DARKTRACE

Construire une pile de sécurité moderne

Pourquoi vos solutions NDR et de sécurité de la messagerie doivent fonctionner ensemble

Table des matières

Résumé

Bien que de nombreuses cyberattaques débutent dans la boîte de réception, celle-ci est rarement leur destination finale. Les acteurs malveillants lancent des attaques multi-étapes pilotées par l'IA, qui commencent dans un email et se propagent rapidement à travers les réseaux et les environnements cloud. Dans ce contexte, les solutions de sécurité isolées peinent à reconstituer le fil des attaques, laissant des angles morts critiques qui ralentissent la défense. La défense la plus efficace contre les menaces modernes repose sur une approche unifiée avec l'IA, qui permet de relier en profondeur la sécurité de la messagerie et des réseaux.

Ce livre blanc explore :

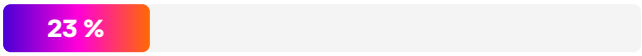
- **Comment l'IA accélère les attaques multi-étapes et multi-domaines**
- **Pourquoi les solutions isolées pour messagerie et réseau ne parviennent plus à suivre le rythme**
- **Comment une approche IA unifiée et multicouche améliore la détection et la réponse aux menaces**
- **Avantages sécuritaires, opérationnels et commerciaux d'une approche intégrée**

Pourquoi la sécurité unifiée n'est plus facultative

Les attaques par email deviennent de plus en plus furtives grâce à l'IA

Les emails restent l'un des points d'accès initiaux les plus ciblés et les plus efficaces pour les cybercriminels, et l'IA rend ces menaces de plus en plus convaincantes et difficiles à détecter. Les acteurs malveillants utilisent l'IA générative pour créer à grande échelle des emails de phishing extrêmement personnalisés, tout en exploitant des techniques émergentes comme le phishing via code QR.

Selon Gartner, la messagerie demeure un vecteur d'attaque majeur pour les malwares et le vol d'identifiants, avec pour objectif ultime la compromission du réseau.



- **23 % des responsables sécurité** ont identifié l'ingénierie sociale comme la cause principale d'une récente attaque externe contre leur organisation, le **phishing arrivant juste derrière avec 21 %.**

(Forrester Security Survey 2024).

...et il en va de même pour les menaces réseau

Une fois à l'intérieur d'une organisation, les attaquants peuvent utiliser l'IA pour accélérer et automatiser chaque phase du cycle de vie de l'attaque.

Cela peut inclure :

- La recherche des fournisseurs d'infrastructure et d'hébergement gratuit potentiels
- Une reconnaissance plus rapide des organisations ciblées
- Un comportement adaptatif des malwares
- La collecte d'identifiants à grande échelle
- Le développement de charges utiles
- L'aide à la création de scripts malveillants et aux techniques d'évasion

Ces avancées permettent aux attaquants d'agir plus vite, avec une précision accrue et à des volumes bien supérieurs qu'auparavant. Selon le National Cyber Security Centre (NCSC) du Royaume-Uni, d'ici 2027, l'IA renforcera presque certainement la capacité des attaquants à exploiter les vulnérabilités, facilitant ainsi les intrusions sophistiquées par des acteurs étatiques et non étatiques.

Déjà, 74 % des professionnels de la sécurité estiment que les attaques pilotées par l'IA représentent un défi majeur pour leur organisation (State of AI Cybersecurity 2025).

Pourquoi les solutions isolées ne suffisent pas

Face à un paysage de menaces de plus en plus complexe, de nombreuses organisations ont accumulé un ensemble hétéroclite d'outils leaders sur leur marché : un pour la sécurité de la messagerie, un autre pour la surveillance réseau, d'autres encore pour la protection des endpoints ou du cloud. Mais ces solutions isolées fonctionnent rarement en véritable symbiose.

Le plus souvent, elles se contentent de partager des données via une plateforme SIEM ou SOAR, générant des alertes qui manquent du contexte nécessaire pour comprendre l'ampleur réelle des attaques. Cette approche fragmentée crée des angles morts entre les différentes étapes de la chaîne d'attaque, obligeant les équipes de sécurité à reconstituer manuellement les événements à partir de tableaux de bord et de journaux déconnectés. Et puisque les attaquants se déplacent de plus en plus rapidement et de manière plus furtive à travers les environnements, ces retards dans la détection et l'investigation peuvent s'avérer catastrophiques.

