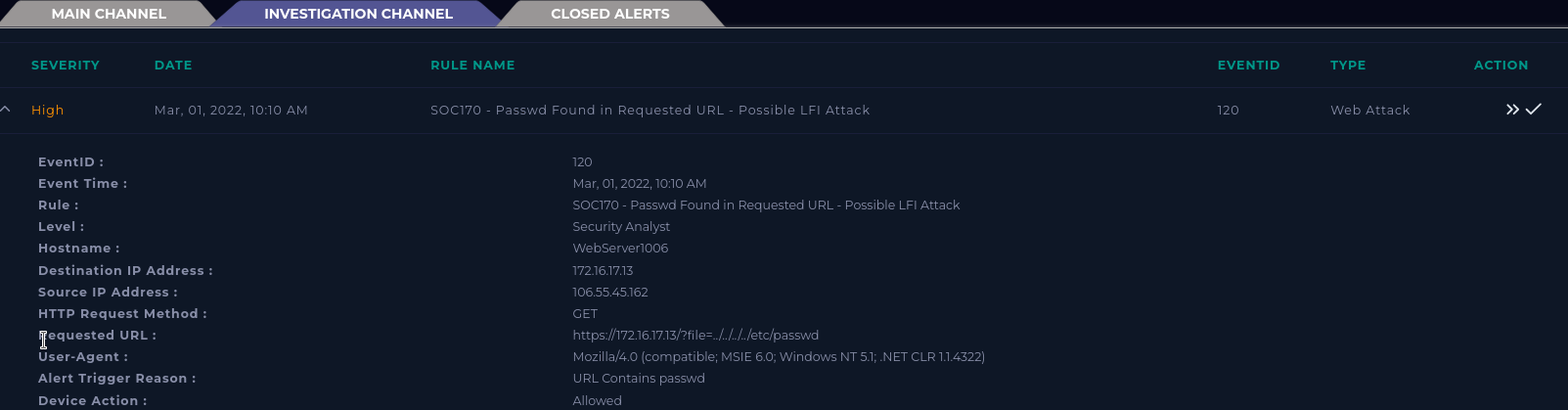
I will be creating a case on LetsDefend ‘SOC170 - Passwd Found in Requested URL - Possible LFI Attack’.



Summarizing the alert

When did the event occur?

Mar, 01, 2022, 10:10 AM

What is the destination IP?

172.16.17.13

What is the source IP?

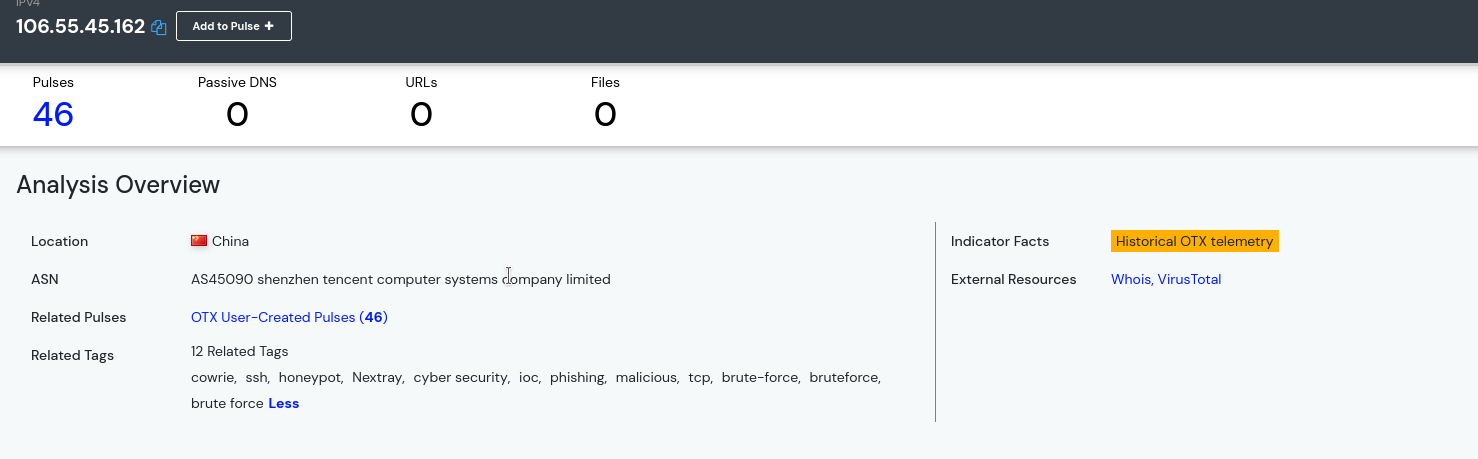
106.55.45.162

Why did the alert occur?

The requested URL (https://172.16.17.13/?file=../../../../etc/passwd) contained passwd.

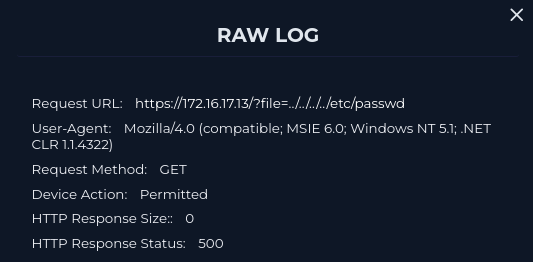
Collecting data

According to VirusTotal, source IP 106.55.45.162 has a negative community score and originates from China Beijing. AlieanVault warns that this IP has been reported as malicious.



The destination IP 172.16.17.13 matches WebServer1006, who’s last login was Feb, 19, 2022, 01:01 PM. This means that the traffic came from the internet to the network.

Searching the logs for a matching source address finds one result matching the alert.



Fortunately, the malicious attack failed. HTTP Response Status 500 shows an error and the response size is empty. This means that the attack does not need to be escalated and the system does not need to be contained.