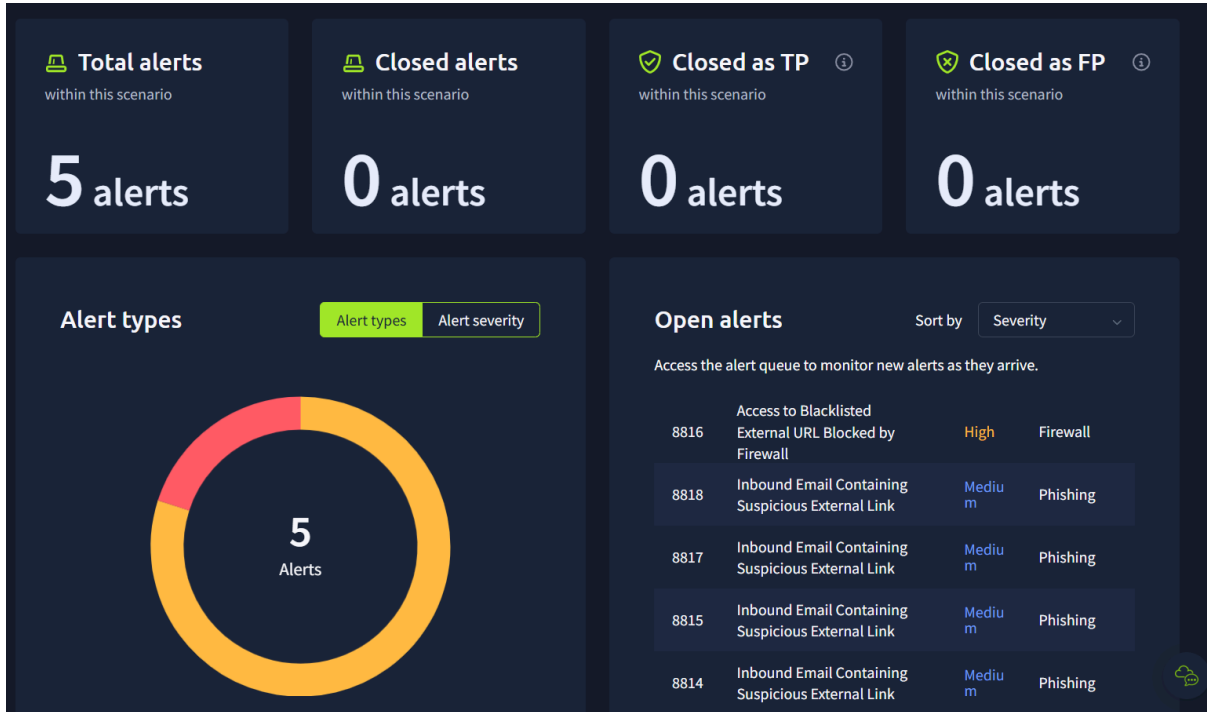


Scenario Overview

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.

ID	Alert rule	Severity	Type	Date	Status	Action
8818	Inbound Email Containing Suspicious External Link	Medium	Phishing	Feb 25th 2026 at 20:13	Awaiting action	
8817	Inbound Email Containing Suspicious External Link	Medium	Phishing	Feb 25th 2026 at 20:12	Awaiting action	
8816	Access to Blacklisted External URL Blocked by Firewall	High	Firewall	Feb 25th 2026 at 20:11	Closed	
8815	Inbound Email Containing Suspicious External Link	Medium	Phishing	Feb 25th 2026 at 20:10	Closed	
8814	Inbound Email Containing Suspicious External Link	Medium	Phishing	Feb 25th 2026 at 20:07	Closed	

2 / 93
Community Score 42

2/93 security vendors flagged this domain as malicious

Reanalyze More

bit.ly
Registrar: Libyan Spider Network (int)
Creation Date: 18 years ago
Last Analysis Date: 20 hours ago

URL Redirect (alphaMountain.ai) computersandsoftware marketing & merchandising top-1K

