Lettre des "Lundi de la cybersécurité" n° 92

Organisation d'une Purple Team

Optimisation des tests d'intrusion
et mise en place de plans de remédiation

Sabine Pirou, notre intervenante au Lundi de la Cybersécurité du mois de mai, a soutenu sa thèse professionnelle, qui marquait la fin de son MBA « Management de la Cybersécurité » de De Vinci Executive Education (Institut Léonard De Vinci), en novembre 2025.

Elle a brillamment traité son sujet *:* ***Organisation d'une Purple Team - optimisation des tests d'intrusion et mise en place de plans de remédiation***, tant sur le contenu que sur la manière de le présenter. J'étais dans le jury et j'ai été séduit. Je lui ai mis la note exceptionnelle de 19/20 en me disant : « *Celle-là* je vais l'inviter à animer un Lundi de la Cybersécurité sur ce sujet d'actualité de la cybersécurité, ce sera un beau cadeau fait à celles et à ceux qui seront connectés le 18 mai à 18 h 00 ».

Au menu de sa thèse professionnelle : comment organiser un test, les méthodologies qui intègrent la Purple Team, les concepts proches du test d'intrusion à ne pas confondre, et donc comment pousser le concept de Purple Team au-delà des méthodologies existantes.

Les attaquants, dans l'agression simulée, avec leurs tentatives d'intrusions, d'infections, de vols de données, font partie de la **Red Team**, les défenseurs, avec le SOC, le SIEM et autres outils indispensables sont dans la **Blue Team**. Et pour ne rien perdre des évènements, une **Purple Team** observe tout ce qui se passe avant, pendant et après l'attaque pour en tirer les enseignements qui permettront de diminuer le risque cyber auquel toute organisation peut être confrontée.

L'idée est que chaque organisation se prépare à subir la prochaine cyberattaque en évitant l'effet de sidération quand elle survient, et à se préparer en conséquence.

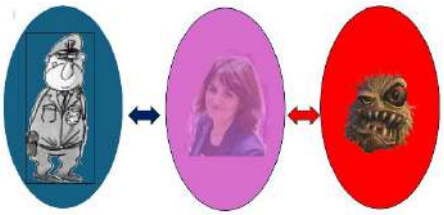
Je donne la plume à Sabine Pirou

Dans un monde de plus en plus exposé au risque de cyberattaque, le test d'intrusion est devenu un outil pour évaluer la cybersécurité d'une organisation. Son principe est de simuler une cyberattaque sur un périmètre et une période définie. Pour améliorer son efficacité, le concept de Purple Team a été développé pour aider la Red Team qui simule l'attaque et la Blue Team qui doit défendre l'organisation, à travailler de concert.

Mais son adoption est encore timide et les méthodologies développées par les professionnels sont incomplètes. Pourtant la Purple Team est un levier puissant pour améliorer l'efficacité d'un test d'intrusion.

Lors de cette présentation, nous développerons le fonctionnement d'un test d'intrusion classique : sa définition, les acteurs, son déroulement, et les autres concepts proches. Puis nous détaillerons les apports de la méthodologie de la Purple Team dans le cadre d'un test : sa définition, les détails de la méthodologie et comment aller plus loin, les avantages apportés pour vos clients, les avantages apportés pour vos équipes, ainsi que les pièges à éviter. Nous terminerons cette présentation sur la Purple Team et son apport dans le cadre des réglementations NIS 2 et DORA.

Qui est Sabine PIROU ?



Sabine Pirou est Offensive Security Coordinator au sein d'un VOC d'un grand groupe industriel, après 20 ans d'expérience dans le secteur bancaire. Son expertise consiste à coordonner, planifier des tests d'intrusion, et à en garantir le succès, via des méthodologies collaboratives innovantes.

Elle travaille également sur des projets de sensibilisation cyber et travaille sur le statut du hacker éthique.

Titulaire d'un MBA en cybersécurité, elle a eu l'opportunité de travailler sur le concept de Purple Team dans un contexte universitaire, et à déployer ensuite cette méthodologie sur le terrain. Elle est également membre du CEFCYS : CErcle des Femmes de la CYberSécurité.

Demande d'inscription au lundi 18 mai, 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 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).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 18 mai, 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.

Quelques minutes avec une association :

Suivant 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 donnerons 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 de quelques minutes avec une association sera animée par **Paul Richy** de la Commission de Normalisation Cybersécurité de l'AFNOR, et membre de l'ARCSI.

