PROJECT_03 – Security Monitoring & Incident Response

Incident Scenarios and Response Steps

Simulated Phishing Attack Exercise

Platform: TryHackMe SOC Simulator – Introduction to Phishing

Date: February 25, 2026

Analyst: Lala Alili

Overview: This document describes a real-time phishing simulation where 4 alerts were triaged. - 1 False Positive - 3 True Positives (all escalated to High severity)

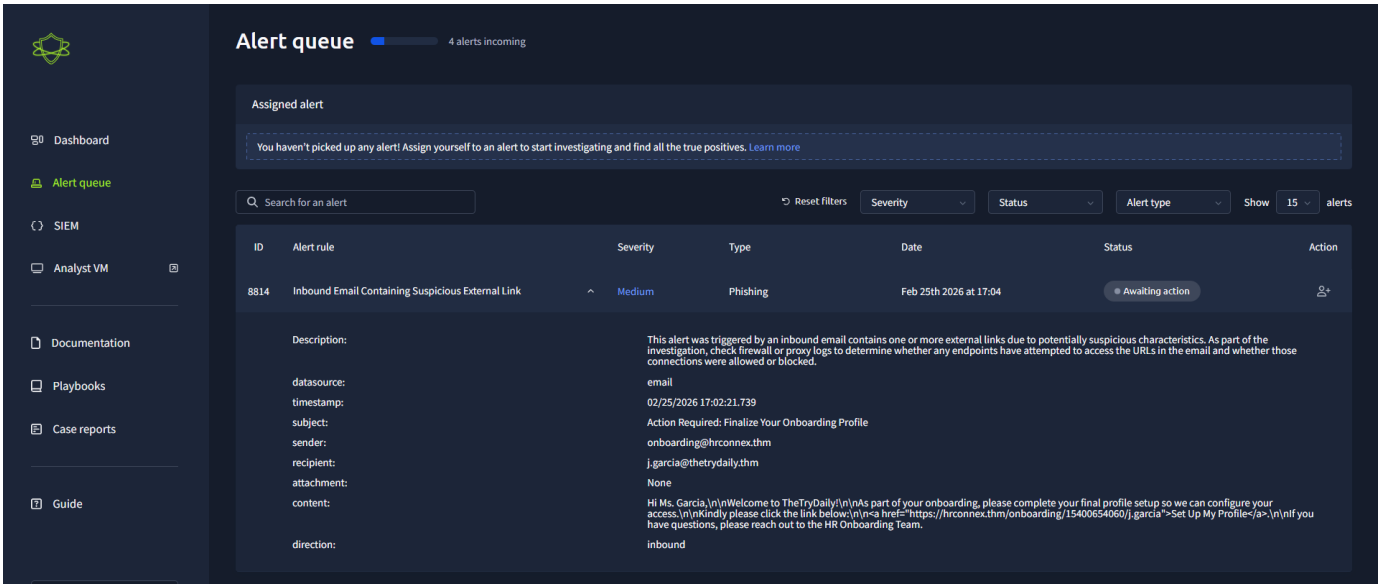
Purpose: Demonstrate SOC triage, classification, escalation and response workflow.

Severity Levels Used

High – Potential credential theft / malware / user compromise

Medium – Suspicious but unconfirmed

Low – False positive or minimal risk



ID: 8814

Alert rule: Inbound Email Containing Suspicious External Link

Description: This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.

