



Nucleon

Protect data that matter

Endpoint Prevention Detection and Response Platform



À Propos de Nucleon Security



2018
1^{er} EDR
Zero-Trust



+15k
Malwares
par jour



+1,5 Md
Évènements
par jour



9
pays





Quelques Références



Royaume du Maroc
Ministère de l'Équipement et de l'Eau
Direction Générale de l'Hydraulique





Vos Enjeux Cybersécurité

Augmentation continue des cyberattaques



Manque de professionnels de la cybersécurité



Complexité des solutions de détection



Ransomware
ont augmenté de 105 % par rapport à l'année précédente et sont en hausse de 232 % depuis 2019.

Sonicwall



Il y a une pénurie de plus de 3 millions de professionnels de la cybersécurité dans le monde.

World Economic Forum



89% des solutions disposent de commentaires négatifs sur le volet utilisation

Gartner

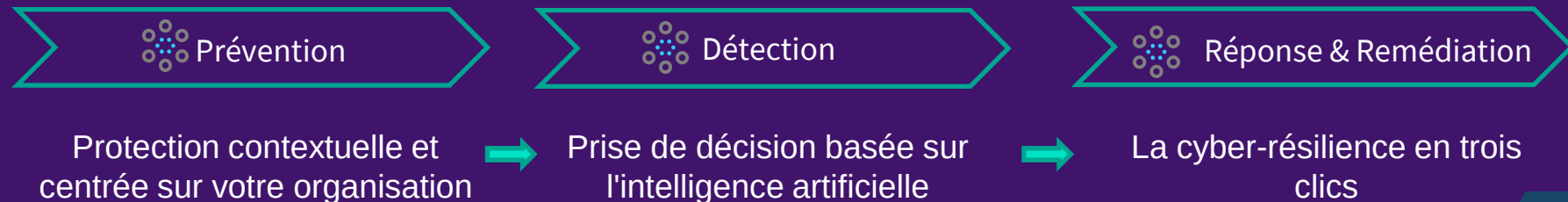
Les cybercriminels ont encore un grand avenir devant eux





Notre proposition de valeur

Une cybersécurité renforcée pour les équipes débordées





Le Paradigme Nucleon Smart Endpoint

1 Prévention

Durcissement du système et des applications

Multi-Layer
Zero-Trust



Machine
Learning engine

2 Détection

Identification des nouvelles souches malveillantes grâce à l'intelligence artificielle



