

## Hacker éthique et cybersécurité Opportunités et défis



### Hackers éthiques et cybersécurité

Organisateurs



Pr Ahmed Mehaoua



Par webinaire Zoom

Lundi 16 juin  
18h00 - 20h00



White hats en Bretagne



Myriam QUEMENER



Yassir KAZAR



Béatrice Laurent



Gérard Peliks

### Hackers éthiques et cybersécurité, conditions juridiques et déontologiques

Voilà une question de sémantique : Dans l'esprit de beaucoup d'internautes, un hacker est un méchant pirate qui attaque les Systèmes d'Information qu'il trouve sur Internet pour en retirer de l'argent ou porter atteinte à l'image d'individus ou d'organisations. On le représente cagoulé, penché méchamment sur son clavier, en train de ricaner en pensant à son mauvais coup imminent.

Mais un tel individu n'est pas **un hacker**, c'est **un cracker**. Un hacker est un passionné de codage dans divers langages informatiques. Il essaie de comprendre à quoi sert tel programme. Son but n'est pas de nuire, comme le cracker, mais d'aider au combat contre la cybercriminalité. C'est un « **white hat** », voir l'image du visuel en bas à gauche (en effet, la Bretagne est un territoire en pointe dans la cybersécurité). Les crackers sont des « **black hats** ». Pour lever l'ambiguïté, quand le but d'un hacker est très avouable, on ajoute à hacker le qualificatif « **éthique** ». Et voilà notre hacker réhabilité dans son rôle de défenseur.

Et dans quel but un hacker analyse t'il le code d'une application ? Souvent il fait ça sous contrat avec un organisme qui propose son travail de recherche de failles à une entreprise qui développe des applications. En effet, un œil extérieur est souvent plus performant pour détecter des failles involontaires laissées par les

développeurs dans une application que ceux qui la développent. C'est le domaine des chasseurs de faille, le **Bug Bounty**.

Le travail d'un hacker, ajoutons-lui le mot éthique, est-il bien légal ? Si on constate que la porte d'une maison est ouverte, a-t-on le droit d'y entrer pour voir ce qu'elle contient ? Je pense que non, à moins d'y être invité. Mais si les volets des fenêtres sont ouverts, en passant dans la rue devant cette maison, a-t-on le droit de jeter un coup d'œil à l'intérieur ? Sans doute un coup d'œil furtif et curieux, oui, mais pas de rester regarder avec insistance. Il y a là des problèmes juridiques et le droit sera abordé dans notre « Lundi de la Cybersécurité » par Myriam QUEMENER. Il y a aussi des problèmes techniques et contractuels, et cet aspect sera abordé par Yassir KAZAR.

Un chasseur de faille est-il une canaille ? Non s'il fait le travail pour renseigner les développeurs sur les failles qui résident dans les applications qu'ils développent. Le travail du chasseur de faille doit se faire donc sous contrat et être bien évidemment soumis à une discrétion totale. C'est un des points qui seront abordés dans notre évènement du lundi 16 juin.

Hackers éthiques, chercheurs de failles dans les aspects techniques et juridiques, seront les thèmes du Lundi de la Cybersécurité du mois de juin. Les hackers éthiques ont désormais une place de choix à prendre en matière de cybersécurité sous certaines conditions juridiques et déontologiques qui vous seront présentées.

## Je donne la plume à Myriam QUEMENER



Associer Hacking et cybersécurité peut sembler à priori quelque peu incompatible.

Il n'en est rien c'est tout le sens de ma démarche et de celle d'Amélie Kock dans notre dernier ouvrage.

Au niveau de la protection des systèmes d'information des organisations, des entreprises et des collectivités territoriales. Les hackers éthiques agissent pour faire face aux risques toujours croissants de cyberattaques.

Ils ont désormais une place de choix à prendre en matière de cybersécurité à certaines conditions juridiques et déontologiques qui vous seront présentées.

## Je donne la plume à Yassir Kazar

Derrière le terme Bug Bounty tout droit venu des États-Unis, se cache une approche de la détection des failles de sécurité informatique : rémunérer une foule de spécialiste en recherche de failles pour les failles détectés.

Sommes-nous à l'aube de l'ubérisation de l'infosec ? Est-ce juste un autre buzzword de plus qui fera son temps et sera aux oubliettes ? Va-t-il réellement remplacer les tests d'intrusions tels que nous les connaissons ? A quoi faut-il s'attendre en termes de ROI du côté des entreprises ? Jusqu'à quel point le Bug Bounty va modifier l'approche de la sécurité dans les entreprises ? Comment une telle approche peut s'intégrer dans les processus des équipes informatique opérationnelles ? A quoi ressemble les communautés derrière les différentes plateformes qui existent ? à quoi faut-il s'attendre en termes de rémunération du côté des Hackers ?



Voici quelques-unes des questions et bien d'autres auxquelles nous allons essayer de répondre sans engouement excessif ni dénigrement gratuit de cette activité naissante, afin de donner à tout à l'auditoire les clés nécessaires pour bien appréhender le Bug Bounty."

## Qui est Myriam QUEMENER ?

**Myriam QUEMENER** est Magistrat honoraire, ancienne avocate générale à la cour d'appel de Paris, Docteur en droit.



Elle est l'autrice de plusieurs ouvrages sur la cybercriminalité et la cybersécurité, dont Hacker « éthique » et cybersécurité, opportunités et défis, écrit avec Amélie Köcke, et sorti le 26 novembre 2024.

