

Simulated SOC: Intro to Phishing

by

(TryHackMe's SOC Simulator)

Date: 10.05.2025

Project: Simulated SOC: Intro to Phishing Project

Contents

Executive Summary-----	2
Introduction-----	2
Project Scenarios Objectives-----	3
1. Introduction to Phishing-----	3
2. Phishing Unfolding-----	4
Disclaimer -----	5
Introduction to Phishing scenario-----	5
Phishing Unfolded scenario -----	36
References -----	36
Tools-----	36

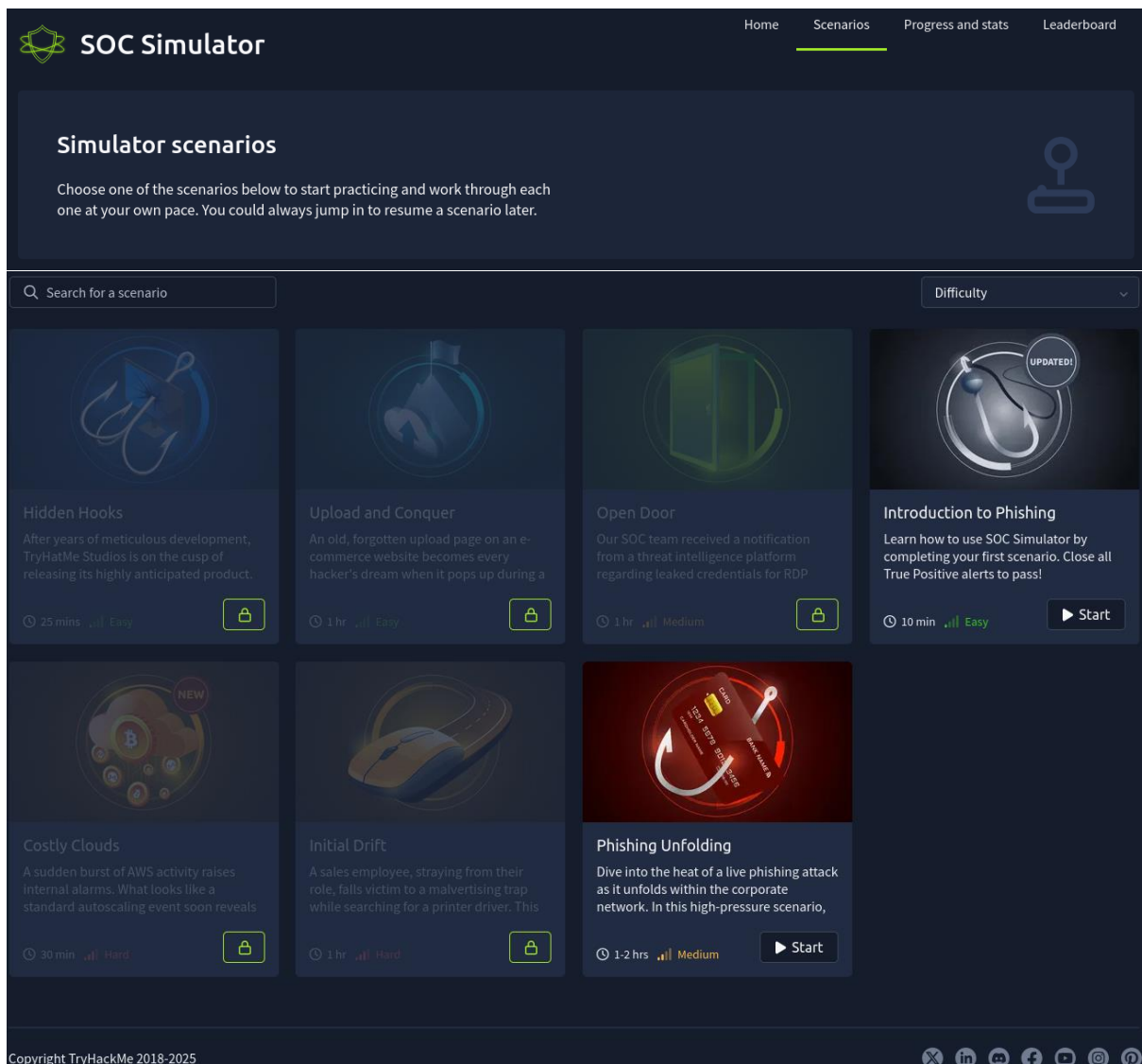
Executive Summary

Introduction

The TryHackMe “SOC Simulator” service is an interactive platform designed to simulate real-world Security Operations Center (SOC) environments. The simulator includes a dashboard, alert queue, built in SIEM (Splunk) and an analyst VM workstation for threat intel investigations.

It provides scenarios involving phishing attacks, malware, and insider threats, requiring users to investigate alerts, classify incidents, and write reports. The purpose of this project is to practice incident response skills in a simulated realistic setting, document the investigative process, and provide possible recommendations based on the findings.

The SOC Simulator service includes 7 unique scenarios to tackle as a simulated SOC analyst. However, most of these scenarios are restricted to Business users, intended for corporate environments only. For individual users, only two scenarios are currently accessible to premium users like myself, both centered around phishing-based threats.



This project will cover, engage in and document actions primarily focused on phishing attacks through the “Introduction to Phishing” and “Phishing Unfolded” scenarios through the SOC Simulator.

Project Scenarios Objectives

1. Introduction to Phishing

Difficulty: Easy | **Duration:** 1 hour

SOC Simulator protect (TryHackMe)

By Thomas Lium

Description:

This is a beginner-level scenario designed to introduce users phishing via the SOC Simulator platform. It teaches how to:

Task Objective:

- Monitor and analyze real-time alerts.
- Identify and document critical events such as suspicious emails and attachments.
- Close all True Positive alerts to pass
- Create detailed case reports based on your observations to help your team understand the full scope of alerts and malicious activity.

Skills Gained:

- Basic alert handling
- Understanding and analyzing phishing behavior
- Basic Splunk SIEM search query
- Working with a simulated SOC dashboard

2. Phishing Unfolding

Difficulty: Moderate | **Duration:** 1-2 hours

Description:

This is a more advanced scenario that simulates a **live phishing attack** within an organization. The attacker sends a phishing email, which leads to:

- A user clicking a malicious link or attachment
- Execution of suspicious PowerShell commands
- Potential credential theft or lateral movement
- Persistent activity by the attacker inside the network

Task Objective:

To investigate a multi-stage phishing attack — from initial email delivery to compromise — and understand how such attacks unfold in real time.

- Monitor and analyze real-time alerts as the attack unfolds.
- Identify and document critical events such as PowerShell executions, reverse shell connections, and suspicious DNS requests.
- Create detailed case reports based on your observations to help the team understand the full scope of the breach.

Skills Gained:

- Incident investigation

SOC Simulator protect (TryHackMe)

By Thomas Lium

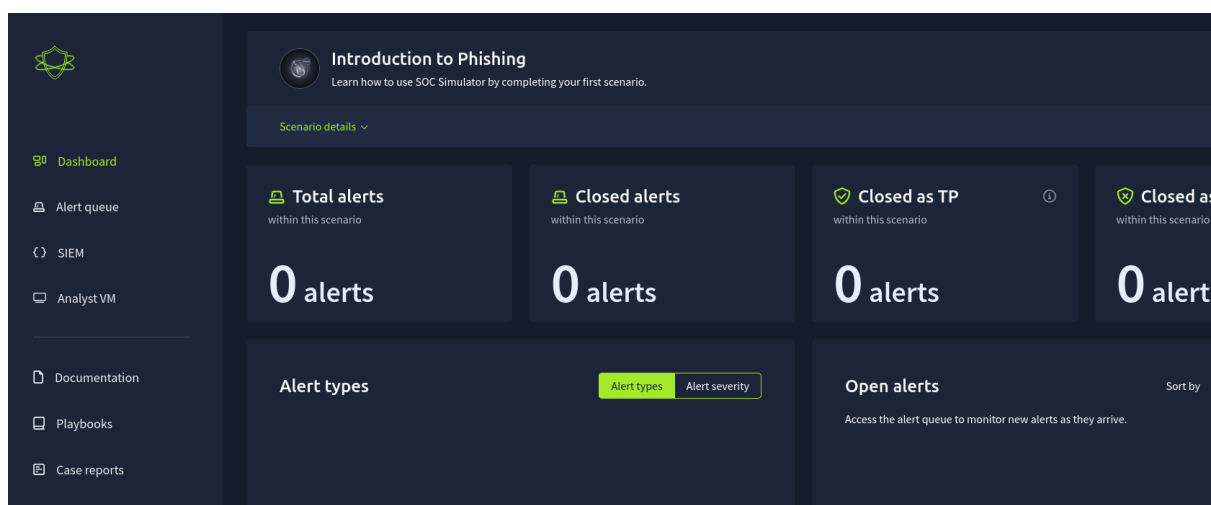
- Analyzing phishing-related behavior
- Threat detection and response
- Writing SOC case reports

Disclaimer

This project is for educational and training purposes only. All scenarios and activities were conducted within the controlled environment provided by TryHackMe's SOC Simulator. No real systems, networks, or users were involved.

