

Forum:[Hack Forums](#)

Thread: [Is there anyway to know if a computer is being monitored by EDR](#)

Skidsuper - October 17, 2024, 6:49 pm

EDR (Endpoint Detection and Response) is a cybersecurity solution that monitors and responds to threats on endpoints, such as computers or devices, in real-time. Does anyone know if there is a way to know if a computer that you are using is being monitored by EDR.

Charlie Sheen - October 17, 2024, 7:37 pm

Perhaps finding an unknown process in task manager. Monitor network traffic.

Pimping - October 17, 2024, 7:48 pm

I think you would know if an EDR is running on your pc as there is alerts
also EDRs are made for business/corporations and expensive. usually are not made for normal users

Riggs - October 17, 2024, 7:53 pm

A lot of EDR agents deployed on user devices are intentionally hidden from user view with tamper protection controls enabled. Depending on if you have local admin to the device, you could try looking in task manager, looking at running processes, or run Wireshark and look for any network comms coming to/from the EDR server to the agent. Maybe also the event viewer security logs.

Bastille - October 18, 2024, 1:35 am

Of course :

- check the appwiz.cpl
- check the registry :
 - > HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
 - > HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- check the running processes :
 - > process hacker
 - > process monitor (sysinternal)
 - > process explorer (sysinternal)
- Wireshark / Glasswire / Portmaster (for any network traffic)

Py_Dev - October 18, 2024, 1:01 pm

use process xp. Check for dll hooks.

Money- - October 19, 2024, 12:44 am

It really depends on what type of EDR though. They are many types out there. Some are even just honeypot setups and they have EDR configured to it too to test stuffs and all.

TheShadowArmy - November 10, 2024, 11:21 am

(Oct 17, 2024 06:49 PM)Skidsuper Wrote: [\[CITE\]](#) EDR (Endpoint Detection and Response) is a cybersecurity solution that monitors and responds to threats on endpoints, such as computers or devices, in real-time. Does anyone know if there is a way to know if a computer that you are using is being monitored by EDR.

I did some research and I found that if you are using Windows or Mac you can check your task manager for processes like:

csagent.exe, falconservice.exe for crowdstrike.

cb.exe, cbcomms.exe for carbon black

SentinelAgent.exe for SentinelOne.

MsSense.exe For MS Defender.

You can also check your network traffic for IP addresses associated with EDR with Win + R "resmon"

Look for the network tab and for the Process and Network Activity section and it should show process names along with their PID and their total network usage, you can then view the TCP Connections under the processes to see the IP, port and process names associated with that process, you should look for processes that I mentioned above by the way.

kazuma - November 11, 2024, 11:54 am

EDR really should get buzz word of the year. using wireshark would be the most basic way to try identify anything suspicious happening over the network.

Skidsuper - November 16, 2024, 7:49 am

(Nov 10, 2024 12:21 PM)TheShadowArmy Wrote: [\[CITE\]](#) I did some research and I found that if you are using Windows or Mac you can check your task manager for processes like:

csagent.exe, falconservice.exe for crowdstrike.

cb.exe, cbcomms.exe for carbon black

SentinelAgent.exe for SentinelOne.

MsSense.exe For MS Defender.

You can also check your network traffic for IP addresses associated with EDR with Win + R "resmon"

Look for the network tab and for the Process and Network Activity section and it should show process names along with their PID and their total network usage, you can then view the TCP Connections under the processes to see the IP, port and process names associated with that process, you should look for processes that I mentioned above by the way.

Thank you this could be helpful. Are there ways to install video games in the computer without alerting EDR.

DramaKing - November 16, 2024, 8:46 am

(Nov 16, 2024 08:49 AM)Skidsuper Wrote: [\[CITE\]](#) Thank you this could be helpful. Are there ways to install video games in the computer without alerting EDR.

EDR does not normally trigger alerts if video games are present.

Skidsuper - November 16, 2024, 11:22 am

(Nov 16, 2024 09:46 AM)DramaKing Wrote: [\[CITE\]](#) EDR does not normally trigger alerts if video games are present.

Does it not monitor every new software installed?

DramaKing - November 16, 2024, 6:17 pm

(Nov 16, 2024 12:22 PM)Skidsuper Wrote: [\[CITE\]](#) Does it not monitor every new software installed? I didn't say that EDR doesn't monitor and log software installations, just that it wouldn't generate alerts for legitimate software. Now if you're intending to game on a company computer, you have other things to worry about.

Lzz00 - December 9, 2024, 8:13 am

EDR does not normally trigger alerts if video games are present.