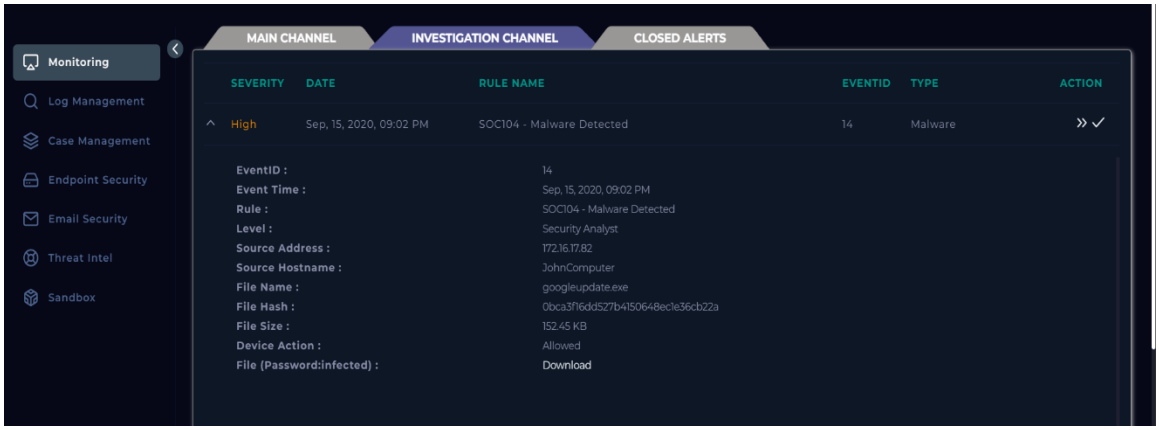
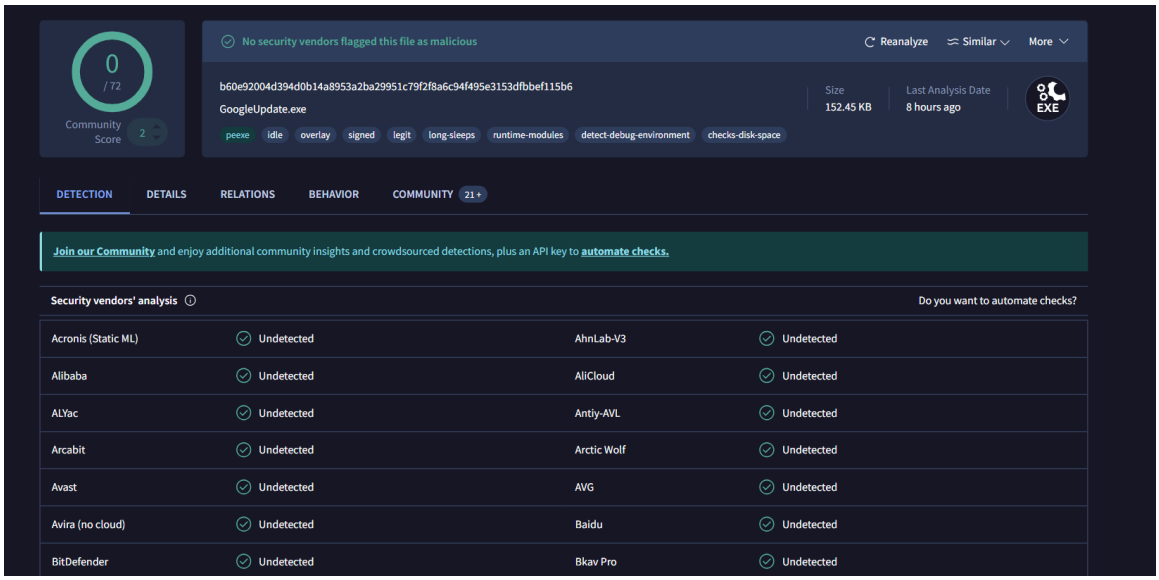
SOC104 - Malware Detected [Let's Defend – Write-up]

