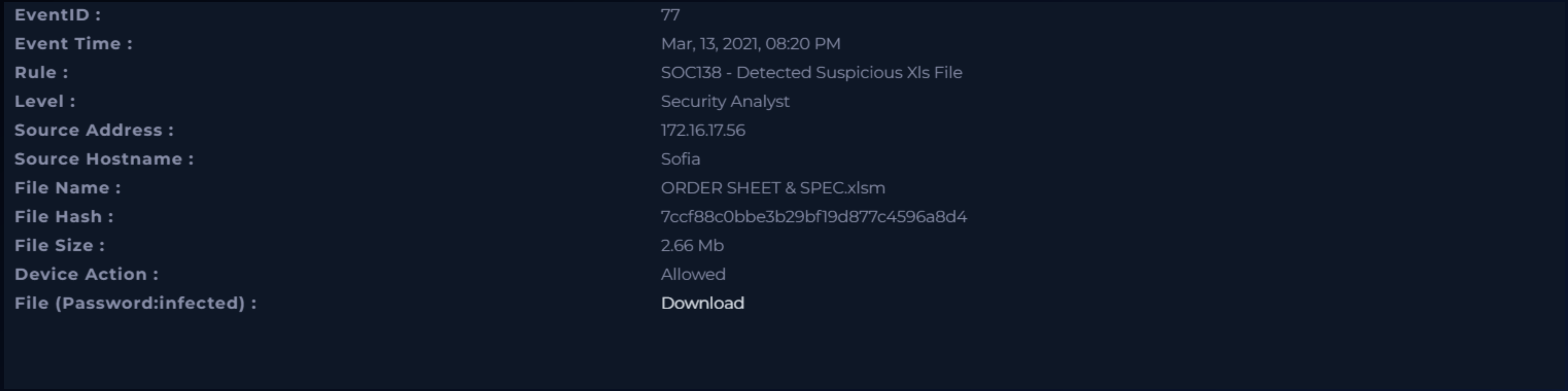
Lets Defend SOC LAB –Malicious file Download Attempt

INVESTIGATED BY : MEHRIER B. TOUHID

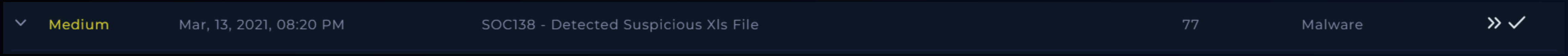
Investigating the Alert Information

- We find what caused the alert
- The action taken by the system
- The file and user Information

