

Sécuriser l'ère de l'IA grâce à la sécurité comportementale

Partenariat primé. Technologies complémentaires.

Microsoft aide les entreprises à créer, déployer et développer leurs solutions d'IA. Darktrace vous aide à utiliser l'IA en toute sécurité.

À mesure que l'IA passe d'un rôle d'assistance aux employés à l'exécution d'actions sur les identités, les données, les applications et les infrastructures, les équipes de sécurité doivent aller au-delà de la simple connaissance des autorisations accordées. Elles doivent déterminer si les utilisateurs, les systèmes d'IA et les agents se comportent comme prévu une fois intégrés à l'environnement de l'entreprise.

Microsoft met en place les contrôles d'identité, de gouvernance, de protection des données et de sécurité qui définissent les actions autorisées pour les utilisateurs et les systèmes d'IA. Darktrace apporte une compréhension contextuelle des comportements de l'IA, des utilisateurs et des infrastructures. Cette approche aide les équipes à repérer les activités qui s'écartent des comportements habituels de l'entreprise ou des objectifs prévus, et à intervenir avant que les risques ne s'aggravent.

Comment Darktrace étend la sécurité Microsoft



Renforcer les investissements Microsoft existants

Complétez les contrôles natifs de Microsoft en matière d'identité, de gouvernance, de conformité et de sécurité par une analyse contextuelle des comportements et des capacités de réponse autonome.



Comprendre l'activité dans son contexte métier

Allez au-delà des autorisations et des politiques pour comprendre comment les utilisateurs, les agents IA, les applications et l'infrastructure se comportent réellement.



Sécuriser l'IA à mesure que son adoption prend de l'ampleur

Étendez la sécurité comportementale à Microsoft 365 Copilot, Microsoft Agent 365 et aux autres solutions d'IA de l'entreprise, à mesure que les clients passent d'E5 à E7.



Analysez et intervenez plus rapidement dans tous les domaines

Corrélez les activités de l'IA, de la messagerie électronique, des identités, du cloud, du réseau, des points de terminaison et des technologies opérationnelles (OT), afin d'analyser les attaques comme des incidents uniques plutôt que comme une succession d'alertes isolées.

Darktrace + Microsoft : une sécurité couvrant l'IA, les utilisateurs et les infrastructures

Microsoft fournit les plateformes et les contrôles de sécurité, tandis que Darktrace apporte un contexte comportemental en temps réel à l'ensemble de votre environnement Microsoft. Les tableaux ci-dessous montrent comment Darktrace complète les capacités de Microsoft dans chaque domaine.

/ SECURE AI + Microsoft

Sécuriser l'adoption de l'IA, de l'usage à l'exécution

Darktrace / SECURE AI complète les fonctionnalités de Microsoft en matière d'IA, de gestion des identités et de gouvernance en offrant une visibilité sur l'utilisation réelle de l'IA, des prompts aux utilisateurs en passant par les agents, les activités de développement et l'IA fantôme.

Microsoft fournit

Darktrace ajoute

Microsoft 365 Copilot - Expériences d'IA d'entreprise au sein de Microsoft 365.

Surveille les prompts, les sessions et les réponses pris en charge afin de détecter les expositions de données sensibles, les tentatives de contournement des protections (jailbreak) et les comportements inattendus de l'IA.

Microsoft Copilot Studio - Outils pour créer, configurer et déployer des agents IA.

Met en relation le développement et la configuration des agents avec leur comportement en cours d'exécution afin de détecter les mauvaises configurations, les activités anormales et les écarts par rapport aux objectifs prévus.

Microsoft Entra + Agent 365 - Identité, autorisations, cycle de vie et gouvernance des utilisateurs et des agents.

Offre une visibilité sur les identités, les autorisations et les actions des agents afin d'identifier les accès excessifs, les connexions inattendues et les comportements à risque.

Microsoft Entra Global Secure Access - Contrôles d'accès sécurisés pour les utilisateurs, les appareils et l'activité web.

Étend la détection de l'IA fantôme grâce à l'analyse des activités prises en charge par les passerelles Web sécurisées, afin d'identifier les services et les utilisations d'IA non autorisés.

Microsoft Foundry + Defender for Cloud + Purview - fonctionnalités de développement de l'IA, de gestion de la posture de sécurité, de gouvernance et de protection des données.

Identifie les activités de développement à risque, les mauvaises configurations et les autorisations excessives, tout en associant les informations acquises lors du développement à l'activité de l'IA au moment de l'exécution.

