V. 1.0. 2023

NANO CORP.

NANO Corp. vs. Suricata

www.nanocorp.fr

Introduction

Dans un environnement où la cybersécurité évolue rapidement, il est essentiel de disposer du NDR le plus efficace. Comparer Suricata et n.Scope NDR permet aux utilisateurs d'évaluer leurs capacités respectives, et suggère déjà que n.Scope offre des fonctionnalités supérieures.

À propos de NANO CORP.

Armé d'une technologie brevetée, le n.Scope NDR de NANO Corp. combine l'intelligence des réseaux et de la cybersécurité, offrant une capacité d'analyse supérieure par rapport aux solutions concurrentes. Cette prouesse technique permet d'identifier avec une précision inégalée les menaces les plus insaisissables, redéfinissant ainsi les normes d'excellence dans le domaine de la sécurité des réseaux.

À propos de Suricata

Suricata est une technologie inventée dans les années 2000, une époque où la cybersécurité n'était pas confrontée au chiffrement des données. Comparer Suricata à n.Scope NDR n'est pas toujours simple, car ils peuvent sembler très similaires, mais Suricata est une technologie imparfaite qui n'est ni précise ni évolutive.

Données clés

Suricata

42

Nombre de protocoles réseau que Suricata est capable d'analyser

70 %

Taux de faux positif à la classification, entraînant un taux de détection de menaces faussement positives encore plus élevé

10 Gbit/s

Bande passante que les solutions Suricata cherchent à atteindre, mais elles y échouent régulièrement, tout en utilisant des équipements dédiés et coûteux

NANO CORP.

+120

Nombre de protocoles réseau que le n.Scope NDR est capable d'analyser, conduisant à une meilleure observabilité et une détection plus fine des menaces.

0.01%

Taux de faux positif à la classification, conduisant à un taux de détection des menaces faussement très faible.

100 Gbit/s

Bande passante que le n.Scope NDR peut atteindre avec une empreinte très légère, sans perte de trafic ni d'observabilité.

C'est également…

Suricata est très gourmand en termes de ressources, entraînant des problèmes de performance qui réduisent l'observabilité (en abandonnant le trafic chiffré) et un taux élevé de faux positifs. De plus, il nécessite davantage de configurations et de mises à jour, ajoutant de la complexité en matière de sécurité pour les utilisateurs moins expérimentés.

Table comparaison

Couverture réseau

	Suricata	Nano Corp.
Sonde physique	+ Adapté uniquement pour un déploiement sur machine physique, on-premise	++ Peut être installé sur des équipements standards pour de bien meilleures performances
Sonde Virtuelle (Machine Virtuelle)	- Très difficile à déployer dans un Hyperviseur. Nécessite beaucoup de 'bidouilles' et reste difficilement maintenable	++ Déployable dans tous les environnements hypervisés
Sonde Cloud	- N'est pas disponible sur les plateformes cloud.	++ Peut être installé dans le cloud (AWS, GCP, etc.) avec de bien meilleures performances
Déploiement	- Nécessite une compilation des binaires sur le matériel, avec beaucoup de configuration manuelle, même en entreprise	+ Logiciel entièrement packagé, déployable en quelques minutes partout dans le monde.
Compatibilité	+ Peut avoir des problèmes avec certains équipements standards, mais fonctionnera sur de nombreux OS	+ Fonctionne sur la plupart des matériels, compatible avec de nombreux OS et kernels Linux. Facilement redéployable sur de nouveaux matériels.

Deep Observability

Protocole de tunnels	+ Support limité des tunnels (MPLS, GRE, etc..)	++ Supporte davantage de protocoles de tunnel
Support de protocoles réseau	- Supporte 2,5 fois moins de protocoles que le n.Scope NDR et peut mettre des années à en supporter d'autres.	+ Supporte 120+ protocoles et est régulièrement mis à jour. Ce qui le rend supérieur pour de l'observabilité.

Le saviez-vous ?

Non évolutif

Sans une interface unique capable de gérer plusieurs sondes à la fois, les solutions basées sur Suricata sont souvent inadaptées aux grandes entreprises, centres de données ou FAI qui auraient besoin de piloter plusieurs sondes.

Le saviez-vous ?

Aveugle

Alors que Suricata ferme les yeux sur les menaces sur les données réseau cryptées (manquant entre 40 et 95% du trafic), n.Scope NDR extrait et enrichit consciencieusement toutes les métadonnées des protocoles chiffrés.

