Ransomware

Principaux avantages

- La Cyber IA auto-apprenante neutralise un ransomware émergent, sans s'appuyer sur des règles ou sur les signatures de menace
- L'Enterprise Immune System identifie même les souches de ransomware nouvelles et extrêmement ciblées
- Antigena répond de façon autonome en temps réel – peu importe où, quand et comment l'attaque est lancée
- Le Cyber AI Analyst analyse automatiquement les incidents de type ransomware, en rassemblant les informations clés dont vous avez besoin pour commencer à réagir

Figure 1 : La Cyber IA identifie une attaque de type ransomware

$381 millions de dollars de pertes causées par les ransomwares l'année dernière pour seulement 350 entreprises

Source: Hiscox, 2020

Avec l'évolution rapide de l'essence même des équipes et des innovations techniques, les attaques de type ransomware sont de plus en plus sophistiquées et répandues.

De nouvelles souches de ransomware émergent pour exploiter les malwares sans fichier et les tactiques d'exfiltration de données tandis que les attaquants opportunistes prennent avantage de tout changement pour lancer des campagnes plus efficaces. Les outils de sécurité conventionnels détectent uniquement les cybermenaces connues en utilisant des règles et des signatures. Ils ne décèlent pas les souches évolutives de ransomware pour lesquelles de telles signatures n'existent pas.

Les équipes de sécurité ne peuvent pas faire face à ces menaces en utilisant uniquement des contrôles traditionnels, notamment lorsqu'elles sont en sous-effectifs ou absentes du bureau. Les entreprises doivent plutôt se tourner vers les technologies de sécurité capables d'arrêter les ransomwares dès qu'ils émergent avant qu'ils ne causent des dégâts.

Plateforme de Cyber IA Darktrace : Identifier et répondre aux ransomwares émergents

La plateforme de Cyber IA Darktrace est capable de neutraliser un ransomware sophistiqué en temps réel, sans s'appuyer sur des renseignements sur les menaces ou des signatures connues. Basé sur le machine learning (apprentissage automatique) non supervisé et sur des techniques d'apprentissage approfondies, la Cyber IA apprend les « modèles comportementaux » normaux pour chaque utilisateur et technologie au sein de l'entreprise afin d'identifier les écarts subtils qui indiquent une menace émergente.

L'Enterprise Immune System utilise les connaissances évolutives de la Cyber IA sur ce qui constitue « l'identité » de votre entreprise pour mettre en évidence toutes les cybermenaces, y compris un ransomware jamais vu auparavant qui échappe à toutes les autres stratégies de défense. Élément clé de l'approche du « système immunitaire », le Cyber AI Analyst analyse automatiquement chaque menace pour vous aider à identifier facilement chaque appareil touché et à communiquer l'étendue de l'incident de type ransomware.

Lors du signalement d'une attaque sérieuse, Darktrace Antigena, la technologie Autonomous Response de la plateforme, maîtrise l'activité malveillante en quelques secondes, en neutralisant de manière chirurgicale les attaques tout en permettant à l'entreprise de poursuivre ses activités normales. La technologie s'adapte de manière intelligente aux menaces à mesure qu'elles se déploient et offre une couverture 24h/24, 7j/7 de tous vos collaborateurs, lorsque les équipes de sécurité sont débordées ou simplement absentes.

Antigena Network : Neutraliser les attaques à la vitesse de la machine

Lorsque le ransomware émerge, Antigena Network est la seule solution capable d'interrompre les attaques à la vitesse de la machine avec une précision extrême, même si la menace est extrêmement ciblée ou totalement inconnue. Elle répond de façon autonome par des actions intelligentes proportionnées, par exemple en interrompant une connexion, en appliquant un « modèle comportemental » normal pour un appareil spécifique. Lorsque votre équipe de sécurité est débordée ou absente, Antigena Network garantit votre tranquillité d'esprit en sachant que votre entreprise est entièrement protégée 24h/24, 7 j/7.

Darktrace est le créateur de la technologie Antigena Autonomous Response qui utilise la Cyber IA et ses connaissances évolutives de l'entreprise pour s'adapter aux menaces en temps réel et mettre en œuvre l'action la plus appropriée en fonction de votre contexte spécifique. Au lieu d'appliquer une mesure binaire (par exemple, mettre entièrement en quarantaine l'appareil) comme le feraient les outils traditionnels, Antigena agit de manière chirurgicale pour arrêter l'attaque, en veillant à ce que les activités normales de l'entreprise se poursuivent. La technologie peut également s'intégrer à vos investissements de sécurité existants afin d'améliorer l'ensemble de votre dispositif de sécurité, en fournissant des informations augmentées par l'IA et des moyens d'action aux pare-feu, aux systèmes SIEM (gestion des informations et des événements de sécurité) et autres outils.

