PRÉSENTATION DE LA SOLUTION

Des opérations de sécurité basées sur l'intelligence artificielle

Une prévention, une détection et une réponse plus rapides aux menaces

Résumé

Alors que le paysage des menaces continue de s'accélérer, la tâche à accomplir reste la même. Pour réduire le cyber-risque, il faut prévenir le plus grand nombre possible de cyber-menaces tout en détectant les intrusions réussies et en y réagissant le plus rapidement possible afin de minimiser les dommages et les dépenses.

L'investissement de Fortinet dans l'intelligence artificielle (IA) permet aux organisations de tirer de plus en plus parti de l'IA et d'autres techniques avancées, déployées sur la surface d'attaque numérique et le long de la chaîne de cyberdéfense, afin de réduire leur risque de cybersécurité à un moment où l'on manque de personnel de sécurité. Aussi, la Fortinet Security Fabric offre-t-elle la plate-forme de cybersécurité la plus complète, la plus intégrée et la plus automatisée de l'industrie.

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

Accélérer le volume, la vitesse et la sophistication du paysage des menaces

De 2018 à 2019, la quantité totale des informations sur les menaces, y compris les nouveaux fichiers, sites web, exploits et autres, que reçoit FortiGuard Labs, a augmenté de 34% pour atteindre un total de 940 TB. Il ne fait aucun doute que le volume même des cyber-menaces dans la nature continue d'augmenter, parallèlement à l'expansion de la surface d'attaque numérique de la plupart des organisations.

En outre, la vitesse des campagnes de cyber-attaques a continué à s'accélérer. En 2019, le cycle de vie moyen d'une campagne de menace donnée, depuis l'apparition initiale à la prévalence maximale et à l'émergence d'une nouvelle variante ou campagne, était souvent d'un mois ou moins. Il existe un écosystème mature de cybercriminalité dans lequel les kits d'exploitation, les logiciels malveillants en tant que service (MaaS), les robots à louer et d'autres encore ont considérablement réduit le « délai de mise sur le marché » pour les cybercriminels. On peut dire que, dans l'ensemble, cette industrie est passée à un développement et à une livraison agiles.

Dans le même temps, la sophistication de nombreuses cyber-menaces s'est également accrue et ne se limite pas aux attaques très ciblées des États-nations. Les efforts de malveillance dans tous les domaines, y compris l'ingénierie sociale, les techniques d'évasion des logiciels libres et une foule d'autres innovations, donnent lieu à des menaces de plus en plus convaincantes pour les utilisateurs finaux et difficiles à détecter par les contrôles de sécurité traditionnels.

Données sur les menaces de FortiGuard Labs

Utiliser la vitesse des machines et l'intelligence pour garder une longueur d'avance

