ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte rendu du Lundi de la cybersécurité du 18 mai 2026

Organisation d'une purple team : optimisation des tests d'intrusions et mise en place de plans de remédiation

Présenté par Sabine PIROU

Organisé par Pr. Gérard Peliks, Béatrice Laurent et Pr. Ahmed Mehaoua
Rédigé par Rayan Al Mohaize, étudiant en Master 2 Cybersécurité

Table des matières

I Introduction

L'événement « Lundi de la Cybersécurité » est une série mensuelle de conférences en ligne organisée de manière indépendante par Gérard Peliks et Béatrice Laurent. Elle a pour vocation d'explorer chaque mois une thématique différente liée aux enjeux contemporains de la sécurité numérique et de la société.

1 Le thème de la Purple Team

Le Lundi de la cybersécurité du 18 mai 2026 portait sur la Purple Team. Lors de ce webinaire, Sabine PIROU nous a présenté comment s'organise une Purple Team et en quoi elle peut apporter une plus-value dans les activités de pentest et de remédiation aux vulnérabilités. Cette présentation s'accompagne d'exemples concrets et de l'expérience de Sabine PIROU pour enrichir la compréhension des enjeux de la Purple Team.

2 Les intervenants

Pour animer ce Lundi de la cybersécurité, **Sabine PIROU** nous a fait l'honneur de partager avec nous ses connaissances et son expérience pour nous présenter l'organisation d'une purple team et comment optimiser un pentest et un plan de remédiation. Sabine PIROU est Offensive Security Coordinator au sein d'un VOC dans 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.

Par la suite, **Paul RICHY**, membre de la Commission de Normalisation Cybersécurité de l'AFNOR et membre de l'ARCSI, a animé le quart d'heure des associations pour présenter l'AFNOR ainsi que ses travaux de normalisation en sécurité des systèmes d'information, notamment dans le cadre des normes 27001, 27002 et 27005, en rappelant les échelons mondiaux, européens et français.

II La Purple Team (Par Sabine PIROU)

1 Présentation d'un test d'intrusion "classique"

Tout d'abord, Sabine PIROU nous présente ce qu'est un test d'intrusion "classique", c'est-à-dire sans purple team.

Un test d'intrusion permet de reproduire une fausse cyberattaque, réalisée par des pentesters ou hackers éthiques. L'objectif est d'évaluer la solidité d'un SI, d'identifier les vulnérabilités, de proposer des correctifs et des remédiations, et de sensibiliser les détenteurs du SI testé. Dans ce contexte, le test d'intrusion réunit plusieurs acteurs que l'on peut distinguer en 2 groupes :

- **La Red Team :** Le côté offenssif
- **La Blue Team :** Le côté défensif

Le pentest se fait en plusieurs phases et la première est le cadrage. Cette phase est obligatoire et constitue la plus importante de l'ensemble du processus. Elle s'organise

sous forme de meeting avec le client pour présenter les équipes, expliquer les objectifs, comprendre le contexte, le domaine d'activité, les besoins et les antécédents cyber de l'entreprise cliente, et enfin définir le périmètre de test. Ce cadrage est assuré par plusieurs acteurs :

- Le commanditaire du pentest,
- Un membre de la sécurité informatique chez le client,
- Un membre connaissant l'environnement ou l'application testée
- Un membre représentant les utilisateurs de l'environnement ou de l'application pentestée,
- Un membre représentant la Red Team.

Ce cadrage permet également de comprendre en profondeur le SI, d'en définir la criticité et d'en définir les méthodes d'identification et l'organisation des droits d'accès entre les différents utilisateurs. Enfin, ce cadrage va permettre de mettre en place un planning pour éviter de perturber l'activité de l'entreprise. Par exemple, dans le luxe, le pentest ne sera pas fait pendant la Fashion Week car l'entreprise ne peut pas prendre le risque de troubler ses activités à ce moment-là.

Il existe trois modalités de pentest :

- **Black Box :** Les attaquants n'ont aucun accès ni aucune information sur le SI, il faut partir de zéro. Cela impose une première étape d'OSINT
- **Grey Box :** La plus classique. Les attaquants disposent de quelques informations générales telles que la segmentation des comptes ou l'architecture.
- **White Box :** Cette modalité est plus proche d'un audit. Les attaquants ont toutes les informations et il est possible de poser des questions aux équipes en charge du SI.

Il est aussi possible de faire du pentest sans informer la Blue Team pour voir s'ils sont capables de détecter les attaques en situation réelle. D'après Sabine PIROU, la meilleure stratégie est celle de la Grey Box Reversal. Elle consiste à donner à la Red Team des informations sur le SI de la même manière qu'une Grey Box, sans que la Blue Team ne soit informée du pentest.