	Suricata	Nano Corp.
Empilement de protocoles	+ Support limité avec de très grandes baissse de performance. Ce qui rend impossible d'utiliser Suricata en Data Center	++ Haut support de l'empilement de protocoles pour les réseaux complexes. Idéal pour les réseaux haut-débit
Traitement du trafic chiffré	- Faible support du chiffrement, Suricata abandonne le traffic chiffré, qui représente parfois 95% du trafic réseau	+ Fort support du chiffrement, le n.Scope supervise et inspecte tous les flux chiffrés
JA3/JA3S	+ Supporte JA3/JA3S avec des services supplémentaires payants	+ Supporte pleinement JA3/JA3S.
Couverture d'attaque		
Approche de détection	-- Utilise la détection par signature, une technologie obsolète face à l'augmentation du chiffrement et les malwares générés automatiquement.	+ Utilise l'analyse comportementale avec de l'Intelligence Artificielle. Détecte les menaces réseau et les comportements anormaux des menaces 0-days
C2	- Support limité des menaces C2, basé sur l'analyse d'URL et des feed CTI externes	++ Détecte des menaces C2 avancées, comme les tunnels cachés
Mouvements latéraux	- Support limité pour les mouvements latéraux .	++ Détecte les menaces de mouvements latéraux avancées, comme le brute force, l'auto-réplication en allant au-delà du HASSH
Botnet	- Ne détecte pas les comportements de botnet	++ Détecte les menaces basées sur le comportement des botnets, tels que les DoS sortants et le cryptomining.
Reconnaissance	- Ne détecte pas les comportements de reconnaissance	++ Détecte les menaces basées sur la reconnaissance, tels que les scans de ports et l'account discovery
Exfiltration	- Ne détecte pas les comportements d'exfiltration	++ Détecte les menaces basées sur le comportement d'exfiltration, tels que les tunnels cachés

Le saviez-vous ?

Faible observabilité

Le parseur réseau de Suricata ne classifie que 42 protocoles. En revanche, n.Scope NDR prend en charge plus de 120 protocoles réseau, accélérant ainsi les investigations avec une observabilité approfondie.

Le saviez-vous ?

Faible détection

Le taux de fausses positives de Suricata atteint 70%. Avec seulement 0,1% du trafic représentant des flux de données malveillants, sa précision tombe à une simple fourchette de 0,014% à 1%.

I.A.

Tandis que Suricata n'utilise toujours pas d'Intelligence Artificielle à ce jour, n.Scope NDR emploie déjà des modèles avancés de détection de menaces.

	Suricata	Nano Corp.
DDoS	- Détecte supposément les DoS, et peine à détecter les DDoS à cause de la surcharge de données	++ Déjà déployé sur des réseaux ISP majeurs pour la détection DDoS
Malware, Trojan	+ Spécialisé dans la détection de malwares en trafic réel, mais obsolète en cas de chiffrement	+ Peut être utilisé pour détecter les comportements et protocoles de communication de malwaresl
Moteur de règles	- Possède un moteur de règles, mais il est trop permissif, ce qui provoque de nombreux faux positifs	+ Moteur de règles adapté à l'analyse réseau, réduisant drastiquement le taux de faux positif
Machine learning		
Identification des appareils	- N/A	+ Grâce au support de nombreux protocole (cdp, lldp, dhcp, etc.), le n.Scope peut identifier finement les équipements
Cartographie réseau	- Le moteur de Suricata ne permet pas de cartographier les réseau sous aucune forme	+ Dispose d'une technologie avancée de cartographie réseau, aidant les utilisateurs à comprendre rapidement leur réseau
Détection des cybermenaces	- N'utilise pas d'apprentissage automatique pour la détection	+ Utilise à la fois des règles et des algorithmes ML innovants pour obtenir des taux de détection élevés et minimiser les faux positifs.
Forensic		
Smart PCAP	- Stocke uniquement les paquets qui ont déclenché une alerte	+ Stocke tous les paquets, filtrés et contextualisant une alerte, pour une meilleure analyse forensic
Buffer	- N/A	+ Avec un Buffer intelligent, le n.Scope enregistre les évènements pré-déclenchement, idéal pour le forensic

