

Cahier de laboratoire

Suivi individuel - Conception et opération de la sécurité

AUTEUR

Yanis Amani

SEMESTRE

Automne

MODULE

3275.1 · 3275.2

MISE À JOUR

2026-10-17

Objet : progression et maîtrise des compétences - problématiques rencontrées, travaux effectués et résultats, recherches documentaires complémentaires.

Sommaire

1. Contexte	2
2. Séance du 18 septembre 2026 : découverte et auto-évaluation	3
2.1. Exercice 1 : Auto-évaluation initiale	3
2.2. Exercice 2 : Critères principaux et secondaires	5
2.3. Exercice 3 : Évaluer la triade CIA sur des cas concrets	6
2.4. Exercice 4 : Principaux secteurs, domaines et objets d'application	7
2.5. Activité 4 : Aspect humain, risques et biais cognitifs	9
2.6. Activité 1 : Évaluer ses compétences actuelles comme DevSecOps	11
2.7. Activité 3 : Protection concrète d'un WordPress (Ricardo)	14
2.8. Activité 2 : Recommandations d'organismes de sécurité	15
2.9. Activité 5 : Définir le vocabulaire de base de la cybersécurité	19
2.10. Activité 6 : Rôle de responsable de la sécurité d'une entreprise	21
2.11. Activité 7 : Pourquoi la surface d'attaque du kernel Linux est devenu récemment un problème ? Que faire (cas : opérateur cloud) ?	24
2.12. Travail personnel : ISO 27001	26
2.13. Synthèse de la séance	28
3. Séance du 25 septembre 2026	30
3.1. Exercice 5 : Inventaire des moyens/mesures techniques de la cybersécurité	30
3.2. Exercice 6 : Que sont les menaces ? D'où proviennent-elles ? Exemples ? ..	30
3.3. Exercice 9 : Sensibilisation aux zones d'ombres liées à l'inventaire des menaces	31
3.4. Exercice 11 : Exemple d'analyse de risque simplifiée	32
4. Séance du 2 octobre 2026	33
4.1. Activité 8 : Résumer les formes courantes de cybercriminalité et leurs conséquences	33
4.2. Intervention Pascal Linder	34
4.3. Activité 9 : Que faire dans Concevoir, Valider et Opérer (cas : une entreprise) ?	38
5. Séance du 9 octobre 2026	40
5.1. Activité 10 : Qu'est-ce qui alimente la veille cybersécurité et technologique ?	40
5.2. Activité 11 : Schéma général conception et opération de la sécurité	42

Contexte

Cahier tenu au jour le jour pour les modules 3275.1 et 3275.2 (semestre d'automne).
Chaque entrée date le travail fait, ses résultats et les notes en vrac.

Séance du 18 septembre 2026 : découverte et auto-évaluation

Énoncés partagés : Exercices partagés (Google Docs). Ci-dessous, les exercices personnels réalisés en séance.

Objectifs

Poser mes bases en sécurité : évaluer mon niveau initial, maîtriser la triade CIA et ses terrains d'application, me situer en DevSecOps, comprendre le facteur humain et décortiquer ISO 27001.

Le matin pose les fondations : auto-évaluation chiffrée (exercices 1), triade CIA et critères secondaires (exercices 2 et 3), puis secteurs et échelles d'application (exercice 4). L'après-midi resserre sur la pratique : positionnement DevSecOps via CI/CD et roadmap (activité 1) et facteur humain avec six familles de biais et leurs mitigations (activité 4). Le travail personnel décortique ISO 27001 : périmètre SMSI, risques top-down, SoA et cycle PDCA. L'activité 3 traite de la veille OSINT autorisée, du recensement de serveurs WordPress et du recul sur les protections.

2.1. Exercice 1 : Auto-évaluation initiale

Objectifs

- Poser une base chiffrée de mon niveau initial en sécurité.
- Noter chaque thème de 1 à 5.
- Repérer mes forces et mes lacunes avant le semestre.

2.1.1. Métiers pertinents

- **Tous les métiers** : point de départ commun avant de parler sécurité.
- **Exemples** : développeur, admin systèmes/réseau, chef de projet.

2.1.2. Déroulement

- Noter de 1 à 5 mon niveau sur chaque thème.
- Recopier le tableau, puis le remplir pendant la séance.

Thème	1 à 5
Compréhension générale des enjeux de la sécurité (pourquoi c'est important, quels types de menaces existent, comment les traiter)	4
Compréhension des thèmes déjà vus - niveau théorique	3
Mise en pratique de ces thèmes - niveau appliqué	3
Conscience de la sécurité quand je conçois / développe / maintiens un projet (y compris contributions open source éventuelles)	4

Réflexes de développement sécurisé concret	3
Gestion des risques (avoir déjà dû, même informellement, déterminer les menaces puis évaluer les risques / impacts d'un choix, par exemple technique)	3
Outils cryptographiques (compréhension et usage régulier)	4
Confinement OS et réseaux (sandboxing, segmentation réseau, etc.)	2
Conscience des risques liés au facteur humain (ingénierie sociale, phishing)	5
Suivi de sources d'information sécurité (blogs, mailing-lists, CVE, etc.) de logiciels spécifiques, de plateformes spécifiques, ou générales	4
Envie d'appliquer ce que je vais apprendre en 3275.1 et 3275.2 (semestre d'automne) dans mon projet de semestre	4

2.1.2.1. Questions de synthèse

Thème le plus à l'aise : le facteur humain (5/5). Je suis beaucoup d'histoires de hacking, et le constat revient sans cesse : phishing et ingénierie sociale restent la faille la plus simple, bien avant la technique pure.

Thème à progresser en priorité : le confinement OS et réseaux (2/5). Je connais mal le sandboxing et la segmentation, alors que le sujet m'intéresse ; c'est là que la marge de progrès est la plus grande.

Entreprise vs développement logiciel : la distinction est claire pour moi. L'entreprise intègre plus de variables humaines, donc plus de points d'attaque et de défense. Elle tient aussi compte des contraintes de gestion : ressources, budgets, activités, politique interne. Pour mon projet, il s'agit d'analyser les menaces et d'appliquer la sécurité à chaque étape du cycle de vie, avec un confinement adapté aux risques et impacts.

2.1.3. Résultats

Profil déséquilibré entre culture et technique :

- **5 :** facteur humain.
- **4 :** enjeux généraux, cryptographie, conscience dev, veille, envie d'appliquer.
- **3 :** théorie, pratique, réflexes de dev sécurisé, gestion des risques.
- **2 :** confinement OS et réseaux, mon seul vrai trou.

En bref, je sais pourquoi on se fait attaquer, je sais moins comment cloisonner proprement.

2.1.4. Interprétation des résultats

Mon point d'appui est la sensibilisation, avec le réflexe de me méfier du maillon humain. Mon chantier est le confinement : sandboxing, segmentation, moindre privilège. Pour le projet de semestre, je vise donc la confidentialité et l'intégrité par la technique, pas seulement par la vigilance. Je mesurerai le progrès en refaisant cette grille en fin de module.

2.2. Exercice 2 : Critères principaux et secondaires

Objectifs

- Distinguer les trois critères principaux CIA.
- Identifier les critères secondaires qui les rendent applicables : identification et traçabilité, authentification, sensibilisation, résilience.

2.2.1. Métiers pertinents

- **Tous les métiers** : chaque rôle arbitre entre ces critères à son niveau.
- **Exemples** : développeur, administrateur, RSSI.

2.2.2. Déroulement

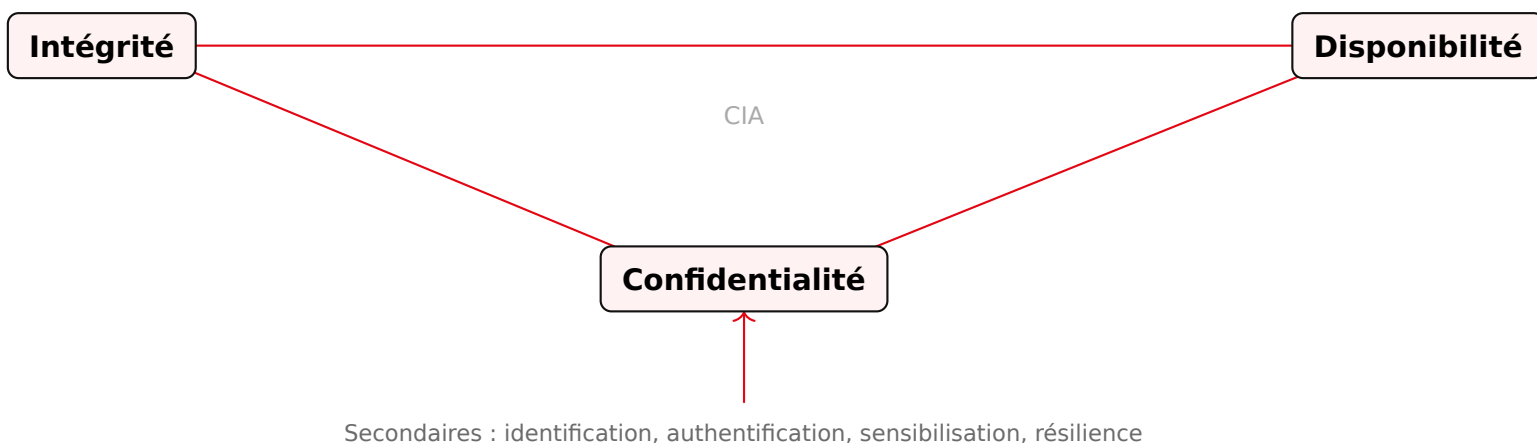
Critères rappelés en cours, notés en vrac.

Critères principaux :

- Confidentialité
- Intégrité
- Disponibilité

Critères secondaires :

- Identification :
 - Responsable / traçabilité → non-répudiation / imputabilité
 - Accès
- Authentification
- Sensibilisation
- Résilience



2.2.3. Résultats

Les trois critères principaux (confidentialité, intégrité, disponibilité) forment le triangle du schéma. Quatre critères secondaires l'entourent et le rendent applicable : l'identification (avec traçabilité et accès), l'authentification, la sensibilisation et la résilience.

2.2.4. Interprétation des résultats

Les critères secondaires sont plus concrets que la triade seule. Côté développeur, authentification et traçabilité apparaissent dans chaque login et chaque journal. Côté

admin, la résilience se joue dans les sauvegardes et la reprise après incident. Pour le projet de semestre, je justifierai chaque mesure par le critère qu'elle protège.

2.3. Exercice 3 : Évaluer la triade CIA sur des cas concrets

Objectifs

- Appliquer la triade CIA à quatre cas réels.
- Justifier chaque note de 1 à 4.
- Comparer les profils pour voir quel critère domine selon le secteur.

