

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

Alert 1

SEVERITY	DATE	RULE NAME	EVENTID	TYPE
Low	Feb, 14, 2021, 03:00 AM	SOC101 - Phishing Mail Detected	59	Exchange
EventID : 59				
Event Time : Feb, 14, 2021, 03:00 AM				
Rule : SOC101 - Phishing Mail Detected				
Level : Security Analyst				
SMTP Address : 27.128.173.81				
Source Address : hahaha@ihackedyourcomputer.com				
Destination Address : mark@letsdefend.io				
E-mail Subject : I hacked your computer				
Device Action : Blocked				

SOC Investigation – 6 Challenges

1. Alert Understanding:

The alert SOC101 – Phishing Mail Detected indicates a phishing email attempt detected by the Exchange email security system.

2. Source & Sender Analysis:

The email was sent from an external sender (hahaha@ihackedyourcomputer.com) using IP address 27.128.173.81, which appears suspicious.

3. Email Content Analysis:

The subject “I hacked your computer” is a threatening message commonly used in phishing campaigns.

4. Scope & Impact Assessment:

The email was delivered to a single user only with no evidence of wider distribution.

5. User Interaction Check:

The email was blocked automatically and no user interaction occurred.

6. Response & Closure:

The incident was contained successfully, classified as a true positive, and closed with no impact.

Alert 2

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

1. Alert Understanding:

The alert SOC101 – Phishing Mail Detected indicates a phishing email detected by the Exchange email system. The email was allowed and delivered to the user.

2. Source & Sender Analysis:

The email originated from an external sender (admin@netflix-payments.com) using IP address 112.85.42.180. The domain impersonates a legitimate Netflix service.

3. Email Content Analysis:

The subject “Netflix Deals!” uses brand impersonation and promotional language commonly associated with phishing attacks.

4. Scope & Impact Assessment:

The email was delivered to a single user with no evidence of wider distribution.

5. User Interaction Check:

The email was allowed, and potential user interaction cannot be ruled out.

6. Response & Closure:

The incident was confirmed as a true positive. User awareness and monitoring are recommended, and the alert is closed with potential exposure noted.

Alert 3

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

1. Alert Understanding:

The alert SOC101 – Phishing Mail Detected indicates a phishing email attempt detected by the Exchange email security system. The email was blocked automatically.

2. Source & Sender Analysis:

The email originated from an external sender (ndt@zol.co.zw) using IP address 146.56.209.252. The sender domain is suspicious and does not belong to UPS.

3. Email Content Analysis:

The subject “UPS Your Packages Status Has Changed” impersonates a shipping company and is a common phishing lure.

4. Scope & Impact Assessment:

The email targeted a single user only with no evidence of broader distribution.

5. User Interaction Check:

The email was blocked before delivery and no user interaction occurred.

6. Response & Closure:

The phishing attempt was contained successfully, classified as a true positive, and closed with no impact.

Alert 4

Low	Aug, 29, 2020, 11:05 PM	SOC101 - Phishing Mail Detected	8	Exchange
EventID :	8			
Event Time :	Aug, 29, 2020, 11:05 PM			
Rule :	SOC101 - Phishing Mail Detected			
Level :	Security Analyst			
SMTP Address :	63.35.133.186			
Source Address :	info@nexolberica.com			
Destination Address :	mark@letsdefend.io			
E-mail Subject :	UPS Express			
Device Action :	Allowed			

1. Alert Understanding:

The alert SOC101 – Phishing Mail Detected indicates a phishing email detected by the Exchange system. The email was allowed and delivered to the user.

2. Source & Sender Analysis:

The email originated from info@nexoiberica.com using IP address 63.35.133.186. The sender domain is not associated with UPS and is suspicious.

3. Email Content Analysis:

The subject “UPS Express” impersonates a legitimate shipping service and is commonly used in phishing campaigns.

4. Scope & Impact Assessment:

Based on the available logs, the phishing email targeted a single user only.

5. User Interaction Check:

The email was delivered to the user. No confirmed interaction is visible, but user exposure is possible.

6. Response & Mitigation:

The alert is classified as a true positive phishing attempt. User awareness is recommended, and the alert has been closed.