**Report 6: Phishing Email with Malicious Link**

**Title**: Phishing Email Attempt with Malicious Link  
**Date**: June 1, 2025  
**Platform**: TryHackMe SOC Level 1 Simulator  
**Severity**: High  
**Detection Tool**: Splunk  
**Category**: Phishing / Email Threats

**Steps Taken:**

**•** Reviewed the user report and noted the email details:

• Subject: Your Account Has Been Locked

• Recipient: jane.doe@tryhackme.local

• Searched Splunk for the email event using:

• index=mail\_logs "Your Account Has Been Locked"

• Found email from: support@microsoft-support365.com, which contained a link that seemed suspicious

• http://ms365login-auth[.]com/reset?email=jane.doe@thmsim.local

• Looked at the URL proxy logs to see if the link was clicked by the user, but it does not seem like the user clicked the link

• Scanned the domain in VirusTotal

• The domain was newly registered

• Flagged as phishing and malicious

**Final Assessment:**

**True Positive**. This was a phishing attempt containing a malicious URL designed to steal user credentials. The user did not click the link, and no compromise occurred.

**Mitigation:**

• Blocked the malicious domain (ms365login-auth.com) in the proxy and firewall

• Quarantined the email and scanned other inboxes for the same subject/sender

• Deny the malicious domain from the email filters