TryHackMe SOC Simulation — Lab Write-up

Author: Brice Dickey

This write-up documents the TryHackMe SOC Simulation lab activities: alert triage, phishing detection, log correlation, IOC extraction, and remediation planning. The Evidence section includes selected screenshots from the lab environment.

Key Findings

- Multiple phishing emails with suspicious URLs were identified.
- Firewall logs showed blocked or attempted outbound connections to suspicious domains/IPs.
- Several alerts were validated as true positives; some were false positives after analysis.
- A timeline of events was constructed correlating email receipt, firewall connections, and analyst actions.

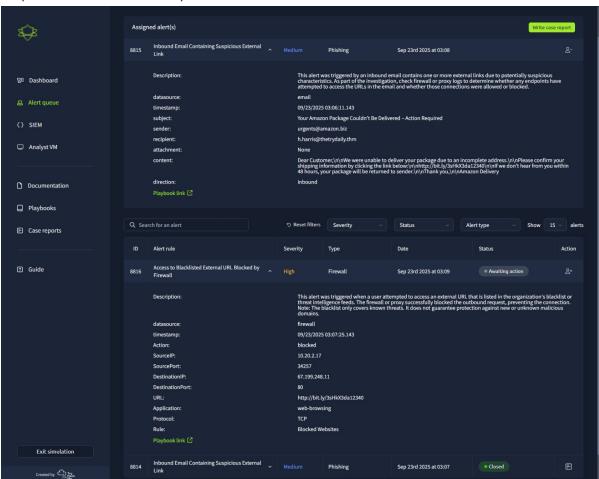
Techniques & Tools Used

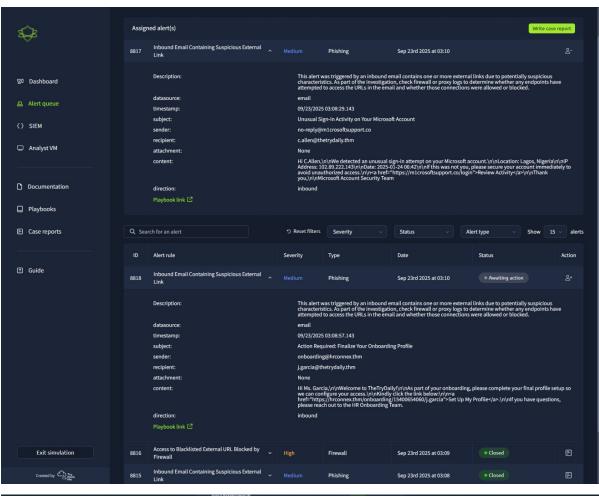
- SIEM dashboard for alert triage and search queries (Splunk/ELK style)
- Email header analysis and phishing URL lookup
- Firewall log correlation and IP/domain enrichment
- Python for quick CSV parsing and IOC extraction

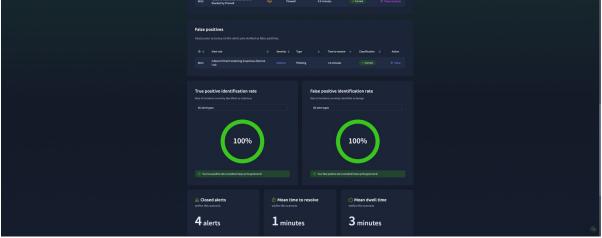
Example Detection Queries

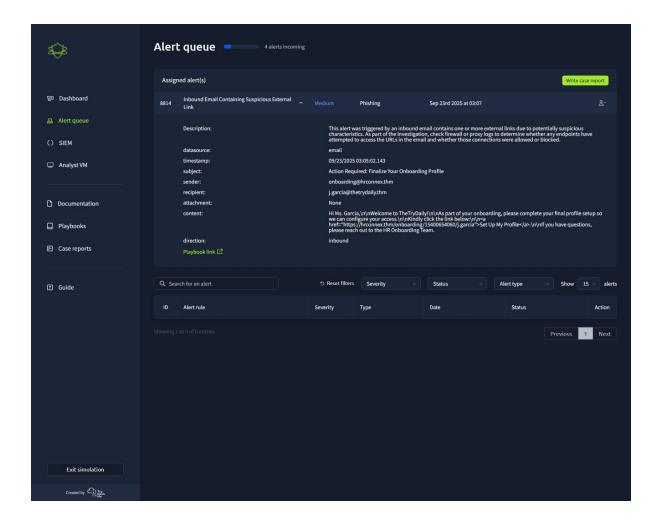
Splunk: index=firewall sourcetype=fw_logs dest_ip=1.2.3.4 OR dest_ip=5.6.7.8 | stats count by src_ip, dest_ip, _time **KQL:** DeviceEvents | where Timestamp >= ago(7d) and RemoteUrl contains "suspicious-domain.com"

Evidence (Selected Screenshots)









Remediation Recommendations

- Isolate affected hosts and perform forensic imaging.
- Block malicious IPs/domains at perimeter and email gateway.
- Reset credentials and enforce MFA for affected accounts.
- Tune SIEM rules with identified IOCs and update detections.
- Conduct user awareness training on phishing indicators.

Conclusion

The lab exercise reinforced SOC skills in alert triage, log correlation, and incident response. The included evidence supports the findings and recommended containment steps.