Deep logging &
Remote actions

3 Réponse

Réponse aux incidents facilitée grâce à de l'outillage embarqué



System cleaning
and Rollback

4 Remédiation

Revenir à un état résilient suite à une attaque



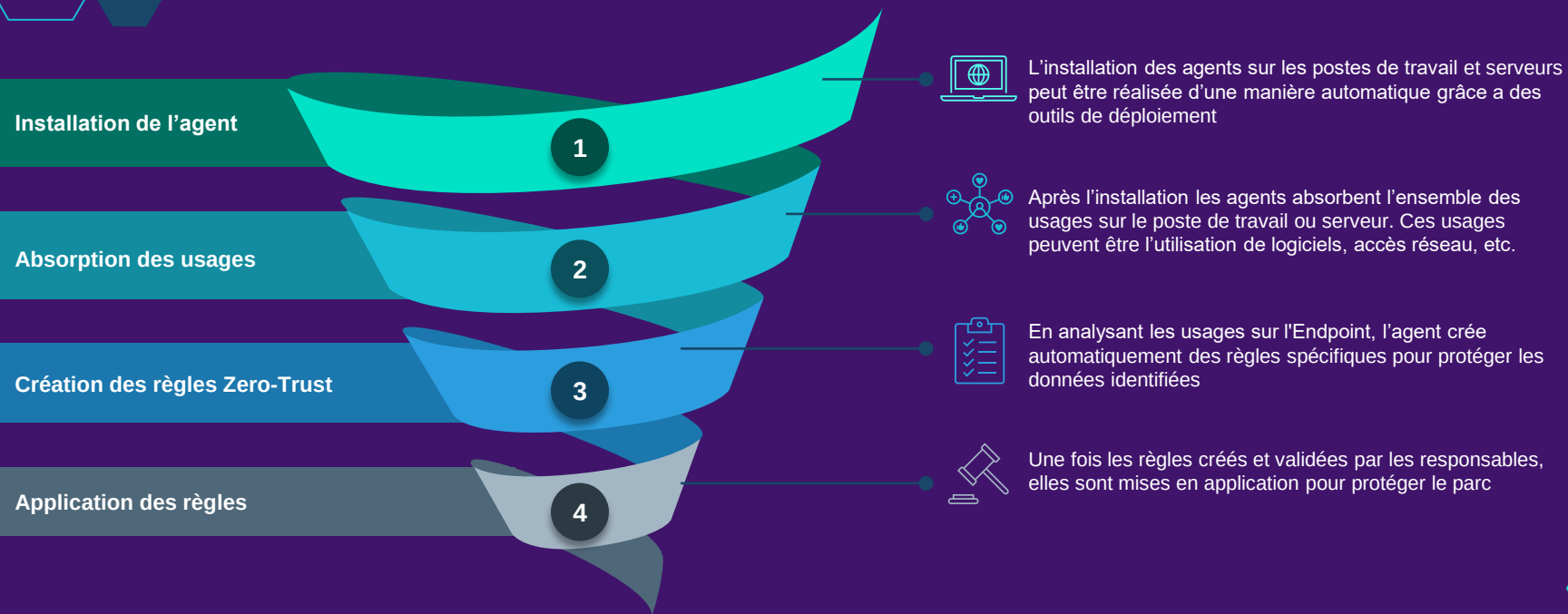


1

Prévention

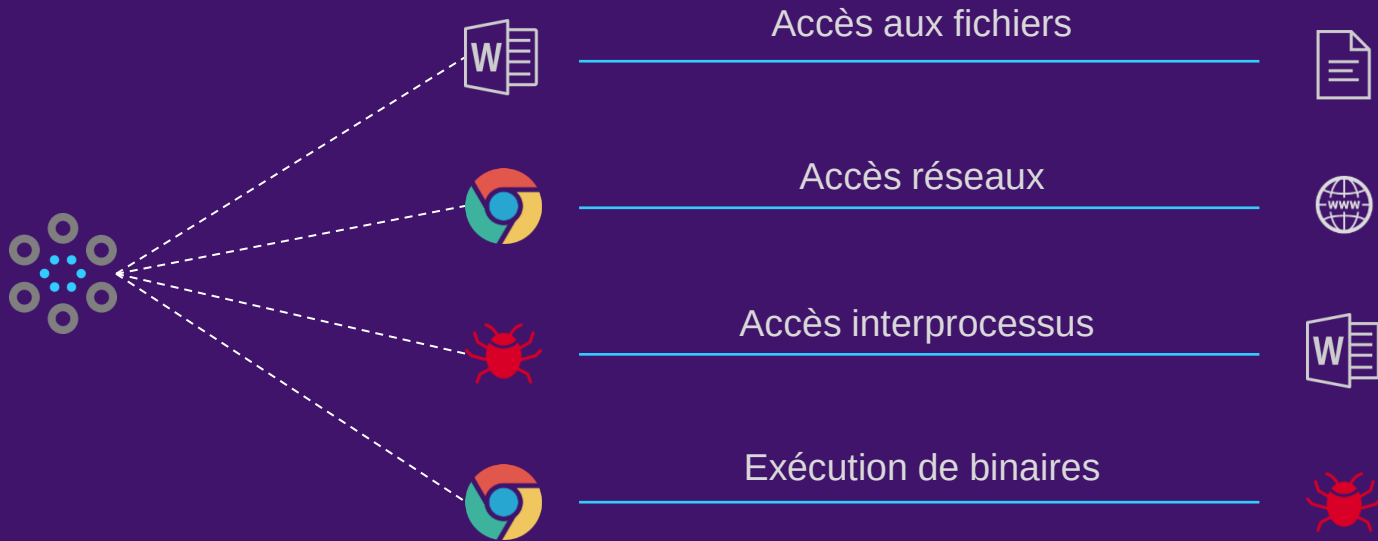
Durcissement du système et des applications

