Rapport sur les menaces dans le cloud 2019

Études de cas

Synthèse

Ce rapport recense 11 scénarios d'attaques dans le cloud identifiées par notre cyber IA, y compris des attaques par hameçonnage ciblé, des menaces internes et un logiciel malveillant « zero day » Ces études de cas montrent que les indicateurs faibles d'activités malveillantes ont uniquement pu être détectés grâce à l'IA Darktrace, solution native de cloud capable de détecter et de neutraliser les cybermenaces sophistiquées dans les environnements hybrides et multi-cloud.

Introduction

Des petites entreprises cherchant à réduire leurs coûts 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 habitudes chez les entreprise du numérique, de plus en plus diversifiées. Les organisations sont aujourd'hui capables de repousser les limites de l'innovation, mais elles étendent d'autant 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.

Ce patchwork complexe de plateformes cloud offre généralement des avantages en termes d'efficacité, de flexibilité et d'innovation, mais il 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 hérités ne s'appliquent pas aux environnements hybrides ou multi-cloud, ou 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 encouragent toujours une approche de la sécurité 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 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 (qui s'accompagne d'une mentalité nouvelle et peu habituelle mais requise pour s'adapter à l'agilité et à la vitesse du cloud) en fait 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. La sécurité du cloud n'est pas 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 solution 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 où elle établit sa présence sur un réseau.

L'IA Darktrace : Un cyber système immunitaire pour le cloud et bien plus

Basé sur l'intelligence artificielle, l'Enterprise Immune System de Darktrace comble ces vides critiques en proposant une approche unique, auto-apprenante et capable de détecter et de neutraliser les attaques dans le cloud qui échappent aux autres outils.

La solution fonctionne en apprenant le « modèle comportemental normal » de chaque utilisateur, périphérique et conteneur dans les environnements hybrides et multi-cloud, sans définir à l'avance ce qui constitue un élément « bénin » ou « malveillant ». 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 faibles et subtils indiquant une attaque sophistiquée au moment où elle émerge à différents points du réseau.

Les solutions ponctuelles préprogrammées sont indéniablement utiles pour compléter cette approche, mais l'IA native du cloud de 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'origines sont multiples: campagnes d'hameçonnage ciblé, piratage de compte professionnel, exfiltration de données lente et discrète, ou encore mouvement latéral sur le cloud.

En déployant la cyber IA de Darktrace, les organisations peuvent exploiter pleinement les avantages du cloud en ayant l'assurance que leur sécurité est résiliente et que leurs données critiques sont bien protégées.

> Darktrace représente une nouvelle référence en matière d'IA pour la cyberdéfense. Notre équipe dispose désormais d'une couverture complète et en temps réel de nos applications SaaS, de nos conteneurs cloud, ainsi que de nos capteurs répartis dans toute la ville.
>
> **Ville de Las Vegas**

Une vue unifiée pour les environnements hybrides et multi-cloud

Grâce à son interface intuitive Threat Visualizer, Darktrace offre une visibilité complète de toute votre infrastructure numérique, même variée : elle recouvre les environnements cloud comme AWS et Azure, ou encore les applications comme Salesforce et Office 365.

Menace interne dans le cloud

À la différence des attaques extérieures, les menaces internes bénéficient d'une position unique pour échapper aux mécanismes de contrôle traditionnels, étant donnés leur accès privilégié au réseau et leur connaissance intime de celui-ci. Que ces mécanismes s'appuient sur une détection logique binaire ou qu'ils se contentent de surveiller le périmètre, un employé mécontent peut facilement contourner les défenses statiques du cloud pour exfiltrer ou manipuler des données critiques sans attirer les soupçons.

