Proposé par SPIE ICS et Fortinet

Comment améliorer la détection des menaces cyber grâce aux nouveaux outils issus de l'intelligence artificielle ?

S'il est un terme devenu incontournable pour toute entreprise au cours de l'année écoulée, c'est bien celui d'Intelligence Artificielle. L'IA a vocation à devenir un puissant levier d'efficience au sein des organisations publiques et privées. Elle peut aussi les aider à intégrer de nouvelles technologies de renforcement au service de leur cybersécurité. A condition toutefois de s'appuyer sur des données saines, structurées et sécurisées. Et de sensibiliser les utilisateurs aux nouveaux usages issus de l'IA. Entretien croisé entre Michael Bazy, Channel Systems Engineer chez Fortinet et Bogdan Stefanescu, Directeur Centre de Compétences chez SPIE ICS.


© DR


© R. Wailliez

De gauche à droite : **Michael Bazy**, Channel Systems Engineer chez Fortinet et **Bogdan Stefanescu**, Directeur Centre de Compétences chez SPIE ICS.

Comment cet apport de l'IA se concrétise-t-il aujourd'hui, plus particulièrement dans les stratégies de cybersécurité ? Et comment le cadre législatif européen suit-il cette évolution ?

Bogdan Stefanescu. Je souhaite rappeler brièvement que les algorithmes d'intelligence artificielle permettent de réaliser trois fonctions principales. La classification : comment catégoriser les données pour pouvoir ensuite les exploiter plus simplement. La prédiction : grâce à un historique d'analyses et des corrélations, on peut prédire ce qui va se produire avec un certain niveau de probabilité. La dernière fonction, qui a trait à la partie dite « générative » de l'IA c'est la génération de contenus. Celle-ci s'opère à partir d'une masse d'informations, stockées, analysées et interprétées pour ensuite générer de nouveaux contenus. Les algorithmes d'IA reproduisent aujourd'hui des comportements humains comme la créativité, la planification ou le raisonnement.

L'Union européenne réfléchit à un cadre juridique spécifique à l'Intelligence Artificielle. Ce cadre permettrait de définir les risques liés à son utilisation, et plus particulièrement, à la notion de « risque inacceptable ». Cela permettrait d'interdire l'usage de l'Intelligence Artificielle dans les cas de risques inacceptables : des systèmes considérés comme une menace pour les personnes. Ces risques se divisent en trois grandes catégories. D'abord, ce qui est en lien avec les manipulations comportementales de personnes. Ensuite, le « score social » (la classification des personnes en fonction du statut socio-économique). Enfin, les systèmes d'identification biométriques et de reconnaissance faciale.

Michaël Bazy. Nous constatons chez Fortinet que nos clients ont de plus en plus recours à des solutions d'Intelligence Artificielle pour automatiser la détection des menaces et améliorer la gestion des règles de sécurité. L'exploitation de modèles de menaces permet aussi de caractériser plus facilement les incidents. On peut enfin utiliser l'IA pour synthétiser l'information et générer des contenus à la fois sécurisés et adaptés à chaque utilisateur. Quant au cadre législatif, il a effectivement évolué pour mettre davantage l'accent sur la réponse aux incidents. La volonté du législateur européen est d'améliorer la gestion des risques – tout en tenant compte des défis et des opportunités posées par l'intelligence artificielle générative.

Est- ce que les organisations sont prêtes à intégrer l'IA dans leurs stratégies cyber ? A quelles conditions ce déploiement peut-il se faire ?

Bogdan Stefanescu. Si aujourd'hui une grande majorité des entreprises reconnaissent qu'il est primordial de déployer des technologies d'IA, seule une faible majorité se déclare prête à les mettre en œuvre dans ses processus quotidiens. Cela soulève une vraie question : comment injecter des données propres, complètes et bien labélisées dans des outils capables de les traiter et de donner

des bons résultats de manière sécurisée ? Cette phase de préparation est importante : elle requière beaucoup d'énergie et une véritable hygiène de traitement. Peu d'entreprises y arrivent encore aujourd'hui.

Michaël Bazy. Les entreprises doivent envisager une stratégie permettant d'équilibrer l'innovation et la sécurité. L'automatisation des tâches répétitives ou l'analyse avancée des données permettent effectivement de prendre des décisions plus éclairées. Mais les entreprises doivent rester prudentes quant à la sécurité de leurs données et leur conformité réglementaire. Il existe plusieurs manières d'exploiter les données et d'utiliser les modèles d'IA, que ce soit via des LLM ou du Deep Learning. Il faut donc bien les choisir et la tâche n'est pas si aisée qu'on le pense.
De plus, les employés, doivent être formés et sensibilisés aux risques et aux opportunités associés à l'usage de l'IA. La fuite de données, par exemple, représente un facteur de risque majeur lorsqu'elles se retrouvent intégrées par inadvertance dans les modèles d'apprentissages. Il est donc essentiel de collaborer avec des fournisseurs d'IA capables de partager leurs engagements en matière de sécurité et de confidentialité. Il est également possible de fournir des solutions d'intelligence artificielle privées ou avec des paramètres de sécurité renforcés, pour protéger les données sensibles et empêcher les exfiltrations involontaires de données.

