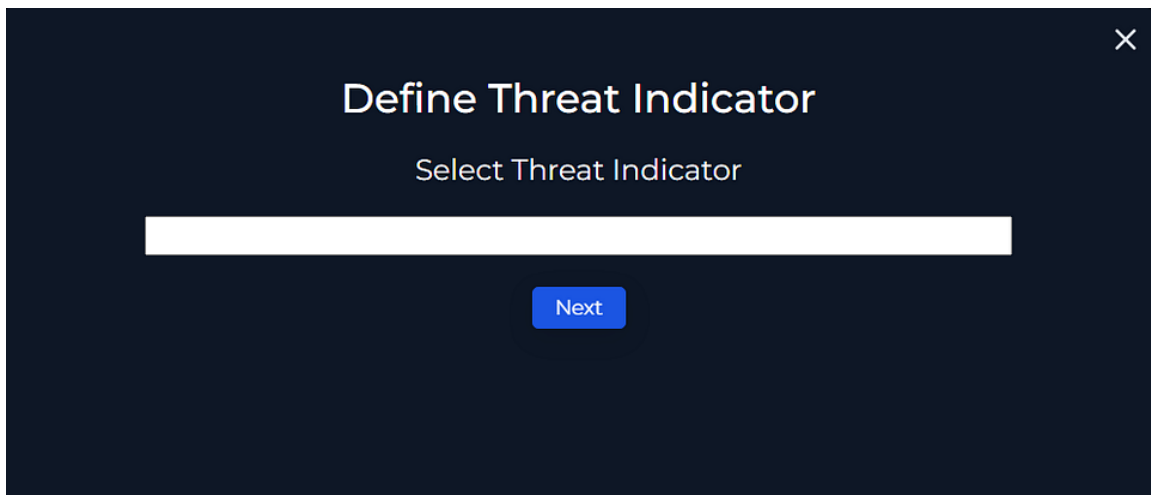


# SOC138 - Detected Suspicious Xls File [Let's Defend – Write-up]

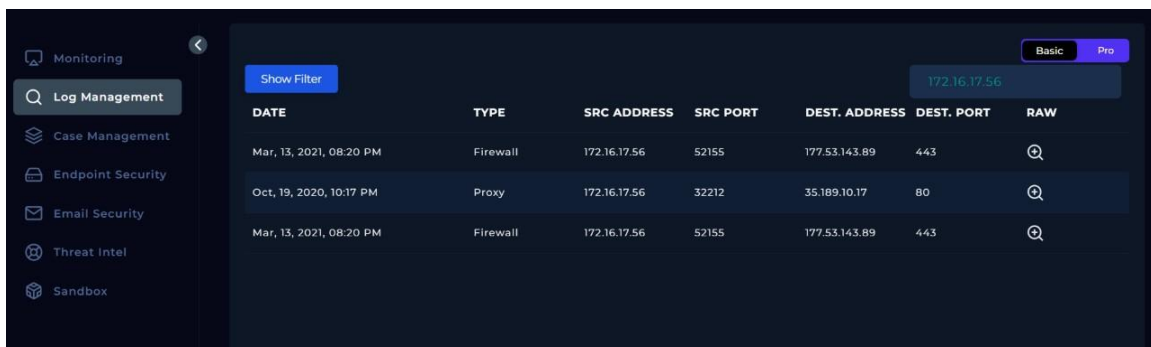
The alert for Detected Suspicious Xls File served as a key starting point for the investigation. It provided the necessary visibility to initiate the analysis process and helped in identifying the subsequent activities within the environment. This detection was essential for understanding the sequence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