Introduction to Phishing scenario

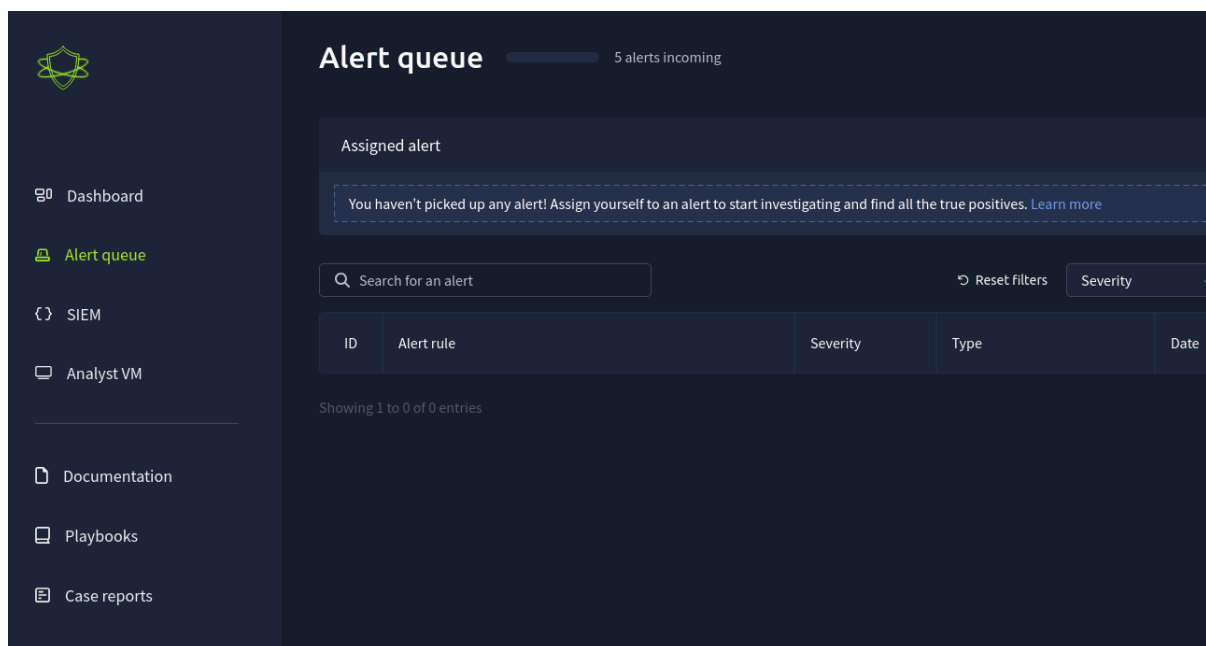
Once the environment has loaded up, we are greeted at the Dashboard in the SOC Simulator platform. From here, it will take a few minutes for the incident alerts to come in real time. But before that happens, let's further explore the SOC Simulator.



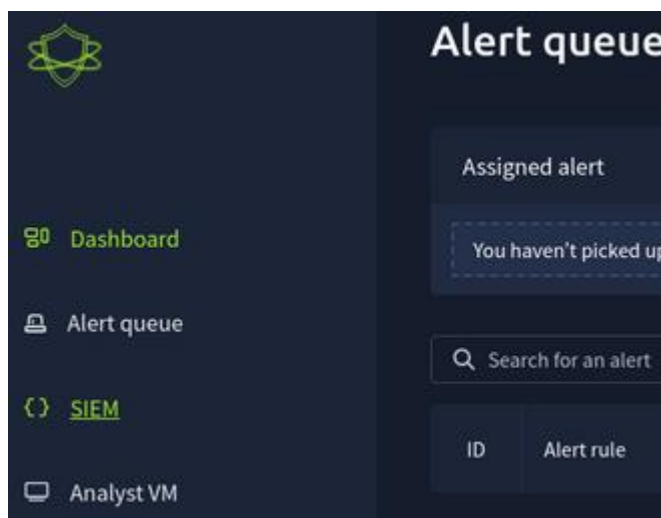
SOC Simulator protect (TryHackMe)

By Thomas Lium

Under dashboard section is “Alert Queue”, where alerts will be accessible as they come in. This is where initial alerts will be triggered and shown with information on incident. Information within the alerts will be used to do further investigation of event and its contents.



Under the alert queue is a built in SIEM based on Splunk to be used analyze logs regarding the incoming alerts to gain a better understanding and look for additional information.



By clicking the SIEM, we are redirected to the splunk server within the simulator.

splunk>enterprise

Apps

Messages

Settings

Search

Analytics

Datasets

Reports

Alerts

Dashboards

New Search

1 *

Server error

34 of 34 events matched

No Event Sampling

Job

Events (34)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

List

Format

50 Per Page

Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Action 1

a Application 1

a attachment 1

a content 16

a datasource 2

a DestinationIP 10

Time

Event

5/17/25

3:48:50.540 PM

attachment: None

content: We would love to schedule a live demonstration to showcase our product capabilities Let us know a time that works for your team

datasource: email

direction: inbound

recipient: j.carter@thetrydaily.thm

sender: gamble@headwearreporter.net

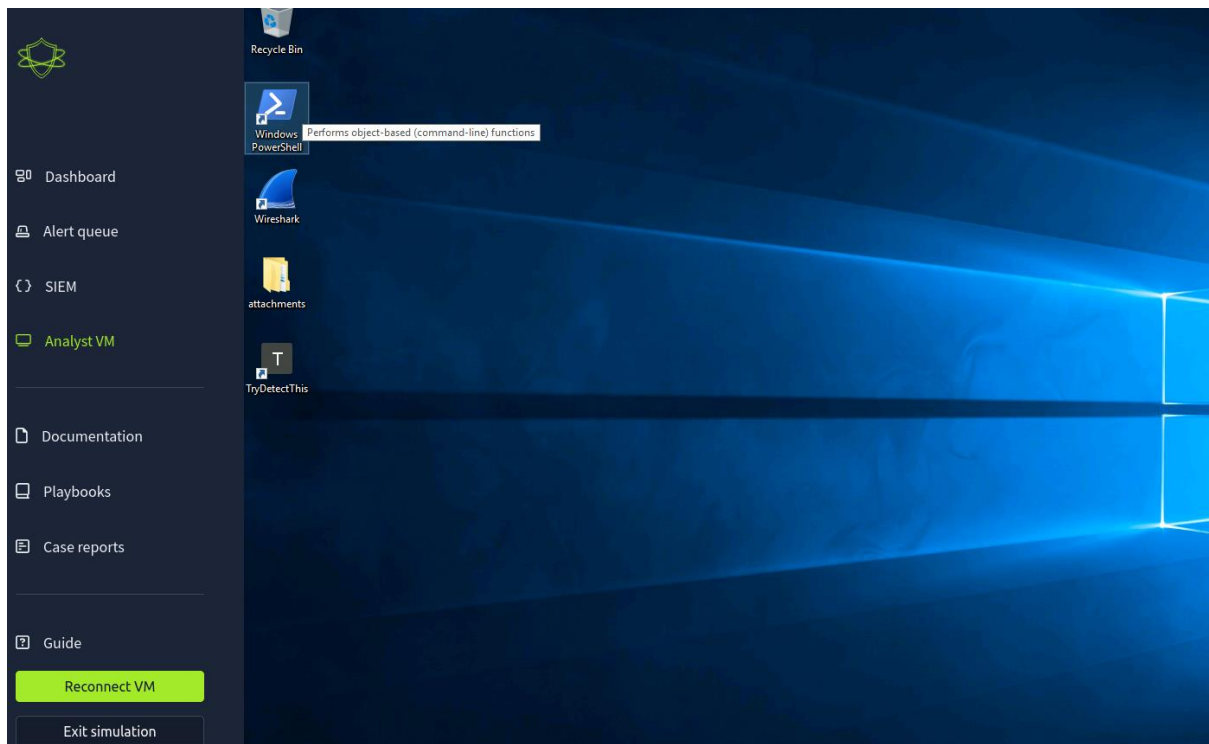
subject: Request for Product Demo: Exploring Partnership Potential

timestamp: 05/17/2025 16:48:50.540

Show as raw text

host = 10.10.161.255:8989 | source = eventcollector | sourcetype = _json


At last, there is a Analyst VM workstation for the simulated analyst to do threat intelligence research. On the workstation are 3 apps, Powershell, WireShark and “TryDetectThis”. The TryDetectThis application is a URL/IP and File threat intelligence tool to lookup reputation and function.



The first email alert came in, the mail triggered a built-in rule for emails containing external links.

SOC Simulator protect (TryHackMe)

By Thomas Lium



Dashboard
Alert queue
SIEM
Analyst VM
Documentation

Alert queue

4 alerts incoming

Assigned alert

You haven't picked up any alert! Assign yourself to an alert to start investigating and find all the true positives. [Learn more](#)

Reset filters

Severity

Status

ID	Alert rule	Severity	Type	Date
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:48

Showing 1 to 1 of 1 entries

8814
Inbound Email Containing Suspicious External Link
Medium
Phishing
May 17th 2025 at 16:48
Awaiting Action

Description:

This alert was triggered by an inbound email contains one or more external links due to potentially suspicious activity. Please investigate, check firewall or proxy logs to determine whether any endpoints have attempted to access those connections were allowed or blocked.

datasource:

email

timestamp:

05/17/2025 16:46:53.540

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 access.\n\nKindly click the link below:\n\n<https://hrconnex.thm/onboarding/15400654060/j.garcia>\n\nIf you have questions, please reach out to the HR Onboarding Team.

direction:

inbound

To analyze the suspicious email, the alert contained the following information:

- **Title:** Inbound Email Containing Suspicious External Link
- **Category:** Phishing
- **Date and Time:** May 17th 2025 at 16:48
- **Description:** This alert was triggered by an inbound email containing one or more external links due to potential investigation, check firewall or proxy logs to determine whether any endpoints have attempted to those connections were allowed or blocked.
- **Datasource:** email
- **Timestamp:** 05/17/2025 16:46:53.540
- **Subject:** Action Required: Finalize Your Onboarding Profile
- **Sender:** onboarding@hrconnex.thm
- **Recipient:** j.garcia@thetrylythm
- **Attachment:** None
- **Content:** Hi Ms. Garcia,[...]Welcome to TheTrulyDaily![...]As part of your onboarding, please complete your final access[...]click the link below[...][https://hrconnex.thm/onboarding/154006540069\[...\]The](https://hrconnex.thm/onboarding/154006540069[...]The) HR Onboarding Team
- **Direction:** inbound

SOC Simulator protect (TryHackMe)

By Thomas Lium

The email, sent to j.garcia@thetrydaily.thm on May 17, 2025, at 16:48 CEST, is an onboarding notification titled "Action Required: Finalize Your Onboarding Profile." The title uses urgency in the title by stating "Action Required", encouraging the user to engage now. It comes from onboarding@hrconnex.thm, seemingly the HR Onboarding Team, and asks Ms. Garcia to complete her profile via a link (<https://hrconnex.thm/onboarding/15400654060/j.garcia>) for TheTryDaily. It offers support via the same email. The sender domain and destination domain aligns up with each other by both domains using the ".thm" extension. The alert flags it as potential phishing despite matching domains because it contains URL to an external source.