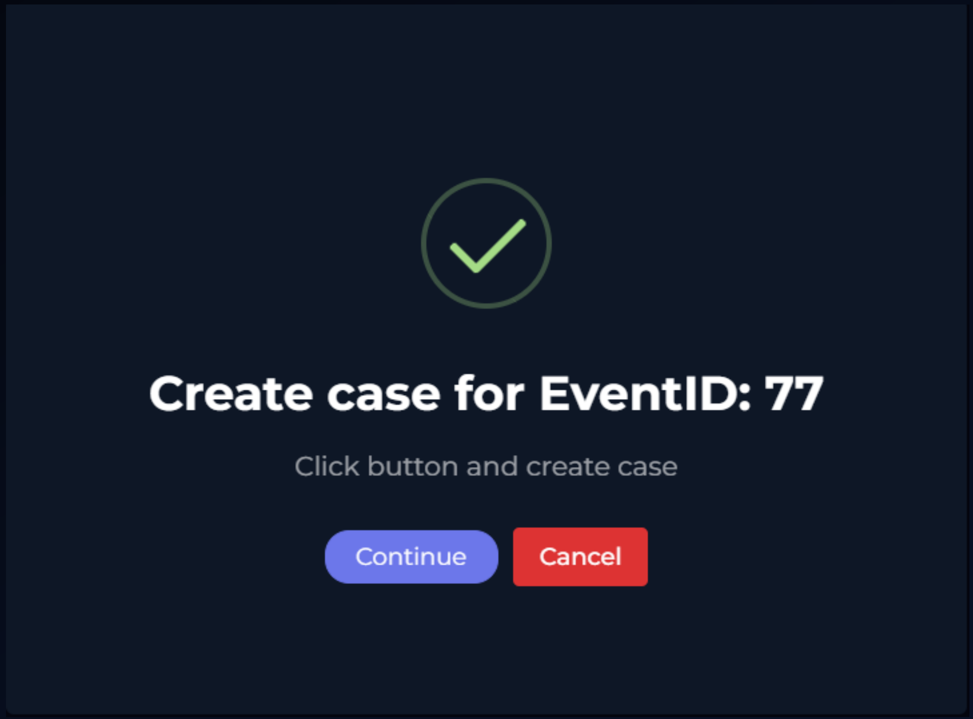


EventID :	77
Event Time :	Mar, 13, 2021, 08:20 PM
Rule :	SOC138 - Detected Suspicious Xls File
Level :	Security Analyst
Source Address :	172.16.17.56
Source Hostname :	Sofia
File Name :	ORDER SHEET & SPEC.xlsm
File Hash :	7ccf88c0bbe3b29bf19d877c4596a8d4
File Size :	2.66 Mb
Device Action :	Allowed
File (Password:infected) :	Download

Took Ownership of the attack by creating a case



Medium	Mar, 13, 2021, 08:20 PM	SOC138 - Detected Suspicious Xls File	77	Malware

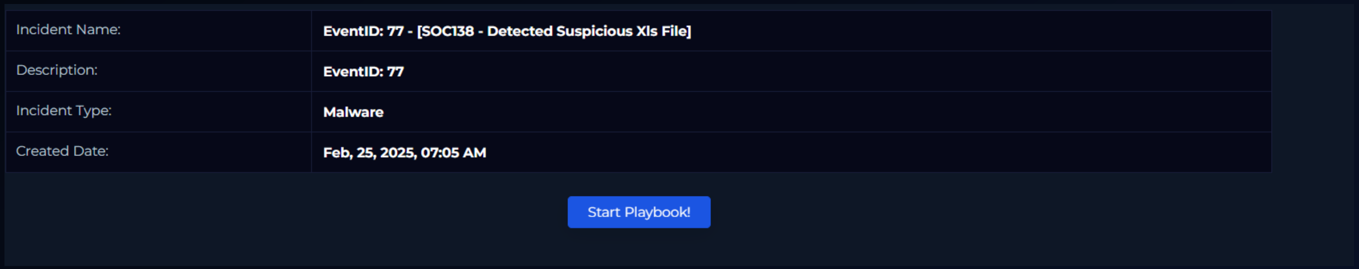


Create case for EventID: 77

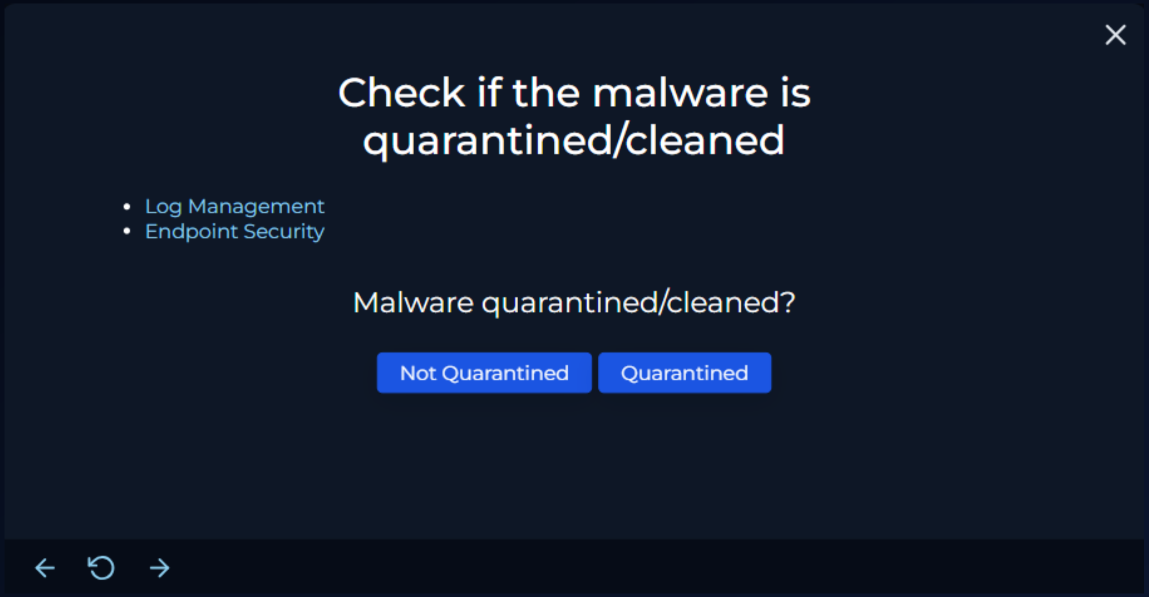
Click button and create case

Using Playbook to respond to this Incident

- Check if the Malware is clean or not .
- Check the log .
- Check the endpoint device .



