

# 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

The screenshot shows the TryHackMe SOC Simulator interface. On the left, there's a sidebar with navigation links: Dashboard, Alert queue (which is selected and highlighted in green), SIEM, Analyst VM, Documentation, Playbooks, Case reports, and Guide. The main area is titled "Alert queue" and shows a progress bar indicating "4 alerts incoming". Below this, a section titled "Assigned alert" displays a message: "You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. Learn more". A search bar and filter buttons for "Reset filters", "Severity", "Status", "Alert type", and "Show 15 alerts" are present. The main table lists one alert:

ID	Alert rule	Severity	Type	Date	Status	Action
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	Feb 25th 2026 at 17:04	<span>Awaiting action</span>	<span>View</span>

Details for the alert ID 8814 are shown in a expanded view:

Description:	Value
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 17:02:21.739
subject:	Action Required: Finalize Your Onboarding Profile
sender:	onboarding@hrconnex.thm
recipient:	j.garcia@trydaily.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 <a href="https://hrconnex.thm/onboarding/15400654060/j.garcia">https://hrconnex.thm/onboarding/15400654060/j.garcia</a> \n\nSet Up My Profile
direction:	inbound

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

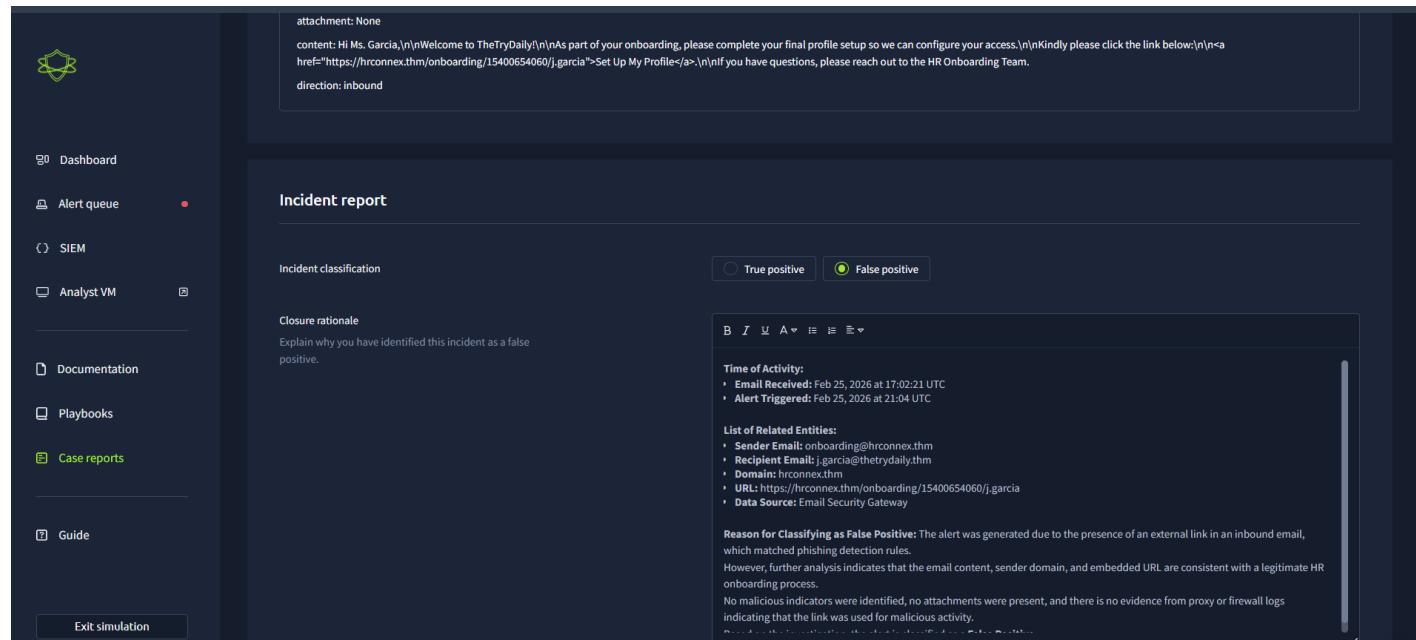
sender: onboard@hrconnex.thm

recipient: j.garcia@thetrydaily.thm

attachment: None

content: Hi Ms. Garcia,  
Welcome to TheTryDaily!  
As part of your onboarding, please complete your final profile setup so we can configure your access.  
Kindly please click the link below:  
[Set Up My Profile](https://hrconnex.thm/onboarding/15400654060/j.garcia)  
If you have questions, please reach out to the HR Onboarding Team.