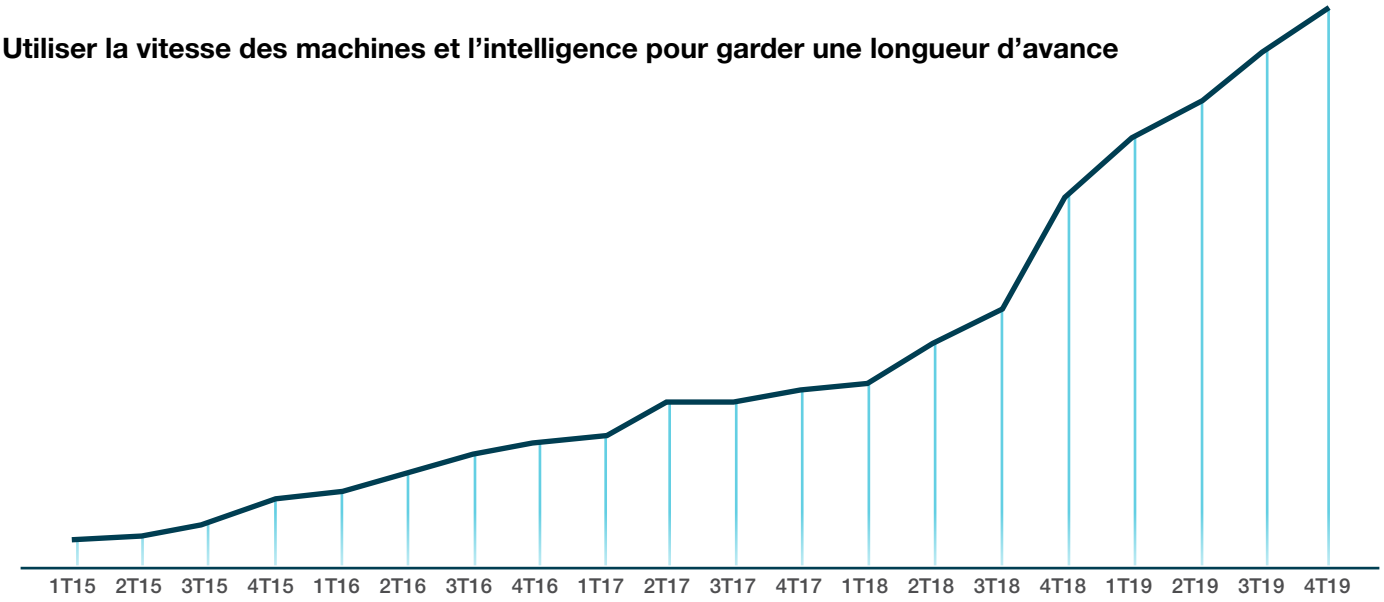

Schéma 1 : Volume de la cyber-menace entre le 1T 2015 et le 4T 2019.

Heureusement, les progrès de l'IA et de la puissance de calcul permettent (lorsqu'ils sont correctement formés et appliqués) de suivre le rythme de ce paysage de la cybermenace. Que l'objectif soit de tenir à jour les renseignements sur les menaces mondiales, d'identifier les incidents propres à une organisation avant qu'ils ne se transforment en brèches, ou même de mettre en place une prévention en temps réel répartie dans toute l'infrastructure de sécurité, l'IA peut et est effectivement disponible pour aider.

Opérations de sécurité basées sur l'intelligence artificielle

Fortinet utilise et fournit une gamme de technologies avancées, y compris l'IA, pour aider les organisations à prévenir, détecter et répondre rapidement à l'évolution constante du paysage des cyber-menaces. Certaines de ces technologies aident à générer les renseignements sur les menaces fournis aux clients et utilisés par les contrôles de sécurité en ligne qui protègent les points d'extrémité, le réseau, les applications et les vecteurs d'attaque dans le cloud. D'autres sont déployées de manière centralisée au sein des organisations pour continuer à rechercher les menaces qui ont pu contourner ces contrôles et pour accélérer la réponse aux incidents. D'autres encore peuvent être déployées dans toute l'entreprise, souvent en mode bloquant pour prévenir les attaques en temps réel.

Ces solutions peuvent être utilisées dans diverses combinaisons pour établir une défense coordonnée contre les cybercriminels, tout au long de la chaîne de cyberdéfense. L'étendue de la couverture donne aux organisations de nombreuses possibilités d'arrêter les cyber-menaces à plusieurs étapes avant une violation de données ou un autre impact important sur les opérations.

