Eric Le Calvez (BPCE-SI)

I. Écosystème et Chiffres Clés (BPCE SI)

Profil Groupe : BPCE Solutions Informatiques gère la sécurité applicative et la lutte contre la fraude externe.

- **Effectifs :** ≈ 2 600 collaborateurs.
- **Clients :** 30 millions ; **Parc :** 2 000+ applications bancaires, 96 000 postes de travail.
- **Flux :** 18 500 transactions/seconde en pointe ; 11,6 millions de visiteurs/mois sur la banque en ligne.
- **Implantation :** Présence dans 19 villes.

II. Organisation et Risques Bancaires

Gouvernance Sécurité :

- **Direction Sécurité Groupe :** Rôle régalien, gestion des risques, sensibilisation, contrôles Niveau 2.
- **Sécurité Infrastructure :** SOC, architecture, accompagnement projets infrastructure.
- **Sécurité Applicative :** Accompagnement projets (Réglementation, SSI, Fraude).
- **Établissements (RSSI) :** Contrôles Niveau 1 & 2, sensibilisation locale.

Risques (Image (réputation), Réglementaire, Financier) :

- **Intrusion réseau**
- **Défacement de sites web**
- **fuite de données**
- **ransomware**
- **fraude**

III. Cadre Règlementaire et Normatif

Directives Majeures :

- **DSP2 (Directive Services de Paiement 2) :** En vigueur depuis 13/01/2018. Encadre les agrégateurs, initiateurs de paiement et impose l'**Authentification Forte (AF : 2 facteurs parmis c : conaissance, prosessions, inhérence)**.
- **RGPD :** Protection des données personnelles.
- **PCI DSS :** Normes de sécurité des données de cartes bancaires.
- **NIS / LPM :** Directive auropéenne NIS (Network Information Security), Sécurité des réseaux et systèmes d'information critiques.

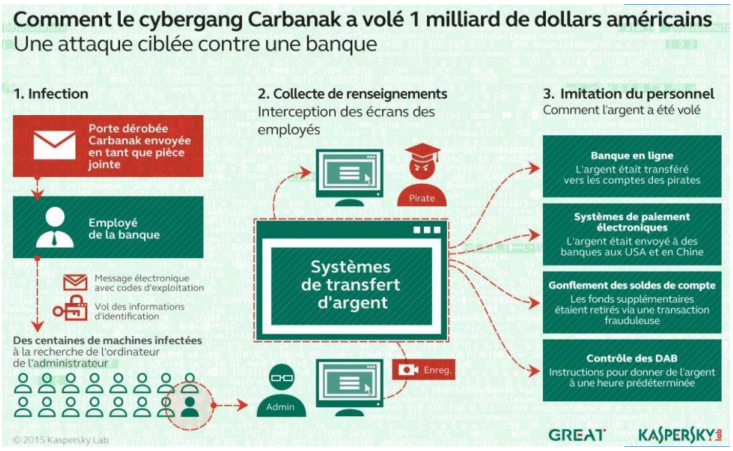
IV. État des Lieux de la Fraude (2024)

Indicateurs de Fraude :

- **Préjudice Global :** 1,189 milliard d'euros (globalement stable sur 3 ans).
- **Taux de Fraude :** Carte (0,053% - bas historique), Virement instantané (0,046%).
- **Succession :** Le chèque passe en 3ème position (en baisse) ; le virement est une source majeure de revenu pour les fraudeurs.
- **Smishing :** Forte recrudescence du phishing par SMS (fausses alertes Caisse d'Épargne).

Répartition (Valeur vs Volume) :

- **Valeur :** Carte (40%), Virement (30%), Chèque (23%), puis prélevement et retrait aux DAB
- **Volume :** Carte (94%), Chèque (2,2%), Virement (1,7%), DAB (1,4%). Les fraudeurs cherchent la facilité !



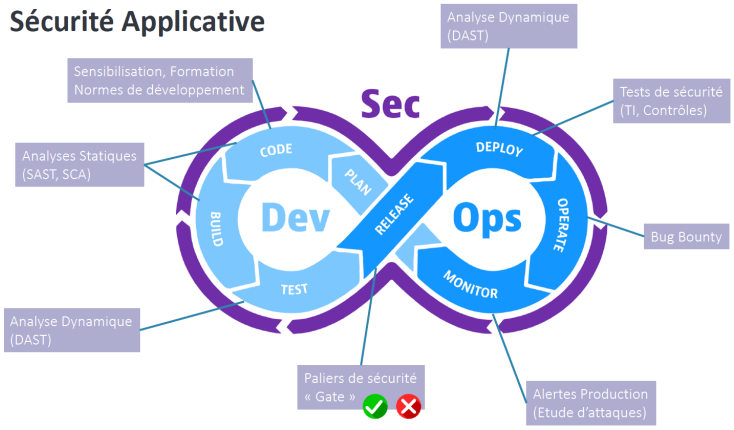
Smishing = phishing + ingénierie sociale. Ex : "Paiement en cours, si vous n'êtes pas à l'origine, contactez nous au ..."

V. Sécurité Applicative et Processus Projet

Cycle de Vie Sécurisé :

- **Étude / Amont :** Veille, innovation, accompagnement métiers, définition des exigences (RGPD, Fraude, Logs).
- **Conception / Architecture :** Définition d'exigences de sécu, RGPD, Fraudes, Logs, continuité d'activité.
- **Développement (DevSecOps) :**
  - **Veille sur les composants logiciels**
  - **SAST / SCA(Software COmposition Analysis) :** Analyses statiques du code et des composants tiers.

  - **DAST :** Analyses dynamiques.
  - **Code Audit :** Revue humaine ou test automatisés.
- **Homologation :**
  - **Security Gates :** blocage des releases si vulnérabilités hautes
  - Si ça passe pas on retourne au développement.
- **Avant la production : CSMP** (Contrôle Sécurité avant Mise en Prod), analyse des risques résiduels.
- **En production :** Security Center (SAV de la sécu du produit en gros), remontées client (par ex : phishing), evaluation des risques et SOC (detection de fraudes).



