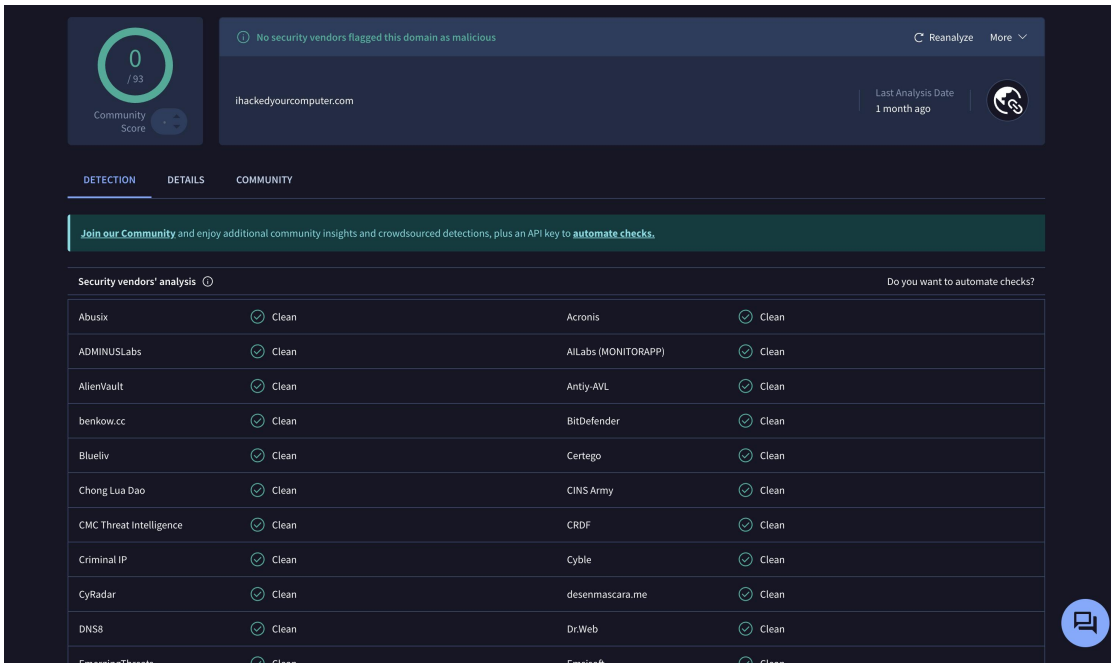
Name : Amr Khaled Elgendy
Group : AMIT - Cyber Security Online 87
Task : Real Siem Alerts

Alert 1 – SOC Investigation Report
Event ID : 59
Sender: hahaha@ihackedyourcomputer.com
Recipient: mark@letsdefend.io
Subject: I hacked your computer
Date : Feb, 14, 2021, 03:00 AM

A SOC101 – Phishing Mail Detected alert was generated by the Exchange email security system, indicating a suspicious email attempt.

Initial reputation checks showed that the sender domain was not flagged as malicious by security vendors. However, further analysis of the email content revealed a classic sextortion scam pattern that relies on fear-based social engineering rather than technical compromise.



The message contained no URLs, attachments, or malware indicators, and no evidence of system compromise was found. The email targeted a single user only, with no signs of wider distribution.

The email was blocked automatically by the email security gateway, and no user interaction occurred.

The incident was confirmed as a **true positive scam email**, successfully contained, and closed with **no impact** to the user or organization.