Absorption des usages internes





Les règles Multi-Layer Zero-Trust



Source	Type	Target	Action	Options
× Explorer × Keepass	× Read × Write	× Keepass Files	✓ Allow	🔊 🔒 ✓ 🔔 💬
× Any	× Read × Write	× Keepass Files	✗ Block	🔊 🗑️ 🕒 🔔 💬





Les règles Multi-Layer Zero-Trust

Quelques cas d'usages spécifiques



Maitrise
des
supports
amovibles



Maitrise
du
stockage
cloud



Maitrise
du
stockage
partagé



Sécurisation
des
développem
ent interne





2

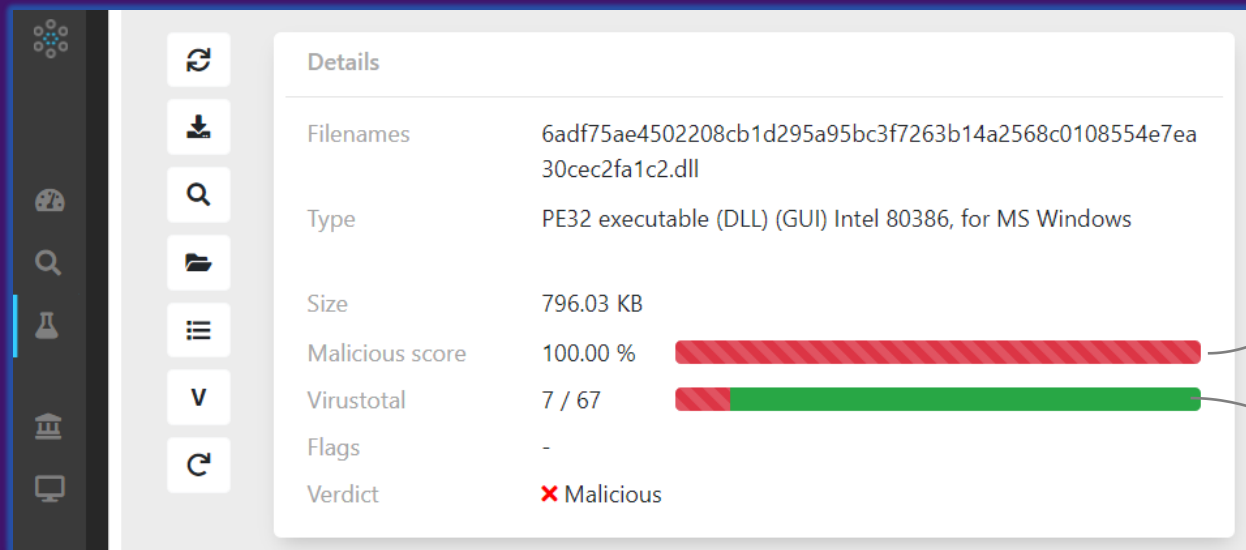
Détection

Identification des nouvelles souches malveillantes grâce à l'intelligence artificielle



Moteur Machine Learning & Corrélation

Un taux de detection exceptionnel



Nucleon Security IA

Autres solutions





3

Réponse

Réponse aux incidents facilitée grâce à de l'outillage embarqué



Hunting

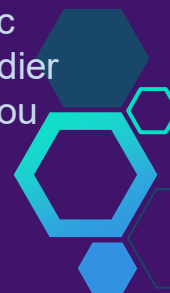
Date	Host	Type	Process	Target	Action
02/11/2020 15:34:12.934	Nucleon-ZenBook-ABO	Execute	C:\Windows\explorer.exe	C:\Users\Antoine\Desktop\mimikatz_trunk\x64\mimikatz.exe	❌ Block