VI. Stratégies de Lutte contre la Fraude

Modèles d'Attaque :

- **Historique :** Attaques physiques (violentes ou astucieuses).
- **Moderne :** Attaques logiques (Carbanak : infection → reconnaissance → imitation personnel → virement/DAB), Ingénierie sociale (faux conseillers).
- **Impact DSP2 :** Passage du phishing simple au **phishing temps réel** ou à l'ingénierie sociale pour contourner l'2AF.

Outils de Défense : IA, Machine Learning, règles métiers, bon sens.

Triangle d'Équilibre : **Blocage** vs **Alerting** vs **Faux Positifs**.

VII. Compétences de l'Expert en Accompagnement

Hard Skills : Architectures sécu, dev, réglementation, analyse de risques.

Soft Skills : Curiosité, esprit critique, synthèse, communication/conciliation (écoute client final).

- CERT (Computer Emergency Response Team) : Une unité d'experts chargée de centraliser, traiter et répondre aux incidents critiques de sécurité au niveau national ou sectoriel.
- CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) : Un laboratoire agréé par l'ANSSI pour réaliser des audits techniques et évaluer la robustesse des produits de sécurité (en vue d'une certification).
- SOC (Security Operations Center) : Une plateforme opérationnelle qui assure la surveillance continue (24/7) des systèmes d'information pour détecter et analyser les menaces en temps réel.
- OIV : Opérateur d'Importance Vitale.

Philippe Rose (CESTI THALES)

I. Fondamentaux et Enjeux de la Certification

Objectifs de l'Évaluation :

- **Légaux :** Conformité avec la loi (ex : RGS).
- **Marché :** Accès à des contrats spécifiques ou exigences clients.
- **Concurrentiels :** Se démarquer de la concu. Différenciation commerciale via un gage de confiance.
- **Protection de l'image / PI :** Sauvegarde de l'image de marque et de la Propriété Intellectuelle (PI).

Processus Tripartite (Acteurs Clés) :

- **Le Demandeur (Sponsor/Developer) :** Soumet le produit et finance l'étude.
- **Le CESTI (Laboratoire) :** Centre d'Évaluation de la Sécurité des Technologies de l'Information. Tiers indépendant réalisant l'audit.
- **L'Autorité de Certification (Certification Body - CB) :** En France, l'ANSSI. Délivre le certificat final après revue des travaux du CESTI.

Accréditations selon des normes ISO :

- **COFRAC (en France) :** Organisme d'accréditation.
- **ISO 17065 :** Norme pour les organismes de certification (CB).
- **ISO 17025 :** Norme pour les laboratoires d'essais (CESTI/ITSEF).

Les certifications peuvent être : publique (en France, par le centre de certif de l'ANSSI), ou **privée** (accepte les risques que l'état ne prendrait pas)

II. Le CESTI : Rôle et Déontologie

Statut et Indépendance :

- **Agrément :** Délivré par l'ANSSI (renouvelé tous les 2 ans).
- **Évaluation "Boîte Blanche" :**
- **Cloisonnement :** Séparation stricte des activités d'évaluation et de conseil/développement pour garantir l'impartialité.
- **Compétences :** Expertise technique validée par l'ANSSI sur des domaines précis (Smartcards, Réseaux, OS, etc.).

III. Schémas de Certification en France

Selon les besoins, l'ANSSI délivre 2 types de certifications : CC et CSPN, un CESTI peut être agréés pour l'un des deux ou les 2. Ces certifications peuvent servir à des besoins d'homologation, de qualification ou d'agrément. **Les certifs sont valable 5 ans !**

Critères Communs (CC - ISO 15408) :

- **Niveaux EAL (Evaluation Assurance Level) :** De **EAL1** (tests basiques) à **EAL7** (conception formellement vérifiée).
- **Reconnaissance :** Internationale (CCRA) et Européenne (SOG-IS).
- **Portée :** Évalue la robustesse de l'implémentation ET la rigueur du cycle de vie (développement, livraison).

CSPN (Certification de Sécurité de Premier Niveau) :

- **Philosophie :** Créée en 2008 pour pallier la lourdeur des CC.
- **Format :** Évaluation en temps/charge contraints ($\approx$ 2 mois, 25-50 jours.homme).
- **Focus :** Orientée **tests d'intrusion** (Pentest).
- **Taux d'échec :** Environ 50% des produits échouent lors de la première tentative.
- pas plus cher que CC

IV. Concepts Techniques et Méthodologie

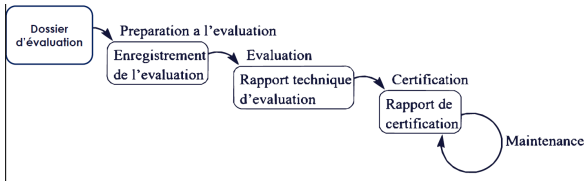
Documents de Référence :

- **TOE (Target of Evaluation) :** Le périmètre exact du produit évalué.
- **ST (Security Target) :** Document décrivant les menaces et les fonctions de sécurité du produit.
- **PP (Protection Profile) :** Exigences de sécurité génériques pour une catégorie de produits (ex : pare-feu).

Système de Cotation des Attaques (AVA_VAN) : L'évaluation calcule le niveau de résistance via un cumul de points sur 5 facteurs (exemple sur 13 points) :

1. **Temps écoulé :** Préparation et exécution (ex : < 1 semaine = 1 pt).
2. **Expertise :** Niveau de l'attaquant (ex : Layman, Proficient, Expert sur 3 pts).
3. **Connaissance du produit :** Informations publiques vs confidentielles. (ex : restreint = 3 pts)
4. **Fenêtre d'opportunité :** Accès physique/logique requis. (ex : modéré = 4 pts)
5. **Moyens techniques/Équipement :** Standard vs Hautement spécialisé. (ex : specialisé 2pts)

Règle d'or : La vulnérabilité est avérée si la cotation est **inférieure** à la limite fixée par le niveau AVA_VAN (EAL) visé.



