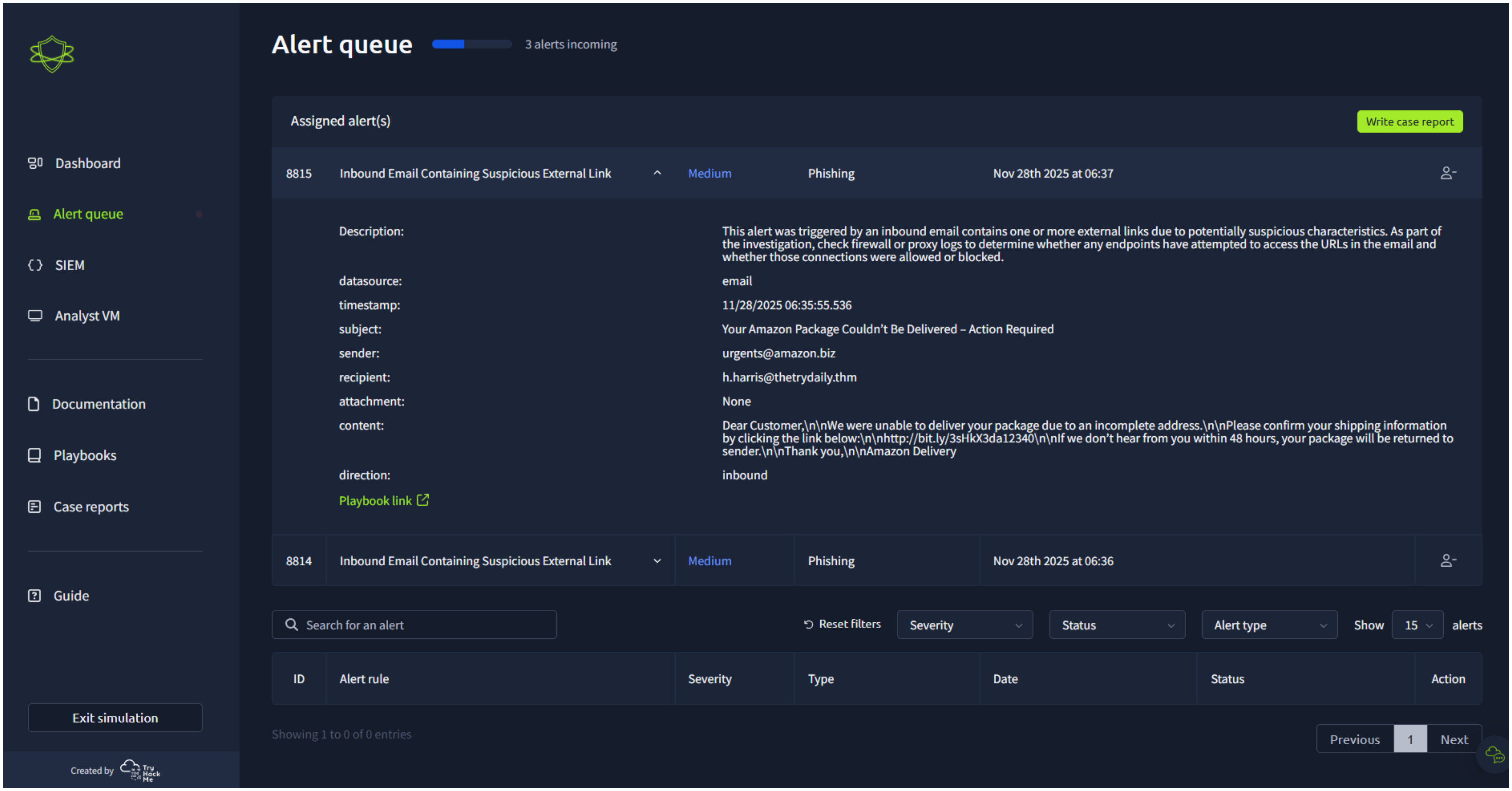


Alert queue

3 alerts incoming

Assigned alert(s)

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/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