Même des investissements massifs dans des solutions EDR et XDR laissent souvent des lacunes, notamment concernant l'activité réseau, créant une fausse confiance dans la visibilité par le SOC. Les agents ne peuvent pas être déployés partout dans un réseau moderne, et les outils traditionnels qui se concentrent uniquement sur les activités « known bad » (connues comme malveillantes) ne détectent pas les menaces inconnues, inédites ou internes.

La réalité est claire :

seule une solution véritablement intégrée, reliant de manière fluide la télémétrie de la messagerie et du réseau, peut offrir la rapidité, la visibilité et l'agilité nécessaires pour détecter et répondre aux attaques modernes qui tirent parti de l'IA.

Au cœur de l'attaque : comment les menaces passent de la boîte de réception à la compromission interne

Examinons une attaque récente observée par Darktrace.

Dans ce cas précis, la solution Darktrace du client était configurée en mode Détection uniquement, sans activation des mécanismes de réponse. La compromission a donc pu s'aggraver jusqu'à ce que l'équipe de sécurité intervienne sur la base des alertes générées par Darktrace.

Si la réponse autonome avait été activée, elle aurait appliqué des actions rapides pour contenir l'attaque. Néanmoins, Darktrace a pu offrir une visibilité étendue sur les différentes composantes de l'environnement numérique du client et reconstituer le déroulement de l'attaque, permettant ainsi au client de mettre rapidement en œuvre des mesures de remédiation. Le schéma ci-dessous illustre la progression de l'attaque à travers l'environnement du client.

Ce scénario de menace met en évidence un schéma récurrent des attaques modernes :

elles se déplacent de manière fluide à travers l'ensemble de l'environnement numérique, de la messagerie au réseau, et au-delà. Lorsque la sécurité fonctionne en silos, les équipes de défense se retrouvent avec une vision fragmentée, retardant la détection, perturbant la réponse et, in fine, donnant l'avantage aux attaquants.

