

TryHackMe Case Study - 1

Case report for event ID: 8816

Scenario:

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
8816	Access to Blacklisted External URL Blocked by Firewall	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.	Firewall	High	Nov 11th 2025 at 10:46

Alert Details:

```
datasource: firewall
timestamp: 11/11/2025 04:58:44.287
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:

Incident Classification: False Positive

Explanation:

Time of Activity: 10:46 AM on 11/11/2025

List of Related Entities:

Source IP: 10.20.2.17

Destination IP: 67.199.248.11

SourcePort: 34257

DestinationPort: 80

URL: <http://bit.ly/3sHkX3da12340>

Reason for Classifying as False Positive:

The reason this event was classified as a False Positive is because the user tried to access an external URL that had been blacklisted on the firewall. There were no other signs of attack, the alert was only created due to a trigger action from the firewall. Hence, No attack but delivered an alert

TryHackMe Case Study - 2

Case report for event ID: 8814

Scenario

Assigned alert(s)

8814 Inbound Email Containing Suspicious External Link Medium Phishing Nov 11th 2025 at 04:58

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: 11/11/2025 04:56:21.287

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

Playbook link

Write case report

Checking Email data on SPLUNK:

11/11/25
5:00:16.287 AM { [-]
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.
datasource: email
direction: inbound
recipient: j.garcia@thetrydaily.thm
sender: onboarding@hrconnex.thm
subject: Action Required: Finalize Your Onboarding Profile
timestamp: 11/11/2025 05:00:16.287
}
Show as raw text

Type	Field	Value	Actions
Selected	host	10.10.86.212:8989	▼
	source	eventcollector	▼
	sourcetype	_json	▼
Event	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 \n\nIf you have questions, please reach out to the HR Onboarding Team.	▼
	datasource	email	▼
	direction	Inbound	▼
	recipient	j.garcia@thetrydaily.thm	▼
	sender	onboarding@hrconnex.thm	▼
	subject	Action Required: Finalize Your Onboarding Profile	▼
	timestamp	11/11/2025 05:00:16.287	▼
Time	_time	2025-11-11T05:00:16.287+00:00	▼
Default	index	main	▼
	linecount	1	▼
	punct	***;***//***;*** : ***;***;***;***;	▼

The email looks legitimate, the sender email and the link have the same information and the email does not create much of an emergency. It is like a notice for the final step.

Checking the URL on “trydetectthis.thm” on the Analyst VM they have provided

The screenshot shows a web browser window titled "TryDetectThis". The address bar indicates "Not secure | www.trydetectthis.thm/". The main content area has two tabs: "URL/IP Check" (selected) and "File Analysis". Under "URL/IP Check", there is a "URL/IP Security Check" section with the sub-instruction "Analyze any URL or IP address for potential security threats". A text input field contains the URL "https://hrconnex.thm/onboarding/15400654060/j.garcia". Below the input field is a large green button labeled "Analyze URL/IP". Further down, a message box displays "URL/IP Analysis Complete" with "Status: CLEAN". The system tray at the bottom right shows the date and time as "5:21 AM 11/11/2025".

It states that the URL is “CLEAN”

Incident Report:

Incident Classification: False Positive

Explanation:

Time of Activity: 10:43 AM on 11/11/2025

List of Related Entities:

sender: onboarding@hrconnex.thm

recipient: j.garcia@thetrydaily.thm

URL on the Email: <https://hrconnex.thm/onboarding/15400654060/j.garcia>

Reason for Classifying as False Positive:

The reason this event was classified as a False Positive is because after the Email analysis, the contents within the email appears to be legitimate. The sender email address and the URL

provided in the email appears to be from the same context.

The results from SPLUNK don't display any suspicious information about the email. Simultaneously, results from "TryDetectThis.thm" also finalizes the URL as "CLEAN". The email was only triggered as an alert due to its source being external. No malicious attachments or suspicious contents were identified. Hence, the incident being a "False Positive".