on, and any data collection gaps that could affect confidence.

TODO TO BE FILLED BY THE DETECTION ENGINEER

7 Per-Host Behavior Analysis and Detection Engineering Workflow

7.1 PD-WS-1

7.1.1 Detection Engineering Synthesis (ATT&CK-mapped)

Goal: Provide an ATT&CK-mapped synthesis of the adversary tradecraft as a detection engineering deliverable: what happened, and what detection coverage can be built/validated on this host.

Example: on PD-WS-1, observed host telemetry indicates the threat actor utilized certutil.exe (S0160) for Ingress Tool Transfer (T1105) to deploy Rubeus (S1071), subsequently executing AS-REP Roasting (T1558.004) against the mcameron principal; following successful Password Cracking (T1110.002), obtained credentials were leveraged via Valid Accounts (T1078) to facilitate Lateral Movement (T1021.002); the attacker then performed OS Credential Dumping (T1003) for privilege escalation, established Persistence through a Windows Service (T1543.003), and employed Pass the Ticket (T1550.003) maneuvers; concluding the operation, the actor engaged in Collection (T1005), Archiving (T1560.001), and Exfiltration (T1041) of sensitive data, followed by the Removal of Indicator Artifacts (T1070) to obfuscate their presence.

Detection engineering focus: (1) identify high-fidelity behavioral invariants on the machine, (2) map telemetry sources required to detect each stage, and (3) propose + validate SPL correlations to catch the chain end-to-end.

TODO TO BE FILLED BY THE DETECTION ENGINEER

7.1.2 Tactics, Techniques, and Procedures (TTP-by-TTP “Detection Decomposition”)

BITS Jobs - T1197

Detection Objective

In this section, the Detection Engineer explains why the adversary used the technique in the context of the incident, what tactical objective it served in the attack chain, and how it contributed to the attacker’s broader goals. The intent is to connect observed actions to motivation and outcome, so the reader understands the technique’s role in progression, for example, enabling Credential Access, Privilege Escalation, Lateral Movement, Persistence, Collection, or Defense Evasion, rather than viewing it as an isolated event.

TODO TO BE FILLED BY THE DETECTION ENGINEER

Behavioral Breakdown

In this section, the Detection Engineer characterizes how the technique works, using the recovered sample (capability analysis) and/or the captured telemetry. The section should also state the technique’s objective in the attack chain, and its relationship to preceding and subsequent techniques, within a unified attack narrative.

TODO TO BE FILLED BY THE DETECTION ENGINEER

7.1.3 Tool / Tradecraft Analysis

If the analysis uncovers the use of a publicly available, open-source tool in an open repository, rather than an attacker-crafted artifact, the detection engineer is expected to break down the tool's operating procedure and identify the key choke points and invariants that can be leveraged to derive high-value indicators for future detection rules.

TODO TO BE FILLED BY THE DETECTION ENGINEER

7.1.4 Artifact Analysis

If capability analysis of a recovered sample from the RE folder is performed, the Detection Engineer is expected to document all relevant analysis steps in this section and provide a detailed, step-by-step explanation of the methodology followed, identifying the behaviors, choke points, and invariants on which the resulting behavior-based detection is built.

TODO TO BE FILLED BY THE DETECTION ENGINEER

WinDbg Trace File Analysis (If Applicable)

When WinDbg is used in the analysis of the identified technique, the Detection Engineer is expected to document the complete analysis process in this section, clearly detailing each step of the methodology used with the debugger and the observations made throughout the trace file analysis.

TODO TO BE FILLED BY THE DETECTION ENGINEER

7.1.5 Detection Engineering Deliverables

Host-Based Model (If Applicable)

Here, the Detection Engineer is expected to map the identified detection opportunities and their associated telemetry sources to the Summiting the Pyramid (STP) framework, assessing their respective levels of detection capability and robustness. Here, the Detection Engineer is expected to focus on the framework's host-based model, where applicable to the identified technique.

TODO TO BE FILLED BY THE DETECTION ENGINEER

The following table provides a partial example for the BITS Jobs technique (T1197).

