PRÉSENTATION DE LA SOLUTION

FortiAI Virtual Security Analyst™

Permettre aux équipes surchargées des opérations de sécurité de passer de la réactivité à la proactivité

Résumé

L'augmentation constante du volume, de la vitesse et de la sophistication des menaces submerge les équipes chargées des opérations de sécurité des entreprises dans tous les secteurs. Heureusement, les architectes sécurité qui tentent de réduire leur charge de travail disposent d'un nouvel outil : l'intelligence artificielle (IA) de nouvelle génération. Fortinet, qui a été l'un des premiers à utiliser l'intelligence artificielle dans le domaine de la cybersécurité, relève ces défis avec FortiAI Virtual Security Analyst™. FortiAI intègre sur site la dernière technologie de protection contre les violations de données basée sur l'intelligence artificielle pour analyser les menaces entrantes en moins d'une seconde. Les équipes de sécurité ont ainsi la possibilité d'arrêter les pirates et les logiciels malveillants avant qu'ils ne pénètrent dans leurs réseaux.

61 % des entreprises déclarent qu'aujourd'hui elles ne peuvent pas détecter les tentatives de violation de données sans l'utilisation des technologies d'intelligence artificielle.[1]

Le paysage des menaces avancées met à rude épreuve les équipes surchargées des opérations de sécurité presque jusqu'au point de rupture, sans aucun allègement en vue. L'augmentation rapide du volume, de la vitesse et de la sophistication des menaces oblige les architectes sécurité à trouver des solutions. En raison du volume élevé d'alertes, nombre d'entre elles sont ignorées en raison d'un manque de bande passante dans 42 % des entreprises.[2] De plus, l'aide sous forme de nouveaux membres d'équipe n'est pas disponible dans de nombreuses entreprises. Le manque de compétences en matière de cybersécurité s'aggrave même, atteignant plus de 4 millions de personnes.[3]

L'évolution de l'intelligence artificielle dans la cybersécurité

Les entreprises de cybersécurité utilisent depuis plusieurs années l'apprentissage automatique (AA) dans la lutte contre les cybercriminels, notamment dans le domaine de la détection des menaces. Les algorithmes d'apprentissage utilisent l'apprentissage automatique pour permettre une identification de plus en plus précise des caractéristiques des fichiers malveillants. Il en résulte une détection en temps réel des menaces avancées, y compris des attaques de type « zero-day ».[4] Cette évolution des technologies de sécurité est aujourd'hui une nécessité pour les entreprises. Par exemple, une étude récente révèle que plus de 6 entreprises sur 10 seraient incapables de détecter les menaces critiques sans elle.[5]

Mais une meilleure détection des menaces ne suffit pas à faire en sorte que les équipes chargées des opérations de sécurité se sentent moins débordées. En fait, une meilleure détection entraîne un volume encore plus important d'alertes qui doivent être traitées manuellement. Au contraire, une automatisation *accrue* est également nécessaire, en particulier dans le domaine de la réponse aux menaces et de la stratégie de sécurité. Heureusement, l'émergence d'une nouvelle génération d'intelligence artificielle promet de soulager le stress des membres des équipes chargées des opérations de sécurité tout en les rendant globalement plus productives.

L'intelligence artificielle de nouvelle génération : des réseaux neuronaux profonds

Pour décrire le potentiel de l'intelligence artificielle de nouvelle génération en matière de cybersécurité, il est utile de définir les termes avec précision (figure 1) :

- L'**intelligence artificielle** est un terme général qui fait référence à la capacité d'une machine à imiter le comportement humain intelligent.
- L'**apprentissage automatique** est un composant de l'intelligence artificielle qui utilise les données pour résoudre des problèmes linéaires tels que la réalisation de prévisions ou l'exécution de tâches. Les réseaux neuronaux artificiels (RNA) sont une méthode d'apprentissage automatique courante. Ils utilisent du matériel et des logiciels pour créer une configuration modelée sur le fonctionnement des neurones du cerveau humain via l'apprentissage automatique. Les modèles sont alimentés en permanence par de grandes quantités d'informations que le système analyse et ajuste en fonction des nouvelles tactiques et capacités adoptées par un logiciel malveillant ou un vecteur d'attaque.
- Les **réseaux neuronaux profonds** (RNN), parfois connus sous le nom d'apprentissage profond, sont une technique d'apprentissage automatique qui utilise plusieurs réseaux neuronaux artificiels, avec deux ou plusieurs couches entre les couches d'entrée et de sortie, afin de modéliser des relations complexes et non linéaires.

