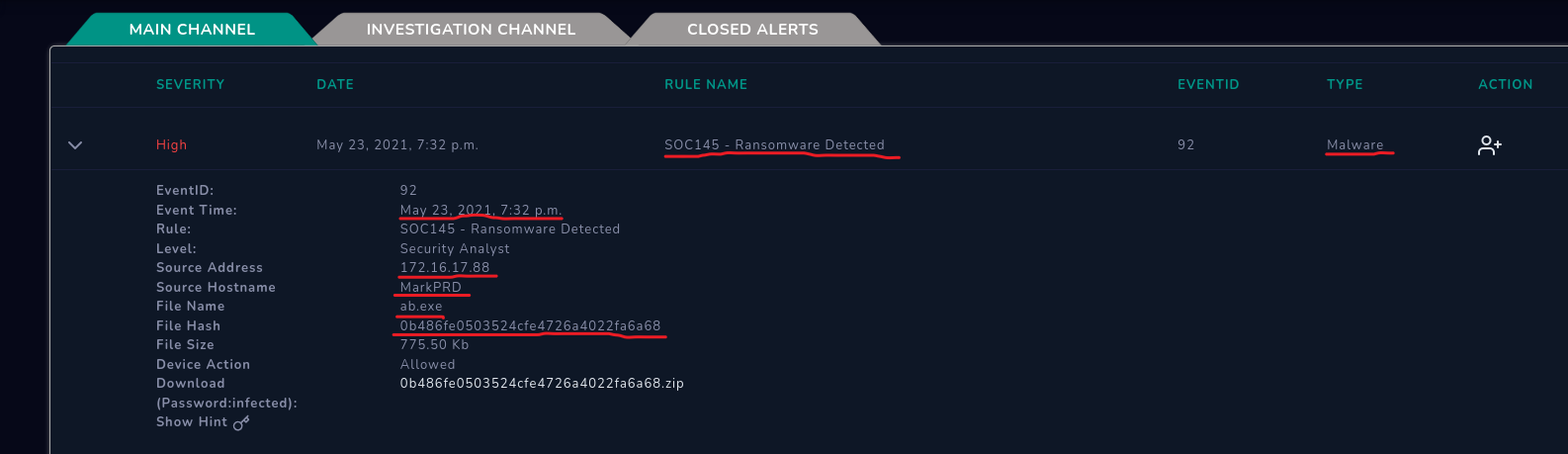
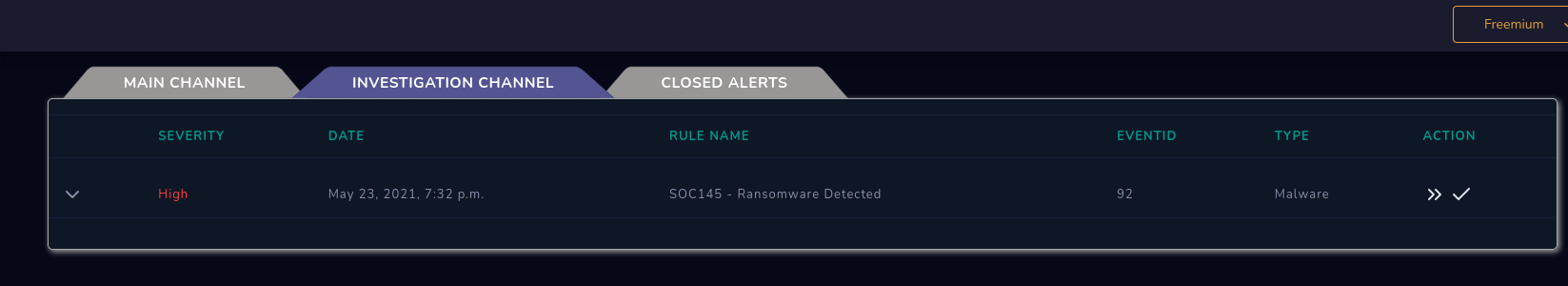
**INCIDENT RESPONSE PROJECT**

