

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 screenshot shows the 'MAIN CHANNEL' tab with a table of alerts. The first alert is highlighted with a red 'High' severity and a 'Malware' type. Below the table, a detailed view of the alert is shown, including fields like EventID, Event Time, Rule, Level, Source Address, Source Hostname, File Name, File Hash, File Size, Device Action, Download, and Password/Infected status.

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	May 23, 2021, 7:32 p.m.	SOC145 - Ransomware Detected	92	Malware	+

EventID: 92
Event Time: May 23, 2021, 7:32 p.m.
Rule: SOC145 - Ransomware Detected
Level: Security Analyst
Source Address: 172.16.17.88
Source Hostname: MarkPRD
File Name: ab.exe
File Hash: 0b486fe0503524cfe4726a4022fa6a68
File Size: 775.50 Kb
Device Action: Allowed
Download: 0b486fe0503524cfe4726a4022fa6a68.zip
(Password/Infected):
Show Hint

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.

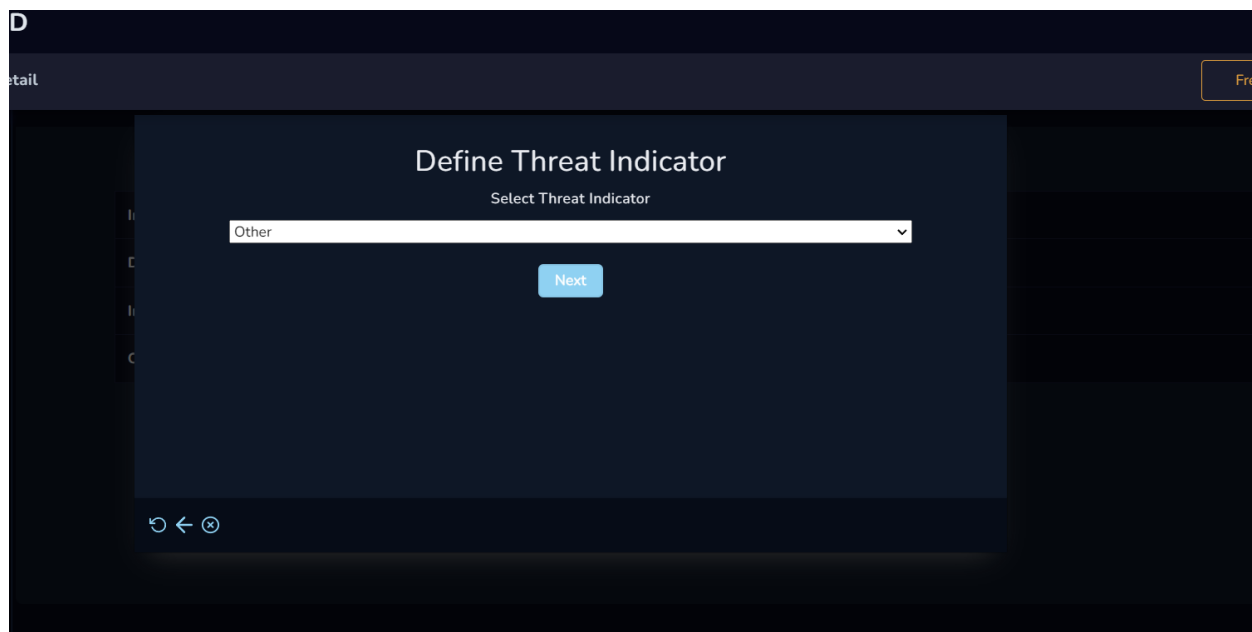
The screenshot shows the 'INVESTIGATION CHANNEL' tab with the same alert. The 'ACTION' column now shows a checkmark and a right arrow, indicating that the alert has been acknowledged or investigated.

