DARKTRACE

Réponse Cyber IA : Rapport sur les menaces 2019

Introduction

À l'ère du numérique, les chefs d'entreprise font face à des facteurs de risques extrêmement urgents dans un contexte de cybermenaces automatisées et à évolution rapide. Ces risques se sont considérablement renforcés ces dernières années en raison de l'évolution et de la sophistication des menaces, mais également de la complexité, de la diversité et du développement de nos entreprises digitales.

Auparavant, lorsque les auteurs des menaces étaient moins expérimentés et que les réseaux étaient plus prévisibles, une approche traditionnelle de la sécurité était souvent suffisante pour tenir à distance les cybermenaces. En configurant les outils de sécurité avec une combinaison de règles ou de signatures, les équipes de sécurité ont cherché à détecter les menaces en leur attribuant à l'avance une définition « bénigne » ou « malveillante », en s'appuyant sur des représentations d'attaques qui ont été conçues sous la forme d'une règle ou qui ont été observées « à l'état sauvage », puis analysées par rétro-ingénierie en vue d'une détection future.

Et pourtant, la fréquence croissante de nouvelles attaques externes et de menaces internes, ainsi que la complexité et la subtilité des comportements quotidiens dans une entreprise, ont progressivement désarmé les équipes de sécurité qui s'appuient toujours sur des contrôles traditionnels. Les défenses traditionnelles ne sont pas en mesure de détecter les nouvelles tactiques et techniques des cybercriminels créatifs qui sont maintenant capables de se fondre dans le réseau et de ravager des infrastructures vastes et complexes en quelques secondes.

Sachant que les nouvelles menaces pénétreront inévitablement dans l'entreprise, le secteur s'est interrogé sur la façon d'équiper les cyberdéfenseurs pour leur permettre de détecter et de réagir aux menaces émergentes qui sont déjà dans l'entreprise, mais qui peuvent être traitées avant de provoquer une crise. Les chefs d'entreprise et les équipes de sécurité se sont tournés vers l'intelligence artificielle pour faire face à la menace.

L'application IA de Darktrace est unique et apprend le « modèle comportemental normal » de chaque entreprise afin de détecter de petits écarts, indicateurs d'une menace, connue ou inconnue, externe ou interne, subtile ou à évolution rapide. En apprenant continuellement et en s'adaptant en permanence en fonction des nouvelles informations reçues, l'intelligence artificielle de Darktrace détecte les indicateurs précoces de cybermenace qui autrement seraient passés inaperçus, sans s'appuyer sur les règles, les signatures ou les hypothèses antérieures.

Synthèse

Ce rapport passe en revue sept études de cas d'attaques qui ont été interceptées et neutralisées par l'IA de cyberdéfense, y compris des menaces internes, des ransomware et des attaques IoT.

Alors que tous les scénarios de menaces étaient différents (certains à évolution rapide, d'autres lents et furtifs), dans tous les cas, les indicateurs subtils de l'activité suspecte ont pu être détectés uniquement à l'aide de l'IA de Darktrace qui apprend ce qui est normal pour l'environnement de l'entreprise et réagit de manière autonome aux attaques avant que des dommages soient causés.

Réagissez avec Darktrace Antigena

Au regard de l'écart de compétences qui se creuse et de l'augmentation du volume et de la vitesse des attaques, l'IA est non seulement essentielle pour détecter les menaces émergentes, mais est également fiable pour renforcer la première ligne de défense d'une entreprise. L'IA a le pouvoir de réagir en temps réel, laissant le temps à l'équipe de sécurité d'intervenir.

Avec sa compréhension riche et évolutive du « modèle comportemental normal » pour chaque utilisateur, appareil et groupe d'homologues lié au sein d'une entreprise, l'IA de Darktrace est non seulement capable de réagir aux indicateurs précoces de cybermenace avant que des dommages soient causés, mais peut également agir de manière extrêmement ciblée. Au lieu de générer des quarantaines générales qui ne causeraient que davantage de perturbation, Darktrace Antigena – la solution de réponse de cyber IA du système – fonctionne en appliquant chirurgicalement le « modèle comportemental normal » sur un appareil infecté ou un employé mécontent, neutralisant la menace en quelques secondes et maintenant délibérément les opérations normales.