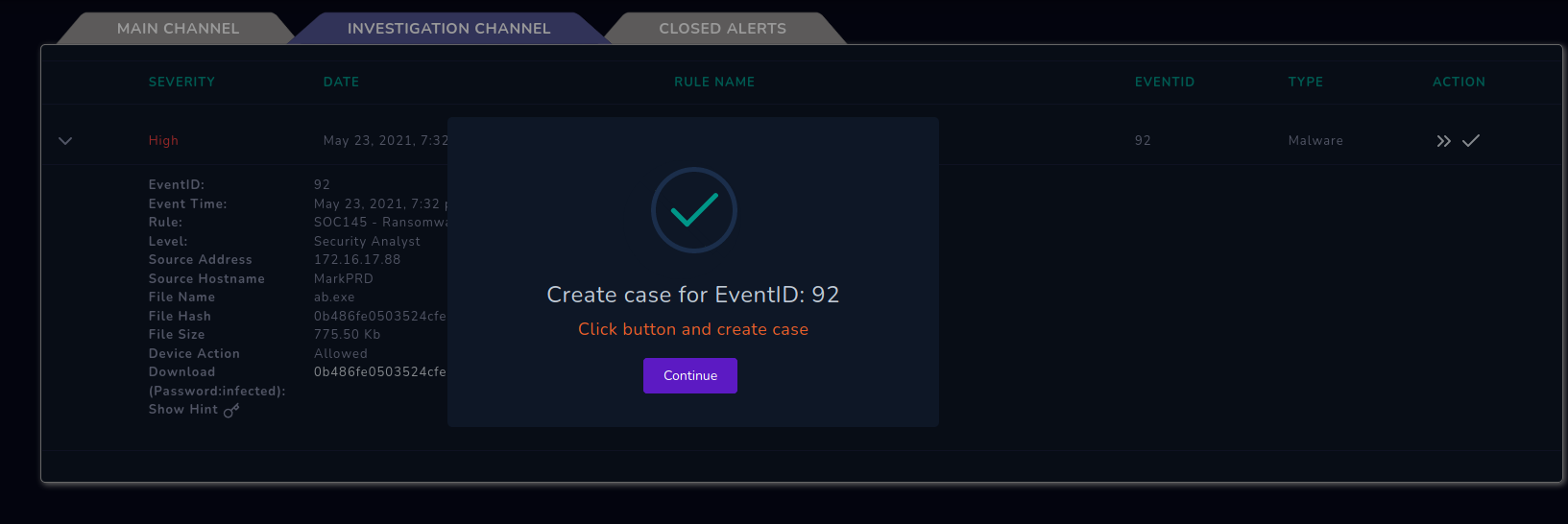
I have created a free account on

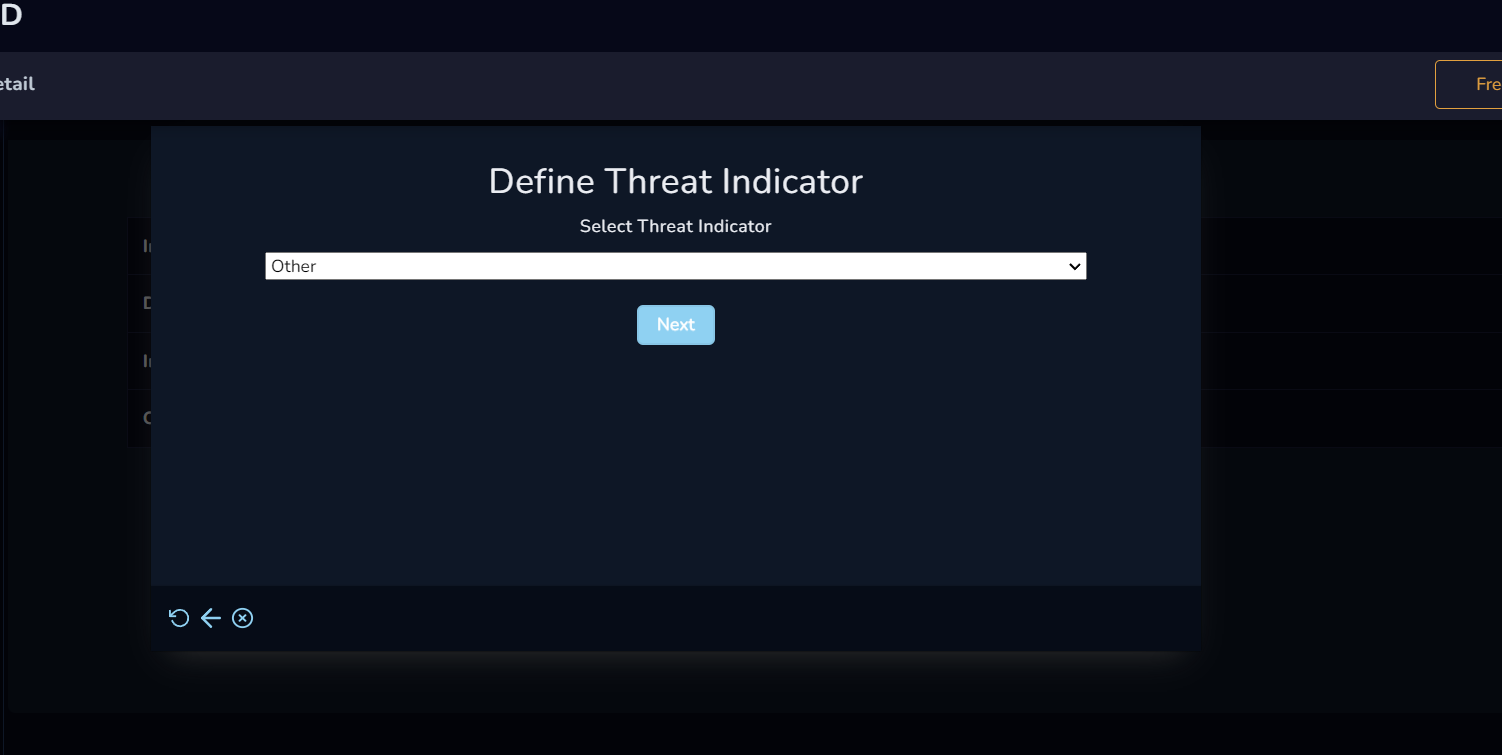
**<https://letsdefend.io>**

1.The first alert I have picked is **SOC145 - Ransomware Detected.**

