DARKTRACE

Checklist de l’acheteur

pour l’évaluation des solutions NDR

Le système le plus efficace pour comparer les solutions NDR

Introduction

Le marché de la détection et de la réponse réseau (Network Detection and Response/NDR) est aujourd'hui saturé de discours marketing et de promesses autour de l'IA, ce qui complique la tâche des CISO et des décideurs IT lorsqu'il s'agit d'identifier des solutions réellement efficaces et adaptées à leurs besoins.

Ce guide vous propose un cadre d'évaluation structuré ainsi qu'une checklist pratique pour faciliter les comparaisons objectives et éclairées entre les fournisseurs de solutions NDR, sur la base de capabilités mesurables. Bien que chaque équipe et organisation dispose de cas d'usage qui leur sont propres, ces critères constituent un point de départ pertinent pour évaluer et comparer les acteurs du marché.

PARTIE 1

Méthodologie

Comment utiliser ce document

Cette checklist a été conçue pour vous aider à évaluer et comparer les solutions NDR modernes.

La Partie 2 du document présente les catégories d'évaluation, réparties en plusieurs sections : feuille de route organisationnelle et ROI, périmètre et déploiement, analyse comportementale, réseau, détection des menaces, triage et investigation et fonctionnalités complémentaires.

Chaque catégorie comprend une description et une liste de questions à poser aux fournisseurs de solutions NDR. Nous vous recommandons d'identifier les capabilités prioritaires pour votre organisation et d'utiliser ces questions dans vos critères d'évaluation.

Voici comment tirer le meilleur parti de ce document :

Initier les échanges avec les fournisseurs

Utilisez cette checklist comme **point de départ de discussion** avec les fournisseurs. Posez des questions ouvertes afin de mieux comprendre dans quelle mesure chaque solution s'aligne avec vos priorités.

Comparer les solutions

Servez-vous de la checklist pour **comparer les solutions** de manière structurée et identifier celles qui répondent, qui dépassent ou qui ne satisfont pas vos exigences.

Clarifier et valider les points délicats

En cas de doute sur certaines fonctionnalités, appuyez-vous sur les critères correspondants de la checklist pour **approfondir les échanges**, demander des précisions ou des démonstrations. Assurez-vous que les fournisseurs vous fournissent des informations fiables et précises.

Prioriser les capabilités

Attribuez à chaque critère un niveau de priorité, élevé, moyen ou faible, en fonction de votre profil de risque et de vos objectifs de sécurité. Cela permet de **concentrer** l'évaluation sur les **capabilités réellement essentielles.**

Pour garantir une évaluation équitable et objective des solutions de sécurité réseau, il est **recommandé d'adopter une approche comparative de type A/B**, en évaluant les fournisseurs côte à côte selon les mêmes critères. **Cette méthode limite les biais, met en évidence les différences réelles et assure des conditions de comparaison équitables.**

Voici quelques facteurs à prendre en compte afin de garantir une comparaison équitable :

Déploiement

Définissez un périmètre identique : assurez-vous que chaque solution bénéficie du même niveau de visibilité sur les sous-réseaux et les entités réseau ciblés.

Établissez un calendrier précis : testez toutes les solutions dans le même environnement et sur une durée identique. Cela permet de comparer les phases d'apprentissage et leur évolution dans le temps, lesquelles peuvent être différentes d'une solution à une autre.

Paramétrage et configuration

Comparez les solutions dans des conditions de performance optimales : consultez les fournisseurs retenus pour comprendre leurs meilleures pratiques de déploiement, notamment dans les environnements réseau complexes ou si vous escomptez des résultats spécifiques.

Raisonnez à long terme : adaptez la solution en gardant une vision à long terme. Un correctif ou un processus de configuration rapides ne permettront pas de révéler les besoins futurs en configuration.

Visibilité des données : assurez-vous que toutes les solutions peuvent conserver et interroger l'ensemble des données pendant la période d'évaluation.

Évaluation

Coordonnez vos critères d'évaluation : appliquez les mêmes critères d'évaluation préalablement définis à tous les fournisseurs.

Comprenez les mécanismes de classification des menaces propres à chaque fournisseur : les scores, les étiquettes, les explications et les critères peuvent varier selon le fournisseur. Assurez-vous de pleinement maîtriser les nuances pour une comparaison équitable.

Prenez en compte les fonctionnalités actives et passives : certaines capabilités peuvent être désactivées lors d'un essai ou d'un test POC, mais avoir un impact majeur en production. Les actions de réponse en sont un exemple. Réfléchissez à la manière dont les fonctionnalités passives influenceraient le comportement de la solution face aux attaques réelles lorsqu'elles seront activées.

Restez en contact : communiquez avec les fournisseurs si des résultats semblent incohérents. Cela permet d'évaluer leur capacité de support et de remédiation.

Conclusion

Évaluez les solutions sur la base des résultats obtenus : comparez les résultats sur la base des métriques et des critères de succès définis. Cela peut inclure la réduction du bruit d'alerte, le nombre d'incidents critiques détectés et le gain de temps pour les analystes sur la période de test.

Analysez également les aspects qualitatifs : allez au-delà des chiffres pour prendre en compte l'expérience utilisateur, la relation avec l'équipe du fournisseur, la qualité du support, les intégrations disponibles et les capabilités de la plateforme au sens large.

Examinez les critères d'évaluation et les résultats : revoyez les critères et les résultats en interne, puis communiquez-les aux fournisseurs sélectionnés.

PARTIE 2

Catégories d'évaluation

La checklist suivante présente les capabilités clés à considérer lors de l'évaluation de solutions NDR modernes. Utilisez-la comme une comparaison structurée des fournisseurs, pas uniquement pour vérifier la présence d'une fonctionnalité, mais surtout pour évaluer la solidité, l'efficacité et l'approche utilisée par chaque solution pour ces fonctionnalités. Certains fournisseurs peuvent revendiquer certaines capabilités ou fonctionnalités. Cependant, une analyse plus approfondie peut révéler qu'elles ne se traduisent pas par des résultats pertinents en termes de sécurité.

