Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

L'intelligence artificielle au cœur des enjeux de cybersécurité

Synthèse des ateliers du Congrès annuel du CESIN, opportunités et défis

Paris, le 14 décembre 2023 — Les ateliers du CESIN consacrés à l'intégration de l'intelligence artificielle dans le domaine de la cybersécurité révèlent des opportunités et des défis auxquels font face les acteurs du secteur. La 11è édition du congrès sous la thématique de *« la cyberdéfense à la vitesse de l'IA »*, a rassemblé plus de 170 responsables de la cybersécurité, qui ont débattu autour de 8 thématiques* liées aux implications de l'IA.

Alors qu'un accord vient d'être validé autour de propositions destinées à constituer la base du futur règlement *AI Act* européen, les ateliers du CESIN ont offert un aperçu non-exhaustif des opportunités et défis inhérents à l'arrivée de l'IA dans le domaine de la cybersécurité. Cette approche collaborative essentielle permet aux membres du club d'anticiper les évolutions futures de la cybersécurité, afin d'orienter les organisations vers des pratiques plus sûres face à l'évolution des menaces.

Au cœur des discussions, l'automatisation des processus a émergé comme un thème central. Alors que le sujet de l'IA au service des attaquants a été traité lors des conférences du congrès, les participants aux ateliers ont souligné la capacité de l'IA à transformer la détection des incidents, la réponse aux menaces cyber, et l'évaluation des risques. Cette automatisation promet une amélioration significative de l'efficacité opérationnelle des équipes IT. Les opportunités identifiées sur cet axe comprennent la priorisation des actions de remédiation, la réduction des faux positifs, la détection d'anomalies, comme le repérage de comportements suspects, la fraude ou les vulnérabilités. Des inquiétudes subsistent néanmoins au plan de la consolidation des alertes et des coûts associés à certaines approches.

Malgré les perspectives prometteuses plusieurs challenges sont identifiés. L'IA, encore à un stade embryonnaire, soulève de nombreuses interrogations quant à son évolution et à son utilisation non régulée, avec le Shadow IA par exemple, ou sur l'opacité de la modélisation des scénarios. Par ailleurs, la question des données réellement exploitables est pointée du doigt ; avec l'idée émise de

développement d’un datalake dédié à la cybersécurité et l'implication de champions associés à divers experts pour favoriser l'exploitation efficace des données dans ce type de contexte.

D’autres questions se posent quant à sécuriser les projets qui se déploient au sein des entreprises, nécessitant un travail d’exploration de la part des responsables Cyber. **Mylène Jarossay, Présidente du CESIN**, précise *« Nous observons une déferlante de projets métiers s'appuyant sur l'IA et de nouvelles pratiques autour de l'IA générative. Les équipes cyber comptent bien également profiter de l'IA pour affûter leurs capacités de défense. Ce sont de grandes opportunités qui se dessinent dans les entreprises et les équipes cyber doivent très vite construire la gouvernance et le cadre technique nécessaires pour accompagner et sécuriser ces projets tout en s'emparant de cette évolution technologique pour leurs propres performances. »*

Les ateliers ont aussi mis en avant le rôle crucial des ressources humaines dans la gestion de l'impact de l'IA au sein des organisations. Avec des opportunités pour le staffing RH, comme la cartographie des cas d'usage, la définition de cadres de responsabilités, l'acquisition de compétences et d’expertises spécifiques. Ces actions clés viendront maximiser les avantages de cet avènement, tout en minimisant les risques.

Si on note une amélioration et un gain de temps significatif dans l'analyse des risques avec l’apport de l'IA, la majorité des participants voit un danger à utiliser l’IA pour construire leurs analyses de risques. Parmi les freins ils évoquent la fuite et l’exposition des données, la fiabilité des résultats, la perte d’expertises ou la perte de maîtrise du raisonnement, voire la capacité des humains à appréhender les résultats.

La confiance dans l'IA, en particulier dans le contexte des IA génératives, est une des grandes préoccupations. Des actions telles que l'éducation, l'audit, et la mise en œuvre de cadres et de normes émergentes sont ici encore recommandées pour renforcer la confiance et garantir la conformité.

In fine, bien que l'IA offre des opportunités considérables pour renforcer la cybersécurité, son adoption nécessite une approche stratégique. Les ateliers ont mis en lumière la nécessité d'une vigilance continue pour maximiser les avantages de l'IA, tout en minimisant les risques potentiels tels que la perte de contrôle. Outre les nouveaux besoins de compétences et le renforcement des expertises, parmi les préconisations, les participants appellent à la création d'un livrable sur les bonnes pratiques, l'établissement de chartes structurées et l’accompagnement d'une gouvernance solide.

***Les 8 thématiques des ateliers du Congrès du CESIN**

- IA & RH
  Quelle nouvelle démarche d'analyse de risques avec l'avènement de l'IA ?
  L'IA au service de la détection et de la réponse à incident
  Quelles données sont réellement exploitables aujourd'hui ?
  Quelle confiance dans l'IA ?
  Conformité dans un monde d'IA
  Risques versus bénéfices de l'IA
  Quelle organisation et encadrement des usages de l'IA dans l'entreprise ?

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité. Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.
Le CESIN compte plus de 900 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

www.cesin.fr