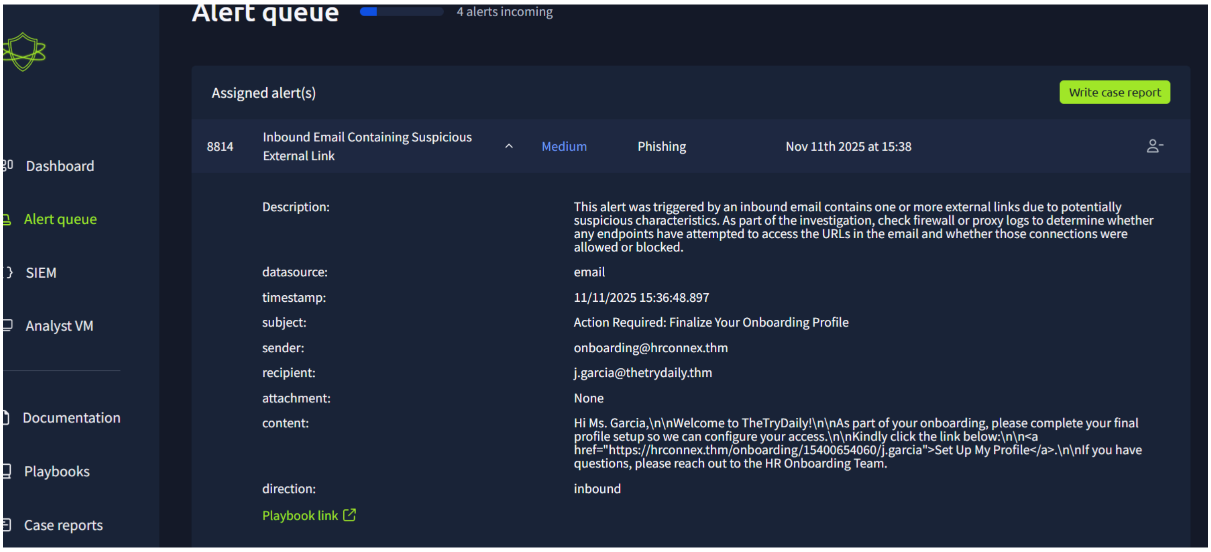
SOC lab False Positive Triage

The home lab simulation presents the Security Operations Center (SOC) dashboard, showcasing a variety of active alerts and incidents across a controlled test environment. The interface displays real-time log sources, SIEM summary panels, and a visible sequence of triggered rules. Several false positives appear—highlighted by alerts for benign user activities, such as normal administrative logins and authorized software updates. The analyst has annotated the screenshot with key metrics, clearly marking the volume of false positives compared to genuine threat detections. This initial setup illustrates the baseline challenge, emphasizing the need for fine-tuning of correlation rules, alert thresholds, and source filtering.



Assigned alert(s)