Performance

	Suricata	Nano Corp.
Scalabilité	– Prétend atteindre 40Gbit/s mais a des difficultés à atteindre 6-8Gbit/s. Abandonne le trafic chiffré et s'appuie surs des cartes FPGA coûteuses	+ Atteint 100Gbit/s sans pertes sur du matériel COTS, idéal pour une observabilité profonde et la forensic
Ratio Matériel / Ressources	– Gourmand en ressources : 1Gbit/s nécessite 5 cœurs CPU & 64GB RAM. À 10Gbit/s avec 50 cœurs CPU & 256GB RAM, il perd des paquets	++ Efficacité : 1Gbit/s nécessite 1 cœur & 4GB RAM. 10Gbit/s nécessite 8 cœurs & 16GB RAM sur du matériel COTS
FPGA	– Utilise des cartes FPGA coûteuses pour être efficace, mais qui limite les protocoles supportés, réduisant l'observabilité	+ Surpasse Suricata sans avoir besoin de FPGA, ce qui en fait un choix supérieur en tout point
Performance monitoring	– Inadapté pour la supervision de la performance ; son système basé sur les logs limite le forensic et la visualisation des événements	+ Bien que ce ne soit pas un outils de supervision de performance, n.Scope offre des fonctionnalités d'observabilité & de supervision de la performance
Perte de paquets (%)	– Abandonne le trafic chiffré pour éviter trop de perte de paquet, mais atteint quand même 40% de perte avant d'arriver à 10Gbit/s	+ Certifié à 100Gbit/s par Spirent, n.Scope NDR ne perd aucun paquet, comme le confirment tous les benchmarks
False positives	– Taux élevé de faux positifs à la détection de protocoles (juqu'à 70%) - réduisant ensuite la détection des vraies menaces à moins de 1%	++ Le taux de faux positifs est < 0.01% dans la classification des protocoles, avec >95% de détection de menaces réelles
Onboarding	– Prend jusqu'à 6 mois pour une personnalisation manuelle ; nécessite un étalonnage régulier, consommant le temps des spécialistes	+ Opérationnel en quelques minutes ; ses algorithmes de M/L deviennent pleinement fonctionnels en moins de 3 semaines

Limitations des logs

Stockage	– Les logs consomment du stockage, réduisant l'historicité et provoquant des retards de détection & entravant le forensic	+ Utilise une technologie avancée de compression et de base de données pour un stockage à long et des requêtes
Vitesse de requête	– Ses logs verbeux consomment de l'espace et du temps ; entraînant souvent des coûts supplémentaires pour une vitesse de requête basse	+ Utilise un schéma de données intelligent, est plus rapide en vitesse de requête, nécessite moins de matériel pour une meilleure analyse

Le saviez-vous ?

Coûteux

L'appétit de Suricata pour les ressources est considérable. Pour une ligne à 1Gbit/s, sa sonde demande 8 cœurs CPU et 64 Go de RAM. Et à 10Gbit/s ? Attendez-vous à de nombreuses pertes de paquets. Tandis que la sonde de n.Scope NDR est en ligne à 10Gbit/s et n'exige que 2 cœurs CPU et 4 Go de RAM.RAM.

Conception ancienne

Les solutions Suricata s'en tiennent à de la détection basée sur des signatures, une méthode en déclin dans le monde de la cybersécurité. En effet, le chiffrement et l'IA en font une course impossible à suivre. Ce qui fait que Suricata est incapable de faire face aux menaces 0-day.