Toutes les fonctionnalités n'ont pas besoin d'être couvertes par un seul fournisseur, mais cette checklist vous permet de définir des attentes claires pour une architecture de sécurité réseau moderne.

Feuille de route organisationnelle et évaluation du ROI

Critères	Questions à poser aux fournisseurs
Paramètres de l'analyse de rentabilité	▪ Le fournisseur propose-t-il des modèles de ROI, une vision claire du coût total de possession, une transparence sur la gestion des licences et l'impact sur les ressources opérationnelles ?
Transparence sur l'utilisation de l'IA dans les opérations de sécurité	▪ Le fournisseur explique-t-il clairement comment l'IA est utilisée pour la détection, l'alerte et la réponse. Inclut-il des détails tels que les types de modèle (supervisés, non supervisés, basés sur des règles), les sources des données d'apprentissage, la gestion des faux positifs ou la supervision humaine ?
	▪ Le fournisseur est-il conforme aux normes de gouvernance de l'IA : ▪ ISO/IEC 42001:2023 - — Technologies de l'information — Systèmes de management de l'intelligence artificielle — Exigences ▪ ISO/IEC 23894:2023 - — Technologies de l'information — Intelligence artificielle — Lignes directrices pour la gestion des risques
	▪ Le fournisseur documente-t-il les limites de l'IA, les mécanismes d'explicabilité et la manière dont les mises à jour sont gouvernées et communiquées ?
Transparence du fournisseur et alignement sur la feuille de route	▪ Le fournisseur propose-t-il une documentation produit complète, un calendrier de mises à jour régulier, un modèle de support à long terme et l'implication des clients dans la feuille de route produit.
Scalabilité du produit et métriques de performance	▪ Le fournisseur a-t-il la capacité d'accompagner la croissance sur les différents environnements, avec des indicateurs clairs, comme le débit, la densité des capteurs, la latence ou la capabilité d'ingestion ?
Flexibilité tarifaire	▪ Le fournisseur propose-t-il un modèle de gestion des licences évolutif, avec des remises basées sur le volume et la durée ?
Flexibilité de déploiement	▪ Le fournisseur prend-il en charge le déploiement multi-environnements ? Cela peut inclure : sur site, réseaux virtuels, environnements conteneurisés, cloud hybride, appareils distants, emails, appareils OT ou environnements cloisonnés.
Flexibilité de gestion des licences	▪ Le fournisseur propose-t-il des options de gestion des licences flexibles pour accompagner les évolutions de l'infrastructure, par exemple la migration d'adresses IP sur site vers des charges de travail dans le cloud ?
Capabilités de base	▪ Quelles capabilités sont incluses nativement ? Lesquelles nécessitent un achat séparé ou des licences additionnelles ?

Périmètre et déploiement

Aspect	Description	Points clés à prendre en compte
Surveillance hors bande	Analyse passive du trafic réseau sans impact sur l'environnement de production	▪ Réplication de port via SPAN ou TAP, typiquement sur un switch central ▪ Analyse du trafic réseau brut (paquets) ▪ Surveillance réseau passive au lieu d'un déploiement en ligne ▪ Identifie automatiquement tous les actifs réseau sans dépendre des utilisateurs ni d'un balayage actif ▪ La solution doit être sans agent par défaut ▪ Qualité des données collectées : s'agit-il uniquement des adresses IP source et destination ? En général, plus les données sont riches, meilleure est l'analyse.
Intégrations	Connexion de technologies tierces pour améliorer les workflows de détection, de réponse et d'investigation.	▪ Ne dépendant pas, mais pouvant s'intégrer à des outils tels que : ▪ Pare-feu, VPN, solutions SASE et ZTNA ▪ Solutions EDR et XDR ▪ Plateformes SIEM and SOAR ▪ Microsoft 365 ▪ Services cloud tels que Microsoft Azure et AWS ▪ Plateformes IAM, dont Microsoft Entra ID, Okta et Duo ▪ Applications SaaS telles que Dropbox, Salesforce, Slack et Zoom ▪ Outils de gestion des vulnérabilités tels que Rapid7 et Tenable. ▪ Solutions de gestion des workflows et des tickets, dont ServiceNow et Jira ▪ Enrichissement via des flux de renseignement sur les menaces et les CVE connues.
Rétention des données	Conservation des paquets réseau bruts et des métadonnées, pour analyse et investigation	▪ Capacité à conserver : ▪ Fichiers PCAP ▪ Flux et principales métadonnées ▪ Données de journaux pour des investigations approfondies
Réseaux isolés et hautement sécurisés / cloisonnés	Pas de perte de fonctionnalité de base en environnements isolés	▪ Possibilité de fonctionner de manière entièrement autonome, sans aucune connexion sortante ▪ Peut conserver l'ensemble des données sur site au sein d'une appliance fournie ▪ Ne dépend d'aucune connectivité externe pour : ▪ Détection et réponse ▪ Investigations d'incidents ▪ Mises à jour continues des modèles IA ▪ Renseignements sur les menaces provenant de sources tierces ▪ Stockage des fichiers PCAP et fonctionnalités de recherche ▪ Création de modèles personnalisés de détection et de réponse ▪ Configurations personnalisées et modifications des modèles système et des modèles de détection et de réponse