Alert queue

0 alerts incoming

Assigned alert(s)

Write case report

8814

Inbound Email Containing Suspicious External Link

^

Medium

Phishing

May 17th 2025 at 16:48

⋮

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:

05/17/2025 16:46:53.540

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\nSet Up My Profile\n\nIf you have questions, please reach out to the HR Onboarding Team.

direction:

inbound

Q Search for an alert

Reset filters

Severity

Status

Alert type

Show 15

ale

ID	Alert rule		Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	▼	Medium	Phishing	May 17th 2025 at 16:52	● Awaiting action	⋮
8817	Inbound Email Containing Suspicious External Link	▼	Medium	Phishing	May 17th 2025 at 16:52	● Awaiting action	⋮

Take ownership of the alert by selecting "Action" and set alert to "Assigned alerts" for the analyst to work on. Assigned alerts can contain multiple alerts.

Assigned alert(s)					
8814	Inbound Email Containing Suspicious External Link	^	Medium	Phishing	May 17th 2025 at 16:48
Description:		This alert was triggered by an inbound email contains one or more external links due to investigation, check firewall or proxy logs to determine whether any endpoints have att those connections were allowed or blocked.			
datasource:		email			
timestamp:		05/17/2025 16:46:53.540			
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 comp access.\n\nKindly click the link below:\n\n<a href="https://hrconnex.thm/onboarding/ you have questions, please reach out to the HR Onboarding Team.			
direction:		inbound			

From the information in the assigned alert, copy the senders email domain and search in Splunk SIEM to look for the specific event. Open the SIEM section and move to Splunk. The result for the search of the email address domain, brings up 3 recorded events.

splunk>enterprise

Apps

Search

Analytics

Datasets

Reports

Alerts

Dashboards

New Search

1

hrconnex.thm

Server error

3 events

(5/17/21 3:04:57.000 PM to 5/17/25 4:04:57.000 PM)

No Event Sampling

Events (3)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

List

Format

50 Per Page

Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a attachment 1

a content 2

a datasource 1

a direction 2

a index 1

linecount 1

a punct 2

a recipient 2

a sender 2

a splunk_server 1

a subject 2

a timestamp 3

Time

Event

5/17/25

3:50:48.540 PM

attachment: None

content: Hi Ms. Garcia,\n\nWelcome to TheTryDaily!\n\nAs part of your onboarding, please complete your final profile setu href="https://hrconnex.thm/onboarding/15400654060/j.garcia">Set Up My Profile.\n\nIf you have questions, please reach ou

datasource: email

direction: inbound

recipient: j.garcia@thetrydaily.thm

sender: onboarding@hrconnex.thm

subject: Action Required: Finalize Your Onboarding Profile

timestamp: 05/17/2025 16:50:48.540

Show as raw text

host = 10.10.161.255:8989 | source = eventcollector | sourcetype = _json

5/17/25

3:46:53.540 PM

attachment: None

content: Hi Ms. Garcia,\n\nWelcome to TheTryDaily!\n\nAs part of your onboarding, please complete your final profile setu href="https://hrconnex.thm/onboarding/15400654060/j.garcia">Set Up My Profile.\n\nIf you have questions, please reach ou

datasource: email

To narrow down the search to find the specific event we are looking for, add in unique information to the search query related to the specific email we are looking for. I noted down the timestamp earlier, include the timestamp in the query with the following search:

hrconnex.thm timestamp="05/17/2025 16:46:53.540"

New Search

1 hrconnex.thm timestamp="05/17/2025 16:46:53.540"

Server error

1 event (5/17/21 3:04:57.000 PM to 5/17/25 4:04:57.000 PM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 50 Per Page