Comment choisir le bon modèle d'IA ? Et comment appréhender sa consommation en ressources ?

Bogdan Stefanescu. Ma conviction m'amène à privilégier des algorithmes adaptés en fonction des données à analyser pour répondre à des enjeux très spécifiques. Pourquoi cela ? On attend de plus en plus de ces algorithmes qu'ils ne mobilisent que les ressources dont ils ont besoin : ils doivent s'inscrire dans une dynamique Numérique Responsable. Je crois en un modèle d'IA complètement décentralisé : c'est la raison pour laquelle nous avons initié une démarche de Recherche & Développement via une chaire de recherche avec l'INSA de Lyon. Nous souhaitons déployer l'IA sur des infrastructures classiques et l'adapter à des cas d'usage bien spécifiques.
Cette chaire a pour objectif de créer un moteur d'IA en Edge Computing, capable d'analyser des données en temps réel, au plus proche de leur source de production, et de les traiter localement de manière responsable. Son ambition est de favoriser l'accès des ETI et organisations publiques au data management en mettant à leur disposition une alternative « on premise » (sur site) dans un climat de confiance numérique renforcée, alliant souveraineté et Numérique Responsable.

Quels sont les cas d'usages que vous voyez émerger aujourd'hui sur le marché ?

Bogdan Stefanescu. La connaissance du contexte des organisations est un élément très important. Il s'agira ici de solutions spécifiques de détection des menaces, par exemple d'analyse en temps réel de données de trafic réseau ou d'apprentissage automatique pour la détection des anomalies. Ces solutions peuvent intégrer et analyser un vaste nombre de rapports de menaces, pour mieux repérer et signaler les vecteurs d'attaque. Ensuite, la gestion des identités et l'authentification sont également capitales. Lorsque l'on sait que la reconnaissance biométrique et faciale est utilisée pour mieux cibler une personne au cours d'une attaque, il faut y accorder une importance de premier plan. Enfin, il ne faut pas négliger la sécurité de l'architecture et du code en tant que tels. Désormais, des outils d'IA permettent d'examiner le code et d'en faire ressortir les potentielles vulnérabilités.

Michaël Bazy. Pour ce qui est des Large Language Models (LLM), les solutions disponibles intègrent de plus en plus des fonctionnalités d'assistance. Un ingénieur faisant des requêtes spécifiques à une base de données doit aujourd'hui connaître plusieurs langages de programmation : l'apport de l'IA pourrait lui permettre de se concentrer sur des tâches plus essentielles, comme l'analyse d'incidents. C'est ici que les LLM entrent en jeu : ils peuvent être utilisés au sein des SOC (Security Operation Centers) pour générer des réponses standards à des questions courantes. Concernant un vecteur d'attaque en forte croissance, le phishing, les LLM peuvent être entraînés pour identifier des tentatives de cyberattaques. Dernier cas d'usage : l'analyse de « logs », de journaux. L'IA permet de traiter des volumes conséquents de données, de comprendre le contexte d'une attaque et de repérer les anomalies.

Quel est l'apport du partenariat entre Fortinet et SPIE ICS ? Comment tire-t-il parti des forces des deux entreprises ?

Michaël Bazy. L'une des forces du partenariat entre Fortinet et SPIE ICS c'est notre engagement commun en faveur de l'éco-responsabilité et du Numérique Responsable. Notre objectif est d'optimiser l'utilisation de l'Intelligence Artificielle d'une façon à la fois durable, raisonnée et efficace, et de proposer à nos clients les meilleures solutions disponibles. Fortinet bénéficie d'une grande expertise en matière de cybersécurité, tandis que SPIE ICS est reconnue dans sa maîtrise des solutions Fortinet.

Bogdan Stefanescu. SPIE ICS est une Entreprise de Services Numériques française et souveraine. Ce partenariat s'inscrit dans une stratégie de développement de solutions technologiques communes et de services autour de la cybersécurité. Nous disposons du niveau de partenariat le plus haut avec Fortinet. Nos deux entreprises sont liées par des valeurs partagées sur le Numérique Responsable, que nous prenons en compte dès la conception même des infrastructures.