Aspect	Description	Points clés à prendre en compte
Environnements cloud, cloud hybride, IaaS, PaaS, SaaS	Couverture et visibilité des environnements entièrement cloud et cloud hybride	▪ Extension native de la couverture réseau aux environnements cloud, avec une visibilité unifiée via une seule plateforme ▪ Capacités de déploiement dans des environnements entièrement cloud-native et hybrides, y compris lors de la transition du on-premises vers le cloud ▪ Ingestion des journaux de flux (par exemple : AWS VPC Flow Logs, Azure NSG Flow Logs) ▪ Sans agent par défaut, ou possibilité d'utiliser le mirroring VPC ou des taps virtuels ▪ Cartographie dynamique de l'architecture Azure, y compris les ressources éphémères telles que les conteneurs et les applications serverless ▪ Options de déploiement de machines virtuelles et dans les environnements d'orchestration de conteneurs ▪ Intégration avec des services tels qu'AWS Security Hub, IAM, CloudTrail et leurs équivalents Azure afin de comprendre les identités, le plan de contrôle et le contexte réseau
OT/CPS et appareils IoT	Couverture et visibilité des technologies opérationnelles / systèmes cyber-physiques (OT/CPS) et des dispositifs Internet des objets (IoT, IIoT, mIoT, BMS, SCADA, IHM, PLC)	▪ Couverture native des systèmes IT/OT convergents et cloisonnés, des appareils IoT, IIoT et des appareils de périphérie distants, au sein d'une plateforme unique ▪ Déploiement possible dans des environnements entièrement isolés ▪ Inspection approfondie des paquets (DPI) sur les protocoles spécifiques aux environnements OT ▪ Découverte active de l'inventaire des actifs OT et analyse des vulnérabilités ▪ Couverture de tous les niveaux du modèle Purdue, du niveau 0 (processus physiques) au niveau 5 (réseaux d'entreprise) ▪ Solution indépendante des fournisseurs (vendor agnostic) ▪ Évaluation continue des risques et corrélation des vulnérabilités grâce à l'analyse en temps réel du comportement des actifs, de l'exposition réseau et de l'exploitabilité
Endpoints des travailleurs à distance	Visibilité réseau complète sur les appareils des postes de travail distants	▪ Visibilité complète au niveau réseau des endpoints des travailleurs à distance et des appareils en déplacement, en complément des alertes EDR ▪ Couverture des petits bureaux satellites ou des espaces de travail partagés disposant de peu ou pas d'infrastructure réseau

Analyse comportementale réseau

Aspect	Description	Points clés à prendre en compte

Intelligence artificielle et apprentissage automatique	Utilisation de multiples techniques IA pour la détection, l'investigation et la réponse aux menaces	▪ Approche multicouche de l'IA, appliquée de manière séquentielle et hiérarchique, comprenant notamment :
		  ▪ Apprentissage automatique non supervisé
		  ▪ Apprentissage automatique supervisé
		  ▪ Apprentissage bayésien
		  ▪ Algorithmes de clustering
		  ▪ Méthodes Ensemble Réseaux neuronaux de graphes (GNN)
		  ▪ Traitement du langage naturel (NLP)
		  ▪ Modèles de langage spécifiques à un domaine (DSLM)
		  ▪ Grands modèles de langage (LLM) personnalisés et dédiés à la sécurité

IA auto-apprenante	IA qui apprend l'environnement unique dans lequel elle est déployée, en s'adaptant et en évoluant de manière autonome	▪ Construit une compréhension de ce qui est « normal » pour chaque environnement, sans s'appuyer sur des règles ou signatures prédéfinies ▪ Détecte les activités anormales en se basant sur le comportement normal, plutôt que sur des données historiques d'attaques ▪ Réduit considérablement les efforts continus d'ingénierie de détection manuelle par rapport aux outils traditionnels ▪ S'adapte automatiquement aux changements de l'environnement sans nécessiter de mise à jour ou de configuration manuelle ▪ Classe automatiquement les appareils en groupes et en clusters en fonction de la similarité de leurs comportements ▪ Solution entièrement configurable, permettant un réglage fin lorsque nécessaire
Déploiement de l'IA	Emplacement de l'IA pour l'apprentissage continu et le traitement des données	▪ L'IA est déployée localement et apprend en fonction de chaque environnement unique dans lequel elle est installée
Conformité	Détection des activités liées à la conformité	▪ Capacité à détecter les violations des politiques de conformité, telles que l'utilisation non autorisée d'outils de GenAI ▪ Possibilité de créer et de modifier des modèles de conformité personnalisés

Aspect	Description	Points clés à prendre en compte
Analyse du trafic chiffré	Capacité à identifier des activités anormales et suspectes dans le trafic réseau chiffré	▪ Capacité éprouvée à détecter des menaces connues et inédites dans le trafic chiffré sans nécessiter de déchiffrement
Déchiffrement	Déchiffrement du trafic réseau chiffré	▪ Capabilité de déchiffrer le trafic réseau si nécessaire, par exemple à des fins de conformité ▪ Options de déchiffrement natives et via des solutions tierces ▪ La détection des comportements anormaux et malveillants ne dépend pas du déchiffrement
Analyse du trafic réseau entrant et latéral	Analyse des flux réseau Nord-Sud et Est-Ouest	▪ Le fournisseur analyse-t-il le trafic réseau entrant afin de prévenir les intrusions et violations de sécurité ? ▪ Le fournisseur analyse-t-il le trafic réseau interne pour détecter et répondre aux menaces, telles que les mouvements latéraux et les menaces internes ?
Rétention	Stockage du trafic réseau, des événements et des métadonnées associées. Conserve le trafic réseau brut et les métadonnées pour permettre une analyse rétrospective et garantir la conformité aux exigences légales	▪ Conserve le trafic réseau brut et les métadonnées pour permettre une analyse rétrospective et garantir la conformité aux exigences légales
Visibilité des actifs	Identification et gestion des entités réseau	▪ Découverte et cartographie automatiques des actifs réseau depuis une vue centralisée ▪ Capabilité d'accès aux informations détaillées de chaque actif et à l'historique de son activité réseau ▪ Marquage automatique et manuel des appareils pour faciliter l'identification, la recherche et la gestion