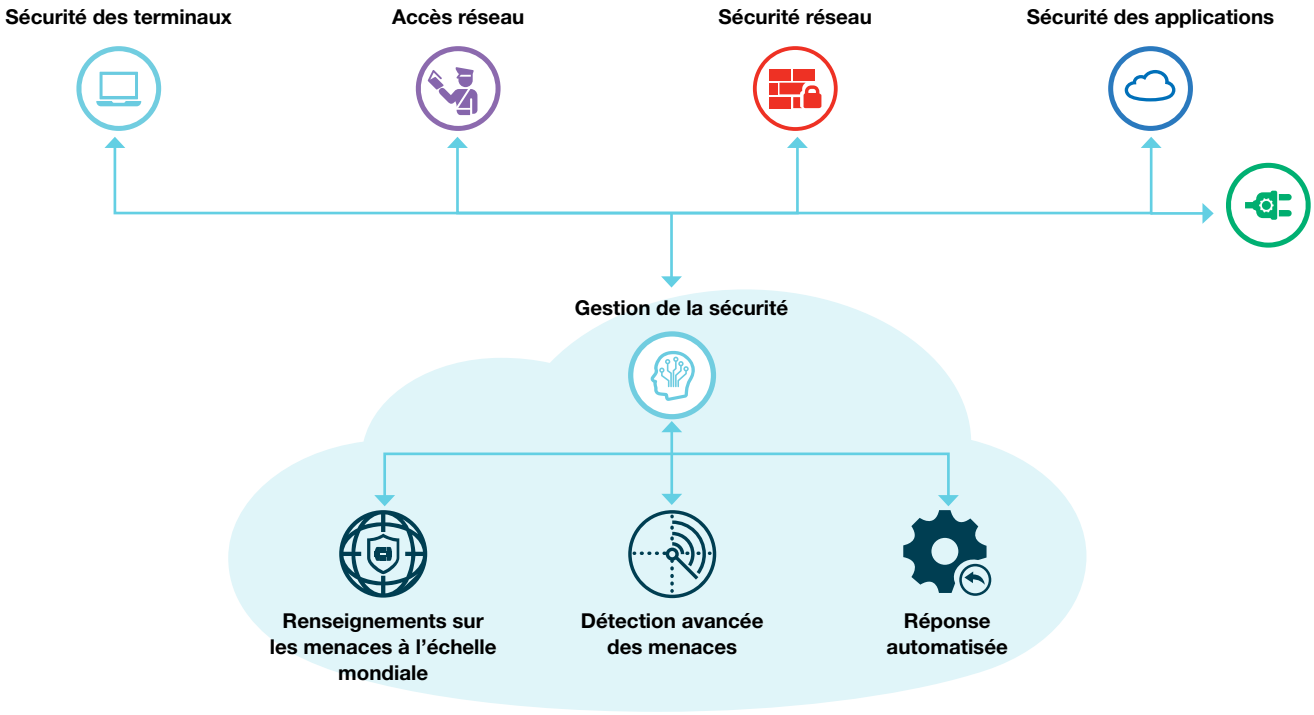

Schéma 2 : L'IA alimente une grande partie des moyens de prévention, de détection et d'intervention de Fortinet.

L'IA pour la prévention des menaces

Depuis le point d'extrémité, en passant par le réseau, ses applications et le cloud, Fortinet offre une efficacité de sécurité de premier ordre de manière indépendante et cohérente. Les produits Fortinet comprennent la plate-forme de protection des terminaux FortiClient (EPP), le pare-feu de nouvelle génération (NGFW) de FortiGate, la passerelle de messagerie électronique sécurisée FortiMail (SEG) et le Firewall pour application Web (WAF).

Tous ces programmes sont alimentés par les renseignements sur les menaces de FortiGuard Labs, un groupe mondial et multidisciplinaire de recherche sur les menaces. Couvrant plus de 10 domaines différents de la cybersécurité, FortiGuard Labs maintient une vue globale des cyber-menaces, basée sur une combinaison de collectes proactives de menaces, de plus de 200 partenariats de partage d'informations entre les secteurs d'activité et d'un réseau mondial de 5 millions de capteurs de dispositifs.[3]

FortiGuard Labs génère des renseignements sur les menaces à partir d'analyses fondées sur l'IA de plus de 100 milliards d'événements de sécurité par jour.[2]

Afin d'ingérer, de corréler et d'analyser efficacement la grande quantité de données brutes reçues quotidiennement, FortiGuard Labs a mis en place une infrastructure d'arrière-plan robuste et un processus hautement automatisé pour transformer rapidement les données sur les menaces en renseignements sur les menaces, qui sont régulièrement fournis aux produits de prévention des menaces Fortinet par le biais de mises à jour des services d'abonnement.

Schéma 3 : Les renseignements sur les menaces fournis par FortiGuard Labs permettent à de nombreux produits Fortinet d'identifier les dernières cyber-menaces.

Le premier système d'IA de Fortinet, développé en 2011, a été conçu pour aider à filtrer l'énorme volume de nouveaux sites Web qui apparaissent chaque jour, en signalant ceux qui présentent le plus de risques pour une enquête supplémentaire par les chercheurs de la menace. Aujourd'hui, environ 130000 à 150000 nouveaux sites Web sont enregistrés chaque jour, ce qui rend l'évaluation humaine de chacun d'entre eux de plus en plus irréalisable. Pour gérer l'augmentation exponentielle du nombre de sites Web nécessitant une inspection, quatre systèmes d'apprentissage automatique sont utilisés. Ces systèmes traitent la quantité massive de télémesures de sites Web reçues par le réseau de capteurs Fortinet afin de hiérarchiser les sites Web à haut risque, tels que ceux qui hébergent des algorithmes de génération de domaines (DGA) ou des serveurs de commande et de contrôle (C2), pour une analyse plus approfondie.