Dans la lutte contre les cybercriminels avancés, la Cyber IA de Darktrace redonne le contrôle aux défenseurs, transformant l'organisation la plus complexe et la plus vulnérable en une entreprise digitale résiliente qui assure sa propre défense.

Menace interne

Un employé balaye le réseau à la recherche de vulnérabilités

Malveillante et persistante

La menace interne est l'un des vecteurs d'attaque les plus dangereux et les plus courants dans l'entreprise, qu'elle soit malveillante ou non. Les employés malveillants représentent une menace particulièrement importante pour l'entreprise, car leur accès privilégié et leurs connaissances du réseau leur permettent de mener des missions d'attaque d'envergure et d'exfiltrer ou de manipuler silencieusement des données critiques sans éveiller les soupçons.

L'IA de Darktrace a identifié et neutralisé ce type d'employé malveillant dans une grande société d'investissement en Afrique du Sud. L'IA auto-apprenante a pu contenir une menace persistante alors qu'elle franchissait les multiples étapes de la chaîne d'attaque, de la reconnaissance jusqu'à l'écriture et à l'exécution de scripts. En apprenant continuellement, Antigena s'est adapté à la menace au fur et à mesure de son évolution et l'a contenue efficacement à chaque étape.

Comportement suspect

L'étape de reconnaissance a commencé lorsqu'un ordinateur portable a envoyé des « ping » vers des centaines d'adresses IP internes pour identifier celles qui étaient actives. Il a ensuite balayé le réseau à la recherche des noms des machines réactives et les a scannées pour rechercher les canaux de communication ouverts. L'IA de Darktrace a signalé le comportement suspect comme étant une activité scannant le réseau de façon inhabituelle et a instantanément déclenché une réaction d'Antigena. En s'appuyant sur son évaluation dynamique de la menace, Antigena a décidé d'appliquer le « modèle comportemental normal » du groupe de pairs de l'appareil pendant une heure, empêchant l'ordinateur portable de dévier de son comportement précédent ou de celui de ses homologues.

Pourtant, quelques heures plus tard, la menace est revenue. L'ordinateur portable a commencé à exécuter des commandes sur des centaines d'autres ordinateurs internes dans la plage d'IP qu'il avait identifiée initialement. Ces commandes incluaient le déplacement de fichiers de script polyvalents et l'utilisation d'un outil d'administration à distance. Ces programmes pouvaient être exploités pour localiser des informations et des documents sensibles, ou pour ouvrir une porte dérobée et permettre à un pirate externe de détourner des informations.

> Antigena a décidé d'appliquer le « modèle comportemental normal » du groupe de pairs de l'appareil pendant une heure

Antigena intervient

Aucune écriture de fichier similaire n'a été observée sur le réseau pendant cette période, ce qui a semblé particulièrement inhabituel à l'IA de Darktrace. Compte tenu de sa compréhension de l'évolution de la menace dans le contexte du réseau et de sa réponse autonome précédente, Antigena a décidé de bloquer toutes les connexions sortantes utilisant le canal de transfert de fichier SMB, contenant instantanément tout mouvement latéral à travers le réseau.

Une fois la menace neutralisée, l'équipe de sécurité a pu enquêter et confirmer que l'ordinateur portable appartenait à un membre de l'équipe informatique qui avait utilisé un outil de balayage illicite pour rechercher des faiblesses dans le réseau. C'est un exemple particulièrement révélateur du pouvoir de l'IA de Darktrace et de la façon dont Antigena peut intervenir à différentes phases d'une chaîne d'attaque et neutraliser les menaces persistantes à un stade précoce.