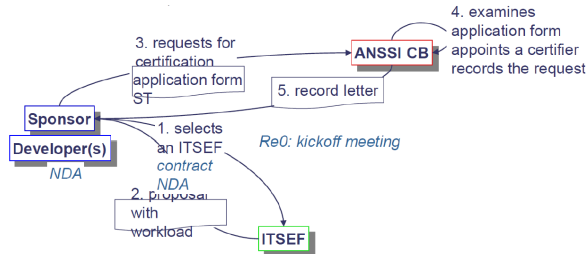


FIGURE 1 – Enregistrement evaluation / Certification request

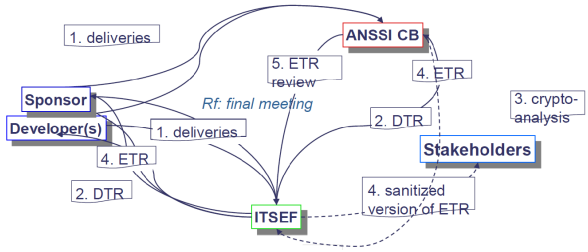


FIGURE 2 – processus d'évaluation

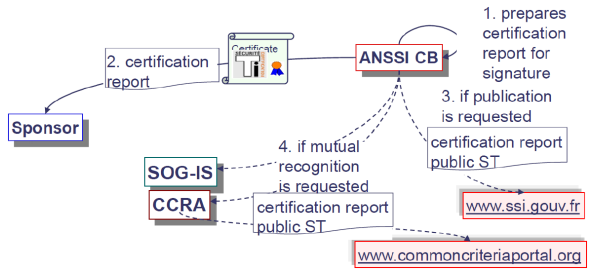


FIGURE 3 – processus certification / certification decision

V. Architectures Complexes et Composition

Le Principe de la "Coupole" : Très peu de développeurs créent tout de A à Z. La certification permet d'assembler des briques déjà certifiées pour mutualiser les efforts.

- **Exemple Passeport :** Application (EAL5+, certifiée en Allemagne) sur OS (EAL7, certifié en Hollande) sur Composant (EAL5+, certifié en France).
- **Contrainte :** La couche supérieure (N) doit impérativement respecter les **guides d'utilisation** de la couche inférieure (N-1).

VI. Accords de Reconnaissance Mutuelle

CCRA (Monde - 31 pays) :

- Reconnaissance limitée à **EAL2** (niveau d'attaquant basique) depuis 2014.
- Harmonise les certificats à l'échelle mondiale pour faciliter l'exportation.

SOG-IS (Europe - 17 pays) :

- Reconnaissance jusqu'à **EAL4**, voire **EAL7** pour les domaines spécialisés (Smart Cards).
- Audits de centres de certification et de laboratoires beaucoup plus poussés que le CCRA.

VII. Cadre Réglementaire : RGS et Secteur Privé

Référentiel Général de Sécurité (RGS) :

- S'impose aux SI des administrations françaises.
- **Qualification :** Utilise la certification comme socle.
- **Niveaux :** Élémentaire (CSPN), Standard (EAL3+), Renforcé (EAL4+).

Schémas Privés : Des secteurs comme le bancaire (EMVCO, VISA, Mastercard) ou les contenus multimédia imposent leurs propres schémas, souvent basés sur les travaux des CESTI agréés nationalement.

VIII. Évolutions : EU Cyber Security Act (2019)

Nouveaux Niveaux de Confiance EU :

— **Basique** / **Substantiel** / **Élevé**.

Schémas ENISA en cours :

— **EUCC :** Transposition des CC pour les produits ICT. Premier schéma opérationnel.

— **EUCS :** Certification dédiée aux services **Cloud**.

— **EU5G :** Spécifique aux réseaux mobiles.

Changement de Paradigme : Le schéma européen **supplantera** les schémas nationaux. Les agences nationales (ANSSI) conservent l’agrément des laboratoires et la gestion du niveau "Élevé".

Martine Gilralt-Torrent (CERT-IST THALES)

I. Fondamentaux des CERT / CSIRT

Définitions et Services :

- **CERT / CSIRT :** Computer Emergency (ou Security Incident) Response Team.
- **Rôle :** Centre d'alerte et de réaction aux attaques informatiques pour entreprises/administrations.
- **Services (RFC 2350) :** Gestion des vulnérabilités (avis de sécurité), gestion des incidents (Incident Response), renseignement sur la menace (CTI : IOC, TTP), point de contact.
- **PSIRT :** Product Incident Response Team

Typologie et Écosystème :

- **Types :** Nationaux (CERT-FR), ministériels, régionaux (ex : Breizh Cyber), internes (entreprise), externe/commerciaux (ex : cert La Poste), sectoriels (CERT Maritime), PSIRT (spécifiques aux produits, ex : Cisco).
- **Réseaux : FIRST** (mondial, +816 membres, 113 pays), **TF-CSIRT** (européen), **InterCERT France** (national).

Le Cert-IST :

- **Identité :** Créé en 1999 (assoc loi 1901), opéré par **Thales** à Labège (Toulouse). CERT commercial (ou externe). En lien avec l'association Cert-IST.
- **Missions :** veilles/alertes sur menaces/attaques/IOC(indice of compromission), aide au traitement d'incidents, surveillance des dépôts de nom de domaine.

II. Typologie des Attaquants et Motivations

1. Hacktivistes (Activistes) :

- **Motive :** Revendications politiques/sociales, visibilité médiatique.
- **Actions :** DDoS, défacement, Hack & Leak (Doxxing).
- **Groupes :** Anonymous, NoName057 (pro-Russes, JO 2024), IT Army of Ukraine.

2. Cyber Gangs (Cybercriminalité/eCrime) :

- **Motive :** Gain financier (ROI), extortion. Écosystème pro (Développeurs, Sellers, Ops).
- **Actions :** Scams (Nigeria 4-1-9, Romance, Pig butchering), Ransomware, FOVI/BEC.
- **Acteurs 2024 :** RansomHub, PLAY, LockBit 3.0, Medusa, Akira.

3. Étatiques (Spies & State Sponsored / APT) :

Motive : Espionnage industriel, déstabilisation politique, supériorité militaire. Budgets illimités.