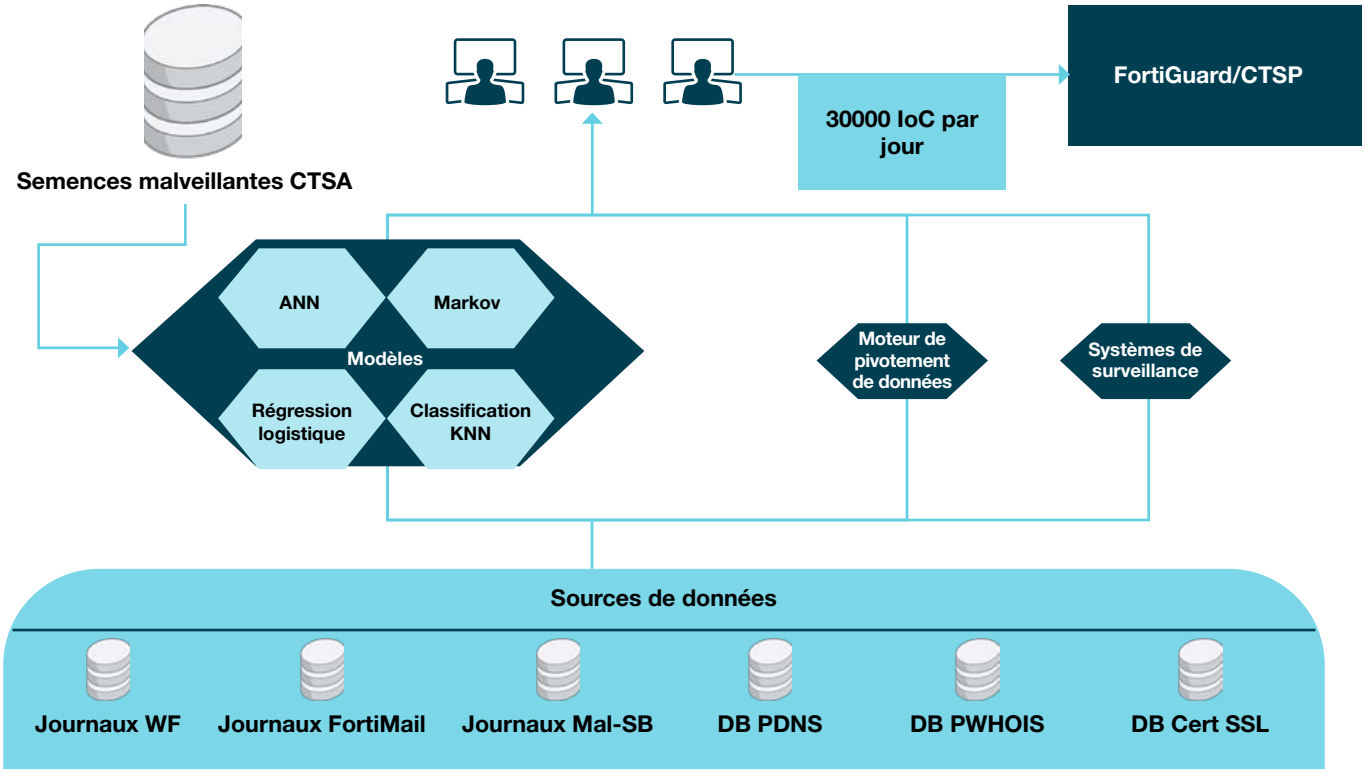

Schéma 4 : Fortinet recueille chaque jour un grand nombre de sites Web provenant de sources multiples et applique quatre modèles d'apprentissage machine distincts pour classer les sites par ordre de priorité en vue d'une analyse plus approfondie, ce qui permet de générer en fin de compte 30000 indicateurs de compromission (IoC) par jour.

Le grand projet suivant, lancé en 2012, portait sur l'accélération du volume d'échantillons basés sur des fichiers, qui s'élevait à plus de 23 millions par jour fin 2019. Ce système automatise également un processus d'analyse des logiciels malveillants, qui nécessite huit heures ou plus d'effort manuel de la part d'un chercheur sur les menaces. Plus précisément, un réseau de neurones artificiels (RNA) facilite la génération de nouvelles informations sur les menaces qui sont également fournies aux clients à peu près toutes les heures.

▪ Approche

- **Couche 1 =** Traitement du fichier d'entrée
- **Couche 2 =** plus de 15 milliards de nœuds identifient les bonnes et les mauvaises caractéristiques
- **Couche 3 =** mathématiques mises à part (1 = malveillant, 0 = propre)

