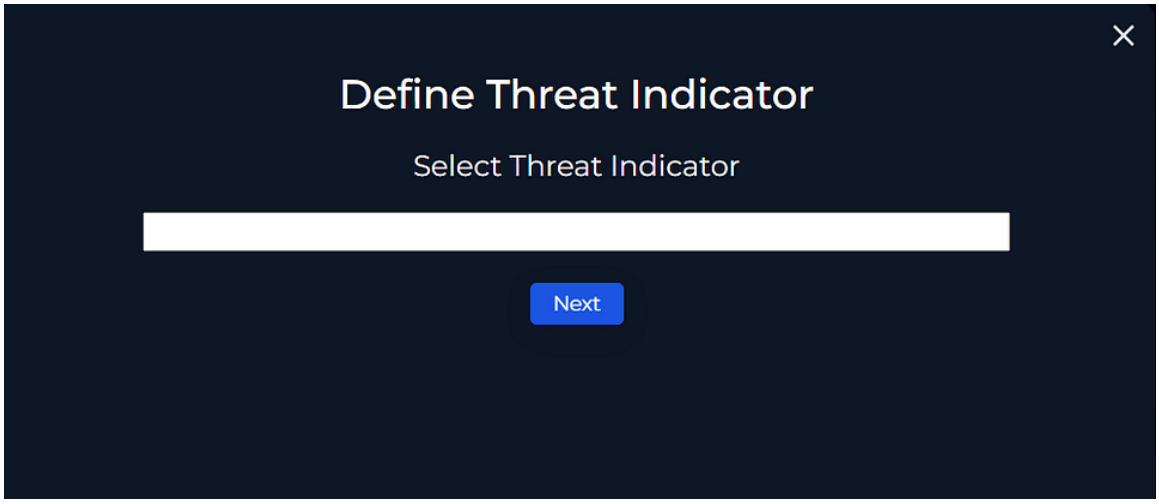
SOC138 - Detected Suspicious Xls File [Let's Defend – Write-up]

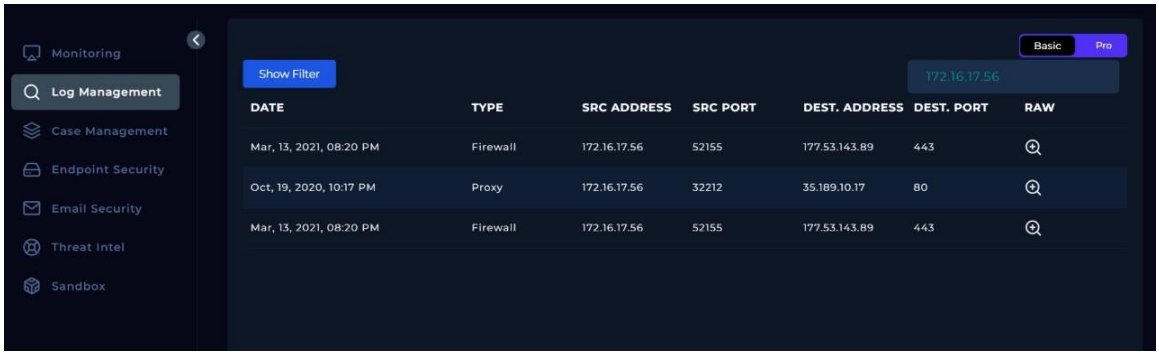
The alert for Detected Suspicious Xls File served as a key starting point for the investigation. It provided the necessary visibility to initiate the analysis process and helped in identifying the subsequent activities within the environment. This detection was essential for understanding the sequence of events during the incident response.

