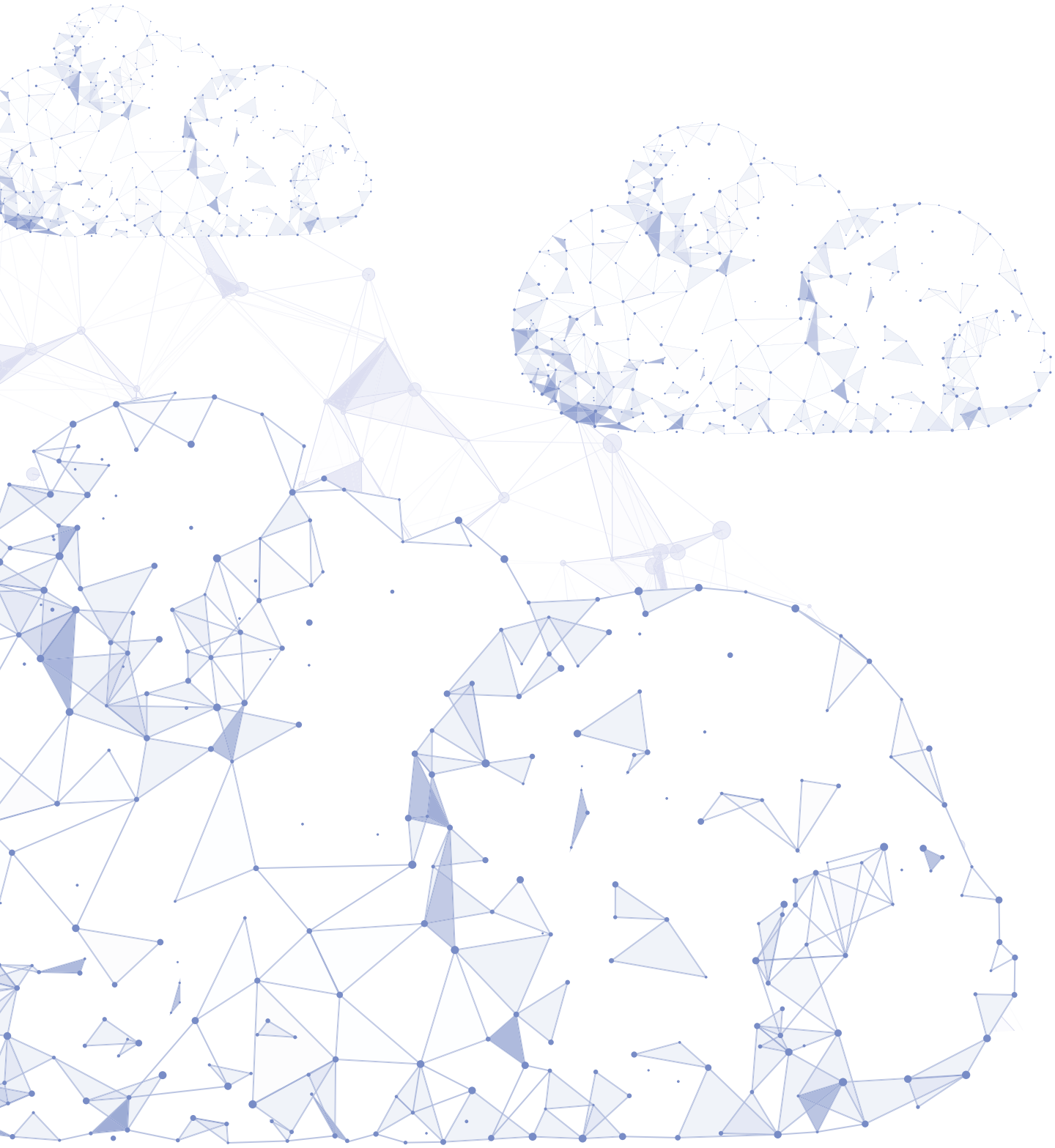
DARKTRACE



Cyber IA Darktrace

Un système immunitaire pour la sécurité du cloud

> À l'heure où les organisations développent leur présence numérique dans des environnements hybrides, multi-cloud et IoT, elles ont la responsabilité de protéger et de contrôler une plus grande diversité de secteurs. Cette complexité ouvre de nouvelles perspectives pour les criminels, qui peuvent alors affecter la fiabilité opérationnelle, perpétrer de nouveaux types de crimes et impacter directement le fonctionnement des entreprises.
>
> **– Forrester**

Contents

Introduction 1

La plateforme de cyber IA 2

Informations d'identification compromises 4

- Attaque SharePoint 5
- Tentative de connexion à un SaaS depuis l'Équateur 5
- Connexion inhabituelle dans une banque du Panama 6
- Attaque par force brute automatisée 6
- Prise de contrôle d'un compte Office 365 compromis 7

Menaces internes 8

- Employé du service informatique mécontent 9

Erreurs de configuration 10

- Attaque Shodan via une faille dans le cloud 11
- Informations à caractère personnel non chiffrées dans AWS 11
- Installation involontaire d'un logiciel de minage de cryptomonnaies 12
- Exposition de propriété intellectuelle dans Azure 12
- L'ingénieur DevOps trop zélé 13

Scénarios de déploiement 14

Conclusion 16

Introduction

Des petites entreprises cherchant à réduire leurs coûts jusqu'aux grands centres d'innovation à l'origine de projets de transformation numérique, le voyage vers le cloud change en profondeur le visage de l'entreprise numérique et le paradigme traditionnel du périmètre réseau n'est plus qu'un souvenir. À mesure que ce périmètre s'efface, l'infrastructure hybride et multi-cloud commence à faire partie des actifs numériques de toute l'entreprise de plus en plus diversifiée. Les organisations sont aujourd'hui capables de repousser les limites de l'innovation, tout en étendant leur surface d'attaque à une vitesse inquiétante.

Ainsi, le numérique est une arme à double tranchant, et il serait dangereux de sous-estimer les problèmes de sécurité auxquels sont confrontés les dirigeants d'entreprise dans leur voyage vers le cloud. Le « cloud » recouvre en effet un large éventail de systèmes et de services, et il incombe bien souvent à une seule équipe de sécurité isolée de gérer la sécurité des charges de travail dans le cloud sur les environnements AWS et Azure, des communications par e-mail dans Office 365, des données client dans Salesforce, du partage de fichiers via Dropbox, et des serveurs virtualisés dans les centres de données traditionnels sur site.

Cette mosaïque complexe de plateformes cloud offre généralement des avantages en termes d'efficacité, de flexibilité et d'innovation, mais elle a un impact néfaste sur la cohérence et la traçabilité de la stratégie de sécurité. Le cloud sous toutes ses formes est souvent un territoire méconnu des équipes de sécurité traditionnelles. Les outils et pratiques de sécurité habituelles ne s'appliquent pas aux environnements hybrides ou multi-cloud, ou ils sont trop lents ou compartimentés pour protéger efficacement l'infrastructure contre les attaques sophistiquées.

Même si un grand nombre de solutions de sécurité natives de cloud s'avèrent utiles en termes de conformité et d'analyse basée sur des journaux, elles sont rarement assez robustes et unifiées pour offrir une couverture suffisante : elles continuent à encourager une approche "cloisonnée", et comme elles s'appuient sur des règles, des signatures ou des suppositions antérieures, elles ne sont pas en mesure de détecter les menaces nouvelles ou internes et subtiles, avant qu'elles ne se transforment en crise.

Pire encore, le manque de visibilité et de contrôle des équipes de sécurité sur ce secteur s'ajoute au besoin d'une mentalité nouvelle et peu habituelle pour s'adapter à l'agilité et à la vitesse du cloud. L'entreprise devient donc une cible attrayante pour les cybercriminels, qui cherchent toujours à maximiser les profits tout en restant suffisamment discrets pour ne pas attirer l'attention des autorités et éviter toute détection. La sécurité du cloud n'est pas à la hauteur de ce qu'elle devrait être, et les cybercriminels le savent mieux que quiconque.

Pourtant, sous bien des aspects, les organisations ont aujourd'hui besoin de bien plus qu'une simple solution de sécurité du cloud : elles ont besoin d'une protection à l'échelle de toute l'entreprise, d'une plateforme unifiée agissant à la vitesse du numérique, capable de s'adapter aux menaces futures afin de détecter les signes indicateurs d'une attaque sophistiquée au moment même où elle établit sa présence sur un réseau.

La plateforme de cyber IA

Limites de l'approche en silo de la sécurité du cloud

Les fournisseurs de service cloud et les prestataires tiers proposent de nombreuses solutions de sécurité « cloud-native » permettant à leurs clients de protéger leur partie du modèle de responsabilité partagée. Toutefois, ces solutions ponctuelles, qu'elles soient natives ou tierces, sont généralement mal équipées pour détecter et neutraliser les menaces sophistiquées dans le cloud.

