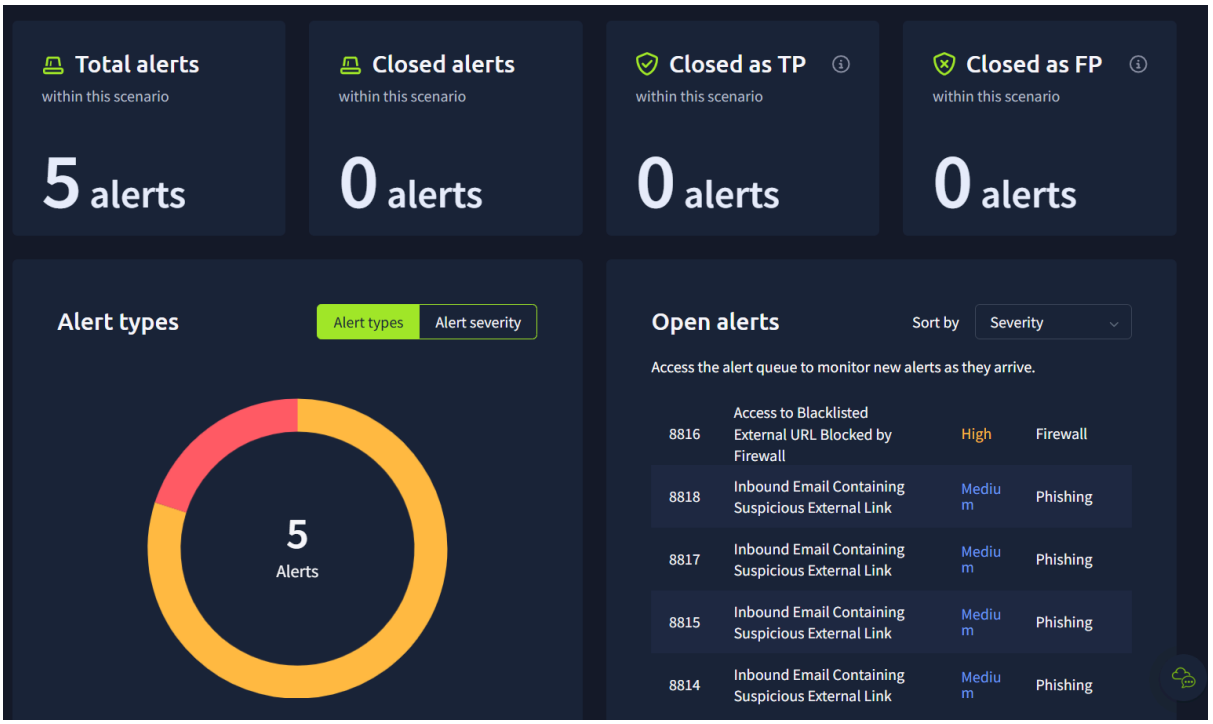
Scenario Overview

The scenario began with five open alerts, including one High-severity firewall alert and four Medium-severity phishing alerts. Alerts were prioritized based on severity and potential impact.



Triage Methodology

No escribas explicación aquí. Solo método.

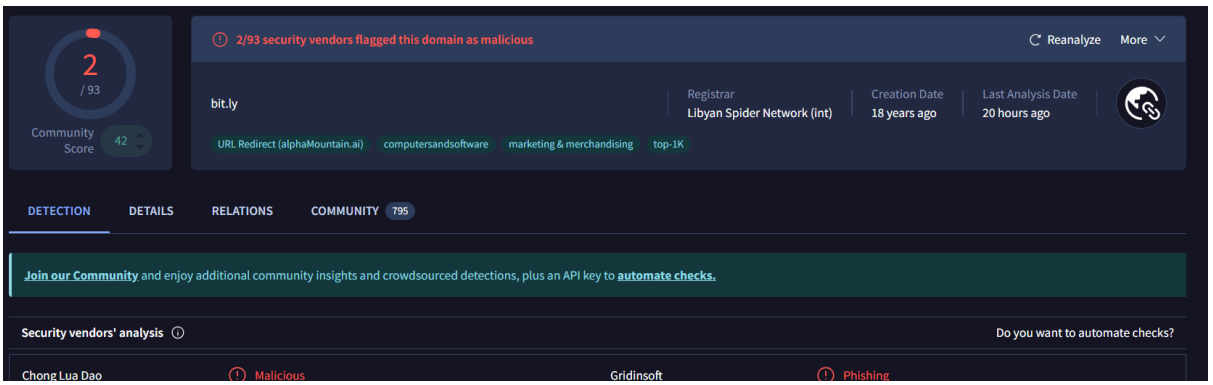
- Severity-based prioritization
- Email and firewall log correlation
- Threat intelligence validation (VirusTotal)
- User interaction verification
- Evidence-based escalation decisions