2.3.1. Métiers pertinents

Tous les métiers sont concernés, avec un poids différent selon le cas :

- **Banque** : RSSI, analyste risques.
- **AlertSwiss, streaming** : administrateur réseau.
- **E-commerce** : développeur.

2.3.2. Déroulement

- Noter de 1 à 4 (maximum) la confidentialité (C), l'intégrité (I) et la disponibilité (A) de chaque cas.
- Recopier le tableau, puis le remplir.

Cas	C	I	A
Site d'e-commerce	3	3	3
Banque en ligne suisse	4	4	4
Diffusion message AlertSwiss	1	4	4
Service de streaming vidéo	2	2	4

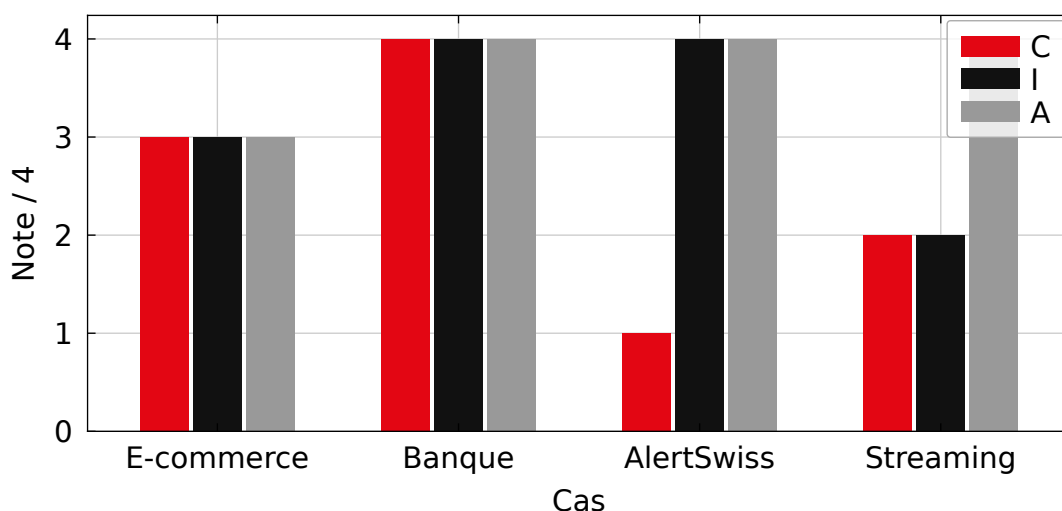


Fig. 1. - Notes C-I-A par cas (1 à 4). Rouge : C, noir : I, gris : A.

Justification des notes :

- **E-commerce (3/3/3)** : I et A sont élevés, car une commande modifiée ou une minute d'indisponibilité coûte directement de l'argent. C est à 3 : données clients et paiement, sans atteindre le niveau d'une banque.

- **Banque en ligne (4/4/4) :** C et I sont prioritaires (données financières, exactitude des opérations). A est aussi à 4 dans mon évaluation, car l'accès continu est attendu. Les contraintes légales influencent ces objectifs, sans imposer à elles seules la note maximale.
- **AlertSwiss (1/4/4) :** C est à 1, les messages étant publics. I est à 4, car une fausse alerte peut provoquer une panique. A est à 4, car le message doit passer en pleine crise.
- **Streaming (2/2/4) :** C et I sont à 2 (catalogue public, image corrompue peu coûteuse). A est à 4, car un service qui rame fait fuir les abonnés.

2.3.3. Résultats

La banque présente le profil maximal (4/4/4) et l'e-commerce un profil équilibré (3/3/3). AlertSwiss et le streaming partagent le même contraste : une confidentialité basse (1 et 2) face à une disponibilité à 4. Ce qui les sépare est l'intégrité, maximale pour AlertSwiss, moyenne pour le streaming.

2.3.4. Interprétation des résultats

Chaque profil impose une priorité de conception différente :

- **Banque :** prioriser C et I, tout en maintenant A.
- **AlertSwiss :** protéger l'authenticité du message et sa diffusion en pleine crise.
- **Streaming :** dimensionner l'infrastructure pour absorber la charge du soir.

Le lien avec ISO 27001 est direct : la note dépend du contexte, comme dans l'analyse de risques, et la SoA (déclaration d'applicabilité) trace ensuite ce choix.

2.4. Exercice 4 : Principaux secteurs, domaines et objets d'application

Objectifs

- Recenser où la sécurité s'applique et qui elle concerne.
- Distinguer secteurs public, privé et domaines transverses.
- Situer les échelles moi, nous et tous.

2.4.1. Métiers pertinents

- **Admin systèmes et réseau :** infrastructures critiques, OT.
- **Développeur :** cloud, logiciels.
- **RSSI :** entreprise.
- **DPO :** dossiers patients, fiscalité.
- **Ma position :** côté dev, je construis une partie des services que les autres protègent.

2.4.2. Déroulement

Secteur public :

- Défense et sécurité nationale : armée, renseignement, police, protection civile.
- Santé publique : hôpitaux, services d'urgence, dossiers patients.
- Administrations et collectivités : état civil, fiscalité, vote, services en ligne.
- Éducation et recherche : universités, laboratoires, données scientifiques.
- Infrastructures critiques : énergie, eau, transports, télécommunications.
- Justice : tribunaux, casiers, preuves numériques.

Secteur privé :

- Entreprises : PME et grands groupes, secrets industriels, SI interne, postes de travail.
- Objets protégés : contrats, comptabilité, propriété intellectuelle, continuité d'activité.

Domaines transverses, au global :

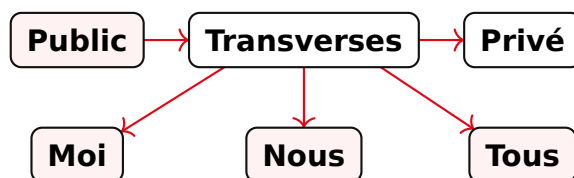
- Santé et pharmaceutique : dispositifs médicaux, essais cliniques, brevets, chaînes de production.
- Informatique et technologique : cloud, logiciels, matériel, opérateurs télécoms, prestataires.
- Finance et assurance : banques, paiements, données clients.
- Industrie et énergie : OT (technologies opérationnelles), SCADA, chaînes logistiques.

Qui est concerné ?

- Moi : mes comptes, mes appareils, mes projets de développement.
- Nous : l'entreprise ou l'équipe où je travaille, ses clients et ses fournisseurs.
- Tout le monde : chaque citoyen utilise des services dont la compromission a un impact collectif.

2.4.3. Résultats

Le secteur public couvre la défense, la santé, l'état civil, la justice et les infrastructures critiques (énergie, transports). Le secteur privé protège le SI interne, les contrats, la comptabilité et la propriété intellectuelle. Les domaines transverses relient les deux : dispositifs médicaux, cloud, banques, SCADA. Je suis concerné à chaque échelle : moi par mes comptes et mes projets, nous par mon équipe et ses clients, tous par les services collectifs que chaque citoyen utilise.

**2.4.4. Interprétation des résultats**

Aucun secteur ne fonctionne sans sécurité. Hôpital, banque et chaîne logistique protègent des objets différents, mais une compromission bloque leur activité de la même façon. Côté dev, chaque ligne de code atterrit dans un de ces secteurs : une faille dans une app de vote ou de paiement ne reste jamais théorique. À l'échelle nationale et des alliances, la cybersécurité conditionne le fonctionnement de la société, car une compromission peut toucher des services essentiels dans plusieurs pays à la fois.

Pour le projet de semestre, le périmètre se fixe en trois questions :

- Qui utilise le service ?
- Que protège-t-il ?
- Que coûterait une compromission à chaque échelle ?

2.5. Activité 4 : Aspect humain, risques et biais cognitifs

Objectifs

- Comprendre les biais cognitifs qui affectent la sécurité.
- Savoir les repérer et les limiter.
- Comprendre pourquoi ils changent selon la personne et la culture.

2.5.1. Métiers pertinents

Tous les métiers sont concernés : RSSI, auditeur, chef de projet, développeur. La sensibilisation n'est pas un bonus, c'est une mesure de réduction du risque.

2.5.2. Déroulement

2.5.2.1. Risques et biais cognitifs liés au cerveau

Les heuristiques sont des raccourcis du cerveau, utiles au quotidien mais dangereux en sécurité. Elles produisent six types de biais :

Type	Description / impact sécurité	Stratégie spécifique
Sensori-moteurs	Fatigue visuelle, réflexes erronés sur une interface trompeuse, erreurs de frappe sous stress.	Design clair, pauses, automatisation des actions critiques.
Attentionnels	Surcharge, distraction, cécité au changement : une alerte ignorée dans un flux trop dense.	Limiter les alertes simultanées, hiérarchiser, automatiser le filtrage.
Mnésique	Mémoire sélective, faux souvenirs, oubli des procédures.	Registres d'incidents, procédures visibles, révision régulière.
De jugement	Confirmation, ancrage, disponibilité, optimisme : on valide une hypothèse et on rejette le contraire.	Avocat du diable, scénarios indépendants, données chiffrées.
De raisonnement	Attribution fondamentale, analogies erronées, logique binaire : on blame la personne au lieu du contexte.	Post-mortems sans blâme, analyse du contexte avant attribution.
Liés à la personnalité	Dunning-Kruger, conformisme, aversion au risque, anxiété.	Évaluation objective, mentorat croisé, diversité des profils.

2.5.2.2. Stratégies générales

- **Red teaming** : simuler l'attaque pour briser la confirmation.

- **Diversité cognitive** : mélanger profils et expériences pour contrer l'ancrage.
- **Hypothèses écrites** : documenter ce qu'on suppose et pourquoi, cela expose l'ancrage.
- **Processus standardisés** : cadres comme l'ISO 27001 réduisent la dépendance à la mémoire individuelle.
- **Psychological safety** : permettre de signaler une erreur sans sanction, cela limite la confirmation et l'attribution fondamentale.

Références : Biais cognitif, Heuristique de jugement.

2.5.2.3. Risques liés à une personne ou à une culture

Personne particulière :

- Traits : confiance excessive (Dunning-Kruger), anxiété, faible motivation → biais amplifiés.
- État : fatigue, stress, surcharge → tous les biais s'aggravent.
- Compétences : un expert réseau peut sous-estimer la cryptographie.

Stratégies individuelles : évaluation objective (tests, audits), adaptation des tâches, suivi de la charge, mentorat.

Culture :

- Culture du silence ou du blâme : on cache les erreurs, on renforce la confirmation.
- Culture hiérarchique : on ose pas contredire un supérieur → ancrage renforcé.
- Biais d'in-group : plus de confiance envers son propre groupe, vigilance réduite face à l'extérieur.
- Perception du risque : prévention collective vs. responsabilité individuelle.

Stratégies culturelles : post-mortems sans blâme, formation interculturelle, leadership exemplaire (la direction montre l'exemple), adaptation locale des messages.

Références : Biais de groupe, Psychological safety.