Contrôles natifs : Nécessaires, mais insuffisants

Les contrôles de sécurité natifs sont bien souvent exclusivement conçus pour un fournisseur de cloud unique, et ne couvrent qu'une petite partie de l'entreprise hybride multi-cloud. Cette caractéristique limite considérablement le périmètre de détection et ajoute plus de complexité à une pile de sécurité déjà difficile à appréhender.

En général, les contrôles natifs facilitent la conformité, la collecte de journaux et la création de stratégies statiques, mais ils ne sont pas conçus pour la détection et la neutralisation des menaces sophistiquées sur plusieurs services de cloud et silos de données.

Contrôles tiers : Nécessaires, mais insuffisants

Les contrôles tiers comme les solutions CASB et CWPP sont également utiles, mais insuffisants. Les systèmes CASB, par exemple, participent à la découverte, à la création de stratégies granulaires et à la conformité, mais ils échouent souvent lorsqu'il s'agit de détecter des cybermenaces les plus sophistiquées : informations d'identification compromises, ransomware, menaces internes d'employés mécontents ou encore espionnage industriel.

Même si les contrôles tiers fournissent en général une visibilité multi-cloud, ils ne fournissent aucune information sur le réseau physique de l'organisation. Cette limite est importante : corréler les renseignement provenant du cloud et du réseau de l'entreprise est parfois le seul moyen pour un système de sécurité de mettre en évidence la présence d'une menace émergente.

Un cyber système immunitaire pour le cloud et bien plus

Basée sur l'intelligence artificielle, la plateforme de cyber IA de Darktrace comble ces vides critiques en proposant une approche unique à l'échelle de toute l'entreprise. Elle est ainsi capable de détecter et de neutraliser les attaques dans le cloud qui échappent aux autres outils.

À l'image du système immunitaire humain, cette technologie développe un sens inné de ce qui constitue l'identité de chacun. Elle apprend le « modèle comportemental normal » de chaque utilisateur, appareil et conteneur dans les environnements hybrides et multi-cloud. L'IA auto-apprenante de Darktrace analyse en permanence le comportement de tous les utilisateurs et de tous les appareils de l'entreprise. Elle est ainsi capable de détecter les signaux même faibles et subtils indiquant une attaque sophistiquée, sans pour autant définir à l'avance ce qui constitue un élément « bénin » ou « malveillant ».

Les solutions ponctuelles préprogrammées sont indéniablement utiles pour compléter cette approche, mais Darktrace est la seule solution reconnue pour sa capacité à stopper l'ensemble des cybermenaces qui pèsent sur le cloud. Il peut s'agir d'attaques internes ou externes ou d'erreurs de configuration critiques susceptibles d'exposer l'entreprise à des failles, et ce quel que soit leur point d'origine. Ces points d'origine sont multiples : campagnes d'hameçonnage ciblé, piratage de compte professionnel, exfiltration de données lente et discrète, ou encore mouvement latéral sur le cloud.

Protection unifiée sur-mesure

Grâce à sa compréhension des actifs numériques de toute l'entreprise, Darktrace corrèle toutes les activités sur site avec le trafic des environnements hybrides et multi-cloud en temps réel. Cela lui permet de comprendre qu'un comportement anodin observé isolément dans le cloud peut indiquer une activité malveillante bien plus généralisée.

Par exemple, nous pouvons voir qu'un utilisateur s'est connecté à AWS dans le cloud. Ce comportement n'est pas malveillant en soi, mais Darktrace sait également que le compte Office365 de ce même utilisateur a probablement été compromis quelques instants auparavant, car elle a détecté un emplacement de connexion inhabituel. Darktrace comprend que la connexion à AWS est en réalité très suspecte.

> Les leaders de la sécurité cherchent de plus en plus à gagner en efficacité en intégrant des produits ponctuels à des plateformes de sécurité qui elles sont plus larges.
>
> **– Gartner**

Corrélation d'informations au niveau des conteneurs

Malgré la démocratisation des conteneurs auprès des développeurs, la sécurité reste souvent à la traîne. Les conteneurs étant virtualisés, le trafic intra-serveur est difficile à superviser. Alors que les systèmes basés sur des règles suivent uniquement les données entre différents serveurs, Darktrace est capable de fournir une visibilité sur les environnements en conteneurs au sein de chaque serveur.

De plus, Darktrace étend la visibilité des conteneurs et les rapprochent de l'activité de toute l'infrastructure numérique (cloud, IoT, messagerie électronique, systèmes industriels et autres environnements). Une anomalie constatée au niveau du trafic réseau d'un conteneur peut ainsi être associée à une base de données dans le cloud, qui peut elle-même être corrélée à un compte de messagerie de l'entreprise.

Découvrez des scénarios de déploiement page 14

AI Analyst : Analyse automatisée des menaces

Le Cyber AI Analyst ajoute une étape supplémentaire : il analyse automatiquement les menaces détectées par l'Enterprise Immune System et produit un tableau de bord dynamique de la situation ainsi que des rapports générés par l'IA permettant de communiquer la dimension d'un incident de sécurité donné.

En corrélant en temps réel le trafic cloud avec le reste du réseau, l'AI Analyst est capable de mener des centaines d'analyses simultanément, en rassemblant une constellation d'alertes et d'indicateurs pour développer une compréhension pertinente des incidents, le tout à la vitesse de la machine. Il communique ensuite ses résultats et ses recommandations sous la forme d'incidents AI Analyst, qui sont enrichis grâce aux informations de contexte et de sécurité, et peuvent alors être examinés et traduits en actions concrètes par les dirigeants ou les utilisateurs finaux.

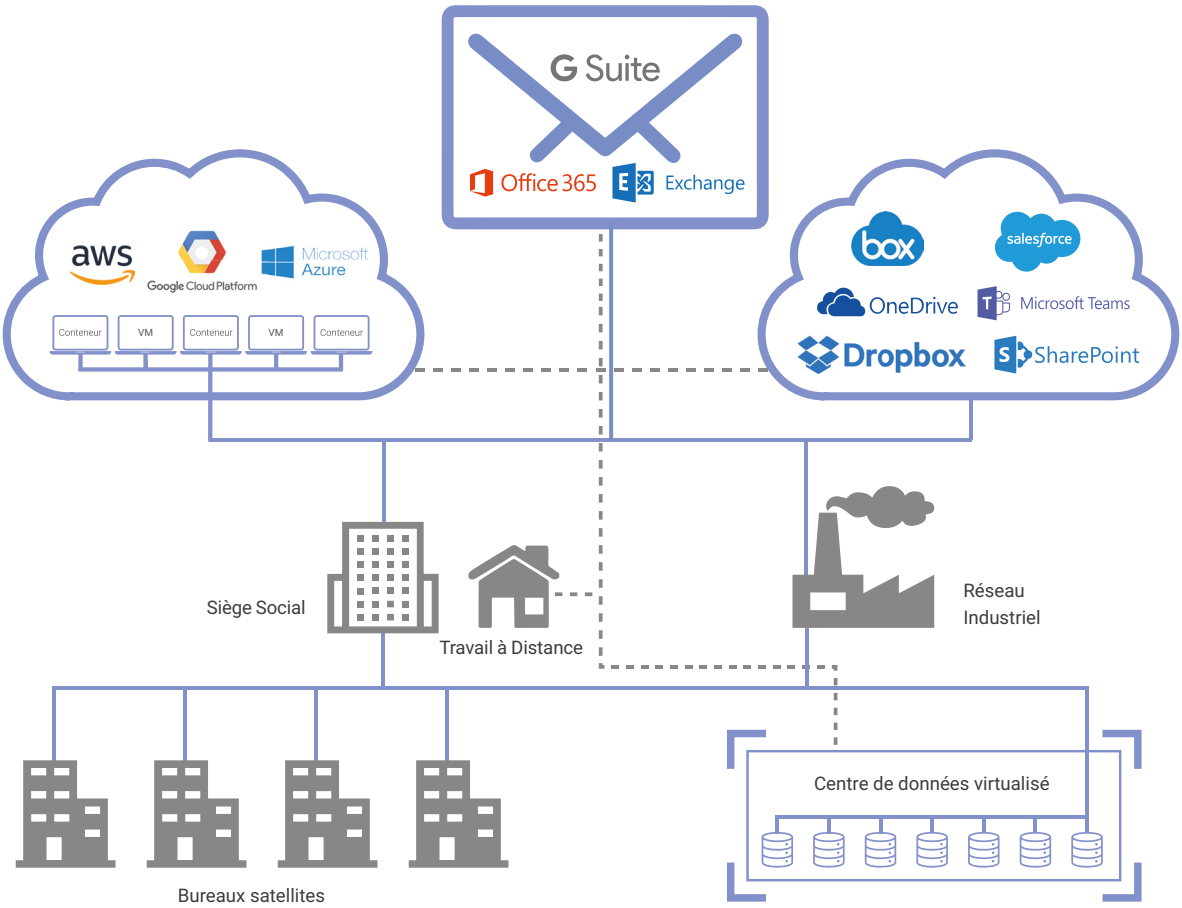


Figure 1: La couverture unifiée de tous les actifs numériques offerte par Darktrace

Informations d'identification compromises

29 % des fuites de données impliquent le vol d'informations d'identification

Source: Verizon 2019

Les cybercriminels expérimentés peuvent subtiliser des identifiants de comptes de plusieurs façons. Cela peut être par le biais d'une attaque d'ingénierie sociale, ou encore en utilisant un malware « intelligent » capable de filtrer le trafic et les actifs éphémères du cloud pour y rechercher des mots de passe. Les données volées étant faciles à acheter et à vendre sur le Dark Web, la fréquence et la gravité des vols d'informations de connexion augmente d'année en année.