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a attachment 1

a content 1

a datasource 1

a direction 1

a index 1

linecount 1

a punct 1

a recipient 1

a sender 1

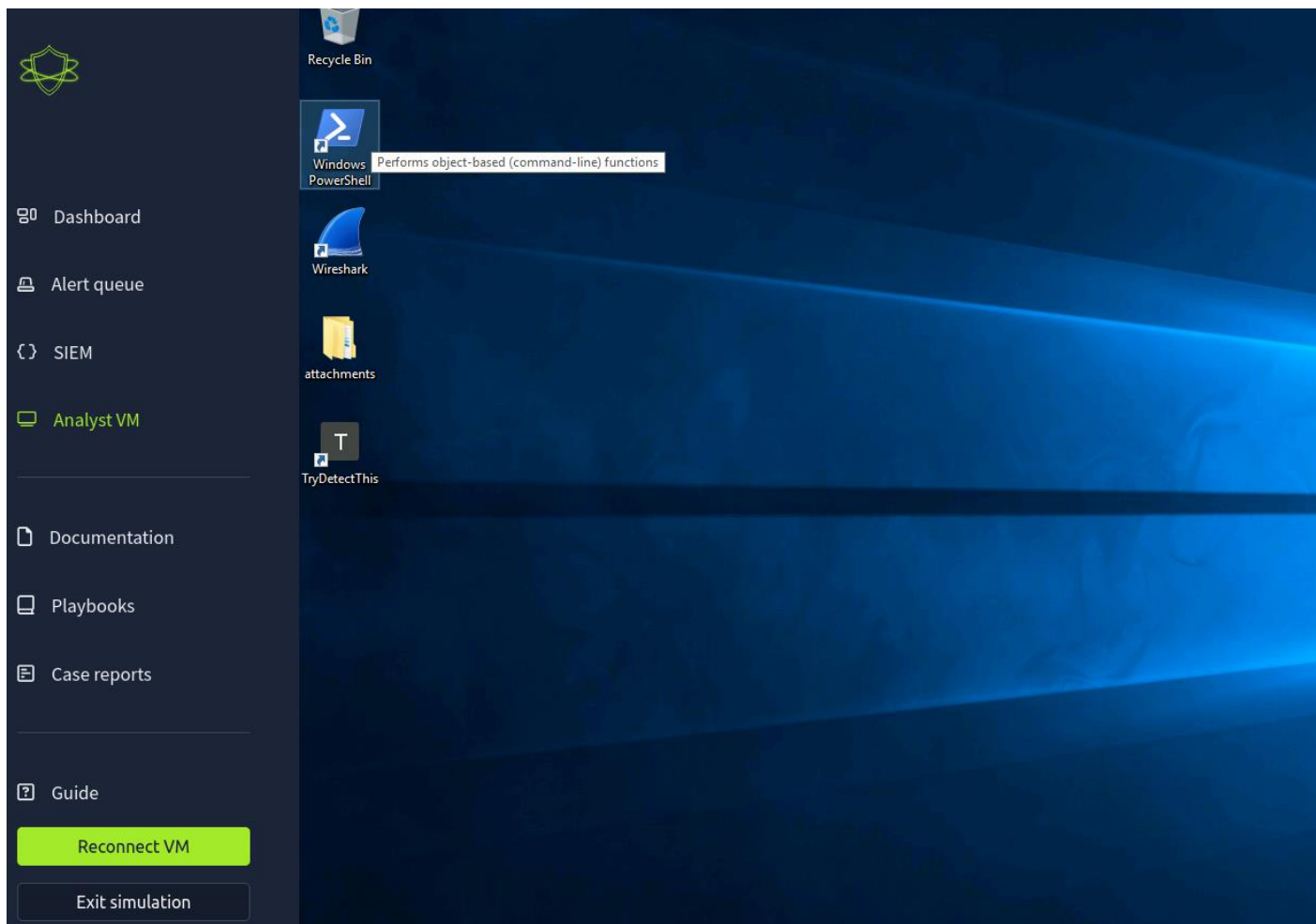
a splunk_server 1

a subject 1

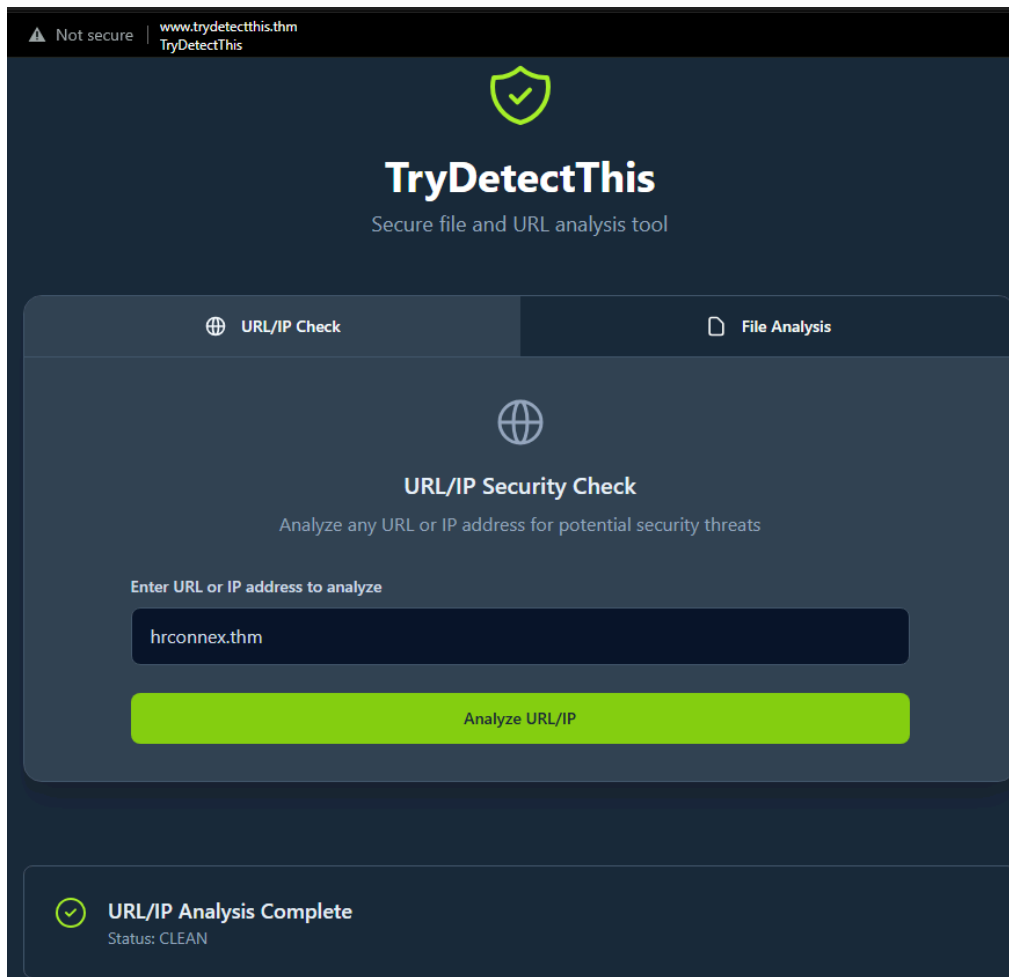
a timestamp 1

i	Time	Event
>	5/17/25 3:46:53.540 PM	<pre>{ [-] attachment: None content: Hi Ms. Garcia,\n\nWelcome to TheTryDaily!\n\nAs part of your onboarding, please complete your final profile setup so we c href="https://hrconnex.thm/onboarding/15400654060/j.garcia">Set Up My Profile.\n\nIf you have questions, please reach out to the datasource: email direction: inbound recipient: j.garcia@thetrydaily.thm sender: onboarding@hrconnex.thm subject: Action Required: Finalize Your Onboarding Profile timestamp: 05/17/2025 16:46:53.540 }</pre> <div>Show as raw text</div> <div>host = 10.10.161.255:8989 source = eventcollector sourcetype = _json</div>

1 event found, this is the one specific to the alert we are looking at. The log contains the sender's domain and the external URL listed in the main content that triggered the alert.





Inside the Analyst VM workstation, open the "TryDetectThis" application to look up the listed domain reputation and external URL function. TryDetectThis tool is for threat intel research.




TryDetectThis

Secure file and URL analysis tool

 URL/IP Check

 File Analysis



URL/IP Security Check


Analyze any URL or IP address for potential security threats

Enter URL or IP address to analyze

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

Analyze URL/IP

Paste



URL/IP Analysis Complete

Status: CLEAN

The domain of the sender and external URL came up CLEAN Analysis, meaning the domain and URL is seemingly safe. This points to the possibility that this might be a false positive.

Q Search for an alert

Reset filters

Severity

Status

Alert type

ID	Alert rule	Severity	Type	Date	Status
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:52	Awaiting action
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:52	Awaiting action
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	May 17th 2025 at 16:51	Awaiting action
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:50	Awaiting action

Description:

This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. Investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email. Those connections were allowed or blocked.

datasource:

email

timestamp:

05/17/2025 16:48:02.540

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 address 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 the sender.\n\nThank you,\n\nAmazon Delivery

direction:

inbound

By now, 4 additional alerts have come in. 3 new email alerts and 1 high risk alert from the firewall.

The next email alert coming in was triggered when another email contained an external URL within the email.

8815	Inbound Email Containing Suspicious External Link	^	Medium	Phishing	May 17th 2025 at 16:50
Description:			This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. Investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email. Those connections were allowed or blocked.		
datasource:			email		
timestamp:			05/17/2025 16:48:02.540		
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 address 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 the sender.\n\nThank you,\n\nAmazon Delivery		
direction:			inbound		

Lookup the specific alert on Splunk using unique information within the email such as domain and timestamp for the alert. Search up in Splunk:

amazon biz datasource=rcemail timestamp="05/17/2025 16:48:02.540"

SOC Simulator protect (TryHackMe)

By Thomas Lium

New Search

1 amazon.biz datasource=email timestamp="05/17/2025 16:48:02.540"

Server error

✓ 1 event (5/17/21 3:04:57.000 PM to 5/17/25 4:04:57.000 PM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

Format Timeline ▼ – Zoom Out + Zoom to Selection × Deselect

		List ▼	Format	50 Per Page ▼
< Hide Fields				
All Fields				
		i	Time	Event
SELECTED FIELDS		>	5/17/25 3:48:02.540 PM	{ [-] 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 datasource: email direction: inbound recipient: h.harris@thetrydaily.thm sender: urgents@amazon.biz subject: Your Amazon Package Couldn't Be Delivered - Action Required timestamp: 05/17/2025 16:48:02.540 } Show as raw text
INTERESTING FIELDS				host = 10.10.161.255:8989 source = eventcollector sourcetype = _json
a host 1				
a source 1				
a sourcetype 1				
a attachment 1				
a content 1				
a datasource 1				
a direction 1				
a index 1				
# linecount 1				
a punct 1				

Found the specific event on Splunk.

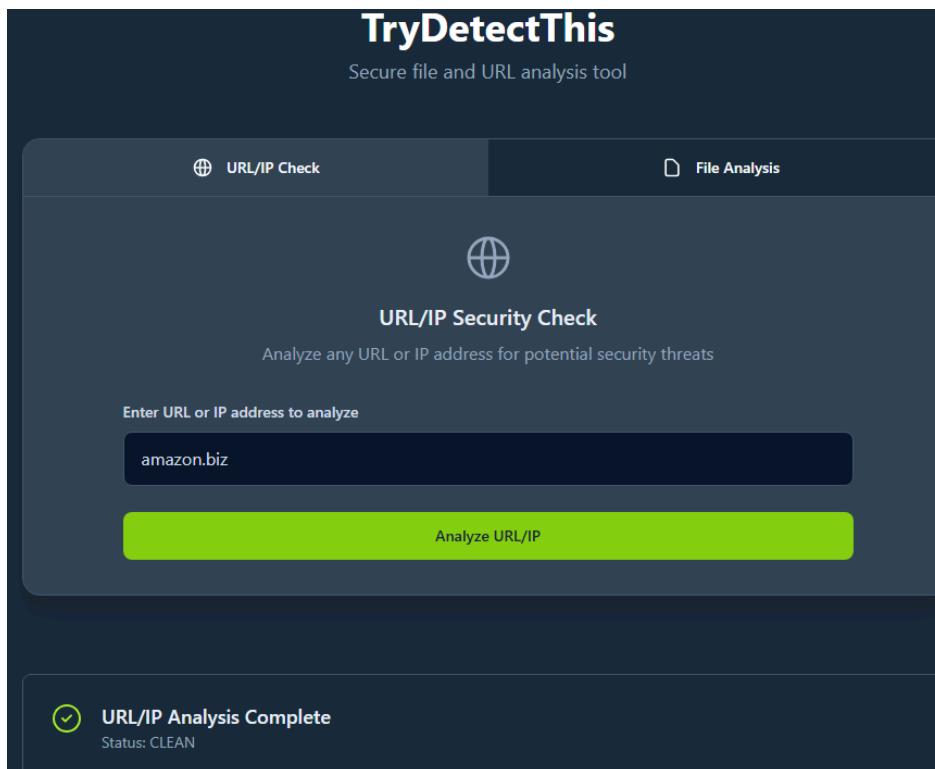
- **Description:** This alert was triggered by an inbound email containing one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.
- **Timestamp:** 05/17/2025 16:48:02.540
- **Subject:** Your Amazon Package Couldn't Be Delivered – Action Required
- **Sender:** urgents@amazon.biz
- **Recipient:** h.harris@thetrydaily.thm
- **Attachment:** None (No attachment)
- **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

This email seems to be coming from Amazon at domain “amazon.biz” sent to the user h.harris at our organisation “TheTryDaily”. The .biz extension seems a little suspicious. Subject says package could not be delivered and uses urgency to request action. The main content asks the viewer to clicking the link below listed as a bit.ly URL. Bitly is a common URL shortener, used by many phishers to mask or hide a potential malicious link. The URL is highly suspicious, as Amazon most likely wouldn't use Bitly instead of a trusted amazon domain. The email also uses urgency by stating action is required within 48 hours, a common tactic for phishing campaigns to encourage engagement.

SOC Simulator protect (TryHackMe)

By Thomas Lium

Use the TryDetectThis application to lookup the sender domain and listed external URL.



The screenshot displays the TryDetectThis application interface, which is a secure file and URL analysis tool. The interface is dark-themed with a blue header. The main content area is divided into two tabs: "URL/IP Check" (selected) and "File Analysis". The "URL/IP Check" tab shows a globe icon and the title "URL/IP Security Check" with the subtitle "Analyze any URL or IP address for potential security threats". Below this, there is a text input field labeled "Enter URL or IP address to analyze" containing the text "amazon.biz". A large green button labeled "Analyze URL/IP" is positioned below the input field. At the bottom of the interface, a status bar indicates "URL/IP Analysis Complete" with a green checkmark icon and the text "Status: CLEAN".

