SOC INCIDENT RESPONSE

FINAL INVESTIGATION REPORT

Incident: CEO Workstation Compromise via Phishing Attack

Classification: CONFIDENTIAL

To	CISO / Security Team
From	Tier 2 SOC Analyst
Report Date	05 June 2026
Incident Ref	INC-2024-CEO-001
Severity	CRITICAL

Table of Contents

Table of Contents....2
Part 1: Operational Metrics & Validation....3
1.1 Key Performance Indicators (KPIs)....3
1.2 TryHackMe SOC Dashboard....3
Part 2: Technical Incident Report (TIR)....4
2.1 Incident Overview....4
2.2 Attack Lifecycle Timeline....4
2.3 Indicators of Compromise (IOCs)....4
2.4 Investigation Methodology & Splunk Queries....5
Part 3: Executive Summary, Metric Analysis & GRC Strategy....7
3.1 Executive Summary....7
3.2 Metric Interpretation & Analysis....7
Mean Dwell Time – 12 Minutes....7
True Positive Rate – 95%....7
3.3 NIST Cybersecurity Framework (CSF 2.0) Mapping....7
3.4 Remediation Plan....8
Appendix A: References & Standards....9

Part 1: Operational Metrics & Validation

1.1 Key Performance Indicators (KPIs)

The following metrics were recorded upon completion of the SOC simulation environment on TryHackMe and reflect the analyst's performance across 11 triaged alerts during the investigation period.

Metric	Value
True Positive Identification Rate	**95%**
False Positive Identification Rate	**5%**
Total Number of Closed Alerts	**11**
Mean Time to Resolve (MTTR)	**5 minutes 30 seconds**
Mean Dwell Time	**12 minutes**

Table 1 – SOC Analyst KPI Summary (TryHackMe SOC Simulator)

1.2 TryHackMe SOC Dashboard

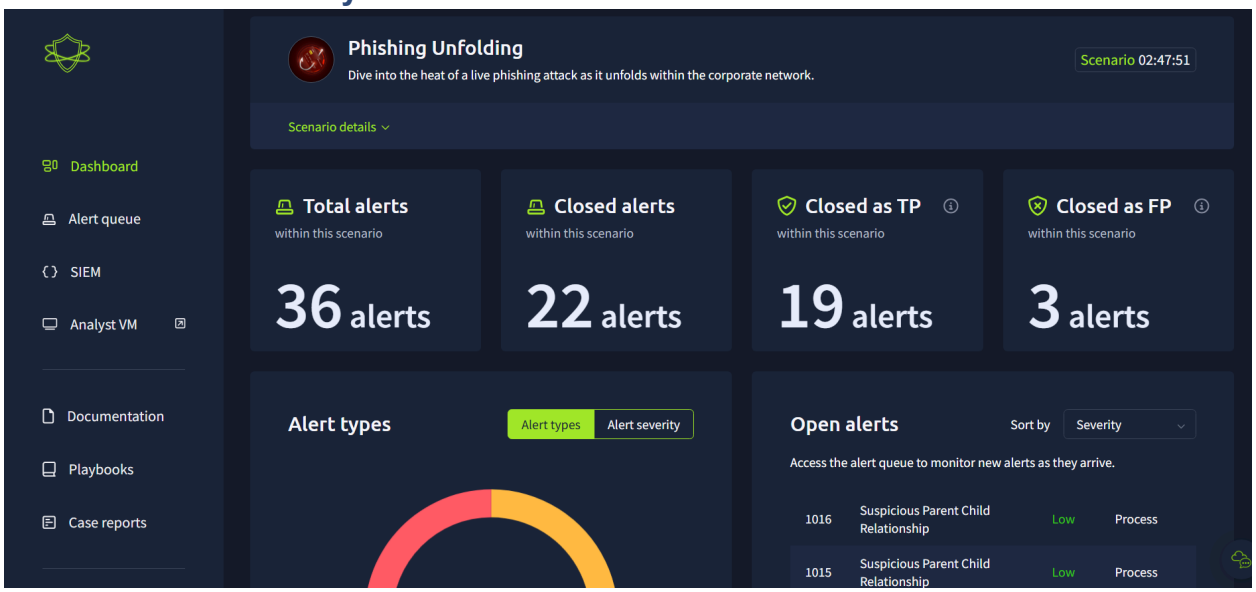


Figure 1 – TryHackMe SOC Metrics Dashboard

Part 2: Technical Incident Report (TIR)