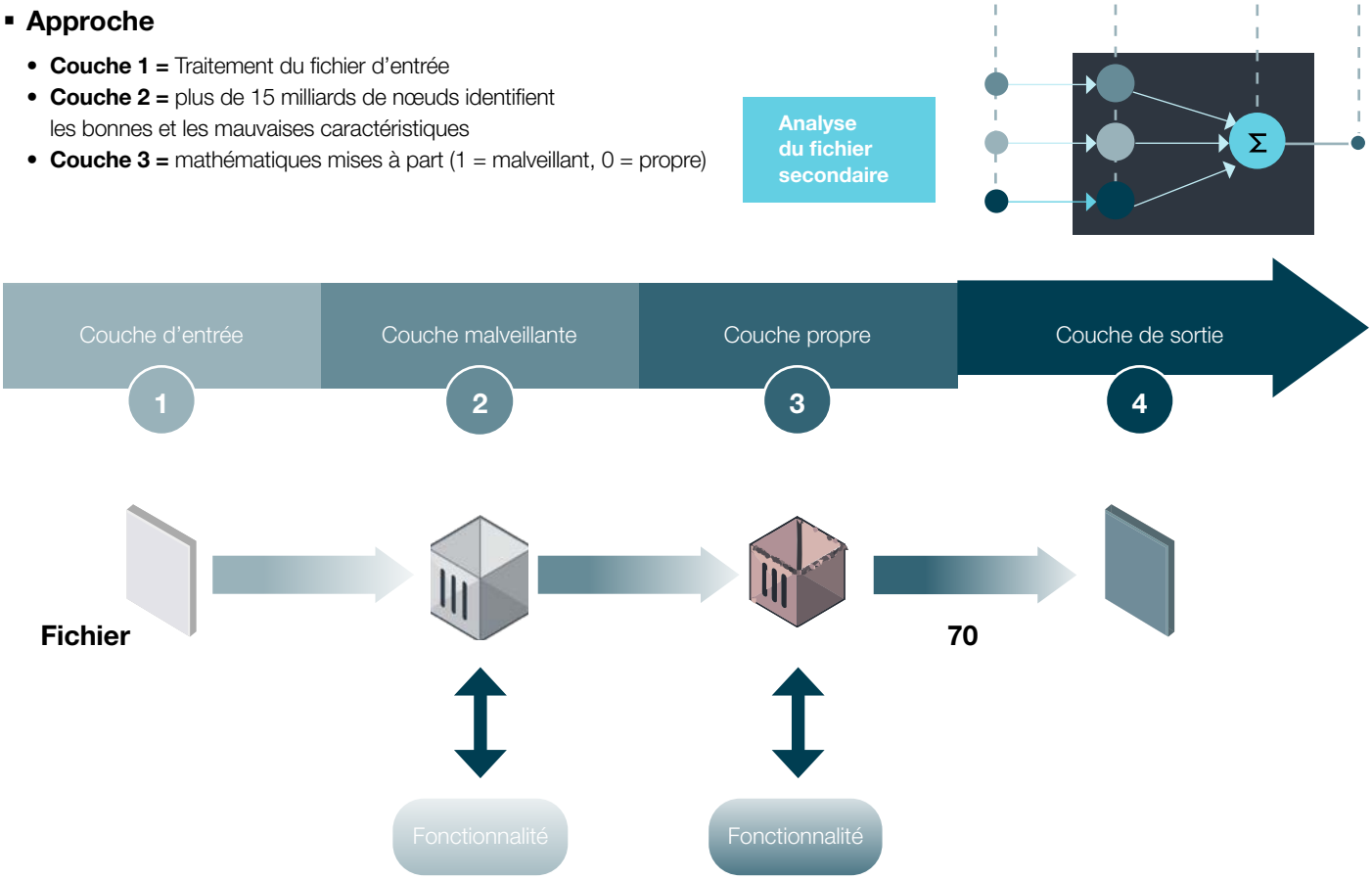

Schéma 5 : Les réseaux de neurones artificiels (RNA) de Fortinet sont composés de plus de 15 milliards de nœuds, qui ont été appris à partir de données uniques sur les menaces mondiales recueillies pendant de nombreuses années. En utilisant un apprentissage automatique pour entraîner le modèle, la détection des menaces est constamment mise à jour au fur et à mesure de leur évolution, et la précision globale est améliorée.

Plus récemment, deux couches d'un apprentissage automatique ont également été intégrées dans le **WAF de FortiWeb** pour protéger l'infrastructure Web publique. Une couche établit des profils pour chaque paramètre dans une application Web donnée et identifie les écarts. La deuxième couche détermine si les écarts représentent une menace cyber (par opposition à une erreur humaine ou autre) en les examinant par rapport à des seuils prédéfinis d'activité malveillante. Cette approche a permis de réduire considérablement le réglage continu du WAF qui était nécessaire par le passé. Il existe également de nombreux modèles d'apprentissage automatique qui alimentent la capacité antivirus de nouvelle génération de **FortiEDR**, basée sur le comportement.

FortiGuard Labs fournit à ses clients plus d'un milliard de mises à jour de sécurité chaque jour.[4]

FortiGate, FortiMail et FortiClient sont intégrés à **FortiSandbox**, qui complète l'analyse traditionnelle de l'exécution virtuelle par deux filtres basés sur l'apprentissage automatique. Un filtre est utilisé pour l'analyse statique de fichiers, et l'autre est appliqué aux comportements observés lors de l'exécution de Sandbox. Avec ces deux filtres, le Sandbox assisté par apprentissage automatique est souvent capable de renvoyer des déterminations de menace de 10 millisecondes. Dans FortiMail et FortiClient, les clients sont en mesure de mettre en quarantaine les contenus suspects jusqu'à la fin de l'analyse de Sandbox et de bloquer même les menaces précédemment inconnues à l'aide des filtres FortiSandbox basés sur l'apprentissage automatique.