Cheval de troie « zero day »

Connexions et téléchargement suspects

Nouvelle souche de logiciel malveillant

Bien que les outils de sécurité traditionnels soient souvent capables d'identifier les menaces connues ayant déjà été détectées, l'IA possède la capacité unique de repérer les signaux faibles et subtils d'une cybermenace jamais vue auparavant. Cette capacité est devenue indispensable ces dernières années, car les cybercriminels avancés développent sans cesse de nouvelles tactiques, techniques et procédures, conçues spécialement pour échapper aux contrôles préprogrammés avec des signatures des attaques précédentes.

La capacité de Darktrace à réagir à ces indicateurs subtils a été vitale pour un fabricant américain de contrôles d'IoT industriel, lorsqu'il a été attaqué par un cheval de Troie « zero day ».

Un jeudi à 1h30 du matin, l'IA a averti le Directeur informatique de l'entreprise d'un téléchargement suspect d'un fichier nommé « OfficeActive.bin ». Malgré la ressemblance du fichier avec un produit Microsoft, Darktrace a indiqué qu'il avait été téléchargé à partir d'une source non identifiée qui était à 100 % rare pour le réseau.

> Malgré la ressemblance du fichier avec un produit Microsoft, Darktrace a indiqué qu'il avait été téléchargé à partir d'une source non identifiée

Faire confiance à la réponse de l'IA

À l'époque, Antigena était configuré en mode « Passif » : un mode débutant qui limite l'IA à communiquer ce qu'elle aurait fait en réponse à la menace, sans agir réellement, ce qui permet à l'équipe de prendre confiance dans les décisions du système. L'équipe informatique a pu observer la façon dont Antigena aurait bloqué l'attaque à un stade précoce et dont il s'est adapté à une nouvelle menace au fur et à mesure de son évolution.

Face au modèle d'activité hautement inhabituel, Antigena avait d'abord recommandé d'appliquer le « modèle comportemental normal » du groupe de pairs de l'appareil pendant deux heures, ce qui aurait bloqué la menace sur son parcours tout en maintenant les opérations normales.

Alors qu'il observait des téléchargements plus suspects, Antigena a renforcé sa réponse, en appliquant le « modèle comportemental normal » individuel de l'appareil pendant cinq minutes. Finalement, lorsque l'appareil a tenté d'établir une nouvelle connexion externe, Antigena a réagi de nouveau, en suggérant que l'IA bloque chirurgicalement toutes les connexions sortantes de l'appareil pendant une heure.

Supprimer la menace

Dans les minutes qui ont suivi l'identification de l'alerte, le Directeur informatique a contacté l'utilisateur final et a effectué une recomposition d'urgence afin de supprimer la menace sur la machine. Le processus complet a duré 20 minutes. Une fois la menace neutralisée, le Directeur informatique a copié l'URL et le nom du fichier du cheval de Troie dans Virus Total afin de vérifier si la menace avait été observée et enregistrée ailleurs. La recherche n'a donné aucun résultat, confirmant qu'il s'agissait d'un cheval de Troie « zero day » découvert de manière unique par l'IA de Darktrace.

Piratage IoT : Système de caméras en circuit fermé (CCTV)

Espionnage industriel ?

Faille au sein d'un système de caméras de sécurité

La connectivité croissante des appareils courants a introduit de nouvelles vulnérabilités dans l'entreprise. Les dispositifs IoT, souvent conçus avec des contrôles de sécurité de base non intégrés, sont systématiquement ciblés par les auteurs de menace et utilisés comme tremplin pour accéder au réseau.

Dans une société japonaise de conseil en investissement, Darktrace a découvert qu'un système de caméras en circuit fermé connecté à Internet avait été infiltré par des pirates inconnus. Les intrus avaient ainsi mis un pied dans le réseau et pouvaient consulter tous les enregistrements vidéo de la caméra. Installé pour surveiller l'ensemble des bureaux, de celui du PDG à la salle de réunion, le système de caméras était devenu lui-même un risque de sécurité.

> L'IA a réagi à la vitesse de la machine, empêchant une fuite grave d'informations

Une réaction rapide

L'IA de Darktrace a rapidement détecté que quelque chose n'allait pas. D'énormes volumes de données ont été observés se déplaçant en direction et à partir du serveur CCTV non chiffré, car le pirate rassemblait des données afin d'exfiltrer des informations sensibles.