2.1 Incident Overview

On the morning of the incident, a sophisticated spear-phishing campaign successfully compromised the CEO's workstation (win-3450) within the corporate environment. The attacker leveraged social engineering, a malicious .LNK file, a publicly hosted PowerShell reverse-shell script, and DNS tunnelling to establish persistent access and exfiltrate sensitive financial data within a 28-minute window.

2.2 Attack Lifecycle Timeline

All timestamps are derived from Splunk SIEM logs within the TryHackMe environment. The attack maps directly to the MITRE ATT&CK framework phases noted below.

Timestamp	MITRE Phase	Event Description
08:22:49	Initial Access	CEO Michael Ascot receives spear-phishing email from john@hatmakereurope.xyz (subject: "Important Invoice").
08:23:00	Execution	User opens 'ImportantInvoice-February.zip' and extracts a malicious .LNK shortcut file.
08:24:10	Defense Evasion	.LNK file executes a PowerShell script that downloads powercat.ps1 from a public GitHub repository.
08:25:05	Command & Control (C2)	Reverse shell established to an ngrok.io tunnel endpoint from host win-3450.
08:32:20	Discovery	Attacker runs whoami and systeminfo commands to enumerate the CEO workstation.
08:45:00	Lateral Movement Prep	Attacker maps network drive Z: to \\FILESRV-01\SSF-FinancialRecords using net use.
08:50:00	Exfiltration	Attacker uses robocopy, compresses data into exfilt8me.zip, then exfiltrates via DNS tunnelling (nslookup).

Table 2 – Chronological Incident Timeline (Mapped to MITRE ATT&CK)

2.3 Indicators of Compromise (IOCs)

The following indicators were identified through SIEM log analysis and should be immediately propagated to all detection controls, threat intelligence platforms, and shared with peer organisations via appropriate ISACs.

Indicator Type	Indicator Value
Email Sender (Spoofed)	john@hatmakereurope.xyz
Malicious Attachment	ImportantInvoice-February.zip
Download URL	https://raw.githubusercontent[.]com/besimorhino/powercat/master/powercat.ps1

C2 Domain	*.ngrok.io
Compromised User	michael.ascot
Compromised Host	win-3450
Target Network Share	\\FILESRV-01\SSF-FinancialRecords
Exfiltration Method	DNS tunneling via nslookup

Table 3 – Indicators of Compromise (IOCs) – INC-2024-CEO-001

2.4 Investigation Methodology & Splunk Queries

Tools Used:

- Splunk SIEM (TryHackMe SOC Simulator interface)
- Windows Event Viewer (simulated)

Splunk Search Queries Executed:

Query 1 – Identify Initial PowerShell Execution

```
index=* powershell.exe    --> Invoke-WebRequest downloading powercat.ps1 from
raw.githubusercontent.com
```

Query 2 – Confirm C2 Beaconing via ngrok

```
index=*   ngrok.io        -->   Outbound   connections   confirmed   to   ngrok
reverse-tunnel endpoint
```

Query 3 – Identify DNS-based Exfiltration

```
index=*  nslookup.exe     --> Abnormally high volume of DNS lookups with
Base64-encoded data strings
```



Figure 2 – Splunk SIEM: PowerShell Parent Process & nslookup Child Process (Screenshot Placeholder)

Part 3: Executive Summary, Metric Analysis & GRC Strategy

3.1 Executive Summary

On the morning of the incident, at approximately 08:22, the company's CEO received a targeted phishing email disguised as an invoice from a known European partner. The email contained a compressed attachment that, when opened, installed a remote access tool on the CEO's workstation without triggering antivirus alerts.