- **Chine :** APT1, APT10 (Stone Panda), APT41 (Winnti). Cibles : Gov, tech, santé.
- **Russie :** APT28 (Fancy Bear), APT29 (Cozy Bear), Sandworm. Cibles : OTAN, infra critiques.
- **Iran :** APT33 (Elfin), OilRig. **Corée du Nord :** APT38 (Lazarus - vol financier).
- **USA :** Equation Group (NSA). **France :** Babar, Snowglobe (visant l'Iran).

III. Le Marché de l'Offensive et 0-Days

Escroqueries :

- Nigerian scam ("419 scam", "brouteurs")
- Pig butchering : arnaque spéculation financière (crypto actifs)
- Romance scam
- Faux antivirus / faux support technique
- **FOVI** (faux ordres de virement), **BEC** (Business Email compromise)

Filières de Vente :

- **Marché Blanc :** Bug Bounty (légal, récompense par l'éditeur).
- **Marché Gris :** Brokers gouvernementaux (ex : Zerodium).
- **Marché Noir :** Vente illégale aux cybercriminels.

Coûts Zerodium :

- **Bypass PIN/Passcode :** ≈ 100 000 $.
- **Accès Browser/Email :** ≈ 500 000 $.
- **Full accès Mobile (Zero-click) :** 2 à 2,5 millions $.

IV. Évolution des Attaques et Tendances

Chronologie du Crime : Carding (2005) → Trojans Bancaires (Zeus, 2007) → Bank Heist (SWIFT, 2016) → Ransomware (2020).

Tendances 2024-2025 :

- **Chasse aux accès :** Phishing, InfoStealers, contournement MFA (OKTA, 1Password).
- **Cloud Intrusions :** +75 % en un an. Exploitation des SaaS (Snowflake, Salesforce).
- **IA :** Ransomware 3.0 (attaques pilotées par IA).
- **Supply Chain :** Ciblage des sous-traitants pour atteindre les grands comptes.

V. Méthodologies d'Analyse d'Attaque

Attaques visant le grand publique

- **Arnaques** : nigérianes, sextorsion (vous avez été filmé), faux technicien Microsoft
- **Phishing** : vol de données / identifiants
- **Infection par un botnet** : Emotet, Trickbot...
- **Ransomware et crypto-mineurs**

Attaques visant les entreprises

- **visant les services financiers** : arnaque au président, FOVI (faux ordre de virement), social engineering, BEC (Business Email Compromise).
- **cyber-espionnage** : APT (Advanced Persistant Threat)
- **ransomware** : même techniques que APT
- **Supply chain Attack** : les entreprises sont de plus en plus sécurisé donc on attaque les sous traitants.

1. Cyber Kill Chain (Lockheed Martin) : Processus linéaire en 7 étapes :

- **Reconnaissance** : Identification et sélection des cibles.
- **Weaponization** : Création d'un couplage entre un logiciel malveillant et un exploit (outil d'attaque).
- **Delivery** : Transmission de la charge utile vers la cible (e-mail, clé USB, site web).
- **Exploitation** : Activation du code malveillant en exploitant une vulnérabilité pour obtenir un accès.
- **Installation** : Mise en place d'une persistance (backdoor) pour maintenir l'accès au système.
- **Command & Control (C2)** : Établissement d'un canal de communication pour piloter à distance le système compromis.
- **Actions on Objectives** : Accomplissement du but final (exfiltration de données, sabotage, chiffrement).

2. MITRE ATT&CK : Base de connaissances matricielle des TTP (*Tactics, Techniques, Procedures*). Indique le/les entrypoint, les méthodes de consolidation et de persistance, et l'impact...

- **Tactics :** Le "pourquoi" (ex : Persistance, Privilege Escalation).
- **Techniques :** Le "comment" (ex : DLL Side-Loading, Phishing).
- **Matrices :** Enterprise (Windows, Linux, Cloud), Mobile, ICS (Industriel).

VI. Défenses et Coopération

Stratégies de Défense :

- **2000 - Passive Defense** : Focus sur le durcissement des systèmes et du réseau (*OS + network Hardening*).
- **2004 - Alarm** : Mise en place des journaux d'événements et de la détection (*Log & Detection : IDS, Syslog*).
- **2010 - Security Monitoring** : Époque de la supervision de la sécurité via les centres opérationnels (*Security Supervision : SOC, SIEM*).
- **2016 - Understand Enemies** : Introduction de l'anticipation grâce à la connaissance des menaces (*Cyber Threat Intelligence : CTI, EDR*).
- **2023+ - Be prepared to recover** : Priorité à la capacité de survie et de reconstruction après une attaque (*Resilience*).

Protocoles de Partage :

- **TLP (Traffic Light Protocol) :** RED (strict), AMBER (restreint), GREEN (communauté), CLEAR (public).
- **PAP (Permissible Action Protocol) :** Actions autorisées avec l'info.
- **Chatham House Rule :** Protection des sources (anonymat)

Constat : L'attaquant n'a besoin que d'un maillon faible ; le défenseur a besoin d'une seule trace oubliée pour traquer.

1 VII. Conclusion

- **Complexité du contexte actuel** :
  - Tension entre le besoin de flexibilité des users et des attaquants toujours plus compétents/organisés.
  - Changement de paradigme : l'intrusion est inévitable. La question n'est plus "si" elle arrive, mais "quand" et comment en limiter l'impact.
- **Sujets de préoccupation majeurs** :
  - Protection contre le phishing et les *infostealers*.
  - Risques liés à la *supply-chain*.
  - Sécurisation du Cloud (leaks Github, Microsoft 365) et des systèmes industriels/IoT (SCADA, ICS, OT).
- **Stratégie de défense globale** :
  - **Regarder à l'extérieur** : Connaître la menace pour mieux l'anticiper.
  - **Surveiller dedans** : Superviser la sécurité en continu.
  - **Réagir** : Capacité de traitement et de résolution des incidents.