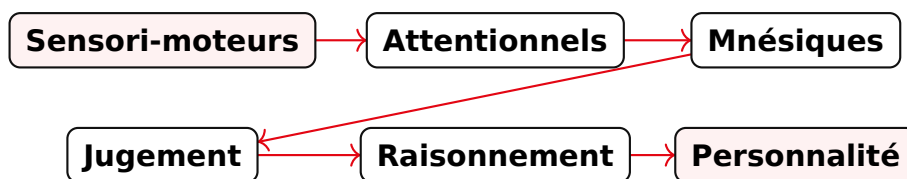
2.5.2.4. Activité 4 : Que faire pour limiter ces risques de prise de décision ?

- **Écrire les hypothèses avant de décider** : noter ce qu'on suppose et pourquoi, puis relire à deux, ce qui rend l'ancrage visible.
- **Faire relire par un profil différent** : un dev relit l'analyse d'un admin, ou l'inverse ; le red teaming joue le même rôle contre la confirmation.
- **Appliquer une procédure écrite** : checklists et cadres type ISO 27001 pour les actions critiques, au lieu de compter sur la mémoire.
- **Signaler sans être sanctionné** : post-mortem sans blâme, erreurs remontées vite, car le silence coûte plus cher que l'aveu.
- **Surveiller la charge** : pauses, rotation des tâches de vigilance, alertes hiérarchisées, car un opérateur fatigué clique et ignore.

2.5.3. Résultats

J'ai identifié six familles de biais, du sensori-moteur à la personnalité, chacune avec une stratégie précise. Les risques individuels tiennent à la fatigue, au Dunning-Kruger et à l'expertise partielle ; les risques collectifs, à la culture du blâme et à une hiérarchie qui verrouille la contradiction. Les mitigations suivent la même découpe : mentorat et suivi de charge pour l'individu, post-mortems sans blâme et leadership exemplaire pour le

collectif. J'en retiens cinq réflexes : hypothèses écrites, relecture croisée, procédures, signalement sans sanction, gestion de la charge.



2.5.4. Interprétation des résultats

Le facteur humain explique l'échec de mesures techniques pourtant correctes : un admin en surcharge ignore une alerte, un utilisateur confiant clique sur un lien. Comme ces risques varient selon la personne et la culture, la sécurité est un système sociotechnique, pas juste des pare-feu. La prochaine étape consiste à intégrer ces observations au projet de semestre : charge cognitive, culture d'équipe, diversité des points de vue.

2.6. Activité 1 : Évaluer ses compétences actuelles comme DevSecOps

Objectifs

- Mettre au clair mes compétences actuelles et mes lacunes, pour savoir où progresser.
- Prendre en compte formations suivies, expériences passées, connaissances théoriques et pratiques.

2.6.1. Métiers pertinents

DevSecOps.

2.6.2. Résultats

Mon expérience passe exclusivement par des pipelines CI/CD GitLab, sans intervention manuelle sur les vérifications. À chaque intégration, les outils d'analyse des langages vérifient compilation, style et typage, et remontent aussi une partie des vulnérabilités de sécurité. Je consulte en complément les rapports GitHub chaque semaine.

Je me suis positionné sur la roadmap DevSecOps de roadmap.sh (captures ci-dessous) : les nœuds barrés sont acquis, le reste est à explorer.

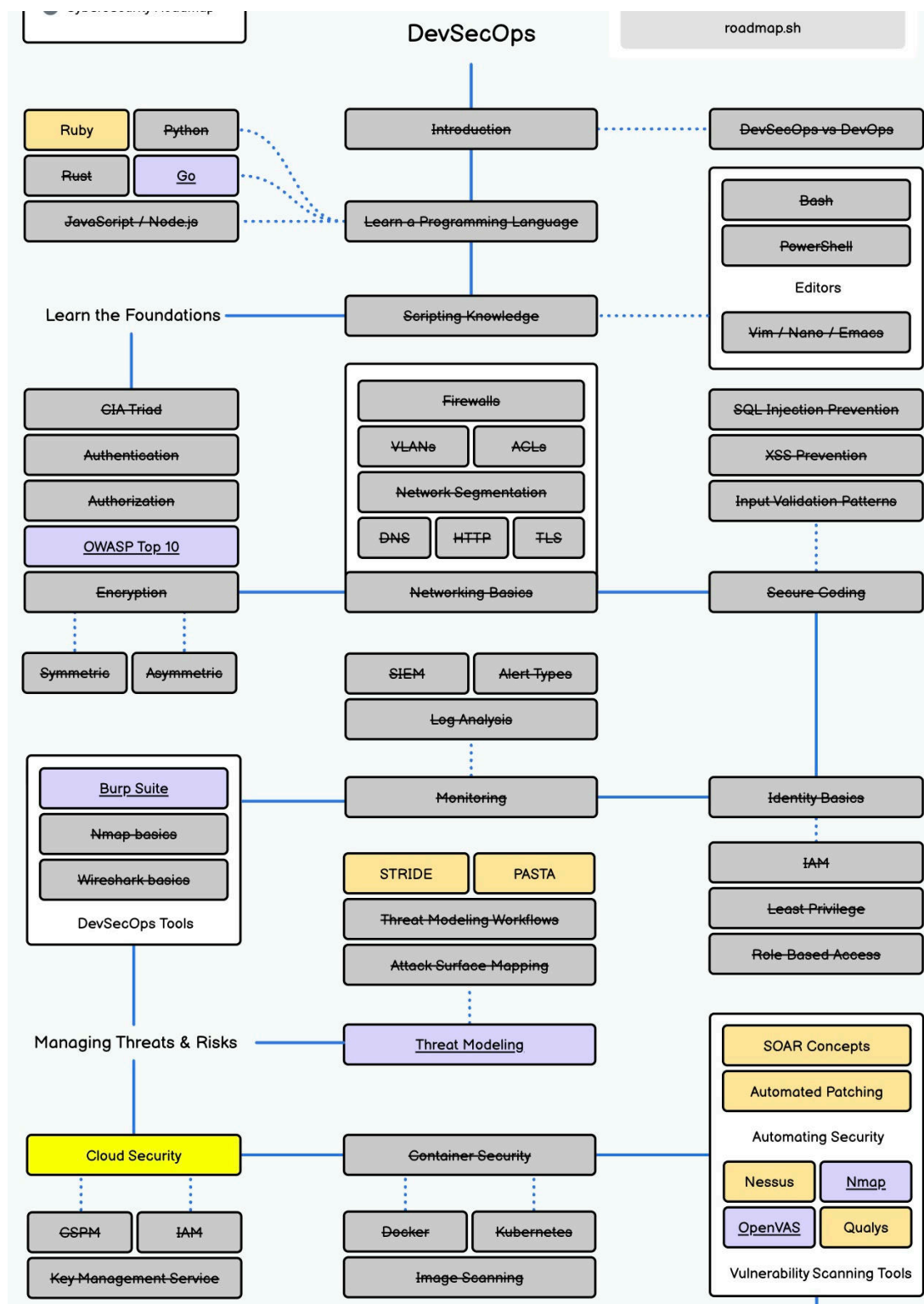


Fig. 2. – Auto-positionnement sur le roadmap DevSecOps (roadmap.sh) - partie 1 : acquis barrés.

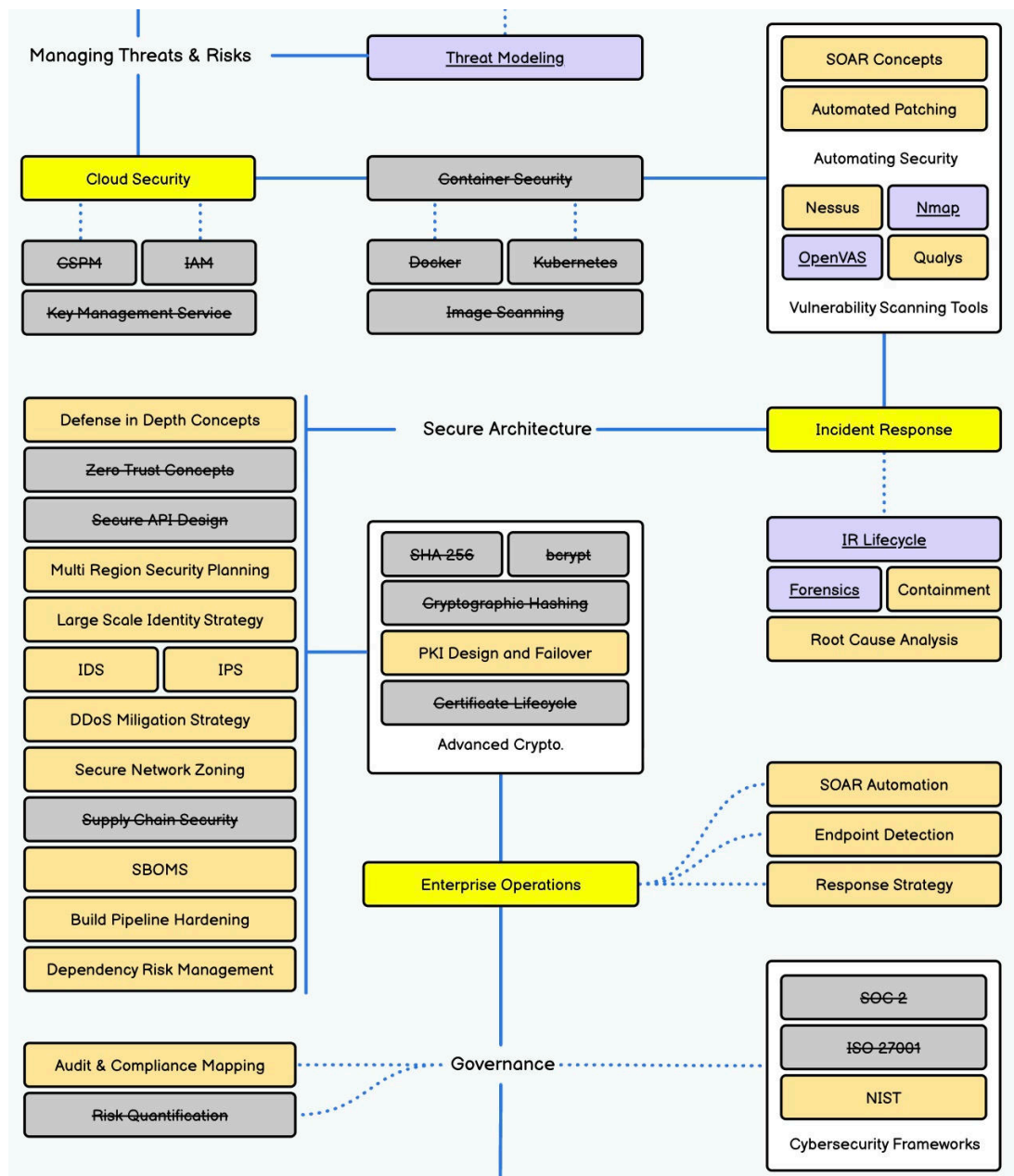


Fig. 3. – Auto-positionnement sur le roadmap DevSecOps (roadmap.sh) - partie 2 : acquis barrés.