Incident type: Phishing

Severity level: Medium

Date and time detected: Feb 25th 2026 at 21:04

Alert details

datasource: email

timestamp: 02/25/2026 17:02:21.739

subject: Action Required: Finalize Your Onboarding Profile

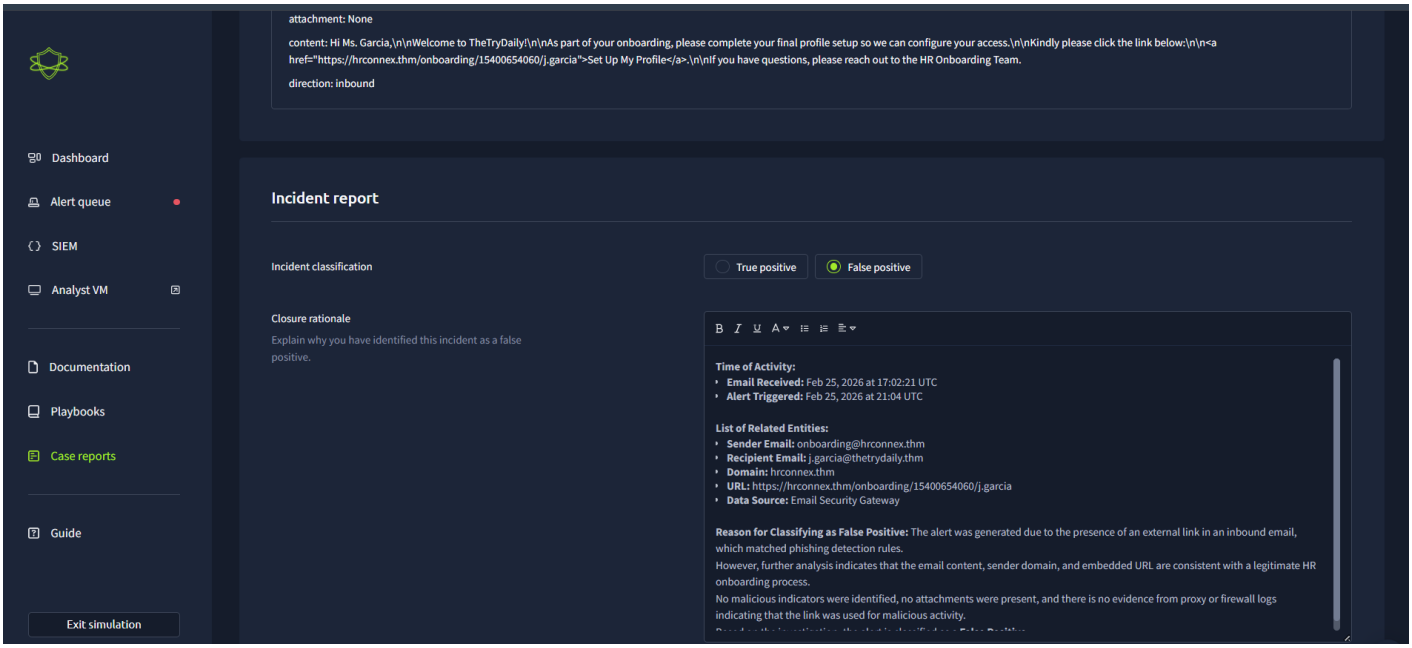
sender: onboarding@hrconnex.thm

recipient: j.garcia@thetrydaily.thm

attachment: None

content: Hi Ms. Garcia,\n\nWelcome to TheTryDaily!\n\nAs part of your onboarding, please complete your final profile setup so we can configure your access.\n\nKindly please click the link below:\n\nSet Up My Profile.\n\nIf you have questions, please reach out to the HR Onboarding Team.

direction: inbound



Incident Report

Time of Activity

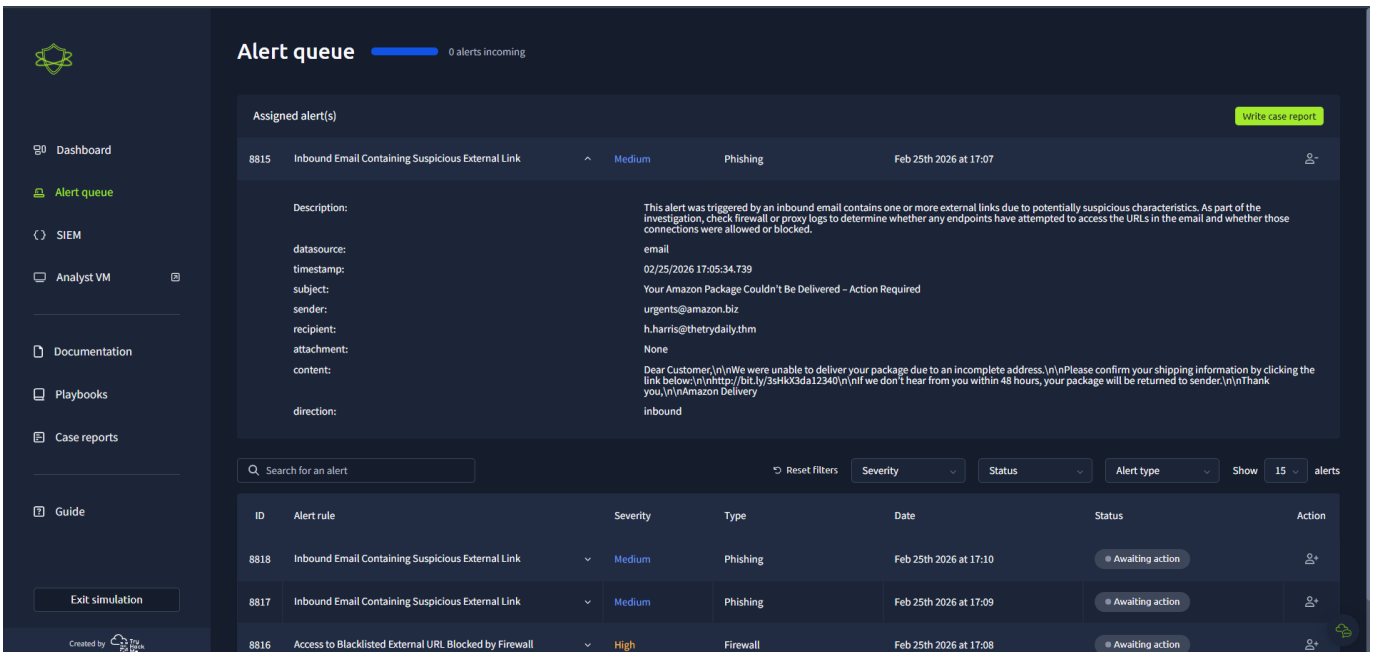
- **Email Received:** Feb 25, 2026 at 17:02:21 UTC
- **Alert Triggered:** Feb 25, 2026 at 21:04 UTC

