Report – EventID 27 “UPS Your Packages Status Has Changed”

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

1. Alert Metadata

- **EventID:** 27
- **Event Time:** Oct 29, 2020, 07:25 PM
- **Rule:** SOC101 - Phishing Mail Detected
- **SMTP Address:** 146.56.209.252
- **Source Email:** ndt@zol.co.zw
- **Destination Email:** susie@letsdefend.io
- **Email Subject:** UPS Your Packages Status Has Changed
- **Device Action:** Blocked

2. Investigation Steps

1. Reviewed alert details and SOC101 detection rule.
2. Verified sender domain authenticity.
3. Analyzed email subject for phishing tactics (fake package notification).
4. Checked SMTP IP against blacklists for malicious activity.
5. Confirmed device action (Blocked) to prevent exposure.
6. Documented investigation and captured screenshots.

3. Analysis

- Email is a **phishing attempt** impersonating UPS.
- Sender domain `zol.co.zw` is **suspicious and not official UPS**.
- Subject line aims to create urgency to click links.
- The device **blocked** the email, preventing user exposure.

4. Findings

- Real phishing attempt, correctly detected and blocked.
- Attackers use brand impersonation and urgency as social engineering tactics.
- SMTP IP requires monitoring for potential future attacks.

5. Conclusion

- **True Positive** – alert accurately identified a phishing email.
- Effective security controls prevented compromise.