SOC Simulator protect (TryHackMe)

By Thomas Lium

TryDetectThis

Secure file and URL analysis tool

🌐 URL/IP Check

📄 File Analysis

🌐

URL/IP Security Check

Analyze any URL or IP address for potential security threats

Enter URL or IP address to analyze

http://bit.ly/3sHkX3da12340

Analyze URL/IP

Paste

⚠️

URL/IP Analysis Complete

Status: MALICIOUS

The domain “amazon.biz” came up clean, but the external URL came up as malicious function. This points to the possibility of being a phishing email with a malicious link.

This email alert “8815” is a **True Positive**

SOC Simulator protect (TryHackMe)

By Thomas Lium

ID	Alert rule	Severity	Type	Date	Status
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:52	Awaiting action
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:52	Awaiting action
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	May 17th 2025 at 16:51	Awaiting action
<div> <div>Description:</div> <div>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.</div> </div> <div> <div>datasource:</div> <div>firewall</div> </div> <div> <div>timestamp:</div> <div>05/17/2025 16:49:16.540</div> </div> <div> <div>Action:</div> <div>blocked</div> </div> <div> <div>SourceIP:</div> <div>10.20.2.17</div> </div> <div> <div>SourcePort:</div> <div>34257</div> </div> <div> <div>DestinationIP:</div> <div>67.199.248.11</div> </div> <div> <div>DestinationPort:</div> <div>80</div> </div> <div> <div>URL:</div> <div>http://bit.ly/3sHkX3da12340</div> </div> <div> <div>Application:</div> <div>web-browsing</div> </div> <div> <div>Protocol:</div> <div>TCP</div> </div> <div> <div>Rule:</div> <div>Blocked Websites</div> </div>					

The next alert triggered is for "Access to Blacklisted external URL blocked by firewall". The alert is from the network firewall, the alert contains the following information:

- Title: Access to Blacklisted External URL Blocked by Firewall
- 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 successfully blocked the outbound request, preventing the connection. Note: The blacklist only covers known or known malicious domains; it does not provide protection against new or unknown malicious domains.
- Timestamp: 05/17/2025 16:49:50
- Action: Blocked
- Source IP: 10.20.2.17
- Source Port: 54217
- Destination IP: 67.199.248.11
- Destination Port: 80
- URL: <http://bit.ly/3HxkdA2340>
- Application: web browsing
- Rule: Blocked Websites

This alert tells us that a user within our network has attempted to visit an external URL that was listed in our organizations blacklist of domains. These domains will be automatically blocked if visited by our users. The firewall successfully blocked the outbound request. It states that the IP 10.20.2.17 using port 54217 had tried to visit IP 67.199.248.11 at port 80 at URL <http://bit.ly/3HxkdA2340>. The domain "bit.ly" was apart of our organization's blacklist of domains, likely because it is a URL shortener often used to hide actual malicious domains.

Add the alert to assigned alerts with the 2 other emails we previously covered.

Alert queue

0 alerts incoming

Assigned alert(s)

Write case report

8816	Access to Blacklisted External URL Blocked by Firewall	^	High	Firewall	May 17th 2025 at 16:51	
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:		05/17/2025 16:49:16.540				
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				
8815	Inbound Email Containing Suspicious External Link	▼	Medium	Phishing	May 17th 2025 at 16:50	
8814	Inbound Email Containing Suspicious External Link	▼	Medium	Phishing	May 17th 2025 at 16:48	

Search up the log to the firewall alert in Splunk using the information given in the alert queue. The search query “datasource=firewall SourceIP="10.20.2.17" SourcePort=34257” narrowed it down.

New Search

1 datasource=firewall SourceIP="10.20.2.17" SourcePort=34257

Server error

1 event (5/17/21 3:04:57.000 PM to 5/17/25 4:04:57.000 PM) No Event Sampling

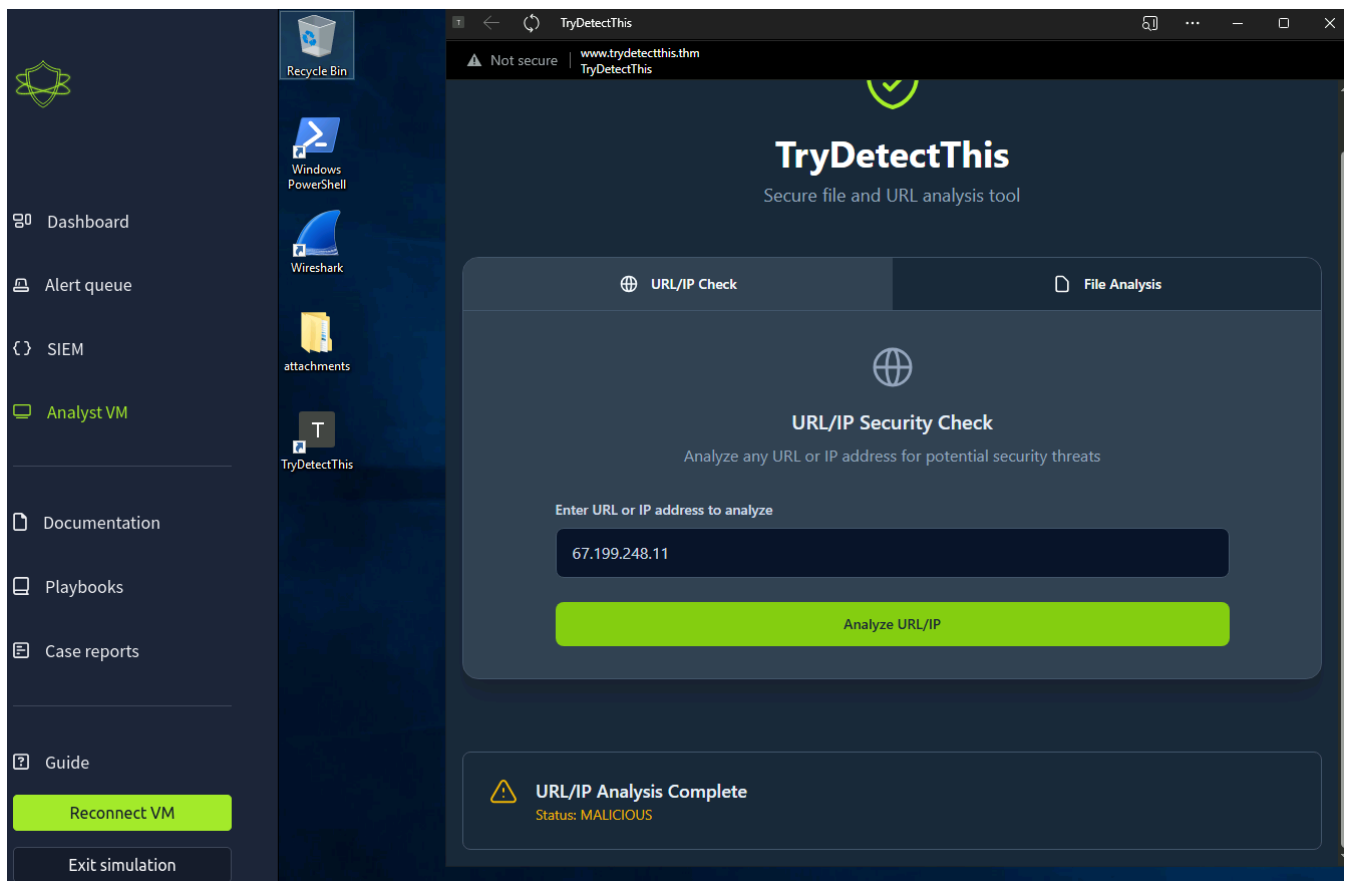
Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

		List	Format	50 Per Page
<div><div>< Hide Fields</div><div>All Fields</div></div> <div><div>SELECTED FIELDS</div><div>a host 1</div><div>a source 1</div><div>a sourcetype 1</div><div>INTERESTING FIELDS</div><div>a Action 1</div><div>a Application 1</div><div>a datasource 1</div><div>a DestinationIP 1</div><div># DestinationPort 1</div><div>a index 1</div><div># linecount 1</div><div>a Protocol 1</div><div>a punct 1</div><div>a Rule 1</div></div>		i	Time	Event
		>	5/17/25 3:49:16.540 PM	<div>{ [-]</div> <div>Action: blocked</div> <div>Application: web-browsing</div> <div>DestinationIP: 67.199.248.11</div> <div>DestinationPort: 80</div> <div>Protocol: TCP</div> <div>Rule: Blocked Websites</div> <div>SourceIP: 10.20.2.17</div> <div>SourcePort: 34257</div> <div>URL: http://bit.ly/3sHkX3da12340</div> <div>datasource: firewall</div> <div>timestamp: 05/17/2025 16:49:16.540</div> <div>}</div> <div>Show as raw text</div> <div>host = 10.10.161.255:8989 source = eventcollector sourcetype = _json</div>

<

In the Splunk log for the specific firewall alert, we see the matching information in the log. The URL contains a blacklisted domain, was blocked for that reason. The Destination IP hosting the web service on port 80 should be further investigated through threat intel.



The destination IP was flagged as Malicious.