DETECTION DETAILS RELATIONS COMMUNITY 795

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

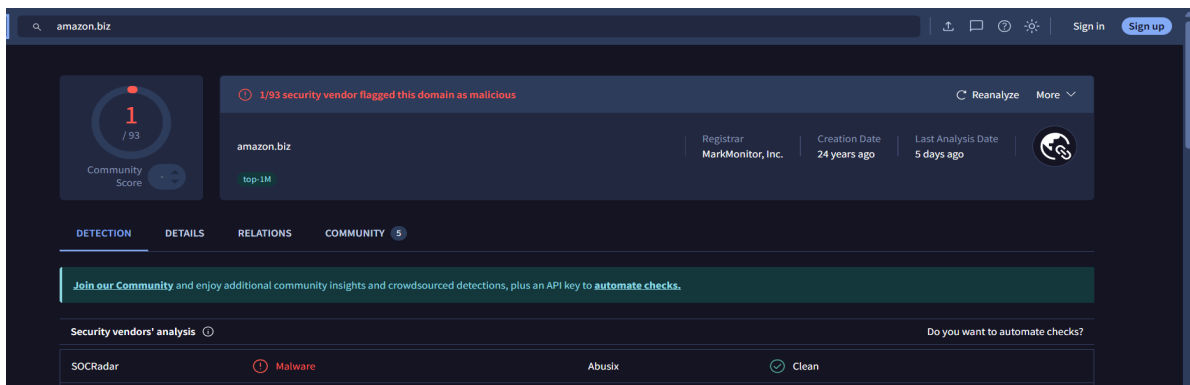
Chong Lua Dao Malicious Gridinsoft Phishing

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.



The screenshot displays a security dashboard for the domain 'amazon.biz'. At the top, there is a search bar with 'amazon.biz' entered and a 'Sign up' button. The main content area features a 'Community Score' of 1/93, a warning icon indicating that 1/93 security vendors flagged the domain as malicious, and a 'Reanalyze' button. Below this, the domain 'amazon.biz' is listed with a 'top-1M' ranking. The dashboard includes tabs for 'DETECTION', 'DETAILS', 'RELATIONS', and 'COMMUNITY'. A green banner encourages joining the community for additional insights. Under 'Security vendors' analysis', there is a table with columns for vendor name and status: SOCRadar (Malware), Abusix, and Clean. A 'Do you want to automate checks?' prompt is also visible.

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

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.

m1crosoftsupport.co

0 / 93
Community Score

No security vendors flagged this domain as malicious

m1crosoftsupport.co

Last Analysis Date
2 days ago

DETECTION DETAILS COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

SOC Radar Suspicious Abusix Clean

Do you want to automate checks?

Does this alert require escalation?

✓ Escalation

10 / 10 points

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.

Event

```
{ [-]
  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 yo
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.
  datasource: email
  direction: inbound
  recipient: j.garcia@thetrydaily.thm
  sender: onboarding@hrconnex.thm
  subject: Action Required: Finalize Your Onboarding Profile
  timestamp: 02/25/2026 22:58:46.254
}
```

Show as raw text

```
{ [-]
  attachment: None
  content: Hi IT Team,\n\nHope you're doing well! I'm reaching out because one of our new hires, J. Garcia, hasn't received her onboarding email from
hrconnex.thm, which is our new third-party HR partner for handling account setup and paperwork.\n\nHe was supposed to receive a link to complete her
profile and sign some documents, but it hasn't come through - not in her inbox or spam. We've double-checked the email address on our end, and it's
correct.\n\nLet me know if you need any more info from my side.\n\n
  datasource: email
  direction: internal
  recipient: j.carter@thetrydaily.thm
  sender: h.harris@thetrydaily.thm
  subject: Unable to Receive Onboarding Email from hrconnex.thm
  timestamp: 02/26/2026 02:07:50.783
}
```

Show as raw text

host = 10.10.217.1:8989 | source = eventcollector | sourcetype = _json

```
{ [-]
  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.
  datasource: email
  direction: inbound
  recipient: j.garcia@thetrydaily.thm
  sender: onboarding@hrconnex.thm
  subject: Action Required: Finalize Your Onboarding Profile
  timestamp: 02/26/2026 02:06:17.783
}
```

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.