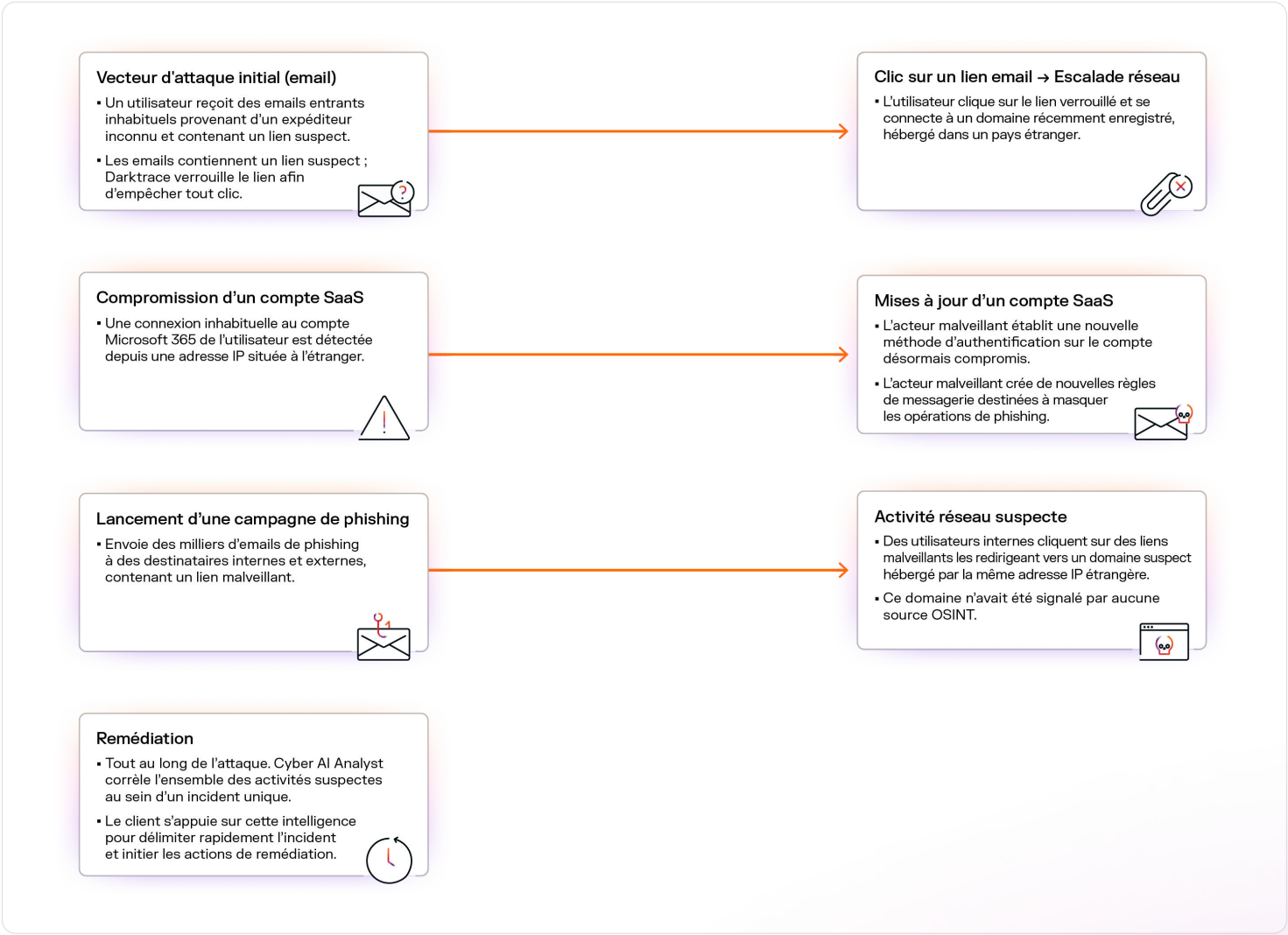


Figure 01: Schéma illustrant la progression d'une attaque, de la messagerie vers le réseau et les applications SaaS

Darktrace / NETWORK + / EMAIL

Deux solutions leaders sur leur marché, une approche IA multicouche unique

Individuellement, Darktrace / NETWORK et Darktrace / EMAIL sont des solutions puissantes et reconnues comme des références du secteur.

/ NETWORK

Reconnue comme Leader dans le Magic Quadrant™ Gartner® 2025 pour la NDR, la solution Darktrace / NETWORK déploie sa puissante IA multicouche au cœur des réseaux modernes, neutralisant en temps réel les menaces connues comme inconnues.

Gartner Peer Insights : ★★★★★ 4,7* (sur 465 évaluations, août 2025)

99 %

Il a été démontré que Darktrace / NETWORK réduit le bruit des alertes **de près de 99 % par rapport à un fournisseur NDR traditionnel**

(Client Darktrace dans le secteur de l'énergie)

08

Darktrace / NETWORK détecte et contient en moyenne les vulnérabilités zero-day **8 jours avant leur divulgation publique.**

(Recherche Darktrace)

/ EMAIL

Désignée Customers' Choice dans le rapport Gartner® Peer Insights™ Voice of the Customer 2025 pour la sécurité de la messagerie, la solution Darktrace / EMAIL apporte une innovation IA inédite destinée à stopper les attaques nouvelles et ciblées sur l'ensemble de l'écosystème de messagerie.

Gartner Peer Insights : ★★★★★ 4,8* (sur 323 évaluations, août 2025)

55 %

55 % des menaces détectées par Darktrace / EMAIL ont réussi à passer à travers l'ensemble des couches de sécurité existantes

(Annual Threat Report 2024)

13

Darktrace / EMAIL détecte les menaces **13 jours plus tôt que les autres solutions**

(Recherche Darktrace)

Une approche IA unique au cœur de la solution

Qu'est-ce qui rend les solutions réseau et messagerie de Darktrace **si puissantes** ?

L'IA au cœur de leur performance.

La plupart des fournisseurs de cybersécurité s'appuient encore sur des mécanismes de détection obsolètes, basés sur des règles et des signatures. Même lorsque l'IA est utilisée, elle se limite généralement à des modèles supervisés, entraînés sur des données d'attaques et des renseignements sur les menaces référencés. Bien qu'efficaces pour identifier les menaces connues, ces modèles nécessitent un réentraînement constant et peinent toujours à détecter des attaques inédites ou pilotées par l'IA, qui ne correspondent pas aux schémas historiques. Il en résulte des anomalies difficiles à interpréter et un afflux d'alertes à faible niveau de confiance, qui submergent les équipes de sécurité, contribuent à la fatigue liée aux alertes et conduisent à des réponses excessives ou peu précises.

