Report – EventID 34 “Netflix Deals!”

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

1. Alert Metadata

- **EventID:** 34
- **Event Time:** Dec 05, 2020, 10:33 PM
- **Rule:** SOC101 - Phishing Mail Detected
- **SMTP Address:** 112.85.42.180
- **Source Email:** admin@netflix-payments.com
- **Destination Email:** emily@letsdefend.io
- **Email Subject:** Netflix Deals!
- **Device Action:** Allowed

2. Investigation Steps

1. Reviewed alert metadata and SOC101 rule details.
2. Verified sender domain authenticity.
3. Analyzed email subject for phishing indicators (brand impersonation).
4. Checked SMTP IP reputation against known blacklists.
5. Documented device action (Allowed) and noted potential exposure.
6. Preserved evidence with screenshots.

3. Analysis

- Email impersonates Netflix to lure recipients.

- Sender domain is **not legitimate**, indicating phishing.
- Subject “Netflix Deals!” aims to attract clicks and potentially steal credentials.
- The email was **allowed**, so the recipient could have been exposed.

4. Findings

- Real phishing attempt detected.
- Brand impersonation is the main social engineering technique.
- Allowed action requires user awareness to prevent compromise.

5. Conclusion

- **True Positive** – the alert correctly identified a phishing attempt.
- Recommend user notification and monitoring SMTP IP `112.85.42.180` for future threats.