Une organisation au Royaume-Uni a décidé de restructurer son service informatique et a licencié plusieurs employés. L'un des employés concernés, responsable informatique, a téléchargé les informations de contact et les numéros de carte de crédit depuis la base de données et les a transférées en secret vers un serveur domestique en utilisant un service de transfert de données autorisé par l'entreprise. Ce responsable informatique savait que ce service en particulier n'était pas régi par des politiques d'entreprise, mais également qu'il était situé dans le cloud. Il a supposé que l'équipe de sécurité n'aurait qu'une visibilité limitée sur ce secteur.

Même si cette activité subtile a échappé aux dispositifs de contrôle natifs du fournisseur de cloud, l'IA de Darktrace a 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 le 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.

Attaque par hameçonnage ciblé dans Office 365

Bien que de nombreuses attaques de phishing soient des campagnes furtives indifférenciées, l'IA de Darktrace a su détecter une grande variété d'attaques par e-mail portant les signes d'un cybercrime coordonné et sophistiqué. Dans un des cas, un attaquant a mis la main sur la liste des contacts d'une municipalité aux États-Unis. Il a alors transmis une attaque par hameçonnage ciblé extrêmement bien formulée aux employés, par ordre alphabétique. Les messages contenaient des contenus malveillants camouflés derrière un lien Netflix, Amazon et d'autres services de confiance.

L'IA de Darktrace a été capable d'analyser ces liens cachés en rapprochant l'ensemble du trafic Office 365 avec les « modèles comportementaux normaux » des destinataires visés sur le réseau. Lorsque le premier e-mail est arrivé, Darktrace a immédiatement reconnu que ni le destinataire, ni aucun membre du groupe de pairs, ni le reste du personnel de la ville n'avaient visité ce domaine auparavant. Darktrace a instantanément envoyé une alerte de criticité élevée et a suggéré de bloquer de façon autonome chaque lien qui entrait sur le réseau.

Curieusement, le fait que Darktrace Antigena (technologie de réponse autonome du système) ait été déployé en mode « passif » a fourni des preuves claires et tangibles de la capacité de Darktrace à contrecarrer les attaques subtiles qui échappent aux outils de contrôle natifs. Alors que Darktrace a détecté la campagne dès la lettre « A », les outils traditionnels utilisés par la municipalité n'ont perçu la menace qu'à partir de la lettre « R ». En mode « actif », Antigena aurait neutralisé l'attaque avant même qu'elle n'atteigne le premier utilisateur.

Erreur de configuration du cloud

La configuration des outils de contrôle de sécurité dans les environnements hybrides et multi-cloud est souvent complexe et rébarbative, car les solutions natives et tierces s'adressant à ce secteur sont souvent disparates, inhabituelles et incompatibles entre les différentes plateformes. Cette complexité, associée à la vitesse et à l'agilité inédites du cloud, provoque régulièrement des erreurs de configuration critiques qui exposent les entreprises aux cybercriminels.

Une institution financière hébergeait un grand nombre de serveurs critiques sur des équipements virtuels 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 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 l'erreur de configuration, le serveur exposé a fini par être découvert et ciblé par des cybercriminels parcourant Internet via Shodan. En quelques secondes, l'IA de Darktrace a reconnu 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.

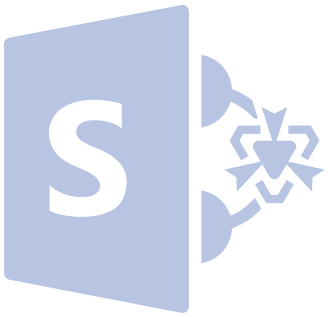
Usurpation d'identité dans un e-mail au sein d'Office 365

L'usurpation d'identité par e-mail implique d'enregistrer un domaine à l'apparence légitime qui ressemble à s'y méprendre à celui d'un contact ou d'un service de confiance, de manière à ce que l'assaillant puisse tromper un destinataire peu méfiant et infiltrer facilement un réseau. Le plus souvent, l'auteur de l'attaque cherche à prendre l'identité d'un dirigeant de haut niveau effectuant une requête urgente, dans l'espoir que l'employé obéira sans repérer la fausse adresse de l'expéditeur. Depuis des années, cette méthode permet aux pirates d'échapper aux outils de contrôle traditionnels, car un nouveau domaine trompe non seulement les destinataires, mais il évite également les solutions de sécurité qui s'appuient sur des listes noires.