| Start Investigation

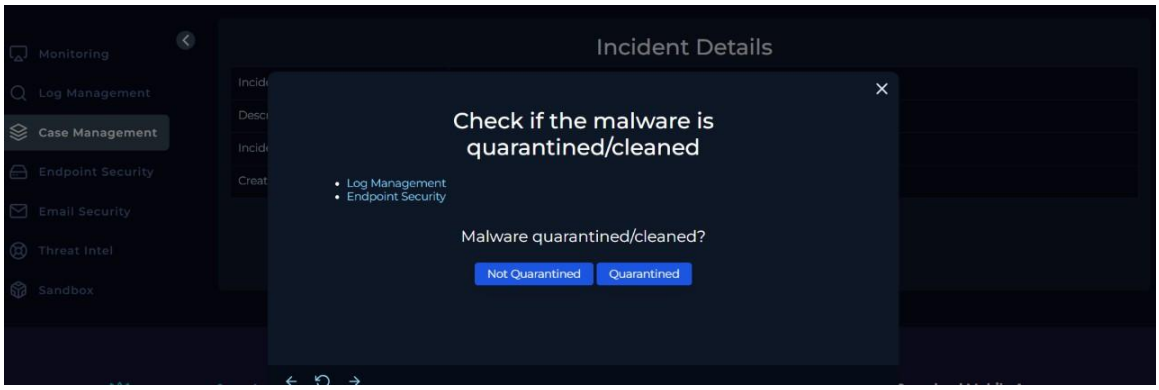
At the beginning of the analysis and closing of the alert, we use Playbook.



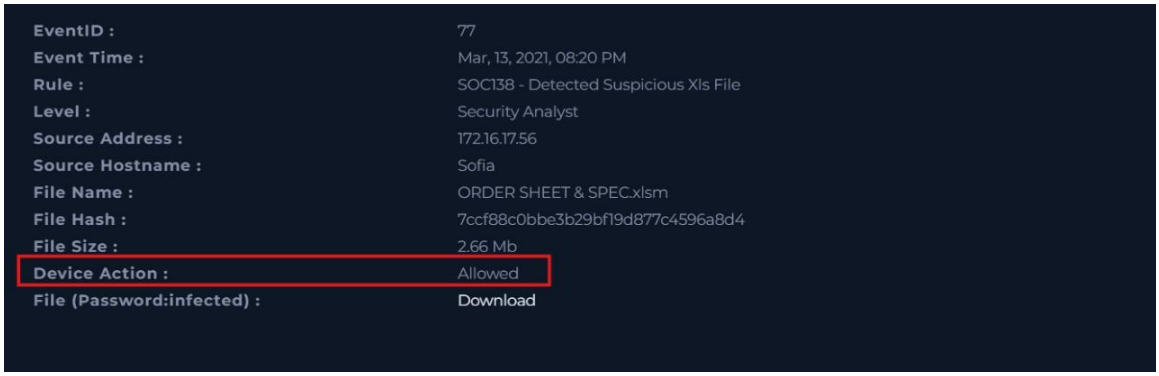
And to define Threat indicator I just saw the Log management.



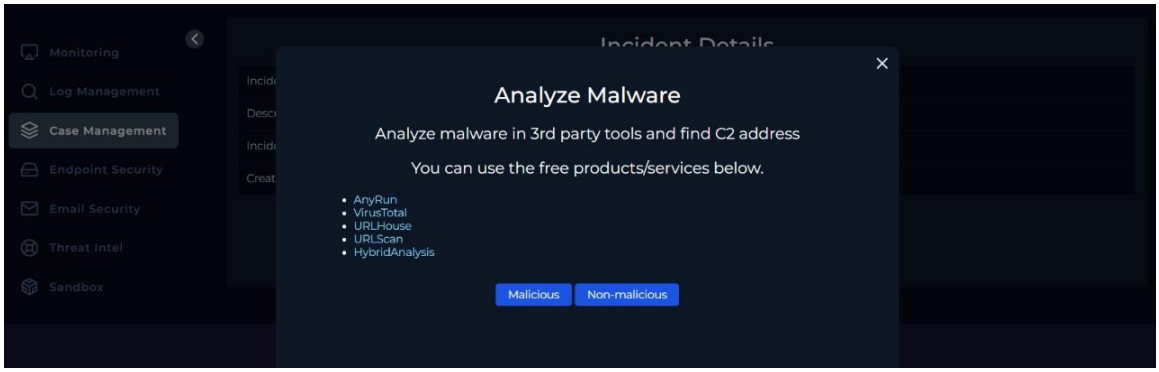
And I saw that the ip 172.16.17.56 which is outgoing traffic, So the answer is **Unknown or unexpected outgoing internet traffic.**