2.6.3. Interprétation des résultats

- **Partie 1, socle acquis** : langages et scripting, triade CIA, cryptographie de base, réseau, secure coding, monitoring et identité, conteneurs.
 - Exception crypto : design et failover d'une PKI non acquis.
- **Partie 2, trois blocs presque entièrement non acquis** :
 - **Incident Response** : cycle IR, forensics, containment, root cause analysis.
 - **Secure Architecture** : defense in depth, zoning réseau, IDS/IPS, anti-DDoS, SBOM, durcissement du pipeline, risque des dépendances.
 - Exceptions acquises : Zero Trust, Secure API Design, Supply Chain Security.
 - **Enterprise Operations** : automatisation SOAR, EDR, stratégie de réponse.

Ce bilan recoupe mon auto-évaluation : une culture générale solide, une lacune sur le cloisonnement et l'opérationnel. Mon expérience CI/CD automatise la détection, mais ne

couvre ni la réponse à incident ni l'architecture à grande échelle. La feuille de route en découle : socle acquis, deux blocs à construire, exploitation à viser.

Socle acquis → **Incident Response** → **Secure Architecture** → **Enterprise Ops**

Prochaine étape : prioriser Secure Architecture et Incident Response, puis compléter par du DAST, de l'analyse de dépendances et une revue de conception en amont.

2.7. Activité 3 : Protection concrète d'un WordPress (Ricardo)

Objectifs

- Recenser des serveurs WordPress par OSINT et intelligence collective.
- Simuler une attaque générique puis ciblée, dans un cadre autorisé.
- Évaluer les protections mises en place.
- Durée indicative : 30 minutes.

2.7.1. Métiers pertinents

- **Analyste OSINT** : collecte des indices.
- **RSSI** : arbitrage.
- **Administrateur WordPress** : mises à jour.
- **SOC** : surveillance.
- **Équipe blue** : applique les contrôles.
- **Équipe red** : décrit seulement les scénarios de l'adversaire.

2.7.2. Déroulement

- **Cadre** : site fictif de Ricardo, autorisation écrite, périmètre limité aux sources passives.
- **Sources croisées** : index publics, pages d'archives, certificats, annonces du propriétaire.
- **Méthode** : qualifier chaque indice, partager uniquement les informations nécessaires.
- **Règle** : une concordance reste une hypothèse à confirmer par le propriétaire, jamais une preuve de vulnérabilité.

Protection	Contrôle	Effet
Inventaire et mises à jour	Référencer WordPress, extensions et thèmes ; corriger les écarts.	Moins de composants exposés.
MFA et moindre privilège	Protéger l'administration par un second facteur et limiter les comptes.	Accès compromis moins étendu.
Segmentation et WAF	Restreindre l'administration et filtrer les requêtes anormales.	Moins d'exposition et de propagation.
Sauvegardes testées	Sauvegarder le site et la base, puis tester la restauration.	Rétablissement plus rapide.
Journalisation et alertes	Centraliser les événements et qualifier les alertes.	Détection et analyse des faux positifs.

2.7.3. Temps 1 : Recensement passif de serveurs WordPress

- Rapprocher les signaux publics, contrôler les dates, supprimer les doublons.
- Conserver pour chaque ressource : source, indice, niveau de confiance.
- Faire confirmer les correspondances par le propriétaire.
- Aucun scan actif, aucune cible réelle testée.

2.7.4. Temps 2 : Attaque générique puis ciblée

La campagne générique recherche des erreurs de configuration, des composants obsolètes et des accès d'administration. Le WAF et les journaux signalent alors une activité répétée, et je vérifie les faux positifs avant de conclure. L'attaque ciblée utilise ensuite l'inventaire pour choisir le serveur le plus exposé ; MFA, moindre privilège et segmentation limitent l'accès et le mouvement vers la base. La réponse simulée enchaîne analyse, isolation et restauration. La simulation reste théorique : aucune commande, payload, credential ni exploitation réelle.

2.7.5. Résultats

- Un inventaire vérifiable de ressources candidates.
- Un scénario montrant l'effet de chaque protection : mises à jour, MFA, moindre privilège, segmentation, WAF, sauvegardes, alertes.
- Une simulation contenue, avec des écarts conservés et le besoin d'une réponse préparée.

2.7.6. Interprétation des résultats

La détection vient du croisement d'indices, pas d'une source isolée. La protection améliore la détection, limite la portée d'un incident et réduit le temps de rétablissement, mais elle ne garantit pas l'absence de compromission. Je retiens trois contrôles essentiels : un inventaire à jour, des faux positifs vérifiés, une restauration testée.

2.7.7. Références

- WordPress : Hardening WordPress
- NIST SP 800-61 Rev. 3 : Incident Response Recommendations

2.8. Activité 2 : Recommandations d'organismes de sécurité

Objectifs

- Résumer et référencer les recommandations de l'OFCS (Office fédéral de la cybersécurité, bacs.admin.ch) ou d'organismes similaires.
- Couvrir le phishing, le ransomware, le DDoS, les data leaks et les supply chains.
- Ajouter les menaces de l'écosystème open source et de Microsoft Exchange.

2.8.1. Métiers pertinents

- **RSSI** : pilote les mesures, arbitre les priorités.
- **SOC, blue team** : appliquent au quotidien.
- **Développeur** : sécurise le code et les dépendances.
- **Chef de projet** : planifie les backups et les playbooks.

2.8.2. Déroulement

Sept menaces, deux recommandations clés pour chacune :

Menace	Position OFCS / autre organisme	2 recos clés
Phishing	Menace n°1 en Suisse selon l'OFCS.	Passer par un favori, jamais par un lien. Activer la 2FA ou FIDO2.
Ransomware	Ne jamais payer selon l'OFCS et CISA.	Backup 3-2-1 offline et testé. Patcher et bloquer les macros.
DDoS	Tenir la charge avec le FAI selon l'OFCS.	Préparer les contacts FAI et un CDN. Activer SYN-cookies, WAF et GeolIP.
Data leaks	Notifier le PFPDT et l'OFCS selon la loi.	Aucune base sur Internet. Appliquer le moindre privilège et le chiffrement.
Supply chain	Doctrine CISA / ESF, pas de page OFCS dédiée.	Exiger un SBOM et un VEX. Cartographier les fournisseurs.
Open source	Principes CISA sur la sécurité open source.	Verrouiller les lockfiles et scanner avec SCA. Tenir un miroir interne avec allowlist.
Exchange	Le NCSC (aujourd'hui OFCS) a signalé plus de 4 500 entités concernées.	Appliquer les CU et SU sans délai. Considérer tout serveur non patché comme compromis.

2.8.2.1. Phishing

- **Bilan 2024 (antiphishing.ch) :**

- 975 309 signalements (+79 % sur un an) ;
- 20 872 sites de phishing confirmés (+108 % sur un an) ;
- ces chiffres décrivent les signalements centralisés par le portail, pas toutes les tentatives.

- **Tendance :** attaques en temps réel imitant M365 et SharePoint, contournant parfois la 2FA simple.

- **Réflexes :**

- ne jamais saisir un mot de passe via un lien, passer par un favori ;
- activer la 2FA ou FIDO2 partout ;
- signaler chaque tentative.

- **Si compromis :** changer le mot de passe, déposer plainte.

- **Côté domaine :** configurer SPF, DKIM et DMARC.

2.8.2.2. Ransomware

- **Trois portes d'entrée :** patch manquant, RDP ou VPN sans 2FA, macro piégée.

- **Règle :** ne pas payer la rançon.

- **Prévention :** backup 3-2-1 offline et testé, macros bloquées par défaut.

- **Si une machine est chiffrée :**

- l'isoler du réseau ;
- analyse forensique avant toute réinstallation ;
- vérifier les déchiffreurs gratuits de No More Ransom.

2.8.2.3. DDoS

- **Mécanisme** : saturation d'un service par botnets ou amplification.
- **But** : l'indisponibilité, pas le vol.
- **Doctrine OFCS** : tenir la charge avec le FAI et la mitigation ; ne pas payer en cas d'extorsion.
- **Préparation** :
 - contacts FAI et CDN prêts à l'avance ;
 - SYN-cookies, WAF, filtrage GeoIP ;
 - site de secours et playbook écrit.

2.8.2.4. Data leaks

- **Origines** : backup exposé, base exposée, exfiltration après intrusion.
- **Règle** : ne pas payer.
- **Réaction** :
 - isoler les systèmes concernés ;
 - inventorier les données touchées ;
 - notifier le PFPDT (art. 24 nLPD) via databreach.edoeb.admin.ch ;
 - notifier l'OFCS sous 24 h si infrastructure critique.
- **Prévention** : aucune base sur Internet, moindre privilège strict, chiffrement des données sensibles.

2.8.2.5. Supply chain

- **Doctrine** : pas de page OFCS dédiée ; elle vient de CISA et de l'ESF.
- **Mesures** :
 - exiger un SBOM (SPDX ou CycloneDX) avec un VEX ;
 - vérifier le SDLC et le SSDF du fournisseur ;
 - cartographier les fournisseurs selon NIST SP 800-161 ;
 - limiter chaque composant au moindre privilège.

2.8.2.6. Menaces de l'écosystème open source

- **Menaces propres** :
 - typosquatting (diango au lieu de django) ;
 - dependency confusion entre registre public et privé ;
 - mainteneurs compromis.
- **Cas marquants** : Log4Shell, xz-utils.
- **Mesures** :
 - miroir interne avec allowlist ;
 - lockfiles verrouillés, pas de mise à jour à l'aveugle ;
 - scan SCA (Dependabot, Trivy) ;
 - évaluation avant adoption, signatures Sigstore vérifiées ;
 - SBOM à chaque build.

2.8.2.7. Microsoft Exchange

- **Trois familles de failles critiques** :
 - **ProxyLogon** : CVE-2021-26855, 26857, 26858, 27065 ; exploité par Hafnium pour déposer un webshell SYSTEM.
 - **ProxyShell** : CVE-2021-34473, 34523, 31207.
 - **ProxyNotShell** : CVE-2022-41040, 41082.

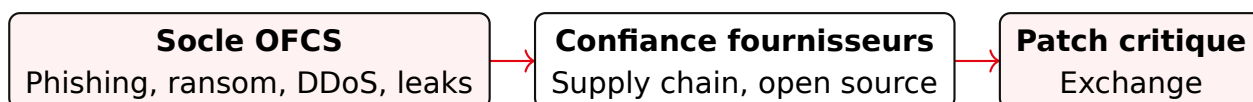
- **Impact suisse** : le NCSC a informé plus de 4 500 entités exposées ; alerte historique reprise par l'OFCS.
- **Mesures** :
 - appliquer les mises à jour cumulatives (CU) et de sécurité (SU) sans délai ;
 - contrôler avec HealthChecker et Test-ProxyLogon.ps1 ;
 - traiter un serveur non patché comme à risque élevé, l'isoler pour investigation.

