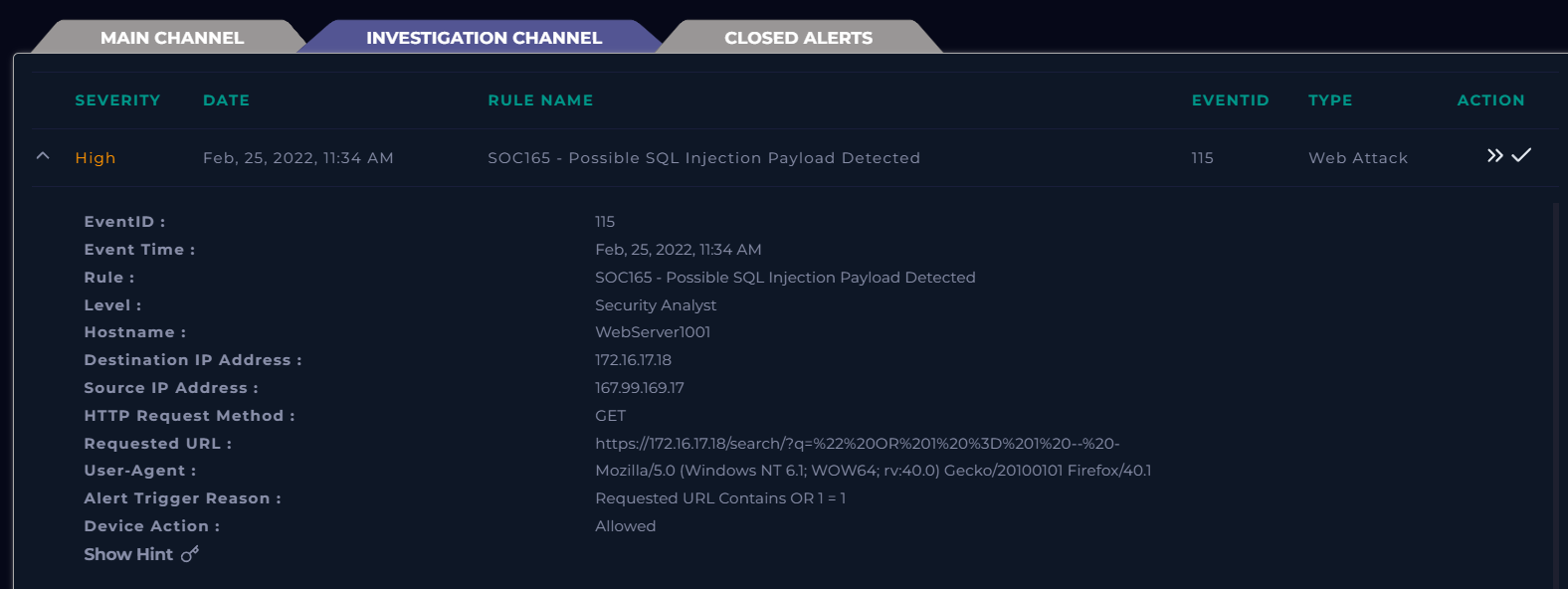
For this example alert,I will be investigating and creating a case on LetsDefend’s alert “SOC165 - Possible SQL Injection Payload Detected”.



First, it is important to gather information received from the alert.

The event occurred at 11:34 AM on Febuary 25, 2022.

The threat IP is 167.99.169.17

The target is one of our web servers (WebServer1001) IP 172.16.17.18.

