How I triaged alerts in TryHackMe's Phishing SOC Simulation

TryHackMe is an exceptional platform, one that I have used for the last 3 or so years. The platform has come under fire by some professionals in the industry, especially after promoting the SAL1 (Security Analyst Level 1) Certificate as a relevant practical experience that can land you entry-level security analyst positions. Like most, I believe that there is no single cert there that can guarantee a job. Whilst certs like the Security+, A+, Net+, and BTL1 can certainly help you reach that goal, they do not guarantee employment. In my opinion, all these certs, including those from TryHackMe, demonstrate your ability and passion to learn, even if the content is not entirely applicable or relevant.

The Introduction to Phishing scenario serves as a means for students or new analysts to practice their triage skills, especially in relation to phishing based alerts. Whilst my SOC experience is minimal, I can confirm that the skills acquired and process of triaging alerts in the simulation are directly applicable to real life L1 analyst duties. As the name suggests, TryHackMe SOC simulations attempt to mimic real world SOC environments. You are given access to an alert feed, analyst VM, and a Splunk instance. Once you have completed the simulation, you are provided with your results, including:

- True positive identification rate
- False positive identification rate
- Number of closed alerts
- Mean time to resolve (MTTR)
- Mean dwell time, and
- AI analysis of your reports/summaries

Alert Summaries and Analysis

This simulation involved 5 alerts; the alert summaries I wrote for each are as follows:

Alert 1: Inbound Email Containing Suspicious External Link

Alert Summary:

subject: Action Required: Finalize Your Onboarding Profile

sender: onboarding@hrconnex.thm

recipient: j.garcia@thetrydaily.thm

url: https://hrconnex.thm/onboarding/15400654060/j.garcia

On July 1st, 2025, the user j.garcia received an email appearing to originate from a HR service (onboarding@hrconnex.thm) requesting completion of an onboarding profile. The embedded URL is not currently flagged by threat intelligence sources, but its characteristics warrant further scrutiny.

- The URL has only been observed twice, both directed to j.garcia, indicating a targeted delivery.

- The HR-themed lure is consistent with phishing tactics.

Alert 2: Access to Blacklisted External URL Blocked by Firewall

Alert Summary:

Action: blocked

SourceIP: 10.20.2.17

SourcePort: 34257

DestinationIP: 67.199.248.11

DestinationPort: 80

URL accessed: http://bit.ly/3sHkX3da12340

user: h.harris@thetrydaily.thm

On July 1st, 2025, user h.harris attempted to access a bit.ly shortened URL which was flagged and blocked by the firewall. The destination IP of this domain is 67.199.248.11. Both the destination IP and accessed URL are listed as malicious in threat intelligence sources.

- Shortened URL usage (bit.ly) is frequently associated with obfuscation tactics used in phishing campaigns.

- Both the destination IP and URL were flagged as malicious.

- The destination IP and URL were only observed once in the environment, indicating a targeted attempt.

Alert 3: Inbound Email Containing Suspicious External Link

Alert Summary:

subject: Action Required: Finalize Your Onboarding Profile

sender: onboarding@hrconnex.thm

recipient: j.garcia@thetrydaily.thm

url: https://hrconnex.thm/onboarding/15400654060/j.garcia

On July 1st, 2025, the user j.garcia received an email appearing to originate from a HR service (onboarding@hrconnex.thm) requesting completion of an onboarding profile. This is the same email as observed in case ID: 8818. The embedded URL is not currently flagged by threat intelligence sources, but its characteristics warrant further scrutiny.

- The URL has only been observed twice, both directed to j.garcia, indicating a targeted delivery.

- The HR-themed lure is consistent with phishing tactics.

Alert 4: Inbound Email Containing Suspicious External Link

Alert Summary:

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

sender: urgents@amazon.biz

recipient: h.harris@thetrydaily.thm

url: http://bit.ly/3sHkX3da12340

On July 1st, 2025, user h.harris received a phishing email impersonating Amazon, claiming a failed delivery and urging the recipient to act. The email contained a malicious shortened URL,

which was clicked by the user, as evident in case ID: 8816. The request was subsequently blocked by the firewall.

- The shortened link (bit.ly) resolved to a known malicious IP.

- The email used urgency as a social engineering tactic, which is common in phishing emails.

- The domain amazon.biz is not a legitimate Amazon domain.

Alert 5: Inbound Email Containing Suspicious External Link

Alert Summary:

subject: Unusual Sign-In Activity on Your Microsoft Account

sender: no-reply@m1crosoftsupport.co

recipient: c.allen@thetrydaily.thm

attachment: None

url: https://m1crosoftsupport.co/login

SourceIP: 10.20.2.25

SourcePort: 32653

DestinationIP: 45.148.10.131

DestinationPort: 443

At 03:00 on July 1st, 2025, user c.allen received a phishing email impersonating Microsoft using a typosquatted domain (m1crosoftsupport.co). Within 2 minutes, the user accessed the embedded malicious URL, indicating a high likelihood of user interaction with a credential harvester.

- The domain includes a 1 instead of I, a classic typosquatting technique.

- The destination IP and URL are both flagged as malicious.

Investigative Process

My approach to investigating these alerts was simple. Take for instance the fifth alert, all I needed to do was look at the content of the alert, gather the key artefacts like the sender, recipient, embedded urls, etc, and then pivot from there. I determined that the URL within the email and the destination IP were both flagged as malicious by the threat intelligence tool, and was also able to correlate the email alert with a DNS log, meaning the user did request that URL (i.e., they clicked the link).

Reflections & Application

Engaging with these TryHackMe simulations has improved my understanding of the basic alert triage process. By analysing legitimate threats, I have also enhanced my ability to quickly recognise phishing attacks, skills that are transferable to many roles. For those interested in the security operations side of things, or general blue teaming, I highly recommend completing this simulation, among the others offered by TryHackMe.