Context information		Process details		File details	
	Hostname	Nucleon-ZenBook-ABO	PID	7300	
	User	Antoine\NUCLEON-ZENBOOK	PPID	6676	
	Host IP	88.138.20.156	Path	C:\Windows\explorer.exe	
	Time	02/11/2020 15:34:12.934	Signature	✔ Microsoft Windows	
	Count	1	Device	🖨 Local	
	Type	Execute	Size	4.41 MB	
	Action	❌ Block (Denied by analysis engine)	md5	800ef617dd...0e0ec39cc6	
	Notified	✔ Yes	sha1	aaactf0817...02af40c145	
			sha56	100f6ab273...a62e77f65b	

	PID	5812
	Path	C:\Users\Antoine\Desktop\mimikatz_trunk\x64\mimikatz.exe
	Command	"C:\Users\Antoine\Desktop\mimikatz_trunk\x64\mimikatz.exe"
	Signature	✔ Open Source Developer, Benjamin Delpy
	Device	🖨 Local
	Size	1.18 MB
	md5	a3cb3b02a6...8a9a5c9e07
	sha1	d241df7b9d...e27cc40fa4
	sha256	31eb1de7e8...01d539a0fc

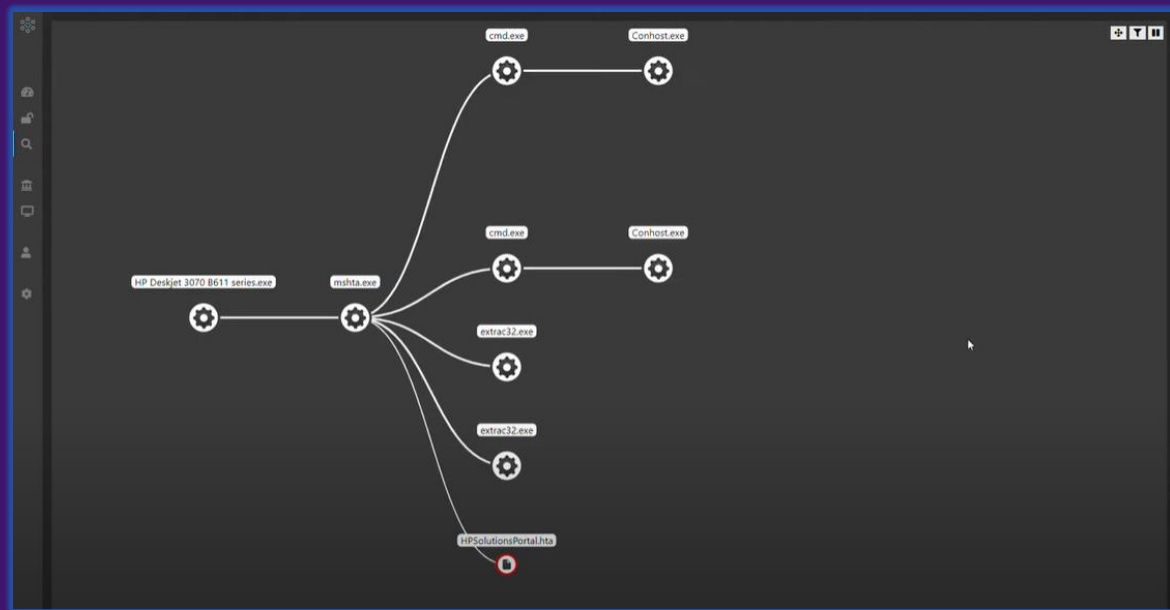
Chaque événement intercepté sur l'Endpoint est stocké sur le serveur (sur site ou cloud) dans une base de données non relationnelle.

Cette base de données peut être interrogée avec plusieurs filtres pour étudier un événement système ou réseau.





