

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
8814	Inbound Email Containing Suspicious External Link	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.	Phishing	Medium	Nov 30th 2025 at 12:15

Alert details ^

datasource: email

timestamp: 11/30/2025 04:13:27.186

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 click the link below:\n[Set Up My Profile](https://hrconnex.thm/onboarding/15400654060/j.garcia)\n\nif you have questions, please reach out to the HR Onboarding Team.

direction: inbound

## Incident report

Incident classification

True positive  False positive

### Closure rationale

Explain why you have identified this incident as a false positive.

B I U A ⌂ ⌂ ⌂ ⌂

Time of Activity: 11/30/2025 04:13:27.186

List of Related Entities:

sender: onboarding@hrconnex.thm  
recipient: j.garcia@thetrydaily.thm  
attachment: None  
Link: <https://hrconnex.thm/onboarding/15400654060/j.garcia>

Reason for Classifying as False Positive: The email that j.garcia@thetrydaily.thm received is from THM HR asking her to complete her info as part of the onboarding process

Submit and close alert

**Complete IR:**

Time of Activity: 11/30/2025 04:13:27.186

List of Related Entities:

sender: onboarding@hrconnex.thm

recipient: j.garcia@thetrydaily.thm

attachment: None

Link: <https://hrconnex.thm/onboarding/15400654060/j.garcia>

Reason for Classifying as False Positive: The email that j.garcia@thetrydaily.thm received is from THM HR asking her to complete her info as part of the onboarding process