Alert Investigation & Resolution

Alert 8816 – Firewall (High)

Category	Details
When	Feb 25, 2026 – 16:12
Who	Host 10.20.2.17
What	Outbound attempt to blacklisted shortened URL
Where	67.199.248.11 – Port 80 (Blocked)
Classification	True Positive
Escalation	No
Indicators	67.199.248.11 / bit.ly link

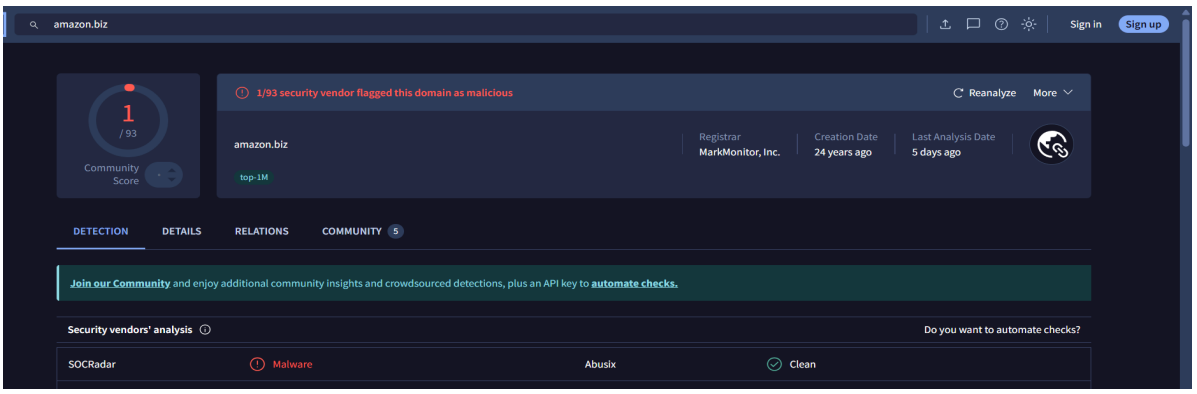
Analysis & Decision Rationale:
Firewall logs confirmed the outbound request was successfully blocked. I validated the destination IP and associated domain using VirusTotal and found no active malicious detections. No additional outbound attempts or suspicious behavior from the host were observed. Since the connection was prevented and no compromise indicators were identified, the alert was closed without escalation.

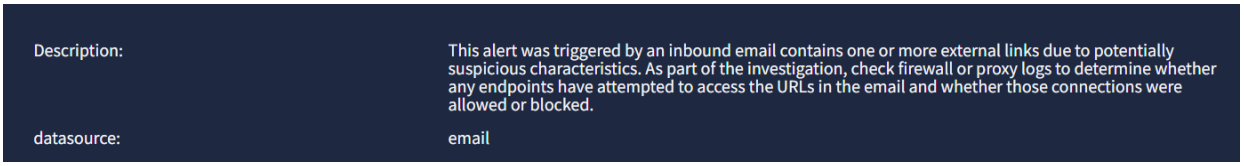


Alert 8815 – Amazon Phishing (Medium)

Category	Details
When	Feb 25, 2026 – 16:11
Who	h.harris@thetrydaily.thm
What	Amazon impersonation phishing email
Where	amazon.biz + shortened URL
Classification	True Positive
Escalation	No
Indicators	amazon.biz / bit.ly link

Analysis & Decision Rationale:
The sender domain (amazon.biz) is inconsistent with Amazon's legitimate domain naming conventions. The email applied urgency and used a shortened URL to obscure the destination. I correlated this alert with firewall logs and confirmed that no successful outbound connection occurred. As no evidence of credential submission or endpoint compromise was observed, escalation was not required.



