

TryHackMe SOC Simulation — Lab Write-up

Author: Brice Dickey

This write-up documents the TryHackMe SOC Simulation lab activities: alert triage, phishing detection, log correlation, IOC extraction, and remediation planning. The Evidence section includes selected screenshots from the lab environment.

Key Findings

- Multiple phishing emails with suspicious URLs were identified.
- Firewall logs showed blocked or attempted outbound connections to suspicious domains/IPs.
- Several alerts were validated as true positives; some were false positives after analysis.
- A timeline of events was constructed correlating email receipt, firewall connections, and analyst actions.

Techniques & Tools Used

- SIEM dashboard for alert triage and search queries (Splunk/ELK style)
- Email header analysis and phishing URL lookup
- Firewall log correlation and IP/domain enrichment
- Python for quick CSV parsing and IOC extraction

Example Detection Queries

Splunk: index=firewall sourcetype=fw_logs dest_ip=1.2.3.4 OR dest_ip=5.6.7.8 | stats count by src_ip, dest_ip, _time


KQL: DeviceEvents | where Timestamp >= ago(7d) and RemoteUrl contains "suspicious-domain.com"

Evidence (Selected Screenshots)

The screenshot displays a SOC simulation interface with a sidebar on the left containing navigation links: Dashboard, Alert queue, SIEM, Analyst VM, Documentation, Playbooks, Case reports, and Guide. The main area shows a list of alerts under the heading 'Assigned alert(s)'. Two alerts are visible:

- Alert 8815:** Inbound Email Containing Suspicious External Link. Severity: Medium. Type: Phishing. Date: Sep 23rd 2025 at 03:08. 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. Metadata includes dataprovider: email, timestamp: 09/23/2025 03:06:11.143, 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. We don't hear from you within 48 hours, your package will be returned to sender. Thank you, Amazon Delivery, direction: inbound. A 'Write case report' button is present.
- Alert 8816:** Access to Blacklisted External URL Blocked by Firewall. Severity: High. Type: Firewall. Date: Sep 23rd 2025 at 03:09. Status: 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. Metadata includes dataprovider: firewall, timestamp: 09/23/2025 03:07:25.143, 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. A 'Playbook link' is provided.

At the bottom of the interface, there is an 'Exit simulation' button and a footer that reads 'Created by TryHackMe'.



Dashboard

Alert queue

SIEM

Analyst VM


Documentation

Playbooks

Case reports

Guide

Exit simulation

Created by 

Assigned alert(s)

Write case report

8817

Inbound Email Containing Suspicious External Link

Medium

Phishing

Sep 23rd 2025 at 03:10

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:

09/23/2025 03:08:29.143

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.\n\nLocation: Lagos, Nigeria\n\nIP Address: 102.89.222.143\n\nDate: 2025-01-24 06:42\n\nIf this was not you, please secure your account immediately to avoid unauthorized access.\n\na href="https://microsoftsupport.co/login">Review Activity/a\n\nThank you,\n\nMicrosoft Account Security Team

direction:

inbound

Playbook link

Search for an alert

Reset filters

Severity

Status

Alert type

Show 15 alerts

ID	Alert rule	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	Sep 23rd 2025 at 03:10	Awaiting action	
<div>Description:</div> <div>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.</div> <div><div>datasource:</div><div>email</div></div> <div><div>timestamp:</div><div>09/23/2025 03:08:57.143</div></div> <div><div>subject:</div><div>Action Required: Finalize Your Onboarding Profile</div></div> <div><div>sender:</div><div>onboarding@hrconnex.thm</div></div> <div><div>recipient:</div><div>j.garcia@thetrydaily.thm</div></div> <div><div>attachment:</div><div>None</div></div> <div><div>content:</div><div>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\na href="https://hrconnex.thm/onboarding/15400654060/j.garcia">Set Up My Profile/a\n\nIf you have questions, please reach out to the HR Onboarding Team.</div></div> <div><div>direction:</div><div>inbound</div></div> <div><div>Playbook link</div></div>						
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	Sep 23rd 2025 at 03:09	Closed	
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	Sep 23rd 2025 at 03:08	Closed	

8818

Access to Blacklisted External URL Blocked by Firewall

High

Firewall

0.0 minutes

Closed

View analysis

False positives

Assess your accuracy on the alerts you marked as false positives.

ID	Alert rule	Severity	Type	Time to resolve	Classification	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	1.0 minutes	Closed	View

True positive identification rate

Rate of incidents correctly identified as malicious

All alert types

100%

Your true positive rate is excellent! Keep up the great work!

False positive identification rate

Rate of incidents correctly identified as benign

All alert types

100%

Your false positive rate is excellent! Keep up the great work!

Closed alerts

within this scenario

4 alerts

Mean time to resolve


within this scenario

1 minutes

Mean dwell time


within this scenario

3 minutes



- Dashboard
- Alert queue**
- SIEM
- Analyst VM
- Documentation
- Playbooks
- Case reports
- Guide

Exit simulation

Created by 

Alert queue 4 alerts incoming

Assigned alert(s)

Write case report

8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	Sep 23rd 2025 at 03:07	
------	---	--------	----------	------------------------	--

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: 09/23/2025 03:05:02.143

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\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

[Playbook link](#)

Reset filters
Severity
Status
Alert type
Show 15 alerts

ID	Alert rule	Severity	Type	Date	Status	Action
Showing 1 to 0 of 0 entries						

Previous
1
Next

Remediation Recommendations

- Isolate affected hosts and perform forensic imaging.
- Block malicious IPs/domains at perimeter and email gateway.
- Reset credentials and enforce MFA for affected accounts.
- Tune SIEM rules with identified IOCs and update detections.
- Conduct user awareness training on phishing indicators.

Conclusion

The lab exercise reinforced SOC skills in alert triage, log correlation, and incident response. The included evidence supports the findings and recommended containment steps.