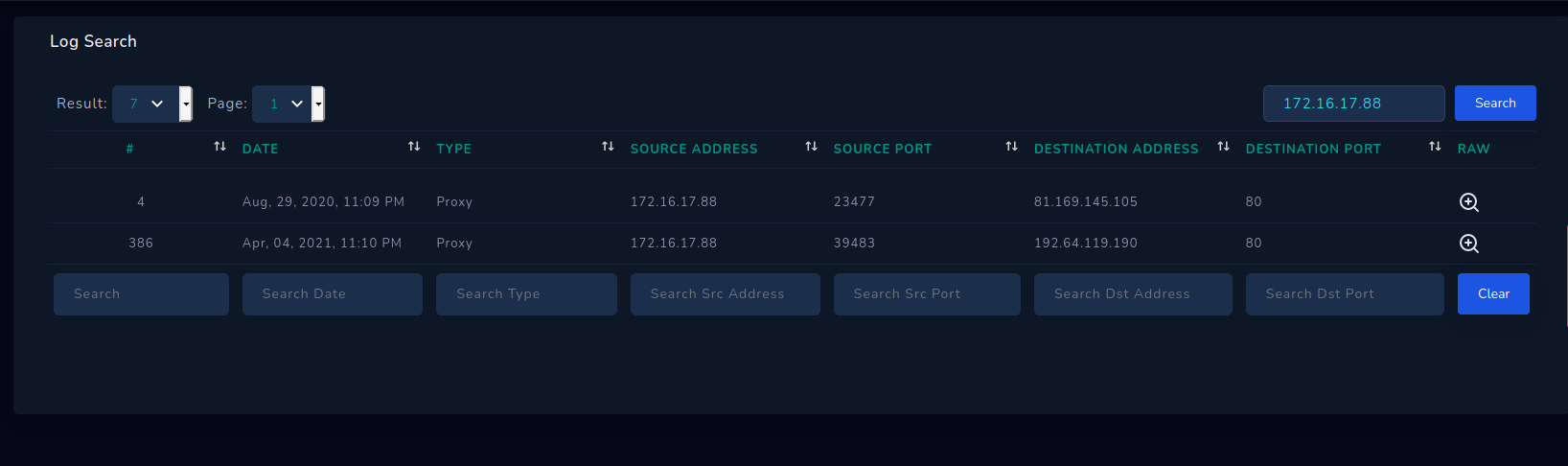
****

The highlights show that this is a high severity incident and the type of the file detected is Malware. The highlights also show the date and time of the file