Les méthodes de pentest, généralement produites par des centres de recherche ou des régulateurs locaux, donnent une certaine structure aux activités de pentest. La plupart de ces méthodos sont développées aux États-Unis, telles que OWASP et MITRE, qui sont les plus importantes à l'international.

À l'issue du pentest, un rapport doit être rédigé par les pentesters et partagé avec les personnes ayant participé au cadrage. Ce rapport contient :

- La classification par criticité des vulnérabilités identifiées,
- L'explication des méthodes utilisées et le détail des failles découvertes pendant le test,
- Les recommandations pour corriger les vulnérabilités identifiées,
- Les délais conseillés pour la remédiation,
- L'organisation du nouveau pentest pour évaluer les correctifs

D'autres concepts sont similaires et peuvent être confondus avec le test d'intrusion :

- **Red Teaming :** scénario plus sophistiqué et plus étendu dans le temps, utilisation de social engineering ou de l'intrusion physique

— **Bug Bounty :** challenge proposé à toute la communauté de la cybersécurité contre prime pour tester la solidité d'un nouveau produit, ou d'une nouvelle version d'un logiciel
— **Scan de vulnérabilités :** contrôle automatisé pour identifier les défauts de conception ou les points d'entrée qui pourraient être exploités sur un réseau ou un logiciel
— **Audit de sécurité/white box :** travail de concert entre les auditeurs et le service informatique, accès direct à toutes les informations techniques, long, cher, mais très complet.

Sous cette forme, le pentest n'est pas assez exhaustif donc il faut en faire régulièrement, tous les 3 mois ou même tous les ans, pour maintenir à jour les SI et suivre l'évolution des menaces. C'est une bonne pratique à intégrer sur le long terme dans le cycle de vie du SI.

2 L'apport d'une purple team à un test d'intrusion

Le pentest révèle certaines problématiques :
— le cadrage n'est pas forcément mené par des experts, ce qui complique la cartographie et la priorisation des vulnérabilités.
— Il y a des problématiques d'organisation et de coordination, car celle-ci doit être parfois menée par les pentesters en plus de leur travail de test d'attaques.
— On note également des problématiques de délais et de budget pour le correctif de certaines vulnérabilités.
— Il est parfois impossible de faire des correctifs sur certaines vulnérabilités en raison d'une organisation trop complexe de certains outils, ce qui mène à une acceptation des risques.
— Enfin, la communication est compliquée avec le management non expert, qui sera dur à convaincre pour débloquer des moyens et investir sur la mise en place de correctif.

C'est face à ce constat qu'intervient la Purple Team. Fonctionnant de manière collaborative, elle permet à la Blue Team et à la Red Team de travailler ensemble pour mettre en place des correctifs, tout en approfondissant les connaissances de chaque équipe. De plus, la collaboration entre des profils internes (Blue Team) et externes (Red Team) offre une vision bien plus large des processus.

La Purple Team est un concept assez récent et encore peu documenté. Le secteur de la finance est le plus avancé dans ce domaine, notamment grâce à TIBER-EU, une méthodologie établie par la Banque Centrale Européenne qui figure parmi les plus complètes et importantes pour la Purple Team. En Asie, les méthodologies AASE (Singapour) et iCAST (Hong Kong) sont les plus incontournables du secteur financier. Très complet, le framework TIBER-EU sert également de base dans tous les autres secteurs d'activité, au-delà de la banque et de la finance.

Cependant, ces méthodologies sous-exploitent le potentiel de la Purple Team. Pour pallier cela, Sabine Pirou présente dans sa thèse une approche qui fait de la Purple Team un véritable relais présent sur la totalité du processus d'un pentest : du cadrage initial avec le client jusqu'au retest des vulnérabilités identifiées et corrigées, garantissant ainsi

l'efficacité des correctifs. Ainsi, cette Purple Team fait intervenir plusieurs acteurs :

- **Le VRP :** Un profil commercial indépendant des équipes Blue et Red. Pédagogue, il accompagne le client, prépare les scénarios d'attaques et définit les indicateurs de réussite avec toutes les parties prenantes.
- **Un facilitateur :** Il informe le client de l'avancement du projet et coordonne les équipes Red et Blue. Il s'assure également qu'un test n'engendre pas un impact trop important sur l'activité du client.
- **Un traducteur :** Il apporte un regard moins technique pour s'assurer que le rapport final soit parfaitement compréhensible par les décideurs.
- **Un animateur :** Il assure la cohésion entre la Blue et la Red Team afin de trouver des solutions. Il stimule la créativité pour mener les tests et mettre en place des remédiations (à travers l'organisation d'ateliers, de brainstormings ou de design thinking).
- **Un chef de projet :** Il assure le suivi global du projet et présente les résultats au client pour valider les solutions, les plannings et les coûts de la remédiation.