Détection des menaces

Aspect	Description	Points clés à prendre en compte
Modèles de détection	Modèles IA permettant de détecter des activités suspectes et malveillantes	▪ Large éventail de modèles de détection standards couvrant des cas d'utilisation liés à la sécurité et à la conformité ▪ Possibilité de visualiser, modifier et personnaliser l'ensemble des modèles directement depuis l'interface utilisateur, sans développement supplémentaire, sans support du fournisseur ni connectivité externe ▪ Capabilité à créer des modèles entièrement personnalisés pour répondre à des cas d'utilisation spécifiques, tels que la conformité ou des scénarios en périphérie (edge cases) en dehors du catalogue standard de modèles

Détection des menaces inédites	Utilisation de la détection d'anomalies pilotée par l'IA pour identifier des attaques émergentes ou zero-day sans indicateurs préalables	▪ Protection reconnue contre des menaces telles que :
		  ▪ Ransomwares inédits et nouvelles variantes
		  ▪ Vulnérabilités zero-day
		  ▪ Menaces internes
		  ▪ Utilisation abusive d'outils légitimes
		▪ Ne repose pas sur :
		  ▪ Flux de renseignement sur les menaces
		  ▪ Comparaison des données avec celles d'autres environnements clients
		  ▪ Règles ou signatures
		  ▪ Ingestion des CVE
		▪ Le fournisseur doit être en mesure de présenter au moins trois exemples documentés et détaillés démontrant la détection de menaces zero-day avant leur divulgation publique, sans s'appuyer sur des règles, des signatures, des données d'entraînement ou des hypothèses préalables

Détection des menaces connues	Correspondance des activités anormales avec des menaces déjà identifiées	▪ Détection de menaces connues telles que ransomwares et malwares ▪ Possibilité d'ingérer et d'utiliser des flux de renseignement sur les menaces si nécessaire
Compromissions existantes	Détection des menaces et compromissions préexistantes dans un environnement	▪ Identification de comportements inhabituels par rapport à des appareils similaires et à des groupes de pairs ▪ Identification d'activités suspectes indiquant une compromission existante
Prise de contrôle de comptes et mouvements latéraux	Détecte les comptes compromis en se déplaçant dans les systèmes pour escalader les accès et le contrôle.	▪ Le produit analyse-t-il le trafic réseau interne pour détecter les anomalies ? ▪ Peut-il corréler l'activité réseau avec des identifiants compromis ou des détournements de session ? ▪ Analyse des flux réseau entrants, sortants et latéraux ▪ Modélisation comportementale pour identifier des schémas de communication anormaux ▪ Simulations d'événements à haute fidélité ▪ Corrélation multi-domaines : réseau, endpoints, identités, SaaS, etc.
Communications C2	Identification du trafic malveillant de type command-and-control, même lorsqu'il est caché dans DNS, HTTPS ou d'autres protocoles courants.	Le fournisseur peut-il détecter : ▪ Schémas de beaconing (callbacks à intervalles réguliers) ▪ Utilisation de protocoles inhabituels (ex. : tunneling DNS, C2 basé sur ICMP) ▪ Connexions vers des adresses IP ou domaines malveillants connus ▪ C2 chiffré sur des ports non standard ou via des services inattendus

Aspect	Description	Points clés à prendre en compte
Logiciels malveillants et livraison de payload	Détecte le transfert de fichiers ou de code malveillant à travers le réseau avant leur exécution	▪ Le fournisseur peut-il détecter des signes de : ▪ Transferts de fichiers malveillants (via SMB, FTP, HTTP) ▪ Transferts d'exécutables ou livraison de fichiers malveillants (payloads) déposés ▪ Livraison via des protocoles rares ou obsolètes (ex. : TFTP, Telnet)
Comportement de menace interne / abus d'identifiants légitimes	Signale les activités inhabituelles d'utilisateurs autorisés pouvant indiquer une intention malveillante ou de la négligence. Détecte l'utilisation abusive d'identifiants valides, qu'ils soient volés ou volontairement partagés	Le fournisseur peut-il détecter des signes de : ▪ Abus de privilèges ▪ Accès ou transfert de données inhabituel ▪ Authentification ou comportement de session anormal ▪ Transferts ou exfiltration de données vers des hôtes externes inconnus ou non approuvés ▪ Transferts sortants importants vers des destinations externes rares ou nouvelles ▪ Données envoyées via des canaux cachés (DNS, HTTPS vers des domaines inconnus) ▪ Utilisation inhabituelle de protocoles (ex. : FTP/SFTP depuis des endpoints qui ne l'utilisent normalement pas) ▪ Anomalies temporelles pour contourner la DLP (ex. : « trickling »)

Exploitation des CVE	Exploitation de vulnérabilités connues dans les systèmes, services ou applications.	▪ Détection d'activités anormales sur les entités du réseau, telles que :
		  ▪ Activité de connexion inhabituelle
		  ▪ Transferts de données anormaux
		  ▪ Connexions vers des endpoints rares
		  ▪ Scan interne inhabituel du réseau
		  ▪ Reconnaissance SMB
		  ▪ Mouvements latéraux
		  ▪ Élévation de privilèges

Scan suspect et reconnaissance	Identifie les activités de sondage et de cartographie des actifs réseau qui précèdent souvent une attaque.	Détection des techniques de scan et de reconnaissance du réseau interne
Détection d'exfiltration de données	Alerte en cas de déplacement non autorisé de données sensibles vers des destinations externes ou cloud, même si les données sont chiffrées.	Détection de connexions vers des endpoints rares Détection des connexions et des chargements vers des services de partage de fichiers tels que WeTransfer, Dropbox, etc. Détection de téléchargements internes volumineux ou de connexions anormales vers des emplacements internes