L'IA auto-apprenante de Darktrace adopte une approche fondamentalement différente de la cybersécurité, en **apprenant en continu** l'environnement numérique unique de chaque organisation. Grâce à une approche IA multicouche, elle intègre de manière stratégique un ensemble de techniques d'IA, notamment l'apprentissage automatique non supervisé, les LLM, les GNN et le NLP, de façon à la fois séquentielle et hiérarchique.

Cette approche lui permet de **s'adapter à l'évolution des menaces** et de construire une compréhension dynamique du comportement normal des utilisateurs, des appareils et des systèmes. En combinant ces modèles d'IA, notre IA auto-apprenante distingue les activités réellement malveillantes des événements inhabituels, mais légitimes, sans s'appuyer sur des signatures, des règles ou des ajustements manuels.

Notre IA auto-apprenante constitue le socle de la plateforme de sécurité ActiveAI de Darktrace, qui corrèle la télémétrie entre les différents domaines pour offrir une couverture complète de bout en bout, notamment sur la messagerie électronique et le réseau. **Cela permet à Darktrace de relier les informations issues de multiples environnements et de créer une vision unifiée du risque.**

Les signaux comportementaux provenant d'une composante de l'environnement, comme une connexion suspecte détectée sur le réseau, peuvent immédiatement guider la prise de décision dans la messagerie électronique, et vice versa. Cette intégration étroite permet une détection des menaces plus rapide, des alertes enrichies et contextualisées, ainsi que des actions autonomes plus intelligentes, sans intervention humaine ni intégrations complexes basées sur des règles.

Grâce à une défense holistique alimentée par l'IA sur le réseau et la messagerie, vous bénéficiez d'une protection unifiée supérieure à la somme de ses parties. Elle offre une protection fluide et adaptative qui reflète la manière dont les attaques réelles se déroulent, donnant aux équipes de défense un avantage constant et consolidé.

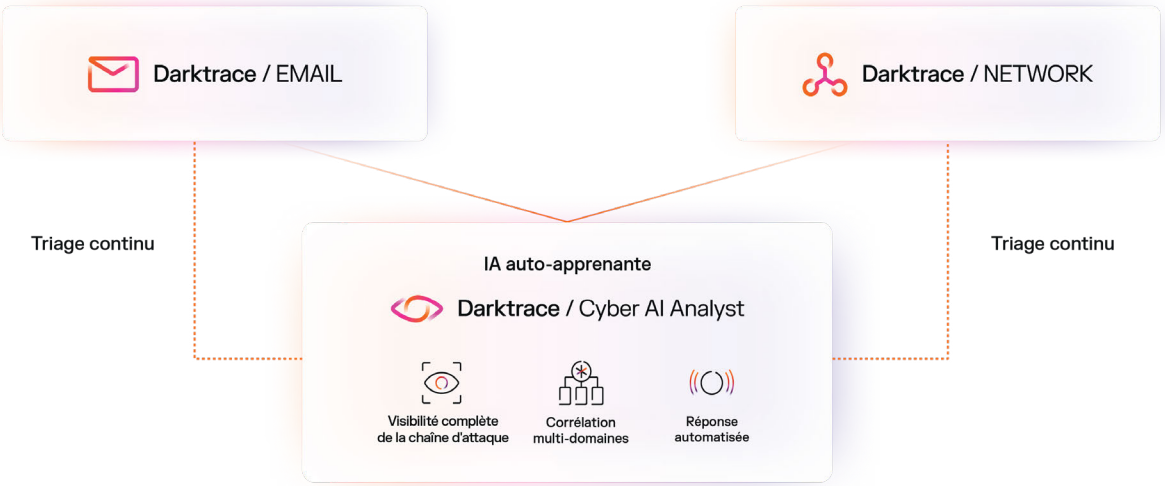


Figure 02 : Ensemble, Darktrace / NETWORK et / EMAIL combinent résilience proactive et visibilité unifiée des menaces, vous aidant à évoluer vers un SOC piloté par l'IA.