created, source address, source Host name, File name, hash of the file and file size.

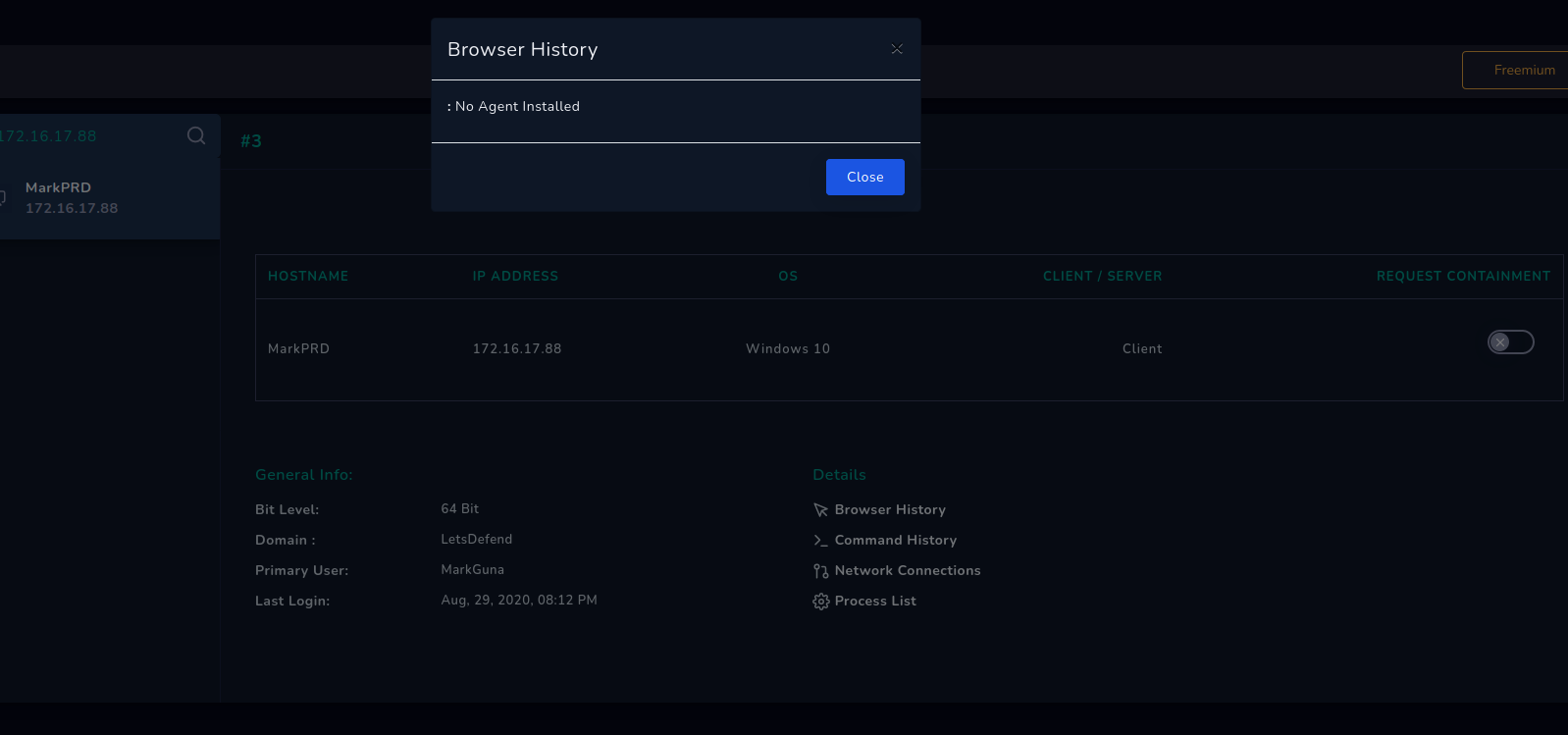
I have Took the ownership of that alert and started creating case. Which created a case.