Triage et investigation

Aspect	Description	Points clés à prendre en compte
Triage automatisé	Élimination du triage manuel et du travail d'investigation qui conduit souvent à la fatigue liées aux alertes	▪ Triage et investigation automatisés des événements réseau pour ne faire remonter que les activités les plus anormales et les plus pertinentes ▪ La technologie apprend de manière autonome pour mettre à jour en continu sa compréhension du comportement normal ▪ Ne nécessite aucune intervention humaine, ni déclenchement, ni script
Priorisation et gestion des alertes	Priorise les alertes en fonction de leur gravité	▪ Priorisation automatique des alertes pour présenter aux analystes les activités les plus critiques ▪ Catégorisation des alertes, de critique à informative ou liée à la conformité ▪ Possibilité d'assigner des alertes à des utilisateurs spécifiques ▪ Consultation et gestion des alertes via une application mobile ou un navigateur ▪ Connexion possible avec des solutions tierces, par exemple ServiceNow ou Jira

Corrélation des alertes	Corrélation de plusieurs alertes liées pour créer des incidents uniques	▪ Corrélation des alertes issues de la plateforme du fournisseur (NDR, OT, email)
		▪ Corrélation des alertes provenant de technologies tierces, telles que :
		  ▪ EDR/XDR
		  ▪ SASE et ZTNA
		  ▪ Applications SaaS
		▪ Regroupement de plusieurs alertes liées pour identifier de véritables incidents, sans intervention humaine

Investigations pilotées par l'IA	Investigations de bout en bout réalisées de manière autonome par un système IA agentique (non basé sur GenAI)	▪ Combinaison automatique des alertes pertinentes pour créer ou enrichir des incidents, avec escalade des cas critiques pour révision humaine ▪ L'IA agentique réalise des investigations avec la qualité d'un analyste SOC de niveau 2 ▪ Ne repose pas sur des chatbots, la GenAI ou l'intervention humaine ▪ Les investigations peuvent être déclenchées manuellement ou automatiquement par des sources externes ▪ Rapports complets générés pour chaque incident, avec chronologie et explication claire du processus d'investigation effectué par l'IA ▪ Disponible pour tous les clients, sans restriction de licence ou exigence de service managé
Chasse aux menaces et analyses avancées	Capabilités supplémentaires permettant la chasse aux menaces, les investigations approfondies, l'analyse forensique et la réponse aux incidents	▪ Possibilité de télécharger et d'analyser des PCAP manuellement si nécessaire ▪ Recherche et analyse avancées du trafic réseau via des requêtes simples, avec création et sauvegarde de requêtes personnalisées ▪ Possibilité pour les utilisateurs avancés d'utiliser une syntaxe de requête complexe et de construire des recherches structurées avancées ▪ Fonctionnalités de recherche avancée incluses dans les fonctionnalités de base du produit, sans licence supplémentaire, coût additionnel ou besoin de connectivité externe

Confinement et réponse

Aspect	Description	Points clés à prendre en compte
Réponse autonome	Prend de manière autonome la meilleure mesure pour répondre aux menaces	▪ Fonctionne 24/7, de manière autonome et à la vitesse machine ▪ Peut choisir et appliquer elle-même la réponse la plus efficace sans intervention humaine ▪ Peut faire évoluer automatiquement le niveau des actions de réponse au fur et à mesure de l'évolution de la menace ▪ Possibilité de configurer une confirmation humaine avant exécution d'une action de réponse au besoin ▪ Paramétrable par sous-réseau, horaires, jours, etc. ▪ Modèles de réponse et paramètres entièrement personnalisables en détail ▪ Ne repose pas sur des règles ou des signatures statiques ▪ Des exemples probants de confinement précoce de menaces inédites, connues et internes existent
Réponse native	Capacité du fournisseur à proposer des actions de réponse nativement, sans dépendre de technologies tierces	▪ Peut répondre nativement aux menaces réseau sans intégration EDR ou de pare-feu ▪ Peut appliquer des actions ciblées pour bloquer un trafic spécifique sans perturber l'activité métier ▪ Peut n'autoriser que ce qui est considéré comme activité normale pour une entité réseau, tout en bloquant le reste ▪ Peut également être appliqué en fonction de ce qui est normal pour un groupe d'appareils similaires ▪ Fonctionne sur des réseaux plats avec peu ou pas de segmentation
Réponse tierces	Capabilité à s'intégrer à des technologies tierces pour renforcer les capabilités de réponse natives	▪ Peut s'intégrer à des solutions tierces pour étendre les actions de réponse, notamment : ▪ Solutions EDR/XDR ▪ Pare-feu ▪ Microsoft 365 et Entra ID ▪ SIEM et SOAR
Confinement des menaces	Empêche la progression des menaces dès les premiers stades	▪ Peut agir dès les premiers signes d'activité suspecte, sans attendre une alerte EDR ou une investigation manuelle ▪ Contient les comportements menaçants ou suspects sans perturber l'activité métier normale ▪ La durée de confinement peut être prolongée si nécessaire, pour donner le temps aux analystes de réagir ▪ Peut mettre en quarantaine de manière autonome de nouvelles entités réseau non reconnues