Interruption du ransomware Ryuk pendant la période d'essai de Darktrace

Lorsque le ransomware Ryuk a frappé une entreprise qui utilisait la version d'essai de Darktrace, l'Enterprise Immune System l'a immédiatement détecté et a indiqué comment Antigena Network aurait pu le bloquer complètement.

Tout d'abord, la Cyber IA a noté une activité administrateur très inhabituelle qui n'a pas été observée sur le réseau auparavant. Après l'incident, l'entreprise a suivi l'attaque initiale dans une partie de son réseau sur laquelle Darktrace n'avait pas de visibilité pendant cette période d'essai.

La Cyber IA a observé le téléchargement du tristement célèbre cheval de Troie bancaire TrickBot après quoi des commandes et un contrôle du trafic ont été observés. Alors que de nombreux appareils ont présenté un comportement anormal, la Cyber IA a identifié un appareil à la source.

Lorsque le ransomware Ryuk a enfin été déployé, plus de 200 000 fichiers ont été chiffrés en seulement 12 heures. Pendant cette période « instable » avec de nombreuses activités SMB suspectes, la Cyber IA a indiqué encore plus clairement l'étendue de l'attaque.

Même si l'équipe n'a pas déclenché d'alertes Darktrace avant le chiffrement, cette attaque de type ransomware aurait pu être bloquée dès lors que l'Enterprise Immune System aurait détecté le premier signe de danger.

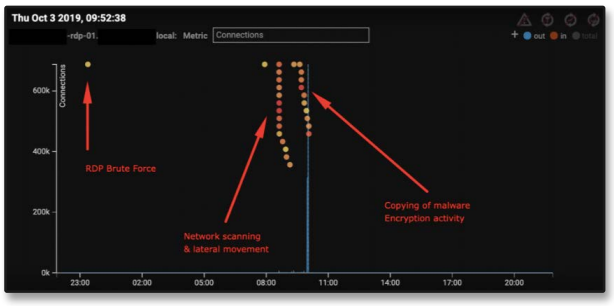

Figure 2 : Le graphique de l'interface utilisateur montre un exemple d'attaque de type ransomware : chaque point représente une alerte de Darktrace.

Autonomous Response en quelques secondes

Si l'entreprise avait déployé la technologie Antigena Network Autonomous Response, le manque d'attention accordé aux alertes de Darktrace n'aurait pas eu d'importance : alors que 4 heures se sont écoulées entre le téléchargement de l'exécutable et le premier fichier chiffré, Antigena aurait neutralisé la menace en quelques secondes. Exemples d'actions qu'Antigena aurait effectuées en réponse à certaines des alertes pour cet incident :

- **Session administrateur SMB inhabituelle :** Informations d'identification compromises utilisées pour se connecter au serveur
  - **Action d'Antigena :** cette seule anomalie ne nécessite aucune action, mais augmente le niveau d'alerte.
- **Nouvelles informations d'identification administrateur sur client :** l'attaquant a utilisé de multiples nouvelles informations d'identification administrateur sur l'appareil
  - **Action d'Antigena :** Possédant désormais une preuve de menace avec un niveau de confiance élevé, Antigena appliquerait le « modèle comportemental normal » de connexion typique de l'appareil ; tous les administrateurs qui se connectent normalement sur cet appareil peuvent continuer à le faire tandis que les nouvelles connexions sont bloquées pendant une heure.
- **Balayage du réseau :** l'attaquant a balayé le réseau afin d'identifier d'autres victimes
  - **Action d'Antigena :** ce serveur n'a jamais balayé le réseau auparavant, seuls les appareils des administrateurs le font. Antigena empêcherait donc l'appareil de balayer le réseau pendant deux heures.
- **EXE depuis un emplacement externe rare :** des contenus téléchargés ultérieurement pour poursuivre l'infection
  - **Action d'Antigena :** Antigena autoriserait toujours l'appareil à effectuer des téléchargements normaux tout en bloquant les téléchargements depuis des emplacements rares.