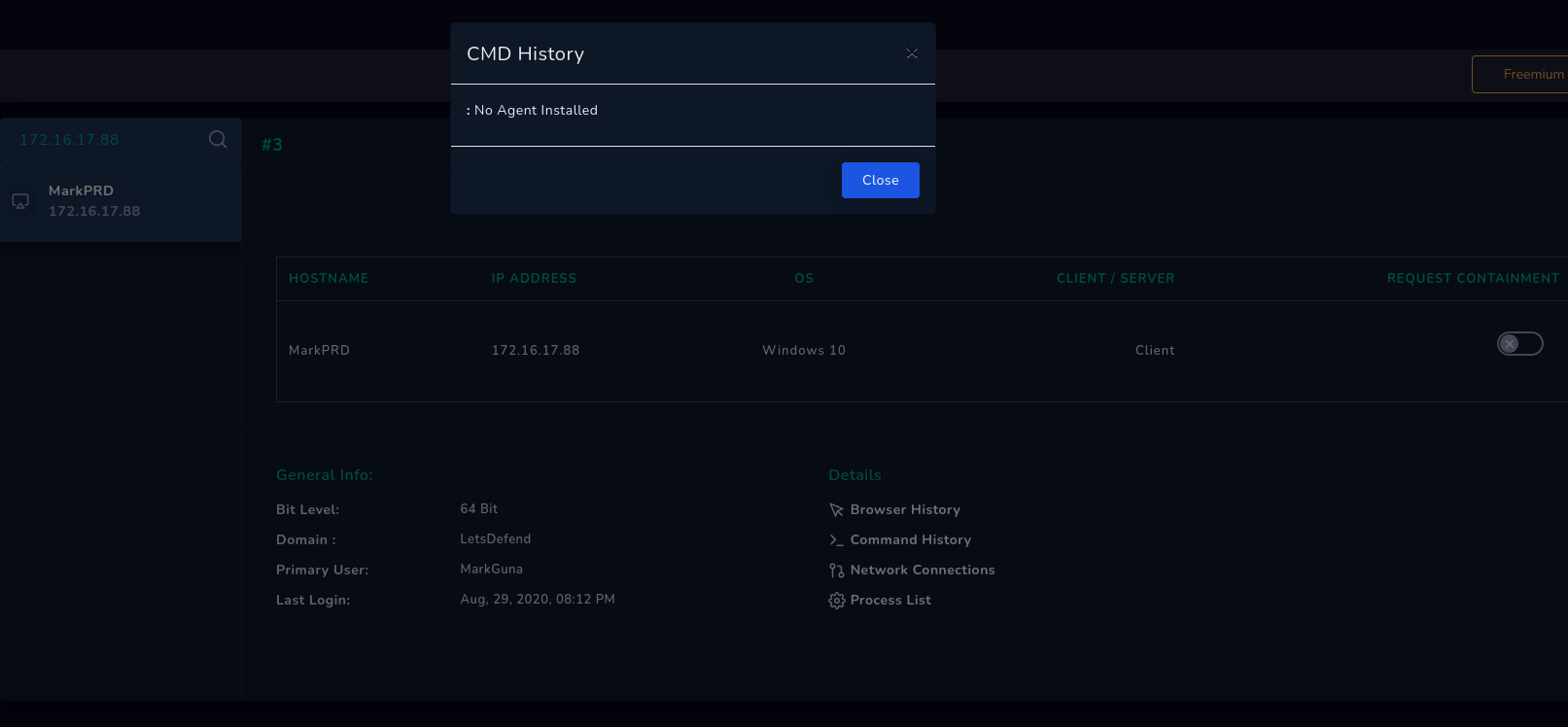
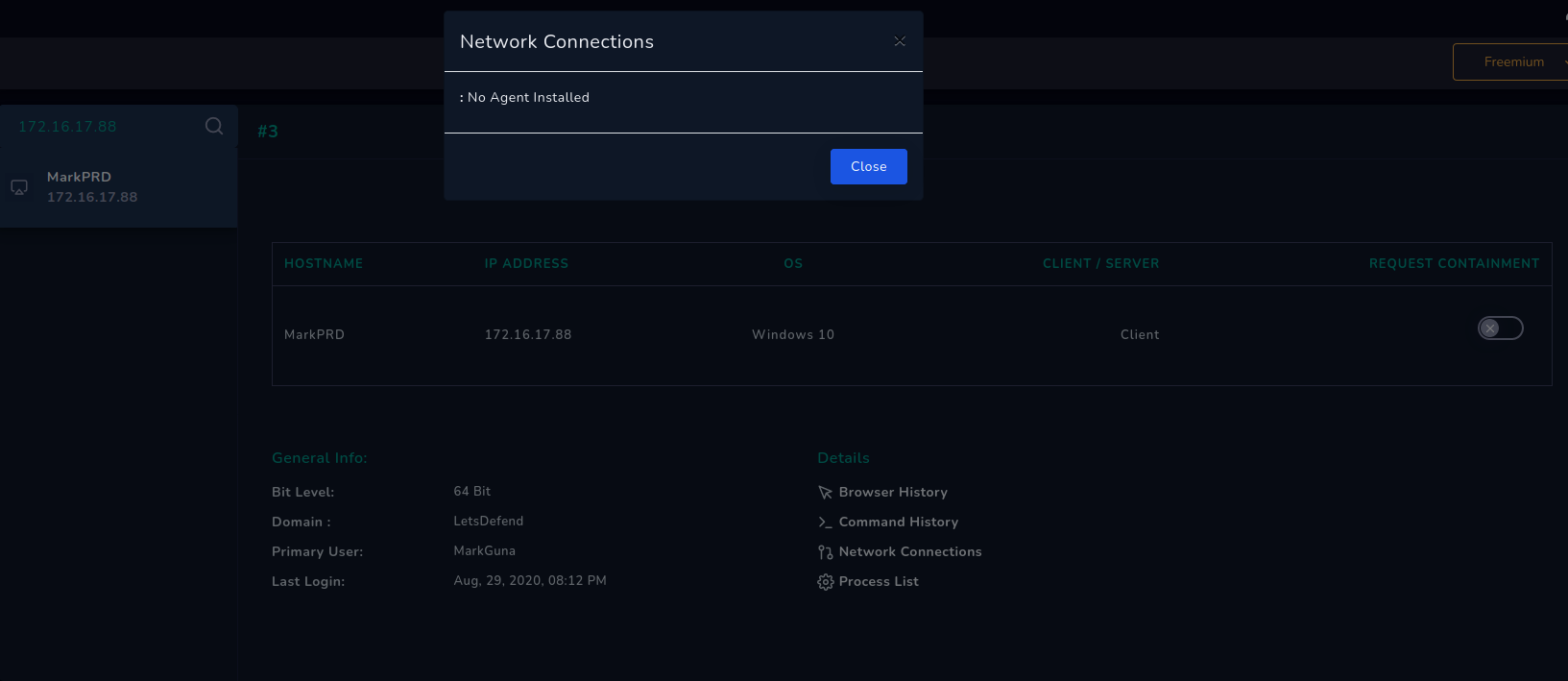