Incident Name:	EventID: 77 - [SOC138 - Detected Suspicious Xls File]
Description:	EventID: 77
Incident Type:	Malware
Created Date:	Feb, 25, 2025, 07:05 AM



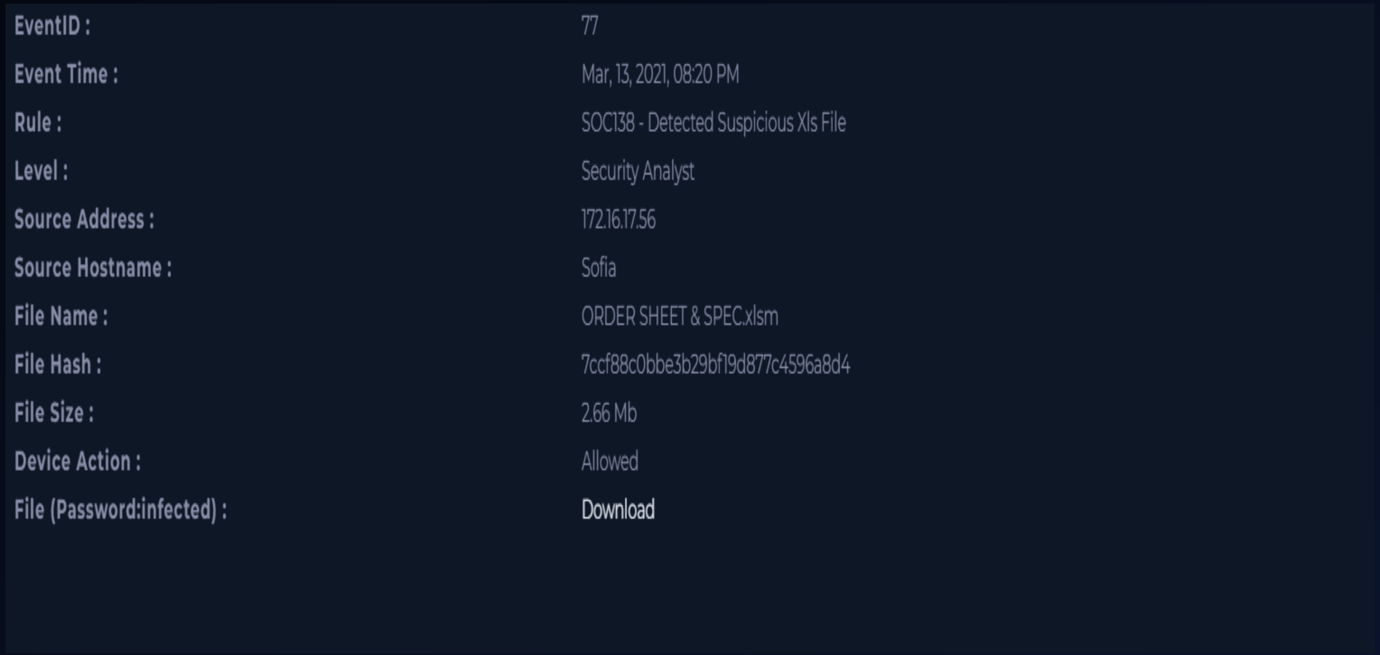
Check if the malware is quarantined/cleaned