Antigena Email :
Arrêter un ransomware à la source

De nombreuses attaques de type ransomware passent par les plateformes de messagerie électronique, prouvant que les passerelles de messagerie et les approches de détection traditionnelles s'appuyant sur des règles et des signatures ne sont pas suffisamment solides pour détecter un ransomware avancé à chaque fois. De plus, ces solutions traditionnelles ont un champ d'action limité et ne réussissent pas à associer l'activité des e-mails aux actions malveillantes liées dans l'ensemble de l'infrastructure digitale.

Grâce au pouvoir de la Cyber IA, Antigena Email bâtit une compréhension approfondie de chaque humain derrière chaque adresse e-mail. La technologie s'adapte à vos équipes dynamiques afin de reconnaître les changements de comportement même subtils qui indiquent une campagne de ransomware.

Elle répond ensuite de façon autonome et proportionnée afin d'arrêter la menace à la vitesse de la machine et de protéger votre entreprise de l'exposition : en suspendant entièrement l'e-mail, en verrouillant un lien ou en convertissant des pièces jointes en un type de fichier inoffensif.

Si le ransomware réussit à arriver dans la boîte de réception et à pénétrer sur le réseau, Antigena Email est capable de collaborer avec l'Enterprise Immune System pour retracer l'origine de l'attaque et empêcher toute propagation latérale.

En mettant en corrélation les modèles d'activité du reste de l'entreprise avec l'environnement d'e-mail, la Cyber IA peut effectuer une analyse des causes profondes afin d'identifier la source de l'e-mail et d'autres activités de l'e-mail qui peuvent être liées à l'incident. Antigena Email récupère ensuite tous les e-mails menaçants des boîtes de réception des autres employés, afin de limiter le plus possible l'étendue de l'attaque de type ransomware.

D'ici 2021, une attaque de type ransomware aura lieu toutes les 11 secondes.