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	May 23, 2021, 7:32 p.m.	SOC145 - Ransomware Detected	92	Malware	» ✓

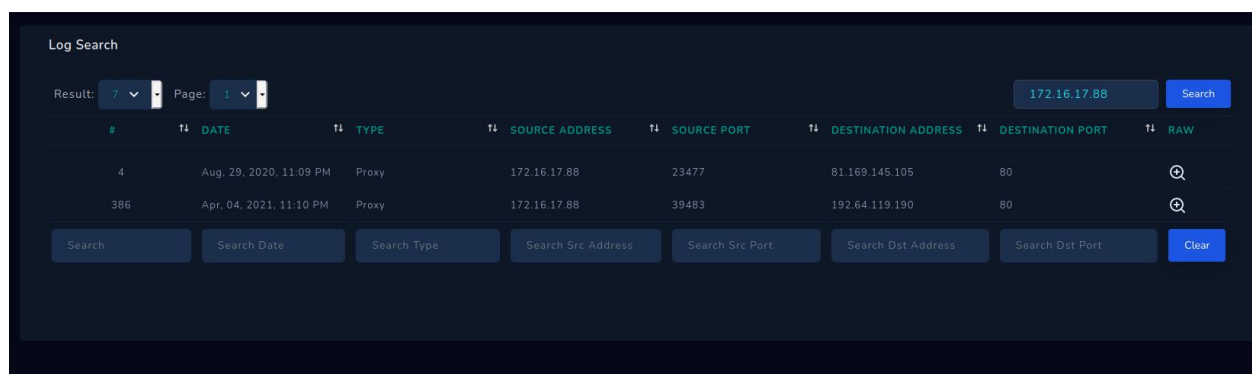
The screenshot shows the 'INVESTIGATION CHANNEL' tab with the same alert. A modal dialog is displayed over the alert, asking the user to 'Create case for EventID: 92'. The dialog includes a green checkmark icon, the text 'Click button and create case', and a 'Continue' button.

Create case for EventID: 92
Click button and create case
Continue

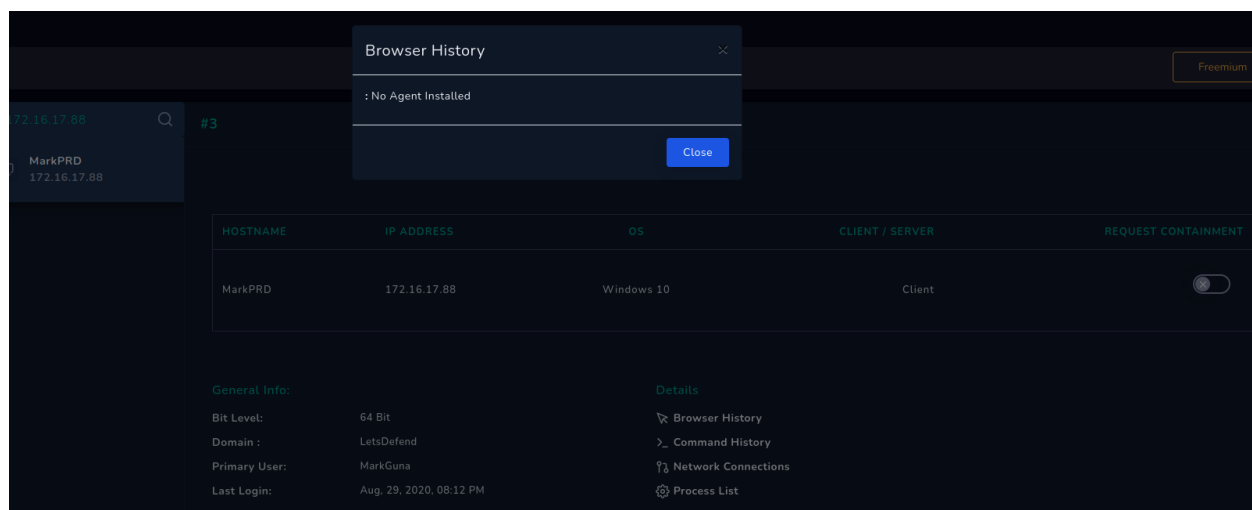
I have Took the ownership of that alert and started creating case. Which created a case.

