À Nancy,
Le 3 juin 2022

COMMUNIQUÉ DE PRESSE

Cybersécurité

L'intelligence artificielle pour anticiper les cyberattaques : lancement de la startup Cybi

L'équipe de Cybi :
Abdelkader Lahmadi, Frédéric Beck, Jérôme François, Régis Lhoste, Fabian Osmond.
Crédit : service communication Loria
Télécharger

Liens utiles :

Site web
https://www.cybi.fr

Twitter
https://twitter.com/CYBI_CYBER
(@cybi_cyber)

LinkedIn
https://www.linkedin.com/company/cybi/

Systèmes d'information, objets connectés, systèmes industriels… ces environnements font face à des attaques informatiques de plus en plus fréquentes et sophistiquées. Les entreprises sont des cibles privilégiées pour les hackers et doivent se protéger de cette menace grandissante. Fruit de l'expertise en cybersécurité de l'équipe RESIST du laboratoire Loria (CNRS, Inria, Université de Lorraine), la startup Cybi propose des solutions d'analyse des chemins d'attaque informatiques et d'automatisation intelligente des opérations de cybersécurité. Soutenue par l'Incubateur Lorrain et la région Grand Est, la startup portée par Inria et l'Université de Lorraine vient de voir le jour à Nancy.

Une technologie de pointe : Scuba
La majorité des solutions de cybersécurité analysent les vulnérabilités individuelles des systèmes informatiques. Or, les hackers opèrent de plus en plus en chemins d'attaque, en utilisant non seulement des vulnérabilités critiques, mais aussi d'autres failles comme portes d'entrée pour pénétrer le réseau informatique et infecter tout le système. Un objet connecté (prise connectée, box internet, automate industriel…), avec un bon score de sécurité individuel peut ainsi devenir un point de passage dans un chemin d'attaque pour atteindre une cible critique lorsqu'il est mis en réseau avec d'autres objets.

Cette technologie de rupture développée par l'équipe de chercheurs et ingénieurs de Cybi a été brevetée en 2020. Elle s'appuie sur des modèles et algorithmes d'intelligence artificielle pour analyser l'intégralité des chemins d'attaque présents sur un réseau et prioriser les vulnérabilités à corriger, en réduisant les risques et les temps de réponse aux incidents.

Détecter et prioriser les vulnérabilités grâce à l'intelligence artificielle
Scuba s'appuie sur des corpus de vulnérabilités : lorsqu'une faille est découverte, lors d'opération de *pentesting* (méthodes d'évaluation de la sécurité d'un système), ou de *bug bounty* (programme de récompense pour des chasses au bug), les constructeurs doivent publier un correctif en libre accès : ces informations sont notamment disponibles dans les bases de données CVE (*common vulnerabilities exposure*).

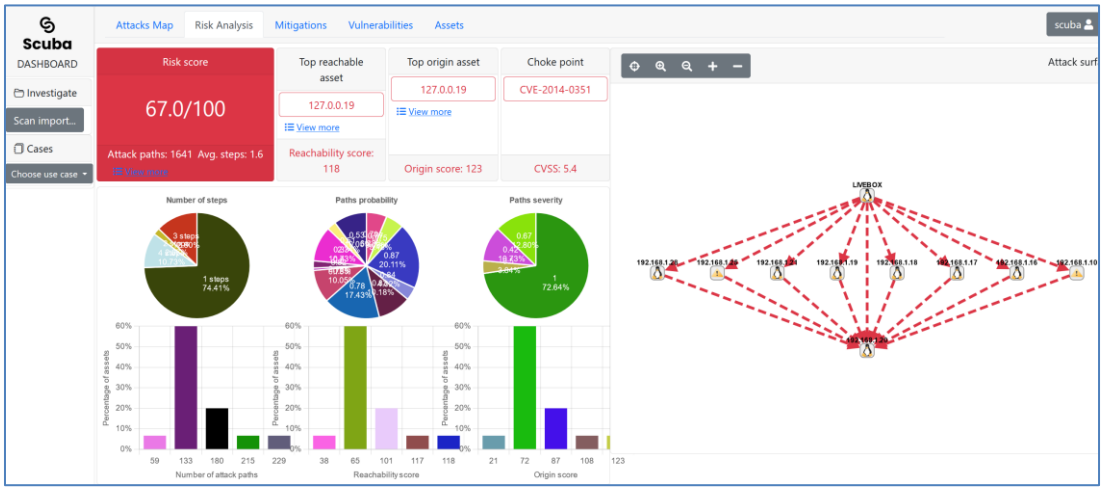
« *Notre outil est capable de lire et comprendre aisément ces grandes quantités de texte grâce à des méthodes de traitement automatique des langues et d'intelligence artificielle. Il peut ainsi analyser de manière automatique les rapports de vulnérabilité et détecter des chaînes d'attaque potentielles*, expliquent les chercheurs. *Nous travaillons également sur une plateforme de test dédiée à l'étude des vulnérabilités des objets connectés, afin d'évaluer les niveaux de sécurité des produits.* »