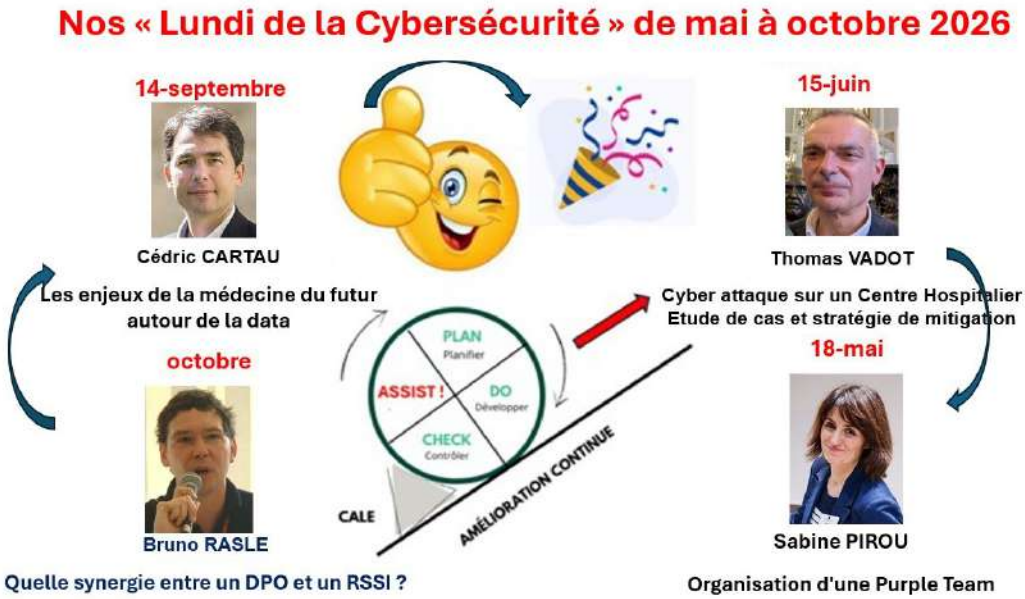
Paul Richy nous présentera l'ISO et ses travaux de normalisation en sécurité des systèmes d'information, notamment les normes 27001, 27002 et 27005, en rappelant les échelons mondiaux, européens et français. Il fera aussi un lien avec les travaux du Sous-Comité 42 du JTC 1 de l'ISO (Intelligence Artificielle et Big Data) et ceux du Comité Technique TC 292 (continuité et résilience).

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez, sur le web de l'ARCSI – Association des Réservistes du Chiffre et de la Sécurité de l'Information :
https://www.arcsi.fr/evt_passes.php

Tous les détails, slides, parfois aussi les enregistrements et des comptes rendus de nos « Lundi ».

Le coin des « Lundi de la cybersécurité » suivants.



Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?

Prompt envoyé à Gemini : **A quoi sert une Purple Team ?**

Réponse de Gemini :

Une Purple Team (équipe violette) sert à faire collaborer les Red Teams et les Blue Teams afin d'améliorer en continu la sécurité d'une organisation.

Voici comment cela fonctionne :

- Red Team : simule les attaques réelles d'un adversaire (test d'intrusion, exploitation de failles, ingénierie sociale, etc.) pour évaluer la défense.
- Blue Team : défend l'organisation (surveillance, détection, réponse aux incidents, durcissement des systèmes).
- Purple Team : agit comme un pont entre les deux, pour transformer les enseignements des attaques simulées en améliorations concrètes des défenses.

Objectifs principaux d'une Purple Team :

1. Améliorer la détection et la réponse : chaque attaque (Red) est observée avec la Blue Team pour voir si elle est détectée et comment réagir mieux.
2. Partager les connaissances : la Red Team explique ses tactiques, techniques et procédures (TTPs) à la Blue Team, qui apprend à reconnaître ces signes d'attaque.
3. Optimiser les outils et les processus : ajuster les SIEM, alertes, règles de corrélation, playbooks, etc.
4. Renforcer la culture sécurité : créer une boucle d'apprentissage continue entre offensive et défensive.

En résumé, une Purple Team ne remplace pas les Red ou Blue Teams, mais les coordonne pour que chaque exercice d'attaque serve à renforcer la défense, plutôt que d'être un simple audit ponctuel.

Inscrivez-vous (mail à beatricelaurent.cde@gmail.com) ou cliquez ici :

JE M'INSCRIS

Gérard