- Log Management
- Endpoint Security

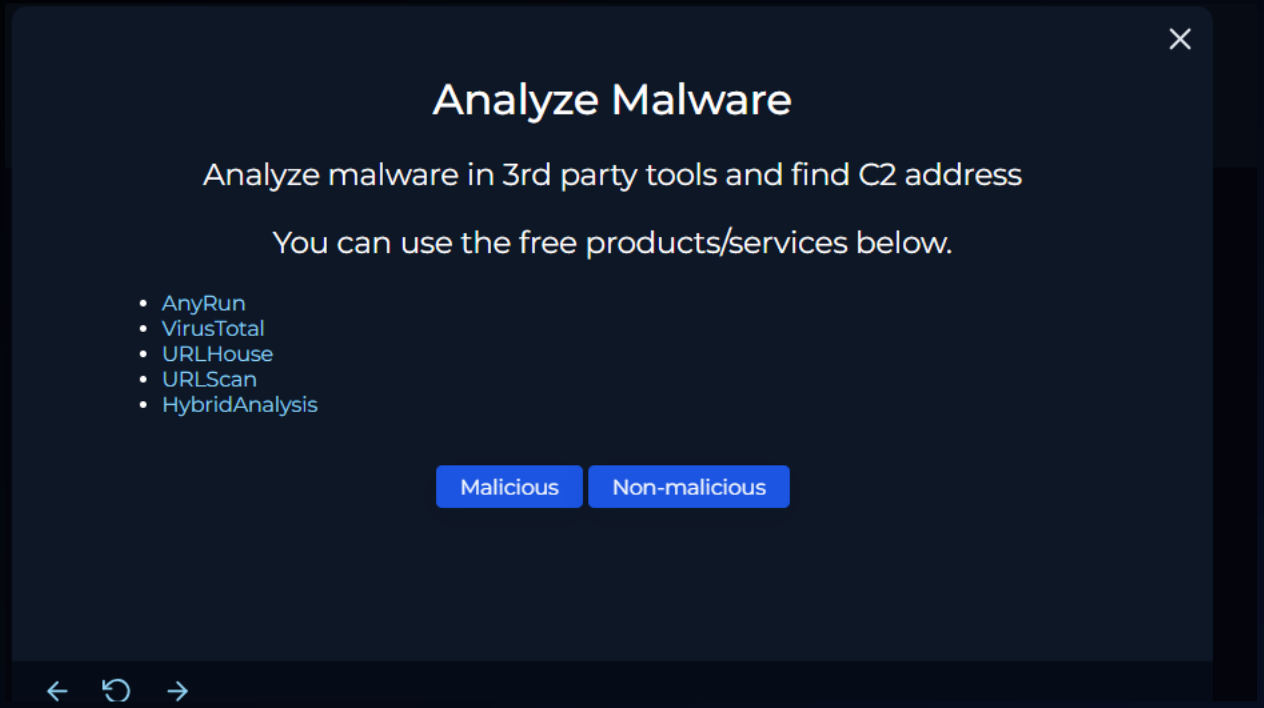
Malware quarantined/cleaned?

Looking Back at the alert Information the Device action was ‘allowed’.

- File was not Quarantined



EventID :	77
Event Time :	Mar, 13, 2021, 08:20 PM
Rule :	SOC138 - Detected Suspicious Xls File
Level :	Security Analyst
Source Address :	172.16.17.56
Source Hostname :	Sofia
File Name :	ORDER SHEET & SPEC.xlsm
File Hash :	7ccf88c0bbe3b29bf19d877c4596a8d4
File Size :	2.66 Mb
Device Action :	Allowed
File (Password:infected) :	Download



Analyze Malware

Analyze malware in 3rd party tools and find C2 address

You can use the free products/services below.

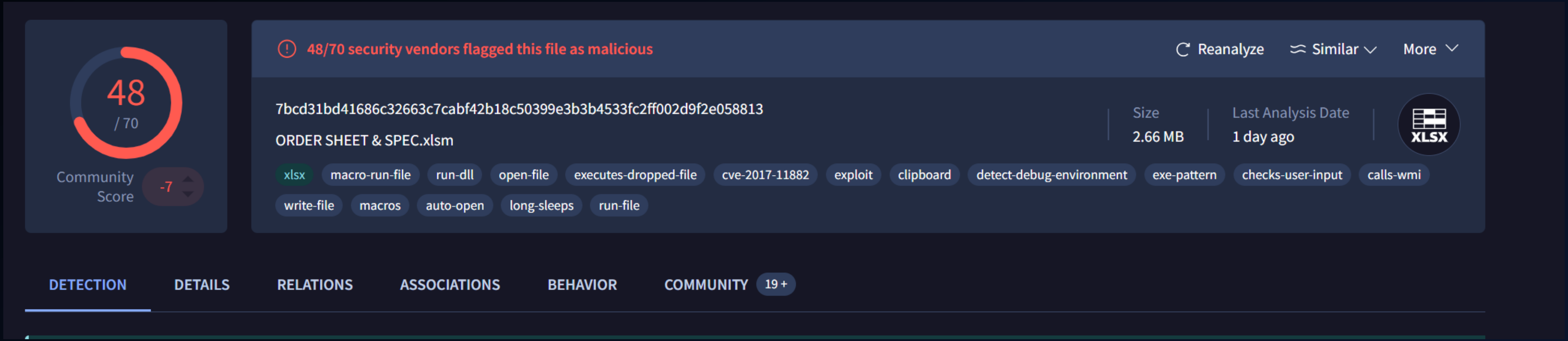
- AnyRun
- VirusTotal
- URLHouse
- URLScan
- HybridAnalysis

Next Step of the playbook is analyze the file .

