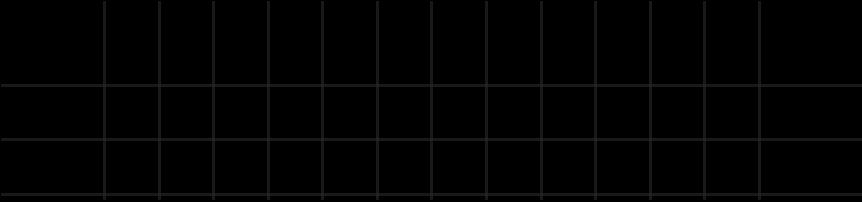


---



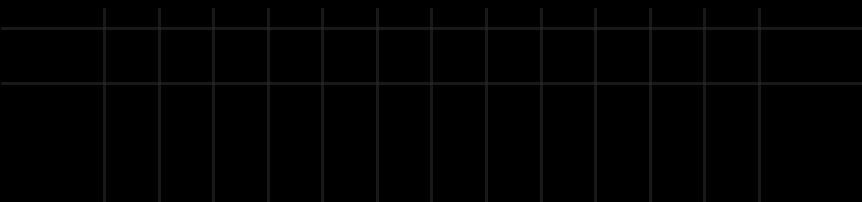
SECURITY ANALYST

---

# PROJECT

---

QUSAY AL-HEMIRY



---

# PORTFOLIO

---

# SOC 1 Log Analysis: Identifying Threats and Suspicious Events - TryHackMe:

- Analyzed a suspicious email and extracted key phishing indicators.
- Examined email headers to identify spoofed sender information.
- Investigated embedded links and attachments to determine malicious intent.
- Identified attacker infrastructure and validated the alert as a phishing attempt.

Tools:- Splunk - Firewall Logs - SIEM Platform

The screenshot shows a Splunk search results page. At the top, there is a search bar with the query "tx=\"main\" firewall SourceIP=\"10.20.2.17\"". Below the search bar, it says "6 hour window". The main area displays a table of log entries. The table has columns: Fields, Time, and Event. One event is shown in detail:

Fields	Time	Event
1 type 1	12/6/25 11:58:56.761 AM	<pre>( [-]   Action: blocked   Application: web-browsing   DestinationIP: 67.199.248.11   DestinationPort: 80   Protocol: TCP   Rule: Blocked Websites   SourceIP: 10.20.2.17   SourcePort: 34257   URL: http://bit.ly/3shKX3da12340   datasource: firewall   timestamp: 12/06/2025 11:58:56.761 )</pre>
2		<a href="#">Show as raw text</a>
3		host = 10.10.45.82:8989   source = eventcollector   sourcetype = _json
4	12/6/25 11:56:34.761 AM	<pre>( [-]   Action: allowed   Application: web-browsing   DestinationIP: 10.20.2.17 )</pre>

PICTURE FROM SPLUNK

A device within the network attempted to access a blocked website using a shortened URL (bit.ly). The firewall detected and blocked the request based on the rule "Blocked Websites". The destination used HTTP over port 80, which is unencrypted and risky. The URL might lead to phishing or malicious content.

The screenshot shows the VM SIEM interface. On the left, there's a sidebar with icons for Dashboard, Alert queue, SIEM, Analyst VM, Documentation, Playbooks, and Case reports. The main area is titled 'Incident classification' and shows two radio button options: 'True positive' (selected) and 'False positive'. Below this is a 'Case report' section with a text input field for detailing the steps taken to analyse and contain the incident. A large text box contains a detailed log entry about a web browsing attempt being blocked by a firewall rule. At the bottom, there's a question 'Does this alert require escalation?' with 'Yes' (selected) and 'No' radio buttons.

PICTURE FROM VM SIEM

At the specified timestamp, the firewall detected and blocked a web browsing attempt from internal host (10.20.2.17) to an external IP over HTTP using a shortened URL. The destination was classified under a "Blocked Websites" rule. This type of activity is suspicious as shortened links are often used to hide malicious or phishing URLs. Due to the nature of the access and the enforcement of blocking by firewall, this alert is considered a True Positive