Les avantages de la Purple Team sont multiples. Pour l'ensemble des acteurs, il est plus agréable de disposer d'une vision claire des rôles et des objectifs à atteindre. Le client bénéficie d'un bien meilleur suivi, ce qui renforce sa satisfaction. De plus, la présence d'un coordinateur entre la Red et la Blue Team facilite grandement le travail des deux équipes. Enfin, toute l'organisation est prise en charge de A à Z, ce qui améliore la productivité, optimise les résultats et consolide les liens humains ainsi que l'entraide entre les équipes défensives et offensives.

3 La purple team à l'aube des réglement NIS2 et DORA

La directive européenne NIS 2, entrée en vigueur en octobre 2024, n'est toujours pas transposée en droit français. Son objectif est d'imposer un socle minimum de sécurité afin d'améliorer la résilience globale et la gestion des risques cyber. Cette réglementation touche 18 secteurs d'activité, ce qui représente un impact considérable pour les entreprises. En mars 2026, l'ANSSI a confirmé dans son Référentiel Cyber France (ReCyF) que la réalisation de pentests réguliers constitue une preuve solide de cette diligence cyber. Dans le cadre de NIS 2, il sera donc nécessaire de démontrer que des tests sont fréquemment menés pour sécuriser les systèmes d'information (SI). Le pentest s'impose comme un moyen privilégié pour y parvenir, ce qui pourrait le rendre, à terme, obligatoire. Dans ce contexte, et conformément à l'approche de Sabine PIROU, mettre en place une Purple Team permet de rentabiliser vos pentests et de garantir l'application effective des correctifs pour une gestion optimale des risque cyber.

La réglementation DORA (Digital Operational Resilience Act) se montre beaucoup plus restrictive que NIS 2 pour le secteur bancaire et financier. Elle impose notamment la réalisation de tests de pénétration avancés, appelés TLPT (Threat Intelligence-Led Penetration Testing). Pour encadrer ces tests, DORA se base sur le framework TIBER-EU, une méthodologie qui intègre nativement la Purple Team. L'adoption de la Purple Team devient donc indispensable dans ce contexte réglementaire. Dès lors, déployer une approche Purple de bout en bout s'avère particulièrement pertinent pour documenter l'intégralité du processus de pentest et ainsi garantir une totale conformité.

III Les normes en sécurité de l'information (Par Paul RICHY)

1 ISO

Fondé en 1947, l'ISO est un organisme mondial présent dans 175 pays. Son fonctionnement est démocratique : chaque pays membre dispose d'une voix unique pour le vote des textes. La France y est représentée par l'AFNOR. Aujourd'hui, l'ISO s'appuie sur environ 300 comités techniques et gère un catalogue de plus de 26 000 normes.

Le développement d'une norme internationale est un processus long qui passe par plusieurs stades de maturité :

- NWIP (New Work Item Proposal) : Proposition de nouveau sujet d'étude.
- WD (Working Draft) : Projet de travail initial.
- CD (Committee Draft) : Projet du comité.
- DIS / FDIS (Draft / Final Draft International Standard) : Projet de norme internationale (final).

Pour être adoptée, une norme doit impérativement faire l'objet d'un consensus, ce qui signifie qu'elle doit recueillir moins de 25% de votes négatifs. Si ce consensus n'est pas atteint, le projet est rejeté : il faut alors tout reprendre à zéro et repasser par chacune des phases réglementaires. De plus, une norme est systématiquement révisée tous les 5 ans, et le processus complet de révision demande en général entre 3 et 4 ans de travail.
L'ISO est structurée en différents comités techniques, parmi lesquels :

- JTC 1 (Secrétariat : USA) – Technologies de l'information : Ce comité compte plus de 3 500 normes à son actif. Il se divise en plusieurs sous-comités clés, dont le SC 27, en charge de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée, ainsi que le SC 42, qui traite de l'intelligence artificielle et du Big Data.
- TC 20 (Secrétariat : USA) – Aéronautique et espace : Il gère près de 700 normes.
- TC 22 (Secrétariat : France) – Véhicules routiers : Il regroupe plus de 1 000 normes.
- TC 34 (Secrétariat : France) – Produits alimentaires : Il rassemble plus de 900 normes.
- TC 292 (Secrétariat : Suède) – Sécurité et résilience : Il compte plus de 60 normes.

