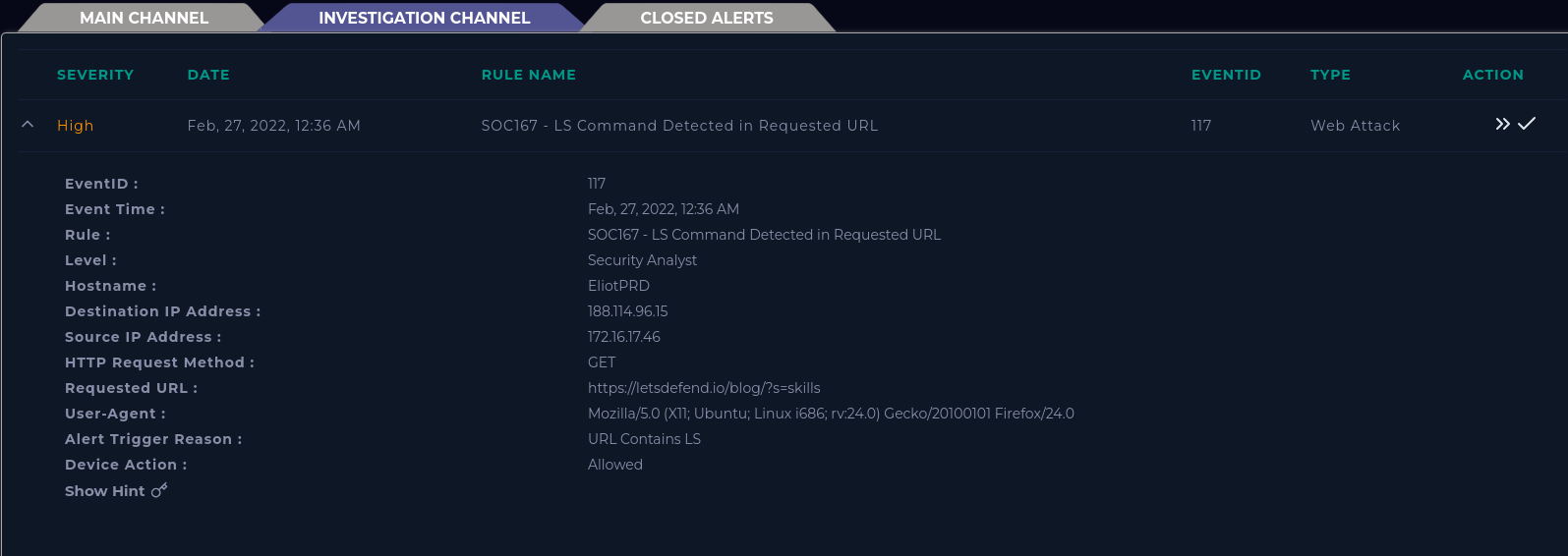
I’m going to create a case for LetsDefend alert “SOC167 - LS Command Detected in Requested URL”.



First, it is important to summarize the information from the alert.

When did it happen?

The attack occurred at 12:36 AM on February 27, 2022.

What is the source IP?

172.16.17.46

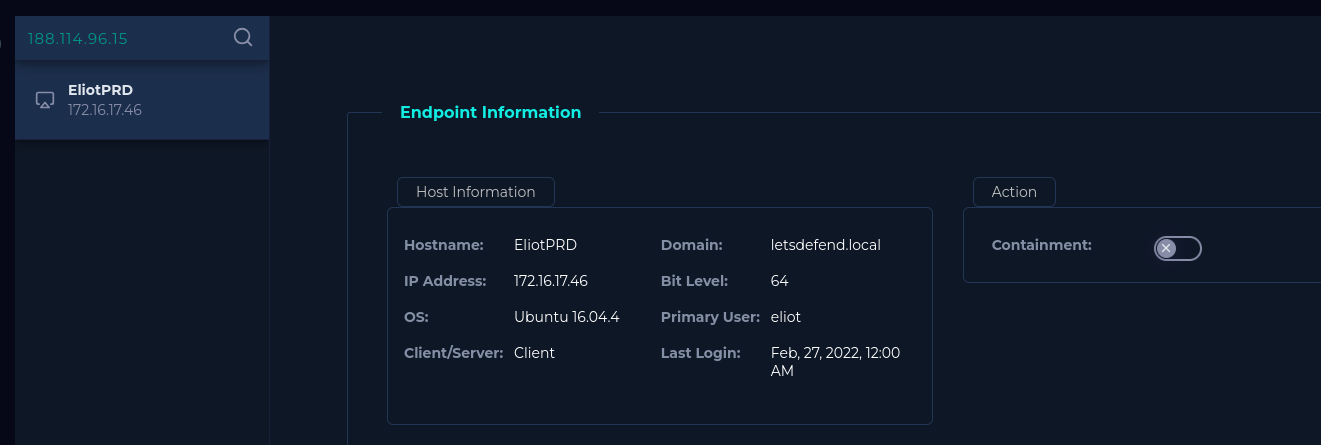
What was the Destination IP?

188.114.96.15.

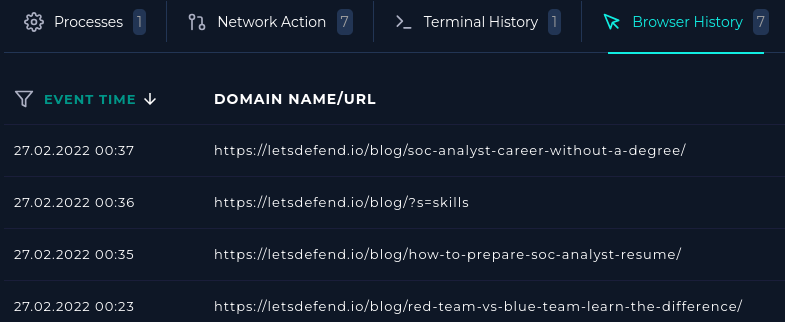
What caused the alert?

The URL contained an LS command commonly used for listing files.

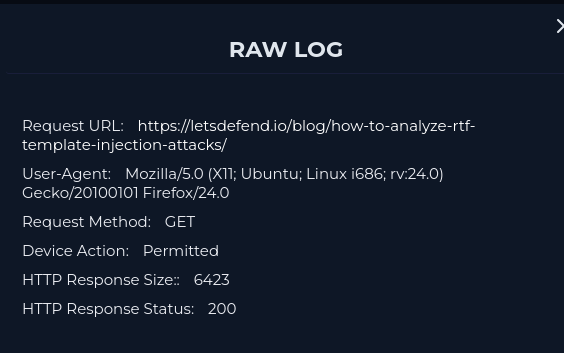
To begin the investigation, I checked the IPs to see which matched with EliotPRD. Using the Endpoint Security I found that the source IP belongs to EliotPRD. Checking the Network actions I find that Eliot has connected to the Destination IP at the exact time stated in the alert.



There was no suspicious activity discovered within the Processes, Terminal, or Browser History. Within the browser history, we also see what websites were visited during the alert, including a matching Requested URL.



From the history the user seems to have just been researching the website letsdefend. Within the log management tool, the raw data shows evidence of this. There are different requests/traffic as the user explores letsdefend pages.



In conclusion this alert was a false positive. The user was browsing LetsDefend.The alert may have been triggered by the ls in skil**ls**.