

Forum:[Hack Forums](#)

Thread: [Best Tools for Threat Detection?](#)

removingusername - January 18, 2025, 3:24 pm

Which tools do you prefer?

jcole - January 18, 2025, 3:28 pm

(Jan 18, 2025 04:24 PM)removingusername Wrote: [\[CITE\]](#) Which tools do you prefer?
I don't have an antivirus on my PC. I just rely on Window's and common sense

Bastille - January 19, 2025, 12:35 am

Threat detection is a domain which relies on many tools such as :

- EDR / XDR (Cortex, Cybereason, SentinelOne, CrowdStrike, ...)
- SIEM (Splunk, ELK, Qradar, ...)
- IDS / IPS (Suricata, Snort, ...)
- Firewall (Fortinet, PaloAlto, ...)
- Threat Intelligence Platforms - TIP (MISP, ...)
- ...

Maybe you meant malware detection ? Or something else ?

Py_Dev - January 19, 2025, 9:25 am

Procexp is all you really need tbh.

parkdrama - January 21, 2025, 5:59 am

(Jan 19, 2025 10:25 AM)Py_Dev Wrote: [\[CITE\]](#) Procexp is all you really need tbh.
if they malware or threat disguise itself as legitimate process?

Py_Dev - January 21, 2025, 9:54 am

(Jan 21, 2025 06:59 AM)parkdrama Wrote: [\[CITE\]](#) if they malware or threat disguise itself as legitimate process?

With process xp you can view the resources consumption and see dlls also has option to upload all hashes to virus total. Only thing is some people hide from proc xp task manager and such

ServersFxcked - January 28, 2025, 4:00 am

Yeah these days some sneaky methods