Within 12 minutes of the email arriving in the inbox, the attacker established a hidden tunnel to the internet and began enumerating the internal network. By 08:45, the attacker had accessed a file server containing sensitive financial records. Within minutes, financial data was compressed and smuggled out of the organisation using DNS queries — a technique that bypasses traditional firewalls because DNS traffic is routinely permitted outbound.

The incident was contained by isolating the CEO's workstation (win-3450) and blocking all outbound traffic to ngrok.io domains. No ransomware was deployed, and no other endpoints showed signs of compromise. However, the confirmed exfiltration of financial records constitutes a data breach requiring legal and compliance notification under applicable frameworks.

3.2 Metric Interpretation & Analysis

Mean Dwell Time – 12 Minutes

A dwell time of 12 minutes means the attacker had unsupervised access to the environment for nearly a quarter of an hour. While this is below the industry average of several hours or days, it was sufficient to:

- Enumerate the local host (whoami, systeminfo)
- Map a network drive to a sensitive file server
- Copy, compress, and exfiltrate financial records via DNS tunnelling

Recommendation: Implement automated endpoint isolation triggered by specific process chains (PowerShell calling net use + robocopy + nslookup) to reduce effective dwell time to under 60 seconds.

True Positive Rate – 95%

This rate indicates excellent detection rule tuning. The 5% false positive rate originated from legitimate IT administrative scripts whose PowerShell patterns overlapped with malicious signatures. The MTTR was marginally inflated because the IT team's update script was initially investigated before being ruled out.

Recommendation: Whitelist verified administrative scripts by hash value and signing certificate within the SIEM to prevent recurrence of this false positive pattern.

3.3 NIST Cybersecurity Framework (CSF 2.0) Mapping

The following table maps identified control failures to the NIST CSF 2.0 framework, providing a structured basis for remediation prioritisation.

NIST Function	Category / Control	Control Failure Observed
PROTECT (PR)	PR.PS-01 – Awareness & Training	CEO lacked training to identify spear-phishing with urgent financial language.
DETECT (DE)	DE.AE-04 – Malicious Code Detection	EDR failed to block powercat.ps1 download from GitHub; native PowerShell execution was permitted.
RESPOND (RS)	RS.MI-01 – Incident Mitigation	No automated isolation policy existed; containment relied on manual analyst action after exfiltration began.

Table 4 – NIST CSF 2.0 Control Failure Mapping

3.4 Remediation Plan

The following remediation controls are recommended for immediate and short-term implementation. Controls are prioritised by risk impact and implementation complexity.

Type	Control Area	Priority	Description
Technical	Email Security	**High**	Deploy sandboxing that recursively extracts/analyses archives (.zip, .rar, .7z) to detect malicious .LNK, .ISO files. Implement delay-based detonation (2–4 minute hold).
Technical	Endpoint Hardening	**High**	Enforce PowerShell Constrained Language Mode for all non-admin users. Block direct downloads from public code repositories (GitHub, GitLab, Pastebin) via endpoint DLP.
Administrative	Policy & Awareness	**Medium**	Mandate quarterly phishing simulations for C-suite and finance personnel (90% pass threshold). Conduct bi-annual Phishing Incident Response Drills.
Administrative	Network Segmentation	**Medium**	Restrict outbound DNS traffic to authorised resolvers only. Deploy DNS filtering to block tunnelling patterns (high-volume encoded queries).

Table 5 – Remediation Plan: Technical & Administrative Controls

Appendix A: References & Standards

- MITRE ATT&CK Framework v14 – https://attack.mitre.org
- NIST Cybersecurity Framework 2.0 – https://www.nist.gov/cyberframework
- TryHackMe SOC Level 1 – Phishing Unfolding Room
- Splunk Search Reference – https://docs.splunk.com

Sentinel Security Services — SOC Incident Response Division