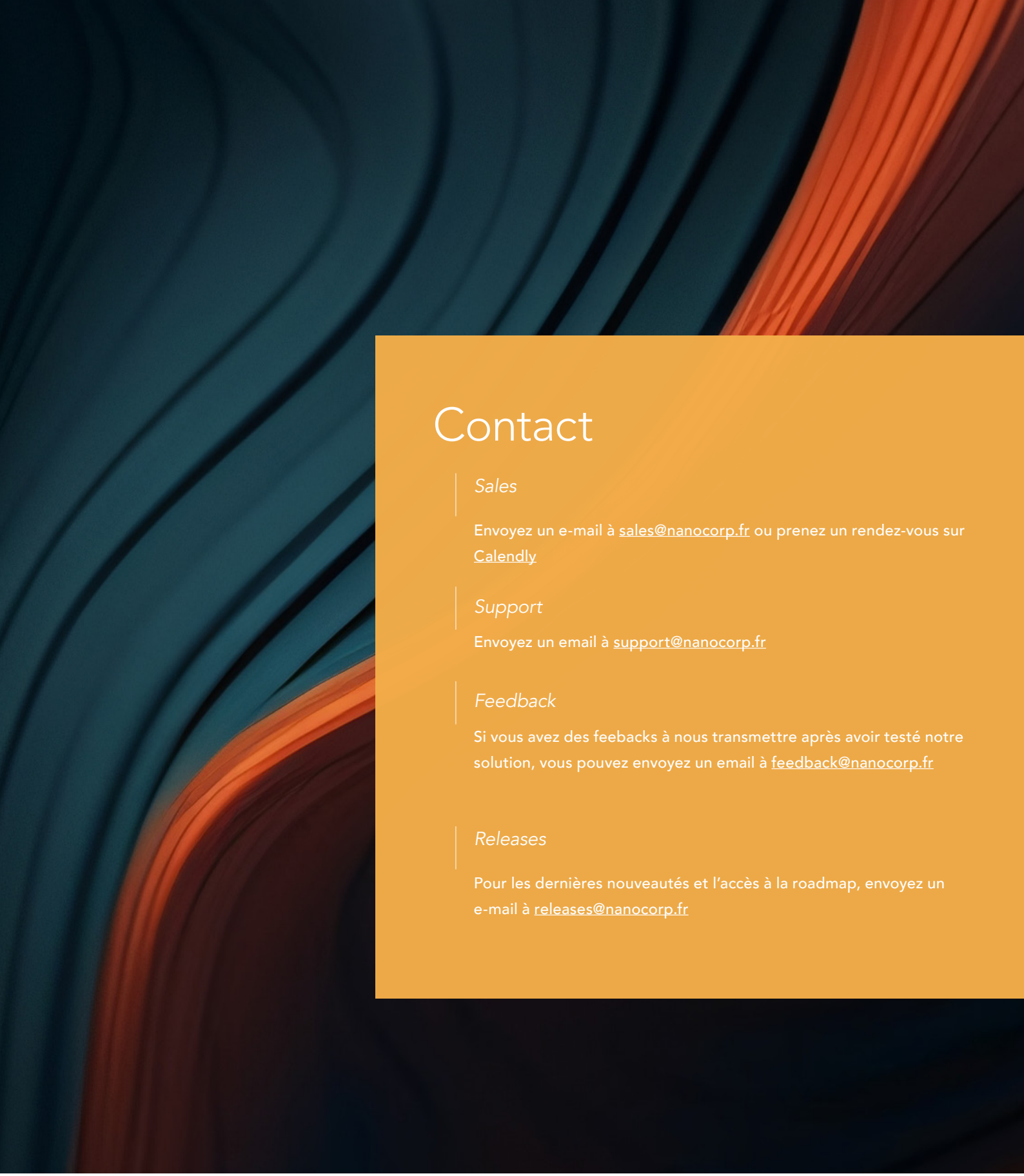
Management

	Suricata	Nano Corp.
Déploiement en < 30 minutes	- Nécessite des ajustements ; prend jusqu'à 10 heures pour le téléchargement, la compilation et la configuration de base	+ n.Scope NDR peut être déployé à distance sur l'infrastructure de l'utilisateur et être opérationnel en quelques minutes
WebUI	- Ne possède pas d'interface Web ; les utilisateurs ajoutent des interfaces tierces comme Kibana ou Splunk, qui est coûteux	+ L'interface Web du n.Scope NDR, permet une visualisation en temps réel des données et est adaptable pour des configurations complexes
Multi-tenancy	- Ne permet pas nativement le multi-tenant	+ Gère les configurations multi-tenant, idéal pour les MSSP hébergeant plusieurs clients sur une seule
Gestion de flotte	- Ne dispose pas d'un système de gestion de flotte car chaque appareil Suricata est indépendant	+ Gère le déploiement de flotte pour les sondes et les logiciels rewind
API RESTful	- Ne possède pas d'API REST intégrée pour la gestion, la configuration ou l'intégration.	+ Utilise l'API REST, permettant un contrôle à distance et une interface facile avec d'autres outils de l'utilisateur

Intégration

Exportation des données	+ Exporte les logs	+ Utilise une BDD open-source, permettant export en JSON, CSV, etc
Nouveau protocole réseau	- L'ajout dépend de la communauté, mais prend souvent des années	+ Ajoute régulièrement de nouveaux protocoles, généralement en moins de 2 semaines
Threat Intel	+ Accepte la Threat Intel, mais avec des limitations	+ Threat Intel léger et agnostique; peut s'intégrer à aux sources de l'utilisateur
Format de log pour SIEM	+ Intégration manuelle avec un SIEM, qui requiert une configuration de l'instance Suricata pour envoyer ses logs	+ Peut automatiquement envoyer des logs à Splunk, Elastic, etc.

	Suricata	Nano Corp.
Plateforme de gestion des incidents	- Capacités d'intégration limitées en dehors d'un SIEM	+ S'intègre avec des systèmes de communication externes, comme Slack, Discord, Pager Duty, emails, etc.
Notifications par email	- Pas de support intégré pour les emails	+ Envoi de notifications par email, Slack, Discord, etc.
Support de sécurité		
CSPN	+ Obtenu en 2022	+ Obtenu en 2023
Communication chiffrée	- Ne supporte pas nativement le TLS, les utilisateurs doivent ajouter des modules pour cela	+ Supporte nativement le TLS pour tous ses éléments



Contact

Sales

Envoyez un e-mail à sales@nanocorp.fr ou prenez un rendez-vous sur Calendly

Support

Envoyez un email à support@nanocorp.fr

Feedback

Si vous avez des feebacks à nous transmettre après avoir testé notre solution, vous pouvez envoyez un email à feedback@nanocorp.fr

Releases

Pour les dernières nouveautés et l'accès à la roadmap, envoyez un e-mail à releases@nanocorp.fr

NANO CORP.

Votre partenaire cybersécurité pour une supervision souveraine de vos réseaux.

nanocorp-fr/

nanocorp_pro

@nanocorp7610