NUCLEON
AHEAD OF CYBER THREATS

Nucleon EDR | Endpoint Detection & Response

Datasheet

Security teams encounter various obstacles while attempting to identify, analyze, and address sophisticated attacks. These difficulties consist of inadequate insight into essential control points, laborious scouring of extensive and heterogeneous data sources devoid of context and association, weariness from alerts due to inadequate signal-to-noise ratios, and the complexity of rapidly curtailing the attack, leading to interruptions in critical business operations, diminished efficiency, and heightened operating expenses.

Comprehensive approach to cyber threat protection

Nucleon Detection & Response provides protection for workstations and servers.

- Set up of successive protection layers to protect you at all levels during an attack
- Identification of weak points in your infrastructure and systems
- Blocking attacks and providing a range of tools for investigation.

Protection adapted to your critical activities and data

Nucleon Detection & Response absorbs your internal uses and identifies your critical data to protect.

- Absorption of behaviors and uses to adapt security mechanisms.
- Automatic creation of specific protection rules, against illegitimate access, leakage and blocking by ransomware.

1 Prevention

System and application hardening.

2 Detection

Identification of new malicious strains using artificial intelligence

3 Response

Easier incident response thanks to on-board tooling

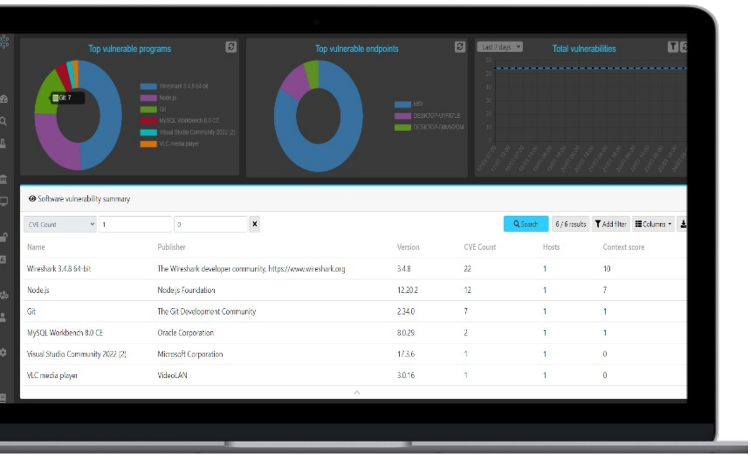
4 Remediation

Return to a resilient state after an attack

Identification of malicious behavior

Zero-Trust policies ensure that attack techniques used by hackers are blocked. Sensitive scripts and administration tools are not allowed in order to block complex infection processes and fileless attacks.

Network accesses are also restricted by policies to avoid abnormal accesses by abused softwares. For example, the Microsoft Office suite only has access to IPs and domains it needs to run and update.



Software vulnerability summary

CVE Count 1 0

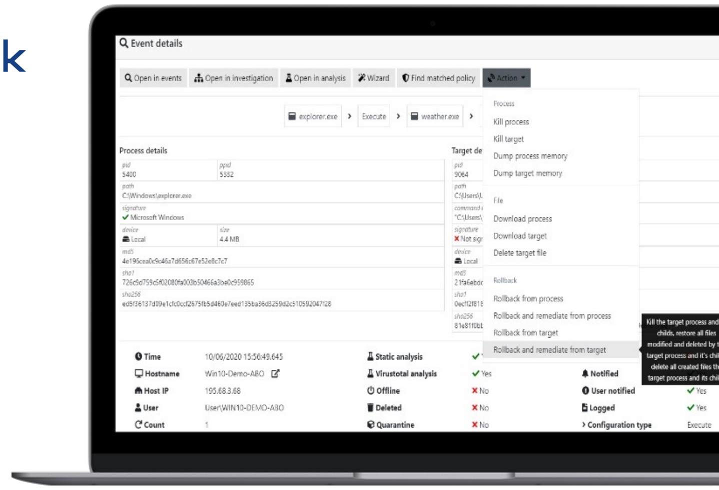
Name	Publisher	Version	CVE Count	Hosts	Context score
Wireshark 3.4.8 64-bit	The Wireshark developer community, https://www.wireshark.org	3.4.8	22	1	10
Node.js	Node.js Foundation	12.20.2	12	1	7
Git	The Git Development Community	2.34.0	7	1	1
MySQL Workbench 8.0 CE	Oracle Corporation	8.0.29	2	1	1
Visual Studio Community 2022 (2)	Microsoft Corporation	17.3.6	1	1	0
VLC media player	VideoLAN	3.0.16	1	1	0

Facilitated investigation

The centralized administration console provides all the tools to identify the source of a suspicious behavior. It is easy to understand the execution flow of a malware or even the one of a business software.

Remediation, isolation and Rollback

In case of data compromission by a malware, or simply by a user, data can be restored from the administration console. This feature always provides a last resort solution in case of a problem, and can be used natively without installing any additional components.



Kill the target process and childs, restore all files modified and deleted by target process and it's chi delete all created files th target process and its chi

Process details

pid 5400 | ppid 5332
path C:\Windows\explorer.exe
signature ✓ Microsoft Windows
device Local | size 4.4 MB
md5 4e196cea0c9c46a7d656c67e52e8c7c7
sha1 726c9d759c5f02080fa003b50466a3be0c959865
sha256 ed5f36137d09e1cfc0ccf2675fb5d460e7eed135ba36d3259d2c510592047f28

Target de

pid 9064
path C:\Users\
command "C:\Users\
signature ✗ Not sig
device Local
md5 21fa6ebd
sha1 0ecff2f81
sha256 81e81f0b

Time	10/06/2020 15:56:49.645	Static analysis	✓		
Hostname	Win10-Demo-ABO	Virustotal analysis	✓ Yes	Notified	
Host IP	195.68.3.68	Offline	✗ No	User notified	✓ Yes
User	User\WIN10-DEMO-ABO	Deleted	✗ No	Logged	✓ Yes
Count	1	Quarantine	✗ No	Configuration type	Execute

In case of detected suspicious behavior, the endpoint can be directly isolated from the network to prevent further damage. In addition, remediation also allows the machine to be cleaned automatically starting from the first action of the the attack.

Benefits

Comprehensive and simplified protection powerd by Zero-Trust

Real-time visibility of system and network activities

A sleek, lightweight agent that doesn't affect production and users' daily lives

Centralized console

Easy install

Cloud or On premise

Privacy