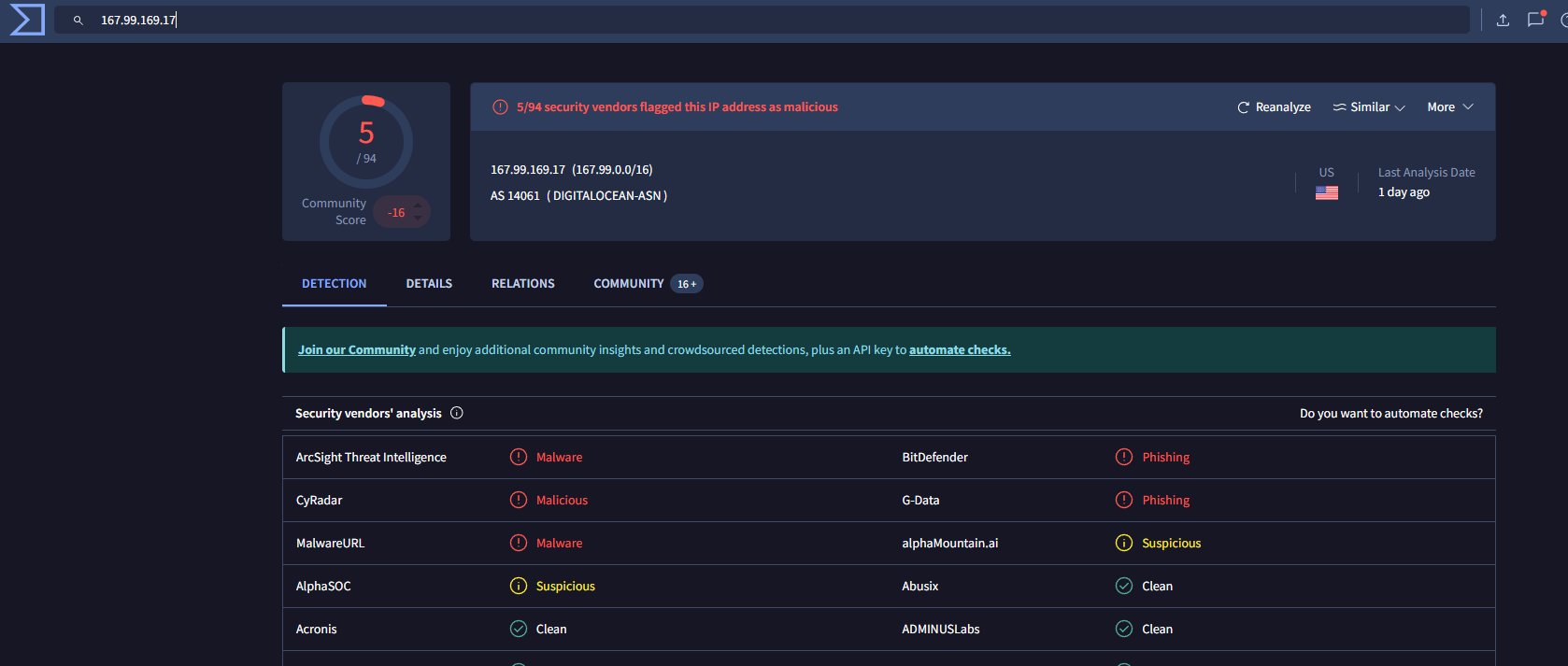
User agent was Mozilla Windows, using Firefox.

From the Rule Name, I can see that the suspected attack method is a SQL injection payload. Beginning by decoding the Requested URL in an online UTF-8 decoder I get the following result.