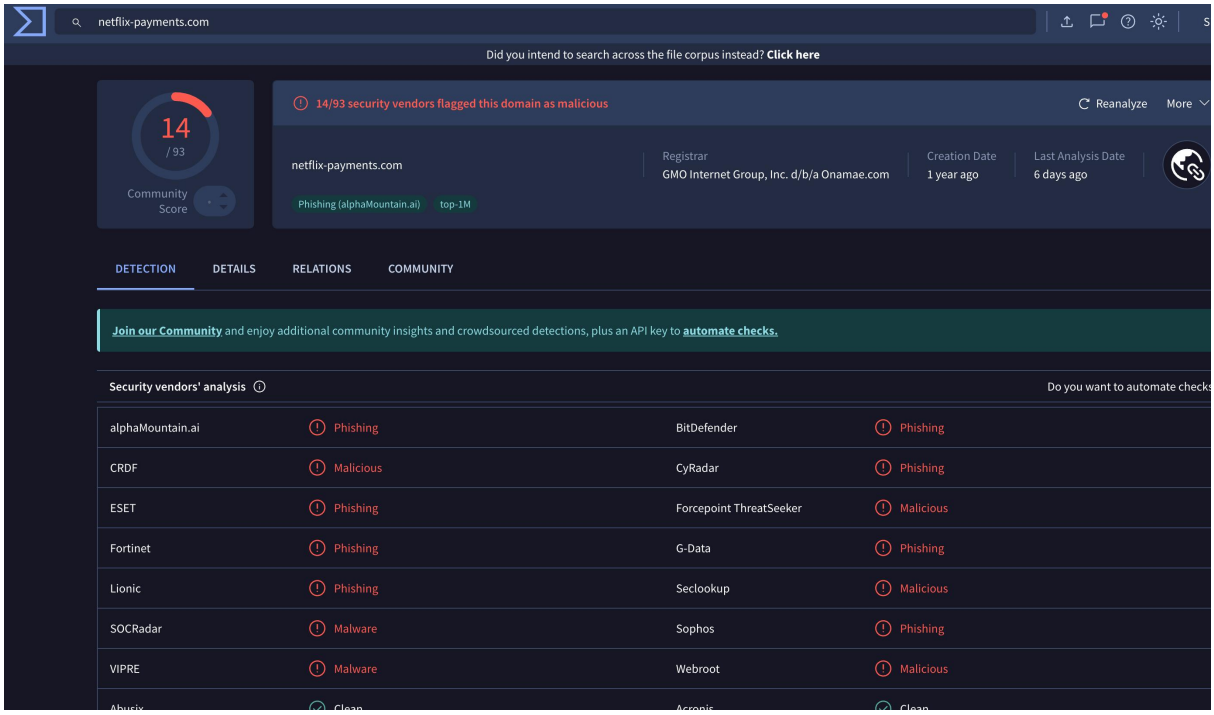
Alert 2 – SOC Investigation Report

Event ID: 34
Sender: admin@netflix-payments.com
Recipient: emily@letsdefend.io
Subject: Netflix Deals!
Date: Dec 05, 2020 – 10:33 PM

A phishing alert (SOC101 – Phishing Mail Detected) was generated by the Exchange email security system after a suspicious email was delivered to the user.

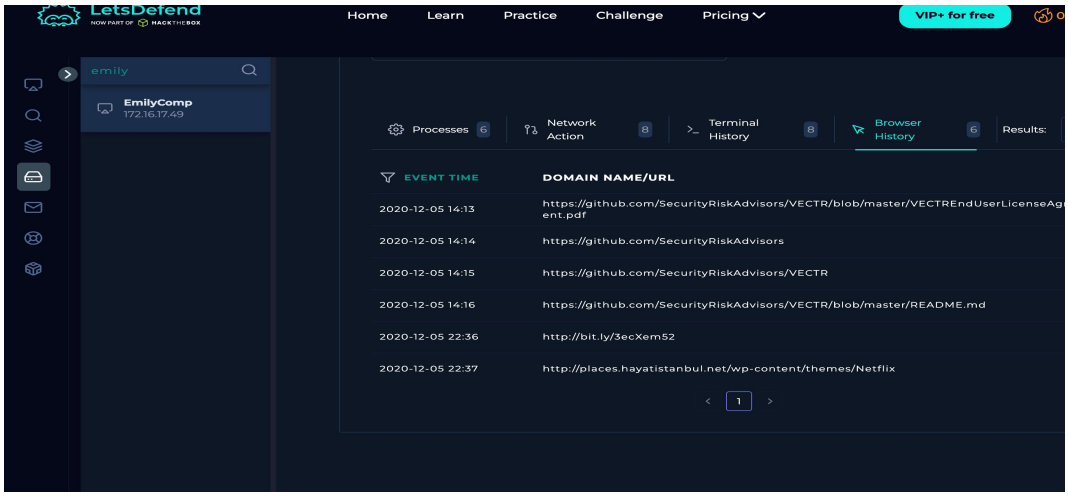
The email originated from an external sender using IP address 112.85.42.180, and the sender domain was identified as impersonating the legitimate Netflix brand.