Un exemple peut aider à illustrer la différence entre l'apprentissage automatique standard et les réseaux neuronaux profonds. L'apprentissage automatique peut être utilisé pour enseigner à un ordinateur l'alphabet anglais et la façon dont les lettres sont placées ensemble pour former des mots. Ensuite, il peut fournir un dictionnaire de mots anglais avec des définitions et des images. Grâce à l'apprentissage automatique, il est possible d'identifier des mots trouvés dans des ensembles de données, tels que « abeille », « polliniser », « fleur », « champ » et « jour ». En revanche, les réseaux neuronaux profonds peuvent apprendre à un ordinateur à décrire « une nouvelle photographie d'une abeille pollinisant une fleur dans un champ pendant la journée », en se basant sur des images de chacune de ces caractéristiques présentées dans le passé.

Les degrés de compréhension et d'analyse rendus possibles par les réseaux neuronaux profonds permettent de faire passer l'intelligence artificielle au niveau supérieur en matière de cybersécurité. Lorsque l'intelligence artificielle est utilisée uniquement pour la détection des menaces, elle peut potentiellement *augmenter* le stress de l'équipe chargée des opérations de sécurité, car elle ne fait qu'ajouter au volume important d'alertes qu'elle reçoit déjà. Elle accroît également la probabilité qu'une menace spécifique ne reçoive pas de réponse rapide.

En revanche, si l'intelligence artificielle peut être utilisée pour prendre des décisions intelligentes sur la réponse à aux menaces et même fournir des informations utiles sur la stratégie de sécurité, elle peut commencer à soulager les professionnels surchargés des opérations de sécurité. Les membres du personnel peuvent rester concentrés sur la stratégie de sécurité alors que la plupart des réponses aux menaces sont traitées en temps réel et de manière automatisée par un *analyste de sécurité virtuel*.

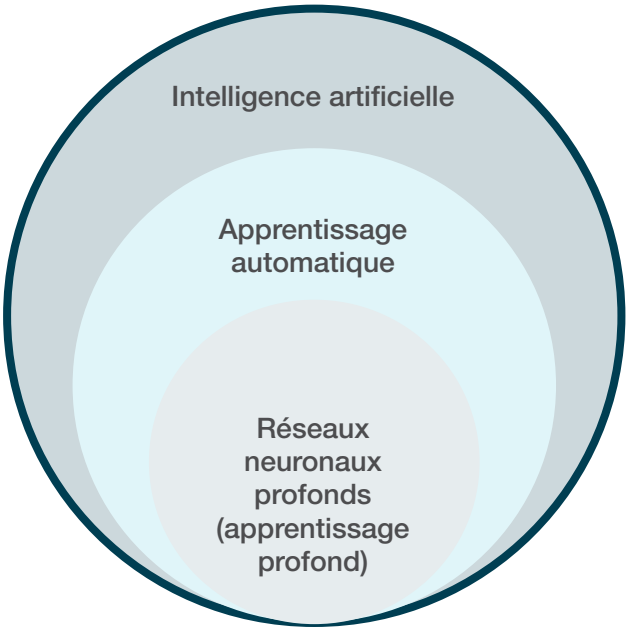

Figure 1. La relation entre l'intelligence artificielle, l'apprentissage automatique et les réseaux neuronaux profonds.

S'appuyer sur huit ans d'intelligence artificielle

Fortinet a été l'un des premiers à adopter l'intelligence artificielle pour la détection des menaces, en déployant un système de détection évolutif (SEDS) basé sur les réseaux neuronaux artificiels, en 2012, après quatre ans d'apprentissage opérationnel avant le lancement. Le système de détection évolutif analyse des millions d'objets par jour et confirme ceux qui sont malveillants. Il alimente ensuite les produits de Fortinet Security Fabric avec ces informations.

Ce système de détection évolutif géré par FortiGuard Labs a subi un apprentissage pendant 12 ans utilisant à la fois l'apprentissage automatique supervisé et non supervisé. Il en résulte une détection extrêmement précise, en temps réel, des menaces inconnues et polymorphes, en fonction de leurs caractéristiques, avec pratiquement aucun faux positif. Depuis lors, Fortinet a ajouté l'analyse en ligne des applications Web au pare-feu d'applications Web (WAF) FortiWeb, a introduit l'analyse basée sur l'intelligence artificielle dans FortiSandbox, et a inclus l'analyse comportementale des utilisateurs et des entités (UEBA) basée sur l'intelligence artificielle via FortiInsight et la sécurité avancée des terminaux avec FortiEDR.