Votre compagnon d'investigation : Cyber AI Analyst

Si l'IA auto-apprenante alimente la détection et la réponse aux menaces inter-domaines, Cyber AI Analyst est le **détective numérique infatigable de votre SOC.**

Il s'agit d'un système IA agentique qui enquête de manière autonome sur toutes les alertes de sécurité pertinentes, qu'elles proviennent de Darktrace ou d'outils de sécurité tiers (firewalls, EDR, SIEM). Bien plus qu'un simple chatbot Gen AI Cyber AI Analyst utilise plusieurs types d'IA pour reproduire le processus d'investigation humaine, incluant le machine learning, des modèles entraînés sur le comportement d'analystes experts, des LLM personnalisés pour la sécurité et le NLP.

Il réalise des investigations et analyses équivalentes aux niveaux 1 et 2 d'un SOC :

- il formule et affine des hypothèses
- il interroge et corrèle des informations
- il suit les attaques complexes à travers plusieurs domaines
- il met en évidence les incidents critiques pour les faire examiner par des humains
- il suggère des actions de réponse basées sur l'analyse du « pattern-of-life »

Il atteint généralement une conclusion en quelques minutes et présente un résumé d'incident clair et interactif, avec alertes liées, analyses contextuelles et visualisations interactives basées sur des graphes, permettant d'explorer et de comprendre même les attaques les plus complexes.

En prenant en charge les investigations et le triage selon le niveau 2 d'un SOC, Cyber AI Analyst libère les analystes humains pour qu'ils puissent se concentrer sur une chasse aux menaces proactive et sur des enquêtes plus approfondies.

Accélération X 10 des investigations grâce à Cyber AI Analyst

Jusqu'à 50 000 heures analyste gagnées chaque année

Comme si vous ajoutiez jusqu'à 30 analystes SOC à temps plein

Avantages d'une approche unifiée

Rassembler la sécurité réseau et de la messagerie électronique apporte une gamme d'avantages quantitatifs et qualitatifs à toute organisation, pouvant être globalement classés en avantages techniques, opérationnels et commerciaux. **Examinons-les de plus près.**

Avantage technique

Sur le plan technique, les avantages peuvent être divisés en deux catégories : intelligence pré-alerte et intelligence liée aux alertes.

Intelligence pré-alerte : collecte des données avant que la menace ne frappe

De nombreux outils de sécurité ne commencent l'analyse qu'une fois que des signes évidents de compromission sont présents. Contrairement à ces outils, notre IA ingère et analyse en continu les données, à la fois sur la messagerie et le réseau, même en l'absence d'alertes. Cette analyse continue permet de construire une compréhension comportementale riche de chaque utilisateur, appareil et domaine interagissant au sein de l'organisation.

Ainsi, au moment où un email arrive dans la boîte de réception d'un utilisateur, Darktrace dispose déjà du contexte du domaine de l'expéditeur sur la base de sa visibilité réseau. De même, si un domaine suspect apparaît dans un email, cette information influence immédiatement l'interprétation des activités réseau futures. Cette compréhension partagée s'étend à l'ensemble de l'écosystème Darktrace. Que l'intelligence provienne de l'email, du réseau, des endpoints ou de sources externes comme les flux de renseignement sur les menaces, elle n'a besoin d'être ingérée qu'une seule fois. Elle enrichit ensuite la détection et la réponse sur tous les produits, garantissant des décisions cohérentes et contextualisées.

Le résultat est un processus dynamique de collecte et de partage d'intelligence qui construit la connaissance au sein de l'outil ; non pas des menaces elles-mêmes, mais des référentiels comportementaux en temps réel. Cela permet à Darktrace de signaler les menaces sans attendre qu'une compromission ne se produise.

Intelligence liée aux alertes : Une corrélation des informations en temps réel

Lorsqu'une alerte de sécurité est déclenchée, Cyber AI Analyst commence immédiatement l'investigation en formulant des hypothèses et en analysant les données en temps réel, ainsi que les données historiques, sur l'ensemble des différents domaines. Il met en lien de manière autonome les comportements associés, par exemple en corrélant un email suspect avec une activité réseau inhabituelle sur l'appareil du destinataire, créant ainsi un incident complet et centralisé pour que le SOC puisse l'examiner.

Ce processus se déroule en quelques minutes et à grande échelle, réduisant drastiquement le volume d'alertes et le travail de triage manuel.