Les scénarios de prises de contrôle de comptes ne représentent que la première étape d'une cybermenace. L'objectif final d'une attaque basée sur le vol d'identifiants de comptes consiste à utiliser les mots de passe dérobés pour s'authentifier auprès des applications et ainsi voler des données. Une fois qu'un attaquant dispose des informations d'identification nécessaires pour se comporter comme un utilisateur réel, il devient très difficile de distinguer l'intrus de l'employé légitime, celui dont il a usurpé l'identité.

En corrélant les données sur l'ensemble des environnements hybrides et multi-cloud, Darktrace apprend le « modèle comportemental normal » de chaque utilisateur. Ce modèle s'appuie sur des centaines d'indicateurs, ce qui lui permet de détecter les écarts de comportement subtils qui indiqueraient une prise de contrôle de compte. En apprenant le « modèle comportemental normal » du groupe de pairs de l'utilisateur concerné, et en tenant compte du contexte de toute l'entreprise, l'IA de Darktrace signale de façon rétrospective tout comportement inhabituel, même dans le cas de faille préexistante.

Figure 2: L'IA de Darktrace détecte une activité inhabituelle relative à un compte de cloud compromis

Attaque SharePoint

Après avoir récupéré des identifiants de comptes volés ou après avoir réussi à accéder au système de transfert de fichier basé dans le cloud d'une organisation, les cybercriminels exécutent souvent des scripts afin d'identifier les fichiers contenant des mots-clés comme « mot de passe ». Darktrace a découvert une menace de ce type dans une banque européenne : les pirates avaient réussi à trouver un fichier Office 365 SharePoint contenant des mots de passe non chiffrés. Les auteurs de l'attaque, ayant contourné les contrôles natifs de Microsoft, pensaient avoir échappé à toute surveillance.

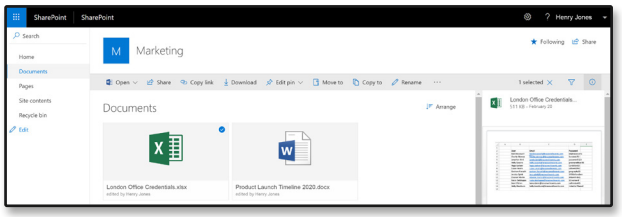


Figure 3: L'accès Sharepoint aux fichiers sensibles

Cependant, l'IA de Darktrace a signalé cette activité comme étant anormale pour l'utilisateur de l'entreprise, son groupe de pairs, ainsi que pour l'organisation dans son ensemble, en détectant l'accès inhabituel à ces fichiers sensibles entre autres indicateurs. Enfin, la compréhension nuancée et en continuelle évolution de l'IA de ce qui constitue une situation normale au sein de l'organisation s'est avérée ici critique ; l'accès suspect au fichier aurait très bien pu être bénin dans d'autres circonstances.

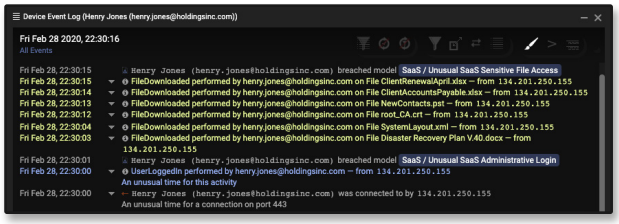


Figure 4: Darktrace identifie le téléchargement de fichiers sensibles

Ces pirates auraient très certainement exploité les mots de passe non chiffrés pour augmenter leurs privilèges et infiltrer davantage l'organisation. Cependant, en apprenant le « modèle comportemental normal » de chaque utilisateur et de chaque appareil de l'organisation, l'IA de Darktrace a pu signaler la menace à l'équipe de sécurité avant qu'elle ne puisse se transformer en crise.

Tentative de connexion à un SaaS depuis l'Équateur

Dans une organisation internationale, Darktrace a détecté une faille au niveau d'un compte Office 365, celui-ci contournait les contrôles natifs d'Azure Active Directory. Même si l'organisation possédait des bureaux dans le monde entier, l'IA de Darktrace détecta une connexion provenant d'une adresse IP inhabituelle d'un point de vue historique pour cette utilisatrice et son groupe de pairs, et a immédiatement alerté l'équipe de sécurité. Darktrace a ensuite signalé qu'une nouvelle règle de traitement des e-mails avait été mise en place sur ce compte pour supprimer les e-mails entrants. Il s'agissait là d'un signe indéniable de compromission, et l'équipe de sécurité a pu verrouiller le compte en question avant que l'assaillant ne puisse causer des dégâts.

Lorsque l'équipe de sécurité a enquêté davantage sur cet incident, elle a découvert que l'utilisatrice avait reçu un e-mail de phishing quelques heures seulement avant que Darktrace ne détecte la menace. L'entreprise avait également déployé Microsoft ATP (Advanced Threat Protection) pour Office 365, mais les mécanismes de défense statiques comme ATP sont uniquement capables de détecter les attaques de phishing en comparant les liens contenus dans les e-mails à des adresses malveillantes déjà connues, et le lien de phishing ne figurait pas sur leur liste. Cet événement témoigne des limites d'une approche basée sur des signatures dans ce secteur. L'organisation a rapidement déployé Antigena, la technologie de Réponse Autonome de Darktrace. Elle bénéficie ainsi d'une protection supplémentaire dans Office 365 grâce à sa capacité à détecter les e-mails de phishing similaires, et ce sans se baser sur des listes noires.

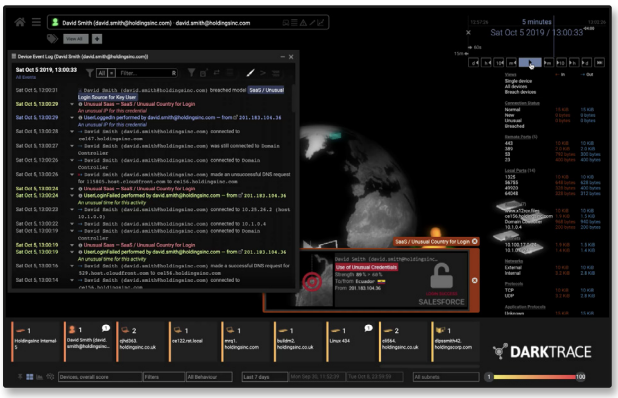


Figure 5: L'IA de détecte l'emplacement inhabituel de la connexion SaaS

Connexion inhabituelle dans une banque du Panama

Un compte Office 365 a été utilisé pour mener une attaque par force brute contre une banque bien connue du Panama. Les tentatives de connexion émanaient d'un pays qui présentait un écart avec le modèle comportemental normal des opérations de l'entreprise.

Darktrace a identifié 885 tentatives de connexion sur une période de 7 jours. Même si la majorité des authentifications provenait d'adresses IP situées au Panama, 15 % des tentatives d'authentification provenaient d'une adresse IP 100 % rare située en Inde. Après analyse, il s'est avéré que ce point de terminaison externe apparaissait sur de nombreuses listes noires de spam, et qu'il avait récemment été associé à un comportement en ligne abusif (avec potentiellement des scans Internet non autorisés ou des activités de piratage).

Figure 6: Interface utilisateur présentant les emplacements de connexion

Darktrace a ensuite assisté à ce qui semblait être un abus de la fonction de réinitialisation de mot de passe : l'utilisateur situé en Inde changeait de privilèges du compte de façon très inhabituelle. L'activité s'est avérée particulièrement suspecte lorsqu'après chaque réinitialisation du mot de passe, on observa des échecs de connexion à partir d'une adresse IP normalement associée avec l'organisation, ce qui suggérait que l'utilisateur légitime n'avait plus accès à son compte.