L'équipe a d'ailleurs récemment testé sa technologie sur des virus bien connus comme Pegasus et Puzzle-maker et a pu identifier leurs chemins d'attaque.

Cybi, une alliée incontournable pour la sécurité des entreprises
La start-up s'ouvre aujourd'hui aux experts de la cybersécurité, aux grandes entreprises et plus particulièrement aux SOC (*Security Operation Centers*), dont la mission est de garantir la sécurité de l'information. Scuba apparaît comme une brique essentielle à la chaîne de sécurisation des systèmes.

« *Grâce à nos solutions d'analyse des vulnérabilités et des chaînes de vulnérabilités, Cybi offre un véritable outil d'aide à la décision, une analyse du risque réel et des recommandations personnalisées pour mettre en place les meilleures techniques pour corriger les failles* », précise Régis Lhoste, président de la startup.

« *L'expertise et la maturité en cybersécurité de l'équipe positionnent Cybi comme startup innovante et visionnaire. Notre solution Scuba arrive au bon moment sur le marché de la cybersécurité. En effet, Scuba offre des fonctionnalités avancées très demandées et trop peu adressées jusqu'alors pour répondre aux menaces de cyberattaques qui se multiplient chaque jour. Nos différents échanges avec les principaux acteurs de la cybersécurité française sont très positifs. Scuba est LA solution attendue par toutes les structures quels que soient leur profil ou leur taille*. », précise Fabian Osmond, directeur général de la startup.



La plateforme Scuba | Télécharger | Crédit : Cybi

CONTACT PRESSE
Fanny Lienhardt
Chargée de relations presse
06 75 04 85 65

UNIVERSITÉ DE LORRAINE
34, Cours Léopold - BP 25233
54052 NANCY Cedex
Tél. : 03 72 74 00 00
communication@univ-lorraine.fr
www.univ-lorraine.fr

L'Université de Lorraine est un établissement public d'enseignement supérieur composé de 10 pôles scientifiques rassemblant 60 laboratoires et de 9 collégiums réunissant 43 composantes de formation dont 11 écoles d'ingénieurs. Elle compte 7 000 personnels et accueille 62 000 étudiants. Retrouvez toute l'actu de l'université sur factuel.univ-lorraine.fr et sur le média The Conversation France. Les chiffres-clés 2021 | Le rapport d'activité 2020-2021 | Plaquettes & magazines | Salle de presse.

Le Loria, Laboratoire lorrain de recherche en informatique et ses applications est un laboratoire commun à plusieurs établissements : le CNRS, l'Université de Lorraine et Inria. Depuis sa création en 1997, le Loria a pour mission la recherche fondamentale et appliquée en sciences informatiques. Ses travaux scientifiques sont menés au sein de 29 équipes structurées en 5 départements, dont 15 sont communes avec Inria, représentant un total de plus de 400 personnes. Le Loria est un des plus grands laboratoires de la région lorraine.
www.loria.fr