List of Related Entities

- **Sender Email:** onboarding@hrconnex.thm
- **Recipient Email:** j.garcia@thetrydaily.thm
- **Domain:** hrconnex.thm
- **URL:** https://hrconnex.thm/onboarding/15400654060/j.garcia
- **Data Source:** Email Security Gateway

Reason for Classifying as False Positive

The alert was generated due to the presence of an external link in an inbound email, which matched phishing detection rules.
However, further analysis indicates that the email content, sender domain, and embedded URL are consistent with a legitimate HR onboarding process.
No malicious indicators were identified, no attachments were present, and there is no evidence from proxy or firewall logs indicating that the link was used for malicious activity.
Based on the investigation, the alert is classified as a **False Positive**.



Alert details

Description: This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.

datasource: email

timestamp: 02/25/2026 17:05:34.739

subject: Your Amazon Package Couldn’t Be Delivered – Action Required

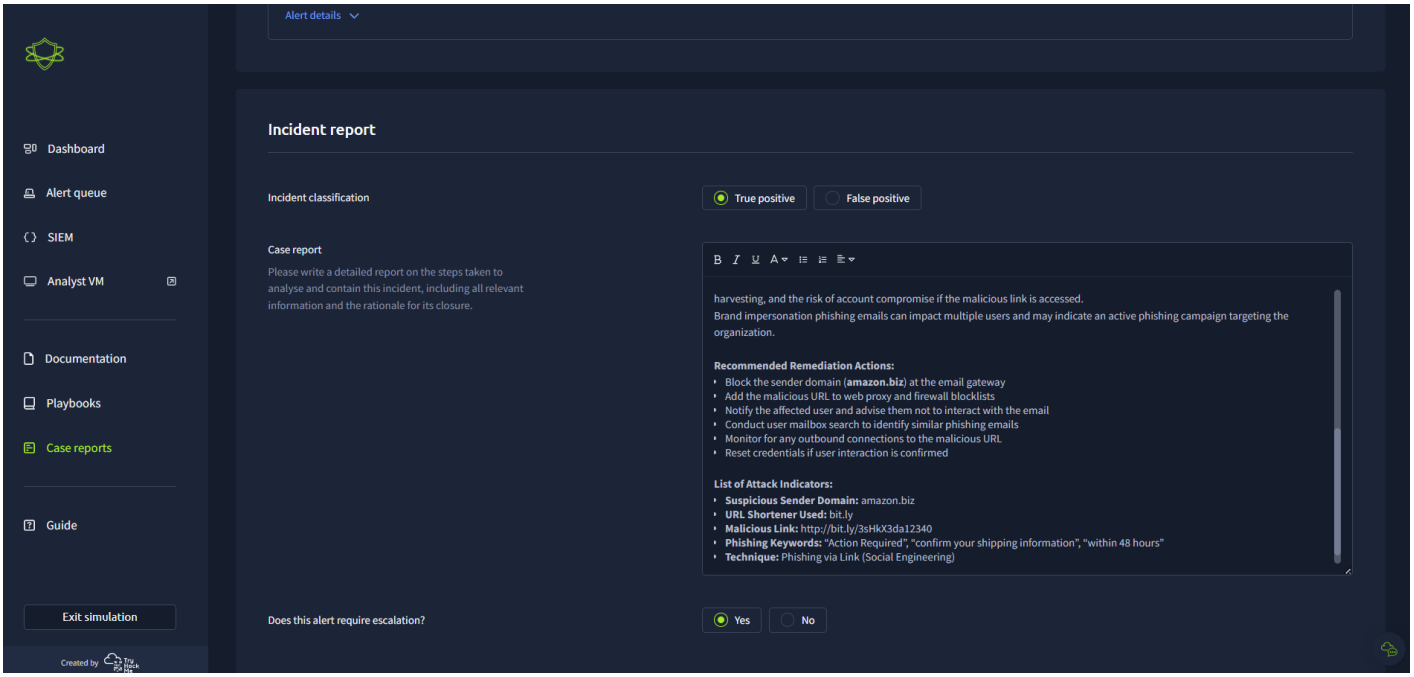
sender: urgents@amazon.biz

recipient: h.harris@thetrydaily.thm

attachment: None

content: Dear Customer,\n\nWe were unable to deliver your package due to an incomplete address.\n\nPlease confirm your shipping information by clicking the link below:\n\nhttp://bit.ly/3sHkX3da12340\n\nIf we don’t hear from you within 48 hours, your package will be returned to sender.\n\nThank you,\n\nAmazon Delivery

direction: inbound



Incident Report

Time of Activity

- **Email Received:** Feb 25, 2026 at 17:05:34 UTC
- **Alert Triggered:** Feb 25, 2026 at 17:05:34 UTC

List of Affected Entities

- **Targeted User:** h.harris@thetrydaily.thm

- **Sender Email:** urgents@amazon.biz
- **Impersonated Organization:** Amazon
- **Malicious URL:** http://bit.ly/3sHkX3da12340
- **Email Infrastructure:** Email Security Gateway

Reason for Classifying as True Positive

The alert demonstrates clear phishing characteristics, including brand impersonation of a well-known organization, a suspicious sender domain that does not match legitimate Amazon domains, and the use of a shortened URL to conceal the final destination.
The email applies urgency and social engineering tactics to coerce the user into clicking the link and providing sensitive information.
Based on these findings, the activity is confirmed as a **True Positive phishing attempt**.

Reason for Escalating the Alert

The alert is escalated due to the high likelihood of user interaction, potential credential harvesting, and the risk of account compromise if the malicious link is accessed.
Brand impersonation phishing emails can impact multiple users and may indicate an active phishing campaign targeting the organization.