03/12 20:45:39	Saas::Admin	Regular	UpdateUser
03/12 20:45:39	Saas::Admin	Regular	ChangeUserLicense
03/12 20:26:43	Saas::Login	Regular	UserLoggedIn
03/12 20:26:43	Saas::FailedLogin	Regular	UserLoginFailed
03/12 20:26:36	Saas::FailedLogin	Regular	UserLoginFailed
03/12 18:31:31	Saas::Login	Regular	UserLoggedIn
03/12 17:57:46	Saas::Admin	Regular	ChangeUserLicense
03/12 17:57:46	Saas::Admin	Regular	UpdateUser
03/12 17:06:57	Saas::Admin	Regular	UpdateUser

Figure 7: L'activité associée au compte SaaS, mettant en évidence la modification des informations de connexion

Attaque par force brute automatisée

Darktrace a détecté plusieurs échecs de connexion à un compte SaaS utilisant les mêmes informations de connexion, et ce chaque jour pendant une semaine. Chaque groupe de tentatives de connexion avait lieu précisément à 18h04 pendant 6 jours. La régularité de l'heure et du nombre de tentatives de connexion indiquait une attaque par force brute automatisée, programmée pour s'arrêter après un certain nombre d'échecs afin d'éviter tout verrouillage du compte.

Darktrace a estimé que ce modèle de tentatives de connexion était hautement anormal et a alerté l'équipe de sécurité. Si Darktrace n'avait pas corrélé les multiples indicateurs faibles et ainsi identifié les signaux subtils d'une menace émergente, cette attaque automatisée aurait continué pendant des semaines ou des mois, en tentant de deviner le mot de passe de l'utilisateur et en s'appuyant sur d'autres informations récoltées au préalable.

Figure 8: Graphique illustrant les tentatives répétées de connexion

Prise de contrôle d'un compte Office 365 compromis

Après avoir cliqué sur un lien malveillant contenu dans un e-mail ciblé, une employée a saisi ses informations de connexion sur une fausse page qui enregistrait cette saisie. Équipés de ses informations, les attaquants ont pivoté vers Office 365, en les utilisant pour se connecter à distance. Darktrace a détecté deux emplacements de connexion inhabituels : la Bulgarie et l'Indonésie.

En apprenant les modèles relatifs aux emplacements habituels de travail des utilisateurs, et en sachant quand et comment ils accèdent aux services de cloud, l'IA de Darktrace a non seulement identifié mais aurait même pu empêcher ces tentatives de connexion inhabituelles. Dans ce cas, les fonctionnalités de sécurité natives n'avaient pas identifié ni bloqué ces connexions malveillantes.

Après avoir accédé au compte Office 365 de l'employée, les attaquants se sont mis en quête d'autres victimes, répétant le même cycle. Alors, Darktrace a constaté un autre changement de comportement : l'envoi de 99 e-mails comportant comme objet « Avis de règlement » à un large éventail d'entreprises. Même si ce comportement pourrait être normal pour certains employés, celui-ci échappait au modèle comportemental normal de l'employée en question.

Darktrace a également constaté la création d'une nouvelle règle de transfert dans la boîte de réception ; cette règle est souvent créée par les attaquants pour diffuser des spams ou dissimuler leur activité.

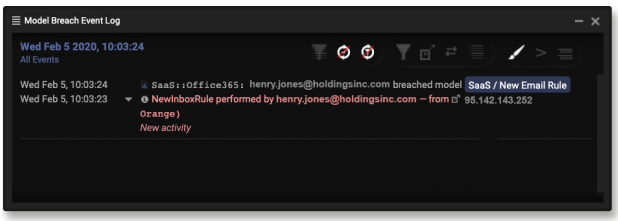


Figure 9: Darktrace détecte la règle de transfert dans la boîte de réception

En supprimant automatiquement les e-mails après les avoir envoyés, l'ensemble de preuves est détruit au sein du système de messagerie. Cependant, en supervisant de façon indépendante les e-mails et les activités des comptes de SaaS, Darktrace a été capable d'identifier les activités de l'attaquant dans leur globalité. La capacité de la plateforme à assimiler les identités et les comportements à l'échelle de l'entreprise entière lui ont permis de détecter l'activité suspecte.

Figure 10: Les emplacements de connexion inhabituels

Menaces internes

> L'IA de Darktrace s'adapte en continu. Elle met en lumière notre réseau et notre infrastructure cloud en temps réel, ce qui nous permet de protéger notre cloud en toute confiance
>
> **CISO, Aptean**

Les menaces internes dans le cloud sont plus souvent problématiques pour les organisations que celles des attaquants, et ce pour une bonne raison : ils se trouvent déjà à l'intérieur du système. Un employé mal intentionné bénéficie d'une position unique lui permettant d'échapper aux mécanismes de contrôle traditionnels ; il dispose d'un accès privilégié au réseau qu'il connaît parfaitement.

Les services de cloud ont contribué à étendre l'impact des menaces internes, ne serait-ce que vis-à-vis du grande nombre d'applications en jeu qui sont des vecteurs d'exfiltration de données, ou encore à cause du manque de visibilité sur ce domaine qui permet d'extraire des données sans être repéré.

Par nature, les outils de sécurité traditionnels ne détectent pas les activités malveillantes qui se produisent au sein même de l'organisation. La sécurité du cloud requiert aujourd'hui une approche complète, qui analyse le trafic sur l'ensemble des actifs numériques et élabore en permanence un « modèle comportemental normal » de l'organisation complète.

Qu'il s'agisse d'un commercial qui passe à la concurrence et emmène avec lui des informations client, ou d'un administrateur informatique mécontent qui manipule des données critiques, l'intelligence artificielle peut être utilisée pour détecter tout activité anormale et inhabituelle symptomatique d'une cybermenace.

Figure 11: Darktrace Antigena bloque une tentative d'exfiltration de donnée sensibles par un attaquant interne

Employé du service informatique mécontent

Darktrace a été témoin d'un cas de menace interne après le licenciement d'un employé qui occupait le poste d'administrateur système. L'organisation qui l'employait avait dû congédier plusieurs personnes au cours de la semaine, mais elle ne s'était pas occupée de reprendre l'ordinateur portable des employés ni de supprimer leur compte professionnel. L'ancien administrateur s'est connecté à leurs comptes SaaS et a rapidement téléchargé plusieurs fichiers sensibles à partir de la base de données client, y compris des informations de contact et des numéros de carte de crédit.

Figure 12: Threat Visualizer affichant un pic du nombre de connexions

Il a ensuite tenté de transférer secrètement ces fichiers vers un serveur domestique en utilisant l'un des services de transfert de données couramment utilisé par l'entreprise. Avant cela, il avait pris de soin de créer un nouveau « compte secret » afin de créer une backdoor pour s'assurer qu'il aurait toujours accès à l'entreprise lorsque l'équipe informatique fermerait son compte professionnel.

Ce responsable informatique savait que ce service en particulier n'était pas régi par des règles d'entreprise, mais également qu'il était situé dans le cloud, supposant alors que l'équipe de sécurité n'aurait qu'une visibilité limitée sur ce secteur. Cependant, Darktrace analyse de façon dynamique les connexions et les événements d'accès aux fichiers dans les services de cloud d'entreprise et les corrèle avec le « modèle comportemental normal » de chaque utilisateur de l'organisation en tenant compte des nouveaux éléments. En tant que plateforme unifiée auto-apprenante, la cyber IA de Darktrace a immédiatement détecté les téléchargements inhabituels de fichiers volumineux, la création du nouveau compte et l'exfiltration de données. La technologie de Réponse Autonome Antigena s'est alors chargée de bloquer la tentative de téléchargement.

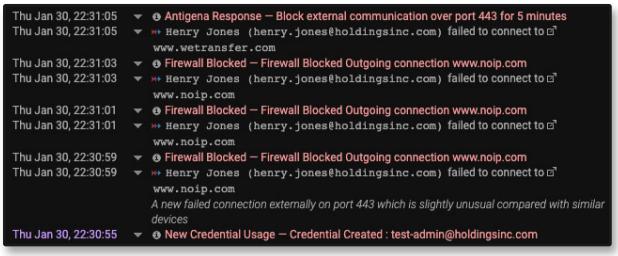


Figure 13: Darktrace Antigena met en œuvre une réponse autonome ciblée

Une analyse a révélé plus tard que l'employé avait d'abord essayé d'envoyer ces fichiers vers un serveur domestique, chez lui. Après avoir échoué, il continuait à essayer d'exfiltrer les données vers de nombreuses autres sources. Malheureusement pour lui, Antigena s'adapte de façon dynamique aux menaces à mesure qu'elles se déroulent et adapte sa réponse proportionnellement. Ainsi, chacune de ces tentatives a été interrompue de manière précise.

Après avoir tout essayé, l'employé a alors tenté de transférer tous les fichiers vers un serveur interne qu'il avait l'habitude d'utiliser lorsqu'il occupait son poste.