WE WILL USE VIRUS TOTAL FOR SIMPLICITY

Using Sandbox Tools to Analyze Malware Hash Value

FILE WAS FLAGGED MALICIOUS BY 48 VENDORS .



48 / 70

Community Score -7

48/70 security vendors flagged this file as malicious

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

ORDER SHEET & SPEC.xlsm

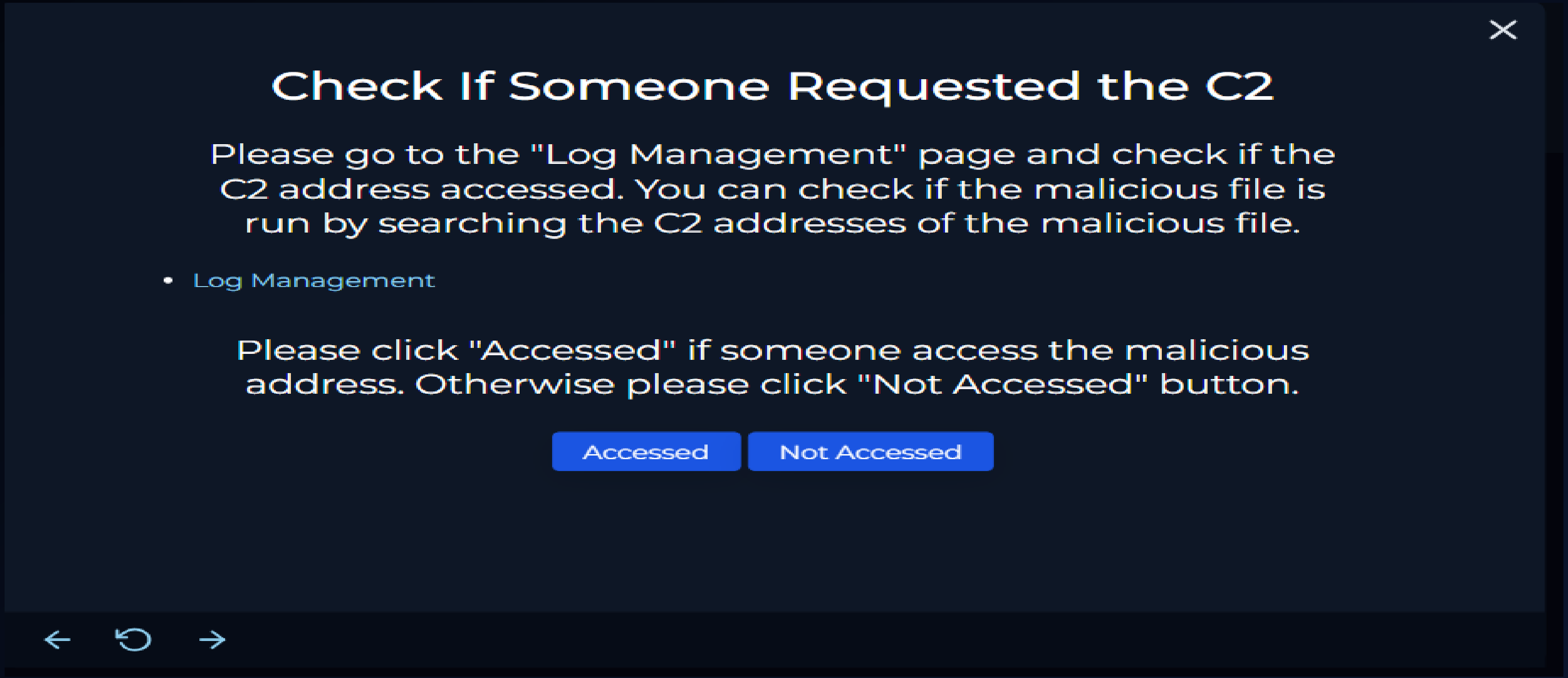
Size 2.66 MB

Last Analysis Date 1 day ago

xlsx macro-run-file run-dll open-file executes-dropped-file cve-2017-11882 exploit clipboard detect-debug-environment exe-pattern checks-user-input calls-wmi write-file macros auto-open long-sleeps run-file