De plus, cette corrélation automatique garantit que les chaînes d'attaque restent intactes, offrant une visibilité continue depuis la compromission initiale jusqu'aux mouvements latéraux ou à l'exfiltration de données. Cette visibilité partagée permet de déterminer la réponse la plus ciblée, proportionnelle à l'ampleur et à la portée de l'attaque.

Contrairement aux solutions ponctuelles ou aux flux de travail SIEM, qui laissent souvent les analystes assembler manuellement des alertes fragmentées sans contexte complet, Darktrace fournit une intelligence post-alerte unifiée, indépendante du point d'apparition initial de la menace.

Notre approche accélère non seulement les investigations et renforce la confiance dans les décisions de réponse, mais soutient également un principe fondamental de la philosophie de sécurité de Darktrace : les défenseurs ne doivent jamais perdre de vue l'attaquant après son point d'entrée initial.

Bien que la messagerie électronique puisse constituer le point d'entrée,

le mouvement suivant des attaquants cible généralement l'infrastructure réseau ou les comptes cloud, rendant indispensable une corrélation continue et inter-environnements entre la messagerie et le réseau.

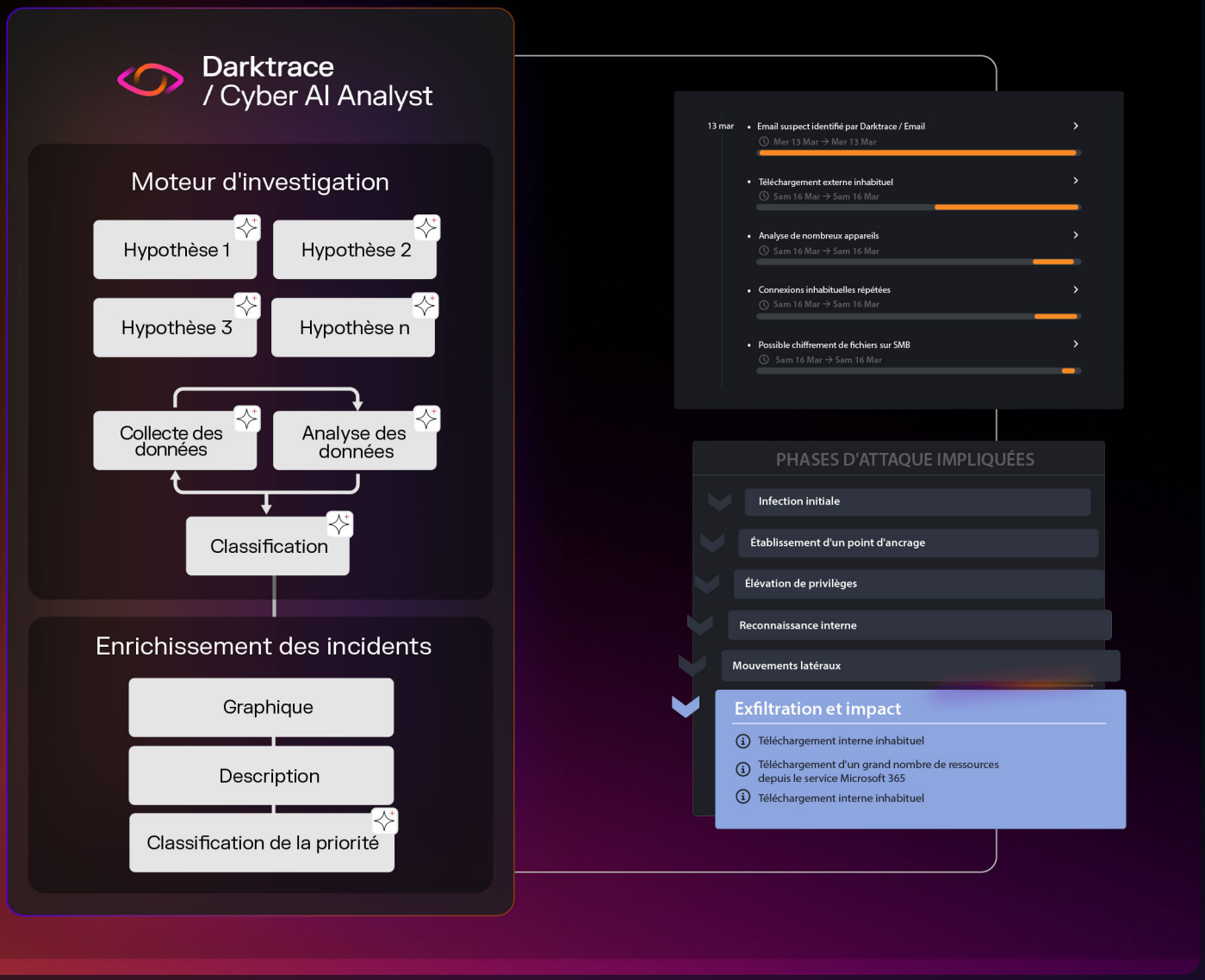


Figure 03: Étapes d'une attaque débutant par la messagerie et se propageant au réseau, avec les différentes phases de la chaîne d'attaque corrélées dans Cyber AI Analyst

« La capacité de Darktrace à synthétiser d'énormes volumes de données élimine efficacement le bruit, permettant à l'équipe de se concentrer sur les vrais risques sans être submergée par des informations non pertinentes. »

■ **CISO, Administration locale**

Avantage opérationnel

Rationalisation des opérations de sécurité entre les équipes

Dans de nombreuses organisations, la sécurité de la messagerie électronique et la réponse aux incidents sont encore gérées par des équipes distinctes. La gestion de la messagerie relève souvent des opérations IT, tandis que la défense réseau et la réponse aux incidents dépendent du SOC. Cette séparation crée des frictions opérationnelles, surtout alors que les emails demeurent le point d'entrée le plus courant pour les cyberattaques.

En déployant la sécurité réseau et messagerie ensemble, au sein d'une plateforme unique et d'un visualiseur de menaces intégré, les informations critiques provenant des emails ne restent pas confinées à une console ou une équipe séparée, mais sont directement accessibles dans les flux de travail principaux du SOC.

Cette visibilité partagée offre à l'équipe de réponse aux incidents une compréhension plus approfondie des vecteurs d'attaque par email sans nécessiter d'escalade ou d'externalisation, et ouvre la voie à une collaboration renforcée entre les différentes branches de l'équipe de sécurité.