	Application (A)	User-Mode (U)	Kernel-Mode (K)
Core to (Sub-) Technique (5)	Microsoft-Windows-Bits-Client/ Operational log, EID 3 "BITS job created" generated by the BITS service itself		Outbound network connection initiated by svchost.exe -k netsvcs -s BITS (Sysmon EID 3)

	Application (A)	User-Mode (U)	Kernel-Mode (K)
Core to Some Implementation of (Sub-) Technique (4)		The destination file is written by svchost.exe (BITS), not by the calling tool (Sysmon Event ID 11 - FileCreate)	
Core to Pre-Existing Tool or Inside Boundary (3)	Event ID 4104 (PowerShell ScriptBlock) containing Start-BitsTransfer	Registry value set in HKLM...\BITS(Sysmon EID 13 - Registry Set)	bitsadmin.exe command line (Sysmon EID 1) - Look for / transfer and / SetNotifyCmdLine
Core to Adversary-Brought Tool or Outside Boundary (2)			IP address or domain name of the remote server hosting the payload
Ephemeral (1)	BITS job DisplayName		SHA256 hash of the downloaded file

Network-Based Model (If Applicable)

Here, the Detection Engineer is expected to focus specifically on the framework's network-based model when applicable to the identified technique.

TODO TO BE FILLED BY THE DETECTION ENGINEER

	Protocol Payload (P)	Protocol Header (H)
Core to (Sub-) Technique (5)		
Core to Some Implementation of (Sub-) Technique (4)		
Core to Pre-Existing Tool or Inside Boundary (3)		
Core to Adversary-Brought Tool or Outside Boundary (2)		
Ephemeral (1)		

ATT&CK Detection Guidance

DETXXX - TODO Description (e.g. "DET0098 - Detect abuse of Windows BITS jobs for download, execution and persistence")

TODO TO BE FILLED BY THE DETECTION ENGINEER

7.1.6 Proposed Detection Rules & Correlations

Based on the preceding analysis tasks, the Detection Engineer is expected to develop Splunk SPL queries, where applicable, to detect the identified technique. These queries should aim to leverage detection approaches positioned as high as possible on the Pyramid of Pain, so that they survive a rebuild of the adversary tooling. The Detection Engineer is expected to develop robust detection rules and identify relevant correlation opportunities to improve detection accuracy, reduce false positives, and strengthen overall detection coverage.

The Detection Engineer is also expected to provide the output of the SPL query they propose, either as a screenshot or a table, demonstrating that the rule fires on the true positive in the captured corpus.

Detection Rule 1 - TODO Purpose

TODO SPL query

Possible False Positives (if applicable):

- ...
- ...

Detection Rule 2 - TODO Purpose

TODO SPL query

Possible False Positives (if applicable):

- ...
- ...

7.1.7 Additional Telemetry Sources and Detection Opportunities to Consider

In this section, the Detection Engineer may highlight additional detection opportunities, provide recommendations, or identify missing telemetry sources relevant to detecting the described technique. This is also where they can add supporting detection rules or queries, such as YARA and Sigma, along with a clear rationale explaining their relevance and potential value for improving detection coverage. This section also allows specifying potential hook points for APIs to intercept.

TODO TO BE FILLED BY THE DETECTION ENGINEER

8 Cross-Host Detection Storyline

In this section, the Detection Engineer is expected to reconstruct the incident as a chronological sequence of attacker actions across all in-scope systems, showing how the intrusion progressed from initial access through various tactics and objectives. The data shown below is provided for illustrative purposes.

PD-WS-1:

Time	Activity
2026-09-09 10:14:22	On PD-WS-1, the attacker initiated access via a spearphishing attachment (T1566.001), relying on a user opening a malicious document to trigger the chain.
2026-09-09 08:57:46	The attacker's payload executed after user interaction, consistent with user execution (T1204).
...	...

PARADOX-DC:

Time	Activity
...	...

9 MITRE ATT&CK® Navigator - Attack Chain Mapping

The ATT&CK Navigator map that shows all techniques referenced in the report is attached to this report as a JSON file. Please refer to it for an overview of all techniques identified for the APT whose behavior was observed throughout this report.

TODO: Attach the ATT&CK Navigator JSON file to this report.

End of Report

*This report was rendered
by SysReptor with
♥*