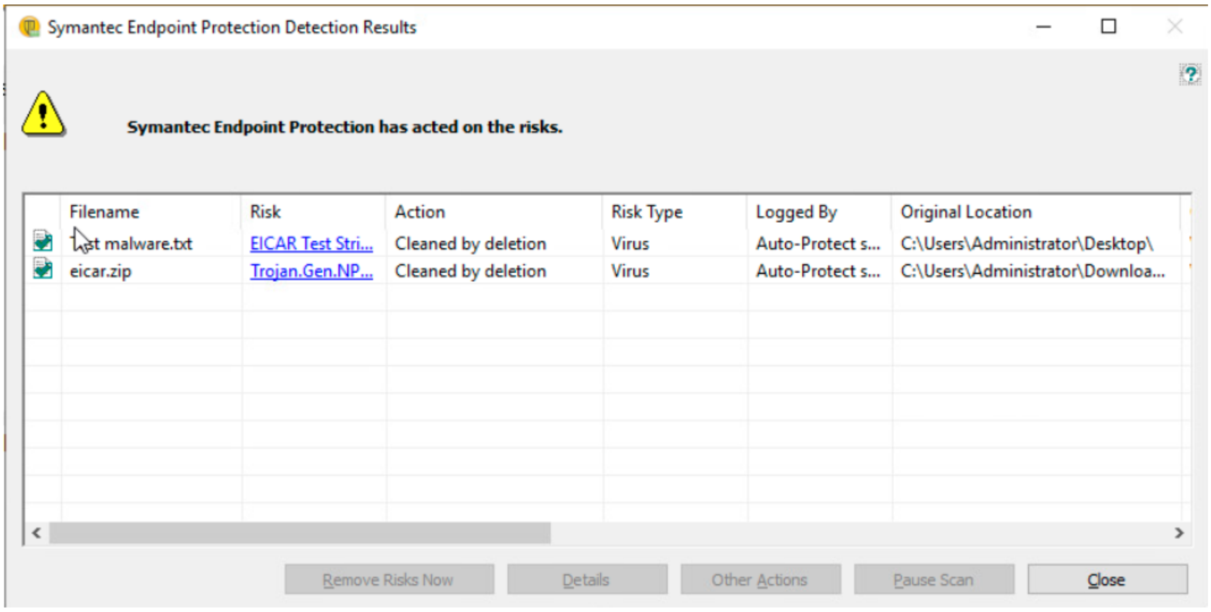
Threat intelligence using symantec

1. Open virtual box and run the windows 10 virtual machine

2. Fire-up the symantec Endpoint Protection manager Application on windows

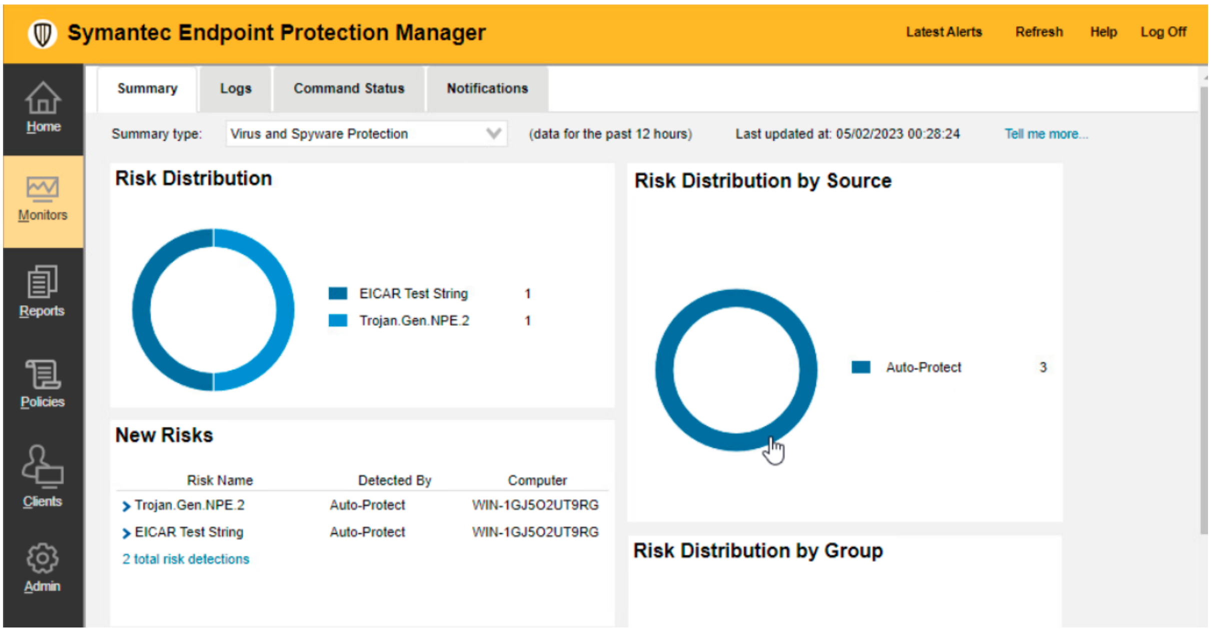
3. When the client gets affected by the malwares it automatically removes the malware and triggers the alert. For this lab download a sample virus from any website.