Son intention était de transmettre les fichiers depuis son poste habituel, mais Darktrace est intervenu pour neutraliser cette connexion.

Figure 14: Antigena bloque les tentatives de transfert de fichiers via le cloud

Même si cette activité subtile a échappé aux dispositifs de contrôle natifs du fournisseur de cloud, l'IA de Darktrace a elle détecté le comportement dangereux en quelques secondes. En apprenant continuellement le comportement normal de chaque utilisateur et de chaque périphérique, le système a pu établir intelligemment un lien entre des connexions très suspectes et des téléchargements effectués à partir de l'appareil du responsable informatique, bien que ce même service cloud soit habituellement utilisé à des fins légitimes par d'autres employés.

L'IA de Darktrace a prévenu l'équipe de sécurité en fournissant des informations précises et détaillées sur la nature de la faille, et en proposant de révoquer ses identifiants, de récupérer rapidement les données et de les sécuriser.

Erreurs de configuration

> Quasiment toutes les attaques qui visent le cloud et aboutissent sont la conséquence d'une erreur de configuration de la part du client.
>
> **– Neil MacDonald, Gartner**

La configuration des outils de contrôle de sécurité dans les environnements hybrides et multi-cloud est souvent complexe. Les solutions natives et tierces s'adressant à ce secteur sont en effet souvent disparates, incompatibles et insuffisantes. Un manque de connaissance du cloud entraîne souvent des erreurs des configuration qui exposent l'entreprise à des attaques. Les développeurs modernes ont aujourd'hui la capacité de déployer une instance de cloud en quelques minutes seulement, généralement sans avoir à consulter l'équipe de sécurité de l'entreprise. En conséquence, la majeure partie de l'organisation manque de visibilité sur ses propres environnements de cloud. Les déploiements hâtifs peuvent créer des vulnérabilités flagrantes qui peuvent passer inaperçues pendant des mois.

Les ramifications potentielles d'une erreur de configuration ont été révélées avec la fuite de données Capital One, qui a affecté plus de 100 millions de personnes en exploitant une vulnérabilité dans le cloud. Cette importante institution financière, dotée d'une sécurité du cloud mature, s'est uniquement aperçu du problème après en avoir été informée par un tiers qui avait croisé par hasard les données volées, trois mois après l'apparition de la faille.

Aujourd'hui, on utilise l'intelligence artificielle pour comprendre le « modèle comportemental normal » de chaque utilisateur, appareil et conteneur et reconnaitre les comportements subtils associés à une erreur de configuration. En s'appuyant sur une technologie auto-apprenante comme la plateforme de cyber IA de Darktrace, les organisations peuvent obtenir la connaissance des environnements de cloud complexes dont elles ont besoin pour détecter les vulnérabilités latentes dès leurs premières manifestations, avant qu'elles ne se transforment en crise.

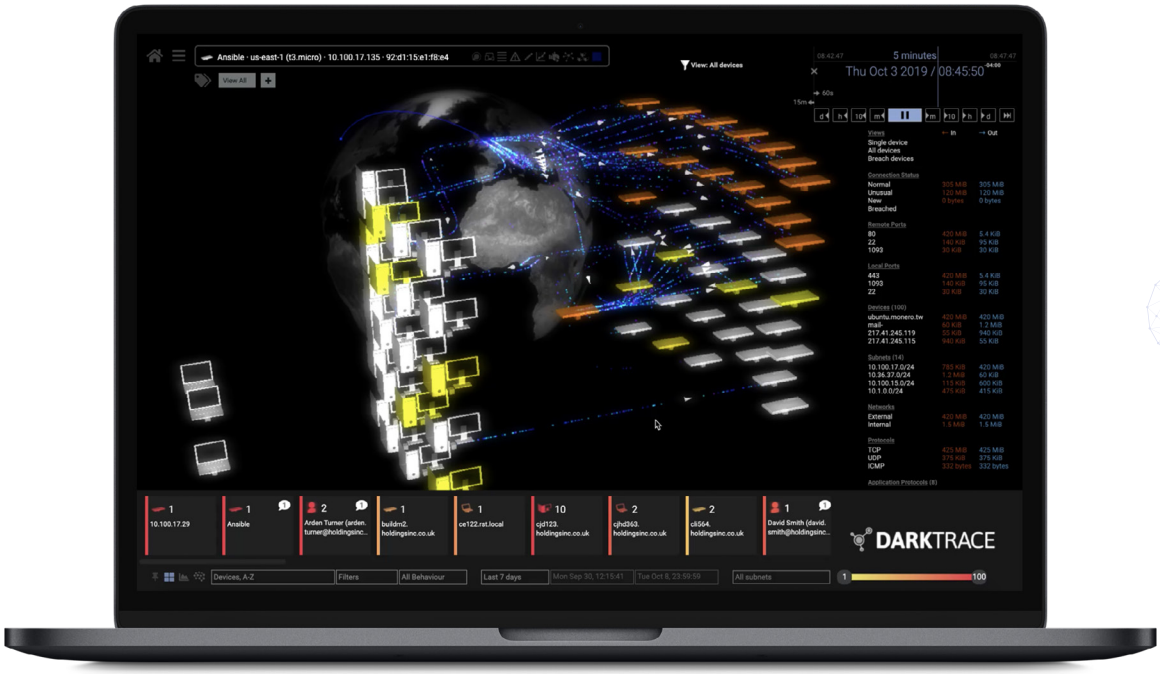


Figure 15: : Une erreur de configuration DevOps entraîne la diffusion rapide d'un logiciel de minage de cryptomonnaies

Attaque Shodan via une faille dans le cloud

Une institution financière hébergeait un grand nombre de serveurs critiques sur des technologies de virtualisation dans le cloud, dont certains devaient être en contact avec le public, alors que d'autres étaient destinés à rester privés. Pendant la configuration de leurs outils de contrôle natifs pour le cloud, l'institution a par erreur exposé un serveur important à Internet, alors qu'il était censé resté isolé derrière le pare-feu. Les origines potentielles du problème étaient multiples : la migration avait peut-être été rapide et chaotique, ou bien l'équipe de sécurité ne connaissait peut-être pas suffisamment le pare-feu natif fourni par leur CSP.

Alors que l'équipe de sécurité n'était pas consciente de cette erreur de configuration, le serveur exposé a fini par être découvert et ciblé par des cybercriminels parcourant Internet via Shodan. L'IA de Darktrace a reconnu en quelques secondes que l'appareil recevait un nombre inhabituel de tentatives de connexion entrantes provenant d'un large éventail de sources externes rares et a signalé la menace à l'équipe de sécurité.

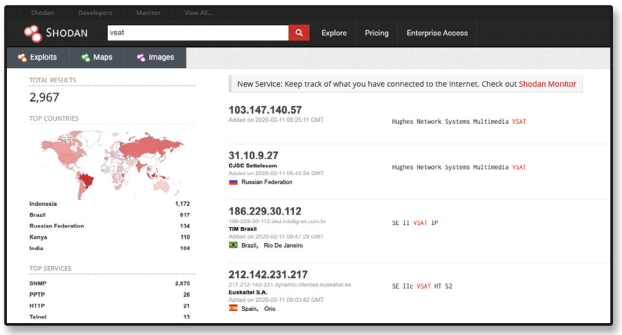


Figure 16: Le site Web Shodan a été utilisé pour rechercher des vulnérabilités

Informations à caractère personnel non chiffrées dans AWS

Aux États-Unis, une municipalité qui avait commencé à externaliser ses bases de données vers AWS a négligé d'interroger les protocoles utilisés par le serveur pour télécharger les informations. Résultat : les adresses, numéros de téléphone et numéros d'immatriculation de ses résidents ont été téléchargés vers une base de données externe à l'aide de connexions non chiffrées.

Ces données hautement sensibles étaient destinées à n'être consultées que par un nombre restreint d'employés de la municipalité. Cette négligence les rendait disponibles désormais pour n'importe quel pirate capable de scanner le périmètre du réseau et de collecter les paquets riches en données durant leur transit.

L'organisation n'avait initialement pas conscience de cette erreur de configuration, elle n'était pas détectée par les outils de sécurité utilisés. En revanche, quand Darktrace a détecté une connexion inhabituelle vers une adresse IP externe rare provenant d'un ordinateur au sein de l'organisation, la solution a confirmé que cette communication divulguait des données publiques sensibles, pouvant être utilisées par un pirate pour alimenter d'éventuelles attaques par hameçonnage ciblé ou même dans le cadre d'une usurpation d'identité. La visibilité totale et en temps réel offerte par Darktrace a donc révélé cet angle mort dangereux et a permis à l'équipe de sécurité de corriger l'erreur de configuration.