Source: Cybersecurity Ventures

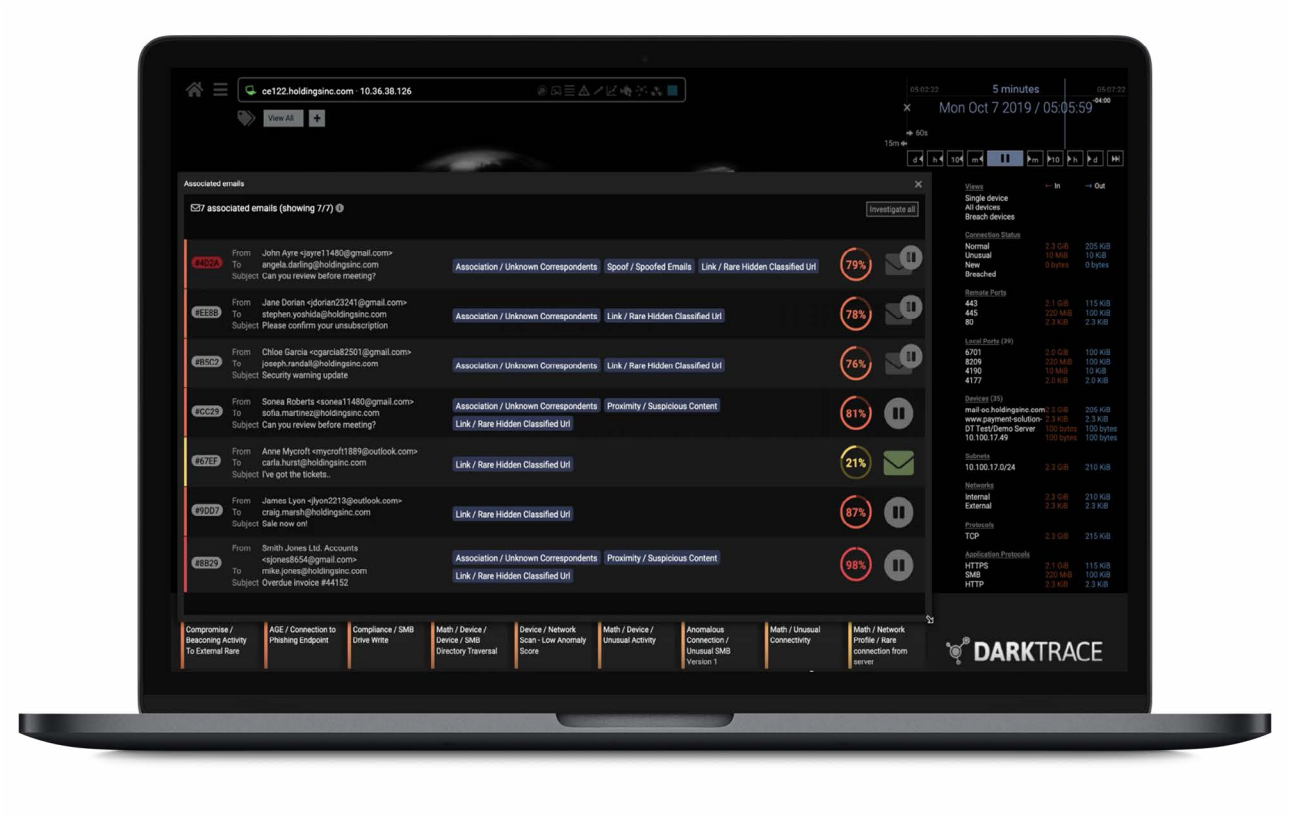

Figure 3 : Antigena Email détecte une série d'e-mails associés à une campagne de ransomware

Neutralisation de liens malveillants dans une municipalité

Une célèbre municipalité aux États-Unis a récemment été victime d'une attaque par e-mail ciblée qui aurait pu être une tentative d'intrusion de ransomware dans l'organisation. Au lieu de cela, Antigena Email a détecté la menace dès son apparition et a fait en sorte d'empêcher tout téléchargement de contenus malveillants, ransomware ou autre.

L'auteur de la menace avait apparemment eu accès au carnet d'adresses de la municipalité, puisque chaque e-mail était personnalisé pour le destinataire et distribué par ordre alphabétique, de A à Z. Alors que chaque e-mail semblait inoffensif, 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 Email a été capable d'analyser ces liens cachés en rapport avec les « modèles comportementaux normaux » des destinataires visés. 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 municipalité n'avaient visité le domaine de l'expéditeur auparavant.

La technologie a instantanément envoyé une alerte de confiance élevée et a suggéré de façon autonome de verrouiller chaque lien qui entrait sur le réseau.

Parce qu'Antigena a été déployé en « mode passif », il n'a pas pu agir de manière indépendante pour arrêter la menace à la vitesse de la machine, mais a révélé l'efficacité de la Cyber IA et de l'Autonomous Response. 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 même qu'elle n'atteigne le premier utilisateur, défendant l'entreprise contre une attaque de type ransomware potentielle répandue.

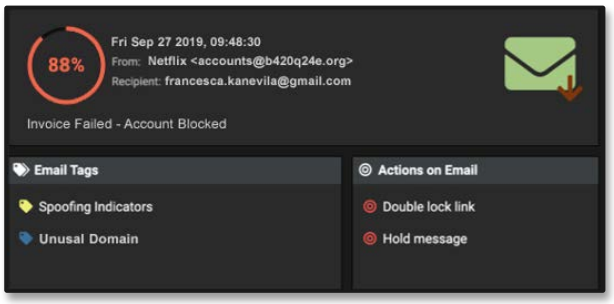

Figure 4 : Antigena Email a signalé chaque e-mail comme étant hautement anormal.

Ransomware suivi jusqu'au compte e-mail personnel

Lorsque le ransomware est arrivé dans la boîte de réception d'une grande société de télécommunications, la plateforme de Cyber IA Darktrace a pu détecter et contenir de manière autonome l'attaque avant qu'elle puisse chiffrer un seul fichier.

La menace initiale s'est produite lorsqu'un employé a accédé à sa messagerie personnelle depuis un smartphone professionnel et a téléchargé à son insu un lien malveillant contenant le ransomware. Quelques secondes plus tard, son appareil s'est connecté à un serveur externe sur le réseau Tor et les activités de chiffrement SMB ont commencé.

En seulement 9 secondes, la Cyber IA a déclenché une alerte prioritaire indiquant le besoin d'une analyse immédiate du comportement rare.

Comme le comportement a persisté pendant les quelques secondes suivantes, la Cyber IA a revu son jugement et a activé Antigena de façon autonome.

L'équipe de sécurité étant rentrée chez elle pour le week-end, Antigena Network a pu arrêter l'attaque de façon indépendante en interrompant toutes les tentatives d'écriture de fichiers chiffrés sur les partages de fichiers du réseau.