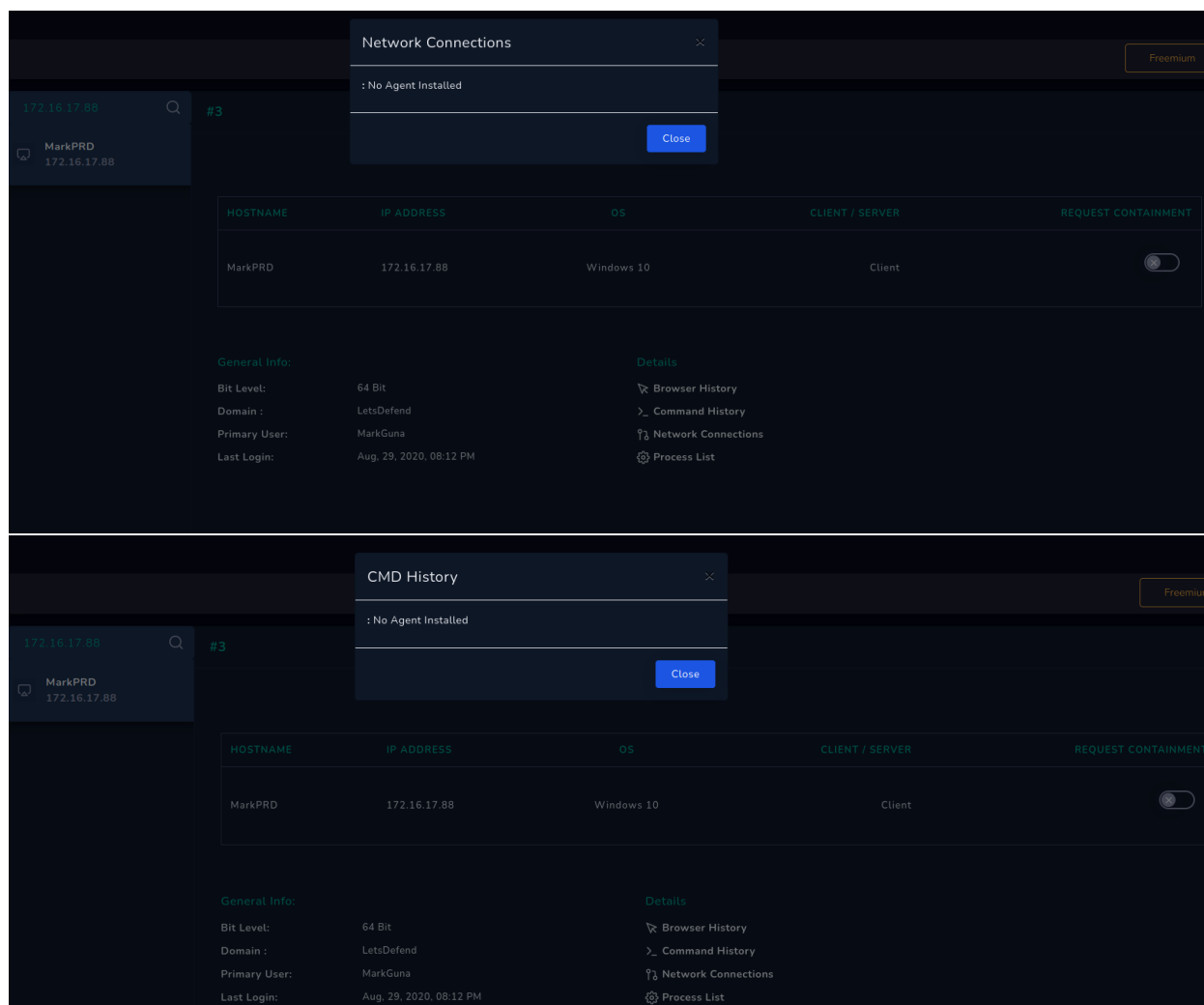


It asked me to define threat indicator, which I have set to others in the given options by checking source address in the Log management and Endpoint security.



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

60

/ 68

60 security vendors and 3 sandboxes flagged this file as malicious

taskhost.exe

calls-wmi checks-usb-bus detect-debug-environment direct-cpu-clock-access invalid-rich-pe-linker-version peexe runtime-modules