direction: inbound



The screenshot shows the 'Alert details' page with the following information:

- attachment:** None
- content:** Hi Ms. Garcia,  
Welcome to TheTryDaily!  
As part of your onboarding, please complete your final profile setup so we can configure your access.  
Kindly please click the link below:  
[Set Up My Profile](https://hrconnex.thm/onboarding/15400654060/j.garcia)  
If you have questions, please reach out to the HR Onboarding Team.
- direction:** inbound

The 'Incident report' section shows the following details:

- Incident classification:** False positive (selected)
- Closure rationale:** Explain why you have identified this incident as a false positive.
- 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: onboard@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.

## 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**.

The screenshot shows the Alert queue interface. The main panel displays an alert titled "8815 Inbound Email Containing Suspicious External Link". The alert is categorized as "Medium" severity and "Phishing". It was created on "Feb 25th 2026 at 17:07". The "Description" field contains a detailed log of the investigation, noting that the alert was triggered by an inbound email containing one or more external links. The "datasource" is listed as "email", with a timestamp of "02/25/2026 17:05:34.739". The "subject" is "Your Amazon Package Couldn't Be Delivered - Action Required", and the "sender" is "urgents@amazon.biz". The "recipient" is "h.harris@thetrydaily.thm". The "content" field shows the email body, which includes a message about an incomplete address and a link to a tracking page. The "direction" is "inbound". Below this, a table lists three alerts, all of which are currently "Awaiting action". The columns in the table are ID, Alert rule, Severity, Type, Date, Status, and Action.

ID	Alert rule	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	Feb 25th 2026 at 17:10	Awaiting action	
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	Feb 25th 2026 at 17:09	Awaiting action	
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	Feb 25th 2026 at 17:08	Awaiting action	