Content analysis revealed the use of brand impersonation and promotional wording commonly observed in phishing campaigns, including a malicious URL designed to redirect the user to a fake Netflix login page.



Scope analysis confirmed the email was delivered to a single user only, with no evidence of additional recipients or internal spread.

User activity review confirmed interaction with the email at **10:36 PM**, indicating potential credential exposure.



The incident was confirmed as a **true positive**. The sender domain, SMTP source IP, and all associated malicious URLs were blocked. The affected user's credentials were reset as a precautionary measure, user awareness was advised, monitoring was enhanced, and the alert was closed with potential exposure noted.

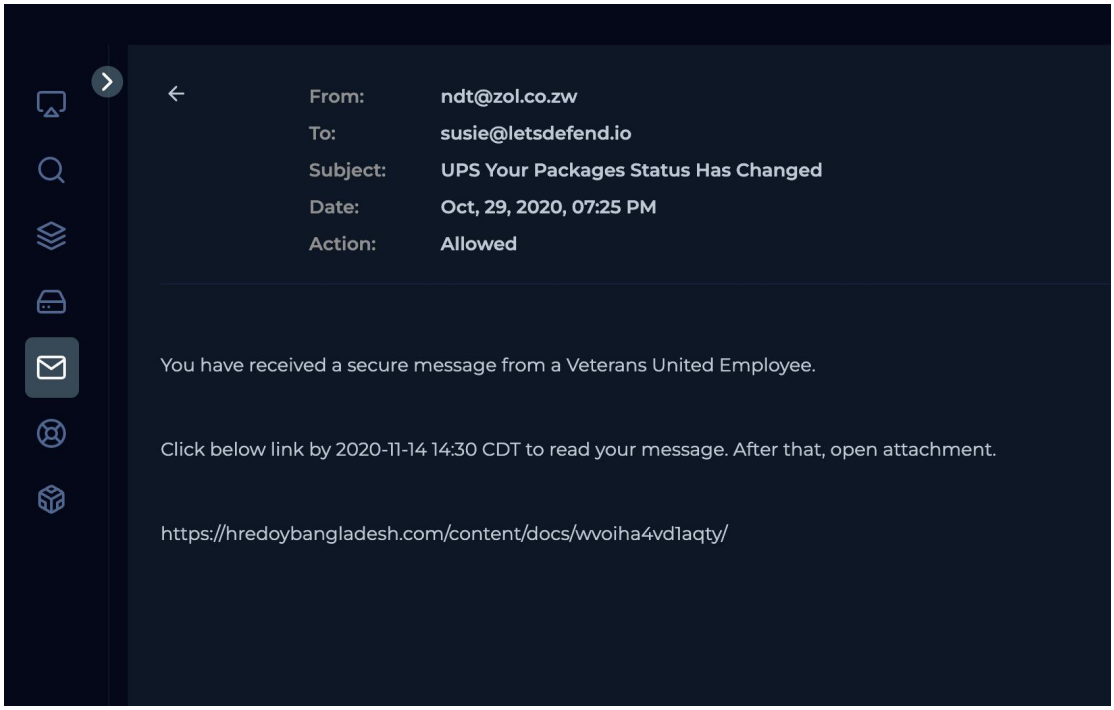
Alert 3 – SOC Investigation Report

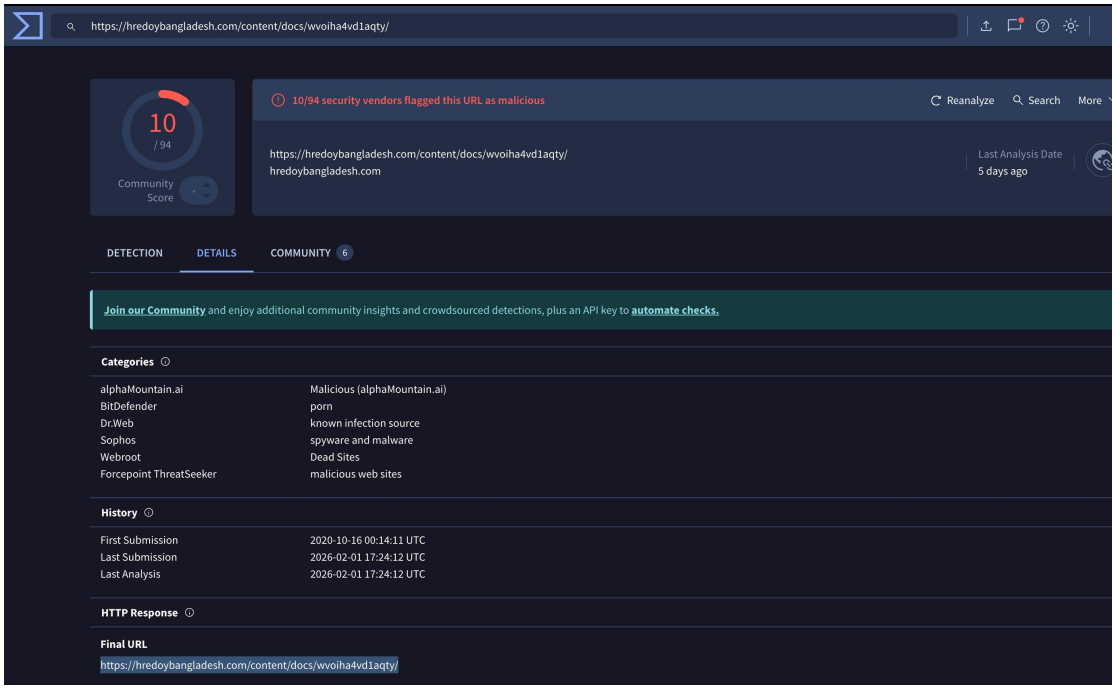
Event ID: 27
Sender: ndt@zol.co.zw
Recipient: susie@letsdefend.io
Subject: UPS Your Packages Status Has Changed
Date: Oct 29, 2020 – 07:25 PM

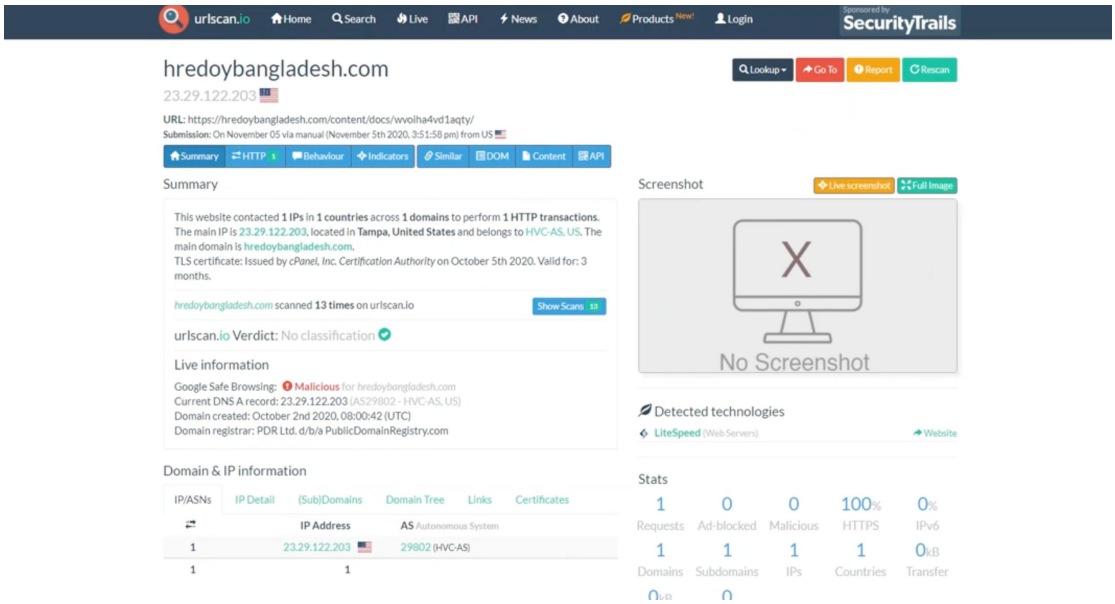
A phishing alert (SOC101 – Phishing Mail Detected) was generated by the Exchange email security system, indicating a phishing attempt. The email was automatically blocked by the security control.

