

Nucleon
Protect data that matter

Nucleon Detection & Response

Datasheet

Approche complète de protection contre les cybermenaces

Nucleon Detection & Response assure la protection des postes de travail et des serveurs.



Mis en place des couches de protection successives pour vous protéger à tous les niveaux lors d'une phase d'attaques.



Identification des points faibles présents sur vos infrastructures



Bloque les attaques et mets à votre disposition tous les outils pour investiguer.

Protection adaptée à vos activités et données critiques

Nucleon Detection & Response absorbe vos usages internes, et identifie vos données critiques à protéger.



Création automatique des règles de protections spécifiques



Elles vont vous offrir une protection de vos données critiques contre tout accès illégitime, fuite et blocage par un ransomware.

1

Prévention

Durcissement du système et des applications

2

Détection

Identification des nouvelles souches malveillantes grâce à l'intelligence artificielle

3

Réponse

Réponse aux incidents facilitée grâce à de l'outillage embarqué

4

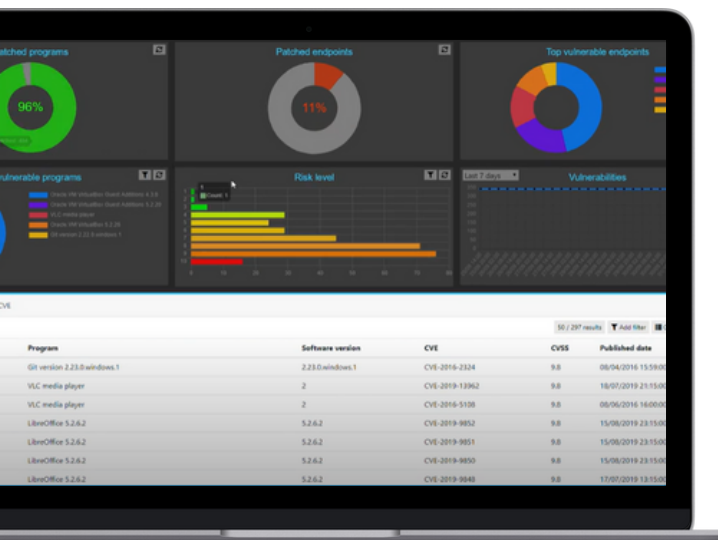
Remédiation

Revenir à un état résilient suite à une attaque

Identification des comportements malveillants

Les politiques Zero-Trust assurent le blocage des techniques d'attaque utilisées par les pirates. Les scripts et outils d'administration sensibles ne sont pas autorisés afin de bloquer les processus d'infection complexes et les attaques « fileless ».

Les accès réseau sont limités également par les politiques afin d'éviter des accès anormaux par des logiciels qui seraient abusés. Par exemple la suite Microsoft Office n'a accès qu'aux serveurs et domaines dont elle a besoin pour fonctionner par défaut.

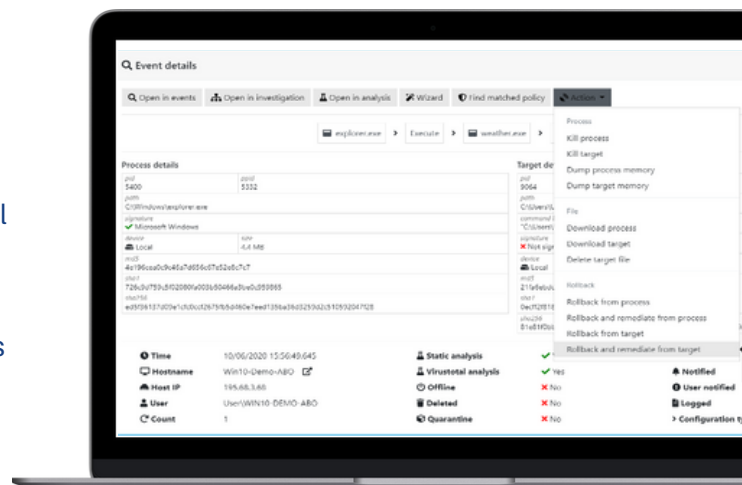


Investigation facilitée

La console d'administration centralisée met à disposition tous les outils pour identifier la source d'un comportement suspect. Il est simple de comprendre le flux d'exécution d'un logiciel malveillant ou même d'un logiciel métier.

Remédiation, isolation et Rollback

En cas de compromission des données par un logiciel malveillant, ou simplement par un utilisateur, les données peuvent être restaurées depuis la console d'administration. Cette fonctionnalité assure toujours une solution de dernier recours en cas de problème et de manière native sans installer de composant annexe.



En cas de comportement suspect détecté, là où les machines peuvent être directement isolées du réseau pour prévenir tout autre dégât. De plus, la remédiation permet également de nettoyer automatiquement la machine depuis la première action de l'attaque.

Avantages



Protection complète et simplifiée autour des politiques Zero-Trust



Visibilité en temps réel des activités système et réseau



Un agent épuré et léger qui n'affecte pas la production et le quotidien des utilisateurs



Console centralisée



Déploiement rapide



Cloud ou On premise



Respect des données personnelles