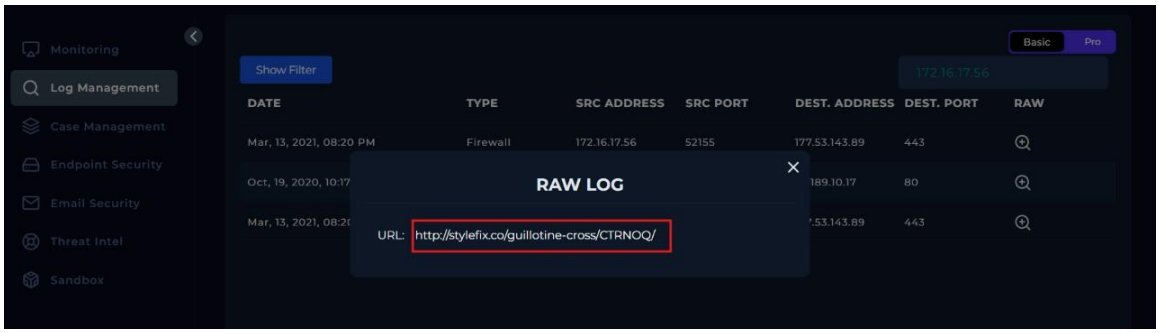


The answer to this question is inside the alert;