The email originated from an external sender using IP address **146.56.209.252**. The sender domain does not belong to UPS and was identified as suspicious based on impersonation behavior.

Content analysis showed the subject line impersonates a well-known shipping company (UPS), which is a common phishing technique used to lure users into interacting with malicious content.







Scope assessment confirmed that the email targeted a single user only, with no evidence of wider distribution across the organization.

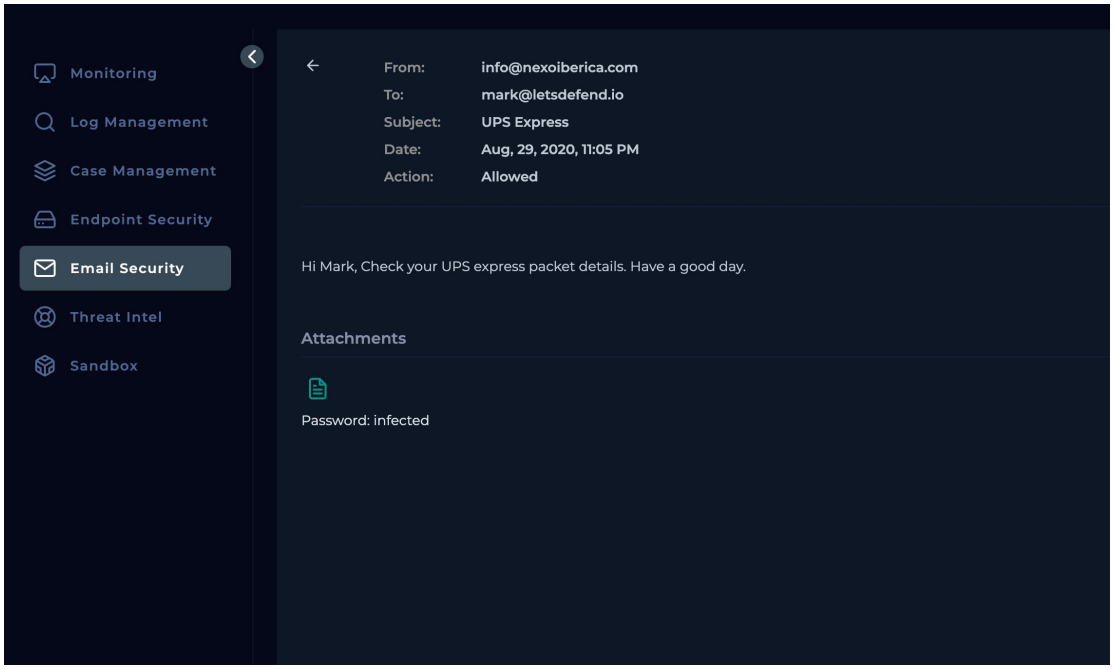
User interaction review confirmed that the email was blocked before delivery and no user interaction occurred.

The incident was confirmed as a **true positive**, successfully contained, and closed with no impact on users or systems.

Alert 4 – SOC Investigationx Report

Event ID: 8
Sender: info@nexoiberica.com
Recipient: mark@letsdefend.io
Subject: UPS Express
Date: Aug 29, 2020 – 11:05 PM

A phishing alert (SOC101 – Phishing Mail Detected) was triggered by the Exchange email security system, indicating a potential phishing email. The email was allowed and delivered to the user.



The email originated from an external sender using IP address 63.35.133.186. The sender domain is not associated with UPS and was identified as suspicious due to brand impersonation.

Email content analysis showed the subject line impersonates a legitimate shipping service (UPS), a common technique used in phishing campaigns to gain user trust.

Scope assessment confirmed the email targeted a single user only, with no indication of wider distribution within the organization.

User interaction review showed that the email was delivered successfully. No confirmed interaction was observed; however, potential user exposure cannot be ruled out.

The incident was confirmed as a **true positive phishing attempt**. User awareness was recommended, monitoring was advised, and the alert was closed.