L'IA pour la détection de menaces spécifiques aux organisations

Un cybercriminel déterminé peut échapper aux contrôles de sécurité les plus stricts axés sur la prévention. Il est essentiel que les organisations appliquent des analyses avancées similaires à leur propre trafic et à leur environnement, en identifiant les incidents avant qu'ils n'entraînent des répercussions commerciales coûteuses. Fortinet offre un certain nombre de produits pour détecter les menaces entrantes, installées et actives tout au long de la chaîne de cyberdéfense.

FortiDeceptor déploie une série d'appâts de grande valeur dans toute l'organisation. Ces leurres attirent la reconnaissance des cyber-criminels, avant le début d'une cyber-campagne, ou les tentatives de se déplacer latéralement dans le réseau afin de voler ou d'exfiltrer des données.

FortiSandbox peut être déployé en ligne (comme mentionné précédemment) ou dans le centre des opérations de sécurité (SOC) afin de détecter des tentatives de livraison de charges utiles armées. Il est complété par FortiAI, qui apporte une version du RNA développée pour l'analyse de fichiers à FortiGuard Labs dans le propre environnement de l'organisation. **FortiAI** permet de détecter en moins d'une seconde des logiciels malveillants jusque-là inconnus, de suivre automatiquement les indicateurs de ces logiciels malveillants dans toute l'organisation, et de fournir une cartographie plus complète du cycle de vie des menaces, semblable à celle générée par un analyste de sécurité qualifié.

Si la diffusion de logiciels malveillants est réussie, **FortiEDR** utilise un traçage de code unique en temps réel qui complète son antivirus de nouvelle génération pour l'identification post-infection de comportements suspects de l'hôte. Ces comportements peuvent être immédiatement désamorcés pour stopper la menace éventuelle, et soumis au cloud où les RNA sont utilisés pour classer rapidement le comportement suspect comme bénin ou malveillant. Cela permet soit d'enquêter et de remédier correctement à l'hôte en question, soit de le remettre en service avec un impact opérationnel minimal.

Enfin, **FortiInsight** se concentre sur l'accès et la circulation des données, une action cybercriminelle commune en phase avancée. Il applique des mesures de probabilité bayésiennes pour identifier les activités anormales au sein de groupes de pairs (utilisateurs ou dispositifs) qui peuvent refléter un risque d'initié ou un hôte compromis. Les administrateurs sécurité peuvent non seulement enquêter sur l'anomalie, mais aussi fournir un retour d'information sur la valeur de chaque alerte. Cela permet de former le modèle d'apprentissage automatique pour qu'il devienne de plus en plus efficace pour signaler un risque d'initié.