Fonctionnalités complémentaires

Aspect	Description	Points clés à prendre en compte
Reporting	Valorise la NDR en transformant les données de détection en rapports clairs et priorisés, soutenant les opérations de sécurité et la conformité cyber	▪ Peut générer des rapports spécifiques pour le suivi de la conformité dans le temps, tels que : PCI-DSS, GDPR, HIPAA, ISO 27001, NIST, SOC2, MITRE ATT&CK, IEC 62443
Gestion continue des menaces et de l'exposition (CTEM)	Complète la NDR en identifiant et réduisant de manière proactive les vulnérabilités, tout en affichant les chemins d'attaque exploitables par les attaquants	▪ Génère un scoring de risque unique et spécifique à votre environnement, plutôt que des indications générales sur le retard de patch ou le risque CVE ▪ Vue priorisée pour la découverte des risques cyber, ciblant les utilisateurs, appareils et vulnérabilités présentant le plus fort risque de compromission ▪ Évalue l'impact potentiel sur les actifs affectés lors d'incidents et permet une réponse plus efficace le long des chemins d'attaque les plus critiques
Préparation et récupération après incident	Soutient les tests, l'affinement et la validation des capabilités de réponse aux incidents	▪ Le fournisseur propose-t-il des simulations reflétant votre architecture, vos configurations et votre stack technologique spécifiques ? ▪ La solution peut-elle simuler des incidents réalistes en direct dans votre environnement réel, y compris cloud, SaaS et infrastructures OT, et pas seulement des scénarios théoriques ? ▪ Le système supporte-t-il les playbooks adaptatifs ou dynamiques évoluant avec l'environnement (par exemple, post-migration cloud ou activités de fusion/acquisition) ? ▪ Quelles sont les dépendances en termes de licences, ressources et compétences pour la mise en place et la gestion continue ?
Gestion de la surface d'attaque	Informe la NDR en mappant les actifs et expositions externes, aidant à prioriser les détections liées aux systèmes à forte valeur ou à haut risque	▪ La solution utilise-t-elle des techniques d'IA pour découvrir automatiquement des actifs inconnus ou « shadow » sans nécessiter de plages IP ou de données initiales ? ▪ Peut-elle détecter les actifs associés à votre marque sur des domaines, des instances cloud et des infrastructures IoT tiers ? ▪ Est-ce qu'elle explore et surveille en continu votre empreinte numérique pour identifier de nouvelles expositions ou des changements ? ▪ Est-elle capable de détecter des vulnérabilités zero-day ou à fort impact sans dépendre de scans périodiques ? ▪ Peut-elle détecter des domaines, services ou actifs non autorisés ou non surveillés créés hors de la gouvernance IT centrale ? ▪ Prend-elle en compte les risques liés à la chaîne d'approvisionnement et aux abus de marque, y compris les domaines de phishing ou les infrastructures usurpées ? ▪ La solution ASM améliore-t-elle d'autres capabilités NDR (ex. défense contre les domaines usurpés, contexte endpoint, corrélation via analyste IA) ? ▪ Peut-elle fournir une vue unifiée lorsqu'elle est combinée avec la télémétrie interne et d'autres outils de gestion des risques ?
Sécurité de la messagerie électronique	Intégration de la sécurité de la messagerie à la NDR	▪ Capabilité à corréler automatiquement les menaces cross-domain depuis la boîte de réception avec l'activité réseau ultérieure ▪ Les outils travaillent-ils ensemble pour améliorer la précision des détections et accélérer les investigations ? ▪ Fournit une approche de défense en profondeur, de la boîte de réception jusqu'au réseau

SECTION BONUS

Comment évaluer l'IA

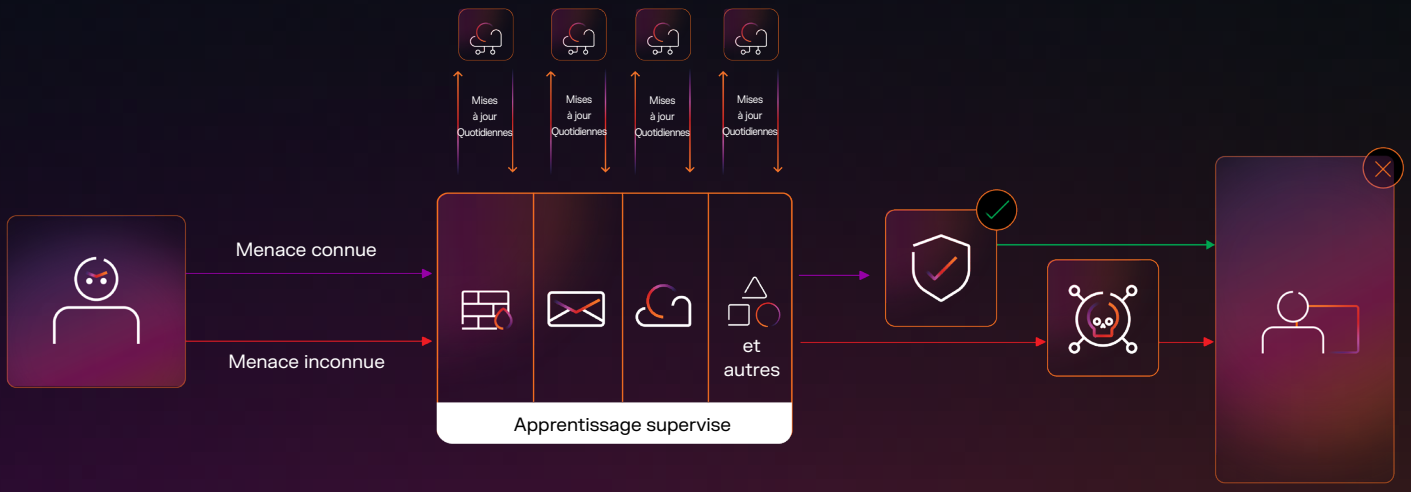
L'IA est souvent présentée comme la solution miracle en cybersécurité, mais la plupart des équipes de sécurité se demandent ce qui se cache réellement derrière ces outils. De nombreux produits prétendent utiliser l'IA, mais reposent souvent uniquement sur du machine learning supervisé ou sur des modèles d'IA générative, efficaces seulement dans des scénarios étroits et bien définis, et incapables de détecter des menaces inédites.

Lors de l'évaluation de solutions NDR utilisant l'IA, il est essentiel de ne pas se fier uniquement aux résultats d'un seul modèle ou d'un type d'IA (comme les LLM basés sur l'IA générative). Cela ne fournira que des résultats limités et pourra générer des données incomplètes ou biaisées.

Ce défi est encore amplifié par l'essor des menaces alimentées par l'IA, qui nécessitent des défenses plus adaptatives et intelligentes. Malheureusement, sans méthode claire pour évaluer ces capabilités, les organisations risquent de prendre du retard, voire d'être prises au dépourvu.

La réalité est que toutes les IA ne se valent pas. Pour être efficace, l'IA en cybersécurité doit dépasser les mots à la mode et intégrer plusieurs techniques avancées qui travaillent ensemble pour gérer la complexité des menaces modernes. Les professionnels de la sécurité doivent comprendre quels types d'IA sont utilisés pour quels cas d'utilisation afin d'évaluer leur efficacité par rapport aux besoins de leur organisation et renforcer leur posture de sécurité.

