De la rondache au pavois : le rôle de la CTI dans l'optimisation de la défense des organisations

La rondache est un petit bouclier léger, idéal pour la parade rapprochée d'un défenseur. En cybersécurité, nous pouvons voir les rondaches comme une métaphore des briques de base de la cybersécurité, tels que les firewalls basiques et les antivirus traditionnels. Mais avec la sophistication, la prolifération et la violence des menaces actuelles, les rondaches ne suffisent plus à protéger les défenseurs. **Le pavois** est une évolution de la rondache. C'est un grand bouclier protecteur qui couvre tout le corps, et qui porté par de multiples défenseurs constitue une ligne de défense collective qui peut résister aux assauts, et aux nuées de flèches. En cybersécurité, nous pouvons voir les pavois comme une métaphore des édifices de cybersécurité, tels, entre autres, que le plan de continuité et de reprises d'activités, la gestion de crises, la gestion des identités, le SOC, le SIEM, le DLP, l'EDR, le XDR, le Zero Trust et bien sûr et surtout la veille sur les cybermenaces.

C'est pour constituer des pavois numériques qu'intervient la **Cyber Threat Intelligence (CTI)**, ou Renseignement sur les Menaces Cyber, CTI couplée à l'OSINT (Open Source Intelligence), source de renseignements librement accessibles sur Internet.

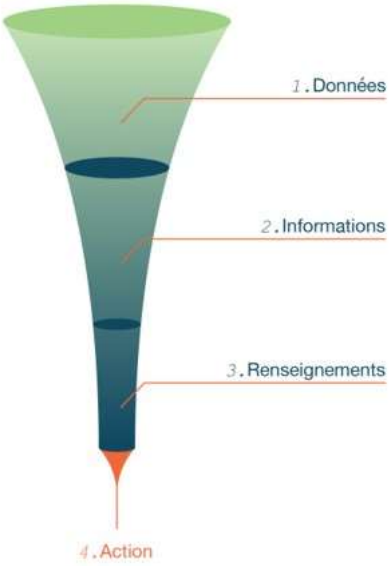
La CTI joue un rôle crucial et transversal dans la cybersécurité moderne. Dans ce « Lundi de la Cybersécurité du mois de novembre, un expert du sujet nous conduira de la e-rondache ou protection simple des données, mais aujourd'hui peu efficace, au e-

pavois, renseignement issu d'un ensemble de données rentrées dans leur contexte. Ce qui comme les pavois qui servaient à dresser un mur de défense solide contre les flèches et les assauts de l'ennemi, constitue une information exploitable pour assurer la protection des systèmes d'Information et des données.

La CTI diminue le risque cyber en connaissant avant une attaque, à quoi on peut s'attendre, comment la parer efficacement et que faire après pour assurer la résilience des systèmes et des données.

Je donne la plume à François STRICHER

Le renseignement cyber circule-t-il vraiment dans nos organisations ?



Du fracas des épées sur la rondache des condottieri à l'ombre monumentale du pavois des fantassins bourguignons, le bouclier n'a jamais cessé d'évoluer pour répondre à l'ingéniosité de l'adversaire. Face à une cybermenace qui s'industrialise, le renseignement sur les menaces d'origine cyber, la CTI, promet d'adapter la forme et la taille du nôtre.

Pourtant, nous n'avons jamais autant collecté d'indicateurs, de flux et de rapports… mais accumuler n'est pas partager, et partager n'est pas agir. Quelle CTI nos organisations consomment-elles réellement ? Le renseignement circule-t-il entre les équipes de sécurité et la direction, ou reste-t-il prisonnier des outils qui l'ingèrent ? Et le terrain renvoie-t-il ce qu'il apprend au contact de l'adversaire ?

C'est à ces questions que j'ai tenté de répondre dans ma thèse de MBA Management de la Cybersécurité. Je vous présenterai ce que j'y ai découvert, ce qui freine cette circulation, et une piste pour que le renseignement devienne enfin Utile, Utilisable… et Utilisé.

Mais je ne veux pas faire cette présentation seul. Au fil de l'exposé, je vous poserai les questions posées à mes interlocuteurs : partage, confiance, moyens… Plus d'un an est passé, une éternité au rythme de la menace : vos expériences viendront éprouver les conclusions d'alors. Tiennent-elles toujours ? Venez avec vos certitudes… et surtout

avec vos doutes !

Petite note du co-organisateur des « Lundi de la Cybersécurité » :

J'ai été, comme chaque année, dans le jury de la soutenance de quelques thèses professionnelles qui marquaient l'achèvement des MBA Management de la Cybersécurité, année 2024-2025 de DeVinci Executive Education (Nanterre).

Parmi les excellents travaux des élèves, l'un d'eux m'avait particulièrement impressionné, tant par son contenu que par la manière de le présenter. Il s'agit de François Stricher et je me suis dit : « celui-là, il faut que je le fasse intervenir dans un Lundi de la Cybersécurité pour que les inscrits en profitent aussi. ». C'est pour le Lundi de novembre 2026.

Gérard Peliks

Qui est François STRICHER ?

Docteur en biochimie, François Stricher a d'abord consacré une vingtaine d'années à l'ingénierie de protéines, notamment en développant des logiciels de modélisation moléculaire, avant de diriger des équipes de R&D, de l'EMBL au CRG jusqu'à l'industrie des biotechnologies.

Reconverti en 2024 dans la cybersécurité et diplômé du MBA Management de la Cybersécurité, il est aujourd'hui responsable des investigations au sein d'un grand organisme public (CTI, SOC, gestion de crise cyber). Il y applique une conviction de chercheur : face à la menace, on ne progresse qu'en partageantSuivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses qui commence autour de 19 h 30, nous donnons pour une quinzaine de minutes la parole à une organisation (association ou agence) qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Quelques minutes avec une association/agence :

l'Agence Nationale des FRéquences, l'ANFR

La séquence des **quelques minutes avec une association/agence,** sera animée par **Catherine Gabay**, Directrice adjointe du Contrôle du Spectre de l'**ANFR, A**gence **N**ationale des **FR**équences**.**

Les brouillages sont une menace cyber à part entière, notamment en cyber OT. Les attaques sur les fréquences peuvent causer de grosses perturbations.

Catherine Gabay nous parlera des actions curatives de l'ANFR sur le terrain, et de ses actions préventives dont des actions pédagogiques. L'ANFR propose des conseils, des contre-mesures, voire des interventions pour diminuer ce risque.

Demande d'inscription au lundi 16 novembre, 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 pour entrer dans la visioconférence Zoom.

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

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront donc connus des organisateurs et seront 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).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 16 novembre dès 18 h 00 ou mieux, un peu avant**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. Ce sont toujours d'agréables échanges qui se font avant 18 h 00.

Lorsque l'organisateur des « *Lundi de la Cybersécurité* » montre du doigt le mail qu'il a envoyé pour le prochain Lundi, l'imbécile regarde le doigt.

Les autres lisent attentivement le contenu du mail, en comprennent l'intérêt, et demandent leur inscription 😉

Les demandes d'inscriptions sont à adresser à Béatrice Laurent :
beatricelaurent.CDE@gmail.com

Gérard