« Darktrace / SECURE AI nous a permis d'obtenir une vision plus claire de l'utilisation de l'IA dans l'ensemble de notre organisation, notamment des outils utilisés par les employés et des types de données présents dans les prompts. » ¹

■ Matthew Davis

Directeur de la sécurité des systèmes d'information,
ESL Federal Credit Union

¹darktrace.com/news/darktrace-extends-behavioral-security-with-general-availability-of-darktrace-secure-ai

Propulsé par l'IA adaptative

L'IA adaptative est la technologie d'IA propriétaire de Darktrace, développée pendant plus d'une décennie pour apprendre le fonctionnement de chaque organisation et appliquer la technique d'IA adaptée à chaque défi de sécurité.

Profil comportemental unique

Une représentation évolutive du fonctionnement et des interactions propres à votre entreprise, englobant l'IA, les collaborateurs et les infrastructures.

360° Insights

Une vision corrélée, en constante évolution, des informations et des menaces dans l'ensemble de l'environnement numérique.

Real-Time AI Analyst

S'appuie sur une compréhension comportementale en temps réel pour détecter, effectuer le triage, mener des investigations et répondre à la vitesse des machines.

/ EMAIL + Microsoft

Protégez les communications en tenant compte de la manière dont les personnes travaillent réellement

Darktrace / EMAIL complète les capacités de Microsoft en matière d'e-mails, de collaboration et de protection des données en comprenant les communications dans le contexte du fonctionnement réel de chaque entreprise.

Microsoft fournit	Darktrace ajoute
Defender pour Office 365 - Protection native des e-mails et de la collaboration.	Contexte comportemental pour aider à identifier et à détecter les attaques sophistiquées et inédites, avec des flux de travail unifiés de mise en quarantaine permettant de rationaliser l'investigation et la remédiation.
Microsoft Teams - Communication et collaboration d'entreprise.	Détecte l'ingénierie sociale et les activités suspectes dans les conversations Teams prises en charge.
Microsoft Purview - Contrôles de protection des données, de gouvernance et de conformité.	Combine l'analyse des comportements, du contenu et des étiquettes de confidentialité pour prévenir les pertes de données par e-mail.
Microsoft Security Copilot - investigations de sécurité et flux de travail opérationnels assistés par l'IA.	Les résultats des investigations de Darktrace et le contexte de sécurité de la messagerie dans les flux de travail déjà utilisés par les équipes de sécurité.

/ HYBRID NETWORK + Microsoft

Comprenez les menaces qui pèsent sur les infrastructures dont dépendent l'IA et l'entreprise

Darktrace / HYBRID NETWORK étend la protection de Microsoft à l'ensemble de l'environnement hybride en s'appuyant sur l'analyse contextuelle des comportements pour détecter les menaces qui se propagent entre le réseau, le cloud, les identités, les points de terminaison et les technologies opérationnelles.

Microsoft fournit	Darktrace ajoute
Microsoft Defender for Endpoint - Détection et protection des points de terminaison.	Met en relation les activités des points de terminaison avec les comportements observés sur le réseau et les infrastructures afin de détecter les menaces qui dépassent le périmètre des appareils individuels.
Microsoft Sentinel - Analyses de sécurité, gestion des incidents et flux de travail des opérations de sécurité.	Intègre les incidents Darktrace et les résultats des investigations pilotées par l'IA aux workflows Sentinel, afin d'aider les analystes à hiérarchiser les menaces et à accélérer la réponse.
Microsoft Azure - Infrastructure et services cloud.	Détection et réponse comportementales sur les charges de travail Azure et l'environnement hybride élargi.
Microsoft 365 + environnements hybrides - Productivité, identité et services d'entreprise.	Fournit une vision contextuelle transversale des identités, du réseau, du cloud, des points de terminaison et des technologies opérationnelles, afin d'analyser les attaques comme des incidents uniques en constante évolution.

Mieux ensemble pour les équipes de sécurité

**Moins de temps passé à regrouper les alertes.
Plus de temps pour agir sur ce qui compte.**

La fonctionnalité Real-Time AI Analyst de Darktrace s'appuie sur sa compréhension des comportements propres à l'organisation pour détecter, analyser et hiérarchiser les menaces émergentes sur l'ensemble de la plateforme. Dans le cadre des intégrations Microsoft existantes, les fonctionnalités d'investigation de Darktrace Cyber AI Analyst peuvent enrichir les processus de travail de Microsoft Sentinel et de Security Copilot, en intégrant les informations contextuelles de Darktrace aux outils déjà utilisés par les analystes.

« Darktrace et Microsoft proposent des approches complémentaires qui permettent à notre équipe de sécurité de travailler plus sereinement. Nous savons que si une menace échappe à l'une des solutions, l'autre pourra la détecter. » ²

■ **Mark Kane,**
Directeur mondial des solutions d'information,
Mainstream Renewable Power

2: darktrace.com/ja/customers/mainstream-renewable-power