2.8.3. Résultats

Trois groupes de menaces :

- **Socle OFCS** : phishing, ransomware, DDoS, leaks, avec des réflexes directs.
- **Confiance fournisseurs** : supply chain et open source déplacent la confiance vers les dépendances.
- **Patch critique** : Exchange montre ce qui arrive quand un patch critique dort.

Chaque menace tient en deux recommandations : un réflexe humain et une mesure technique. Leur point commun est la préparation : backups testés, contacts prêts, inventaires à jour.



2.8.4. Interprétation des résultats

Ces menaces se rangent sur la triade CIA : la confidentialité contre les leaks, l'intégrité contre le ransomware et la supply chain, la disponibilité contre le DDoS. Aucune mesure seule ne suffit : c'est la défense en profondeur, où chaque couche rattrape la précédente. Le tout s'entretient en cycle PDCA : patcher, tester, auditer, corriger. J'en tire trois habitudes pour le projet de semestre : un SBOM à chaque build, des backups testés et un playbook écrit avant l'incident.

2.8.5. Références

Phishing :

- OFCS - Phishing
- antiphishing.ch
- Cybermalveillance - Hameçonnage

Ransomware :

- OFCS - Ransomware
- CISA - Ransomware Guide

DDoS :

- OFCS - DDoS
- OFCS - Attaque DDoS : que faire

Data leaks :

- OFCS - Fuite de données
- Portail de notification PFPDT
- BACS - Fuite de données autorités

Supply chain :

- CISA - Defending Against Software Supply Chain Attacks (PDF)

Open source :

- CISA - Open Source Software Security Principles

Exchange :

- OFCS - Faille Exchange
- CERT-FR - Alerte CERTFR-2021-ALE-004

2.9. Activité 5 : Définir le vocabulaire de base de la cybersécurité**Objectifs**

- Extraire du glossaire Hucency les concepts que je ne connaissais pas encore.
- Les résumer dans les grandes lignes.
- Définir red team, blue team et purple team.

2.9.1. Métiers pertinents

- **RSSI** : arbitre le vocabulaire et les priorités.
- **SOC, blue team** : détectent et répondent aux incidents.
- **Red team** : simule l'attaquant en pentest.
- **CERT** : coordonne la réponse.
- **Développeur, admin** : appliquent les correctifs, contrôlent le Shadow IT.

2.9.2. Déroulement

Ma source principale est le Hucency - Glossaire de la cybersécurité (55 définitions, sourcées ANSSI, CNIL, Cybermalveillance, ENISA). J'ai reformulé les définitions dans les grandes lignes, sans les recopier.

2.9.2.1. Six concepts extraits du glossaire

Terme	Définition (dans les grandes lignes)
APT (Advanced Persistent Threat)	Attaque sophistiquée et furtive qui dure dans le temps. Un groupe structuré, souvent soutenu par un État, s'installe dans le système visé pour espionner, saboter ou voler de la propriété intellectuelle.
CERT (Computer Emergency Response Team)	Centre d'alerte et de réaction aux incidents. Il collecte les signalements, analyse les menaces et coordonne la réponse. En France, le CERT-FR est opéré par l'ANSSI.
Drive-by download	Infection sans action de l'utilisateur. La simple visite d'une page compromise suffit : une vulnérabilité du navigateur ou d'un plugin installe le malware à son insu.
Emotet	Trojan bancaire devenu une plateforme de distribution. Il volait des identifiants puis livrait d'autres malwares, dont des rançongiciels. Il compte parmi les malwares les plus destructeurs.
Log4Shell	Faille critique CVE-2021-44228 de la bibliothèque Apache Log4j, révélée en décembre 2021. Elle permet une exécu-

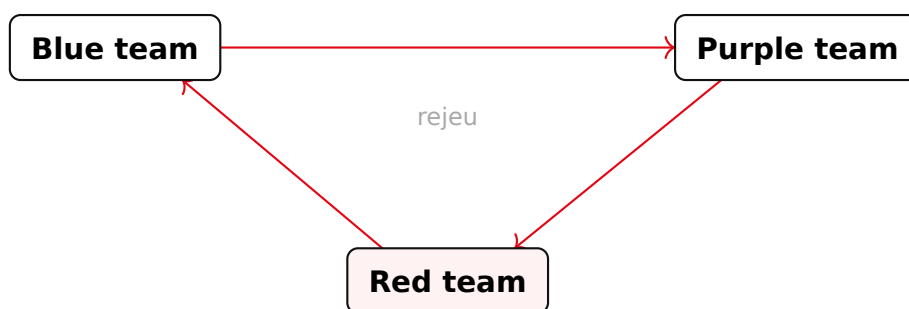
	tion de code à distance et a exposé des millions de systèmes.
Shadow IT	Usages sans aval de la DSI : SaaS, cloud, applis ou appareils perso utilisés par les collaborateurs. Il crée des angles morts, complique la surveillance et augmente le risque de fuite.

Précision que je ne connaissais pas avant lecture : Emotet et Log4Shell montrent deux échelles. Emotet est une menace persistante qui mute (botnet loué à d'autres attaquants), tandis que Log4Shell est une faille supply chain où une seule bibliothèque omniprésente compromet tout l'écosystème.

2.9.2.2. Red team, blue team, purple team

Équipe	Rôle
Red team	Équipe offensive. Elle simule un attaquant réel : pentest, intrusion, phishing ciblé, élévation de privilèges. Son but est de prouver qu'une compromission est possible.
Blue team	Équipe défensive. Elle surveille (SOC, SIEM, EDR), durcit, détecte et répond aux incidents. Son but est d'empêcher la compromission ou de la contenir vite.
Purple team	Fonction de liaison, pas une troisième armée. Elle fait rejouer ensemble les scénarios de la red team à la blue team pour corriger les détections et valider les playbooks. Son but est l'apprentissage continu.

Le cycle est le suivant : la red team attaque, la blue team détecte et répond, puis la purple team compare l'attaque aux alertes, ajuste les règles SIEM/EDR et rejoue le scénario jusqu'à une détection fiable.



2.9.3. Résultats

Les six termes se rangent en trois groupes, plus les équipes :

- **L'attaque** : APT, drive-by download, Emotet.
- **L'organisation de la défense** : le CERT collecte les signalements et coordonne la réponse.
- **Le terrain qui facilite l'attaque** : Log4Shell (dépendance omniprésente), Shadow IT (usages non contrôlés).
- **Qui fait quoi** : red, blue et purple team (attaquer, défendre, faire progresser les deux).

2.9.4. Interprétation des résultats

Aucun acteur ne couvre seul la triade CIA, ce qui relève de la défense en profondeur : le CERT coordonne, la blue team opère au quotidien, la red team vérifie et la purple team boucle l'amélioration. Pour le projet de semestre, j'en tire deux réflexes : nommer chaque risque avec le bon terme (APT, drive-by, Shadow IT) et associer chaque mesure à son équipe (qui détecte, qui teste, qui corrige).

2.10. Activité 6 : Rôle de responsable de la sécurité d'une entreprise

Objectifs

- Endosser le rôle de RSSI.
- Montrer que les deux piliers (triade CIA et fonctions Identifier, Protéger, Détecter, Répondre, Récupérer) forment un cadre de pilotage utile face aux cybermenaces.
- Relier chaque pilier à une décision RSSI concrète et citer les standards qui les portent.

2.10.1. Métiers pertinents

- **RSSI** : porte le cadre, rend compte à la direction.
- **Risk manager** : chiffre les risques sur la grille CIA.
- **SOC, blue team** : détection et réponse.
- **Admin, développeur** : appliquent la protection.
- **Auditeur** : vérifie la récupération par les tests de restauration.
- **DPO** : rejoint le RSSI sur la confidentialité et la notification.

2.10.2. Déroulement

L'affirmation testée est que les piliers CIA et Identifier / Protéger / Détecter-Répondre / Récupérer donnent un cadre assez concret pour décider. Je la défends devant ma direction en trois temps : fixer les priorités avec CIA, organiser l'action avec les fonctions, puis trancher trois décisions de RSSI.

2.10.2.1. 1. La triade CIA fixe le quoi protéger

- **Confidentialité** : limite qui voit.
- **Intégrité** : personne ne modifie sans droit.
- **Disponibilité** : accès quand il faut.

Je repars des quatre cas de l'exercice 3, dont les notes imposent déjà des arbitrages.

Cas (note C/I/A)	Priorité RSSI	Mesure que j'arbitre en premier
Banque en ligne (4/4/4)	Tout au maximum	HSM et 2FA FIDO2, signatures sur chaque ordre, PRA actif-actif.
E-commerce (3/3/3)	Équilibre	Chiffrement des paiements, contrôle des commandes, capacité pour les pics.
AlertSwiss (1/4/4)	I et A	Signature des messages et canal de diffusion redondant, même en pleine crise.

Streaming (2/2/4)	A	CDN et autoscaling, catalogue public donc C faible.
-------------------	---	---

Premier apport du cadre : à disponibilité égale (4), les budgets diffèrent. AlertSwiss investit dans l'authenticité, le streaming dans la capacité. Sans la grille CIA, je répartirais mal le budget.

2.10.2.2. 2. Les fonctions organisent le comment agir

Les fonctions viennent du NIST Cybersecurity Framework (CSF) : Identifier, Protéger, Détecter, Répondre, Récupérer. Le CSF 2.0 ajoute Gouverner (stratégie et supervision par la direction). Je garde les cinq de l'énoncé, Gouverner servant de chapeau.

Fonction	Action du RSSI	Exemple repris de mes activités
Identifier	Inventorier actifs, risques et fournisseurs.	Cartographie des actifs et analyse top-down d'ISO 27001 (travail personnel).
Protéger	Durcir, cloisonner, former.	Backup 3-2-1, moindre privilège, 2FA contre phishing et ransomware (activité 2).
Détecter	Surveiller et alerter.	Journaux, alertes hiérarchisées, filtrage contre la surcharge (activité 4).
Répondre	Isoler, enquêter, notifier.	Playbook : isoler la machine, forensique, notification PFPDT et OFCS (activité 2).
Récupérer	Restaurer et apprendre.	Restauration testée, post-mortem sans blâme, clause 10 d'ISO 27001.

L'ordre est imposé : on ne protège bien que ce qu'on a identifié, on ne répond bien que si on détecte, et on ne récupère que si on a préparé. La boucle de retour vers Identifier porte l'amélioration continue.