Chez un distributeur d'électricité, l'IA de Darktrace a détecté une tentative convaincante d'usurpation d'identité sur un compte de messagerie Office 365. L'e-mail était censé provenir du PDG de l'entreprise, qui demandait à un collaborateur responsable de la paie de mettre à jour les informations de dépôt direct du PDG. Comme le domaine utilisé n'apparaissait pas sur les listes noires traditionnelles utilisées par les autres solutions, l'attaque aurait bien pu réussir si l'IA de Darktrace n'avait pas analysé le flux de messagerie Office 365 de l'entreprise en le corrélant au reste de l'activité.

En apprenant le « modèle comportemental normal » de l'employé, du PDG, et de l'organisation dans son ensemble, y compris au niveau du trafic cloud et réseau, Darktrace a pu détecter immédiatement plusieurs anomalies subtiles dans l'e-mail, dont la fausse adresse de l'expéditeur. Parmi les autres indicateurs faibles, l'IA de Darktrace a calculé automatiquement la proximité anormale du nom de domaine utilisé avec celui des employés internes et des contacts de confiance. L'IA a réagi immédiatement en verrouillant les liens de l'e-mail et en le signalant clairement comme dangereux avant qu'il n'atteigne le service de paie. La compréhension du trafic cloud et réseau a permis à Darktrace de neutraliser une menace de gravité élevée qui aurait échappé aux outils basés sur des signatures.

Attaque SharePoint



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

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 constante évolution par l'IA de ce qui constitue une situation normale dans toute l'organisation s'est avérée critique, étant donné que l'accès suspect au fichier aurait très bien pu être bénin dans d'autres circonstances.

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 se transforme en crise.

Piratage de compte dans la chaîne d'approvisionnement Office 365

En détournant les informations relatives au compte d'un fournisseur de confiance dans la chaîne logistique, les auteurs de menaces sophistiquées peuvent persuader par la ruse des destinataires de cliquer sur un lien malveillant ou de transférer des millions hors de l'entreprise. L'IA de Darktrace a repéré une attaque de ce type ciblant un studio de production de film à Los Angeles, après que les informations de connexion à Office 365 d'un contact chez un fournisseur de confiance avaient été compromises.

Les informations relatives à un compte peuvent être exploitées à de nombreuses fins malveillantes, mais dans ce cas, le criminel semble les avoir utilisées pour parcourir l'historique de correspondance du contact avec un employé du studio. Après avoir parcouru les conversations précédentes, il a envoyé une réponse crédible au dernier e-mail envoyé par cet employé, qui reflétait le style d'écriture du contact et était pertinent dans le contexte de la relation entre les deux personnes et leurs échanges précédents, mais en incluant un lien malveillant.

La cyber IA de Darktrace a su distinguer les indicateurs faibles qui ont révélé que ce « contact de confiance » était un compte contrôlé par un pirate. Elle a repéré que l'e-mail et son contenu sortaient du « modèle comportemental normal » de l'expéditeur supposé. L'employé a été alerté et la charge malveillante a été neutralisée.

La décision d'Antigena s'est fondée sur le fait que ce lien particulier était inhabituel pour l'expéditeur et le destinataire au vu de leurs communications précédentes. À la différence des solutions en silo, l'IA de Darktrace n'a pas traité le destinataire sur le réseau comme une simple adresse e-mail, mais elle a compris la portée globale du « modèle comportemental normal » de l'employé dans le contexte de ses interactions et du réseau tout entier.

