

Nucleon Detection 8 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



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.

Prevention

System and application hardening

Detection

Identification of new malicious strains using

Response

thanks to on-board tooling

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.

	irograms 🕄			C Last 7 days V		abilities 🖬 🕻
	Negrini 1.2.6.944 Vole ja Gr. MySo. Vistoecki 8.5.C5 Mysii blace Comment 2022 (2) M.C. meda jäyje		Lai Desitor-Urret Cesitor-Ourg			
 Software vulnerability summary 						
CVE Count Y 1	0 ×			Q Sourd	6 / 6 results	🕇 Add filter 🛛 🖬 Columns 🔹 🛓
Name	Publisher		Version	CVE Count	Hosts	Context score
Wireshark 3.4.8 64-bit	The Wireshork developer community, http://www.uki.com/	ps://www.wiresherk.org	3.4.8	22	1	10
Nodejs	Node is Foundation		12.20.2	12	1	7
Git	The Git Development Community		234.0	7	1	1
	Oracle Corporation		8.0.29	2	1	1
MySQL Workbench 8.0 CE					1	0
MySQL Workbench 8.0 CE Visual Studio Community 2022 (2)	Microsoft Corporation		17.3.6	1	1	
·	Microsoft Corporation VideoLAN		17.3.6 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.

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.

Q Open in events	A Open in investigation	A Open in analysis R Wizard O Find matched p			hed policy	d palicy 🕐 Action *				
		explorer.exe	> Exec	ute >	e weathe		Frocess Kill process Kill target			
Process details					Target de	Dump process memo	ary .			
ptd 5400	5382	ppid 5382					Dump target memory	y		
path C:Windowslampleter.avo Sonatum						path C3(Users\), command i	S(Jaans)). File			
≪ Microsoft Windows					"CAUsers)	Download process				
device Local	500 4.4 MB					signature X Nat sign	Download target			
md5 4e195cea0c9c45a7d656	m5 4e195ca8kde46a76556c87e52e8c7c7						Delete target file			
10/ 726/567595/K02080%003b50466a3b40c959865					mdS 21faEebor	Rollback				
shu256 ed5/26137d39e1ctc0cct2675fs5d460e7eed1355ba56d52550d2c510592047f28					sto1 Oect12f818					
					10256 81e811068	Rollback and remediate from process		Kill the target process		
						o reprised	Rollback from target		childs, restore all	
0 Time	10/06/2020 15:56:49:64	0/06/2020 15:56:49:645		A Static analysis		1	Rollback and remediate from target		modified and deleted target process and it's	
🖵 Hostname	Win10-Demo-ABO		₫	Virustot	tal analysis	~	es	& Notified	delete all created fil target process and it	
A Host IP	195.68.3.68	3.68		() Offline		×N	0	O User notified	✓ Ye	
🛓 User	User/WIN10-DEMO-A80			Deleted		×N	0	Logged	✓ Ye	
C Count 1		C Quarantine		×N	0	> Configuration ty	e Execut			



Centralized console

Cloud or On premise

Respect for personal data

000 NUCLEON

Easy install