It asked me to define threat indicator, which I have set to others in the given options by checking source address in the Log management and Endpoint security.



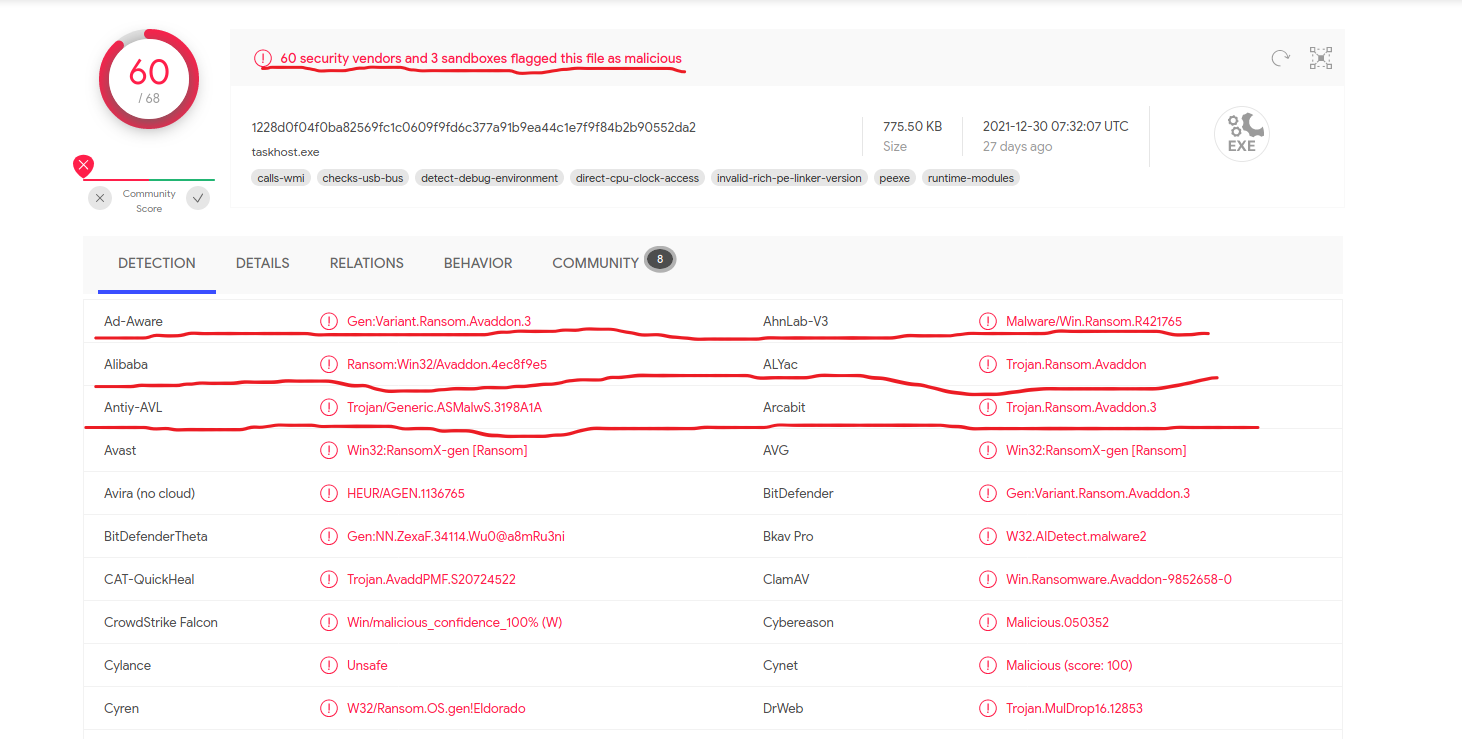
There were no logs shown on the date which the malware got created.



