📄 REAL SIEM ALERTS – SOC101 PHISHING REPORT

Platform: LetsDefend
Role: Junior SOC Analyst
Alert Type: Phishing Mail Detected
System: Microsoft Exchange
Severity: Low

1. Introduction

This report documents the investigation and analysis of four phishing email alerts detected by the **SOC101 – Phishing Mail Detected** rule on the LetsDefend SIEM platform.

The objective is to:

- Analyze real-world SIEM alerts.
- Identify phishing characteristics.
- Demonstrate proper SOC analyst investigation and documentation.

Although all alerts are classified as low severity, phishing remains a serious threat because it can lead to credential theft, financial fraud, or malware infection if not properly handled.

2. Alert Summary

Event ID	Date & Time	Source Email	Destination Email	Subject	Device Action
59	Feb 14, 2021 – 03:00 AM	hahaha@ihackedyourcomputer.com	mark@letsdefend.io	I hacked your computer	Blocked

34	Dec 05, 2020 – 10:33 PM	admin@netflix-payments.com	emily@letsdefend.io	Netflix Deals!	Allowed
27	Oct 29, 2020 – 07:25 PM	ndt@zol.co.zw	susie@letsdefend.io	UPS Your Packages Status Has Changed	Blocked
8	Aug 29, 2020 – 11:05 PM	info@nexoiberica.com	mark@letsdefend.io	UPS Express	Allowed

3. Detailed Alert Analysis

3.1 Event ID 59 – "I hacked your computer"

- **SMTP Address:** 27.128.173.81
- **Source Email:** hahaha@ihackedyourcomputer.com
- **Destination Email:** mark@letsdefend.io
- **Subject:** I hacked your computer
- **Device Action:** Blocked

Analysis:
This email is a classic phishing and social engineering attempt designed to intimidate the recipient. The suspicious sender domain and threatening subject strongly indicate a phishing campaign. The Exchange system successfully blocked the email, preventing delivery to the user.

True Positive: ✅

3.2 Event ID 34 – “Netflix Deals!”

- **SMTP Address:** 112.85.42.180
- **Source Email:** admin@netflix-payments.com
- **Destination Email:** emily@letsdefend.io
- **Subject:** Netflix Deals!
- **Device Action:** Allowed

Analysis:
This email impersonates Netflix to trick the recipient into potential credential theft. Although it was allowed by the email system, the sender domain is not legitimate.

True Positive: ✅

URLs or Attachments: ❌ Not listed in event data

3.3 Event ID 27 – “UPS Your Packages Status Has Changed”

- **SMTP Address:** 146.56.209.252
- **Source Email:** ndt@zol.co.zw
- **Destination Email:** susie@letsdefend.io
- **Subject:** UPS Your Packages Status Has Changed
- **Device Action:** Blocked

Analysis:
This phishing attempt uses a fake UPS notification to lure the recipient. The device successfully blocked the email. The SMTP IP should be monitored for further malicious activity.

True Positive: ✅

URLs or Attachments: ❌ Not listed in event data

3.4 Event ID 8 – “UPS Express”

- **SMTP Address:** 63.35.133.186

- **Source Email:** info@nexoiberica.com
- **Destination Email:** mark@letsdefend.io
- **Subject:** UPS Express
- **Device Action:** Allowed

Analysis:
The email attempts to impersonate UPS. The sender is suspicious, and the subject is intended to trick the recipient. Since the device allowed it, users may be exposed. The SMTP IP should be monitored for future malicious activity.

True Positive: ✅

URLs or Attachments: ❌ Not listed in event data

4. Investigation Process

As a SOC analyst, the following steps were performed for all alerts:

- Reviewed alert metadata and detection rule details.
- Analyzed sender and recipient email addresses.
- Checked email subjects for phishing indicators.
- Verified SMTP IP reputation.
- Observed email behavior (Blocked vs Allowed).
- Documented findings and preserved evidence via screenshots.

5. Findings

- Multiple phishing attempts targeted the organization over time.
- Attackers used social engineering and brand impersonation techniques.
- Low severity alerts may still pose a significant risk.
- Automated security controls successfully blocked some emails, while others required analyst intervention.

6. Conclusion

The **SOC101 phishing alerts** highlight that even low-severity emails require thorough investigation due to their potential impact. Proper alert review, documentation, and user awareness are essential for effective SOC operations.

All four alerts were **True Positives**, demonstrating accurate detection by the SOC101 rule.