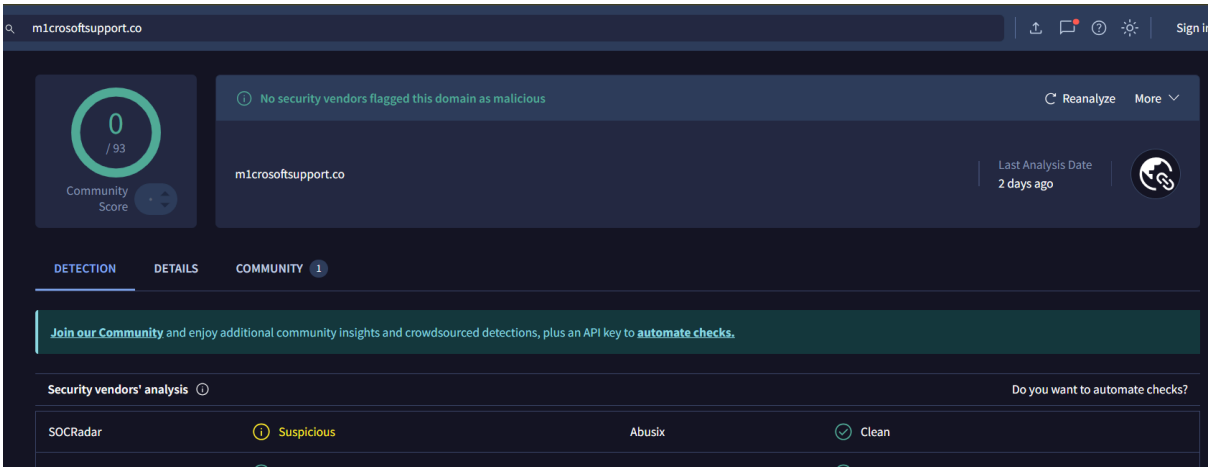


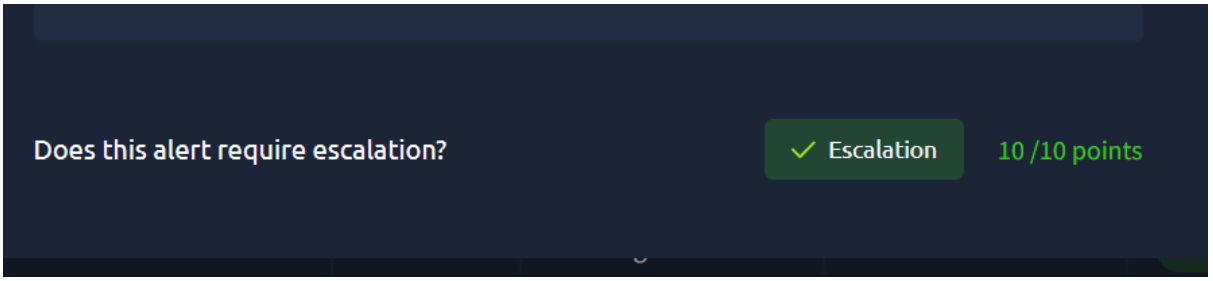
Alert 8817 – Microsoft Typosquatting (Medium)

Category	Details
When	Feb 25, 2026 – 16:13
Who	c.allen@thetrydaily.thm
What	Microsoft impersonation phishing
Where	m1crosoftsupport.co/login
Classification	True Positive
Escalation	Yes
Indicators	m1crosoftsupport.co (typosquatting)

Analysis & Decision Rationale:

The domain used typosquatting (replacing “i” with “1”), indicating intentional impersonation. The email attempted credential harvesting by directing the user to a fraudulent login page. Although no confirmed user interaction was identified in firewall logs, the domain posed organizational risk. Due to the impersonation pattern and potential exposure, the alert was escalated for coordinated blocking and monitoring.