## | Start Investigation

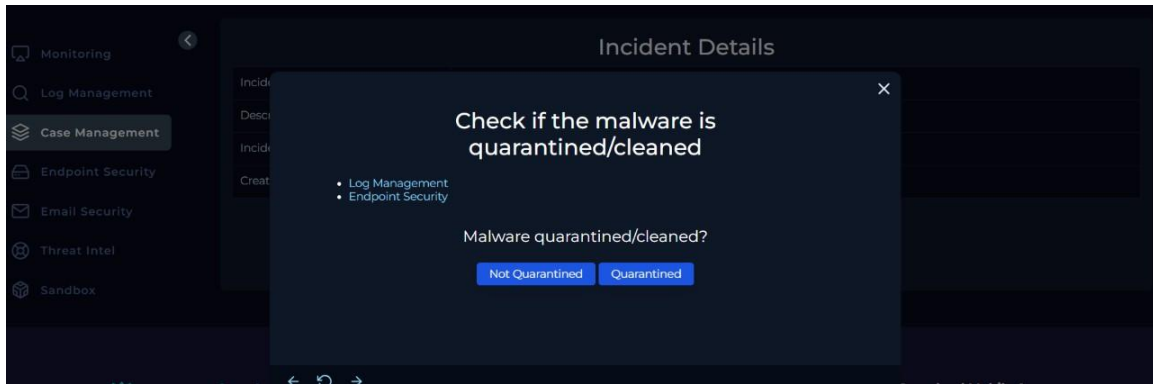
At the beginning of the analysis and closing of the alert, we use Playbook.



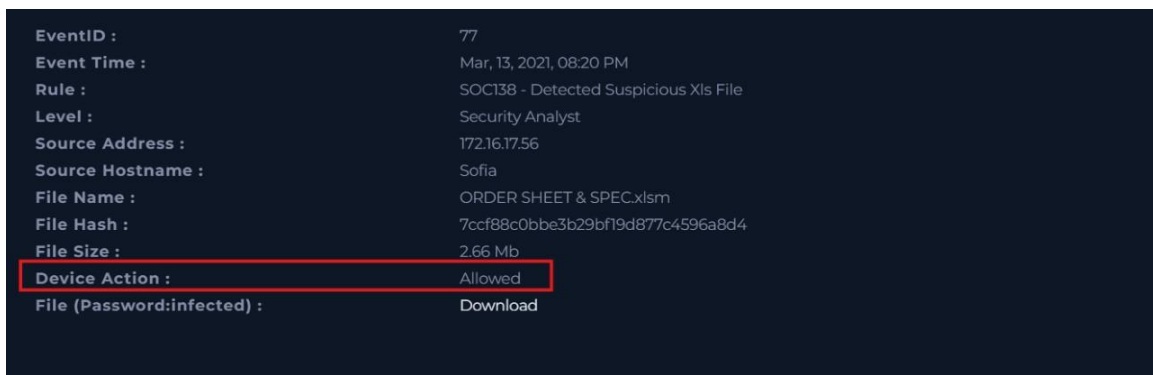
And to define Threat indicator I just saw the Log management.



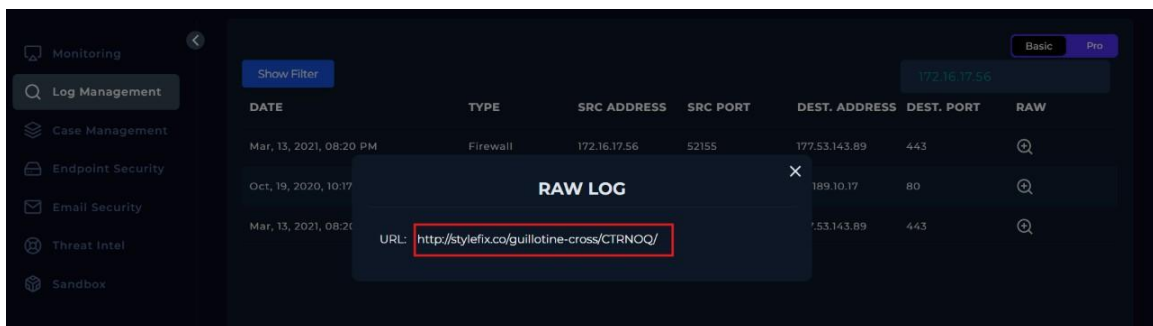
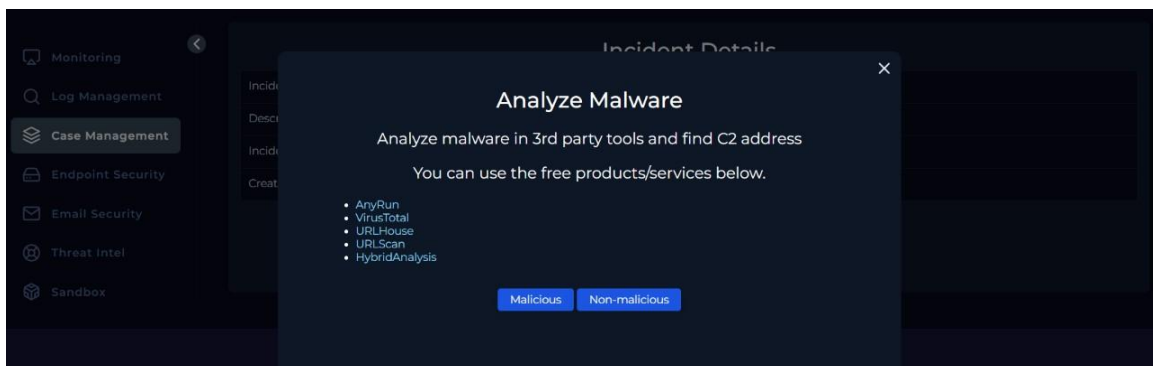
And I saw that the ip 172.16.17.56 which is outgoing traffic, So the answer is **Unknown or unexpected outgoing internet traffic.**