Nucleon Execution Tree

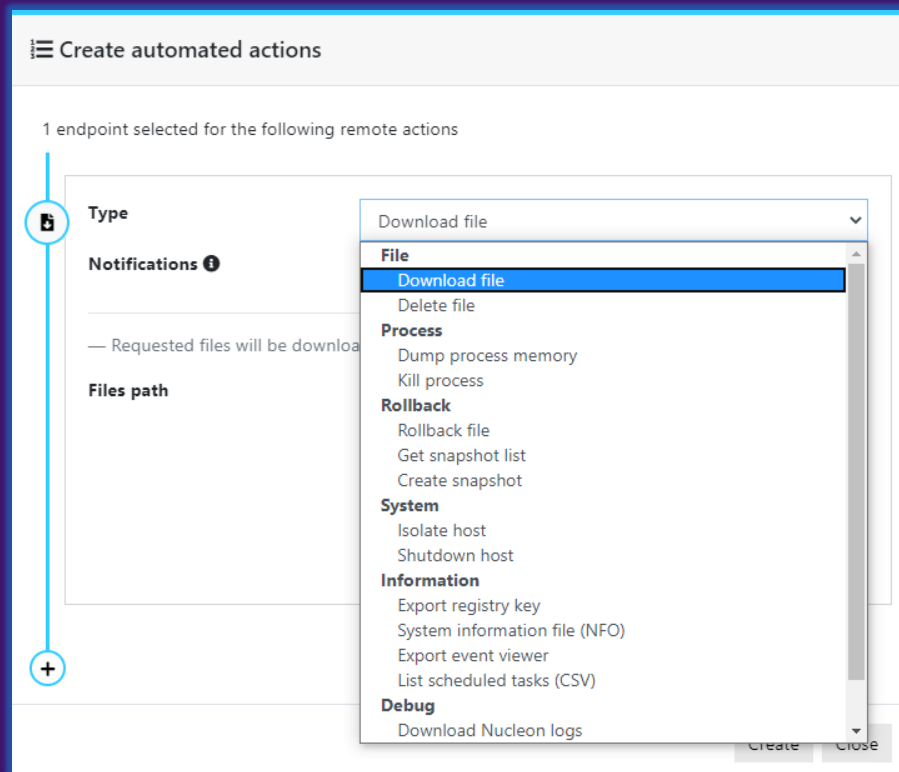


La connaissance détaillée de tous les événements (Deep Logging) permet de créer facilement un arbre d'exécution visuel afin de faciliter toutes les actions d'investigation.





Nucleon Remote Actions



Nucleon Smart Endpoint permet à l'administrateur d'exécuter des commandes à distance sur un ou plusieurs postes de travail ou serveurs.

Ces actions à distance peuvent être réalisées dans un but d'investigation approfondie ou pour remédier à une attaque.





4

Remédiation

Revenir a un état résilient suite a une attaque

System Cleaning and Rollback

Q Event details

Q Open in events | Open in investigation | Open in analysis | Wizard | Find matched policy | Action

explorer.exe > Execute > weather.exe >

Process details

pid	ppid
5400	5332
path C:\Windows\explorer.exe	
signature ✓ Microsoft Windows	
device	size
Local	4.4 MB
md5 4e196cea0c9c46a7d656c67e52e8c7c7	
sha1 726c9d759c5f02080fa003b50466a3be0c959865	
sha256 ed5f36137d09e1cfc0cf2675fb5d460e7eed135ba36d3259d2c510592047f28	

Target details

pid	path
9064	C:\Users\U
command l	
~C:\Users\	
signature	Not signed
device	Local
md5	21fa6ebdc
sha1	0ecff2f81e
sha256	81e61f0bb

Action

- Process
- Kill process
- Kill target
- Dump process memory
- Dump target memory
- File
- Download process
- Download target
- Delete target file
- Rollback
- Rollback from process
- Rollback and remediate from process
- Rollback from target
- Rollback and remediate from target

Time 10/06/2020 15:56:49.645

Hostname Win10-Demo-ABO

Host IP 195.68.3.68

User User\WIN10-DEMO-ABO

Count 1

Static analysis ✓ Yes

Virustotal analysis ✓ Yes

Offline ✗ No

Deleted ✗ No

Quarantine ✗ No

Notified

User notified ✓ Yes

Logged ✓ Yes

Configuration type Execute

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

À partir de n'importe quel événement, un système peut être restauré à un état antérieur.