HENCE, FILE IS MALICIOUS

Next step is to check is the c2 address the file contacted



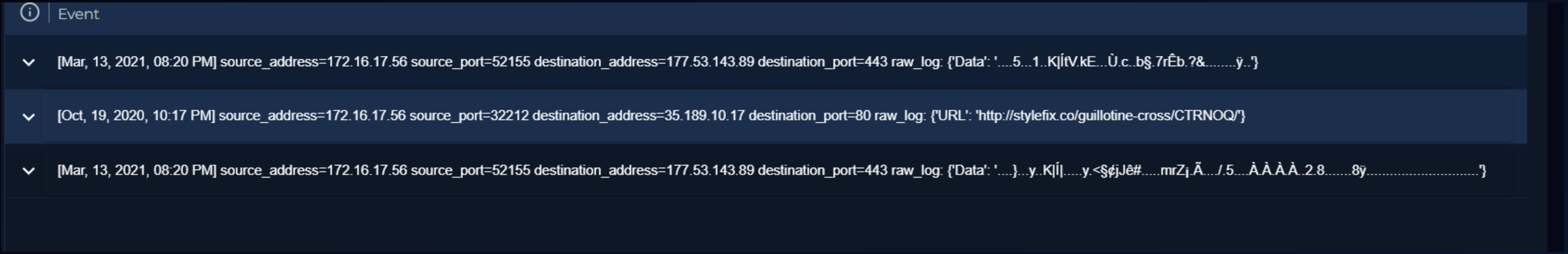
Check If Someone Requested the C2

Please go to the "Log Management" page and check if the C2 address accessed. You can check if the malicious file is run by searching the C2 addresses of the malicious file.

- Log Management

Please click "Accessed" if someone access the malicious address. Otherwise please click "Not Accessed" button.

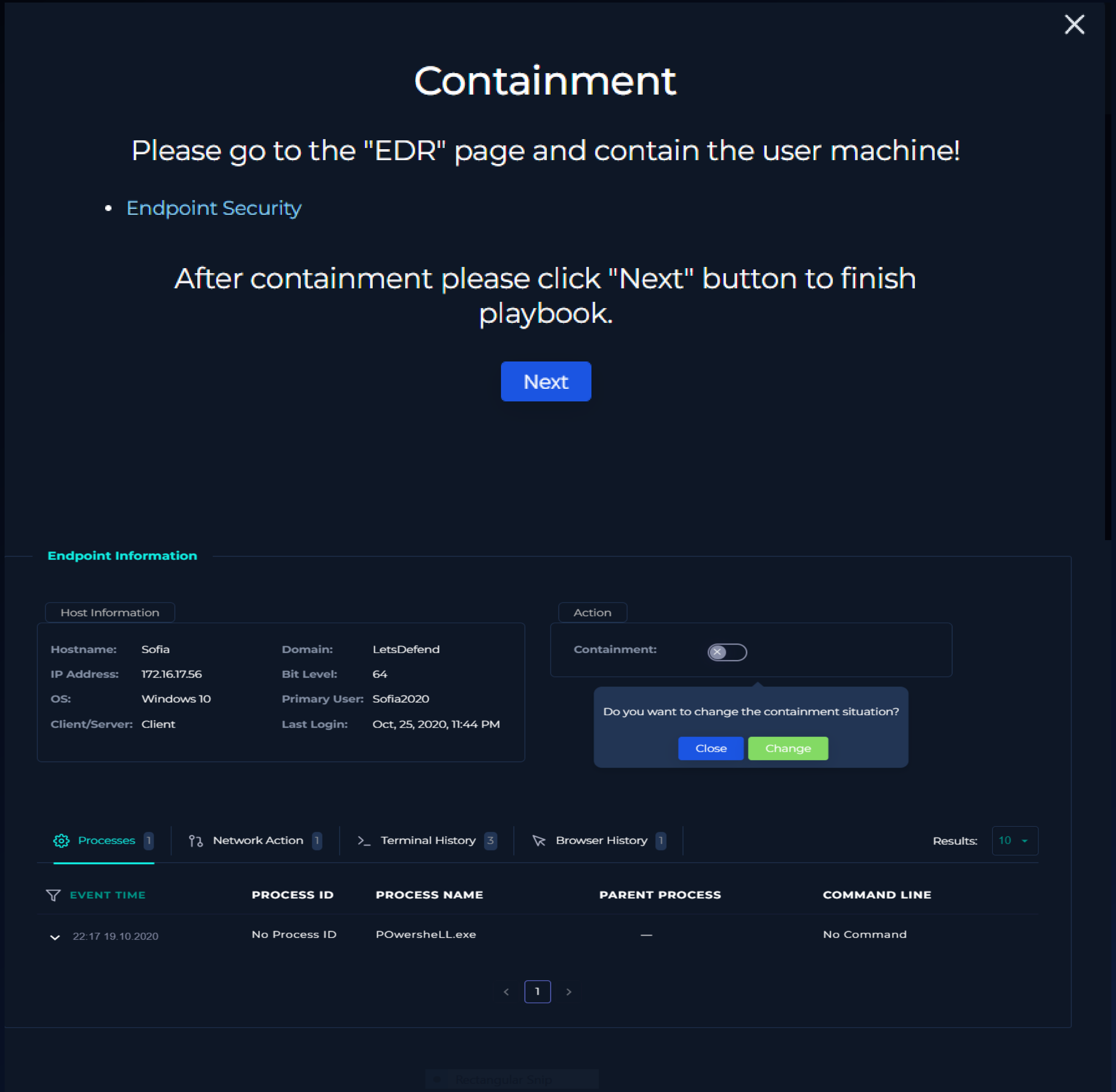
The alert was generated on March 13, 2021,8:20 Pm . At the same time of the alert , we see 2 logs generated which shows that the malware was communicating with the c2 address.



```
[Mar, 13, 2021, 08:20 PM] source_address=172.16.17.56 source_port=52155 destination_address=177.53.143.89 destination_port=443 raw_log: {'Data': '....5...1..K|ÍtV.kE...Ù.c..b§.7rÊb.?&........ÿ..'}
[Oct, 19, 2020, 10:17 PM] source_address=172.16.17.56 source_port=32212 destination_address=35.189.10.17 destination_port=80 raw_log: {'URL': 'http://stylefix.co/guillotine-cross/CTRNOQ/'}
[Mar, 13, 2021, 08:20 PM] source_address=172.16.17.56 source_port=52155 destination_address=177.53.143.89 destination_port=443 raw_log: {'Data': '....}...y..K|Í|.....y.<§¢jJê#.....mrZ¡.Ã..../.5....À.À.À.À..2.8.......8ÿ...........................'}
```