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

3 / 94  
Community Score -1

3/94 security vendors flagged this URL as malicious

Reanalyze Search More

http://stylefix.co/guillotine-cross/CTRNOQ/stylefix.co

Status 404 Last Analysis Date 1 day ago

DETECTION DETAILS COMMUNITY 13

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

BitDefender	Malware	Fortinet	Malware
Sophos	Malware	CyRadat	Suspicious
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean

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

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

47 / 66  
Community Score -11

47/66 security vendors flagged this file as malicious

Reanalyze Similar More

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

ORDER SHEET & SPEC.xlsm

Size 2.66 MB Last Analysis Date 1 day ago

xlsm detect-debug-environment checks-user-input executes-dropped-file macros run-file run-dll auto-open exploit long-sleeps macro-run-file exe-pattern

calls-wmi clipboard write-file open-file cve-2017-11882

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 22+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Code insights

This macro exhibits several behaviors commonly associated with malicious intent:

- Obfuscation:
  - The code uses heavily obfuscated variable and function names, making it difficult to understand its true purpose.

Show more

Crowdsourced AI

Hispasec flags this file as malicious

The macros extracted from the document exhibit several signs of malicious intent, as outlined below:

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

Analysis Overview

Request Report Deletion Show Sample Content

Submission name: ORDER SHEET & SPEC.xlsm

Size: 2.7MiB

Type: [Excel](#) [Details](#)

Mime: application/octet-stream

SHA256: 7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

Submitted At: 2021-03-12 14:37:07 (UTC)

Last Anti-Virus Scan: 2026-01-16 01:20:15 (UTC)

Last Sandbox Report: 2025-07-24 06:01:01 (UTC)

malicious

Threat Score: 100/100

AV Detection: 69%

Labeled As: Trojan.Generic

[#bitdefender](#) [#revalsec](#)

[#macro-on-open](#) [#exploit](#)

[X Post](#) [Link](#) [E Mail](#)

0 Community Score 0

Updated 13 days ago - Click to Refresh

Anti-Virus Results

CrowdStrike Falcon Static Analysis and ML

Malicious (100%)

X No Additional Data

MetaDefender Multi Scan Analysis

Malicious (10/26)

More Details

Analysis Overview

Anti-Virus Scanner Results

Falcon Sandbox Reports (12)