2 Autres :

- **Big-game gunting :** viser les grosses entreprise pour avoir des rançons plus elevées.
- **Association CERT :** FIRST (mondial), TF-CSIRT (Européen), IntelCERT France...
- **SAST :** Static Application Security Testing
- **DAST :** Dynamic Application Security Testing (sandboxé blackbox pour simuler des attaques)

Jerome Mampianinazakason (SynAcktiv)

I. Définitions et Écosystème du Pentest

Vocabulaire de base :

- **Pentest / Test d'intrusion :** Activité méthodique visant à évaluer la sécurité d'un périmètre en tentant de s'y introduire (**Pentest**) ou en déterminant la faisabilité d'une intrusion (**Mission non intrusive**).
- **Acteurs : Client** (payeur), **Audité** (cible technique), **Pentesteur** (auditeur).
- **PASSI :** Prestataire d'Audit de la Sécurité des Systèmes d'Information. Qualification **ANSSI** obligatoire pour certains marchés régaliens (audit de l'organisme + des auditeurs).

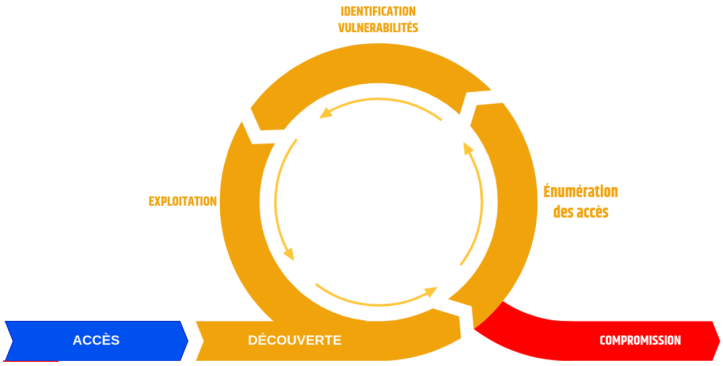
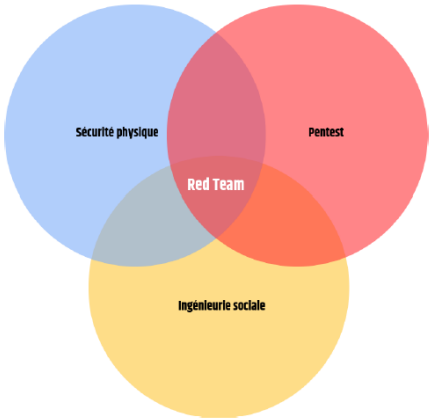


FIGURE 4 – Processus pentest

Typologies d'équipes (Teaming) :

- **Blue Team :** Équipe défensive (SOC, CSIRT). Objectif : détection, analyse d'alertes, réduction des **faux positifs**.
- **Red Team :** Attaque globale simulant un adversaire réel. Combine **intrusion physique**, **ingénierie sociale** (phishing) et **pentest** sur le long terme avec discrétion maximale.
- **Purple Team :** Exercice collaboratif. L'Attaque lance des actions ciblées, la Défense vérifie la levée d'alertes. Si échec, ajout d'**IOC** (Indicateurs de compromission).



II. Cycle de Vie d'une Mission (Phase Commerciale)

Contact client → Evaluation du besoin client → Definition de la mission → Planification

Contact client :

- **Prospection :** Démarcher de nouveaux clients, les appeler, les croiser en conférences etc
- **Repondre aux appel :** Clients récurrents ou nouveaux clients qui viennent vers nous

Evaluation du besoin client :

- **Déroulé** : réunion avec le client potentiel (aussi appelée "avant-vente"), souvent avec un expert technique (genre le pentesteur)
- **Objectifs** : quel est le besoin, comment aider le client, identifier le modèle de menaces, le type de mission, le nombre de jours requis pour la mission, le périmètre, le budget du client.

Les missions en pratique : souvet des tests d'intrusion web/mobile en boite noire ou des tests interne d'une entité (entreprise, filiale, site géographique).

Modèles d'audit (Référentiel PASSI) :

- **Niveaux d'information : Boîte Noire** (zéro info), **Boîte Grise** (comptes fournis), **Boîte Blanche** (accès complet : code source, config).
- **Types de tests :** Audit applicatif (Web/Mobile), Infrastructure (interne/externe), Evaluation du niveau de sécurité globale (phishing/red team/purple team)
- **Différents types d'audit :** Tests d'intrusion (web, externe, interne), Audit de code, Audit de configuration (système/service), Audit d'architecture rzo, Audit organisationnel (groupe ou entreprise).

III. Réalisation Technique de la Mission

Réunion de démarrage → Réalisation des test → Réunions intermédiaires → Rédaction du CR.

Phases Opérationnelles :

- **Kick-off (Réunion de démarrage) :** Validation du contexte, des dates, des pré-requis (VPN, comptes) et des adresses IP d'attaque. **Trace écrite par mail** indispensable pour preuve juridique.
- **Préparation :** Environnement isolé, outils prêts (**Burp Suite**, **ffuf**, **nmap**, **masscan**, scripts Go/Python).

— **Découverte :** Scan de ports (services tiers), identification des technos (NodeJS, PHP, Java), cartographie des fonctionnalités applicatives (CRUD, imports/exports). toujours avec l'autorisation du client

— **Méthodologie :** Appui sur l'**OWASP Testing Guide**, veille techno et expérience. Focus sur l'authentification et les fonctions critiques.

— **Prise de notes :** Capitalisation sur l'avancée, captures d'écrans des preuves d'exploitation (**PoC**), horodatage précis (crucial en Red Team).

Il est capitale de prendre des notes et de noter ce qui a été fait ou non pour avoir des traces pour le rapport et dire ce qu'il a été fait et quand.

IV. Livrables et Restitution

Le Rapport d'Audit (Structure type) :

— **Synthèse managériale :** Vision haut niveau pour les dirigeants (risques métiers, niveau global de sécurité).

— **Détails des vulnérabilités :**

  — **Observation :** Description technique adaptée au contexte.

  — **Preuve (PoC) :** Requêtes/réponses HTTP, lignes de commande (anonymisées : pas de mots de passe réels).

  — **Risque :** Impact théorique vs exploitation réelle.

  — **Cotation :** Gravité = **Probabilité** × **Impact**.

  — **Recommandation :** Correction immédiate (court terme) et structurelle (long terme).

Toujours retirer les informations personnelle ou identifiant de connexion du rapport.

V. Compétences et Profil du Pentesteur

Hard Skills (Socle technique) :

— Maîtrise avancée de **Linux** et des protocoles **Réseau**.