Centrée sur l'attaque



Orientée métier

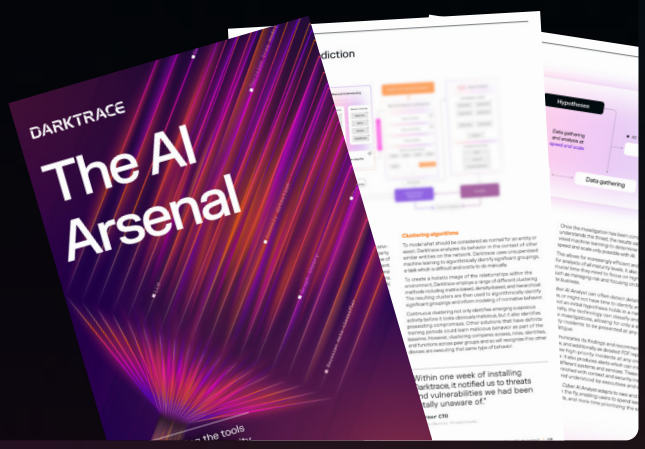
Le schéma ci-dessous compare les outils de sécurité basés sur l'IA qui exploitent les données métier pour détecter les anomalies comportementales et les outils entraînés sur des données d'attaques historiques pour repérer les menaces.

Pour vous accompagner, nous avons créé trois guides distincts sur l'IA en cybersécurité, conçus pour vous guider à chaque étape de votre parcours d'adoption :

Approfondir l'application de l'IA en cybersécurité

Téléchargez le livre blanc Arsenal IA pour découvrir comment les modèles IA peuvent être appliqués à la cybersécurité et comment l'IA auto-apprenante de Darktrace combine plusieurs techniques pour offrir une défense proactive et résiliente contre les menaces.

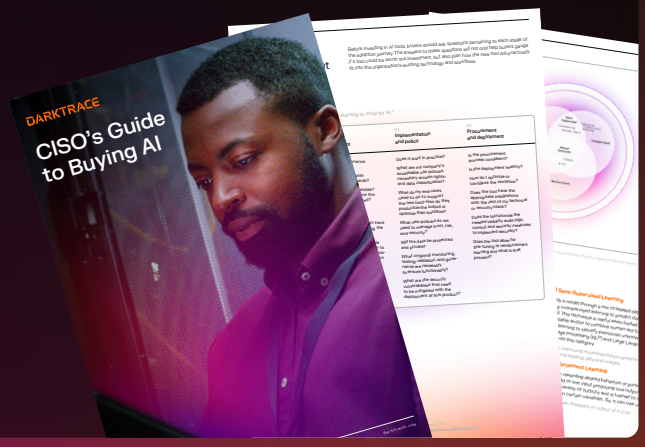
En savoir plus ↗



Évaluer les solutions de sécurité basées sur l'IA

Téléchargez le livre blanc Guide du CISO pour l'achat de solutions IA. Ce document explique comment les acheteurs devraient aborder l'acquisition de solutions basées sur l'IA. Il présente les points clés à considérer à chaque étape du parcours d'adoption de l'IA, les questions spécifiques à poser aux fournisseurs et les éléments à surveiller dans leurs réponses.

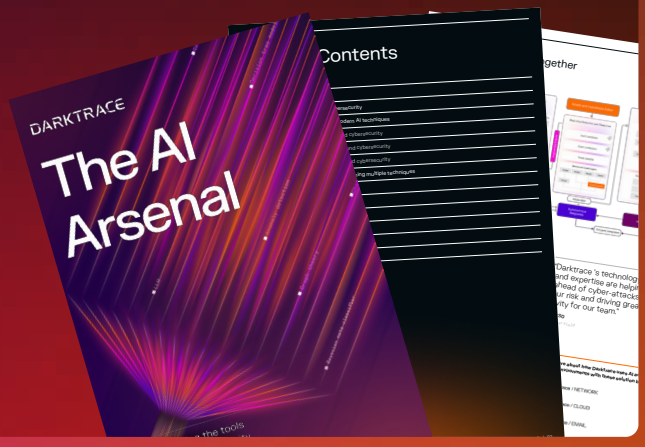
En savoir plus ↗



Évaluer à quel niveau se trouve votre organisation dans son parcours vers la maturité IA

Téléchargez le livre blanc Modèle de maturité IA Ce document propose une analyse complète du modèle de maturité IA de Darktrace, le seul cadre disponible capable d'aider les CISO et les responsables de la cybersécurité à comprendre, évaluer, planifier et faire progresser leur adoption de l'IA.

En savoir plus ↗



PARTIE 3

Le processus d'évaluation

■ Étape 1 :

Évaluation commerciale

La première phase consiste en une évaluation commerciale, ou processus de découverte.

Il s'agit d'évaluer si une solution potentielle correspond aux besoins de votre organisation, non seulement en termes de fonctionnalités principales, mais aussi en termes d'intégration à vos flux de travail, à votre modèle opérationnel et à vos attentes en matière de valeur globale.

Voici nos recommandations pour cette étape :

S'impliquer avec les fournisseurs
Entretenez une communication ouverte avec vos fournisseurs tout au long du processus d'évaluation. Travaillez avec eux pour identifier et comprendre les incohérences de performance. Cette approche collaborative vous permet de tester la réactivité de l'équipe, de résoudre rapidement les problèmes et de prendre une décision éclairée basée sur des données précises.

Prendre en compte les personnes et les partenariats
Considérez les aspects humains qui peuvent influencer de manière significative votre expérience avec la solution. Évaluez la présence locale du fournisseur et la solidité de son équipe de gestion de compte, y compris toute relation avec votre prestataire de services de sécurité gérés (MSSP) le cas échéant. Des partenariats solides et un support accessible peuvent être cruciaux pour le succès et la satisfaction à long terme.