CONTAINING THE ATTACK

We find the host's endpoint device using the source address and then contain the device



Containment

Please go to the "EDR" page and contain the user machine!

- Endpoint Security

After containment please click "Next" button to finish playbook.

Endpoint Information

Host Information

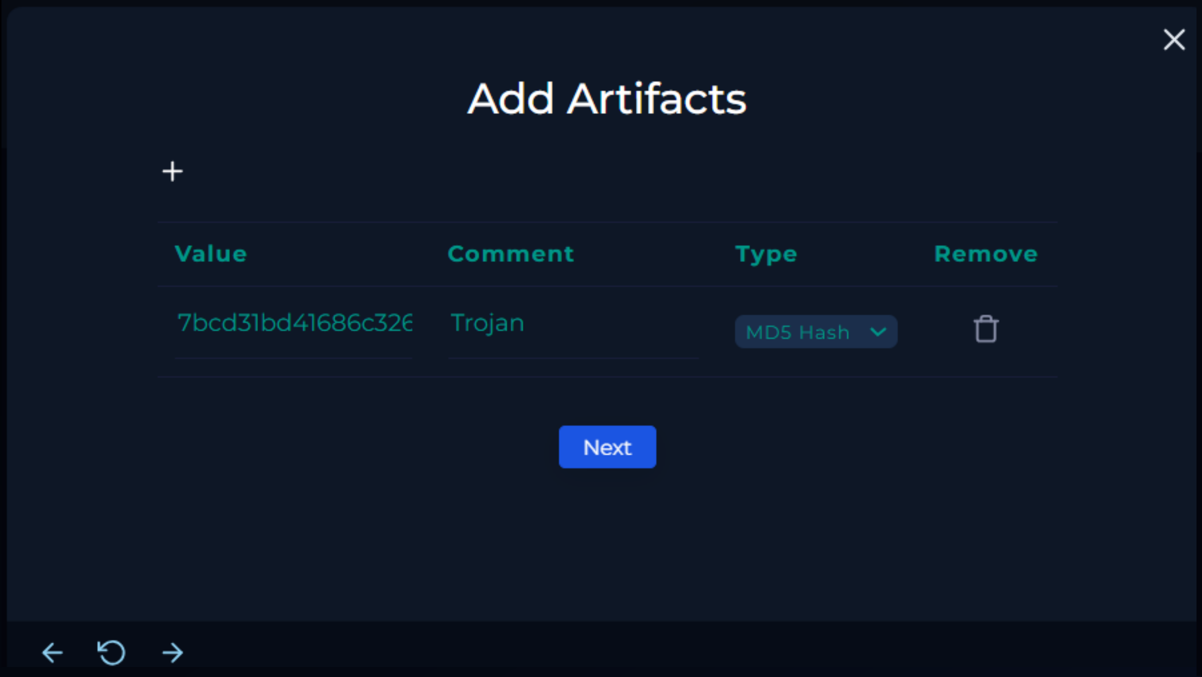
Hostname:	Sofia	Domain:	LetsDefend
IP Address:	172.16.17.56	Bit Level:	64
OS:	Windows 10	Primary User:	Sofia2020
Client/Server:	Client	Last Login:	Oct, 25, 2020, 11:44 PM