— Sécurité Web, Mobile et environnement **Active Directory** (Windows).

— Développement (**Python, Go**) pour l'outillage. Mathématiques pour la **Cryptographie**.

— Cloud (**AWS, Azure, GCP**), **IoT/Hardware** et systèmes industriels.

Soft Skills (Savoir-être) :

— **Éthique et Discrétion :** Interdiction de divulguer les découvertes (Engagement de confidentialité).

— **Rigueur :** Méthodologie stricte pour ne rien oublier.

— **Communication :** Capacité rédactionnelle (FR/EN) et tact lors des restitutions (ne pas blâmer les devs).

— **Apprentissage continu :** Veille constante (Twitter, CertFR, Blog posts), CTF (**HackTheBox**, **Root-Me**).

VI. Conditions de Travail et Évolution

Réalité du métier :

— **Salaire Junior (France) :** 35k – 45k€ (ex : Synacktiv ≈ 44k€ en 2024).

— **Contraintes :** Pression des délais, frustration si rien n'est trouvé, rédaction parfois répétitive.

— **Avantages :** Pas de routine, cadre légal pour des actions "interdites" (Red Team), communauté soudée (conférences : **SSTIC, LeHack, Hexacon, THCon**), pas mal de techno différentes.

— **Inconvénients :** difficile de déconnecter, périmètre pas interessant (site statique...), redaction de rapports peu stimulant, gerer les clients difficile (ne répondent pas, changements de dernières minutes, lorsque l'audité n'est pas le client...)

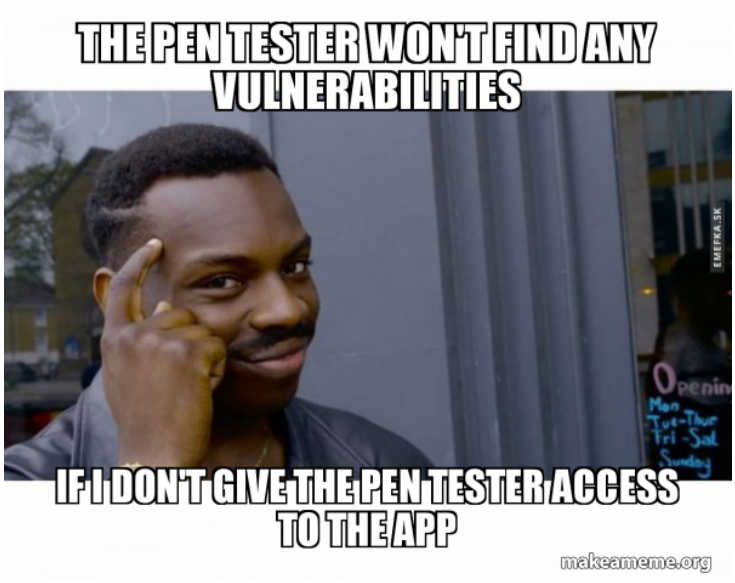
— **Évolutions :** Spécialisation technique pointue, Management d'équipe, passage vers la **Réponse à Incident** ou poste de **RSSI**.

VII. Ressources de Veille et Formation

— **Plateformes :** TryHackMe, PortSwigger Academy, Pentester Lab.

— **Sources de veille :** Blog Synacktiv, Qualys, ipp-sec.rocks, CTFtime.

— **Active Directory :** Zer1t0 (Attacking AD), GOAD (Game of Active Directory).



Pierre Yves Bonnetain (Juridique)

I. RÉPONSE À INCIDENT (MÉTHODOLOGIE)

Étapes Clés :

- **Détection/Qualification :** Réaliser l'attaque via alertes (utilisateurs, outils supervisés). Différencier **panne** et **attaque** (escalade rapide).
- **Analyse :** Circonscrire la cible, identifier les vecteurs, le "patient zéro" et les acteurs. Nécessite **autorité absolue** et **prudence** (éviter perte de traces).
- **Résolution :** Cohabiter ou éjecter l'intrus (attention aux représailles). Résoudre l'incident et gérer la **communication de crise** (interne/externe).
- **Restauration :** Restaurer la confiance. Mise sous observation globale. Analyser le chemin de l'incident pour la **résilience** future.

Le Trilemme de l'Urgence : Choisir 2 parmi : **Prudence**, **Auditabilité**, **Rapidité**.

II. CAS PRATIQUE : INTRUSION SERVEUR WEB

Contexte : E-commerce, flux > 100 commandes/jour, système critique (> 80% CA).

- **Failles initiales :** Pas de maintenance OS, code source uniquement sur serveur, fournisseur disparu, pas de maîtrise interne.
- **Paiement :** Collecte TLS → chiffrement local (clé publique) → stockage → déchiffrement back-office (clé privée).
- **Alerte :** Rejets massifs de CB en opposition signalés par le **SAV** (utilisateurs).

Investigations :

- **Contrainte :** Analyse "à chaud" via réseau (impossible d'arrêter la machine ou copier le disque). Risque de **rootkit** masquant les traces.
- **Traces applicatives :** Modification de classes PHP pour écrire les numéros de CB en clair dans des fichiers.
- **Artefacts :** Dossier `/tmp/.enl` contenant `e2.c` (exploit *linux-sendpage* pour **privesc root**) et un script `zz.txt`.
- **Vecteur d'entrée :** Injections SQL triviales identifiées dans les logs (200 OK).
- **Compromission complexe :** Utilisation d'un **chargeur** (PHP téléchargeant `abcd.php` depuis un serveur russe) et d'un **webshell** (KA_ushell modifié sans auth).
- **Bilan :** Authentification admin contournée via `LIKE` dans la requête SQL (injection triviale). Exfiltration des sources via `tar.gz`.

III. RANSOMWARES ET VARIANTES

Mode Opératoire Classique :

- **Phases :** Reconnaissance → Escalade → Chiffrement (fichiers locaux et partages réseau/sauvegardes).
- **Double/Triple Extorsion :** 1. Chiffrement. 2. Exfiltration (menace de revente). 3. Pression RGPD (menace CNIL). 4. Pression sur les clients/individus.
- **Vecteur :** E-mail (PJ malveillante ou URL) → Téléchargeur → Malware final.