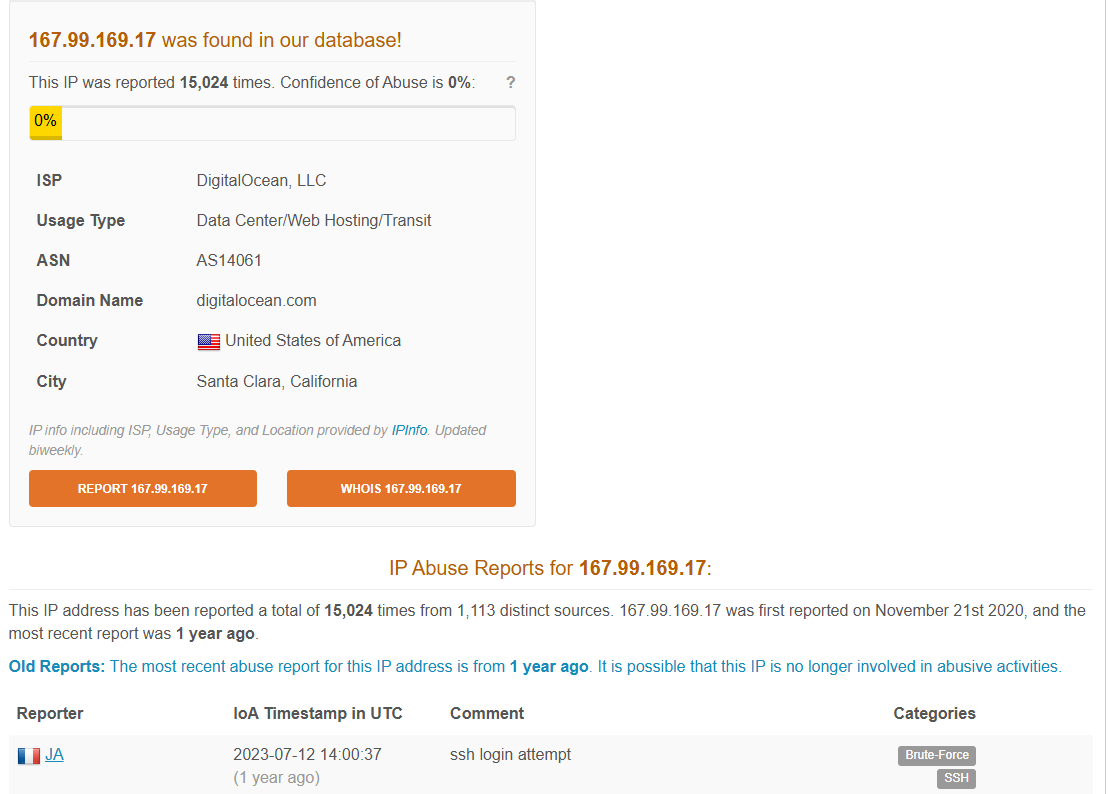
(https://172.16.17.18/search/?q=" OR 1 = 1 -- -).

Within this command some common SQL commands like OR.

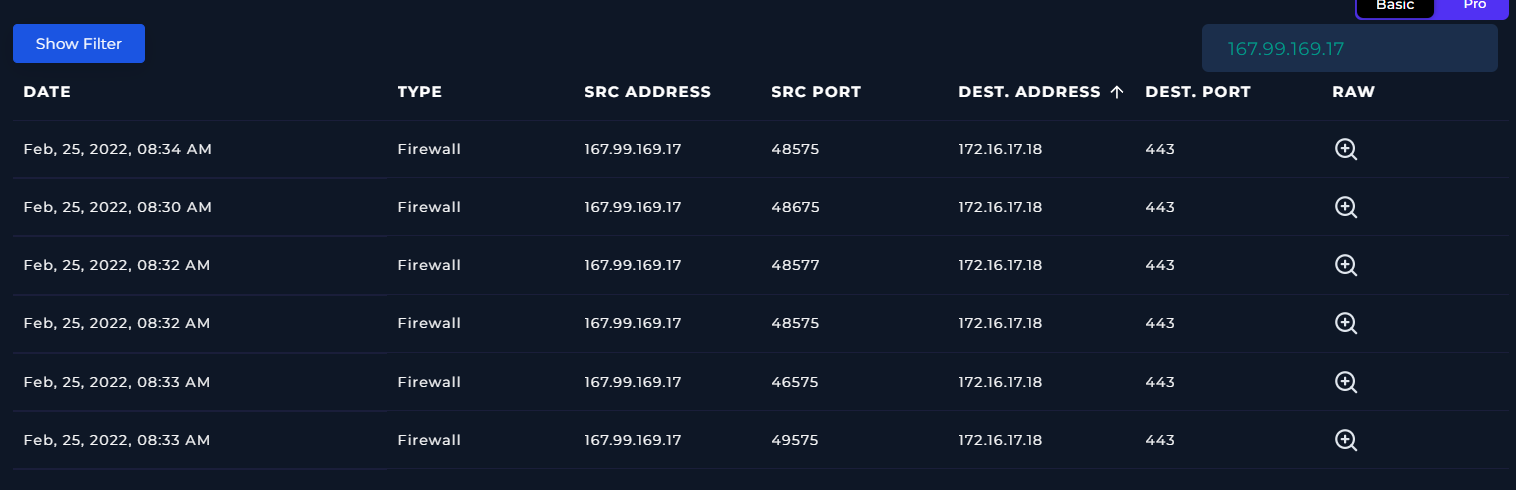
Analyzing the IP address of the attacker 167.99.169.17 in VirusTotal, I find that their were several malicious flags.