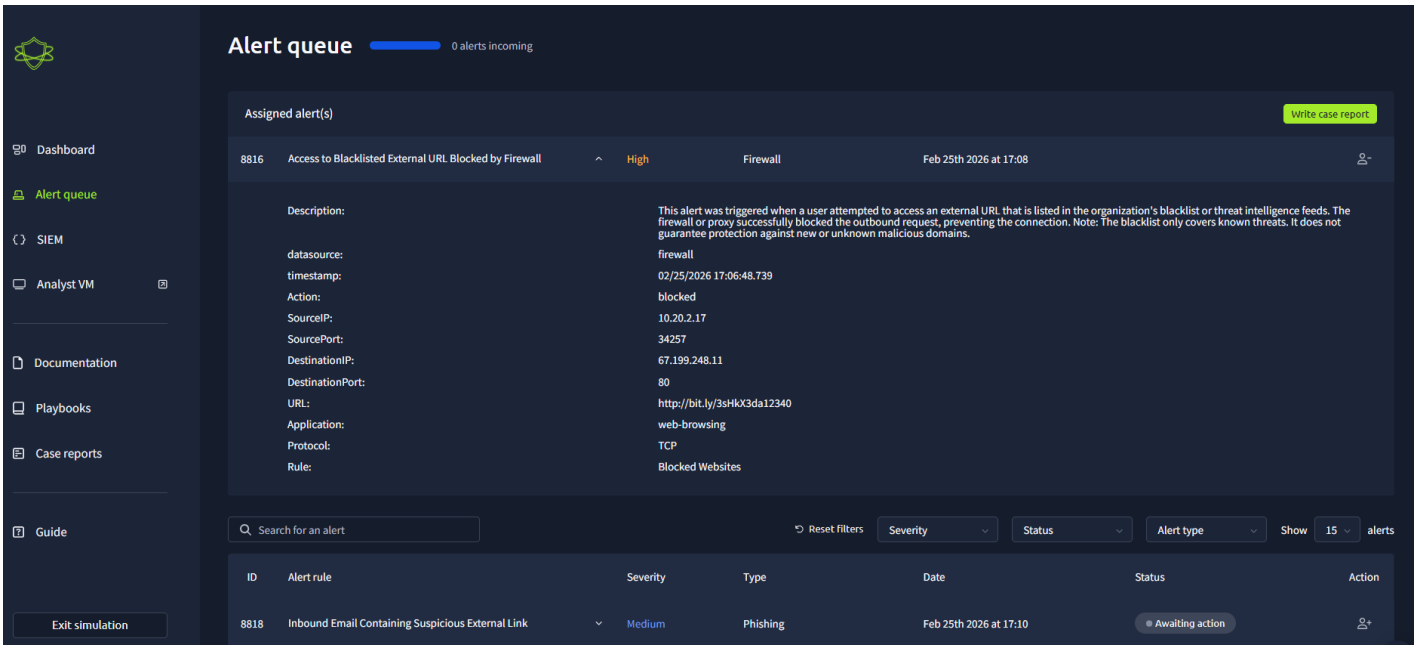
Recommended Remediation Actions

- Block the sender domain (**amazon.biz**) at the email gateway
- Add the malicious URL to web proxy and firewall blocklists
- Notify the affected user and advise them not to interact with the email
- Conduct user mailbox search to identify similar phishing emails
- Monitor for any outbound connections to the malicious URL
- Reset credentials if user interaction is confirmed

List of Attack Indicators

- **Suspicious Sender Domain:** amazon.biz
- **URL Shortener Used:** bit.ly
- **Malicious Link:** http://bit.ly/3sHkX3da12340

- **Phishing Keywords:** “Action Required”, “confirm your shipping information”, “within 48 hours”
- **Technique:** Phishing via Link (Social Engineering)



Description: This alert was triggered when a user attempted to access an external URL that is listed in the organization's blacklist or threat intelligence feeds. The firewall or proxy successfully blocked the outbound request, preventing the connection. Note: The blacklist only covers known threats. It does not guarantee protection against new or unknown malicious domains.