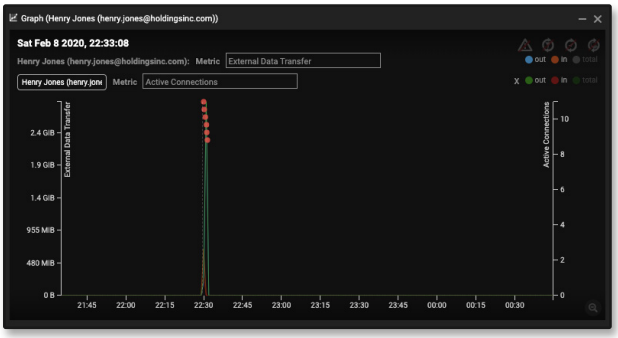


Figure 17: Threat Visualizer montrant le transfert de plus de 2 Go de données vers l'extérieur

Installation involontaire d'un logiciel de minage de cryptomonnaies

Darktrace a détecté une erreur faite par un ingénieur DevOps débutant au sein d'une organisation internationale utilisant des workloads AWS et Azure, ainsi que des systèmes en conteneurs comme Docker et Kubernetes. L'ingénieur a accidentellement téléchargé une mise à jour qui contenait un mineur de cryptomonnaies, ce qui a entraîné une contamination de plusieurs systèmes de cloud.

Après l'infection initiale, le logiciel malveillant s'est mis à communiquer avec un serveur de commande et contrôle externe, ce qui a immédiatement été détecté par Darktrace. Une fois la connexion établie et les instructions d'attaques transmises, l'infection par le logiciel de minage de cryptomonnaies a pu se diffuser rapidement sur l'ensemble de l'infrastructure cloud de l'organisation à la vitesse de la machine, infectant 20 serveurs de cloud en moins de 15 secondes.

Grâce à l'IA de Darktrace et à sa vision dynamique et unifiée de l'infrastructure hybride et multi-cloud, l'environnement de cloud de l'organisation ne se trouvait pas dans un angle mort : l'équipe de sécurité a ainsi pu contenir l'attaque en quelques minutes au lieu de plusieurs heures ou plusieurs jours. Même si l'attaque s'est diffusée à la vitesse de la machine, Darktrace l'a détectée suffisamment tôt pour limiter les coûts causés par l'attaque.

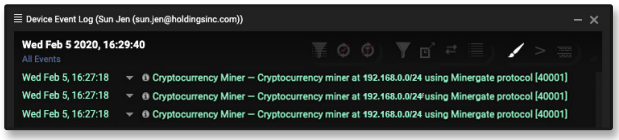


Figure 18: Détection en temps réel du logiciel de minage de cryptomonnaies

Exposition de propriété intellectuelle dans Azure

Un grand site de production en Europe utilisait un serveur Microsoft Azure pour stocker des fichiers contenant des informations sur ses produits et ses projections de ventes. Les fichiers du serveur et l'IP racine étaient protégés par un nom d'utilisateur et un mot de passe, mais les données sensibles avaient été laissées non cryptées. Une activité inhabituelle a été détectée lorsqu'un appareil a téléchargé un fichier ZIP à partir d'une adresse IP externe rare que Darktrace jugeait hautement anormale.

Il s'est avéré par la suite que l'adresse IP externe était un serveur Microsoft Azure qui venait d'être créé et que ce fichier zip était accessible à toute personne connaissant l'URL, celui-ci qui pouvant être simplement obtenu en interceptant le trafic réseau depuis l'intérieur ou l'extérieur du réseau. Des assaillants plus déterminés auraient même pu accéder par force brute au paramètre de fichier « clé » de l'URL.

La perte ou la fuite des données sensibles concernées auraient mis en danger la totalité de la ligne de production. Heureusement, en signalant l'incident dès sa détection, Darktrace a évité la perte de propriété intellectuelle précieuse et aidé l'équipe de sécurité à redéfinir ses pratiques en matière de stockage de données dans le cloud afin de mieux protéger les informations produit.

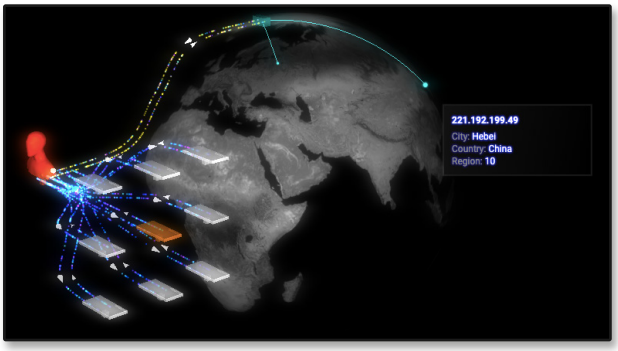
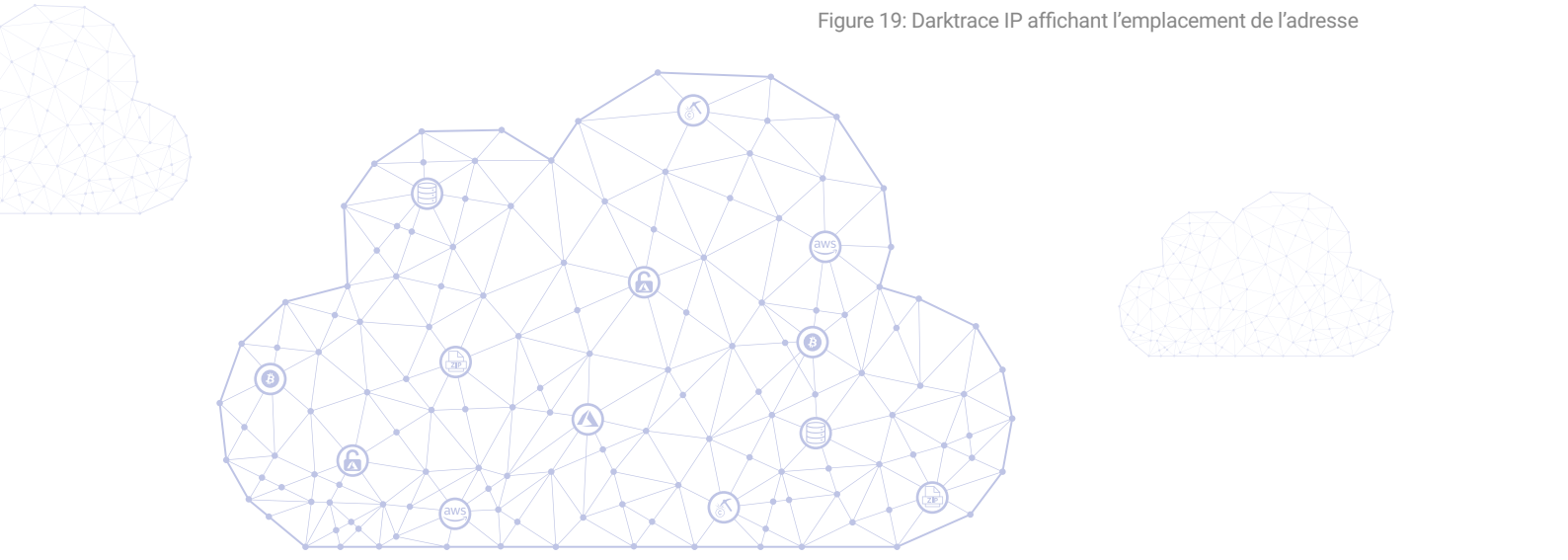


Figure 19: Darktrace IP affichant l'emplacement de l'adresse



L'ingénieur DevOps trop zélé

Au sein d'un groupe d'assurance, un ingénieur DevOps a voulu construire une infrastructure de sauvegarde parallèle dans AWS afin de répliquer les systèmes de production du centre de données de l'entreprise. L'implémentation technique était parfaite et les systèmes de sauvegarde ont été créés. Toutefois, le coût d'exécution du système aurait été de plusieurs millions de dollars par an.

L'ingénieur DevOps n'avait pas connaissance des coûts associés au projet et l'équipe de direction ignorait également le problème. L'infrastructure cloud a été lancée et les coûts ont commencé à s'accumuler. L'IA de Darktrace a signalé ce comportement inhabituel et l'équipe de sécurité a pu appliquer des mesures préventives immédiatement.