« Si vous connaissez votre attaquant et que vous pouvez réagir rapidement, les chances de contrer votre véritable adversaire sont plus grandes si vous pouvez réagir en temps réel. »[6]

FortiAI Virtual Security Analyst : l'intelligence artificielle de nouvelle génération sur site

Aujourd'hui, Fortinet est le premier à proposer sur site un analyste de sécurité virtuel basé sur les réseaux neuronaux profonds. En effet, **FortiAI Virtual Security Analyst** peut vraiment être décrit comme le « système de détection évolutif géré 2.0 » de Fortinet. Il s'agit du premier produit du marché qui intègre une intelligence artificielle indépendante et évolutive sur site pour imiter la fonction d'analyste de sécurité des informations. Comme un analyste de sécurité humain, il s'adapte aux nouvelles attaques et acquiert de l'expérience au fil du temps. Mais contrairement à un analyste humain, il le fait à la vitesse d'une machine. Il utilise les réseaux neuronaux profonds pour automatiser les analyses des incidents et créer des renseignements personnalisés sur les menaces afin de perturber les attaques ciblées à la vitesse de la machine.

Le modèle d'apprentissage non supervisé basé sur les réseaux neuronaux artificiels de FortiAI peut réellement être qualifié d'« intelligence artificielle amicale » (IAA), un terme qui est resté au stade de la théorie jusqu'à présent. Et grâce à ses fonctionnalités d'apprentissage automatique, l'analyste de sécurité virtuel identifie et analyse les menaces avec une rapidité et une précision toujours plus grandes, ce qui permet d'augmenter le personnel de sécurité et de rendre son travail plus productif.

Utiliser l'intelligence artificielle pour en savoir plus sur des entreprises spécifiques

Afin d'accélérer les renseignements sur les menaces à la vitesse de la machine et de suivre l'évolution du paysage des menaces avancées, FortiAI apprend et s'adapte aux nouvelles attaques visant une entreprise spécifique au fil du temps, en améliorant et en optimisant continuellement le cycle de vie de la protection contre les menaces. Ainsi, FortiAI soutient le personnel chargé des opérations de sécurité en identifiant et en analysant les logiciels malveillants basés sur des fichiers ou non, et identifie les systèmes compromis dans l'ensemble de l'entreprise avec une certitude absolue, le tout en moins d'une seconde.

Pour ce faire, FortiAI utilise les réseaux neuronaux profonds pour prendre les décisions qu'un analyste de sécurité prendrait lors de l'analyse manuelle des attaques, notamment :

- La **classification de l'attaque** dans une catégorie personnalisable, notamment les rançongiciels, le cryptominage pirate, les vers, les attaques par porte dérobée, les fuites de données, les botnets et les rootkits
- L'**analyse de l'origine de l'attaque** en retraçant la source initiale de l'infection grâce à un horodatage et en fournissant une visibilité complète de la propagation latérale du patient zéro à tous les systèmes compromis ultérieurement
- L'**analyse des logiciels malveillants** détermine le type de logiciel malveillant en fonction des caractéristiques observées par les réseaux neuronaux artificiels de FortiAI et fournit une chronologie pour chaque événement d'infection. Cela ressemble à un modèle miniature de chaîne de cybercriminalité qui décrit en termes scientifiques ce que la menace a tenté de faire, étape par étape, y compris la technique employée. Par exemple, au « temps zéro », un fichier HTML a été *téléchargé* ; au « temps un », un code malveillant a été exploité dans un navigateur ; au « temps deux », un cheval de Troie a été téléchargé dans un répertoire utilisateur ou temporaire. Ici, FortiAI est prédéfini avec 3 milliards de caractéristiques de logiciels malveillants et en apprend d'autres au fil du temps.

Comme FortiAI Virtual Security Analyst assure ces niveaux d'analyse, son intégration complète avec le pare-feu de nouvelle génération (NGFW) FortiGate permet de bloquer les menaces qu'il identifie. Le personnel chargé des opérations de sécurité peut ensuite appliquer les renseignements aux contrôles de sécurité sur le réseau.