Réduction du temps de compréhension et accélération de la réponse

Avec les données réseau et messagerie unifiées au sein d'une seule plateforme, les équipes de sécurité n'ont plus besoin de passer d'un outil à l'autre pour corréler des alertes disparates. En plus de simplifier le travail manuel, l'approche unifiée entre réseau et messagerie réduit le temps de compréhension des alertes par les utilisateurs.

De plus, la corrélation intégrée des menaces entre messagerie et réseau via Cyber AI Analyst permet un triage plus rapide et des réponses plus confiantes et coordonnées sur l'ensemble des environnements. Contrairement aux flux de travail traditionnels reposant sur la corrélation SIEM ou les playbooks SOAR, Darktrace corrèle les informations en temps réel et automatise des actions de réponse intelligentes.

Valeur commerciale

Déployer la sécurité réseau et messagerie ensemble n'est pas seulement un gain technique et opérationnel, cela apporte également des bénéfices commerciaux.

Avec un seul fournisseur, les organisations profitent d'une relation unique, simplifiant tout, de l'acquisition et la négociation au support continu. Plutôt que de gérer plusieurs contrats, les clients bénéficient d'une équipe de compte unifiée et d'un processus commercial simplifié. L'intégration de services gérés ou professionnels autour des deux produits est également facilitée, permettant d'accéder à une expertise cohérente sur l'ensemble de l'environnement de sécurité.

Investir dans une plateforme unique alimentée par l'IA pose un socle solide pour l'expansion future.

Avec le réseau et la messagerie dans le même ensemble, l'ajout de nouvelles capacités à l'avenir, comme la couverture de l'identité ou du cloud, ne nécessite pas de repenser l'architecture, car la plateforme est conçue pour évoluer avec votre entreprise.

Si les solutions ponctuelles peuvent sembler flexibles au départ, elles conduisent souvent à une couverture fragmentée, des dépenses redondantes et des difficultés d'intégration. Pour les organisations souhaitant construire un SOC moderne et piloté par l'IA, opter pour une solution complète intégrée plutôt que pour les meilleurs produits isolés n'est pas seulement plus simple. C'est aussi plus stratégique. **Avec Darktrace, il n'y a aucun compromis sur la qualité lors de la transition vers une approche plateforme. Chaque achat individuel renforce la plateforme centrale, enrichit l'intelligence partagée et apporte plus de valeur au fil du temps.**

Darktrace a fait preuve d'intégrité, de patience et d'un véritable investissement pour construire une relation solide avec mon équipe. C'est pourquoi nous en sommes ici aujourd'hui.