Alert details

datasource: firewall

timestamp: 02/25/2026 17:06:48.739

Action: blocked

SourceIP: 10.20.2.17

SourcePort: 34257

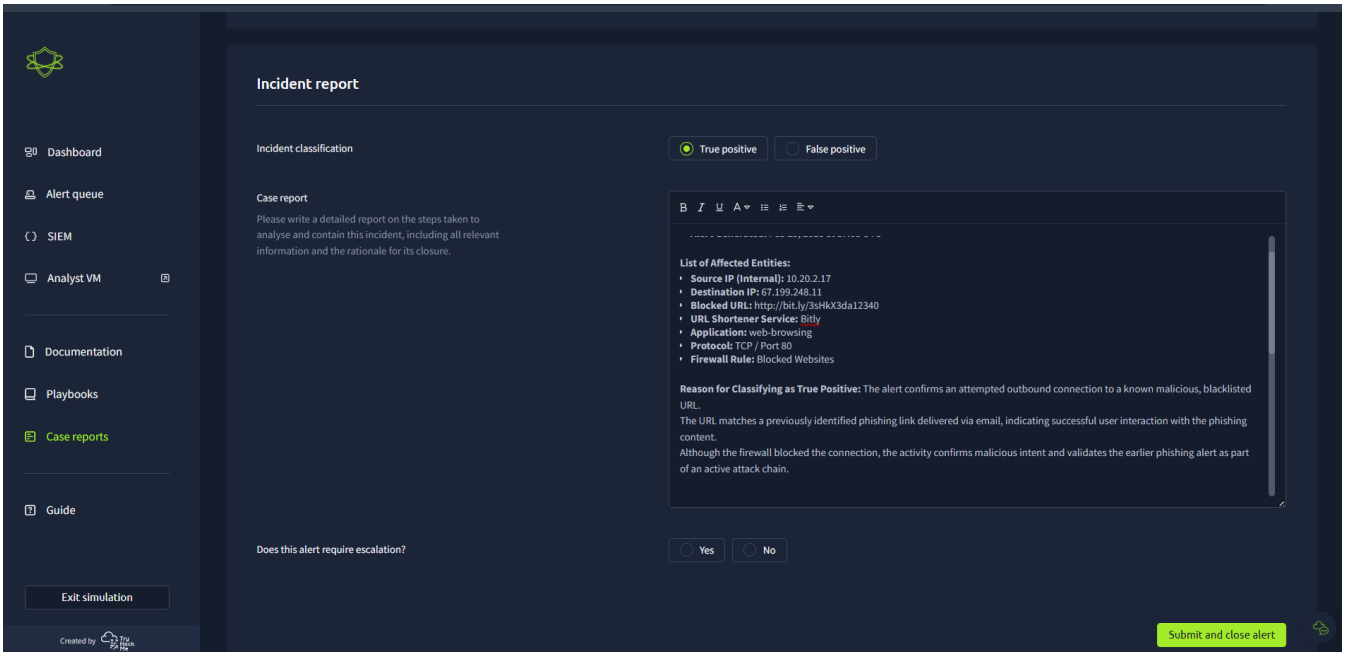
DestinationIP: 67.199.248.11

DestinationPort: 80 URL: http://bit.ly/3sHkX3da12340

Application: web-browsing

Protocol: TCP

Rule: Blocked Websites



Incident Report

Time of Activity

- **Outbound Attempt:** Feb 25, 2026 at 17:06:48 UTC
- **Alert Generated:** Feb 25, 2026 at 17:08 UTC

List of Affected / Related Entities

- **Source IP (Internal):** 10.20.2.17
- **Destination IP:** 67.199.248.11
- **Blocked URL:** http://bit.ly/3sHkX3da12340
- **URL Shortener Service:** Bitly
- **Application:** web-browsing
- **Protocol:** TCP / Port 80
- **Firewall Rule:** Blocked Websites