775.50 KB

Size

2021-12-30 07:32:07 UTC

27 days ago

EXE

Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Gen:Variant.Ransom.Avaddon.3	AhnLab-V3	Malware.Win.Ransom.R421765	
Alibaba	Ransom:Win32/Avaddon.4ec8f9e5	ALYac	Trojan.Ransom.Avaddon	
Antiy-AVL	Trojan/Generic.ASMalwS.3198A1A	Arcabit	Trojan.Ransom.Avaddon.3	
Avast	Win32.RansomX-gen [Ransom]	AVG	Win32.RansomX-gen [Ransom]	
Avira (no cloud)	HEUR/AGEN.1136765	BitDefender	Gen:Variant.Ransom.Avaddon.3	
BitDefenderTheta	Gen:NN.Zexof.34114.Wu0@o8mRu3ni	Bkav Pro	W32.AIDetect.malware2	
CAT-QuickHeal	Trojan.AvaddPMF.S20724522	ClamAV	Win.Ransomware.Avaddon-9852658-0	
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.050352	
Cylance	Unsafe	Cynet	Malicious (score: 100)	
Cyren	W32/Ransom.OS.gen/Eldorado	DrWeb	Trojan.MulDrop16.12853	

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

Incident Details

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 "Yes" if someone access the malicious address. Otherwise please click "No" button.

Accessed

Not Accessed

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

Log Search

Result: 7

Page: 1

172.16.17.88

Search

#	DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
4	Aug, 29, 2020, 11:09 PM	Proxy	172.16.17.88	23477	81.169.145.105	80	
386	Apr, 04, 2021, 11:10 PM	Proxy	172.16.17.88	39483	192.64.119.190	80	