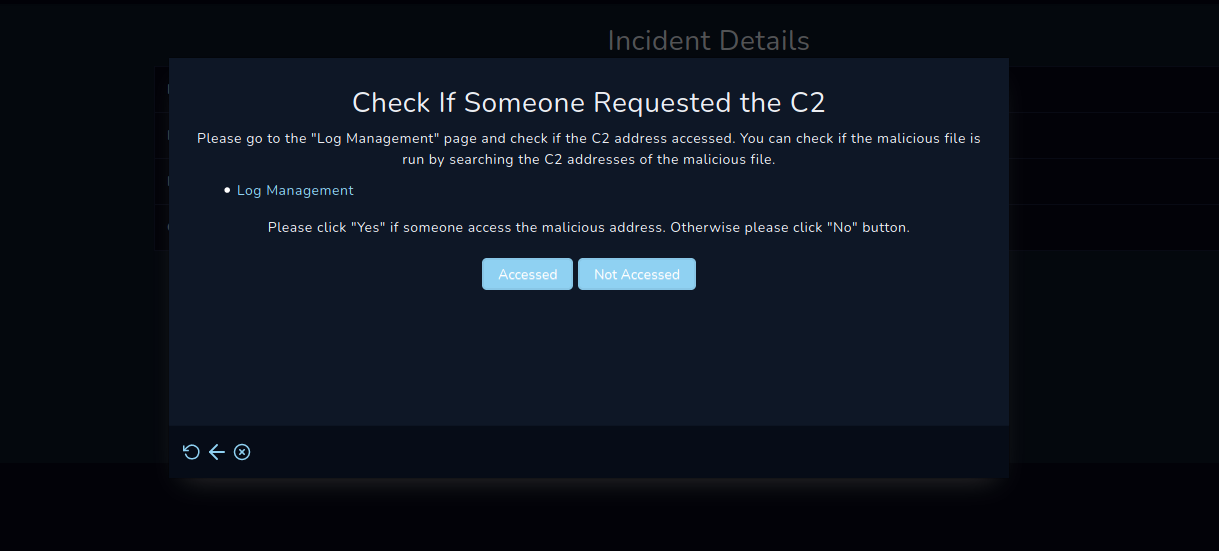


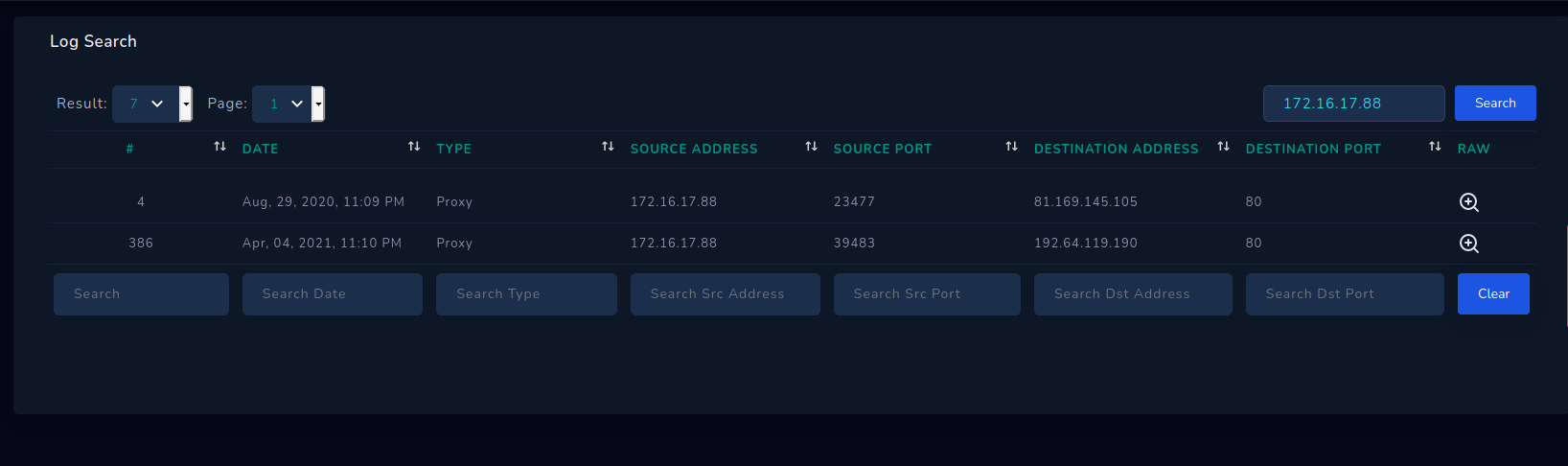
In the endpoint security there was no Browser history, Network connections, CMD History. Maybe the commands and browser history has been removed.

Then it asked me to analyze the file in the open tools like virustotal.com

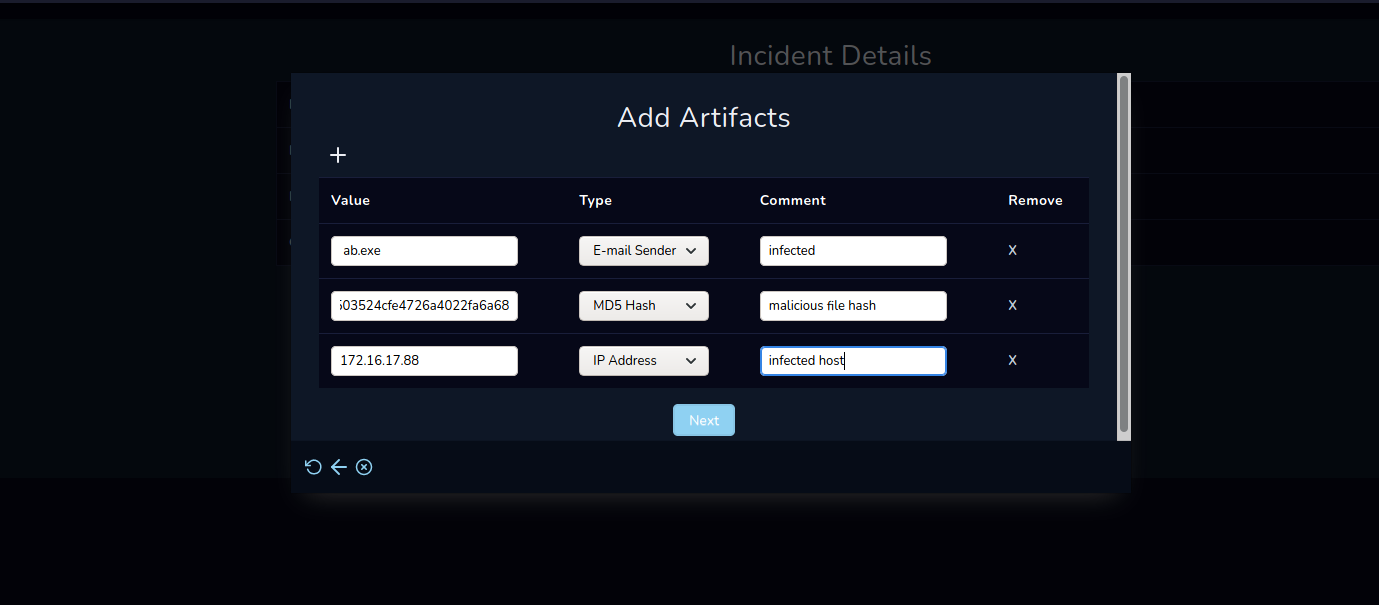


The highlights show that 60 security vendors and 3 sandboxes flagged this file as malicious.