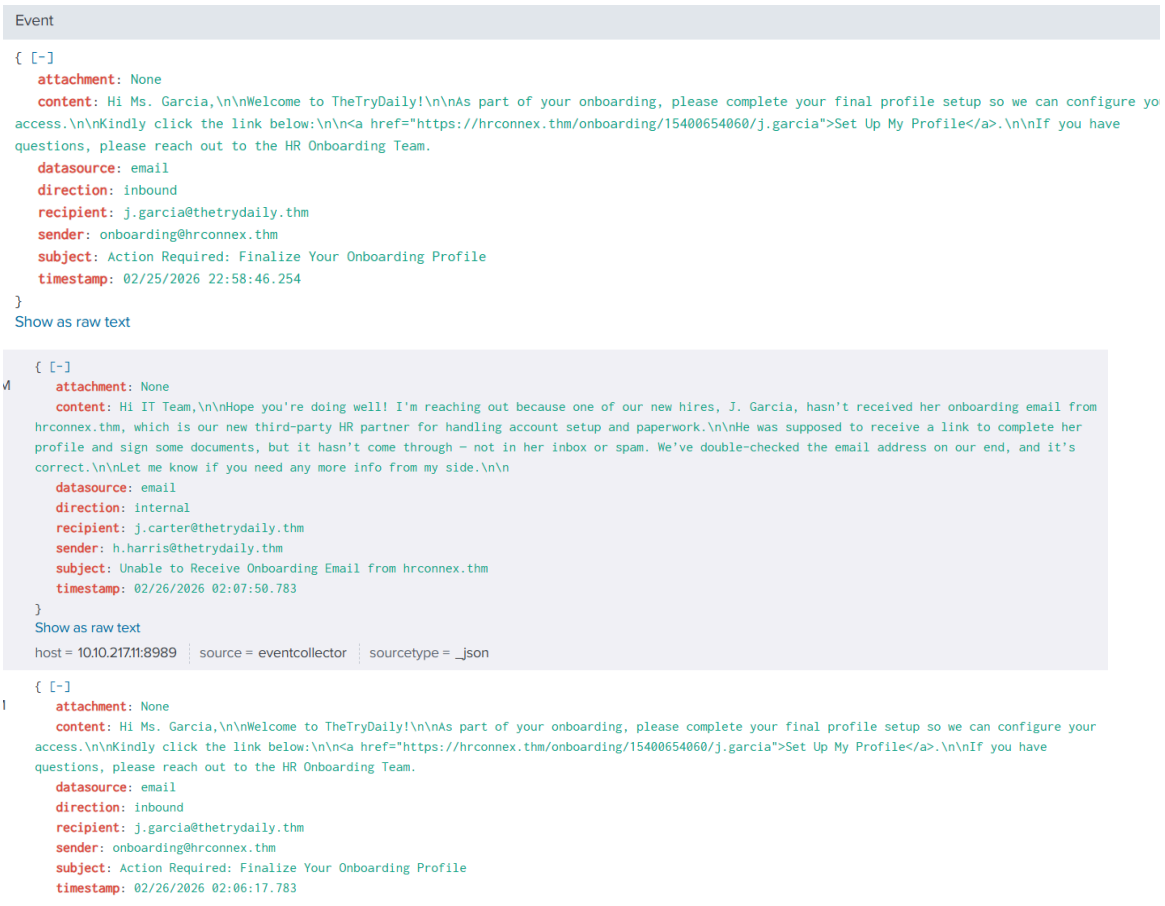




Alert 8814 – HR Email (False Positive)

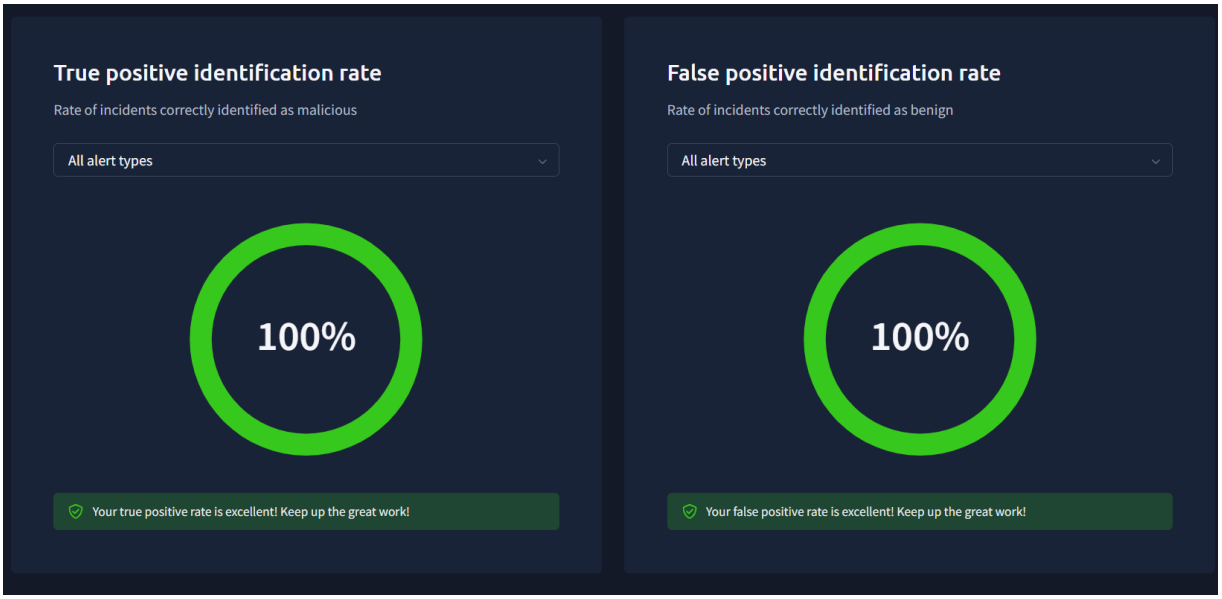
Category	Details
When	Feb 25, 2026 – 16:07
Who	j.garcia@thetrydaily.thm
What	HR onboarding email
Where	hrconnex.thm
Classification	False Positive
Escalation	No
Indicators	hrconnex.thm

Analysis & Decision Rationale:
I performed log correlation in Splunk and identified internal communication referencing hrconnex.thm as a legitimate third-party HR partner. No malicious redirection, suspicious attachments, or firewall activity was detected. Based on contextual validation and absence of threat indicators, the alert was closed as a false positive.



Final Assessment & Analytical Summary

The investigation results demonstrate consistent and well-structured incident classification across multiple alert types. Clear differentiation between legitimate activity and real security threats reflects disciplined analysis and sound decision-making.
A 100% true positive and false positive identification rate confirms accurate threat assessment and appropriate escalation handling throughout the process.



Damien Perdomo Galletti
SOC Analyst (Tier 1) – Incident Response & Log Analysis
February 2026