2.10.2.3. 3. Trois décisions de RSSI qui prouvent le cadre

Décision 1 : arbitrage budgétaire. Je dois choisir entre un WAF et un coffre de backups offline. Pour la banque, l'intégrité des soldes impose les deux. Pour le streaming (C/I faibles), la disponibilité fait passer la capacité avant le chiffrement avancé. Chaque franc est justifié par le critère qu'il protège, comme la SoA d'ISO 27001 trace chaque mesure.

Décision 2 : ransomware un vendredi soir. Le SOC signale une machine chiffrée, ce qui déclenche la chaîne Détecter → Répondre → Récupérer :

1. Isoler la machine.

2. Interdire le paiement (doctrine OFCS et CISA).
3. Mener la forensique avant réinstallation.
4. Restaurer depuis le backup testé.
5. Notifier le PFPDT si des données clients fuient.

Sans playbook écrit à l'avance, je négocie sous stress, et le biais de jugement (activité 4) décide à ma place.

Décision 3 : reporting à la direction. Je rapporte des risques sur CIA et l'avancement des cinq fonctions, pas des CVE. Par exemple : confidentialité des dossiers patients couverte à 80 %, détection encore manuelle, test de restauration réussi en juin. C'est le langage de la fonction Gouverner : la direction comprend, arbitre et signe, ce qui pèse pour viser ISO 27001.

2.10.3. Résultats

Les deux piliers sont complémentaires, sans recouvrement. CIA donne le quoi, c'est-à-dire les priorités (banque 4/4/4, AlertSwiss 1/4/4, streaming tiré par la disponibilité). Les fonctions donnent le comment : identifier avant de protéger, détecter avant de répondre, préparer avant de récupérer. Les trois décisions montrent le cadre en action : un arbitrage budgétaire tracé dans la SoA, une réponse ransomware jouée au playbook, un reporting traduit en risques pour la direction. Chaque pilier seul laisse un angle mort : CIA sans fonctions reste théorique, et des fonctions sans CIA répartissent l'effort à l'aveugle.

2.10.4. Interprétation des résultats

Je n'ai pas à choisir entre les cadres, je les empile : CIA porte l'analyse de risques, les fonctions portent le plan d'action et ISO 27001 porte la preuve (PDCA, SoA). Comme pour la défense en profondeur (activité 2), chaque fonction rattrape la précédente. Le facteur humain (activité 4) reste la condition de tenue : procédures écrites, alertes hiérarchisées et post-mortems sans blâme rendent les fonctions tenables par des humains fatigués.

Pour le projet de semestre, la méthode tient en trois gestes : noter chaque actif en C/I/A, rattacher chaque mesure à une fonction, tracer l'écart dans une mini-SoA. Une liste d'outils devient ainsi une posture défendable devant un auditeur ou une direction.

2.10.5. Références

- NIST, Cybersecurity Framework (CSF) 2.0 : Gouverner, Identifier, Protéger, Détecter, Répondre, Récupérer
- ISO, ISO/CEI 27001 (SMSI, SoA, PDCA)
- OFCS (BACS) : phishing, ransomware, DDoS, fuite de données
- CISA, Ransomware Guide (ne pas payer, backups offline)
- Cybermalveillance.gouv.fr : réflexes et guides pour les entreprises

2.11. Activité 7 : Pourquoi la surface d'attaque du kernel Linux est devenu récemment un problème ? Que faire (cas : opérateur cloud) ?

Objectifs

- Comprendre pourquoi la surface d'attaque du kernel Linux est devenue un problème récemment.
- Déterminer quoi faire dans le cas d'un opérateur cloud.

2.11.1. Métiers pertinents

- **Admin cloud, exploitant hyperviseur** : isolation et patching des nœuds.
- **Architecte sécurité** : choix du runtime et des profils de confinement.
- **SOC, blue team** : détection runtime.
- **RSSI** : arbitre entre exposition multi-tenant et coût des redémarrages.

2.11.2. Déroulement

Risque propre à l'opérateur cloud. Les conteneurs partagent le noyau de l'hôte : une seule faille noyau casse la multi-tenancy. L'attaquant s'évade du conteneur ou de la VM, puis compromet l'hyperviseur ou le nœud hôte.

Pourquoi c'est difficile à contenir en 2026. Le fuzzing assisté par IA, l'industrialisation des proofs of concept (PoC) et l'évolution rapide du noyau accroissent la pression sur les mainteneurs. Les chiffres de CVE par version varient selon la source et la période ; les 2 000 cités par certaines analyses sont un instantané à vérifier, pas une constante.

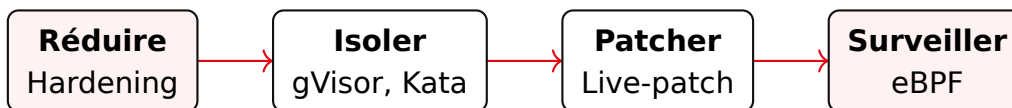
LPE (Local Privilege Escalation) récentes. Copy Fail, Dirty Frag et Dirty Clone sortent souvent avec un PoC public. Le délai entre publication et exploitation varie, et l'impact dépend du noyau, de la configuration et de l'isolation. Le passage conteneur → root est donc un scénario à reproduire et à réduire, pas une conséquence systématique.

Agents autonomes. Des recherches décrivent des agents capables d'adapter des PoC publics. Évasion, root sur l'hôte et mouvement latéral dépendent toutefois de la vulnérabilité et des mesures en place : ce scénario n'est pas systématique.

Facteur	Mécanisme	Effet pour l'opérateur cloud
Fuzzing + IA	Scan massif du code, volume de CVE signalé dans les sources consultées.	Pression sur le rythme de publication et de correction.
LPE sérialisées	PoC public, scénario d'élévation conteneur vers root.	Risque pour le nœud partagé si la faille est exploitable et les mesures inefficaces.
Agents autonomes	Adaptation de PoC publics ; scénario d'évasion et mouvement latéral.	Risque de compromission de l'hôte et de propagation inter-tenants si les conditions sont réunies.

2.11.3. Résultats

Un cycle mensuel de patch ne suffit pas toujours. Je propose un plan en quatre étapes : réduire, isoler, patcher à chaud, surveiller.



Étape 1 : réduire la surface du noyau (hardening). La plupart des failles récentes visent des modules réseau ou des filesystems inutiles en production cloud. Les actions :

- Bloquer leur chargement via `modprobe.d`.
- Désactiver les protocoles non requis et les vieux filesystems.
- Couper les fonctions à risque comme `io_uring` si aucune architecture ne l'exige.
- Restreindre les appels système par des profils `Seccomp` stricts.
- Interdire `clone3`, `unshare` ou `keyctl` aux charges clientes.

Étape 2 : durcir l'isolation (sandboxing). Docker / containerd classique partage le noyau hôte : si le noyau tombe, l'hôte tombe. Pour les charges non dignes de confiance, je passe à gVisor ou Kata Containers. gVisor intercepte et émule les syscalls en espace utilisateur ; Kata Containers place chaque conteneur dans une micro-VM avec son propre noyau.

Étape 3 : moderniser le patching. Redémarrer des milliers d'hyperviseurs ralentit chaque correctif. Le live-patching (KernelCare, Kpatch, Livepatch) charge un correctif en mémoire sans redémarrage immédiat, lorsque correctif et système le permettent. Il ne couvre que les correctifs compatibles et ne supprime pas tous les risques. Les changements structurels passent donc par un pipeline d'infrastructure : drain du nœud, mise à jour, test, redémarrage ou redéploiement progressif.

Étape 4 : détecter au runtime via eBPF. Un outil CNAPP / CWPP basé sur eBPF (Cilium Tetragon, Falco) observe le noyau en temps réel. Il alerte sur une élévation de privilèges sans fichier modifié et signale une structure socket anormale.

Étape	Action que je pilote	Outil ou mécanisme
Réduire	Désactiver modules, filtrer sys-calls.	<code>modprobe.d</code> , <code>Seccomp</code> , sans <code>io_uring</code> .
Isoler	Runtime à isolation forte pour l'untrusted.	gVisor, Kata Containers.
Patcher	Corriger à chaud lorsque c'est compatible ; drain et redémarrage pour les changements structurels.	KernelCare / Kpatch / Livepatch, pipeline drain.
Surveiller	Détecter l'anomalie au cœur du noyau.	eBPF, Tetragon, Falco.

2.11.4. Interprétation des résultats

Le plan applique la défense en profondeur, chaque étape rattrapant la précédente. Le hardening réduit l'exposition, le sandboxing confine les charges non fiables, le live-

patching réduit la fenêtre d'exposition si le correctif est compatible, et la détection eBPF signale les comportements suspects à l'exécution.

Côté opérateur, la triade CIA se lit ainsi : la confidentialité repose sur la séparation des tenants, l'intégrité sur le blocage de l'élévation conteneur → root, et la disponibilité est maintenue pendant le patching si le live-patch est compatible, sinon par drain ou redémarrage. Le moindre privilège et le Zero Trust imposent qu'aucun workload client n'obtienne par défaut un syscall sensible.

Le plan suit le cycle PDCA :

- **Plan** : inventaire des modules et des syscalls.
- **Do** : déploiement des profils et runtimes.
- **Check** : Tetragon et audits.
- **Act** : live-patch et SoA.

Côté ISO 27001, ce plan se trace vers la gestion des vulnérabilités techniques et la sécurité des environnements de développement et d'exploitation. Le certificat ne prouve pas l'absence de CVE noyau ; il prouve qu'un système de patching et de surveillance tourne en continu.

J'en retiens trois réflexes pour le projet de semestre : un runtime isolé pour tout workload non digne de confiance, Seccomp strict par défaut, et le live-patching si compatible, avec drain ou redémarrage pour les changements structurels.

2.11.5. Références

Sources de l'analyse :

- Tom's Hardware : le noyau frôle 2 000 CVE par version, chasseurs IA sur 40 M de lignes, mainteneurs submergés
- LinuxSecurity : état de la sécurité du noyau Linux 2025
- Host.it : CVE noyau Linux, IA et patch sans redémarrage

Isolation et détection :

- gVisor : isolation par interception des syscalls
- Kata Containers : conteneur dans une micro-VM
- eBPF : observation du noyau en temps réel
- Falco : détection runtime cloud-native
- Cilium Tetragon : sécurité runtime basée sur eBPF

2.12. Travail personnel : ISO 27001

Objectifs

- Prendre un seul standard, ISO 27001, et comprendre comment il fonctionne vraiment.
- À qui il s'applique, ce qu'il impose concrètement, comment prouver qu'on le respecte.
- En quoi il se distingue d'un guide technique.
- Explication détaillée dans le document de groupe (Google Docs), lien aussi reporté dans le tableau du cours.