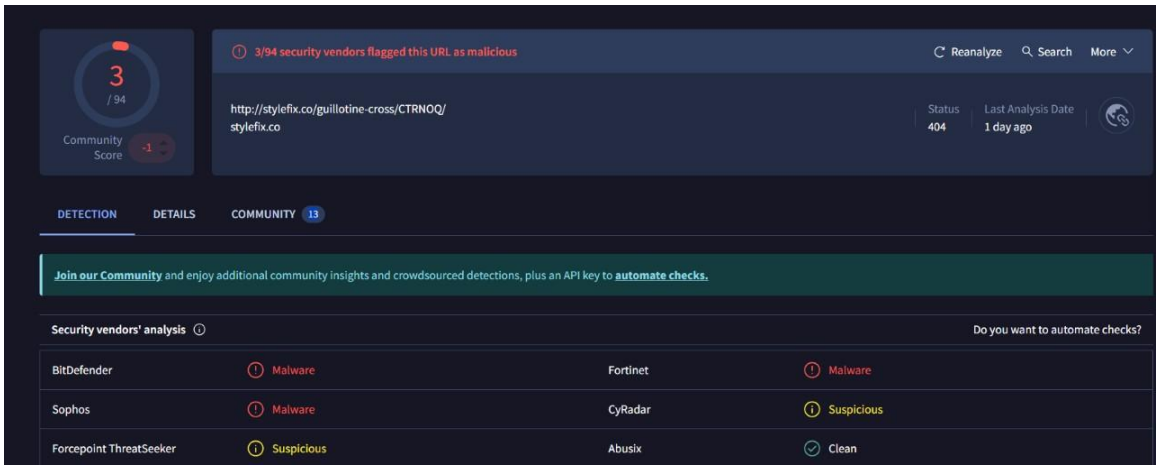


So, the answer is **Not quarantined** because the Device action is allowed

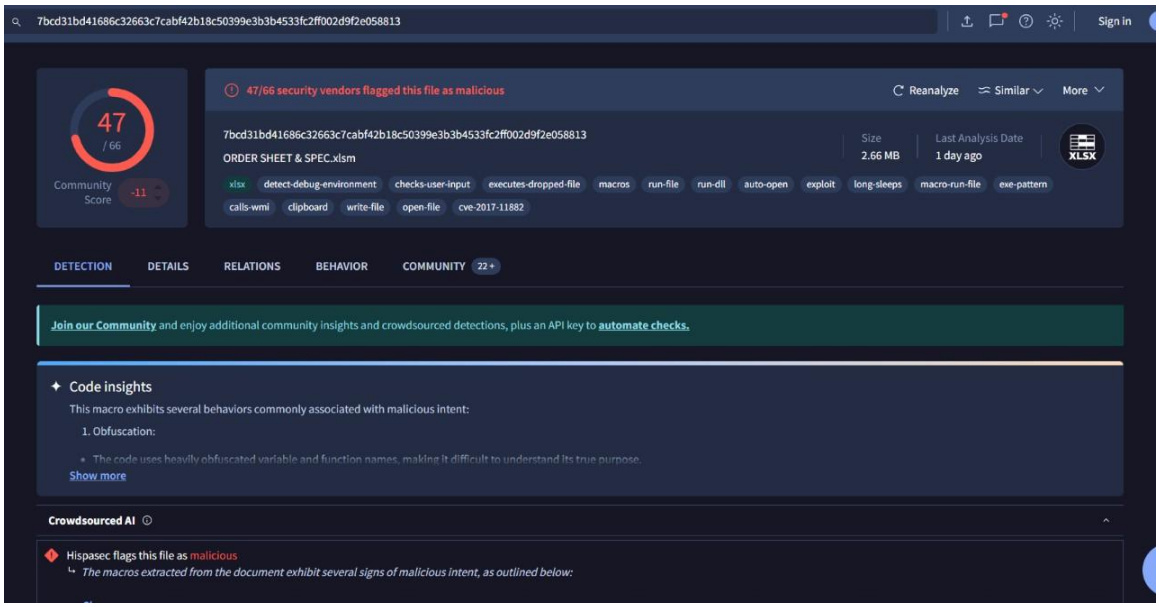




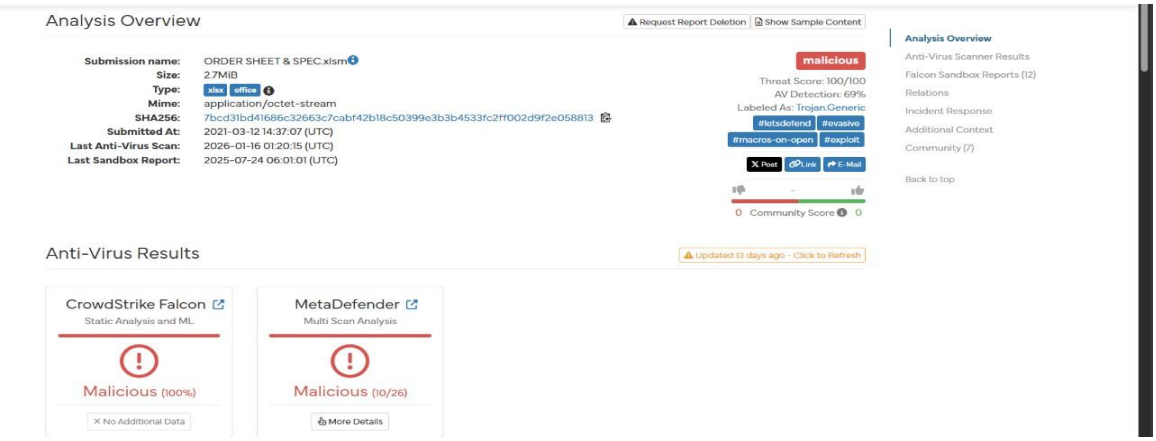
I Analysis this Url to see whether it is Malicious or not



