ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1004	Suspicious email from external domain.	A suspicious email was received from an external sender with an unusual top level domain. Note from SOC Lead: This detection rule still needs fine-tuning.	Phishing	Low	Dec 4th 2025 at 16:01

Alert details

datasource: email

timestamp: 12/04/2025 07:59:24.235

subject: Time Traveling Hat Adventure Explore Ancient Lands for Cheap

sender: osman@fashionindustrytrends.xyz

recipient: kyra.flores@tryhatme.com

attachment: None

content: Travel through time and experience the evolution of hats from ancient Egypt to futuristic Mars Only 500 per ticket

direction: inbound

Incident report

Edit report

Incident classification

(•) True positive ( ) False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

When:
Date: 12/04/2025
Time of activity: 07:59:24

Who:
List of Affected Entities:
- Sender: osman@fashionindustrytrends.xyz
- Recipient: kyra.flores@tryhatme.com

What:
Reason for Classifying as True Positive:
- The email domain is invalid (untrusted)
- The email provides a suspicious offer

Why:
Reason for Escalating the Alert:

Does this alert require escalation?

(•) Yes ( ) No

Complete IR:

When:
Date: 12/04/2025
Time of activity: 07:59:24

Who:
List of Affected Entities:
- Sender: osman@fashionindustrytrends.xyz
- Recipient: kyra.flores@tryhatme.com

What:
Reason for Classifying as True Positive:
- The email domain is invalid (untrusted)
- The email provides a suspicious offer

Why:
Reason for Escalating the Alert:
- The sender may use the email as a pathway to inject trojan or other malware that could damage the system and network.
- The user may have used the corporate email to visit and register to untrusted websites.

How:
Recommended Remediation Actions:
- Block the domain
- Block the email
- Pocket training on how to identify, manage, and report phishing email.
- Pre-shift meeting on how to identify, manage, and report phishing email.

List of Attack Indicators:
- Untrusted domain
- Suspicious product / service offer