2.12.1. Métiers pertinents

Ce standard ne parle pas qu'aux techniciens :

- **RSSI, responsable sécurité** : portent le SMSI (système de management de la sécurité de l'information), rendent compte à la direction.
- **Risk manager, analyste risques** : l'analyse de risque est leur point de départ.
- **Auditeur interne, auditeur de certification** : vérifient la conformité sur preuves.
- **Admin systèmes et réseau, développeurs, DPO** : appliquent les mesures de l'annexe A, chacun sur sa partie.
- **Direction** : sans son engagement écrit, la certification ne passe pas.

2.12.2. Résultats

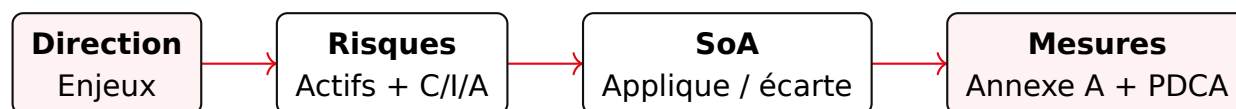
Portée générale, périmètre choisi. La norme s'adresse à toute organisation (entreprise, administration, ONG, petite ou grande), et rien ne la limite à l'informatique. Chaque organisation choisit son périmètre de SMSI : toute l'entreprise, un site, un département, un produit. Tout le reste ne s'applique qu'à l'intérieur de ce périmètre déclaré.

Quatre familles de mesures. L'annexe A (version 2022) liste 93 mesures, réparties ainsi :

- **Organisation** : politiques, rôles, classification de l'information, gestion des incidents.
- **Personnes** : recrutement, sensibilisation, processus de départ.
- **Physique** : accès aux locaux, protection du matériel.
- **Technique** : contrôle d'accès logique, cryptographie, sécurité réseau, développement sécurisé, correctifs.

La sécurité ne se joue donc pas que dans les pare-feu.

Gestion du risque top-down. La direction pose les enjeux, on identifie ensuite actifs et risques sur C, I, A, et on choisit les mesures seulement après. Rien n'est obligatoire par défaut, d'où la Déclaration d'applicabilité (SoA) : on justifie, mesure par mesure, ce qu'on applique, ce qu'on écarte, et pourquoi. L'ordre est imposé : pas de mesures avant les risques, pas de risques hors périmètre, et la SoA comme trace écrite du choix.



Obligations de management plus que détails techniques. Les clauses 4 à 10 décrivent le système : périmètre, rôles, planification, non-conformités, revue de direction. La norme dit quel processus mettre en place, pas quel outil acheter ni quel chiffrement utiliser.

Pensée pour la certification. Un tiers (Bureau Veritas, BSI, SQS) audite l'organisation et délivre un certificat de trois ans, avec un audit de suivi chaque année. Entre-temps, les audits internes et la roue PDCA (Plan, Do, Check, Act) entretiennent le système. Le certificat a un double usage : preuve de confiance pour les clients, boucle d'amélioration en interne.

Un coût réel. Il n'existe pas de chiffre unique, tout dépend du périmètre. Il faut payer l'audit externe et souvent un accompagnement, mais le coût principal est le temps

interne : documentation, analyse de risques, formation. S'y ajoutent parfois des mises à niveau techniques non prévues.

Prévention et réaction. La norme couvre les deux versants : la prévention (analyse de risques, politiques, durcissement, sensibilisation), puis la détection et la réaction (journaux, surveillance, détection d'anomalies, réponse aux incidents testée et suivie).

Pas de niveau numéroté. Contrairement à CMMI, il n'y a pas de note de 1 à 5. La maturité se voit dans la durée : indicateurs suivis, revues régulières, actions correctives (clause 10) qui aboutissent.

Références : document de groupe, ISO/CEI 27001, Wikipedia FR, page officielle ISO.

2.12.3. Interprétation des résultats

La norme est lourde sur le papier, mais je comprends son succès : elle adapte l'effort aux vrais risques, tout en obligeant à écrire ce choix dans la SoA. On ne peut pas dire « on fait de la sécurité » sans le montrer.

Elle colle au rôle de RSSI et d'auditeur. Pour un admin ou un dev, elle fournit un cadre, pas une recette ; les consignes précises se trouvent dans ISO 27002, qui détaille les mesures. Elle applique le PDCA à la sécurité : planifier avec les risques, déployer, contrôler (audits, logs), corriger (clause 10). Ce n'est donc pas un contrôle ponctuel avant un audit client.

Conformité n'est pas sécurité réelle : le certificat prouve qu'un système existe et qu'il est suivi, pas l'absence d'incident. Enfin, vu le coût en temps et en documentation, la direction doit le vouloir, sinon cela reste un classeur vide.

2.13. Synthèse de la séance

2.13.1. Résultats

- **Exercice 1** : auto-évaluation remplie, point faible en confinement OS/réseaux.
- **Exercice 2** : critères principaux CIA et secondaires rappelés et schématisés.
- **Exercice 3** : triade CIA notée et comparée sur quatre cas, avec graphique.
- **Exercice 4** : secteurs public/privé et échelles moi/nous/tous recensés.
- **Activité 1** : positionnement DevSecOps via CI/CD GitLab et roadmap.
- **Activité 3** : OSINT et veille collective autorisée, recensement de serveurs WordPress, simulation d'attaque générique et ciblée, recul sur les protections.
- **Activité 4** : six familles de biais cognitifs, mitigations individuelles et collectives.
- **Travail personnel** : ISO 27001 décortiqué, schéma Direction → Risques → SoA → Mesures.

2.13.2. Interprétation des résultats

Je retiens trois repères pour le semestre. D'abord, la triade CIA n'est pas abstraite : chaque cas (banque 4/4/4, AlertSwiss 1/4/4, streaming, e-commerce) impose sa priorité de conception, et ISO 27001 oblige à tracer ce choix dans la SoA. Ensuite, la sécurité est un système sociotechnique : biais cognitifs et culture d'équipe font échouer les mesures techniques, d'où les réflexes d'hypothèses écrites, de relecture croisée et de post-mortems sans blâme. Enfin, côté pratique, mon CI/CD couvre surtout des contrôles statiques et les vérifications des langages ; il manque encore le confinement (2/5), le DAST et l'analyse de dépendances.

La prochaine étape consiste à évaluer le projet de semestre avec la grille CIA + SoA + facteur humain. L'activité 3 y ajoute la veille OSINT autorisée, qui complète la détection à condition de valider les faux positifs et de tester les protections. La chaîne est donc : cadrer avec CIA et SoA, intégrer l'humain, puis pratiquer en CI/CD.



Séance du 25 septembre 2026

3.1. Exercice 5 : Inventaire des moyens/mesures techniques de la cybersécurité

Objectifs

- Créer un tableau des catégories du slide.
- Expliciter l'objectif de chacune.
- Donner des exemples de mesures techniques.

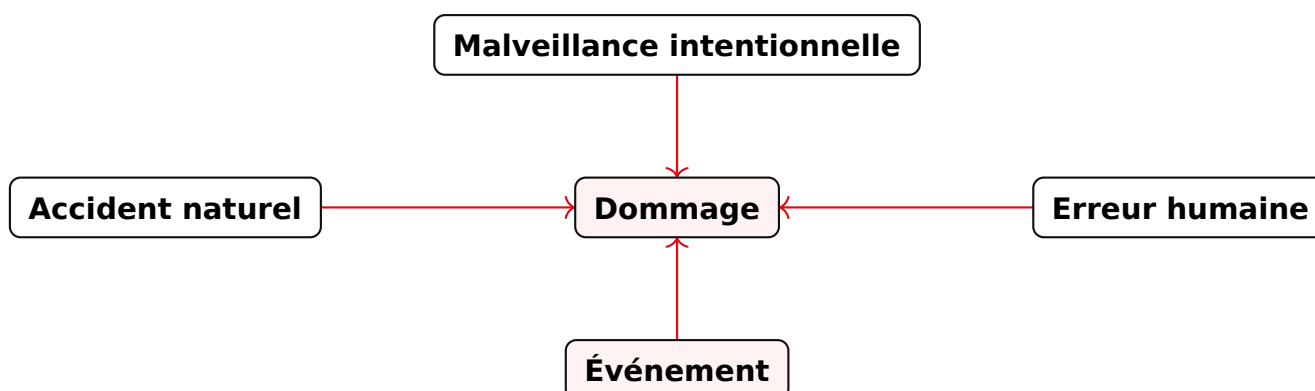
Catégorie	Mesures techniques
Prévention	Formations, tests, cadre réglementaire, mise à jour, chiffrement des accès
Détection	Logs, NDR, EDR, SIEM, monitoring
Confinement	VM, VLAN, sandbox, éviter les dépendances compromises
Contrainte	Architecture, PRA
Récupération	Tests, remise à 100 % en production

3.2. Exercice 6 : Que sont les menaces ? D'où proviennent-elles ? Exemples ?

Objectifs

- Comprendre les notions de menace, vulnérabilité et risque.
- Identifier les principales sources de menaces et leurs conséquences.
- Analyser les relations entre événement, dommage, vulnérabilité et risque.