Symantec Endpoint Protection has acted on the risks.

Filename	Risk	Action	Risk Type	Logged By	Original Location
Test malware.txt	EICAR Test Stri...	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\Administrator\Desktop\
eicar.zip	Trojan.Gen.NP...	Cleaned by deletion	Virus	Auto-Protect s...	C:\Users\Administrator\Downloa...

4. Head over to the monitoring and select the summary to view the malware notification



Summary type: Virus and Spyware Protection (data for the past 12 hours) Last updated at: 05/02/2023 00:28:24

Risk Distribution

Risk Distribution by Source

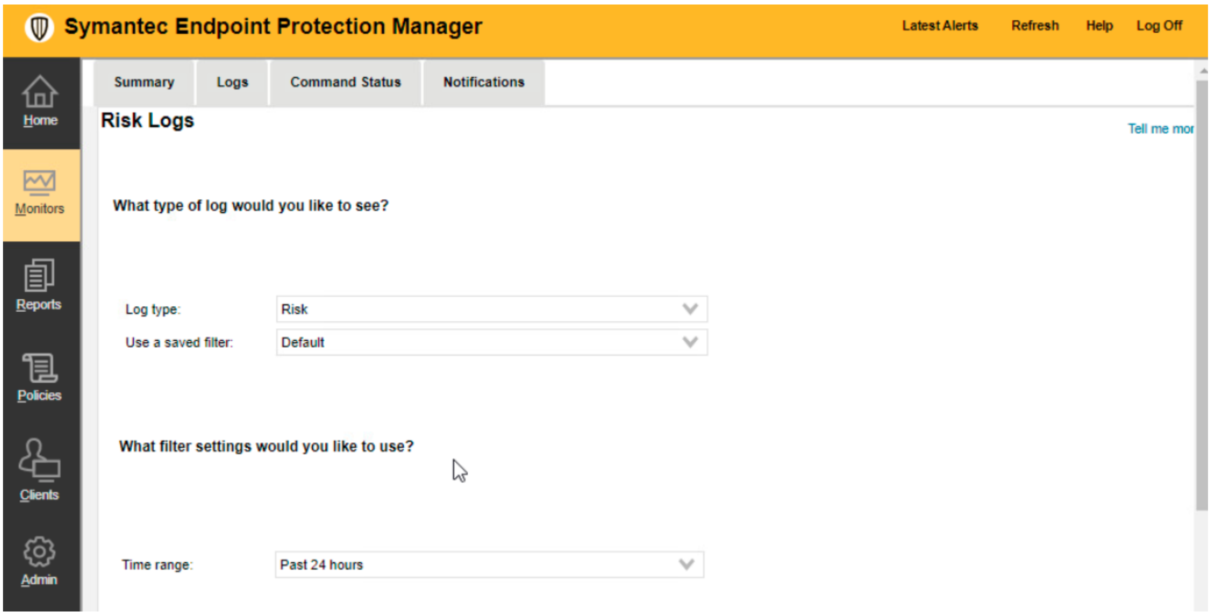
New Risks

Risk Name	Detected By	Computer
Trojan.Gen.NPE.2	Auto-Protect	WIN-1GJ5O2UT9RG
EICAR Test String	Auto-Protect	WIN-1GJ5O2UT9RG