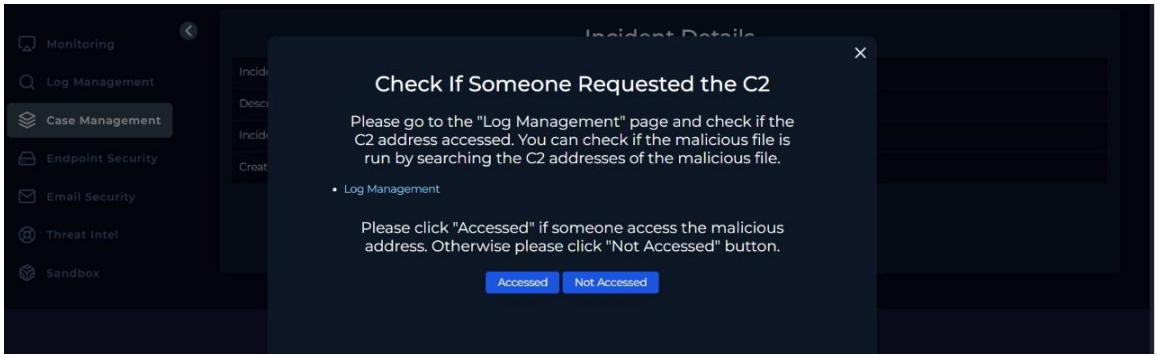
I analyzed it in VirusTotal and it turned out to be harmful (Malware).

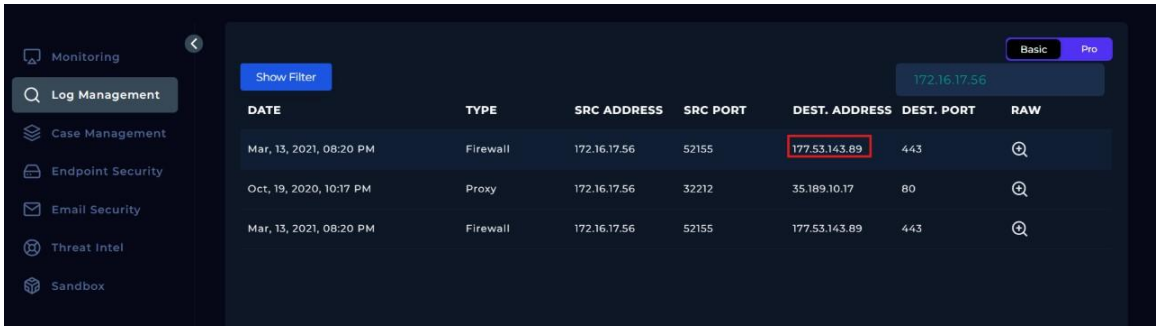


I also analyzed the file's hash, and it turned out to be malicious.

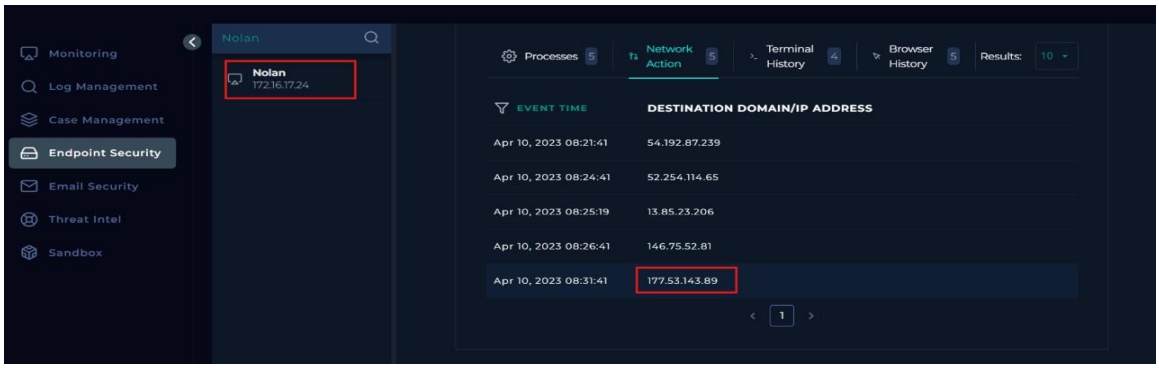


Ans I also used HybridAnalysis for duple check and appear as malicious.