Au moment où le pirate essayait d'exfiltrer les données, Antigena a pris une mesure défensive rapide et précise. Le système a décidé de bloquer chirurgicalement le mouvement de données du dispositif vers un serveur externe tout en autorisant le fonctionnement du système de caméras pour l'usage auquel il était destiné.

L'IA a réagi à la vitesse de la machine, empêchant une fuite grave d'informations commerciales sensibles. En prenant une mesure proportionnée pour contenir l'attaque à un stade précoce, Antigena a accordé à l'équipe de sécurité un temps précieux pour examiner et supprimer la menace avant qu'elle ne cause des dommages.

Piratage IoT : Casier intelligent

Des données client sensibles ciblées

Vulnérabilité de l'IoT

Dans un parc d'attractions en Amérique du Nord, un auteur de menace a tenté de voler des données client sensibles par l'intermédiaire d'un dispositif IoT vulnérable : un casier « intelligent » utilisé par les visiteurs pour entreposer leurs affaires personnelles.

Le réglage par défaut de l'appareil prévoyait un contact régulier entre le casier intelligent et la plateforme en ligne tiers du fournisseur. L'auteur de la menace a identifié la source de ce processus automatisé et l'a détournée pour compromettre l'appareil.

Faible et lente

L'IA de Darktrace a détecté l'attaque peu de temps après que le casier a commencé à envoyer une quantité inhabituelle de données non chiffrées à un site externe rare. Les connexions avaient lieu au moment des communications régulières de l'appareil avec la plateforme du fournisseur, suggérant qu'il s'agissait d'une attaque « faible et lente » conçue spécifiquement pour échapper aux outils de sécurité basés sur des règles.

En analysant en continu les communications en rapport avec le comportement précédent du casier et de celui de ses homologues, l'IA de Darktrace a déterminé qu'une cyberréponse de l'IA était nécessaire. En quelques secondes, Darktrace Antigena a réagi en bloquant intelligemment toutes les connexions sortantes de l'appareil compromis et en laissant le temps à l'équipe de sécurité de supprimer la menace et d'éviter une prochaine exfiltration.

Pour ce parc d'attractions et bien d'autres, la technologie de cyber IA de Darktrace a neutralisé d'innombrables attaques « faibles et lentes » à un stade précoce. En apprenant continuellement, le système détecte les menaces subtiles que les autres outils laissent passer. Il révise constamment sa compréhension en fonction des nouvelles informations reçues et génère des actions autonomes qui s'adaptent à la menace au moment où elle se déroule.

Ransomware

Rapide et implacable

Une escroquerie automatisée

À 7h05 un vendredi, un employé d'une grande entreprise de télécommunications a accédé à sa messagerie personnelle sur un téléphone de fonction et a téléchargé un fichier malveillant à son insu contenant un ransomware. Quelques secondes plus tard, son appareil s'est connecté à un serveur externe sur le réseau Tor.

L'IA de Darktrace a réagi en quelques instants. Neuf secondes après le début des activités de chiffrement SMB, Darktrace a lancé une alerte prioritaire signalant que l'anomalie devait être immédiatement examinée. Comme le comportement a persisté pendant les quelques secondes suivantes, Darktrace a révisé son jugement et a activé Antigena.

L'équipe de sécurité étant rentrée chez elle pour le week-end, Darktrace Antigena est intervenu de façon autonome en interrompant toutes les tentatives d'écriture de fichier chiffré sur les partages de fichiers du réseau. Cette action a neutralisé instantanément la menace avant qu'elle se propage à travers l'infrastructure tentaculaire des télécommunications, laissant le temps à l'équipe de sécurité d'intervenir.

Comme des souches automatisées de ransomware émergent continuellement sur le Dark Web et dans les réseaux d'entreprise à travers le monde, les organisations devront réagir avec l'IA pour faire face à la menace. Ici comme ailleurs, la réponse de cyber IA de Darktrace est devenue un élément essentiel de la lutte, en contenant des attaques rapides avant qu'elles n'aient le temps de chiffrer des données critiques et de paralyser l'entreprise.

