Bug Bounty, IA…Les tendances Cyber à retenir de la DEF CON, le plus grand rassemblement Cyber au Monde

30 000 hackers réunis au même endroit, au même moment. Récapitulatif de la DEF CON 2024 proposé par Axel Dreyfus, co-fondateur de l'École 2600 et Charlie Bromberg, Responsable Service Line Pentest Capgemini France.

Temps de lecture : minute

13 août 2024

30 000 hackers réunis au même endroit, au même moment. Depuis sa création en 1993 par Jeff Moss, alias "Dark Tangent", la DEF CON est devenue le plus grand rassemblement mondial de hackers. Dès 1997, Moss fonde également la Black Hat, un événement dédié aux entreprises et professionnels du secteur. Ces deux conférences sont aujourd'hui des rendez-vous incontournables.

Cette année, la Black Hat et la DEF CON ont réuni plus de 50 000 hackers et professionnels. Ces chiffres font de ces événements les plus importantes manifestations mondiales dans le domaine de la cybersécurité, un événement incontournable pour l'École 2600 et la communauté de cyber française.

Bug Bounty, IA, hardware, les tendances transatlantiques à retenir

Ces événements sont des occasions précieuses pour identifier les

tendances en cybersécurité émergentes et évaluer leur impact potentiel en France et en Europe.

Le Bug Bounty, le principe d’obtenir une récompense pour la découverte de bugs logiciels, connaît par exemple une popularité croissante depuis quelques années et n'est plus une simple mode. Pour preuve, La DEF CON a consacré pour la première fois un village entier à cette pratique, témoignant de son adoption généralisée dans l'industrie américaine.

L'édition de cette année s'est distinguée par l'émergence forte de solutions dopées à l'IA, pour le meilleur comme pour le pire. Le vaste village "AI x CC", sponsorisé par la DARPA (Defense Advanced Research Projects Agency) et l'ARPA-H (The Advanced Research Projects Agency for Health), ou le challenge à 29 millions de dollars de cash prize, témoigne de la place croissante de l'IA dans le paysage cyber.

Les solutions consacrées au "hardware" ont également retenu l'attention, notamment dans les secteurs de l'automobile, des équipements industriels, de l'embarqué, du médical et des *smart cities*. Ces développements témoignent de l’omniprésence du numérique dans tous les aspects de notre vie, rendant la sécurité non seulement plus complexe, mais aussi plus cruciale que jamais. La gestion de l'eau et de l'énergie est devenue vitale, ne laissant d'autre choix que de relever ces défis.

Investissements massifs et pragmatisme, la recette américaine

Sur le plan financier, les acteurs publics et privés américains sont déterminés, comme en témoignent leurs récentes acquisitions de startups françaises. Des entreprises comme Alsid, Sqreen, Datadog, Atempo, Qosmos, Sentryo, SynerTrade, et plus récemment Ping Castle, spécialiste de la sécurité Active Directory racheté par Netwrix, sont désormais sous

pavillon américain.

La question de la souveraineté cyber, qui occupe une place centrale dans le débat français ne peut se concevoir qu'en prenant en compte tous les acteurs de l'écosystème : la rémunération des talents, le retour sur investissement pour les actionnaires, les entrepreneurs et les collaborateurs.

En France, notre approche romantique de la souveraineté, c'est-à-dire de la défendre sans réellement s'en donner les moyens, nous handicape face à des puissances plus pragmatiques.

Les États-Unis quant à eux, n'hésitent pas à investir massivement, à inciter et à contrôler. Ils réussissent à attirer les talents et la valeur, renforçant ainsi leur pouvoir régalien et leur poids économique. La question se pose donc : dans quelle mesure pouvons-nous nous inspirer de cette approche ?

À lire aussi
Cybersécurité : un startup studio lancé au Campus Cyber pour propulser 10 pépites européennes en 5 ans

MADDYNEWS

La newsletter qu'il vous faut pour ne rien rater de l'actualité des startups françaises !

JE M’INSCRIS

Article écrit par Charlie Bromberg et Axel Dreyfus