Reason for Classifying as True Positive

The alert confirms an attempted outbound connection to a known malicious, blacklisted URL. The URL matches a previously identified phishing link delivered via email, indicating successful user interaction with the phishing content.

Although the firewall blocked the connection, the activity confirms malicious intent and validates the earlier phishing alert as part of an active attack chain.

Reason for Escalating the Alert

- User interaction with a confirmed phishing URL
- Potential **credential compromise attempt**
- Indicates **attack progression** (email → click → outbound traffic)
- Requires Tier 2 investigation to assess endpoint impact

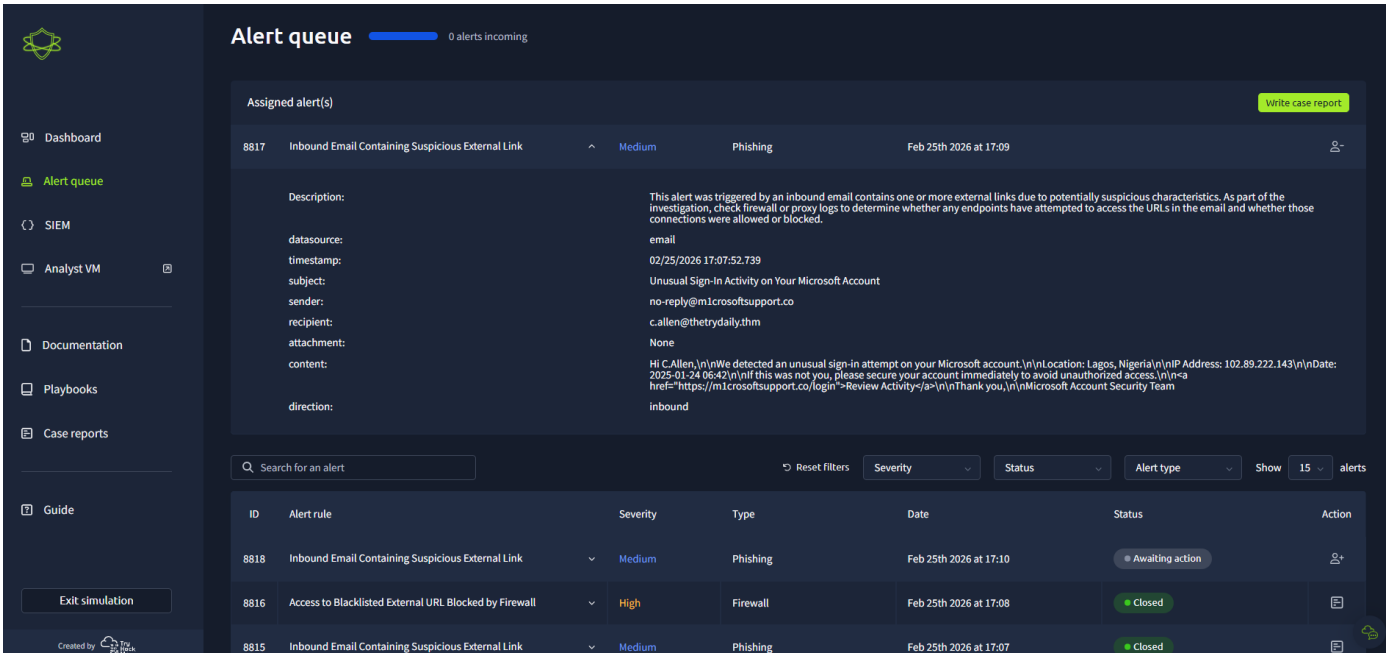
👉 **Blocked ≠ No Incident** (bu SOC-da qızıl qaydadır)