Action

Containment: ☒

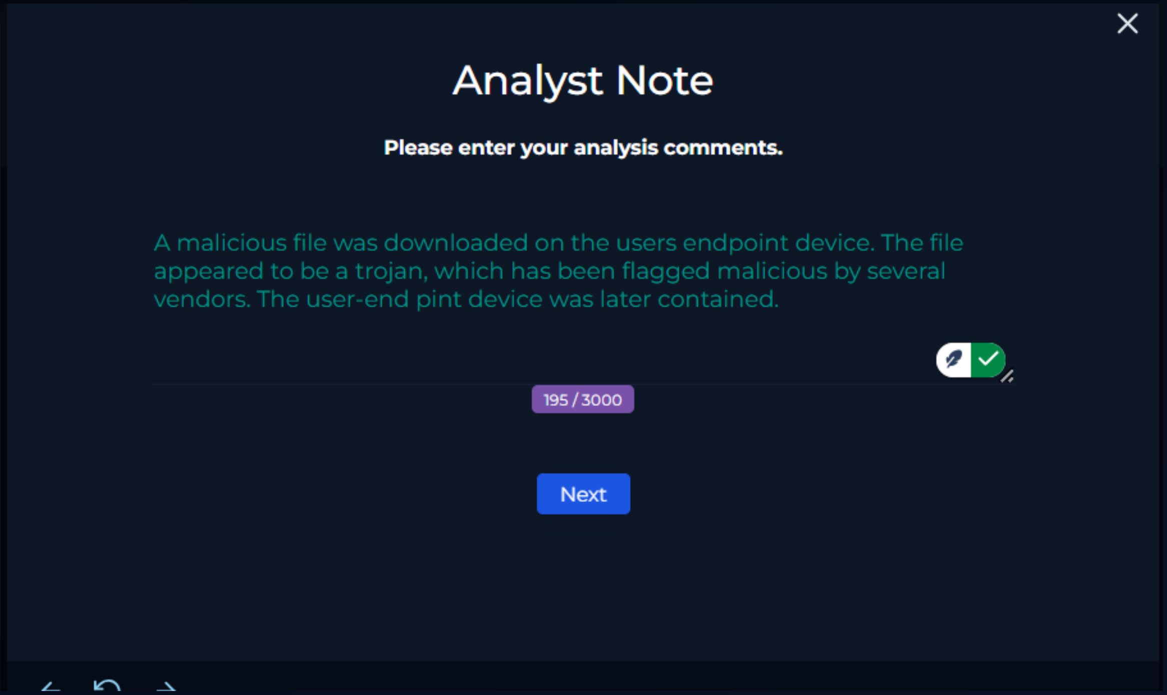
Do you want to change the containment situation?

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
22:17 19.10.2020	No Process ID	POwersheLL.exe	—	No Command



Add Artifacts

Value	Comment	Type	Remove
7bcd31bd41686c326	Trojan	MD5 Hash	🗑



Analyst Note

Please enter your analysis comments.

A malicious file was downloaded on the users endpoint device. The file appeared to be a trojan, which has been flagged malicious by several vendors. The user-end pint device was later contained.

195 / 3000

Finally we record the the malware hash file and label it as a trojan as stated by virus total . Before closing the alert we write a small note summarizing the event .

Credit : Lets Defend.io

PREPARED BY : MEHRIER B. TOUHID