V. 1.1. 2023

NANO CORP.

Guide d'évaluation du n.Scope NDR

www.nanocorp.fr

Les "Preuves de Concept" (PoC) ont pour finalité de mettre en évidence l'apport de la technologie n.Scope NDR dans la détection, en temps réel, des anomalies des réseaux.

Agilité

Prouver que le n.Scope NDR supervise tout type de réseau (IT ou OT) avec une qualité et une précision d'analyse sans égal.

Efficacité

Mettre en lumière les capacités de détection (menaces, shadow IT...) du n.Scope NDR et son apport essentiel aux actions de Forensic (PCAP recording, metadata exploration)

Simplicité

Démontrer la facilité de déploiement de n.Scope NDR, et la clarté de visualisation des réseaux complexes que permettent ses interfaces.

Couverture

Démontrer que le n.Scope NDR est capable de superviser à la fois les réseau IT et les réseaux OT, sur des équipements maitrisés par le client, qu'il est capable de maintenir.

Au début du PoC, des ingénieurs et des spécialistes installent un capteur (la sonde réseau **Probe**) et un outil de supervision et de visualisation (le **n.Scope**) dans un environnement cible.

Pour une flexibilité maximale, les équipements fournis dans le cadre de l'expérimentation prévoient deux capteurs, afin de permettre la collecte des données en plusieurs point du réseau. Une fois activé, le capteur commencera à collecter passivement les communications réseau, transmettant les métadonnées pertinentes à l'outil de supervision, qui fournira les visualisations et l'analyse des données.

Calendrier type de déroulement

Le temps est une denrée rare ! C'est pourquoi pour un PoC de 2 semaines, les utilisateurs ne sont pas sollicités plus d'une demi journée par semaine sur la durée de l'expérimentation.

A l'issue d'un PoC, si le client ne souhaite pas poursuivre avec la plateforme, toutes les données client seront effacées de manière sécurisée, avant re-expédition des équipements.

Calendrier	Étapes	Objectifs
Préparation	• Prévoir (date) l'installation (à - X semaines). • Présenter le déploiement.	Collecter les informations nécessaires, permettre aux clients de préparer le PoC.
Jour #1	• Installer les équipements fournis (serveurs sondes + analytics). • Router du trafic vers les sondes (TAP ou mirroré). • Vérifier que le serveur d'analyse reçoit du flux. • Donner un accès aux utilisateurs.	Commencer la collecte pour l'entrainement des modèles de machine et donner aux clients un premier aperçu.
Semaine #1	• Configuration du n.Scope (SSO, Asset Management, Whitelisting, Blacklisting, etc.) • Workshop de prise en main du n.Scope pour les utilisateurs du client. • Premier retour à chaud des utilisateurs (sur les interfaces, le processus d'on-boarding, la documentation, etc…)	S'assurer que les utilisateurs sont en mesure de commencer à utiliser la solution, et que les premières anomalies sont immédiatement détectées.
Semaine #2	• Explication des premiers résultats, avec un focus sur l'étude des premières données, des premières alertes, etc.	Accompagnement par les experts NANO Corp. dans la présentation des interfaces.
Après	• Rédaction et présentation d'un résumé du déroulement du PoC, d'un ROI et d'un rapport détaillé des résultats. • Présentation d'une stratégie de déploiement et d'un devis dimensionné à l'environnement. • Un Follow-up pour répondre aux questions et présenter la Roadmap.	Démontrer l'intérêt de la solution dans le quotidien des utilisateurs. Montrer que NANO Corp. assure un suivi même en dehors des PoC !

Pré-requis à la réalisation d'un PoC

Durant la phase de préparation, un ensemble de questions et de paramètres sera abordé, afin de définir au mieux le périmètre du PoC ainsi que certaines exigences liées au déploiement.

La sonde requiert un simple flux passif de données réseau, accessible par un TAP ou par SPAN. Les flux de la plateforme n'ont aucun impact sur les flux de production.

Toutes les connexions sont nativement sécurisées et la plateforme n'a pas besoin d'accès internet pour être fonctionnelle.

Besoins en connectivité	• La plateforme nécessite que le firewall du client aient les ports suivants ouverts: - TCP/443 (HTTPS), - TCP8443(mTLS), - TCP8005(mTLS) - TCP/22 (SSH - uniquement pour configuration interne). • Eventuellement un port VPN comme le port 51820 pour Wireguard - uniquement pour des actions de debug à distance sur demande du client.
Besoins en positionnement	• Les sondes doivent être alimentées en données réseau brut (paquets réseau) non-échantillonnées (différent de Netflow, IPFIX, sFlow). • La solution nécessite au préalable l'installation d'un TAP ou la mise en place d'un routage SPAN depuis un switch pour router du flux réseau vers les sondes. • Le client devra être en mesure de fournir des détails sur son infrastructure, afin de pouvoir sélectionner le meilleur emplacement pour les équipements.
Besoins en dimensionnement	• Pour garantir un dimensionnement au plus juste des équipements, il sera utile de définir la taille du réseau à superviser (nombre d'hôtes, d'IP, utilisation du SNMP, d'un SIEM, etc..). • Il sera également nécessaire d'estimer les volumes d'échange de données - à minima, le débit maximal des liens réseaux à superviser.
Besoins en Asset Management	• Pour accélérer la configuration de certaines des fonctionnalités du n.Scope, il pourra être utile de préparer, en amont, une liste des VLAN/VxLAN, des serveurs critiques (DNS, DHPC, etc…) et plages IP à superviser avec un détail sur la criticité de certaines IP par rapport à d'autres (DMZ, Prod, etc..).

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.

NANO Corp a développé une nouvelle génération de NDR, en créant la seule sonde du capable de superviser tous les réseaux, quelle que soit leur complexité et leur topologie. Cette innovation brevetée surveille non seulement chaque paquet traversant le réseau, mais offre également un workflow unique, de l'alerte à l'investigation, permettant un temps moyen de résolution 2,5 fois plus rapide que les solutions concurrentes, garantissant ainsi une sécurité nettement améliorée.

nanocorp-fr/

nanocorp_pro

@nanocorp7610