2 AFNOR

Créée en 1926, l'AFNOR est le membre français de l'ISO. Son rôle est d'émettre des normes au niveau national. Elle s'intègre dans un écosystème à trois niveaux : l'AFNOR agit à l'échelle française, le CEN (Comité européen de normalisation) opère au niveau européen, et l'ISO intervient à l'échelle mondiale.

Au sein de cette structure, la Commission de Normalisation Cybersécurité (CN Cyber) est le représentant français du sous-comité international SC 27, qui est spécifiquement en charge de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée.

Toute personne intéressée peut participer aux travaux de l'AFNOR. Chaque comité technique se réunit deux fois par an en mode hybride. Cependant, contrairement aux réunions exclusivement en présentiel, le format hybride tend à rendre l'élaboration des documents moins fluide. D'après Paul RICHY, le manque de fluidité nuit parfois à la prise en compte des nuances lors de la rédaction des textes réglementaires.

3 ISO 27001

Parue initialement en 2005, la norme ISO 27001 est une norme de management dont le thème central est le Système de Management de la Sécurité de l'Information (SMSI). Les normes de management ont pour objectif de permettre l'obtention d'une certification.

Cette certification repose sur une approche de conformité validée par une Déclaration d'Applicabilité. Ce document définit précisément le périmètre sur lequel la demande de conformité va être examinée, et intègre des mesures de sécurité généralement issues de la norme ISO 27002.

Nuance importante : La certification garantit uniquement que le système mis en place est bien conforme à ce qui a été déclaré dans le périmètre. En revanche, elle ne garantit pas en soi un haut niveau de sécurité opérationnelle.

La norme ISO 27001 s'appuie directement sur les mesures de l'ISO 27002. Par conséquent, lorsque l'ISO 27002 évolue, il est nécessaire de mettre à jour l'ISO 27001. C'est précisément ce qui s'est passé en 2022 lors de la dernière révision majeure de la norme ISO 27001, afin de s'aligner sur les changements structurels de l'ISO 27002.

4 ISO 27002

Norme technique parue en 2005 et a connu 3 révision :

- 2005 11 chapitres et 133 mesures
- 2013 14 chapitres et 114 mesures
- 2022 4 chapitres et 93 mesures. Cette année marque une restructuration profonde de l'ISO 27002

Dans sa version actuelle, la norme abandonne ses anciens chapitres au profit de 4 grandes catégories de mesures (ou contrôles) :

- Mesures organisationnelles : 37 mesures, dont 3 nouvelles.
- Mesures liées aux personnes : 8 mesures, aucune nouvelle.
- Contrôles physiques : 14 mesures, dont 1 nouvelle.
- Mesures technologiques : 34 mesures, dont 5 nouvelles

La version 2022 ne s'est pas contentée de réorganiser les chapitres ; elle a également introduit la notion novatrice d'"attributs". Ces attributs permettent désormais de trier et de classer les mesures selon leurs finalités.

5 ISO 27005

Parue initialement en 2005, la norme ISO 27005 a été révisée en 2011 puis en 2018, avant d'aboutir à sa version actuelle publiée en 2022.

Il s'agit d'une norme qui traite spécifiquement de la gestion des risques liés à la sécurité de l'information. Il est important de souligner que ce n'est pas une méthode d'analyse des risques en soi. En réalité, elle fournit les lignes directrices et les critères qui permettent de valider la conformité des méthodes d'analyse de risques existantes (comme la méthode française EBIOS RM).

6 Conclusion

Toutes ces normes (ISO 27001, 27002 et 27005) partagent la même année de parution pour leur dernière version majeure : 2022. Par conséquent, elles approcheront bientôt de la période réglementaire d'analyse des besoins de révision, appelée la study period. À l'issue de cette phase, trois issues sont possibles :

- **L'obsolescence :** La norme est jugée dépassée et sera supprimée.
- **La reconduction :** La norme reste pertinente et cohérente en l'état. Aucune révision n'est engagée et son année de parution reste inchangée.
- **La révision :** La norme doit être mise à jour. Un chantier de modification est alors lancé, ce qui débouchera à terme sur une nouvelle année de parution correspondant à la nouvelle version.