2 total risk detections

Risk Distribution by Group

5. Select the log type to see
   Risk log
   - Log type- Risk
   - Use a saved filter - Default
   - Time range - Past 24 hours



Risk Logs

What type of log would you like to see?

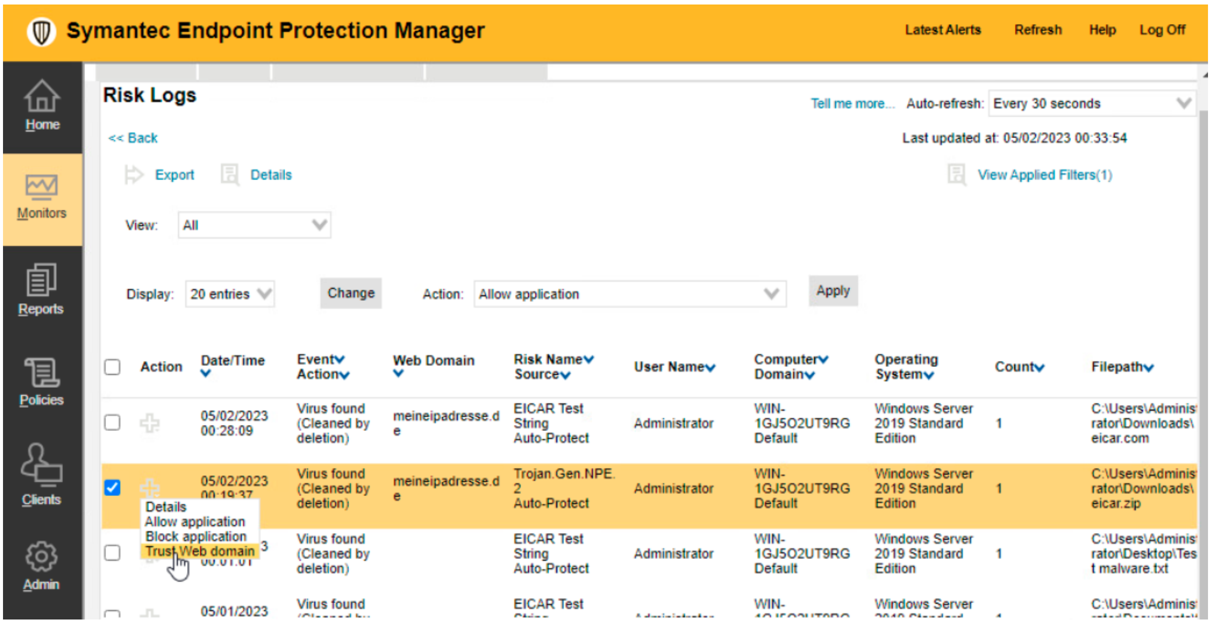
Log type: Risk

Use a saved filter: Default

What filter settings would you like to use?