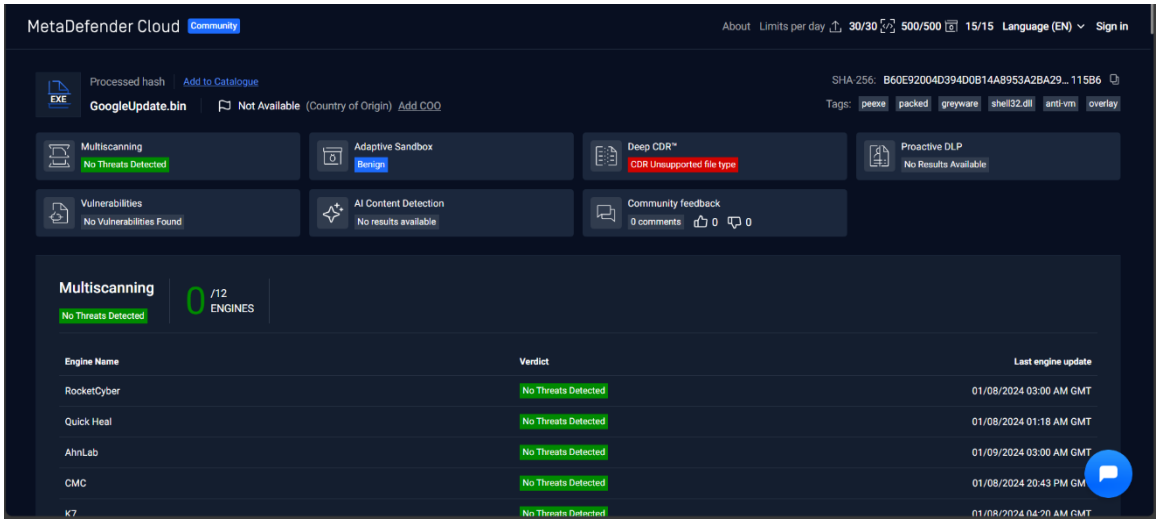
| Start Investigation



The layer contains extensive information, including the IP address, filename, and hash; therefore, my first step was to verify the hash.

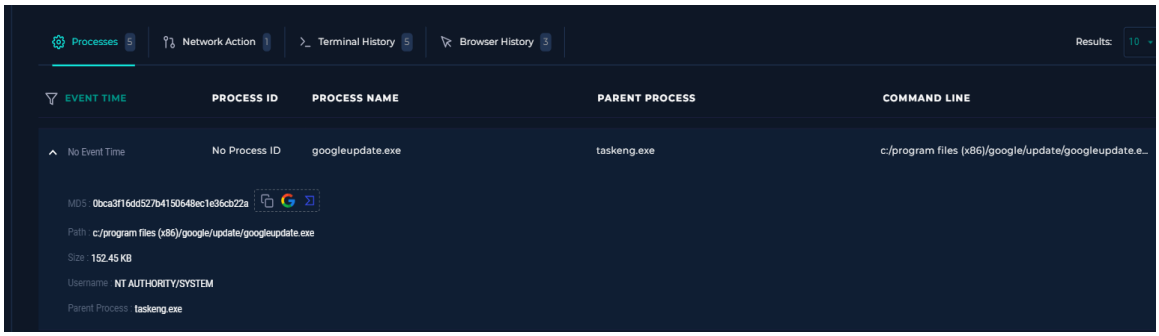


The analysis of the file 'GoogleUpdate.exe' on VirusTotal reveals a clean security profile, with a detection rate of 0/72. All major security vendors have flagged the file as undetected, suggesting it is legitimate and free from known malicious code at this time.

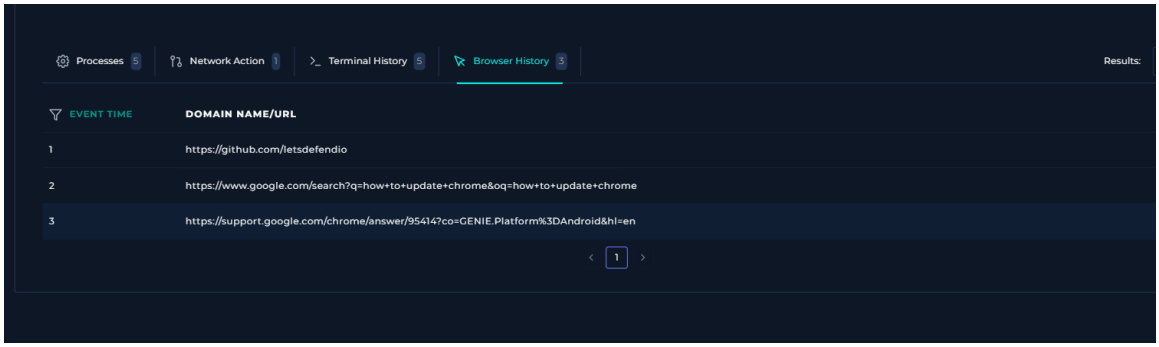


The cross-platform analysis of the file hash on both VirusTotal and MetaDefender Cloud confirms consistent clean status. On VirusTotal, the file yielded a 0/72 detection rate, while MetaDefender reported 0/12, with the 'Adaptive Sandbox' classifying its behavior as benign. These results collectively indicate that the file is legitimate and free from known malicious signatures across multiple security engines.