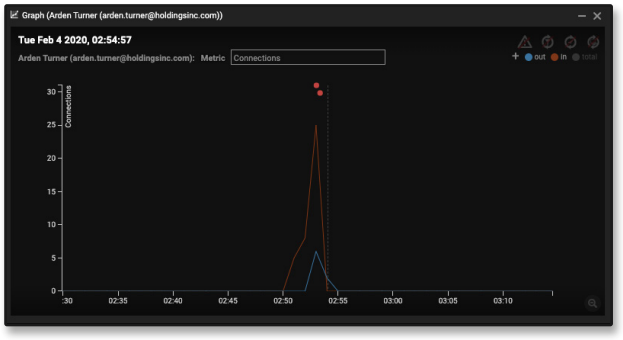


Figure 20: Threat Visualizer affichant un pic du nombre de connexions internes et externes

Scénarios de déploiement

Cloud hybride (IaaS)

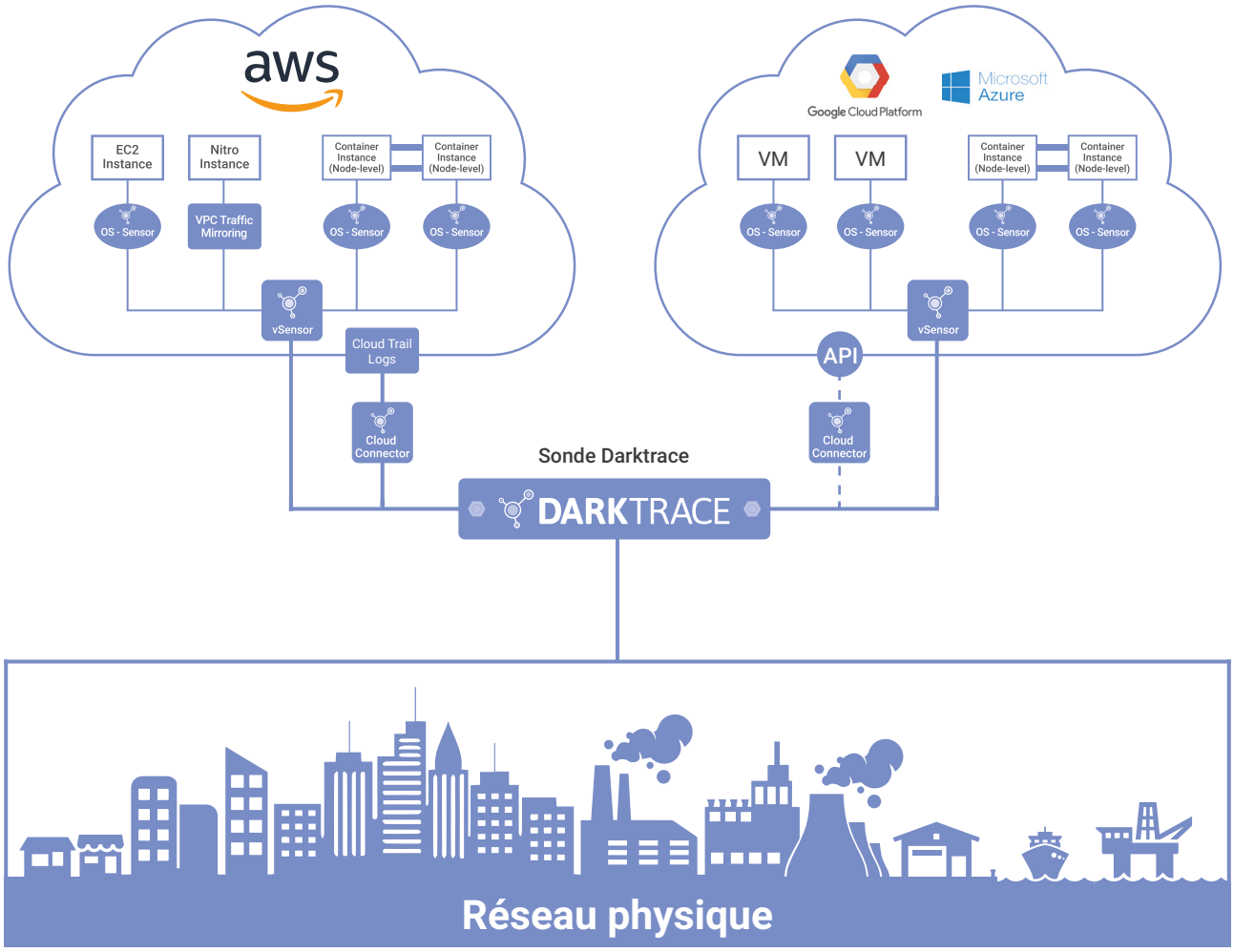
Pour les organisations dotées d'une infrastructure de cloud hybride, Darktrace déploie des sondes virtuelles ou « vSensors » qui capturent le trafic cloud en temps réel et le corrèlent au reste de l'entreprise.

Dans AWS, les vSensors intègrent le trafic en temps réel provenant d'instances Nitro via la mise en miroir du trafic VPC. Les métadonnées d'AWS Nitro peuvent être capturées directement, sans avoir à ajouter de sonde supplémentaire au niveau du serveur. Pour les instances autres que Nitro, Darktrace déploie des « OS-Sensors » à chaque point de terminaison. Chaque OS-Sensor transmet le trafic à un vSensor local qui, à son tour, transmet les métadonnées pertinente à une sonde maîtresse Darktrace dans le cloud ou sur le réseau de l'entreprise afin de les analyser.

Dans Azure, GCP et d'autres systèmes, Darktrace déploie des capteurs vSensors et OS-Sensors afin de capturer le trafic en temps réel selon la méthode décrite ci-dessus. Darktrace prend également en charge les vTAP d'Azure. Une fonctionnalité équivalente pour GCP est en cours de développement.

Les clients AWS et Azure peuvent également déployer des « Darktrace Connectors » afin de superviser l'activité des administrateurs système au niveau de l'API, comme l'activité de connexion ou la création de ressources.

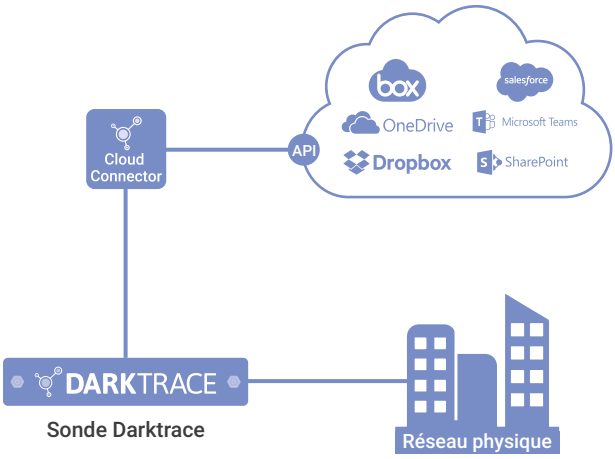
Enfin, Darktrace capture le trafic des conteneurs Docker et Kubernetes à l'aide d'un OS-Sensor spécialisé, qui transmet également les données vers un vSensor local, puis vers une sonde maîtresse Darktrace pour analyse.



Cloud hybride (SaaS)

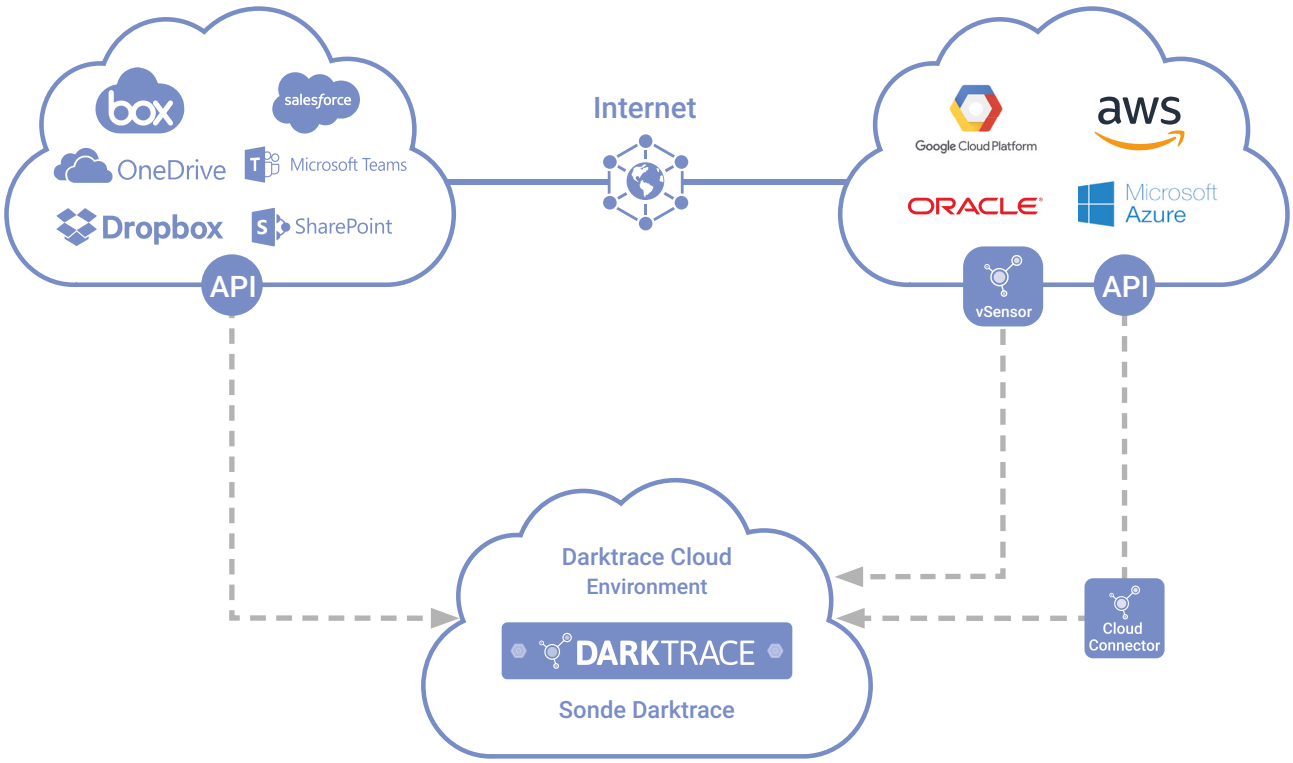
Pour les déploiements hybrides de SaaS, des Darktrace Connectors sont installés à distance sur la sonde maîtresse Darktrace (sur réseau physique ou dans le cloud) afin d'interroger les API de sécurité des solutions SaaS concernées. Ces solutions incluent Office 365, Salesforce, Dropbox, Box, Egnyte et bien d'autres.