## 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

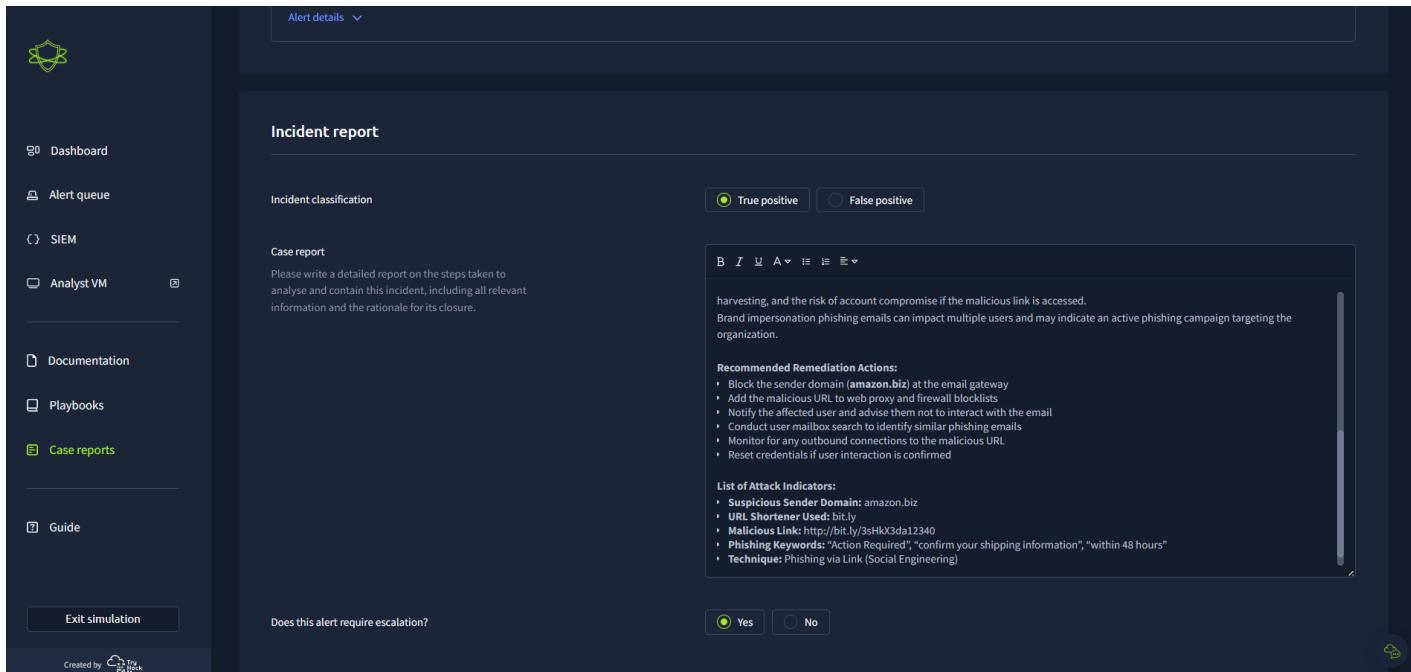
sender: urgents@amazon.biz

recipient: h.harris@thetrydaily.thm

attachment: None

content: Dear Customer,  
We were unable to deliver your package due to an incomplete address.  
Please confirm your shipping information by clicking the link below:  
<http://bit.ly/3sHkX3da12340>  
If we don't hear from you within 48 hours, your package will be returned to sender.  
Thank you,  
Amazon Delivery

direction: inbound



The screenshot shows a dark-themed user interface for managing security alerts. On the left is a sidebar with navigation links: Dashboard, Alert queue, SIEM, Analyst VM, Documentation, Playbooks, Case reports (which is selected), and Guide. At the bottom of the sidebar are buttons for 'Exit simulation' and 'Created by [redacted]'. The main area has a header 'Alert details' with a dropdown arrow. Below it is a section titled 'Incident report' with a sub-section 'Case report'. It contains a text input field with placeholder text: 'Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.' To the right of this is a 'List of Attack Indicators' table with columns for indicator type, name, and description. The table includes rows for Suspicious Sender Domain, URL Shortener Used, Malicious Link, Phishing Keywords, and Technique. At the bottom of the main area are two radio buttons for 'True positive' and 'False positive', and another for 'Yes' or 'No' regarding alert escalation.

## 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)

The screenshot shows the Alert queue interface. On the left, there's a sidebar with navigation links: Dashboard, Alert queue (which is selected and highlighted in green), SIEM, Analyst VM, Documentation, Playbooks, Case reports, and Guide. Below the sidebar is a button labeled "Exit simulation". The main area is titled "Alert queue" and shows "0 alerts incoming". It displays a single assigned alert (ID 8816) with the following details:

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.				
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:	<a href="http://bit.ly/3sHkX3da12340">http://bit.ly/3sHkX3da12340</a>				
Application:	web-browsing				
Protocol:	TCP				
Rule:	Blocked Websites				

Below this, there's a search bar and filter options for "Reset filters", "Severity", "Status", "Alert type", and "Show 15 alerts". A second alert (ID 8818) is listed in the alert queue table:

ID	Alert rule	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	Feb 25th 2026 at 17:10	Awaiting action	

**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

The screenshot shows a dark-themed user interface for an incident report. On the left, a sidebar lists navigation options: Dashboard, Alert queue, SIEM, Analyst VM, Documentation, Playbooks, Case reports (which is selected), and Guide. At the bottom of the sidebar is an 'Exit simulation' button. The main content area has a header 'Incident report'. Under 'Incident classification', there are two radio buttons: 'True positive' (selected) and 'False positive'. Below this is a 'Case report' section with a text input placeholder: 'Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.' To the right of the case report is a 'List of Affected Entities' table with the following data:

	B	I	A	IE	EE
List of Affected Entities:					
• Source IP (Internal):	10.20.2.17				
• Destination IP:	67.199.248.11				
• Blocked URL:	<a href="http://bit.ly/3sHkX3da12340">http://bit.ly/3sHkX3da12340</a>				
• URL Shortener Service:	Bitly				
• Application:	web-browsing				
• Protocol:	TCP / Port 80				
• Firewall Rule:	Blocked Websites				

Below the table is a 'Reason for Classifying as True Positive' section with the following text:

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.

At the bottom of the main content area are 'Yes' and 'No' radio buttons for 'Does this alert require escalation?'. In the bottom right corner, there is a 'Submit and close alert' button.

## 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@microsoftsupport.co](mailto:no-reply@microsoftsupport.co)

recipient: [c.allen@thetrydaily.thm](mailto:c.allen@thetrydaily.thm)

attachment: None

content: Hi C.Allen,  
We detected an unusual sign-in attempt on your Microsoft account.  
Location: Lagos, Nigeria  
IP Address: 102.89.222.143  
Date: 2025-01-24 06:42  
If this was not you, please secure your account immediately to avoid unauthorized access.  
<a href="https://m1crosoftsupport.co/login">Review Activity</a>  
Thank you,  
Microsoft 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.