Report – EventID 8 “UPS Express”

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

1. Alert Metadata

- **EventID:** 8
- **Event Time:** Aug 29, 2020, 11:05 PM
- **Rule:** SOC101 - Phishing Mail Detected
- **SMTP Address:** 63.35.133.186
- **Source Email:** info@nexoiberica.com
- **Destination Email:** mark@letsdefend.io
- **Email Subject:** UPS Express
- **Device Action:** Allowed

2. Investigation Steps

1. Reviewed alert metadata and SOC101 rule details.
2. Verified sender domain `nexoiberica.com` authenticity.
3. Analyzed email subject for phishing indicators (UPS impersonation).
4. Checked SMTP IP for reputation.
5. Noted device action (Allowed) – potential exposure.
6. Captured screenshots and documented findings.

3. Analysis

- Email attempts phishing via UPS impersonation.

- Sender domain is suspicious and not affiliated with UPS.
- Subject line aims to trick the recipient into acting on a fake shipment alert.
- Device allowed the email, exposing recipient to risk.

4. Findings

- Real phishing attempt.
- Social engineering via brand impersonation.
- Allowed email highlights importance of user awareness.

5. Conclusion

- **True Positive** – SOC101 rule correctly identified phishing attempt.
- Recommend monitoring SMTP IP `63.35.133.186` and educating users on phishing threats.