After confirming the file hash was clean, I conducted further research within the Log Management system. By searching for the IP address 172.16.17.82, I was able to track the network activity associated with this file to ensure no suspicious connections were established.



Endpoint monitoring shows the process 'googleupdate.exe' running under the 'NT AUTHORITY/SYSTEM' account. It was initiated by 'taskeng.exe' and is located in the standard Google update directory, with an MD5 hash of '0bca3f16...'.

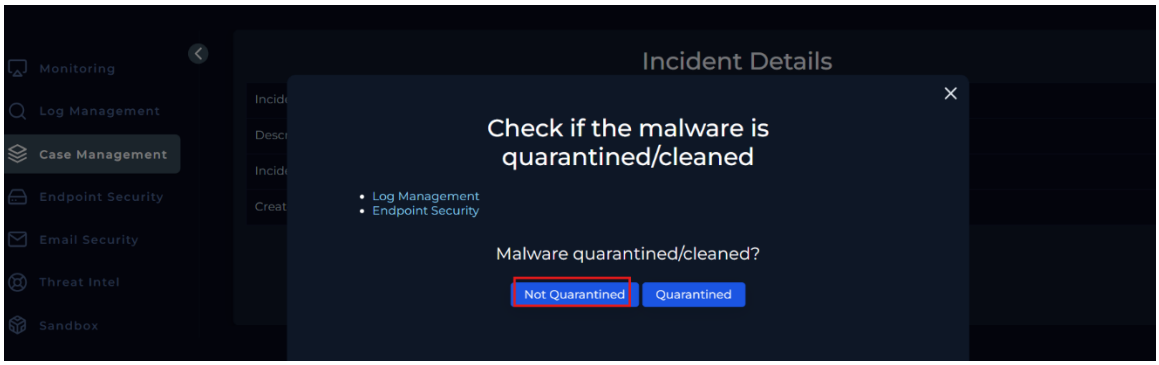


The browser history for the endpoint shows recent activity related to system updates, including searches on how to update Chrome and visits to official Google support pages. Additionally, a visit to a GitHub repository for 'letsdefendio' was recorded.

| Use Playbook

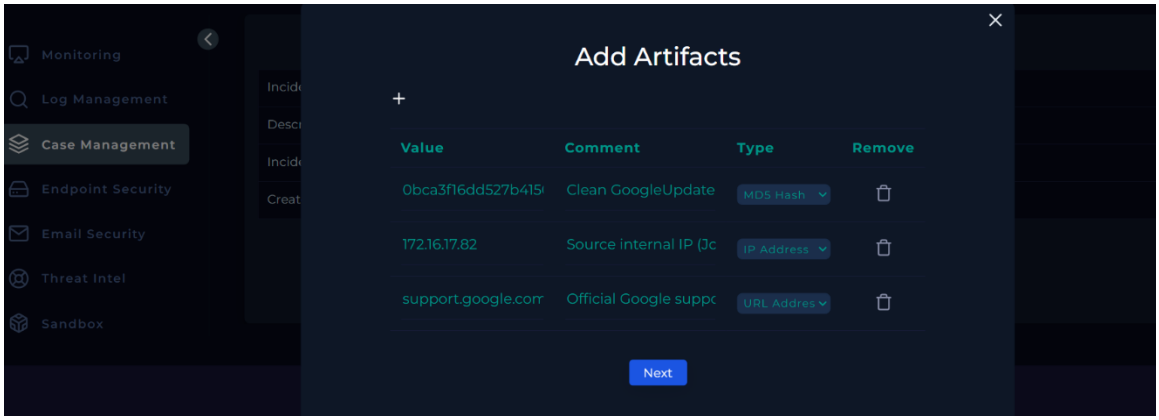
Define Threat Indicator

Answer: other.



Based on the investigation, the file was confirmed as a legitimate utility, and the device action was set to 'Allowed'. The file remains 'Not Quarantined' because no malicious activity was detected.

Based on the investigation the activity was identified as non-malicious.



The investigation concludes that this alert is a **True Positive**.

Summary

The systematic analysis of the file hash, network logs, and browser history provided a clear picture that the activity was legitimate. By correlating the user's search for Chrome updates with the execution of the verified 'googleupdate.exe', I was able to confirm the intent and rule out any malicious behavior, leading to an accurate classification of the alert as non-malicious.