Une fois les Connectors déployés, Darktrace analyse et corrèle en continu les données SaaS avec le trafic du reste de l'entreprise au sein d'une vue unifiée.



Cloud uniquement (IaaS et/ou SaaS)

Si un client utilise le cloud mais ne possède pas de réseau on premise, Darktrace peut fournir un déploiement sur cloud uniquement en tant que service dédié. Pour les déploiements sur cloud uniquement, Darktrace gère une sonde maîtresse dans le cloud qui reçoit le trafic de capteurs et de connecteurs installés dans les environnements IaaS et/ou SaaS du client.



Conclusion

À l'heure où les organisations dépendent de plus en plus des services cloud et des applications SaaS pour rationaliser leurs pratiques professionelles, le paradigme traditionnel du périmètre réseau s'est évaporé pour laisser place à des actifs numériques poreux et en constante mutation.

Les avantages du cloud computing permettent d'assurer les migrations, mais les problèmes de sécurité présentés par le cloud requièrent des technologies auto-apprenantes, capables d'intervenir à la vitesse des déploiements en s'adaptant à la topologie du cloud. De plus, l'expansion des environnements hybrides et multi-cloud requiert une plateforme de sécurité unique capable de corréler l'activité sur l'ensemble de ces systèmes disparates en temps réel.

Darktrace occupe une position de leader mondial dans le domaine de l'intelligence artificielle pour la cybersécurité ; il s'agit de la solution la plus efficace et la plus réputée pour détecter les menaces inédites et les incidents anormaux dans le cloud. Plutôt que de s'appuyer sur des règles et des stratégies prédéfinies, la technologie tient compte de l'incertitude inhérente à l'environnement numérique complexe d'aujourd'hui.

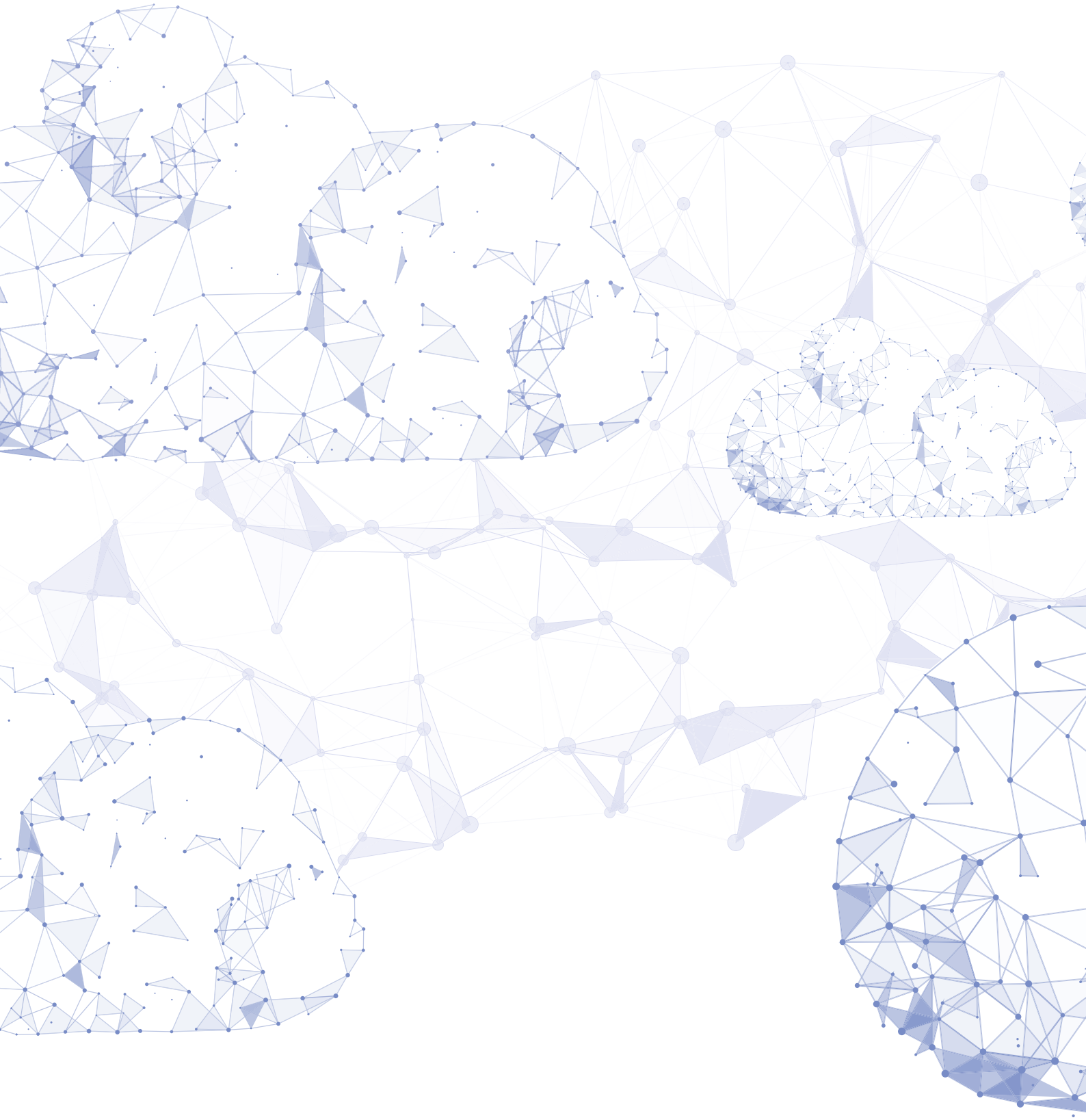
Qu'il s'agisse de réagir à une menace interne, à un pirate ciblant des données dans des conteneurs de test, ou à une erreur de configuration susceptible d'être exploitée ultérieurement, la plateforme de cyber IA de Darktrace élimine les angles morts et protège vos données, partout où elles se trouvent.

Enseignements clés

- Apprend l'identité afin de détecter les menaces basées dans le cloud qui échappent aux autres outils
- Corrèle l'activité des environnements hybrides et multi-cloud
- Offre une visibilité totale et en temps réel qui ne laisse aux attaquants nulle part où se cacher
- Analyse automatiquement les incidents de sécurité avec le Cyber AI Analyst

> Darktrace est une révolution en matière d'IA pour la cyberdéfense. Notre équipe dispose désormais d'une couverture complète et en temps réel de nos applications SaaS et de nos conteneurs cloud.

– DSI, Ville de Las Vegas



À propos de Darktrace

Darktrace est leader mondial de l'IA pour la cyberdéfense et le créateur de la technologie de Réponse Autonome. Notre IA auto-apprenante reproduit le système immunitaire humain et combine machine learning supervisé et non supervisé afin de détecter et neutraliser les cybermenaces. La technologie protège l'ensemble des environnements numériques, incluant le cloud, les emails, l'IoT, ou encore les réseaux bureautiques et industriels.

Darktrace compte plus de 3 500 clients, 1 200 employés et 44 bureaux dans le monde, ainsi qu'un double siège social à San Francisco et Cambridge, Royaume-Uni. Toutes les 3 secondes, l'IA de Darktrace riposte contre une cybermenace, l'empêchant de provoquer des dégâts.

Nous contacter

Paris: +33 1 40 73 84 85

Amérique du Nord: +1 (415) 229 9100

Asie-Pacifique: +65 6804 5010

Amérique latine: +55 11 97242 2011

info@darktrace.com | darktrace.com

@darktrace