- **CISO, Fournisseur de technologie mondial**

Scénarios d'achat

Examinons deux scénarios d'achat : l'un pour une organisation optant pour une stratégie de solutions ponctuelles, l'autre pour une organisation cherchant à consolider son socle de sécurité.

Scénario 1 : Solutions ponctuelles

Configuration initiale

Une organisation peut choisir un outil de sécurité email autonome, souvent sélectionné par les équipes IT ou de messagerie, puis déployer ultérieurement une solution de détection et réponse réseau (NDR) distincte via l'équipe sécurité. Elle peut aussi ne disposer d'aucun outil NDR, ne s'appuyant que sur une solution EDR ou XDR. Pour relier les informations, l'organisation s'appuie alors sur une plateforme SIEM ou SOAR existante afin de corréler les données et d'orchestrer les flux de travail de réponse.

Phase opérationnelle

Si cette approche offre une certaine flexibilité et permet de tirer parti des outils déjà en place, elle introduit une complexité significative. Le SOC doit gérer plusieurs consoles, tableaux de bord et systèmes d'alerte. Les investigations sont souvent plus lentes, les analystes devant corréler manuellement les événements issus de différents outils, chacun reposant sur son propre modèle de données et sa propre logique de détection.

Mise à l'échelle

L'extension de la couverture vers le cloud, les identités ou les couches applicatives nécessite l'acquisition de nouveaux produits ponctuels, leur intégration au SIEM, ainsi que l'ajustement des règles ou des playbooks associés.

Avec le temps, la charge pesant sur les équipes d'ingénierie et d'exploitation s'alourdit : efforts dupliqués entre les outils, visibilité fragmentée et coordination de la réponse irrégulière.

Scénario 2 : Sécurité sur plateforme

Configuration initiale

Une organisation adopte des capacités de détection email et réseau auprès d'un même fournisseur, fournies via une plateforme unique pilotée par l'IA et une interface opérationnelle unifiée. Les deux surfaces alimentent le même modèle comportemental, avec une intelligence et une visibilité partagées de manière transparente sur l'ensemble de l'environnement.

Phase opérationnelle

Les équipes de sécurité bénéficient de flux de travail pré-intégrés, d'un système d'alerte cohérent et d'une corrélation des incidents native. Lorsqu'une attaque initiée par email entraîne une activité interne suspecte, l'ensemble est présenté dans une vue unifiée, réduisant le temps d'investigation et éliminant la nécessité de combler manuellement les écarts entre les outils ou les équipes. Les services optionnels, tels que le service MDR, peuvent opérer sur les deux surfaces sans duplication des efforts.

Mise à l'échelle

À mesure que le paysage des menaces évolue, l'extension vers d'autres domaines, comme les comptes cloud, les identités utilisateurs ou les endpoints, peut se faire de manière incrémentale, sans devoir repenser l'architecture de la pile de sécurité. Les nouvelles capacités s'intègrent au même modèle, préservant le contexte et permettant une protection intégrée sur l'ensemble de l'environnement numérique.

Passer à l'étape suivante

À mesure que les attaquants utilisent de plus en plus l'IA pour rechercher, automatiser et accélérer leurs actions, les défenseurs ne peuvent plus se contenter d'outils superficiellement intégrés ou de processus manuels. Unifier la sécurité réseau et messagerie ne se limite pas à l'efficacité : il s'agit de créer un écosystème de sécurité plus puissant que la somme de ses parties.

Nous avons conçu la plateforme Darktrace ActiveAI Security pour offrir une sécurité proactive et corrélative qui pense comme un attaquant, vous donnant visibilité et agilité pour défendre votre organisation contre les menaces ciblées et multi-domaines qui échappent aux efforts de détection isolés.

Vous êtes prêt à passer à l'étape suivante ?

Demandez une démo personnalisée pour découvrir la protection unifiée en action.

Demandez une démo ↗

Découvrez comment ce client a réduit le délai moyen de confinement de 80 % grâce à Darktrace

Étude de cas ↗

Calculez votre ROI avec Darktrace / EMAIL

Obtenez votre ROI ↗

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