

La Cyber IA pour les municipalités

Des centaines de municipalités et de villes dans le monde entier font confiance à la Cyber IA pour se protéger contre les cyberattaques les plus sophistiquées, y compris les ransomwares et autres attaques automatisées. Lorsque les équipes de sécurité sont dépassées, la machine riposte.

La Cyber IA de Darktrace:

- ✓ Protège plus de 130 organisations du secteur public et 60 municipalités américaines
- ✓ Répond à une menace émergente toutes les 3 secondes dans le monde entier
- ✓ S'installe en seulement 1 heure



Pris en otage

Certaines des attaques de ransomware les plus importantes de l'année dernière ont été menées contre des villes et des autorités locales américaines, entraînant le chiffrement de données critiques et la paralysie de services vitaux.

Ces récentes vagues de ransomwares ont mis en évidence les vulnérabilités auxquelles les infrastructures connectées et les services publics sont confrontés face aux menaces de plus en plus sophistiquées et rapides. Les campagnes de ransomware sont conçues spécifiquement pour identifier et exploiter les faiblesses de leurs cibles, et se répandre sur les réseaux en quelques secondes. Leur rapidité et leur sophistication ne permet pas aux équipes de sécurité de réagir avant que les dégâts ne soient causés.

Les gouvernements et les décideurs politiques reconnaissent l'importance des solutions avancées pour l'ensemble de leurs environnements numériques et s'appuient sur la Cyber IA et la technologie de Réponse Autonome pour protéger les services et les infrastructures critiques des villes et des municipalités.

«Darktrace Antigena est la seule technologie de cyberdéfense automatisée du marché capable de mener nos batailles les plus cruciales.»

Michael Sherwood, Directeur de la Technologie et de l'Innovation, Ville de Las Vegas

La machine riposte

La Cyber IA primée de Darktrace bénéficie de la confiance de centaines de villes, de municipalités et de fournisseurs d'infrastructures nationales essentielles aux États-Unis et dans le monde, y compris la smart city de Las Vegas.

La technologie Darktrace est capable non seulement d'identifier, mais également de répondre aux cyberattaques telles que les ransomwares, avant qu'elles ne chiffrent les fichiers, interrompent les opérations municipales, et ne désactivent les services publics.

Inspirée du système immunitaire humain, l'IA de Darktrace apprend de façon autonome ce qui est normal pour chaque environnement numérique, sans utiliser de règles ou de signatures. L'IA avancée de Darktrace forme une compréhension en constante évolution du domaine numérique unique de chaque organisation, lui permettant ainsi d'identifier et de répondre à une activité malveillante au moment même où elle se produit – y compris les nouvelles menaces jusque-là inconnues de tous.

En utilisant une technologie unique connue sous le nom de «Réponse Autonome», reconnue par Gartner comme l'avenir de la cyberdéfense, Darktrace Antigena contre-attaque en temps réel, neutralisant les ransomwares en quelques secondes.

Lutter contre : Ransomware

Les outils de sécurité traditionnels utilisant des règles et des signatures pour arrêter les cybermenaces en périphérie sont désormais mal équipés pour se défendre contre les attaques automatisées de ransomwares et autres menaces zero-day. Avec l'émergence de malwares plus sophistiquées que jamais, les équipes humaines sont désormais dépassées dans leur capacité à neutraliser les menaces.

Cependant, avec les capacités de détection et de Réponse Autonome de l'IA auto-apprenante de Darktrace, l'identification et l'arrêt des nouvelles attaques de ransomwares et autres menaces zero-day sont désormais monnaie courante. En raison du comportement très anormal du ransomware qui s'écarte du « modèle comportemental normal » numérique, la Cyber IA de Darktrace détectera les attaques dans les secondes suivant l'apparition d'un comportement menaçant sur le réseau.

Dès lors que des connexions anormales sont établies à des serveurs externes, Darktrace Antigena est activé et interrompra les tentatives de chiffrement SMB des fichiers partagés - empêchant instantanément les attaques de se propager au-delà du patient zéro.

«Pour nous, déployer Darktrace n'était pas une option ; c'était une nécessité pour rester en avance sur les menaces avancées et imprévisibles d'aujourd'hui.»

Paul Haugan, Directeur de l'Innovation et de la Technologie, Ville d'Auburn

Étude de cas: Ville de Westland

En février 2017, un employé de la ville de Westland a été victime d'une attaque de phishing après avoir cliqué sur un lien d'email malveillant. Quelques secondes plus tard, le ransomware Cryptolocker a commencé à se répandre sur tout le réseau.

Peu de temps après l'attaque, le DSI de la ville de Westland a décidé de déployer l'IA de Darktrace. La technologie d'auto-apprenante de Darktrace comprend un « modèle comportemental normal » unique pour chaque utilisateur et appareil dans l'ensemble de l'environnement numérique, ce qui lui permet d'identifier les cybermenaces en temps réel. L'IA de Darktrace prend des mesures intelligentes et éclairées pour isoler l'attaque en quelques secondes, le tout sans perturber les systèmes informatiques et les services publics critiques de la ville.

Avec seulement 5 agents de sécurité à plein temps protégeant les données sensibles de plus de 84 000 habitants, la Cyber IA de Darktrace s'est avérée indispensable pour protéger les infrastructures de la ville. La ville de Westland est maintenant convaincue que son infrastructure est protégée, peu importe comment et quand les menaces frappent.

Preuve de Valeur

Découvrez comment la Réponse Autonome peut augmenter votre cyberdéfense en commençant votre essai gratuit de 30 jours. Dans le cadre d'une Preuve de Valeur (POV) Darktrace, vous bénéficierez d'un cyber-technologue Darktrace dédié et d'un accès à notre interface de visualisation des menaces primée, le Threat Visualizer.

- S'installe en 1 heure
- Accès au Threat Visualizer
- Rapport des menaces découvertes en moins d'une semaine
- 100% visibilité de votre environnement

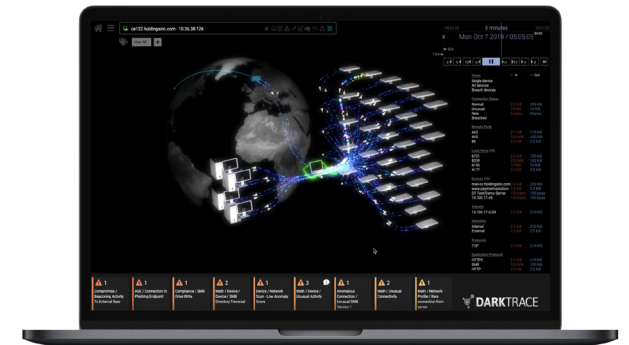


Figure 1: la Cyber IA identifie une attaque de type ransomware