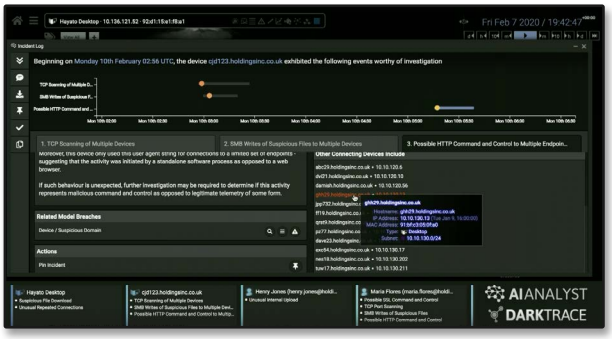

Figure 5 : Capture d'écran de l'IU montrant la Cyber IA signalant des activités SMB anormales similaires.

Si l'entreprise avait déployé Antigena Email, il est probable que le ransomware n'aurait jamais été téléchargé. Aucun outil n'est une solution miracle. Toutefois, même si le ransomware avait réussi à pénétrer sur le réseau via la boîte de réception, Antigena Email aurait fait la corrélation entre l'activité malveillante détectée sur le réseau et l'e-mail compromis d'origine. La technologie aurait récupéré d'autres e-mails similaires dangereux dans les boîtes de réception des employés.

Grâce à une compréhension approfondie et évolutive de l'ADN de votre entreprise, Antigena Email et la plateforme de Cyber IA Darktrace offrent une détection en temps réel et une réponse aux attaques de type ransomware sophistiquées.

L'Enterprise Immune System avec le Cyber AI Analyst : Comprendre l'étendue d'un incident de type ransomware

La Cyber IA auto-apprenante permet à l'Enterprise Immune System de détecter des changements nuancés d'activité qui indiquent un ransomware émergent, sans s'appuyer sur les renseignements sur les menaces connus. Avec sa compréhension sur mesure et en constante évolution des « modèles comportementaux » normaux à travers votre infrastructure, l'Enterprise Immune System met en évidence les écarts les plus subtils, afin de s'assurer que votre équipe de sécurité est informée dès qu'une attaque à la vitesse de la machine frappe.

Le Cyber AI Analyst, élément clé de l'approche du « système immunitaire », analyse automatiquement chaque événement anormal détecté. Pour les campagnes de ransomware, il peut mettre en évidence sur chaque appareil affecté, la source de l'infection, et toutes les informations contextuelles dont vous avez besoin pour initier une réponse.

Le Cyber AI Analyst est connu pour réduire le temps de triage de 92 % et peut mettre en évidence un ransomware émergent comme étant une menace critique nécessitant une intervention humaine. Un « rapport d'incident » généré par l'IA offre une chronologie interactive, une description concise de la campagne, ainsi que des données granulaires sur l'appareil concerné ou le comportement de l'utilisateur.

Ces rapports se mettent à jour de façon autonome au fur et à mesure de l'évolution de la menace et sont cruciaux pour aider les experts de la sécurité à prendre conscience de la situation, et à partager les informations clés même avec les parties prenantes non techniciennes.

Analyse experte d'une attaque Dharma

Lorsqu'une campagne de ransomware Dharma ciblée a été lancée contre une entreprise britannique, l'Enterprise Immune System a été essentiel dans la détection de la menace et a révélé la capacité du Cyber AI Analyst à identifier et signaler une attaque émergente.

La Cyber IA a instantanément perçu le risque lorsqu'un serveur RDP a reçu un grand nombre de connexions depuis des adresses IP rares. Les analyses ultérieures ont révélé que les informations d'identification RDP avaient été probablement compromises un peu avant l'attaque.

Le lendemain, la Cyber IA a observé que l'auteur de la menace utilisait de manière abusive le protocole SMB version 1. Puis, une connexion externe inhabituelle vers une adresse IP marocaine rare et l'échec de la session SMB vers l'adresse IP sur un port très inhabituel ont été observés. Deux heures plus tard, l'auteur de la menace a mis en œuvre une commande plus forte et des canaux de contrôle se connectant à des destinations rares en Inde, en Chine et en Italie.

La Cyber IA a également détecté une reconnaissance interne lorsque les connexions RDP entrantes ont commencé à balayer le réseau et qu'un volume important de données a été transféré vers une adresse IP inhabituelle au Panama.

Enfin, le contenu Dharma a été exécuté. Parallèlement à l'activité de chiffrement, le ransomware a essayé d'infecter d'autres machines en utilisant les informations d'identification d'un administrateur vues pendant la reconnaissance interne. Lorsque le chiffrement a commencé, le personnel informatique a débranché le serveur RDP.

Même si l'équipe n'a pas prêté attention aux alertes précédentes de Darktrace, la Cyber IA a pu identifier chaque étape de cette attaque sophistiquée, permettant à l'équipe de réagir de manière efficace et d'empêcher tout dégât supplémentaire.