Recommended Remediation Actions

- Identify the user associated with **SourceIP 10.20.2.17**
- Notify and interview the user regarding the phishing email
- Perform endpoint scan on the affected host
- Check browser history and downloads
- Monitor for additional outbound attempts
- Force password reset if credentials were entered
- Ensure the phishing email is removed from all mailboxes

List of Attack Indicators

- **Malicious URL:** http://bit.ly/3sHkX3da12340
- **URL Shortening Service:** Bitly (used to obfuscate destination)
- **Destination IP:** 67.199.248.11
- **Protocol / Port:** TCP / 80
- **Firewall Action:** Blocked (blacklisted URL)
- **Application:** Web-browsing
- **Source IP (Internal):** 10.20.2.17
- **Associated Attack Vector:** Phishing via malicious link
- **Threat Intelligence Match:** URL present in blacklist / TI feeds



Description: This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.

Alert details

datasource: email

timestamp: 02/25/2026 17:07:52.739

subject: Unusual Sign-In Activity on Your Microsoft Account

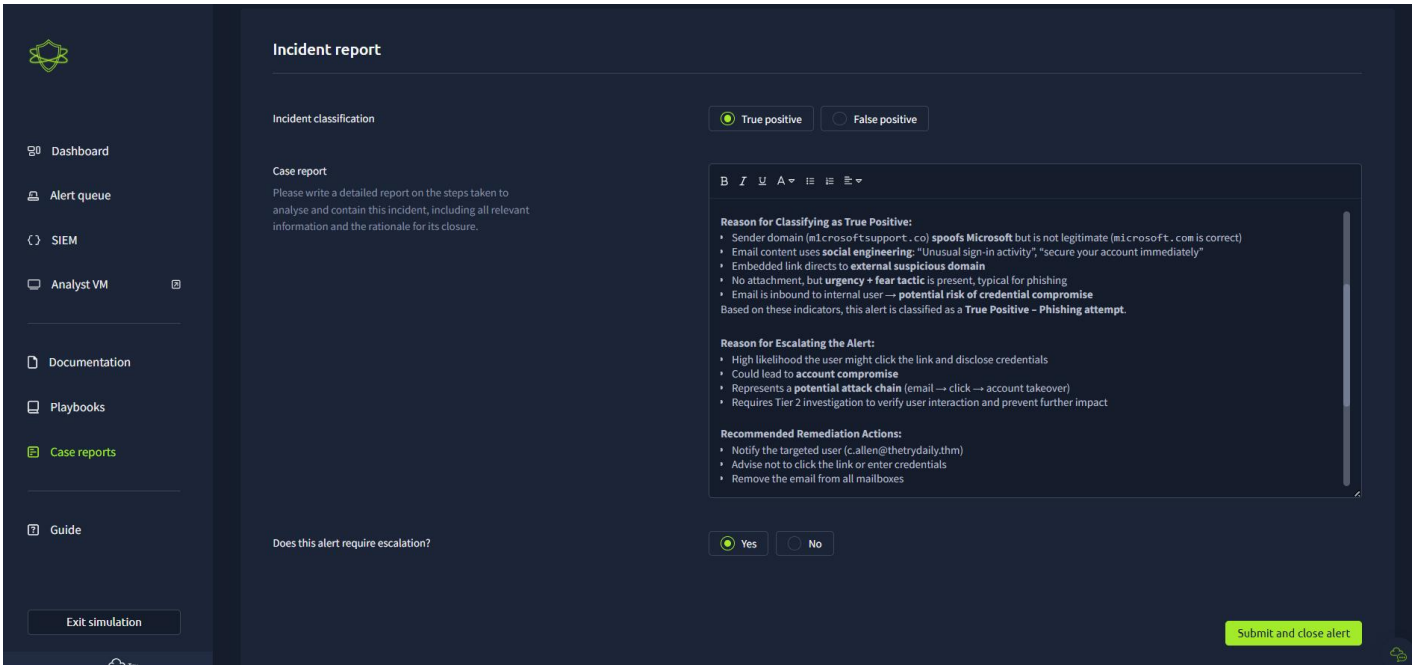
sender: no-reply@m1crosoftsupport.co

recipient: c.allen@thetrydaily.thm

attachment: None

content: Hi C.Allen,\n\nWe detected an unusual sign-in attempt on your Microsoft account.\n\nLocation: Lagos, Nigeria\n\nIP Address: 102.89.222.143\n\nDate: 2025-01-24 06:42\n\nIf this was not you, please secure your account immediately to avoid unauthorized access.\n\nReview Activity\n\nThank you,\n\nMicrosoft Account Security Team