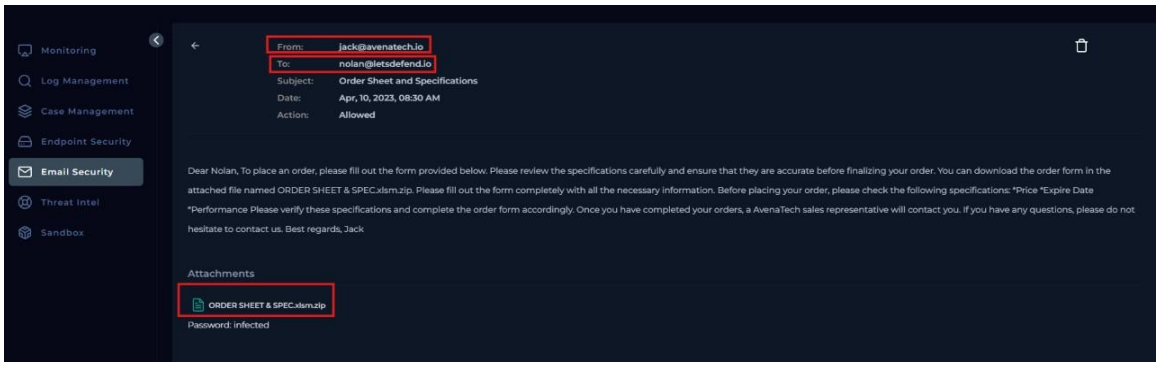




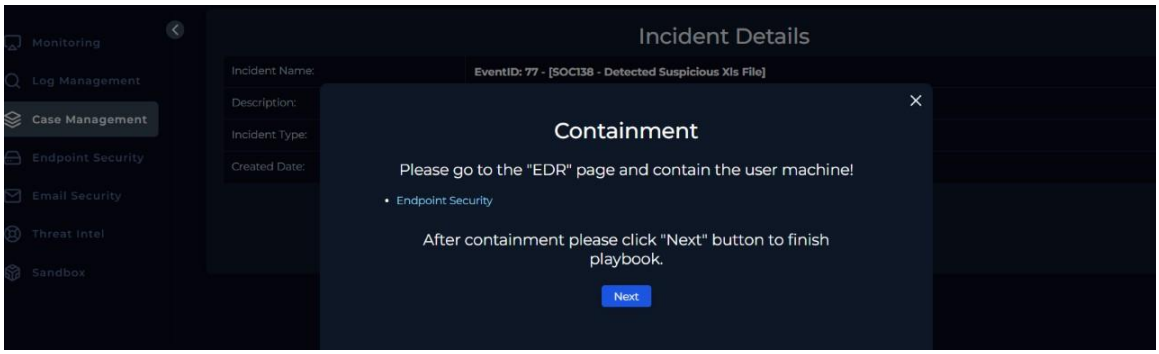
I saw that ip 172.16.17.56 connect to ip 177.53.143.89 which is the attacker's ip
So the **answer is Accessed**.