Le Cas NotPetya (2017) :

- **Propagation :** EternalBlue, PowerShell, WMI.
- **Vecteur original :** Mise à jour corrompue du logiciel comptable **M.E.Doc** (Ukraine). Pas de signature cryptographique des MAJ.
- **Spécificité :** Malgré l'apparence d'un ransomware (demande de 308$ BTC), c'est un **logiciel destructeur** (wiper). La clé de déchiffrement n'est jamais exfiltrée.
- **Assurances :** Refus de remboursement fréquent car classé comme **"acte hostile/guerre"** (attribution Russie par la NSA).

IV. COLLECTE DE PREUVES

Enjeux Juridiques :

- La preuve technique doit être **licite**, **pérenne** et **construite** sans erreur.
- **Anticipation :** Nécessité d'avoir préparé la collecte avant l'incident.
- **Précautions :** Crucial si procédure tribunal (pénal/civil). Garder les archives projets (mails, CR) même après livraison.

I. Traces et Journalisation

Fondamentaux

- **Types de traces : Directes** (liées explicitement à l'activité : logs, fichiers ouverts/téléchargés) vs **Indirectes** (effets de bord : cookies, shellbags, artefacts, dates d'accès).
- **Collecte :** Directe (doit être organisée en amont, incluse dans les chartes) ; Indirecte (longue et coûteuse, faite au besoin).
- **Légalité (RGPD) :** Existence officielle, finalité connue, durée de conservation définie. Risque de **non-opposabilité** ou d'effet **boomerang** (surveillance illicite) si collecte irrégulière.
- **Criminalistique :** Principe de **Locard** (tout acte laisse des traces et l'individu en emporte).

II. Analyse Forensique (Inforensique)

Objectifs et Méthodes

- **Périmètre :** Analyse d'ordinateurs, réseaux, codes, données/artefacts et mobiles.
- **Utilité :** Litiges commerciaux, crimes/délits (outil au centre ou contenant des preuves), réponse aux incidents.
- **Expertise judiciaire :** Apporter des réponses précises pour éclairer le magistrat.
- **Conservation :** Geler la situation (séquestre par commissaire de justice). Conservation dans l'état d'origine (non altéré).

III. Analyse d'Ordinateurs

Préparation et Système

- **Copie bit-à-bit :** Extraction du disque (SSD parfois soudé) et copie intégrale avant analyse.
- **Environnement système :** Dates d'installation, comptes (cachés/actifs), logiciels installés/effacés, historique USB, réseaux Wifi.
- **Horodatage :** Dates de création, modification et dernier accès. Attention à la **granularité** (dépend du système de fichiers).

Fichiers et Récupération

- **Corbeille :** Fichiers renommés/déplacés mais non effacés (propriétaire et date de suppression identifiables).
- **Exhumation (Data Carving) :** Récupération de fichiers après vidage de corbeille.
- **États de récupération : Intégrale** (blocs libres non réutilisés) ou **Partielle** (écrasement partiel par de nouvelles données).

IV. Analyse de Téléphones Mobiles

Marché et Cadre Légal

- **Répartition :** Environ 75% Android / 25% iOS. Existence de téléphones ultra-sécurisés (ex : Encrochat).
- **Art. 226-3 CP :** Interdiction de détenir/vendre des outils d'extraction sans autorisation de l'**ANSSI** (renouvelable tous les 3 ans).

Sources de Données

- **SIM :** ICCID, IMSI, contacts, SMS (téléphonie classique).
- **Mémoire Interne/SD :** Photos, vidéos (métadonnées **EXIF/GPS**), bases SQLite, messageries instantanées (souvent > 10 000 messages).
- **Opérateur (Fadettes) :** Factures détaillées (limitées à 1 an), relais téléphoniques utilisés.

Géolocalisation

- **Par relais :** Zone de présence (maillage fin en ville, étendu en campagne).
- **Par appareil :** GPS précis (dizaine de mètres), bornes Wifi, appairage Bluetooth (voiture).

V. Procédure et Intégrité

Couper les liens

- **Risques téléphone allumé :** Réception de données (écrase les traces), verrouillage/effacement à distance, fuite vers le cloud.
- **Solutions :** Cage de Faraday, mode avion instrumenté, brouilleurs (attention : **prohibés** par l'Art. L33-3-1 sauf dérogation défense/justice).

Procédure Pénale

- **Enquête de flagrance :** < 48h (extensible 2x7j), sous contrôle du procureur.
- **Enquête préliminaire :** Après 15 jours de flagrance.
- **Information judiciaire :** Désignation d'un juge d'instruction, commission rogatoire. L'expert peut intervenir à toutes les étapes.

ANNALES :

Est-ce qu'on peux surveiller un employé ?
Est-ce qu'on peux récupérer le contenu d'un disque dur pour une enquete et comment et selon quelles limites ?
3 elements infractions pénales : l'élément légal, l'élément matériel, l'élement moral
Forensique : pénal, civil, social

Gilles Trouessin (Securite sante)

1. Concepts Fondamentaux (DICA) La **Sécurité-Security** (Immunité) vise à garantir que les informations sont manipulées de façon autorisée via 4 propriétés clés :

- **Disponibilité** : Accessibilité, pas de rétention/blocage.
- **Intégrité** : Correction, pas d'altération/modification.
- **Confidentialité** : Pas de divulgation non autorisée.
- **Auditabilité** : Preuve (traçabilité, imputabilité, irréfutabilité).

2. Sûreté de Fonctionnement (Laprie) Propriété permettant une **confiance justifiée** dans le service. Elle inclut :

- **Fiabilité** : Continuité de service.
- **Maintenabilité** : Aptitude à être réparé.
- **Sécurité-Innocuité (Safety)** : Absence de défaillances catastrophiques pour les personnes/biens.

3. Confidentialité : Discrétion vs Séclusion

- **Discrétion** : Protection électronique (cryptographie réversible, clés symétriques/asymétriques).
- **Séclusion** : Volonté d'anonymat (irréversible).
- **Anonymat vrai** : Irréversibilité totale prouvée.
- **Pseudo-anonymat** : Remplacement par numéros muets (réversible via voie légale).