We know the email alert 8815 coming from urgents@amazon.biz requested the user “h.harris” to visit an external bit.ly URL to complete address information to amazon. This bit.ly link is the exact same URL as the one blocked by the firewall. Note the email from amazon.biz below:

8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:50
Description:		This alert was triggered by an inbound email contains one or more external links d investigation, check firewall or proxy logs to determine whether any endpoints ha those connections were allowed or blocked.		
datasource:		email		
timestamp:		05/17/2025 16:48:02.540		
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 clicking the link below:\n\nhttp://bit.ly/3sHkX3da12340\n\nIf we don't hear from y sender.\n\nThank you,\n\nAmazon Delivery		
direction:		inbound		

SOC Simulator protect (TryHackMe)

By Thomas Lium

This points to the conclusion that the user “h.harris” at TheTryDaily has engaged in a phishing email from “amazon.biz” and clicked on the external URL listed in the mail leading to a bit.ly URL. The connection was blocked by the firewall as bit.ly is a blacklisted domain for automatic block.

This firewall alert “8816” is a **True Positive**

Moving on, there are 2 email alerts left.

Alert queue

0 alerts incoming

Assigned alert(s)

8817	Inbound Email Containing Suspicious External Link	^	Medium	Phishing	May 17th 2025 at 16:52
Description:		This alert was triggered by an inbound email contains one or more external link. For further investigation, check firewall or proxy logs to determine whether any endpoints have attempted to those connections were allowed or blocked.			
datasource:		email			
timestamp:		05/17/2025 16:50:20.540			
subject:		Unusual Sign-In Activity on Your Microsoft Account			
sender:		no-reply@microsoftsupport.co			
recipient:		c.allen@thetrydaily.thm			
attachment:		None			
content:		Hi C.Allen,\n\nWe detected an unusual sign-in attempt on your Microsoft account from 102.89.222.143\n\nDate: 2025-01-24 06:42\n\nIf this was not you, please secure your account by reviewing your recent sign-in activity.\n\n https://microsoftsupport.co/login >Review Activity\n\nThank you for your attention.			
direction:		inbound			

The next email alert contains the following information:

- **Alert ID:** 8817
- **Title:** Inbound Email Containing Suspicious External Link
- **Category:** Phishing
- **Date and Time:** May 17th 2025 at 16:52
- **Description:** This alert was triggered by an inbound email containing one or more external links due to potential investigation, check firewall or proxy logs to determine whether any endpoints have attempted to those connections were allowed or blocked.
- **Datasource:** email
- **Timestamp:** 05/17/2025 16:50:20.540
- **Subject:** Unusual Sign-In Activity on Your Microsoft Account

- **Sender:** no-reply@m1crosoftsupport.co
- **Recipient:** c.allen@thetrulythm
- **Attachment:** None
- **Content:** Hi C.Allen,[...]We detected an unusual sign-in attempt on your Microsoft account.[...]Location: Lagos 10.0.89.222.143[...]InDate: 2025-01-24 06:42[...]If this was not you, please secure your account immediately[...][https://m1crosoftsupport.co/login*-Review-Activity-\[...\]Thank](https://m1crosoftsupport.co/login*-Review-Activity-[...]Thank) you,[...]microsoft
- **Direction:** inbound

This email claims to be from Microsoft (no-reply@m1crosoftsupport.co) about an unusual sign-in from Lagos (IP: 10.0.89.222.143) on January 24, 2025, at 06:42. The senders domain contains a “1” number in the domain as in “m1crosoftsupport.co”, highly suspicious. The link (<https://microsoftsupport.co/login>) is also suspicious, likely leading to a malicious site. Sent to c.allen@thetruly.thm with no attachments.

First impressions, this looks like a phishing email. Let's investigate further through Splunk log and threat intelligence.

New Search

1 m1crosoftsupport.co datasource=email timestamp="05/17/2025 16:50:20.540"

Server error

✓ 1 event (5/17/21 3:04:57.000 PM to 5/17/25 4:04:57.000 PM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ Format 50 Per Page ▼

< Hide Fields		≡ All Fields	i	Time	Event
SELECTED FIELDS			>	5/17/25 3:50:20.540 PM	{ [-] attachment: None content: Hi C.Allen,\n\nWe detected an unusual sign-in attempt on your Micro secure your account immediately to avoid unauthorized access.\n\n<a href="https datasource: email direction: inbound recipient: c.allen@thetrydaily.thm sender: no-reply@microsoftsupport.co subject: Unusual Sign-In Activity on Your Microsoft Account timestamp: 05/17/2025 16:50:20.540 } Show as raw text host = 10.10.161.255:8989 source = eventcollector sourcetype = _json
INTERESTING FIELDS					
a attachment 1					
a content 1					
a datasource 1					
a direction 1					
a index 1					
# linecount 1					
a punct 1					
a recipient 1					

SOC Simulator protect (TryHackMe)

By Thomas Lium

Search: m1crosoftsupport.co datasource=email timestamp="05/17/2025 16:50:20.540"

This splunk search narrowed it down to the specific event.

i

Time

Event

5/17/25
3:50:20.540 PM

{ [-]

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: 05/17/2025 16:50:20.540\n\nPlease secure your account immediately to avoid unauthorized access.\n\n<https://m1crosoftsupport.co/login>>Review Activity\n\nThank you,\n\nMicrosoft Account Support

datasource: email

direction: inbound

recipient: c.allen@thetrydaily.thm

sender: no-reply@m1crosoftsupport.co

subject: Unusual Sign-In Activity on Your Microsoft Account

timestamp: 05/17/2025 16:50:20.540

Show as raw text

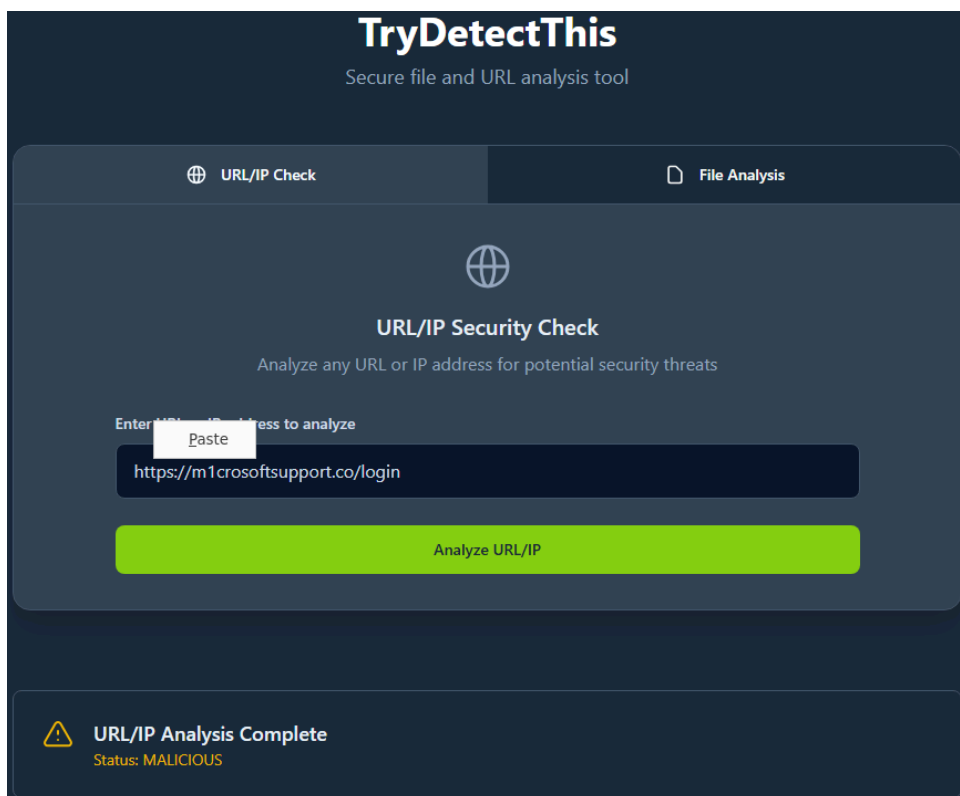
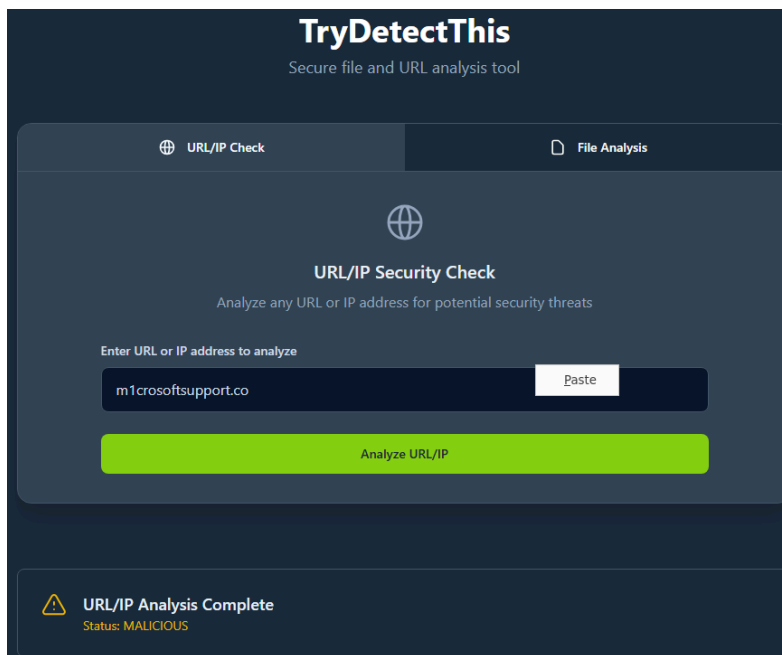
Event Actions

Type	Field	Value
Selected	host	10.10.161.255:8989
	source	eventcollector
	sourcetype	_json
Event	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: 05/17/2025 16:50:20.540\n\nPlease secure your account immediately to avoid unauthorized access.\n\n https://m1crosoftsupport.co/login >Review Activity\n\nThank you,\n\nMicrosoft Account Support
	datasource	email
	direction	Inbound
	recipient	c.allen@thetrydaily.thm
	sender	no-reply@m1crosoftsupport.co
	subject	Unusual Sign-In Activity on Your Microsoft Account
	timestamp	05/17/2025 16:50:20.540
Time	_time	2025-05-17T15:50:20.540+00:00
Default	index	main
	linecount	1
	punct	{ "type": "email", "subject": "Unusual Sign-In Activity on Your Microsoft Account", "sender": "no-reply@m1crosoftsupport.co", "recipient": "c.allen@thetrydaily.thm", "location": "Lagos, Nigeria", "ip_address": "102.89.222.143", "timestamp": "05/17/2025 16:50:20.540", "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: 05/17/2025 16:50:20.540\n\nPlease secure your account immediately to avoid unauthorized access.\n\n https://m1crosoftsupport.co/login >Review Activity\n\nThank you,\n\nMicrosoft Account Support"
	splunk_server	ip-10-10-40-195

The log contains the email information provided. Using the stated information, do threat intelligence research on the senders domain "m1crosoftsupport.co" and listed URL in the main content.