8814 Inbound Email Containing Suspicious External Link Medium Phishing Nov 11th 2025 at 15:38

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 15:36:48.897

subject: Action Required: Finalize Your Onboarding Profile

sender: onboarding@hrconnex.thm

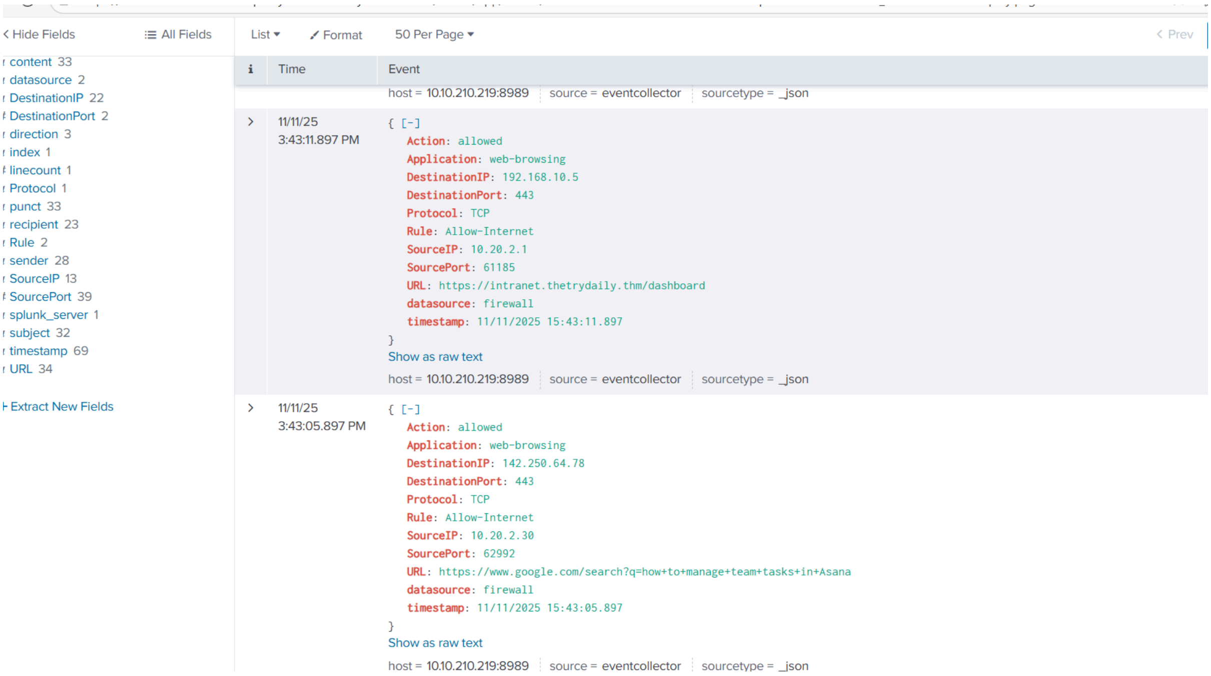
recipient: j.garcia@thetrydaily.thm

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<a 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.

direction: inbound

As I work through the SOC simulation on TryHackMe using Splunk Enterprise, I focus on analyzing firewall logs to determine if a flagged email alert is actually a false positive phishing attempt. I use Splunk's powerful search capabilities to filter all network events corresponding to the timestamp of the suspected phishing email, tracing both incoming and outgoing connections for the recipient's workstation. By looking for unusual traffic patterns, connections to suspicious IP addresses, or any evidence of blocked attempts, I find that all the related network activity is normal and consistent with legitimate business use. No signs of malware payload delivery, command-and-control traffic, or unauthorized data extraction appear in the firewall logs. This process helps me confidently classify the phishing alert as a false positive, demonstrating the effectiveness of combining lab-based SOC skills with real-world log analysis in Splunk.



content 33
datasource 2
DestinationIP 22
DestinationPort 2
direction 3
index 1
linecount 1
Protocol 1
punct 33
recipient 23
Rule 2
sender 28
SourceIP 13
SourcePort 39
splunk_server 1
subject 32
timestamp 69
URL 34

Extract New Fields

i	Time	Event

host = 10.10.210.219:8989 | source = eventcollector | sourcetype = _json

11/11/25 3:43:11.897 PM

```
{ [-]
   Action: allowed
   Application: web-browsing
   DestinationIP: 192.168.10.5
   DestinationPort: 443
   Protocol: TCP
   Rule: Allow-Internet
   SourceIP: 10.20.2.1
   SourcePort: 61185
   URL: https://intranet.thetrydaily.thm/dashboard
   datasource: firewall
   timestamp: 11/11/2025 15:43:11.897
}
```