Voilà comment l'ARCSI a présenté Myriam QUEMENER qui est intervenue aux 16<sup>e</sup> Rencontres :

« Le CyberCercle sera représenté dans la 3<sup>e</sup> table-ronde par l'un de ses « seniors advisors » les plus renommés, **Myriam QUEMENER**, magistrate judiciaire honoraire, docteur en droit. Myriam QUEMENER est une experte reconnue en matière de lutte contre la cybercriminalité et du droit du numérique, régulièrement auditionnée par les instances officielles (notamment le Parlement ou l'ANSSI). Myriam QUEMENER a précédemment occupé des fonctions de direction tant à la Chancellerie qu'en juridiction et a été administrateur général au ministère de l'Intérieur dans un service consacré à la lutte contre la cybercriminalité. Elle a été avocat général près la Cour d'Appel de Paris (délinquance financière, cyber et organisée) et en 2024 directrice de programme et DPO à l'Agence du Numérique en Santé (ANS) ».

## Qui est Yassir KAZAR ?

Yassir KAZAR est serial entrepreneur, PDG de la plateforme française de Bug Bounty YOGOSHA.

Il est enseignant en sécurité offensive et membre de l'ARCSI.

## **Demande d'inscription au lundi 16 juin, par visio-conférence à partir de 18 h 00.**



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien vers la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à Béatrice Laurent co-organisatrice de nos événements :

[beatricelaurent.CDE@gmail.com](mailto:beatricelaurent.CDE@gmail.com)

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux

intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail ([gerard.peliks@noos.fr](mailto:gerard.peliks@noos.fr)).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 16 juin, dès 18 h 00**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. C'est toujours un agréable moment avant 18 h 00.

## Quelques minutes avec Jérôme NOTIN

Suivant la tradition de nos « *Lundi de la cybersécurité* », entre l'exposé des intervenants et la session questions / réponses, autour de 19 h 15, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Cette séquence du « *Lundi de la Cybersécurité* » de juin sera animée par **Jérôme NOTIN**.



Après un début de carrière dans des entreprises privées liées à la cyber sécurité et au logiciel libre, Jérôme Notin rejoint l'ANSSI en 2016 comme préfigurateur du dispositif d'assistance aux victimes d'actes de cyber malveillance. A la création du Groupement d'Intérêt Public ACYMA, dispositif national d'assistance aux victimes ([cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr)) il en est nommé le directeur général.



Il nous présentera le **service 17Cyber** proposé par la Police Nationale, la Gendarmerie Nationale et [Cybermalveillance.gouv.fr](http://Cybermalveillance.gouv.fr).

## Le coin des « *Lundi de la cybersécurité* » précédents.

Vous trouverez, sur le web de l'ARCSI en [https://www.arcsi.fr/evt\\_passes.php](https://www.arcsi.fr/evt_passes.php) tous les détails, slides, parfois aussi les enregistrements et des comptes rendus écrits par Clarisse Véron, élève du master2 « *Cybersécurité et e-Santé* » de l'Université Paris Cité.

Mais attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos futurs lundis. Donc il est conseillé d'être connectés pour les suivre par Zoom.

## Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ? Prompt posé à Gemini (l'IA Générative de Google) :

## Les hackers éthiques sont-ils compatibles avec les règles de la cybersécurité ?

Absolument ! Les hackers éthiques sont non seulement compatibles avec les règles de la cybersécurité, mais ils en sont un pilier essentiel. Loin d'être des acteurs malveillants, ils utilisent leurs compétences techniques pour identifier et corriger les vulnérabilités des systèmes informatiques, des réseaux et des applications, précisément dans le but de renforcer la sécurité.

Voici quelques points qui illustrent cette compatibilité :

- Objectif commun : la sécurité. L'objectif principal des hackers éthiques est d'améliorer la sécurité en découvrant les failles avant que des acteurs malintentionnés ne puissent les exploiter. C'est exactement l'objectif de la cybersécurité.
- Respect des cadres légaux et éthiques. Contrairement aux cybercriminels, les hackers éthiques opèrent dans un cadre légal et éthique strict. Ils obtiennent toujours une autorisation avant de réaliser des tests d'intrusion et suivent des règles de conduite claires pour s'assurer de ne pas causer de dommages.
- Identification proactive des vulnérabilités. Les hackers éthiques simulent des attaques pour identifier les points faibles des systèmes. Cette approche proactive permet aux organisations de prendre des mesures correctives avant qu'une véritable attaque ne se produise, ce qui est un aspect fondamental de la cybersécurité préventive.
- Contribution à l'amélioration continue. Les rapports des hackers éthiques fournissent des informations précieuses sur les vulnérabilités découvertes et les recommandations pour les corriger. Ces informations sont cruciales pour améliorer en continu les mesures de sécurité et adapter les stratégies de cybersécurité aux menaces émergentes.
- Complémentarité avec les mesures de sécurité traditionnelles. Le travail des hackers éthiques complète les mesures de sécurité traditionnelles telles que les pare-feux, les antivirus et les systèmes de détection d'intrusion. Ils apportent une perspective "offensive" qui permet de tester l'efficacité des défenses existantes sous un angle différent.

En résumé, les hackers éthiques sont des alliés précieux dans le domaine de la cybersécurité. Leur expertise et leur approche proactive sont indispensables pour identifier les failles de sécurité et renforcer la résilience des systèmes face aux menaces cybernétiques. Ils agissent dans le respect des règles et contribuent activement à un environnement numérique plus sûr.