Using other scanners such as abuseipdb shows that the IP has been repeatedly reported for IP address abuse.

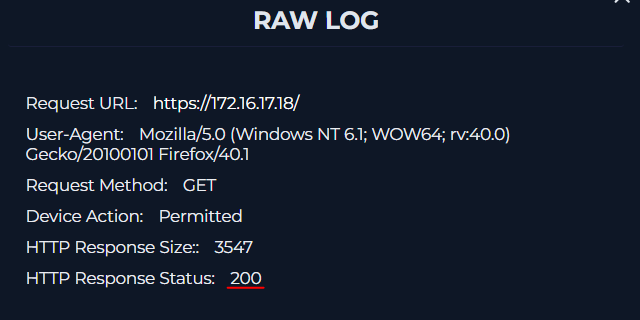


We can safely say that this traffic is Malicious, but what is the attack vector? To determine the attack vector, we need to look into the network logs. Sorting these logs by the attacker’s IP gave six related events.

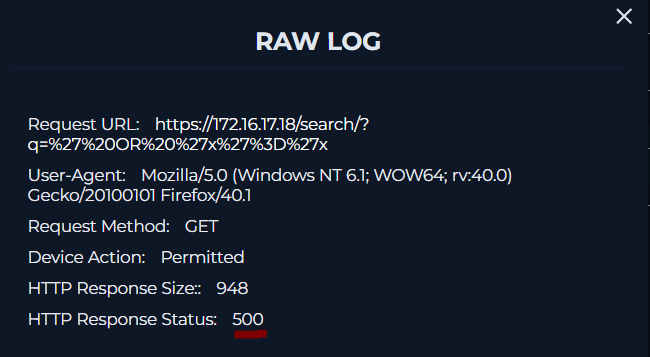


Looking into the logs raw data, the attacker sent multiple requests to the server. Out of these six attempts five were successful as seen from the HTTP Response Status: 500 (server error), and one was successful as seen from HTTP Response Status: 200 (success code).

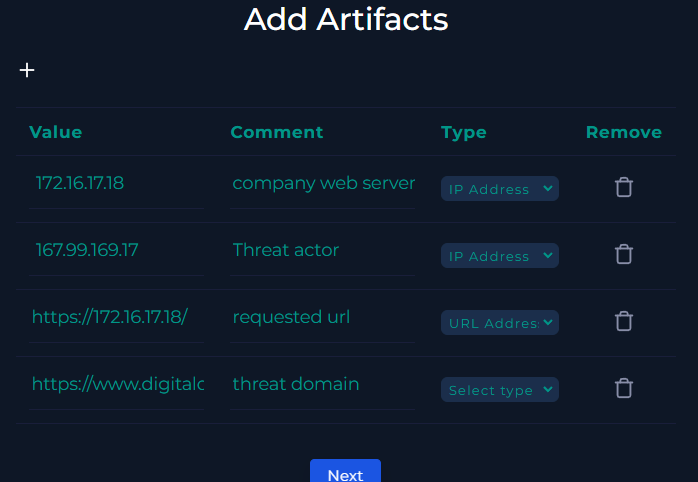
Example of successful request (Feb, 25, 2022, 08:30 AM):



Example of unsuccessful request (Feb, 25, 2022, 08:33 AM):



In this case, their is no other traffic involving our threat actor, and their wasno indication that this was a planned security test.



Analyst note:  
Feb, 25, 2022, 11:34 AM we received an SOC alert of a requested URL to our WebServer1001 endpoint (172.16.17.18). This request was "https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-" and was allowed. The URL when decoded contains "OR 1=1" which allows this request to go through.

Investigation of the source IP found that it was reported malicious, and linked to a domain called digitalocean.com.

The endpoint showed no communication with any outside command and control points via the network logs. The logs show that the attacker was unsuccessful after receiving multiple HTTP replies of 500.