Playbook link

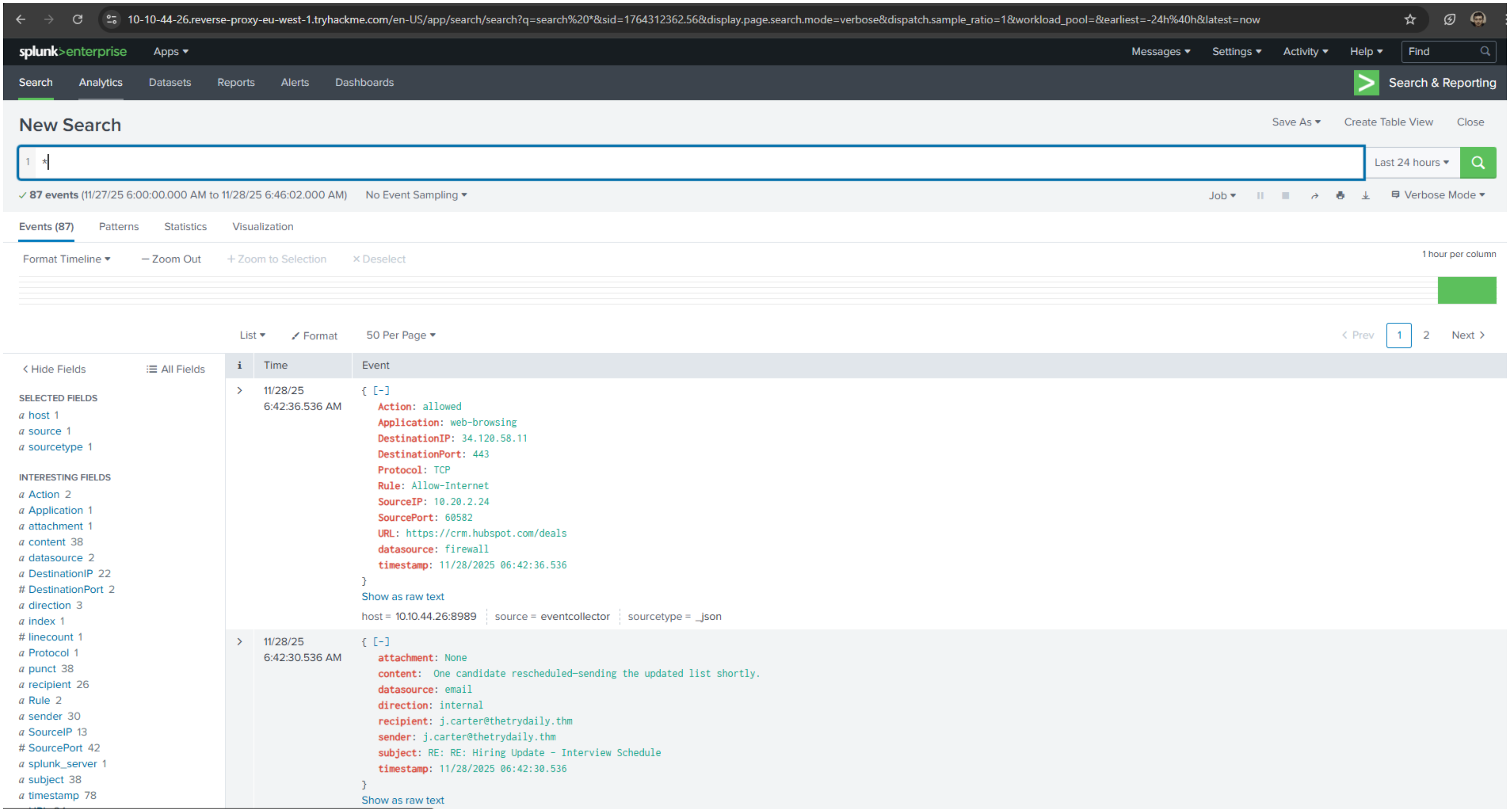
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	Nov 28th 2025 at 06:36

Search for an alert

ID	Alert rule	Severity	Type	Date	Status	Action

Showing 1 to 0 of 0 entries

THM Built-in SIEM for daily practices



```
*
```

✓ 87 events (11/27/25 6:00:00.000 AM to 11/28/25 6:46:02.000 AM)

SELECTED FIELDS

- *a* host 1
- *a* source 1
- *a* sourcetype 1

INTERESTING FIELDS

- *a* Action 2
- *a* Application 1
- *a* attachment 1
- *a* content 38
- *a* datasource 2
- *a* DestinationIP 22
- # DestinationPort 2
- *a* direction 3
- *a* index 1
- # linecount 1
- *a* Protocol 1
- *a* punct 38
- *a* recipient 26
- *a* Rule 2
- *a* sender 30
- *a* SourceIP 13
- # SourcePort 42
- *a* splunk_server 1
- *a* subject 38
- *a* timestamp 78

i	Time	Event
›	11/28/25 6:42:36.536 AM	{ [-] Action: allowed Application: web-browsing DestinationIP: 34.120.58.11 DestinationPort: 443 Protocol: TCP Rule: Allow-Internet SourceIP: 10.20.2.24 SourcePort: 60582 URL: https://crm.hubspot.com/deals datasource: firewall timestamp: 11/28/2025 06:42:36.536 } Show as raw text host = 10.10.44.26:8989 source = eventcollector sourcetype = _json
›	11/28/25 6:42:30.536 AM	{ [-] attachment: None content: One candidate rescheduled–sending the updated list shortly. datasource: email direction: internal recipient: j.carter@thetrydaily.thm sender: j.carter@thetrydaily.thm subject: RE: RE: Hiring Update - Interview Schedule timestamp: 11/28/2025 06:42:30.536 } Show as raw text

Configured Splunk SIEM by THM