Hameçonnage ciblé

Une attaque par e-mail ciblée

Attaque par e-mail

Une municipalité américaine a été la victime d'une attaque ciblée par messagerie. Bien que de nombreuses attaques de phishing soient des campagnes furtives indifférenciées, celle-ci portait l'empreinte d'un cybercrime coordonné et sophistiqué. Chaque e-mail était bien conçu et personnalisé à l'attention du destinataire. L'auteur de la menace avait également mis la main sur l'annuaire de la ville, car l'attaque était envoyée aux destinataires par ordre alphabétique, de A à Z.

Pourtant, alors que chaque e-mail semblait inoffensif et était personnalisé en fonction du destinataire, tous les messages contenaient une charge malveillante cachée derrière un bouton qui était diversement dissimulée sous la forme d'un lien vers Netflix, Amazon et d'autres services de confiance.

> Antigena a détecté la campagne à la lettre « A », les outils traditionnels ont pris conscience de la menace à la lettre « R »

Des liens cachés

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

Curieusement, le fait qu'Antigena était déployé en mode « Passif » a fourni des preuves claires et tangibles de la capacité du système à contrecarrer les attaques subtiles que les autres outils ne voient pas : alors qu'Antigena a détecté et cherché à neutraliser la campagne à la lettre « A », les outils traditionnels de l'équipe de sécurité ont pris conscience de la menace à la lettre « R ». En mode « Actif », Antigena aurait neutralisé l'attaque avant qu'elle n'atteigne un seul utilisateur.

Attaque d'une chaîne logistique

Un imposteur qui a exploité des relations de confiance

Détournement d'un compte e-mail

Certains des cybercriminels actuels les plus créatifs ont appris que le moyen le plus simple de pénétrer dans l'entreprise est souvent par la porte d'entrée, à condition de réussir à gagner la confiance d'un utilisateur légitime. En détournant les informations relatives au compte d'un collègue, d'un associé ou d'un fournisseur de confiance dans la chaîne logistique, les auteurs de menace 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 du compte d'un contact chez un fournisseur de confiance ont 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 passé en revue les fils précédents et appris comment le contact et l'employé communiquaient généralement, il a envoyé une réponse plausible au dernier e-mail de l'employé.

> L'e-mail était convaincant : il reflétait le style d'écriture et le ton du contact

Croyez-le ou non !

L'e-mail était convaincant : il reflétait le style d'écriture et le ton du contact, et paraissait logique au regard de la relation et des discussions précédentes. Il comprenait également un lien malveillant qui aurait pu sembler inoffensif à tout employé sensé recevant un lien d'un contact familier d'une entreprise familière. Ces types d'attaques sont de plus en plus courants et très difficiles à détecter.

La technologie de Cyber IA de Darktrace a su distinguer les faibles indicateurs qui ont révélé que ce « contact de confiance » était un compte détourné contrôlé par un pirate. La réponse de l'IA a signalé au réseau 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.

Ce qui est important, c'est que la décision d'Antigena a été fondée sur le fait que ce lien particulier aurait été rare pour l'expéditeur et le destinataire au vu de leurs communications précédentes et des « modèles comportementaux normaux » de l'employé sur le réseau. L'équipe de sécurité s'est sentie rassurée dans sa posture de sécurité en sachant que l'IA de Darktrace n'avait pas traité le destinataire sur le réseau comme une simple adresse e-mail. Antigena reconnaît que toute l'étendue d'un « modèle comportemental normal » d'un employé se manifeste souvent en différents points du réseau, et d'une façon qui peut être mise en corrélation et analysée favorablement par la cyber IA.

Contact

France : +33 1 40 73 84 85
Canada : +1 416 572 2099
Europe : +44 (0) 1223 394100
Amérique latine : +55 11 97242 2011
info@darktrace.com | darktrace.fr
@darktrace