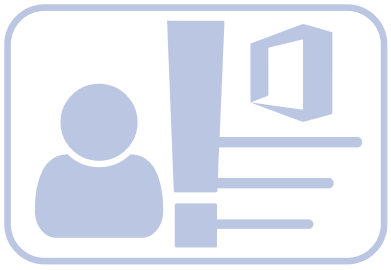
Informations à caractère personnel non chiffrées dans AWS

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 étaient 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, mais cette négligence les rendait disponible 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, qui 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 révélé cet angle mort dangereux et a permis à l'équipe de sécurité de corriger l'erreur de configuration.

Informations de connexion compromises dans Office 365



Les cybercriminels expérimentés peuvent subtiliser des informations de connexion de plusieurs façons. Cela peut-être via 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.

Dans une organisation internationale, Darktrace a détecté une faille au niveau d'un compte Office 365 qui contournait les contrôles natifs d'Azure Active Directory. Même si l'organisation possédait des bureaux partout dans le monde, l'IA de Darktrace a détecté une connexion provenant d'une adresse IP inhabituelle d'un point de vue historique pour cet 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'une signe indéniable de compromission, et l'équipe de sécurité a pu verrouiller le compte 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 capable de détecter les attaques de phishing en comparant les liens contenus dans les e-mails à des adresses malveillantes déjà connues, et ce lien de phishing ne figurait pas sur leur liste. Cet événement a montré les limites d'une approche basée sur des signatures dans ce secteur, et l'organisation a rapidement déployé Antigena. Ils bénéficient ainsi d'une protection supplémentaire dans Office 365 grâce à sa capacité à détecter les e-mails de phishing sans se baser sur des listes noires.

Propriété intellectuelle non chiffrée 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 sur 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 sans protection. 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 ce fichier zip était accessible à toute personne en connaissant l'URL, qui pouvait être simplement obtenue 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.

Attaque « zero day » dans Office 365

Les outils de sécurité traditionnels qui recherchent les signes prédéfinis d'une attaque sont toujours impuissants face aux nouvelles variations de menaces et passent souvent à côté des nouveaux logiciels malveillants. Seul Darktrace, avec sa compréhension riche et en constante évolution de ce qui constitue une situation normale sur l'ensemble du trafic cloud et réseau, est capable d'aider les organisations à détecter les chevaux de Troie « zero day » ou créés sur-mesure dès leurs premières manifestations.

Aux États-Unis, dans une maison d'édition, Darktrace a détecté une usurpation d'identité dans un e-mail envoyé au compte Office 365 d'un employé. Cet e-mail était censé provenir d'un collègue de confiance demandant une facture, mais il contenait un lien de téléchargement malveillant camouflé. Ce lien inédit a facilement évité les contrôles natifs de Microsoft, et n'est même pas apparu sur VirusTotal avant le lendemain.

Pourtant, l'IA de Darktrace a détecté plusieurs indicateurs faibles d'une activité inhabituelle, y compris la rareté du domaine et l'absence de toute communication antérieure entre les deux utilisateurs. Darktrace a signalé l'e-mail comme étant hautement suspect, ce qui a permis à l'équipe de sécurité de neutraliser la menace et d'éviter des dégâts importants.

L'ingénieur DevOps trop zélé dans AWS

L'agilité et la visibilité limitée des activités anormales dans le cloud augmentent considérablement les risques de sécurité, mais des dégâts importants peuvent également être causés par un administrateur bien intentionné.

Dans l'un de ces cas, 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.

À propos de Darktrace

Darktrace est leader mondial de l'IA pour la cyberdéfense et le créateur de la technologie de Réponse Autonome. Son IA auto-apprenante reproduit le système immunitaire humain et est utilisée par plus de 3000 organisations afin de se protéger contre les menaces qui pèsent sur les emails, le cloud, l'IoT, ou encore les réseaux bureautiques et industriels.

Darktrace compte plus de 1000 employés et son double siège social est présent 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

Amérique du Nord : +1 (415) 229 9100
Europe : +44 (0) 1223 394 100
Asie-Pacifique : +65 6804 5010
Amérique latine : +55 11 97242 2011
info@darktrace.com | darktrace.fr
@darktrace