direction: inbound



Incident Report

Time of Activity

- **Email Received:** Feb 25, 2026 at 17:07:52 UTC
- **Alert Triggered:** Feb 25, 2026 at 17:09 UTC

List of Affected / Related Entities

- **Recipient:** c.allen@thetrydaily.thm
- **Sender Email:** no-reply@m1crosoftsupport.co
- **Impersonated Organization:** Microsoft
- **Suspicious URL:** https://m1crosoftsupport.co/login
- **Data Source:** Email Security Gateway

Reason for Classifying as True Positive

- Sender domain (m1crosoftsupport.co) **spoofs Microsoft** but is not legitimate (microsoft.com is correct)
- Email content uses **social engineering**: "Unusual sign-in activity", "secure your account immediately"

- Embedded link directs to **external suspicious domain**
- No attachment, but **urgency + fear tactic** is present, typical for phishing
- Email is inbound to internal user → **potential risk of credential compromise**

Based on these indicators, this alert is classified as a **True Positive – Phishing attempt**.

Reason for Escalating the Alert

- High likelihood the user might click the link and disclose credentials
- Could lead to **account compromise**
- Represents a **potential attack chain** (email → click → account takeover)
- Requires Tier 2 investigation to verify user interaction and prevent further impact

---

Recommended Remediation Actions

- Notify the targeted user (c.allen@thetrydaily.thm)
- Advise not to click the link or enter credentials
- Remove the email from all mailboxes
- Check proxy/firewall logs for any attempted clicks
- Monitor account for suspicious sign-ins
- Reset password if any interaction is confirmed
- Add sender domain to blocklist

List of Attack Indicators

- **Suspicious Sender Domain:** no-reply@m1crosoftsupport.co
- **Malicious URL:** https://m1crosoftsupport.co/login
- **Phishing keywords:** “Unusual Sign-In Activity”, “secure your account immediately”
- **Threat Type:** Credential harvesting / Account phishing
- **Technique:** Social Engineering via Link (MITRE ATT&CK T1566.002)

Summary of Classifications

• Alert 1 (ID 8814 – HR onboarding) → False Positive

• Alert 2 (Amazon impersonation) → True Positive, High

• Alert 3 (Firewall block to malicious URL) → True Positive, High

• Alert 4 (Microsoft impersonation) → True Positive, High

General Response Steps (applied to True Positives)

1. Block sender domain & malicious URL (email gateway, proxy, firewall)

2. Notify affected user – do not click / report email

3. Check proxy/firewall logs for user interaction

4. Endpoint scan on affected host

5. Password reset if click confirmed

6. Mailbox search for similar emails

7. Add IOCs to blocklists

Lessons Learned

This simulation exercise highlighted several critical insights for effective phishing detection and response in a real SOC environment:

- **A blocked outbound connection does not mean the incident is over** If a user has clicked a malicious link (as confirmed by the outbound attempt to a blacklisted URL), an investigation must continue. “Blocked” only prevents further damage — it does not erase the fact that user interaction occurred, which may have already led to credential exposure, malware download, or session hijacking.
- **URL shorteners combined with brand impersonation are high-risk indicators** The use of services like bit.ly to hide the real destination, together with spoofed sender domains (amazon.biz, m1crosoftsupport.co), is a classic and very dangerous phishing pattern. These should trigger immediate high-severity escalation.
- **One phishing email can generate multiple related alerts** A single campaign often produces a chain of events: inbound suspicious email → user click → outbound request to malicious domain. Correlating these alerts (email gateway + proxy/firewall logs) is essential to see the full attack chain and reduce detection time.
- **Fast triage and ongoing user education significantly reduce phishing risk** Quick and accurate alert triage minimizes dwell time, while regular phishing awareness training and simulated campaigns lower the probability of users clicking malicious links in the first place.

These lessons emphasize the importance of layered defenses: strong technical controls (filtering, blocking, correlation) combined with human factors (training, reporting culture) to build resilience against phishing attacks.