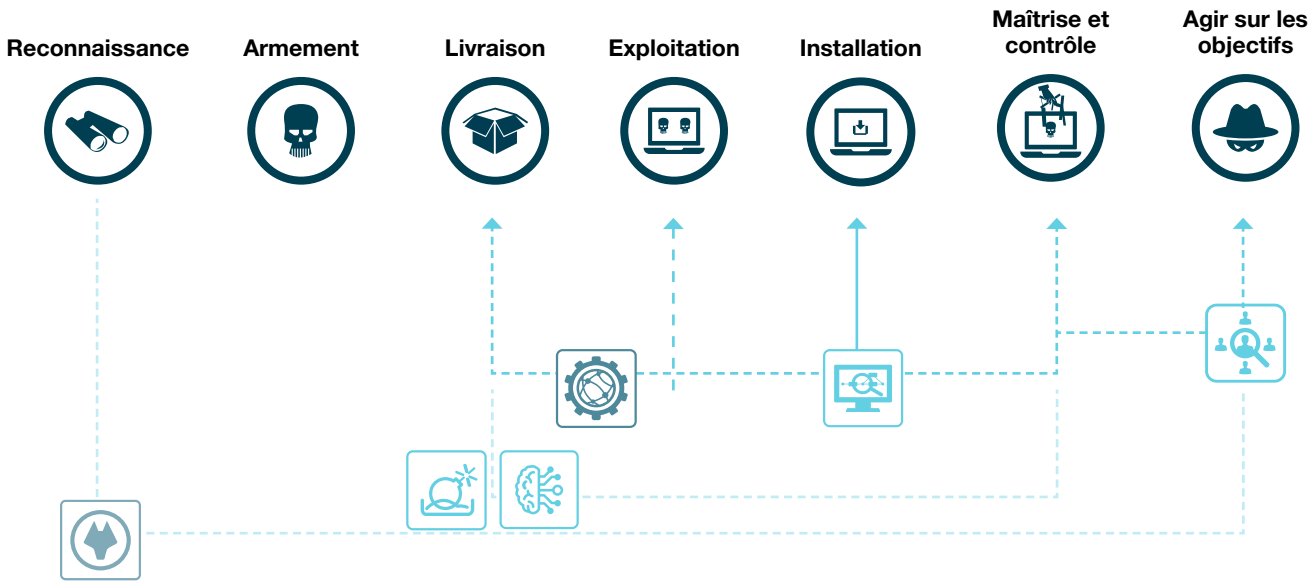

Schéma 6 : Application des solutions Fortinet à la chaîne de cyber-menaces.

L'IA et l'automatisation pour accélérer la réponse aux incidents

La détection est simplement un précurseur de la réponse. C'est pourquoi Fortinet propose une gamme d'offres pour aider les organisations de tous les niveaux de maturité en matière de sécurité à orchestrer et automatiser les actions de réponse. **FortiAnalyzer** fournit des analyses fondamentales, ainsi que des automatismes de base de grande valeur, dans toute la Fortinet Security Fabric. Il convient même aux plus petites ou aux plus récentes équipes de sécurité.

À mesure que les organisations font mûrir leurs fonctions de sécurité et recherchent une visibilité et une réponse multi-fournisseurs, **FortiSIEM** s'intègre à une large gamme de produits informatiques et de sécurité pour ingérer, corréler et appliquer des analyses avancées qui peuvent déclencher des mesures correctrices automatisées dans des environnements hétérogènes.

Les solutions Fortinet permettent aux organisations d'appliquer l'IA dans toute la chaîne de cyber-menaces pour accélérer la détection des menaces et la réponse.[5]

Pour le SOC avancé avec des processus opérationnels bien définis, **FortiSOAR** peut se superposer à n'importe quel outil de collecte de journaux ou de gestion des informations et des événements de sécurité (SIEM) afin de créer des directives qui orchestrent et automatisent ces processus. Il est à noter que l'IA est utilisée pour déterminer la priorité des nouvelles alertes et même pour les assigner à des responsables. Ainsi, les flux de réponse sont établis et deviennent plus efficaces, avec la possibilité, dans de nombreux cas, d'automatiser des étapes clés.

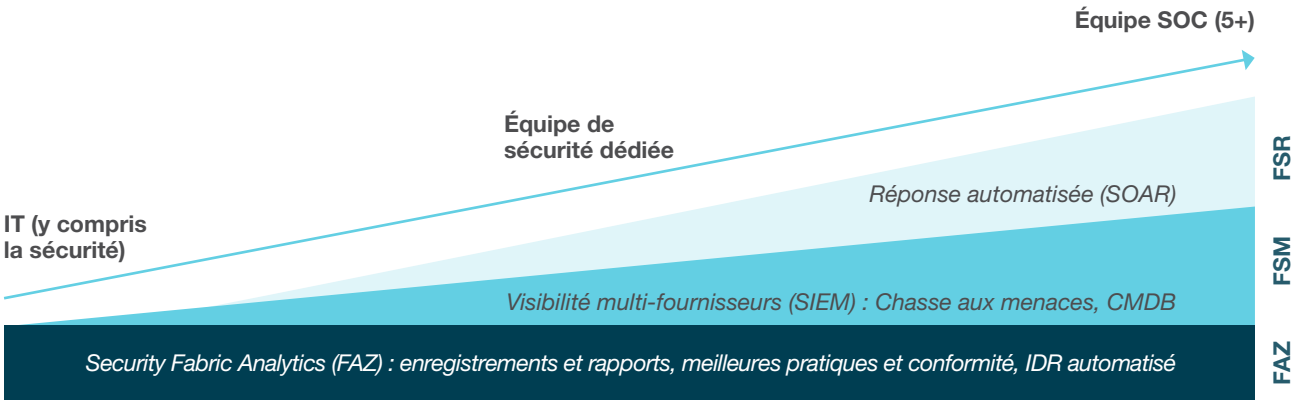

Schéma 7 : Les solutions Fortinet comblent les lacunes de sécurité et réduisent le temps de correction en automatisant la détection et la réponse aux menaces.

L'intelligence artificielle dans le monde, à travers tous les vecteurs d'attaque et la chaîne de cyber-menaces

Fortinet investit depuis longtemps et de manière continue dans l'IA pour relever les défis croissants de la cybersécurité. Les modèles d'apprentissage automatique et les RNA plus sophistiqués, formés par les chercheurs de menaces de FortiGuard Labs, analysent de vastes quantités de télémétrie brute et aident à générer des mises à jour de renseignements sur les menaces à l'échelle mondiale. Ils sont complétés par des systèmes d'IA similaires qui peuvent être déployés dans toute une organisation pour la prévention en ligne, couvrant les points d'extrémité et les courriels vers le réseau et le cloud, ainsi que la détection continue et même la réponse.