Time range: Past 24 hours

6. Get the detailed report in logs and also you can take action accordingly.



Risk Logs

Auto-refresh: Every 30 seconds

Last updated at: 05/02/2023 00:33:54

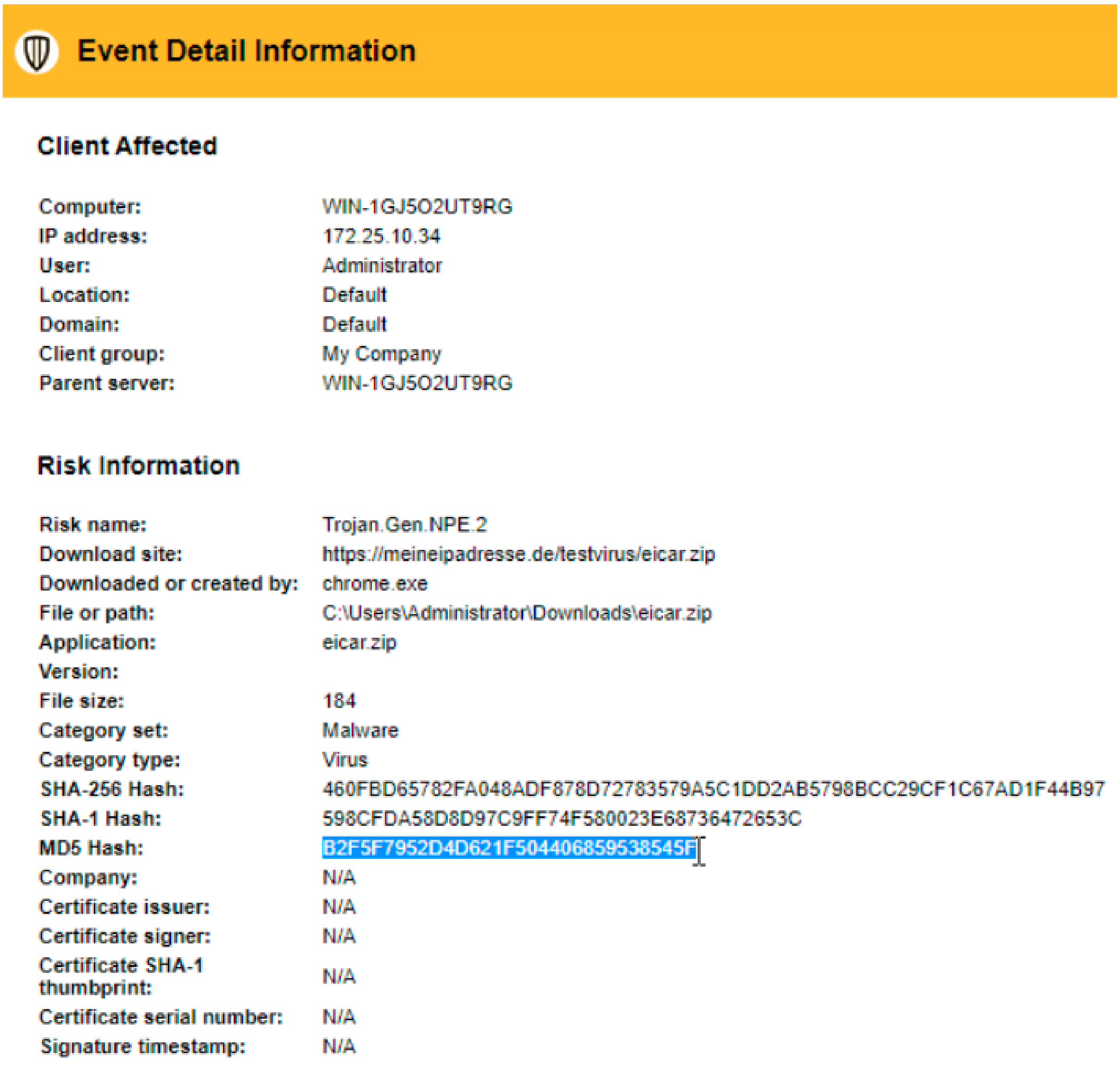
View: All

Display: 20 entries

Action: Allow application

□	Action	Date/Time	Event Action	Web Domain	Risk Name Source	User Name	Computer Domain	Operating System	Count	Filepath
□		05/02/2023 00:28:09	Virus found (Cleaned by deletion)	meineipadresse.de	EICAR Test String Auto-Protect	Administrator	WIN-1GJ5O2UT9RG Default	Windows Server 2019 Standard Edition	1	C:\Users\Administrator\Downloads\eicar.com
☑		05/02/2023 00:19:37	Virus found (Cleaned by deletion)	meineipadresse.de	Trojan.Gen.NPE.2 Auto-Protect	Administrator	WIN-1GJ5O2UT9RG Default	Windows Server 2019 Standard Edition	1	C:\Users\Administrator\Downloads\eicar.zip
□		3 00:01:01	Virus found (Cleaned by deletion)		EICAR Test String Auto-Protect	Administrator	WIN-1GJ5O2UT9RG Default	Windows Server 2019 Standard Edition	1	C:\Users\Administrator\Desktop\Test malware.txt
□		05/01/2023	Virus found		EICAR Test		WIN-	Windows Server		C:\Users\Adminis