SOC Simulator protect (TryHackMe)

By Thomas Lium



Both the senders domain at “m1crosoftsupport.co” and the listed URL under the same domain were flagged as malicious. We can determine that this email alert is a malicious phishing email and is therefore a true positive alert.

The email alert “8817” is a **True Positive**

SOC Simulator protect (TryHackMe)

By Thomas Lium

Alert queue

0 alerts incoming

Assigned alert(s)

8818	Inbound Email Containing Suspicious External Link	^	Medium	Phishing	May 17th 2025 at 16:52
------	---	---	--------	----------	------------------------

Description:

datasource:

timestamp:

subject:

sender:

recipient:

attachment:

content:

direction:

This alert was triggered by an inbound email contains one or more external links due to potentially suspicious investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access those connections were allowed or blocked.

email

05/17/2025 16:50:48.540

Action Required: Finalize Your Onboarding Profile

onboarding@hrconnex.thm

j.garcia@thetrydaily.thm

None

Hi Ms. Garcia,\n\nWelcome to TheTryDaily!\n\nAs part of your onboarding, please complete your final access.\n\nKindly click the link below:\n\nhttps://hrconnex.thm/onboarding/15400654060/j\n\nIf you have questions, please reach out to the HR Onboarding Team.

inbound

The last email alert our SOC simulator receives is another email from “hrconnex.thm”.

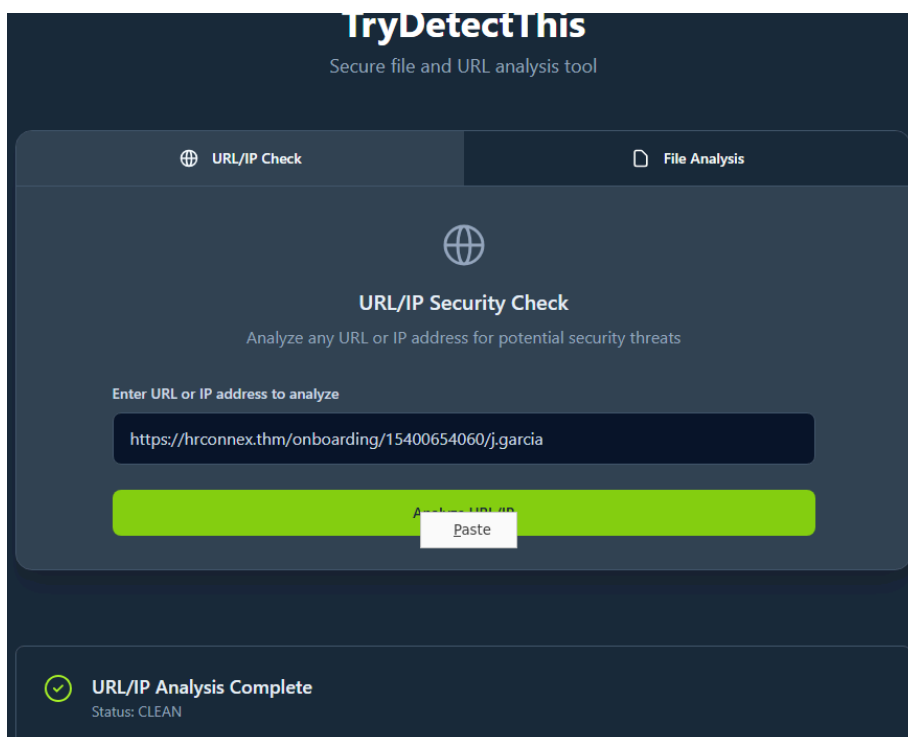
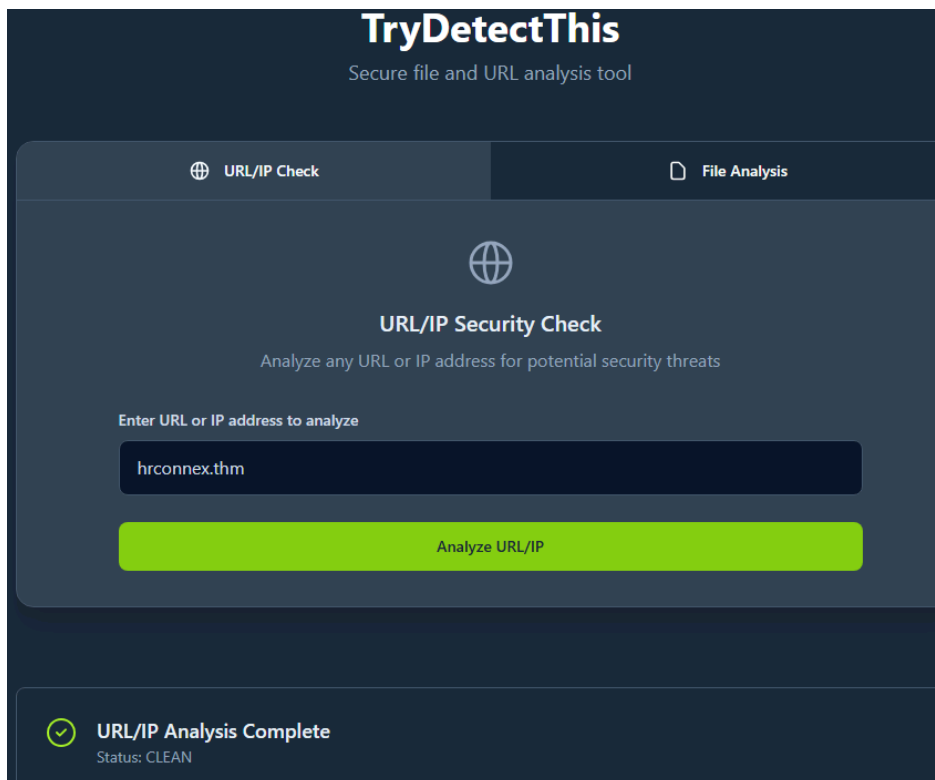
- **Alert ID:** 8818
- **Title:** Inbound Email Containing Suspicious External Link
- **Date and Time:** May 17th 2025 at 16:52
- **Type:** Phishing
- **Description:** This alert was triggered by an inbound email containing one or more external links due to potential investigation, check firewall or proxy logs to determine whether any endpoints have attempted to those connections were allowed or blocked.
- **Datasource:** email
- **Timestamp:** 05/17/2025 16:50:48.540
- **Subject:** Action Required: Finalize Your Onboarding Profile
- **Sender:** onboarding@hrconnex.thm
- **Recipient:** j.garcia@thetrulythm
- **Attachment:** None
- **Content:** Hi Ms. Garcia,[...]Welcome to TheTrulyDaily![...]As part of your onboarding, please complete your final access[...]click the link below[...][https://hrconnex.thm/onboarding/154006540069\[...\]](https://hrconnex.thm/onboarding/154006540069[...])The HR Onboarding Team
- **Direction:** inbound

This email has already been received before. It is in fact the exact same email as the first email that came into the SOC simulator.

The email appears to be a legitimate onboarding request from an HR team ("The HR Onboarding Team") for a new employee, Ms. Garcia, at TheTrulyDaily. This email seems to have been sent twice.

SOC Simulator protect (TryHackMe)

By Thomas Lium



The domain and listed URL came up as clean. The same result as the first version of this same email from hrconnex.thm. It seems that the same email was sent twice and is a false positive again.

Alert queue

0 alerts incoming

Assigned alert(s)

Write case report

8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:52	
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:52	
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	May 17th 2025 at 16:51	
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:50	
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:48	

Q Search for an alert

Reset filters

Severity

Status

Alert type

Show

15

ID	Alert rule	Severity	Type	Date	Status	Acti
----	------------	----------	------	------	--------	------

Showing 1 to 0 of 0 entries

Previous

1

N

That was all the alerts for this scenario, lets write a quick case report for these alerts.

We have determined throughout this scenario that there were 2 false positives and 3 true positives.

First, organize the 2 false positives alerts into the assigned alerts section. These 2 alerts will be reported together as they are related to eachother.

After writing the first report, organize the 3 true positives alerts into the assigned alerts section and provide a case report for the positives as well.

Alert queue

0 alerts incoming

Assigned alert(s)

8818

Inbound Email Containing Suspicious External Link

^

Medium

Phishing

May 17th 2025 at 16:52

Description:

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

datasource:

email

timestamp:

05/17/2025 16:50:48.540

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 access.\n\nKindly click the link below:\n\n<https://hrconnex.thm/onboarding/15400654060/j.garcia>>Set Up My Profile\n\nIf you have questions, please reach out to the HR Onboarding Team.

direction:

inbound

8814

Inbound Email Containing Suspicious External Link

v

Medium

Phishing

May 17th 2025 at 16:48

Search for an alert

Reset filters

Severity

Status

Alert type

Show

The 2 false postives alerts in assigned alerts and click the top right "Write case report".