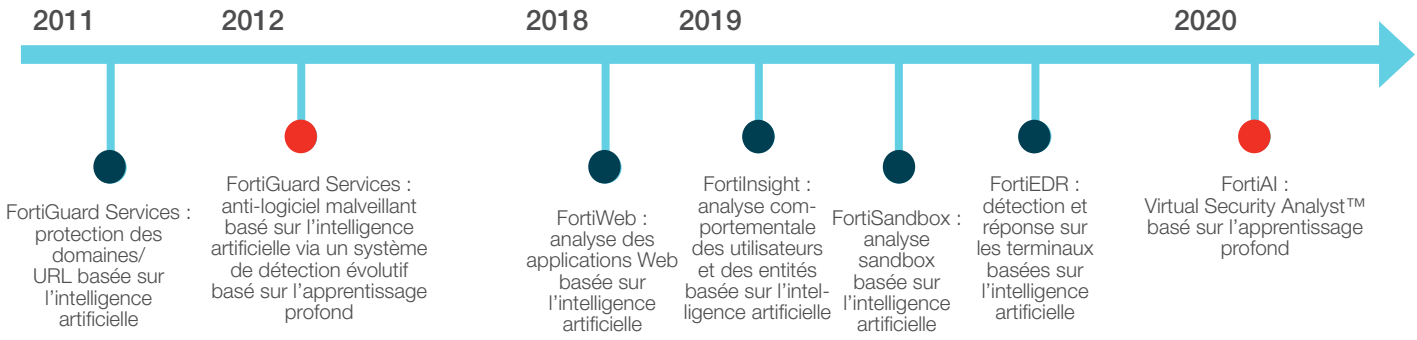

Figure 2. Chronologie du développement de l'intelligence artificielle et de l'apprentissage automatique par Fortinet.

Avantages de FortiAI pour les équipes de cybersécurité

FortiAI Virtual Security Analyst peut aider les équipes surchargées des opérations de sécurité à passer d'une posture de sécurité réactive à une posture de sécurité proactive, tout en augmentant leur efficacité opérationnelle. Il offre les principaux avantages suivants :

1. **Neutralisation plus rapide des attaques.** L'analyse automatisée en temps réel de chaque incident de sécurité permet de réagir plus rapidement aux menaces automatisées qui se propagent à la vitesse de la machine. Comme l'impact d'une intrusion augmente avec le temps, la réponse en temps réel est le meilleur moyen de minimiser les dommages.

« Le champ de bataille du futur est le numérique, et l'intelligence artificielle est l'arme de prédilection incontestée. »[7]

2. **Réduction de la fenêtre Réduction de la fenêtre d'exposition aux menaces.** Grâce à l'analyse appliquée en temps réel, les entreprises sont moins vulnérables en attendant le correctif d'application ou la signature anti-logiciel malveillant d'un fournisseur. Au lieu de cela, après avoir été alertée en moins d'une seconde, l'équipe chargée des opérations de sécurité peut bloquer les logiciels malveillants dans un processus que l'on pourrait qualifier d'« application de correctifs virtuels ».
3. **Amélioration de la productivité grâce à l'élimination virtuelle des faux positifs.** Les entreprises n'ont plus besoin d'appliquer des flux de menaces génériques aux contrôles de sécurité et d'analyser manuellement chaque faux positif.[8]

[1] « Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security », Capgemini, consulté le 27 janvier 2020.

[2] Jon Oltsik, « Dealing with Overwhelming Volumes of Security Alerts », ESG, 3 mars 2017.

[3] « (ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide », (ISC)², 6 novembre 2019.

[4] « Using AI to Address Advanced Threats That Last-Generation Network Security Cannot », Fortinet, 8 juin 2019.

[5] « Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security », Capgemini, consulté le 27 janvier 2020.

[6] David Strom, « Understanding the Relationship Between AI and Cybersecurity », Security Intelligence, 22 mars 2018.

[7] William Dixon et Nicole Eagan, « 3 ways AI will change the nature of cyber attacks », World Economic Forum, 19 juin 2019.

[8] Chris McDaniels, « Is Threat Intelligence Garbage? », Dark Reading, 23 mars 2018.

FORTINET

www.fortinet.fr

juillet 20, 2020 4:08 PM

594577-0-1-FR

sb-FA-fortiai-virtual-security-analyst-a4_FR