Cela permet à Fortinet d'offrir une cyberdéfense robuste basée sur l'IA pour les opérations de sécurité qui utilise les avantages de l'apprentissage automatique global, centralisé et distribué et d'autres IA. Avec des modèles d'IA formés et appliqués pour chaque étape de la chaîne de cyberdéfense, de la reconnaissance à l'action sur les objectifs, les solutions Fortinet sont capables de gérer les risques externes et internes avec une prévention, une détection et une réponse avancées.

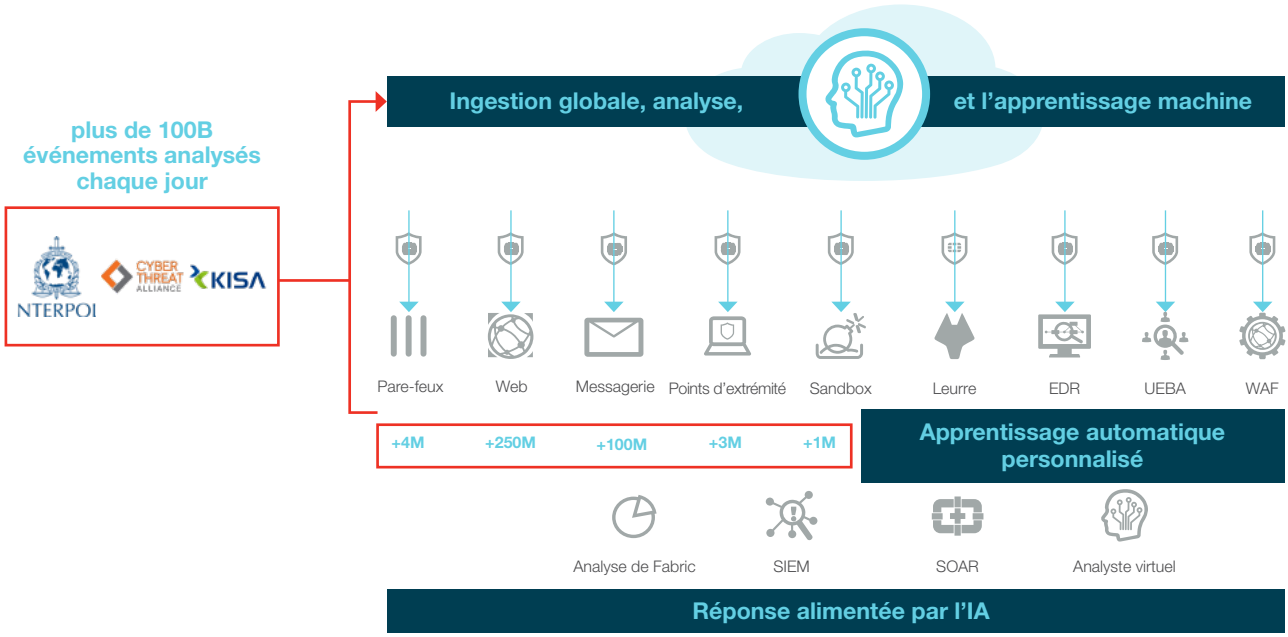

Schéma 8 : Cent milliards d'événements de sécurité sont traités par l'IA de FortiGuard Labs chaque jour afin de fournir, aux produits Fortinet, des mises à jour de renseignements sur les menaces.

[1] « Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security (Réinventer la cybersécurité grâce à l'intelligence artificielle : une nouvelle frontière dans la sécurité numérique), » Capgemini, consulté le 23 mars 2020.

[2] « FortiGuard Security Services (Services de sécurité FortiGuard) », Fortinet, octobre 2019.

[3] « Fortinet Security Fabric Enables Digital Innovation: Broad, Integrated, and Automated (La Fortinet Security Fabric de Fortinet permet l'innovation numérique : Globale, intégrée et automatisée) », Fortinet, 13 février 2020.

[4] « FortiGuard Security Services (Services de sécurité FortiGuard) », Fortinet, octobre 2019.

[5] « Fortinet Introduces Self-Learning Artificial Intelligence Appliance for Sub-Second Threat Detection (Fortinet présente un appareil d'intelligence artificielle autodidacte pour la détection des menaces à la seconde près) », Fortinet, 24 février 2020.

FORTINET®

www.fortinet.fr

septembre 24, 2020 3:42 PM

627225-0-0-FR