Show as raw text

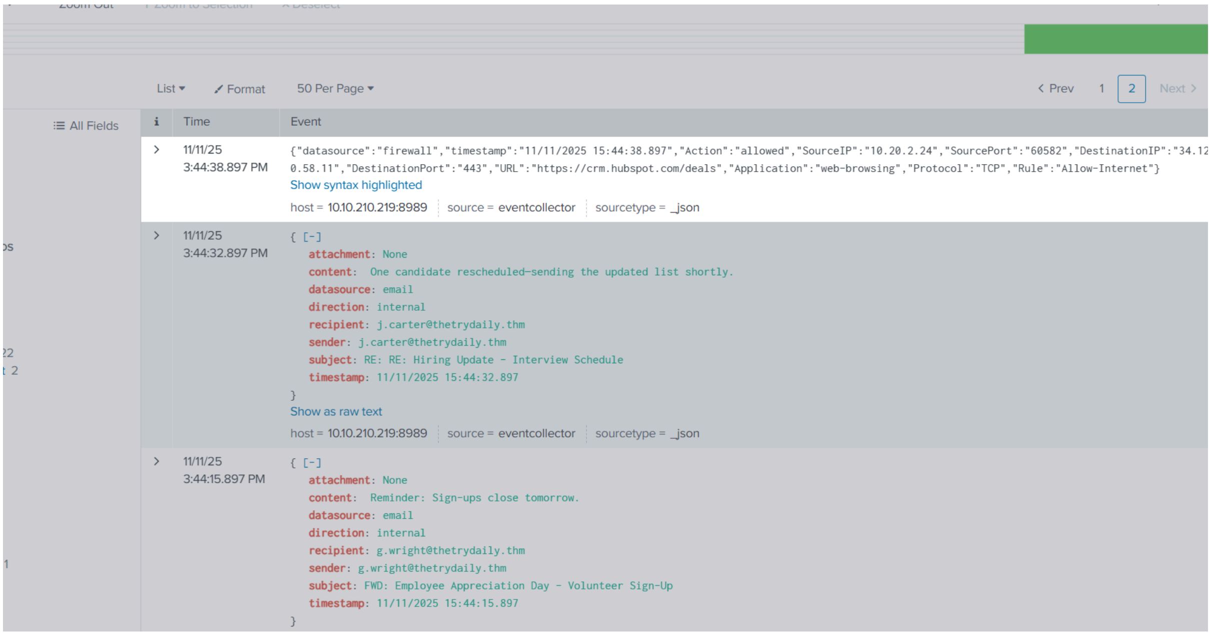
host = 10.10.210.219:8989 | source = eventcollector | sourcetype = _json

11/11/25 3:43:05.897 PM

```
{ [-]
   Action: allowed
   Application: web-browsing
   DestinationIP: 142.250.64.78
   DestinationPort: 443
   Protocol: TCP
   Rule: Allow-Internet
   SourceIP: 10.20.2.30
   SourcePort: 62992
   URL: https://www.google.com/search?q=how+to+manage+team+tasks+in+Asana
   datasource: firewall
   timestamp: 11/11/2025 15:43:05.897
}
```

Show as raw text

host = 10.10.210.219:8989 | source = eventcollector | sourcetype = _json



i	Time	Event

11/11/25 3:44:38.897 PM

{"datasource":"firewall","timestamp":"11/11/2025 15:44:38.897","Action":"allowed","SourceIP":"10.20.2.24","SourcePort":"60582","DestinationIP":"34.120.58.11","DestinationPort":"443","URL":"https://crm.hubspot.com/deals","Application":"web-browsing","Protocol":"TCP","Rule":"Allow-Internet"}

Show syntax highlighted

host = 10.10.210.219:8989 | source = eventcollector | sourcetype = _json

11/11/25 3:44:32.897 PM

```
{ [-]
   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: 11/11/2025 15:44:32.897
}
```

Show as raw text

host = 10.10.210.219:8989 | source = eventcollector | sourcetype = _json

11/11/25 3:44:15.897 PM

```
{ [-]
   attachment: None
   content:  Reminder: Sign-ups close tomorrow.
   datasource: email
   direction: internal
   recipient: g.wright@thetrydaily.thm
   sender: g.wright@thetrydaily.thm
   subject: FWD: Employee Appreciation Day – Volunteer Sign-Up
   timestamp: 11/11/2025 15:44:15.897
}
```