Comparer à niveau de licences similaire
Assurez-vous de comparer des solutions proposant des packages de licences équivalents. Certains fournisseurs offrent différents packages qui ne fournissent pas forcément les mêmes fonctionnalités. Vérifiez quelles fonctionnalités sont incluses afin de garantir une comparaison juste, ainsi que les capabilités à valeur ajoutée.

Penser au support après-vente
Assurez-vous que le fournisseur propose un support après-vente solide, incluant mises à jour régulières, formations et certifications, événements, ainsi qu'un service client réactif. Consultez les avis d'autres clients et d'analystes du secteur, comme Gartner, pour déterminer si le fournisseur est réellement recommandé et apporte de la valeur sur le long terme, et pas seulement pendant la période d'essai ou d'intégration.

■ Étape 2 :

Évaluation technique

La deuxième étape clé est l'évaluation technique, où il est essentiel d'impliquer les utilisateurs quotidiens du produit.

Ce processus de découverte permet de déterminer dans quelle mesure une solution répond aux besoins de votre organisation en termes de performance, d'ergonomie et d'intégration. Il permet également d'évaluer des aspects critiques tels que l'architecture de déploiement, l'efficacité de la détection, l'utilisation de l'IA, l'application des politiques et la compatibilité avec votre infrastructure existante.

Voici les facteurs clés à prendre en compte lors de l'évaluation technique :

Évaluer sur la base de données de performance optimales

Assurez-vous d'évaluer la solution choisie une fois qu'elle est entièrement déployée. Cela est particulièrement important pour les solutions utilisant l'apprentissage automatique non supervisé, qui nécessitent une période d'apprentissage initiale. Collaborez avec votre fournisseur pour le confirmer et comprendre le potentiel réel de chaque solution dans des conditions idéales, incluant le déploiement des intégrations nécessaires.

Évaluer la courbe d'apprentissage

Ne vous limitez pas à l'évaluation des capabilités de détection à un instant donné ; examinez également le taux d'amélioration et de maturité au fil du temps. Cela vous donnera une vision plus fine de la précision à long terme de la solution.

Modèles d'IA et affinage des capabilités

Assurez-vous que le fournisseur offre une transparence totale sur ses modèles IA et leurs capabilités. Vous devez pouvoir personnaliser les modèles de détection et de réponse pour effectuer des ajustements précis selon vos besoins, et créer des modèles personnalisés pour des cas d'utilisation spécifiques non couverts par la bibliothèque de modèles par défaut du fournisseur.

Explications claires et transparentes

Chaque détection, chaque investigation et chaque action de réponse doit être accompagnée d'une explication transparente. Comprenez quels modèles de détection ont été déclenchés, la logique correspondant à toute investigation automatisée, et la liste détaillée des actions de réponse entreprises. Cette transparence est cruciale pour la confiance et une évaluation efficace.

Combiner analyses qualitatives et quantitatives

Allez au-delà des promesses marketing autour de l'IA en combinant analyses qualitatives et quantitatives des capabilités de la solution dans votre environnement spécifique. Évaluez des éléments tels que la visibilité, la précision de détection et l'ergonomie, ainsi que des indicateurs mesurables que vous pouvez comparer avec vos flux existants : temps de tri et d'investigation, nombre total d'incidents générés et temps moyen de réponse.

Comparer les menaces de manière cohérente

Les différents fournisseurs peuvent classer les menaces de façons variées, ce qui peut créer des incohérences dans votre évaluation. Assurez-vous de comparer des métriques équivalentes en demandant des clarifications à votre fournisseur si nécessaire. Cela vous aidera à faire une comparaison juste et précise.

Ne pas évaluer tous les faux positifs de la même manière

Comprenez qu'un « faux positif » peut être défini différemment dans les différentes solutions que vous évaluez. Par exemple, les outils orientés métier utilisant la détection basée sur les anomalies déclencheront des alertes pour des activités considérées comme anormales. Ce sont des détections légitimes, mais « anormal » ne signifie pas toujours « malveillant » et ne correspond donc pas toujours à la définition traditionnelle d'un faux positif. Les solutions utilisant l'IA pour la détection d'anomalies fonctionnent comme un analyste humain expérimenté : elles signalent des activités suspectes selon les données disponibles, puis les utilisent comme contexte pour l'investigation et la réponse. Prenez le temps de comprendre le contexte et l'impact des faux positifs dans chaque solution pour une évaluation plus éclairée. En cas de doute, demandez au fournisseur comment il définit les faux positifs. Testez également la facilité à reconnaître les alertes qui ne sont pas intéressantes ou pertinentes pour votre équipe.

Conclusion

Nous espérons que cette checklist vous apportera un cadre pratique pour évaluer plusieurs solutions NDR et identifier celle qui correspond le mieux aux besoins de votre organisation.

Maintenant que vous disposez de ce cadre, pourquoi ne pas découvrir Darktrace / NETWORK en action et démarrer un essai gratuit de 30 jours afin de tester notre technologie dans votre propre environnement ?

Demandez une démo ↗

À propos de Darktrace

Leader mondial de la cybersécurité basée sur l'IA, Darktrace aide les organisations à garder une longueur d'avance face à l'évolution constante des menaces. Fondée en 2013 à Cambridge, au Royaume-Uni, Darktrace propose une plateforme de cybersécurité essentielle qui protège les entreprises contre les menaces inconnues grâce à une IA capable d'apprendre en temps réel à partir de chaque environnement métier. La plateforme et les services de Darktrace reposent sur plus de 2 700 collaborateurs et protègent près de 10 000 clients dans le monde entier. Pour en savoir plus, rendez-vous sur www.darktrace.com.

Amérique du Nord : +1 (415) 229 9100 Europe : +44 (0) 1223 394 100 Asie-Pacifique : +65 6804 5010 Amérique latine : +55 11 4949 7696

darktrace.com | info@darktrace.com