Search

Search Date

Search Type

Search Src Address

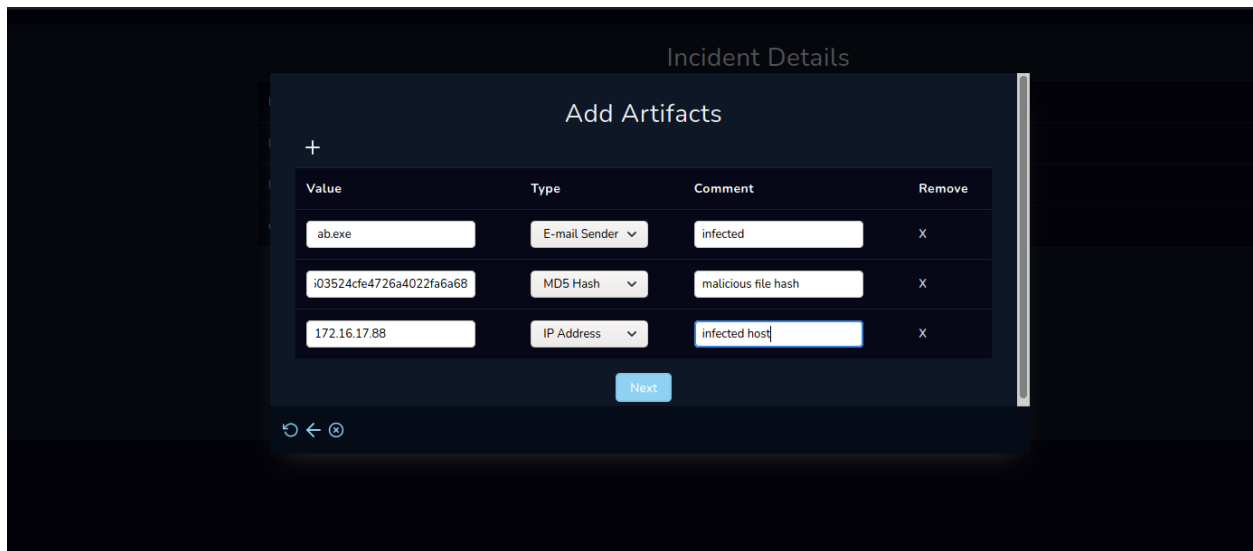
Search Src Port

Search Dst Address

Search Dst Port

Clear

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

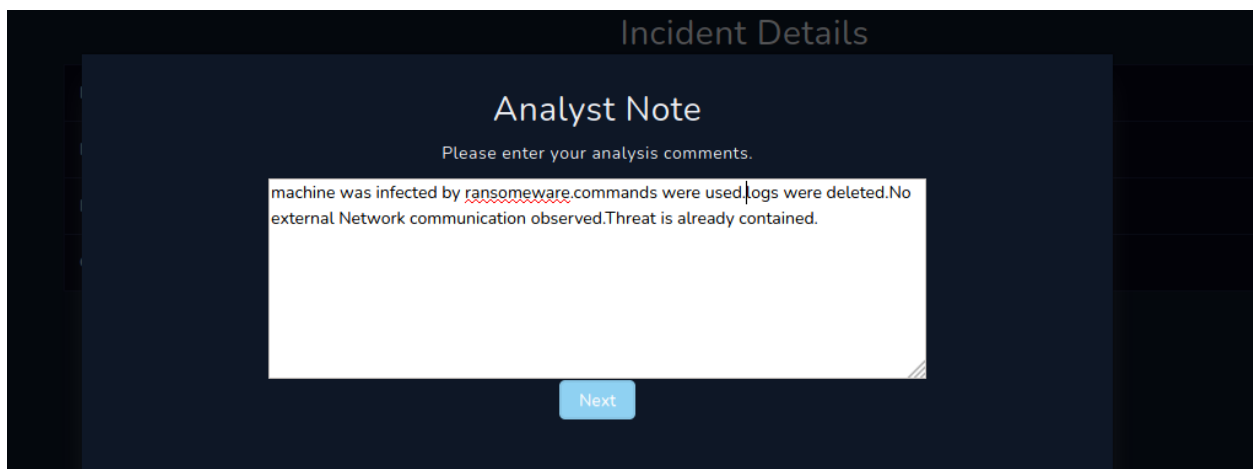


The 'Add Artifacts' dialog is shown with a table containing three rows of artifact data. Each row has a 'Value' field, a 'Type' dropdown, a 'Comment' field, and a 'Remove' button.

Value	Type	Comment	Remove
ab.exe	E-mail Sender	infected	X
03524cfe4726a4022fa6a68	MD5 Hash	malicious file hash	X
172.16.17.88	IP Address	infected host	X

A 'Next' button is located at the bottom right of the dialog.

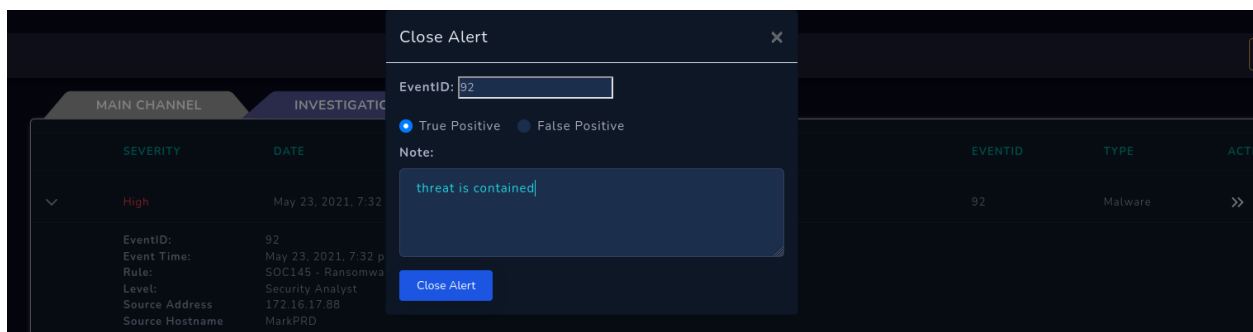
Then I added the artifacts as shown above.



The 'Analyst Note' dialog is shown with a text area containing the following text:

machine was infected by ransomware.commands were used.logs were deleted.No external Network communication observed.Threat is already contained.

A 'Next' button is located at the bottom right of the dialog.



The 'Close Alert' dialog is shown with a text area containing the following text:

threat is contained

A 'Close Alert' button is located at the bottom left of the dialog.

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

High

May 23, 2021, 7:32 p.m.

SOC145 - Ransomware Detected

92

Malware

EventID:

92

Event Time:

May, 23, 2021, 07:32 PM

Rule:

SOC145 - Ransomware Detected

Answer:

True Positive (+5 Point)

Playbook Answers:

Check if System Requested the C2 (+5 Point)

Analyze Malware (+5 Point)

Check if the malware is quarantined/cleaned (+5 Point)

Analyst Note:

commands used.threat is contained.

Editor Note:

It is True Positive alert, because ab.exe is ransomware and encrypted all files on the machine. There is no C2 address, if you do dynamic analysis, you can see how it is acting.

Rate this case

☆

Writeups

✍

Discussion

📄

Share your success on Twitter

🐦