

The screenshot shows the THM Built-in SIEM interface with the following details:

Alert queue (3 alerts incoming)

Assigned alert(s)

Alert ID: 8815 - **Inbound Email Containing Suspicious External Link** - **Medium** - **Phishing** - **Nov 28th 2025 at 06:37**

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: 11/28/2025 06:35:55.536

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 information by clicking the link below:\n\nhttp://bit.ly/3shlkx3da12340\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

Playbook link

Alert ID: 8814 - **Inbound Email Containing Suspicious External Link** - **Medium** - **Phishing** - **Nov 28th 2025 at 06:36**

Search for an alert

Reset filters

Severity

Status

Alert type

Show 15 alerts

Action

ID **Alert rule** **Severity** **Type** **Date** **Status** **Action**

Showing 1 to 0 of 0 entries

Previous 1 Next

Created by THM Hack Me

THM Built-in SIEM for daily practices

10-10-44-26.reverse-proxy-eu-west-1.tryhackme.com/en-US/app/search/search?q=search%20&sid=1764312362.56&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=-24h%40h&latest=now

Splunk > enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards **> Search & Reporting**

New Search

Save As ▾ Create Table View Close

Last 24 hours

87 events (11/27/25 6:00:00.000 AM to 11/28/25 6:46:02.000 AM) No Event Sampling ▾

Events (87) Patterns Statistics Visualization Job ▾

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect 1 hour per column

List ▾ Format 50 Per Page ▾ 1 2 Next >

Selected Fields	All Fields	i Time	Event
SELECTED FIELDS <i>a host</i> 1 <i>a source</i> 1 <i>a sourcetype</i> 1		> 11/28/25 6:42:36.536 AM { [-] <i>Action</i> : allowed <i>Application</i> : web-browsing <i>DestinationIP</i> : 34.120.58.11 <i>DestinationPort</i> : 443 <i>Protocol</i> : TCP <i>Rule</i> : Allow-Internet <i>SourceIP</i> : 10.20.2.24 <i>SourcePort</i> : 60582 <i>URL</i> : https://crm.hubspot.com/deals <i>datasource</i> : firewall <i>timestamp</i> : 11/28/2025 06:42:36.536	
			} Show as raw text <i>host</i> = 10.10.44.26:8989 <i>source</i> = eventcollector <i>sourcetype</i> = _json
INTERESTING FIELDS <i>a Action</i> 2 <i>a Application</i> 1 <i>a attachment</i> 1 <i>a content</i> 38 <i>a datasource</i> 2 <i>a DestinationIP</i> 22 <i># DestinationPort</i> 2 <i>a direction</i> 3 <i>a index</i> 1 <i># linecount</i> 1 <i>a Protocol</i> 1 <i>a punct</i> 38 <i>a recipient</i> 26 <i>a Rule</i> 2 <i>a sender</i> 30 <i>a SourceIP</i> 13 <i># SourcePort</i> 42 <i>a splunk_server</i> 1 <i>a subject</i> 38 <i>a timestamp</i> 78		> 11/28/25 6:42:30.536 AM { [-] <i>attachment</i> : None <i>content</i> : One candidate rescheduled--sending the updated list shortly. <i>datasource</i> : email <i>direction</i> : internal <i>recipient</i> : j.carter@thetrydaily.thm <i>sender</i> : j.carter@thetrydaily.thm <i>subject</i> : RE: RE: Hiring Update - Interview Schedule <i>timestamp</i> : 11/28/2025 06:42:30.536	
			} Show as raw text

Configured Splunk SIEM by THM