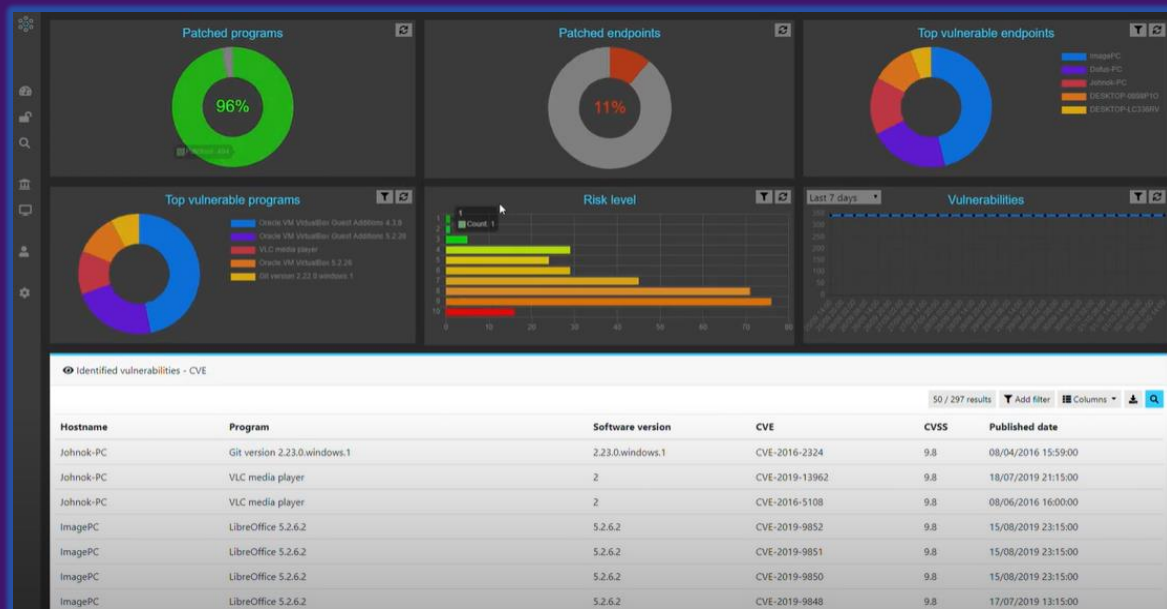




5

Fonctionnalités additionnelles

Gestion des vulnérabilités

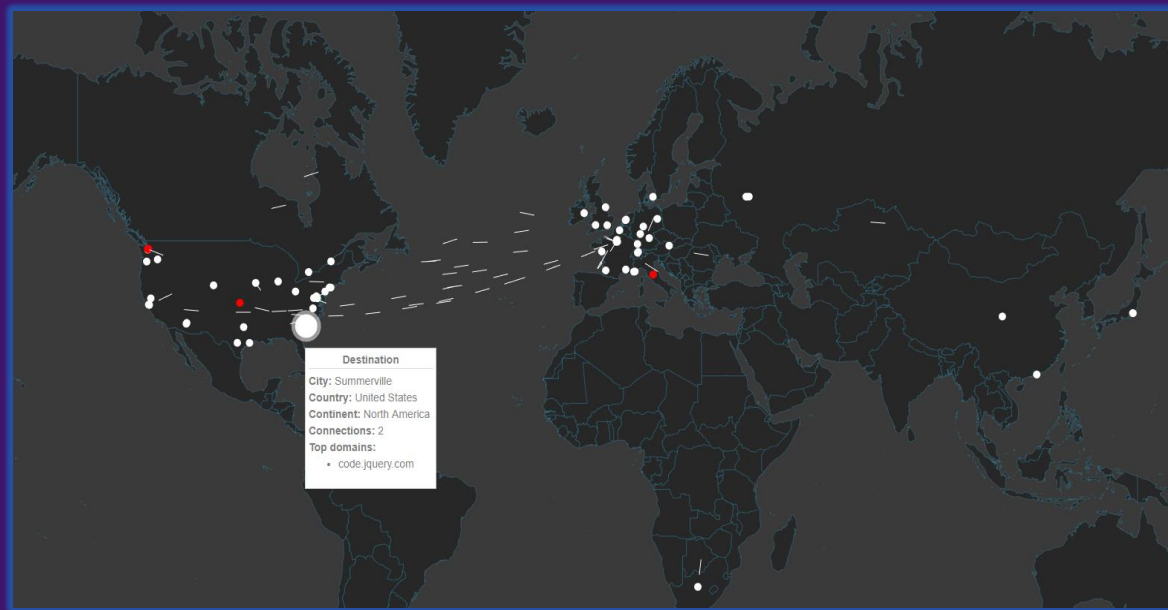


Nucleon Smart Endpoint met en corrélation les versions logicielles et la base de données CVE pour informer l'administrateur dès qu'une nouvelle vulnérabilité est détectée sans aucune planification d'analyse.





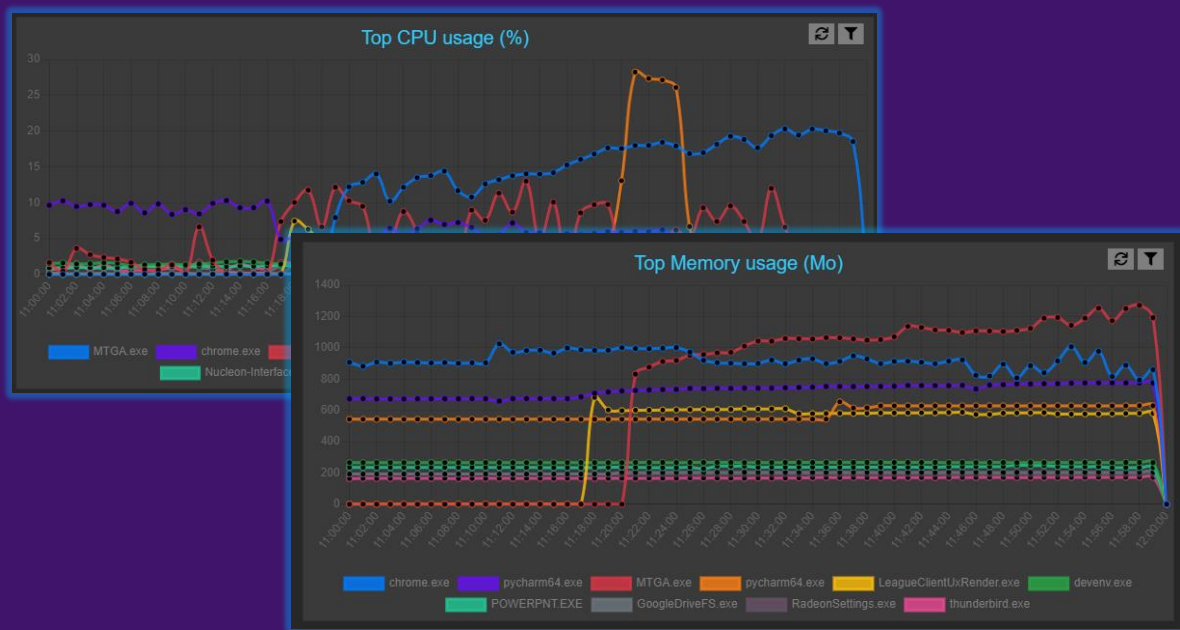
Live Map



Les événements réseaux sont interceptés et géolocalisés, une carte du monde permet de visualiser les connexions réseau en temps réel.



Endpoint Infrastructure Metrics



Les agents collectent des métriques de chaque processus en cours afin de détecter une utilisation anormale des ressources.

Ces statistiques peuvent être utilisées pour détecter des menaces de type crypto-miner.





Contacts

Sales



Sales@nucleon-security.com

Tech Team



Team@nucleon-security.com