4. La Pyramide de la Sécurité Action sur 3 niveaux indissociables :

1. **Personnes** : Responsabilités, "qui fait quoi".
2. **Organisations** : Procédures, meilleures pratiques.
3. **Technologies** : Outils techniques et référentiels.

5. Management des Risques (ISO 27005) Processus universel itératif : **Contexte** → **Appréciation** (Identification, Analyse, Évaluation) → **Traitement** → **Acceptation des risques résiduels**.

- **Protection** : Réduit l'impact (minimisation).
- **Prévention** : Réduit la vraisemblance (mitigation).

6. Structure Documentaire (PSSI) Hiérarchie calquée sur le droit français :

- **PSSI-g (Macro)** : Orientations **Politiques**, document de 2-3 pages pour toute la collectivité.
- **PSSI-d (Midi)** : Orientations **Stratégiques**, 20-30 pages pour les directions-métiers.
- **PSSI-o (Mini)** : Orientations **Tactiques**, 5-10 pages, procédures opérationnelles.

7. Normes et Standards

- **ISO 27001** : Système de Management (SMSI).
- **ISO 27002** : Recueil de bonnes pratiques (14 domaines : RH, actifs, accès, crypto, physique, etc.).
- **ISO 27799** : Adaptation de l'ISO 27002 au secteur **Santé**.
- **RGPD** : Protection des données à caractère personnel (Privacy).
- **HDS** : Hébergement des Données de Santé (Certification/Agrément).

8. Solutions Spécifiques Santé

- **Authentification forte** : Utilisation de la carte **CPS** (Carte de Professionnel de Santé).
- **Échanges** : Messageries sécurisées (ex : MSSanté).
- **Identité** : Distinction entre identité directe, indirecte et informations ré-identifiantes.

9. Triptyque de Mise en Œuvre

- **Juridique** : Loi Informatique & Libertés, conformité CNIL.
- **Organique** : Structures, gouvernance, formation.
- **Technique** : Chiffrement, signature, pare-feu, anti-virus.

10. Enjeux de Réputation Sondage : **83%** des clients arrêtent toute relation après une fuite de données. La transparence "privacy" est le 3ème critère de choix (**68%**) après l'expérience et la réputation.

- **Acteurs & Sujets :** Patients, familles, offreurs de soins, autorités (Nat/Rég/Loc), assureurs (AMO/AMC), réseaux de soins.
- **Objets :** Dossier de santé informatisé, Systèmes I.T., flux d'information.
- **Cadre Légal :** Éthique, déontologie, lois/décrets (UE et National).
- **Modèles de Politique :** DAC, MAC, RBAC, OrBAC.
- **Piliers D.I.C.A. :** Disponibilité, Intégrité, Confidentialité, Auditabilité.

Propriétés et Besoins (ENV13608-1)

4 Propriétés / 10 Besoins Conceptuels / 25 Besoins Contextuels

- **D (Disponibilité) :** Accessibilité des objets, fiabilité des sujets. Exigences : redondance, backup temps réel, archivage ligne.
- **I (Intégrité) :** Complétude et exactitude des objets/-sujets. Outils : Checksum numérique, signature électronique.

- **C (Confidentialité) :** Transport et contexte. Notions : discrétion, anonymat, séclusion (vie privée).
- **A (Auditabilité) :** Privilèges, envoi, remise, échange (Traçabilité/Imputabilité).

Taxonomie de l'Anonymisation

Objectifs : Dépersonnalisation (#1), Pseudonymisation (#9), Occultation.

- **Robustesse :** Résistance à l'inversion (directe/indirecte) et à l'inférence (déductive, inductive, abductive, adductive).
- **Chaînage (Variantes) :**
  - **Spatial :** Local, Régional, National.
  - **Temporel :** Ponctuel, Annuel, Éternel.
  - **Spatio-temporel :** Ubiquité, Coordination, Coopération.
- **Réversibilité :** Techniques réversibles vs irréversibles (diversification/hétéronymisation).

Management de la Sécurité (ISO 27001/27002)

- **Management vs Gestion :** Manager implique vision stratégique et direction ; Gérer est un suivi opérationnel.
- **Processus :** Cycle d'amélioration continue basé sur la gestion du risque.
- **Secteur Santé :** Nécessité de pragmatisme (éviter les "usines à gaz"), respect de la culture soignante, focus sur l'innocuité des soins.

Architecture Technique & TTP (Tierces Parties de Confiance)

Services de Confiance (Interopérabilité) :

- **PKI (Public Key Infrastructure) :** Gestion des clés, certificats, autorités de certification.
- **TTP Fonctions :** Signature élec., Non-répudiation, Horodatage (Timestamping), Archivage sécurisé.
- **Protocoles :** DH (Diffie-Hellman), RSA.
- **Conventions Cryptographiques :**
  - **Distribuées :** Clés échangées/délivrées.
  - **Partagées :** Coordonnées (implicites) ou autonomes (explicites).
  - **Communes :** Négociées (proposées/adaptées) ou imposées (adoptées).

Flux et Domaines de Santé

- **Domaines :** Santé Publique, Gestion Admin/Financière (CPAM/Remboursements), Prévention & Soins, Recherche Clinique.
- **Sécurisation des Flux :** Protection authenticité flux AMO/AMC, anonymisation irréversible des trajectoires de soins (hospitalier), confidentialité extraits dossiers entre P.S.
- **Contraintes :** Droit d'accès (CNIL), Droit à l'oubli (patient) vs Droit de défense (soignant), Secret Médical (ordre public).

Normes et Standards par Niveaux

- **International :** ISO/IEC 27001, 27002, Common Criteria, ISO TC215, IETF.
- **Européen :** CEN TC251 (WGiii), ETSI, ITSEC, OCDE.
- **National (France) :** AFNOR, CNIL, ANS (ex-ASIP), GIP-CPS, GIP-DMP, GIE S/V.

Points de Vigilance QCM :

- **Consentement :** Doit être exprès pour les services au patient.
- **Traçabilité vs Opposabilité :** Compromis entre respect de l'intimité et preuve médicale.
- **DMP :** Risques liés à la mauvaise application cryptographique et impacts irréparables sur la vie privée.