Relations

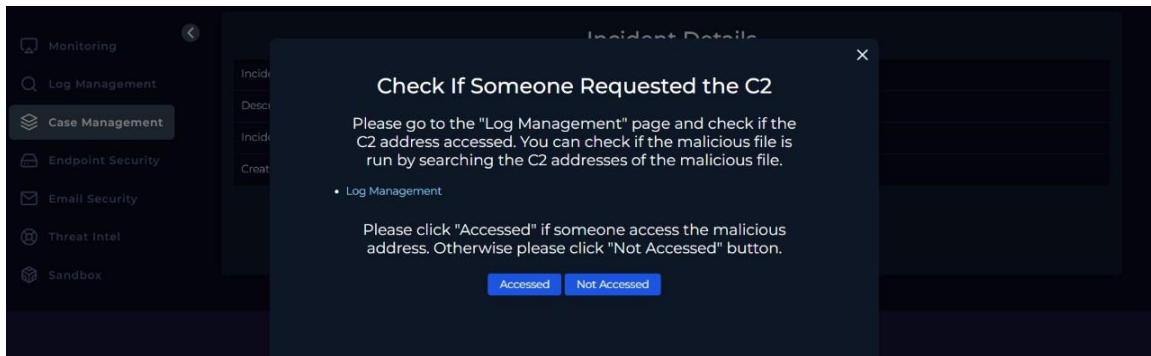
Incident Response

Additional Context

Community (7)

Back to top

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

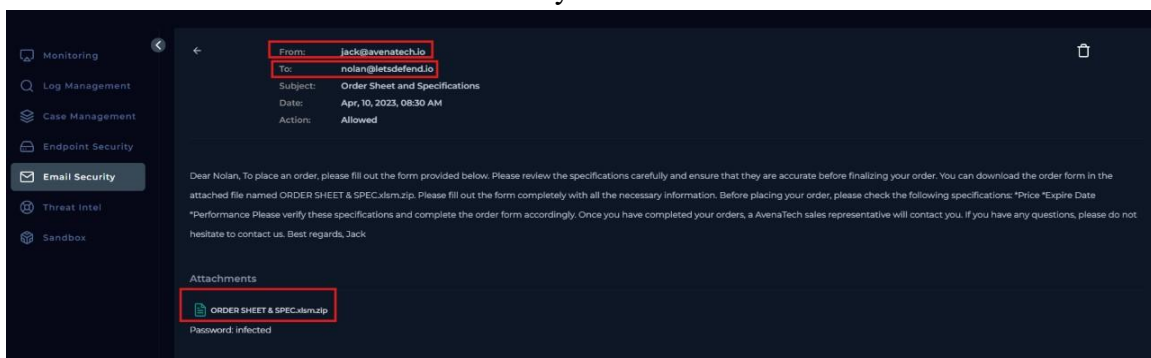


DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 13, 2021, 08:20 PM	Firewall	172.16.17.56	52155	177.53.143.89	443	<a href="#">Q</a>
Oct, 19, 2020, 10:17 PM	Proxy	172.16.17.56	32212	35.189.10.17	80	<a href="#">Q</a>
Mar, 13, 2021, 08:20 PM	Firewall	172.16.17.56	52155	177.53.143.89	443	<a href="#">Q</a>

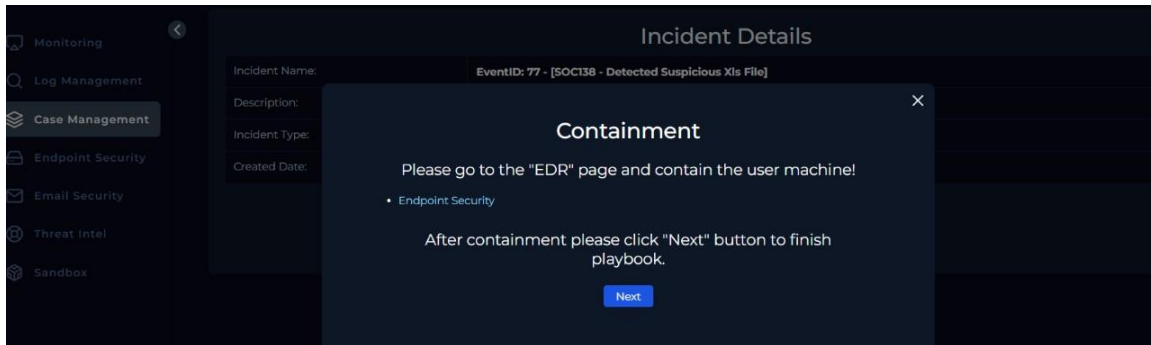
I saw that ip 172.16.17.56 connect to ip 177.53.143.89 which is the attacker's ip  
So the **answer is Accessed**.

EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Apr 10, 2023 08:21:41	54.192.87.239
Apr 10, 2023 08:24:41	52.254.114.65
Apr 10, 2023 08:25:19	13.85.23.206
Apr 10, 2023 08:26:41	146.75.52.81
Apr 10, 2023 08:31:41	177.53.143.89

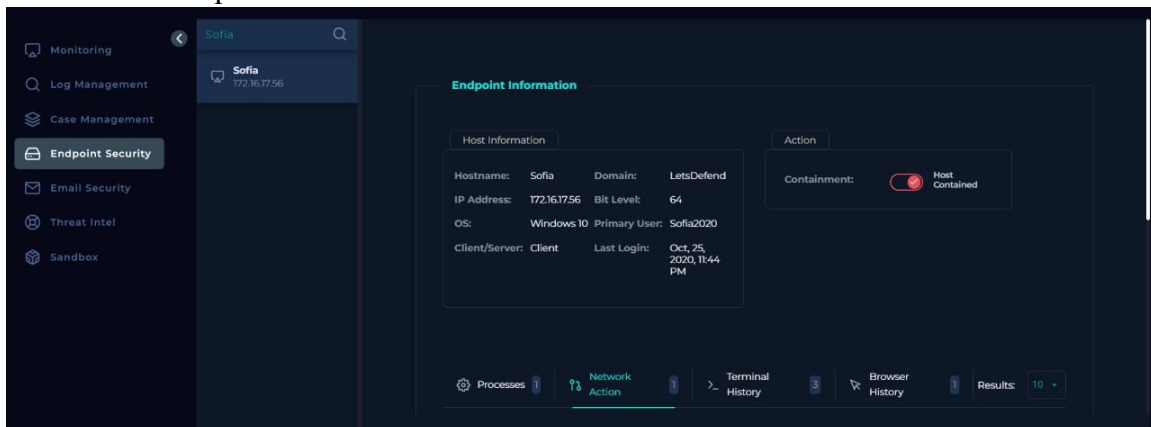
Ans I saw also that the ip 177.53.143.89 connect with Nolan, and for more investigation I checked the email section to see if there any communication.



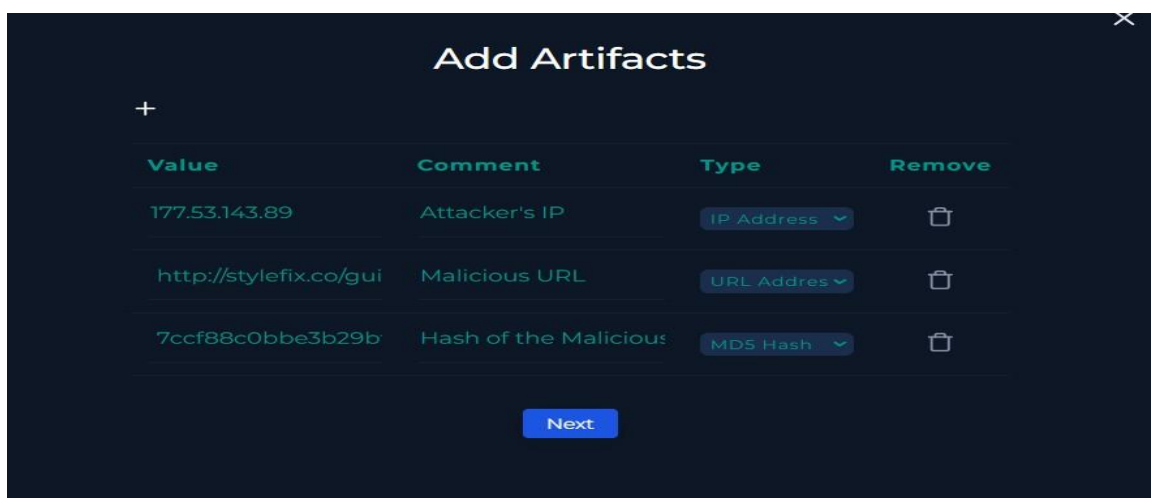
So, it seems that email [jack@avenatech.io](mailto:jack@avenatech.io) sent to [nolan@letsdefend.io](mailto:nolan@letsdefend.io) malicious email that contains the same malicious file that is appear on the Alert. So at the end Yes there is communication to malicious address (177.53.143.89).



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.