SECURITY ANALYST

PROJECT

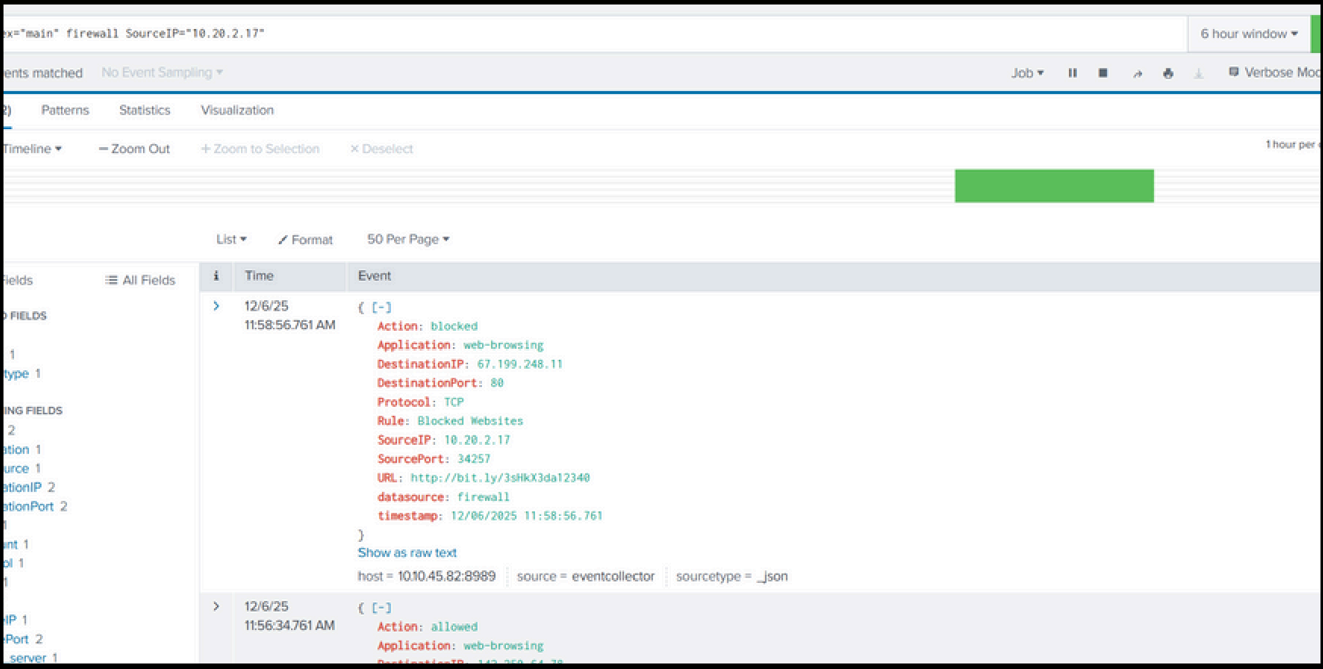
QUSAY AL-HEMIRY

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



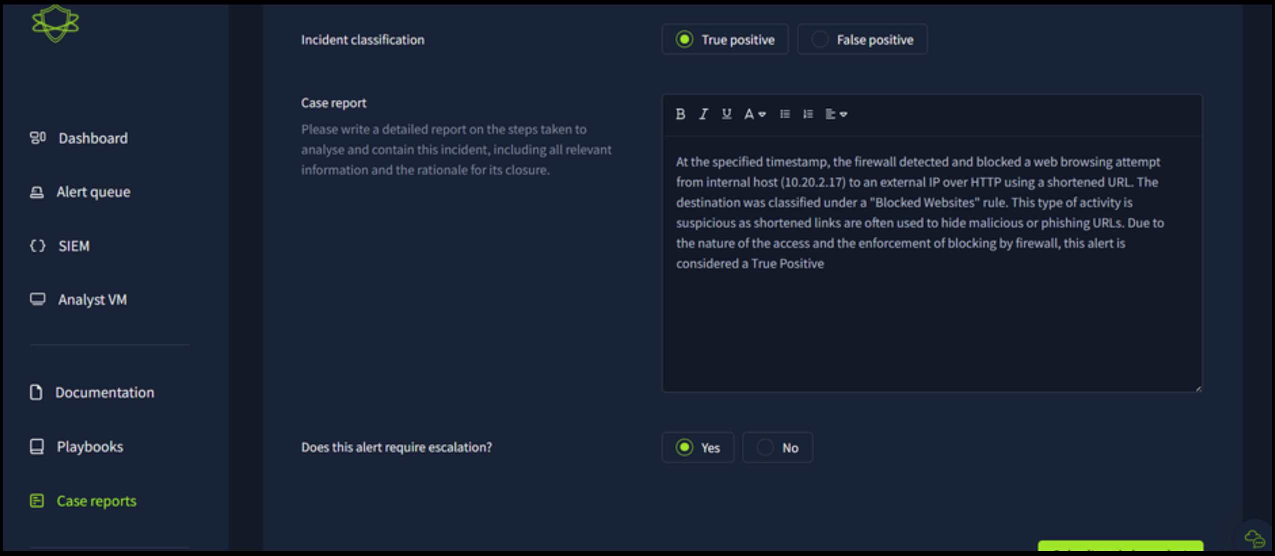
```
ex="main" firewall SourceIP="10.20.2.17"
```

```
12/6/25
11:58:56.761 AM
{ [-]
   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
}
Show as raw text
host = 10.10.45.82:8989   source = eventcollector   sourcetype = _json

12/6/25
11:56:34.761 AM
{ [-]
   Action: allowed
   Application: web-browsing
```

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.



Incident classification: ● True positive ○ False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

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

Does this alert require escalation? ● Yes ○ No

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