Enfin, Paul RICHY évoque la différence entre le BIA et l'analyse de risque classique. aux approches traditionnelles, les comités TC 292 (Sécurité et résilience) et JTC 1/SC 42 (Intelligence artificielle) ne se basent pas sur une analyse des risques par scénarios d'attaque. Ils s'appuient plutôt sur le BIA (Business Impact Analysis ou Analyse de l'impact sur l'activité). Dans ce cadre, on ne cherche pas à modéliser la manière dont une attaque se déroule, mais on évalue directement l'ampleur des dégâts potentiels si un sinistre survient. Cette philosophie est nettement plus orientée vers la reconstruction et la résilience que vers la simple prévention.

En raison du contexte géopolitique actuel, marqué par un recul de la mondialisation au profit de souverainetés régionales, la tendance de la normalisation évolue. Les normes internationales ont de plus en plus tendance à se décliner en réglementations plus locales (à l'échelle européenne ou française). Dans cette dynamique de relocalisation des standards, l'AFNOR sera fortement susceptible de participer activement à ces nouveaux travaux.

IV Qesuestion /reponse

1 Questions posées à Sabine PIROU

Pouvez-vous donner un exemple de vulnérabilité pour chacun des niveaux de criticité ?
La criticité dépend fortement du secteur d'activité et de la sensibilité du système d'information (SI) visé. Par exemple, sur un SI hautement critique, la possibilité de téléverser un document sur une application sans aucun contrôle de sécurité (type de fichier, taille,

contenu) constitue une vulnérabilité majeure. En fin de compte, la classification précise de chaque vulnérabilité repose sur le jugement de l'expert et l'analyse du pentester.

L'intelligence artificielle peut-elle aider les attaquants ?
Oui, absolument. C'est pourquoi, en tant que pentesters, nous devons nous aussi utiliser l'IA pour optimiser nos défenses. Pour mener à bien sa mission, le pentester doit adopter le même mode de fonctionnement et utiliser le même type d'outils que les cybercriminels. Actuellement, l'une des IA les plus utilisées et les plus pertinentes dans ce domaine est Claude.

Est-ce que l'IA va remplacer les pentesters ?
Aujourd'hui, la réponse est non. L'IA reste avant tout un outil d'assistance performant, notamment pour générer de nouvelles idées de scénarios d'attaque ou pour comprendre des langages de programmation mal maîtrisés.
Deux IA spécifiques ont été identifiées et soulèvent cette question :

- **Shannon :** Un outil encore peu efficace qui ne risque pas de remplacer l'humain à court terme.
- **Mythos :** Un outil développé par Anthropic. Celui-ci s'avère extrêmement efficace, à tel point qu'il n'a pas été rendu public car ses capacités font peser des risques jugés trop importants. Mythos fait peur à ses créateur !

La personne responsable de la Purple Team peut-elle être indifféremment interne ou externe à l'entreprise ?
Les deux options sont tout à fait envisageables. De plus, ce rôle ne requiert pas nécessairement un profil d'expert ultra-technique ; il s'agit avant tout de quelqu'un qui maîtrise globalement les enjeux de la cybersécurité et sait coordonner les équipes.

Après un pentest suivi des modifications recommandées, combien de temps une entreprise peut-elle espérer être à l'abri d'une nouvelle cyberattaque ?
Un pentest ne sécurise jamais un système à vie, c'est pourquoi il est indispensable d'en réaliser régulièrement. Si les vulnérabilités identifiées et corrigées ferment des points d'accès précis, les attaquants chercheront systématiquement d'autres chemins pour s'introduire. Le pentest et la démarche Purple Team doivent impérativement s'inscrire dans un cycle d'amélioration continue de la sécurité.

2 Questions posées à Paul RICHY

La France doit-elle respecter les normes ISO ou seulement les normes AFNOR ?
Par principe, les normes sont conçues comme des normes d'adhésion volontaire ; l'application des normes ISO n'est donc pas obligatoire en soi. Toutefois, elles peuvent revêtir un caractère obligatoire si elles sont explicitement exigées dans le cadre d'un contrat. En revanche, certaines normes européennes (CEN) ou françaises (AFNOR) peuvent devenir d'application réglementaire obligatoire dès leur parution.

Quelle est la relation entre les différentes réglementations et normes sur la sécurité des données personnelles ?

Le RGPD (Règlement Général sur la Protection des Données) est une réglementation européenne obligatoire. Pour aider les organisations à s'y conformer, la norme internationale ISO 27701 a été spécifiquement conçue comme une extension de la 27001 dédiée à la protection de la vie privée. Cependant, les nouvelles réglementations émergentes concernant l'Intelligence Artificielle ne respectent pas toujours les principes de l'ISO 27701 et du RGPD.