7. You can view the full details of that alert. Copy the hash value of that file.



Event Detail Information

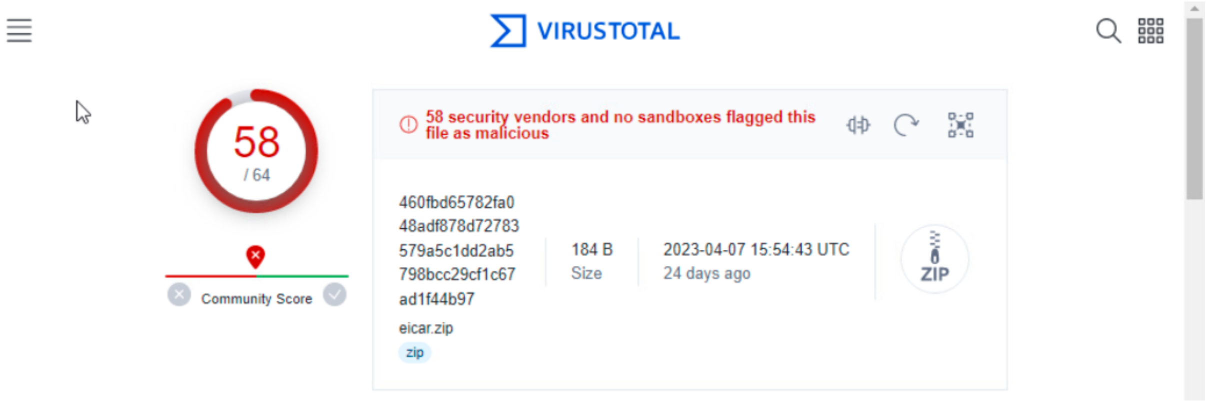
Client Affected

Computer:	WIN-1GJ5O2UT9RG
IP address:	172.25.10.34
User:	Administrator
Location:	Default
Domain:	Default
Client group:	My Company
Parent server:	WIN-1GJ5O2UT9RG

Risk Information

Risk name:	Trojan.Gen.NPE.2
Download site:	https://meineipadresse.de/testvirus/eicar.zip
Downloaded or created by:	chrome.exe
File or path:	C:\Users\Administrator\Downloads\eicar.zip
Application:	eicar.zip
Version:	
File size:	184
Category set:	Malware
Category type:	Virus
SHA-256 Hash:	460FBD65782FA048ADF878D72783579A5C1DD2AB5798BCC29CF1C67AD1F44B97
SHA-1 Hash:	598CFDA58D8D97C9FF74F580023E68736472653C
MD5 Hash:	B2F5F7952D4D621F504406859538545F
Company:	N/A
Certificate issuer:	N/A
Certificate signer:	N/A
Certificate SHA-1 thumbprint:	N/A
Certificate serial number:	N/A
Signature timestamp:	N/A

8. Search the hash value on virustotal.



58 security vendors and no sandboxes flagged this file as malicious

460fbd65782fa048adf878d72783579a5c1dd2ab5798bcc29cf1c67ad1f44b97

eicar.zip

zip

184 B
Size

2023-04-07 15:54:43 UTC
24 days ago