Alert queue

0 alerts incoming

Assigned alert(s)

8818

Inbound Email Containing Suspicious External Link

^

Medium

Phishing

May 17th 2025 at 16:52

Description:

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

datasource:

email

timestamp:

05/17/2025 16:50:48.540

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 access.\n\nKindly click the link below:\n\n<https://hrconnex.thm/onboarding/15400654060/j.garcia>>Set Up My Profile\n\nIf you have questions, please reach out to the HR Onboarding Team.

direction:

inbound

8814

Inbound Email Containing Suspicious External Link

v

Medium

Phishing

May 17th 2025 at 16:48

Search for an alert

Reset filters

Severity

Status

Alert type

Show

Close assigned alerts

Were these alerts true positives or false positives?

☐ True positives

☒ False positives

Close

Write case report

Classify the assigned alerts by false positives and click write case report.

← Case report for multiple alerts

ID 8818

ID 8814

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
8818	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	May 17th 2025 at 17:53

Alert details ▾

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:

List of Related Entities:

Reason for Classifying as False Positive:

Review the alerts and write incident report regarding assigned alerts.

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 ▾ ☰ ☲ ☳ ▾

On 05/17/2025 at 16:46:53.540, an inbound email with the subject "Action Required: Finalize Your Onboarding Profile" triggered Alert ID 8814 due to a suspicious external link (<https://hrconnex.thm/onboarding/15400654060/j.garcia>). The email was sent from onboarding@hrconnex.thm to jgarcia@thetrydaily.thm. The same exact email was sent twice.

Investigation Steps:

1. Analyzed the email in [Splunk SIEM](#), confirming the sender, recipient, and link details (Page 11, 13).

2. Checked the domain [hrconnex.thm](#) using [TryDetectThis](#); result: **CLEAN** (Page 26).

3. Reviewed email content for phishing indicators (e.g., mismatched domains, urgent language); found none beyond the "Action Required" subject.

Findings:

• The domain [hrconnex.thm](#) matches the sender and URL, and is marked as CLEAN.

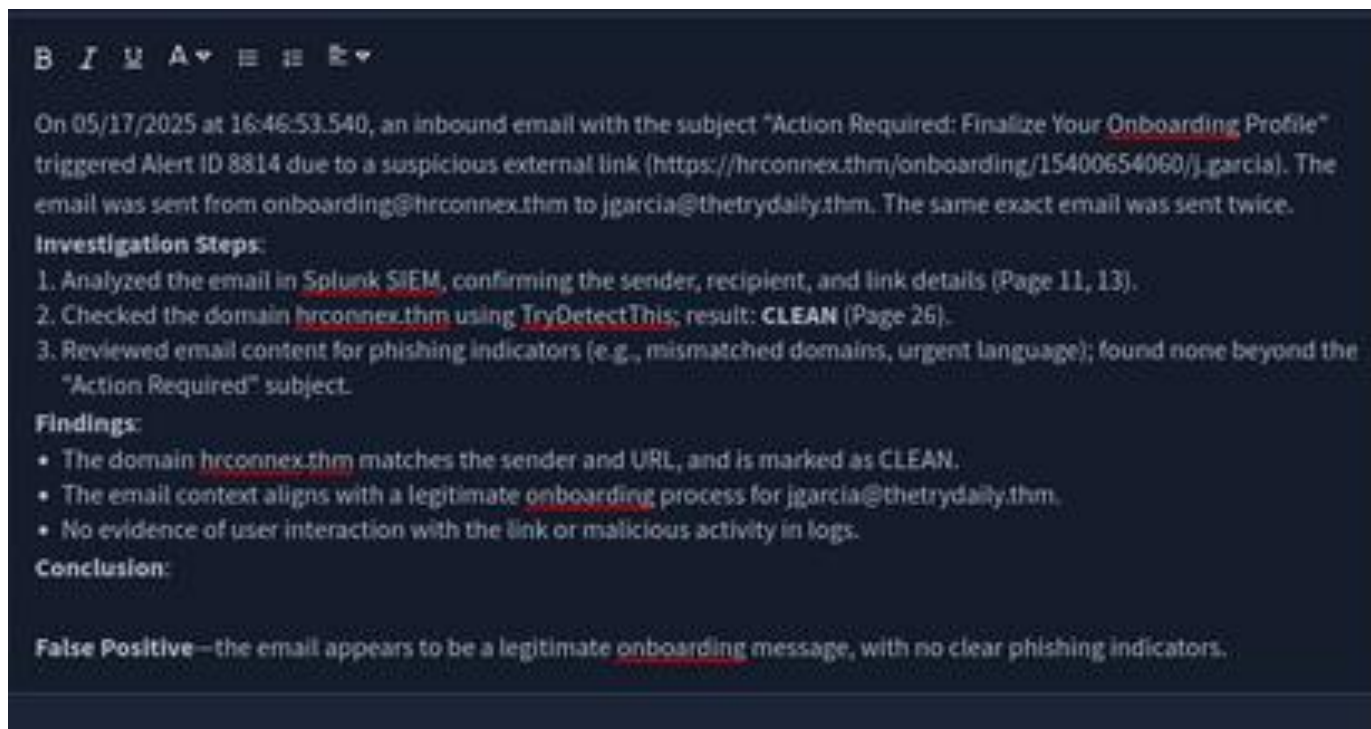
• The email context aligns with a legitimate onboarding process for jgarcia@thetrydaily.thm.

• No evidence of user interaction with the link or malicious activity in logs.

Conclusion:

False Positive—the email appears to be a legitimate onboarding message, with no clear phishing indicators.

Submit and close alert



Case report written and delivered for the 2 false positives alerts. Move on to the remaining 3 alerts.

Alert queue

0 alerts incoming

Assigned alert(s) Write case report

8817	Inbound Email Containing Suspicious External Link	▼	Medium	Phishing	May 17th 2025 at 16:52	⋮
8816	Access to Blacklisted External URL Blocked by Firewall	▼	High	Firewall	May 17th 2025 at 16:51	⋮
8815	Inbound Email Containing Suspicious External Link	▼	Medium	Phishing	May 17th 2025 at 16:50	⋮

Reset filters Severity ▼ Status ▼ Alert type ▼ Show 15 ▼ a

ID	Alert rule	▼	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	▼	Medium	Phishing	May 17th 2025 at 16:52	Closed	
8814	Inbound Email Containing Suspicious External Link	▼	Medium	Phishing	May 17th 2025 at 16:48	Closed	

Showing 1 to 2 of 2 entries Previous 1 Next

Organize the 3 true positive alerts into assigned alerts and click “write case report”. Label the 3 alerts as true positives and write a quick report on them.

Alert queue

0 alerts incoming

Assigned alert(s)

8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:52
------	---	--------	----------	------------------------

Description:

This alert was triggered by an inbound email contains one or more external links due to potential investigation, check firewall or proxy logs to determine whether any endpoints have attempted those connections were allowed or blocked.

datasource:

timestamp:

subject:

sender:

recipient:

attachment:

content:

attempt on your Microsoft account.

If this was not you, please secure your account.

>Review Activity

Thank you,

Microsoft

direction:

Close assigned alerts

Were these alerts true positives or false positives?

True positives

False positives

Close

Write case report

8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	May 17th 2025 at 16:51
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	May 17th 2025 at 16:50

B

I

U

A

▼

≡

≡

≡

≡

≡

The following true positive alerts were identified and investigated based on the "Introduction to Phishing" and "Phishing Unfolded" scenarios:

- Alert ID 8817 (Inbound Email Containing Suspicious External Link)
- Date and Time Detected: May 17, 2025, 17:52
- Severity Level: Medium
- Incident Type: Phishing
- Description: An inbound email triggered an alert due to one or more potentially suspicious external links. Investigation is needed to check firewall or proxy logs to determine if endpoints attempted to access the URLs and whether those connections were allowed or blocked.
- Details:
 - Data Source: Email
 - Timestamp: May 17, 2025, 16:50:20.540
 - Subject: Unusual Sign-In Activity on Your Microsoft Account
 - Sender: no-reply@microsoftsupport.co
 - Recipient: c.allen@thetrydaily.thm
 - Attachment: None
 - Content: Reported an unusual sign-in attempt from Lagos, Nigeria (IP Address: 102.89.222.143) on January 24, 2025, 06:42, with a link (https://microsoftsupport.co/login) to review activity.

The report was contained the related information, phishing email purpose and outcome of the emails. 1 user within our network had clicked a malicious link, but the connection was blocked by the firewall due to the URL containing a blacklisted domain within the link and documented. Another user receives a phishing email, but did not engage in it.



archerlium

Victory! Security breach prevented!

You passed the scenario by identifying all true positives. Your MTTR and dwell time were longer than average, especially for Phishing alerts. Your true positive rate was 60%, which is an improvement over previous runs, but there's still room for further enhancement.

1st 0 85 pts +85 pts



All alerts of this scenario have been delivered and were all correctly identified as true or false positives. Granted with a victory page, security breach to the SOC simulator was prevented.

Phishing Unfolded scenario

Coming soon

References

SOC Simulator, Tryhackme, (2025). "Introduction to Phishing": tryhackme.com

SOC Simulator, Tryhackme, (2025). "Phishing Unfolded": tryhackme.com

Tools

[Splunk \(SIEM\)](#)

[TryDetectThis \(IP/URL reputation scanner\)](#)