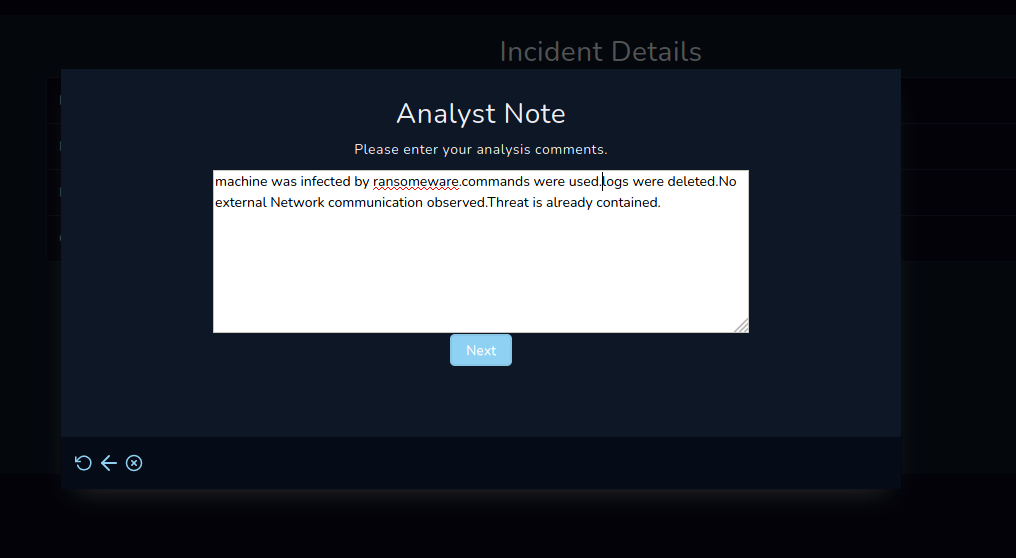


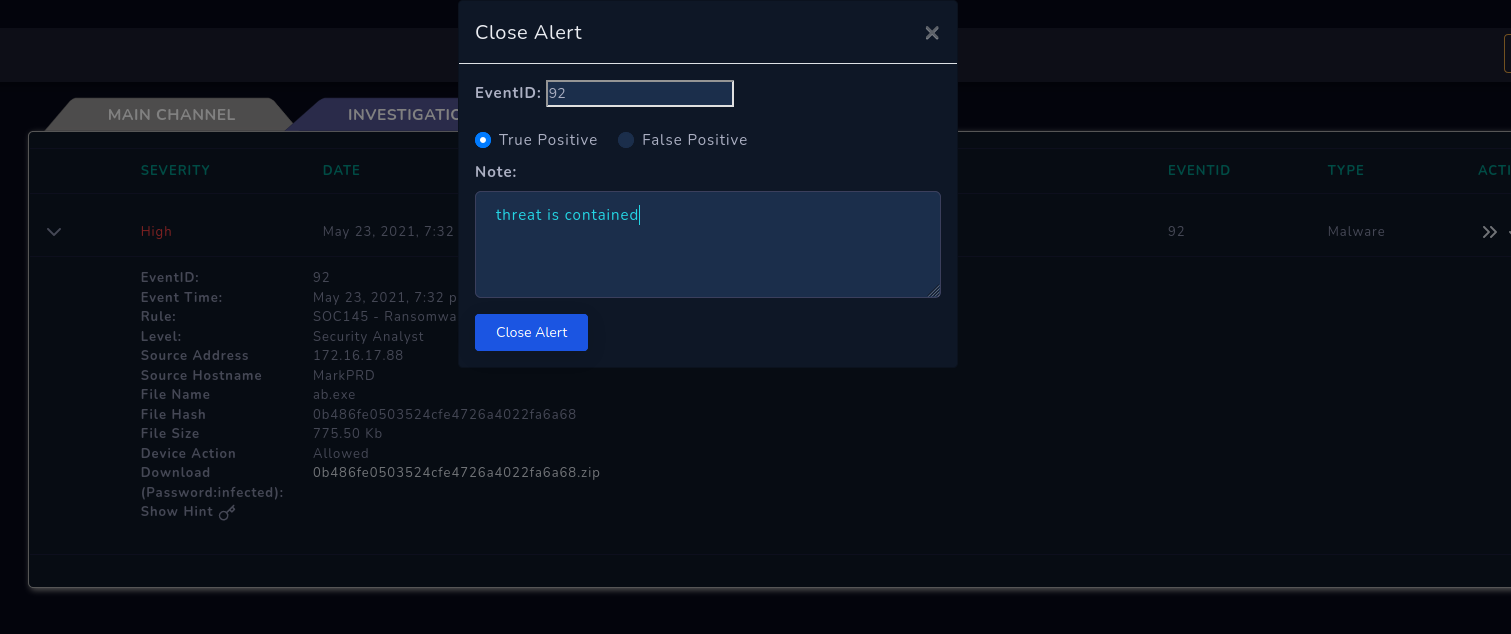
It asked me to check if someone requested the command and controls.

I have checked the source address in the log management, there were no C2 addresses accessed.



Then I added the artifacts as shown above.





I have added the Analyst note. And set the alert to true positive by analyzing from all the above steps.