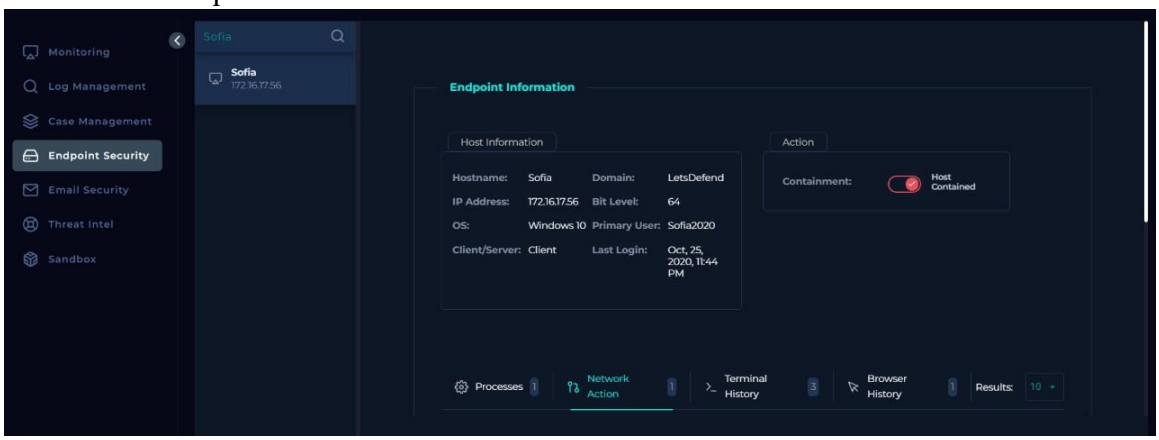
Ans I saw also that the ip 177.53.143.89 connect with Nolan, and for more investigation I checked the email section to see if there any communication.



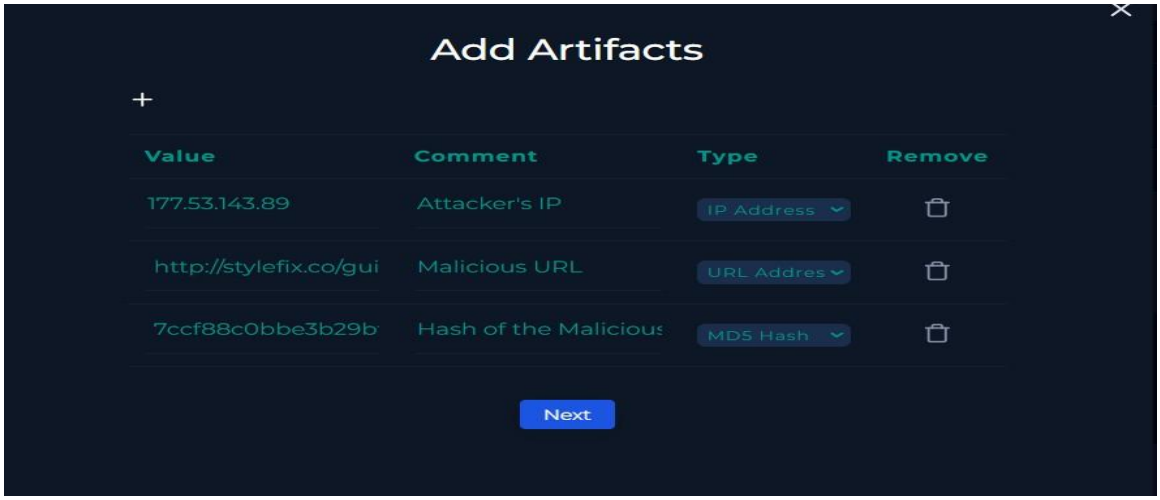
So, it seems that email jack@avenatech.io sent to nolan@letsdefend.io malicious email that is contains the same malicious file that is appear on the Alert. So at the end Yes there is communication to malicious address (177.53.143.89).



After that it's required to isolate the device.



After I fished the these the artifacts;



And yes, it is **True Positive**.

Summary

The investigation of the SOC138 – Detected Suspicious XLS File alert confirmed a True Positive security incident. Analysis revealed that the XLS file was malicious, as verified through multiple threat intelligence platforms including VirusTotal, Hybrid Analysis, and hash reputation checks. Log analysis showed unexpected outbound traffic from the internal host 172.16.17.56 to the external IP 177.53.143.89, identified as the attacker's infrastructure.

Further investigation confirmed that the malicious file was delivered via phishing email, establishing communication between internal users and the malicious external address. Although the device action was initially allowed and the file was not quarantined, the evidence clearly indicated malicious activity. As a result, device isolation was required, and the alert was correctly classified as a True Positive.