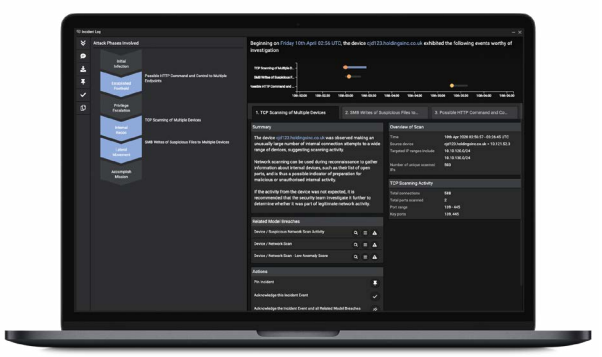

Figure 6 : Capture d'écran de l'IU montrant le Cyber AI Analyst signalant une attaque de type ransomware.

L'Enterprise Immune System a détecté chaque étape de cette campagne en s'appuyant sur un comportement anormal dans le contexte de cette entreprise, sans dépendre de signatures de menace correspondantes.

Dans ce type d'attaque réalisée sur une durée longue avec différents indicateurs d'activité malveillante, le Cyber AI Analyst joue un rôle clé pour montrer clairement la nature et l'étendue de la menace.

Avec un rapport d'incident du Cyber AI Analyst, l'équipe a pu facilement analyser grâce à un résumé général de l'attaque de ransomware et à des détails précis sur chaque étape de l'incident.

.

L'Industrial Immune System : Défendre les systèmes opérationnels contre un ransomware

En matière de lutte contre les ransomwares, l'Industrial Immune System est la solution la plus puissante pour assurer la sécurité d'un environnement opérationnel moderne. En particulier face aux menaces telles que le ransomware EKANS, premier ransomware connu pour cibler les machines ICS, il est vital d'employer des outils de sécurité capables de s'adapter en permanence aux environnements OT et de défendre ces systèmes même contre les attaques « zero day ».

De nombreuses campagnes de ransomware ciblent également les environnements industriels à travers des vulnérabilités dans l'infrastructure informatique. Les vulnérabilités indirectes représentent une menace supplémentaire, car les systèmes OT peuvent devenir des dommages collatéraux lors d'attaques orientées IT. Étant donné les dégâts potentiels pour l'infrastructure cruciale, le besoin d'une technologie de sécurité pouvant corréler des modèles à travers une infrastructure disparate est de plus en plus urgent.

L'IA auto-apprenante permet à l'Industrial Immune System d'identifier clairement les menaces même aussi avancées qu'un nouveau ransomware. La technologie présente la capacité unique d'apprendre ce qui constitue un « comportement normal » pour des technologies et des types de déploiements radicalement différents, qu'il s'agisse d'API vieux de plusieurs décennies, de capteurs distribués ou de systèmes IoT industriel.

De plus, avec sa vue unifiée, la Cyber IA comprend la connexion entre l'activité malveillante dans les systèmes informatiques et le comportement dans les systèmes OT, ce qui la rend nettement capable d'arrêter les menaces qui se déplacent entre les silos de sécurité traditionnels.

Détecter un ransomware dans une raffinerie

Sur un site intégré de raffinerie/distribution de pétrole, l'Industrial Immune System de Darktrace a joué un rôle essentiel pour arrêter une attaque de type ransomware sur le réseau de l'entreprise.

La Cyber IA a identifié les premiers signes d'infection par ransomware dans un appareil de bureau sur le réseau. En plus d'écrire ses propres fichiers de notes de rançon, l'appareil a effectué une série de connexions avec des destinations externes rares via un serveur proxy interne, puis a téléchargé des fichiers potentiellement malveillants, des activités que Darktrace peut détecter et corréler grâce à ses connaissances granulaires de ce qui constitue « l'identité » de l'entreprise.

L'appareil a commencé à effectuer des recherches dans le répertoire SMB, une activité que la Cyber IA a détectée comme étant anormale par rapport à ses connaissances sur l'appareil.

L'Industrial Immune System a signalé cette activité comme étant un ransomware probable, alertant l'équipe de sécurité du client avant que l'infection ne puisse se propager dans les environnements OT.

Grâce à la capacité de la Cyber IA à connecter des modèles comportementaux à travers l'infrastructure diverse, le système industriel a été défendu contre cette attaque à la vitesse de la machine.

Figure 7 : Capture d'écran de l'IU montrant un appareil infecté par un ransomware identifié par la Cyber IA.