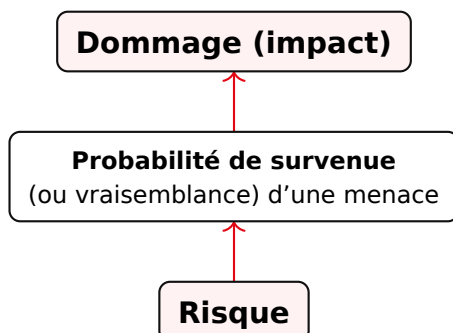
3.2.1. Événement



3.2.2. Vulnérabilité



3.2.3. Risque

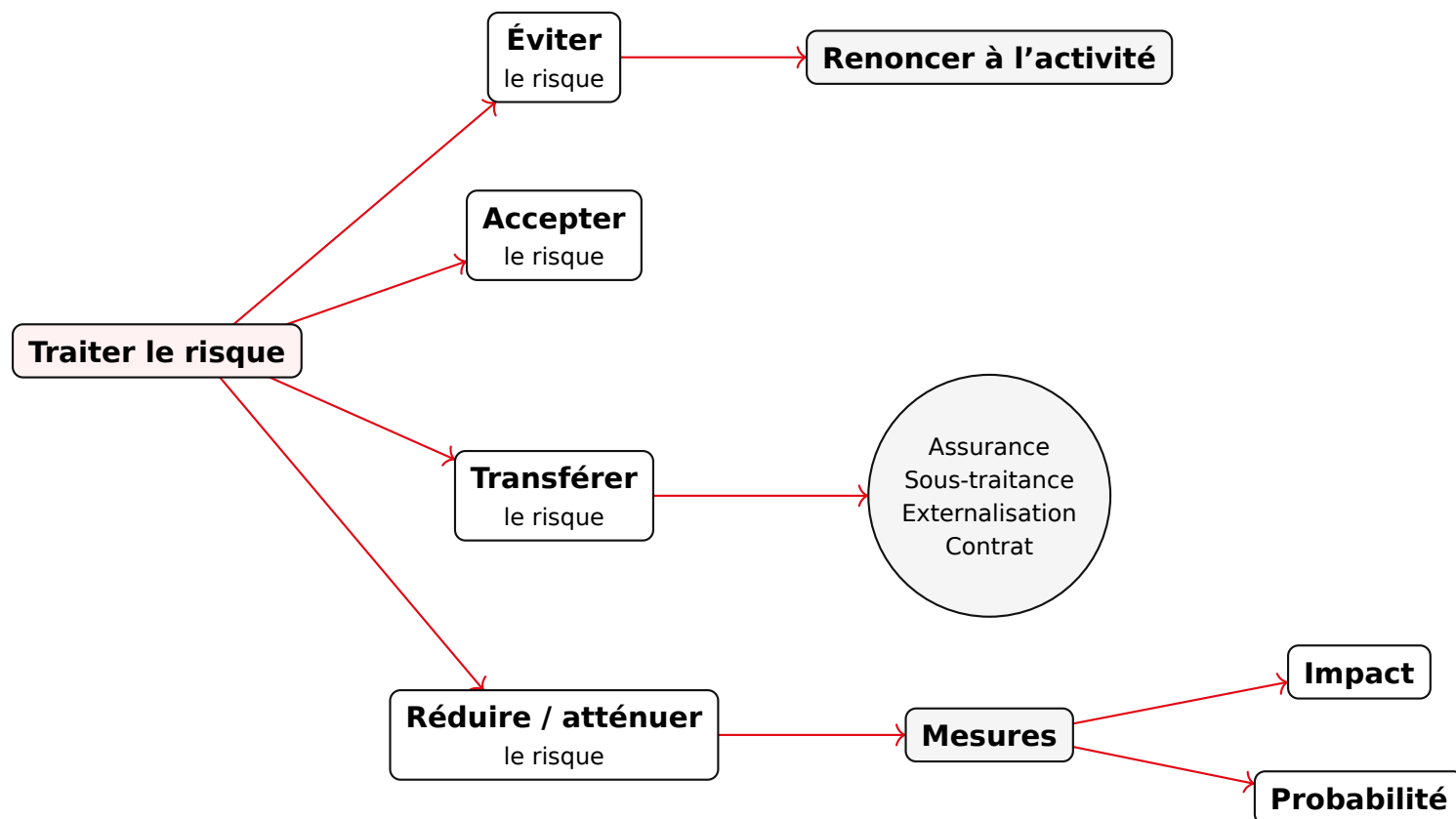


3.3. Exercice 9 : Sensibilisation aux zones d'ombres liées à l'inventaire des menaces

Objectifs

- Identifier les stratégies de traitement du risque.
- Distinguer réduire/atténuer, transférer, éviter et accepter le risque.
- Comprendre comment les mesures agissent sur la probabilité et l'impact du risque.

3.3.1. Traiter



3.4. Exercice 11 : Exemple d'analyse de risque simplifiée

Objectifs

- Identifier une menace : type, catégorie, impact.
- Proposer des mesures de réduction adaptées.

3.4.1. Contexte

Il s'agit d'un cas réel simplifié : la réception unique de données propriétaires auprès d'un fournisseur de données. L'étudiant les exploite sur son ordinateur portable, dans une base MySQL. Le code n'a aucune contrainte particulière, et la structure des données aucune exigence de confidentialité.

3.4.2. Contraintes

- Aucun accès de tiers aux données n'est autorisé avant, pendant ou après le projet.
- La destruction des données est garantie après une date fixe.
- Les procédures sont documentées et toute violation est signalée immédiatement.

Toute violation peut entraîner une pénalité allant jusqu'à 50 000 CHF.

Menaces	Type	Catégorie	Impact	Mesure
Accès DB par tiers	Externe / interne / humain	Cat. C	50 k CHF	Segmentation, verrouillage, formation

Séance du 2 octobre 2026

4.1. Activité 8 : Résumer les formes courantes de cybercriminalité et leurs conséquences

Objectifs

- Résumer les formes courantes de cybercriminalité et leurs conséquences.
- Identifier les criminels.
- Expliquer pourquoi différencier attaque automatisée, aveugle et attaque ciblée.
- Décrire ce que fait l'OFCS pour réduire ces risques.

4.1.1. Métiers pertinents

- **Threat Intelligence Analyst** : qualifie les menaces, distingue le bruit du ciblage.
- **SOC Analyst, Incident Responder** : reçoivent la cybercriminalité en production.
- **GRC Analyst** : voit beaucoup de ces incidents se solder par une obligation de déclaration, non par une sanction technique.

4.1.2. Résultats

D'après le catalogue de l'OFCS, l'escroquerie domine largement au 1er semestre 2026.

Forme	Mécanismes	Conséquence
Fraude	faux remboursements, arnaque au président, faux sites, fraude à l'investissement	Perte financière directe
Hameçonnage	phishing, vishing, smishing, hameçonnage en temps réel	Vol d'identifiants, qui devient une porte d'entrée
Extorsion	rançongiciel puis chantage à la publication	Touche les trois critères à la fois
Vol et fuite de données	infostealers	Identifiants utilisés ailleurs
Disponibilité	DDoS, defacement	Réseaux ORB (appareils piratés servant de relais à des tiers)

4.1.2.1. Les criminels

- **Opportuniste** : peu expérimenté.
- **Professionnel** : l'attaque est un revenu ; il industrialise et revend en service (RaaS).
- **Groupe organisé** : vise des victimes précises.
- **Acteur étatique** : espionne ou sabote avec les mêmes outils.
- **Interne** : ou ce qu'on accuse d'en être un.

4.1.2.2. Pourquoi les distinguer

Ces formes traduisent des rapports coût/bénéfice différents côté attaquant, pas une échelle de gravité. L'attaque aveugle ne coûte presque rien, alors que l'attaque ciblée exige de l'OSINT et de la compétence.

Côté défense, les parades diffèrent donc. Contre l'aveugle, être un peu au-dessus de la moyenne suffit (Reine rouge). Contre le ciblé, le point d'entrée n'est pas forcément le sous-système le plus surveillé. La frontière bouge d'ailleurs : selon le rapport 2026, l'IA rend les messages personnalisés et crédibles.

4.1.2.3. Ce que fait l'OFCS

- **Inform** : catalogue des menaces, fiches « que faire ? », rétrospectives hebdomadaires, rapport semestriel.
- **Recueillir** : portail de signalement et, depuis le 1er avril 2025, obligation dans les 24 h pour les infrastructures critiques.
- **Coordonner** : divulgation coordonnée de vulnérabilités, coopération internationale.
- **Renvoi** : antiphishing.ch, PFPDT (art. 24 nLPD), police cantonale.

4.1.3. Interprétation des résultats

L'OFCS ne réduit pas la cybercriminalité : il réduit l'asymétrie d'information. Son levier le plus efficace a été réglementaire, en rendant les appelants identifiables. Effet : les signalements d'appels au nom de fausses autorités ont baissé de plus de 75 % en juillet 2026.

4.2. Intervention Pascal Linder

Objectifs

- Noter en vrac le déroulé de l'intervention de Pascal Linder sur l'intrusion subie par la HE-Arc.
- Consolider le vocabulaire : acronymes, définitions, relations.
- Résumer ce que j'en retiens en trois à cinq thématiques.
- Indiquer les aspects à approfondir.
- Répondre à la question : que faut-il absolument réussir dans une entreprise pour progresser en cybersécurité ?
- Ajouter du recul et de la critique.

4.2.1. Métiers pertinents

- **Service informatique (SI)** : administrateurs systèmes et réseau ; ils détectent l'intrusion, isolent le réseau, analysent les logs, puis reconstruisent l'Active Directory et réinstallent serveurs et postes.
- **Responsable de la sécurité informatique** : poste créé après l'attaque (un EPT dédié) ; il pilote les nouvelles mesures : MFA, EDR, gestion des accès à privilèges, filtre DNS.
- **Direction** : membre de la cellule de crise ; elle arbitre les priorités de remise en état des services.
- **Communication** : membre de la cellule de crise ; elle gère la communication interne vers plus de 3500 comptes et la gestion médiatique.

- **Analystes de SWITCH CERT et du NCSC** : réponse à incident ; ils conseillent la cellule de crise et proposent de tout remettre à zéro.
- **Analyste forensique** : analyse du disque, suivi des IP de connexion VPN.
- **Enquêteurs de la police et de FedPol** : reçoivent la déclaration, mènent l'enquête pénale.
- **Partenaires et prestataires externes** : renforcent l'équipe pendant la crise.

4.2.2. Déroulement

4.2.2.1. Chronologie de l'attaque

- 9 juin: Intrusion -> utilisateur téléchargeant un malware en voulant installer un
- 10 juin: Notification de son hébergeur lui informant qu'il y a des connexions suspectes sur son compte, il change de mdp
- 13 juin: 1ère connexion de l'attaquant à travers le VPN
- 17 juin: l'attaquant scanne les ports à travers la connexion VPN
- 23 juin: Mouvements latéraux, l'attaquant essaie de se connecter sur d'autres serveurs internes à travers la connexion VPN.
- 27 juin: Connexion au serveur SQL, le service des automates tombe
- 28 juin: Connexion au serveur Exchange
- 29-30 juin: Scan de ports et le service tombe à nouveau, l'attaquant accède à un compte à privilèges, alertes EDR et Dump de data
- 1er juillet: Intrusion confirmée par le service info, VPN désactivé et alertes EDR
- 4 juillet: Informer NCSC SWITCH CERT Audit qu'une attaque est bien confirmée + reçu d'un mail de rançon
- 5 juillet: Séance de crise et collecte de logs

4.2.2.2. Réactions

- Isolation du réseau: couper les services publiés et stopper la connexion internet
- Création cellule de crise (service info, direction, communication, SWITCH, police)
- Contacter nos partenaires pour nous aider dans cette crise
- Déterminer les moyens de communications (interne)
- Déterminer la gestion médiatique

4.2.2.3. 1ers réflexes en parallèle à la recherche et analyse de logs

- copie de sécurité des sauvegardes sur un support externe
- (Re)discussion et modification des priorités de remise en état des services
- Déplacement des boîtes de messagerie dans le cloud (moyen de comm entre le SI et la direction)
- Étude de la reconstruction d'un domaine informatique (adressage réseau, domaine, réinstallation des serveurs)
- Mise en place d'outils de sécurité supplémentaires pour le suivi de l'attaque (EDR, filtre DNS)

4.2.2.4. Réflexions/Contraintes

- **Délai imposé** : tout remettre en service avant la rentrée académique 2022-2023, soit environ un mois et demi. La direction doit trancher fin juillet ; repartir d'un domaine neuf en un mois est jugé irréaliste.
- **Choix de reconstruction** : SWITCH CERT propose de tout repartir de zéro, mais l'école ne retient pas cette option. Elle restaure la sauvegarde antérieure à l'intrusion

(date de début connue), puis réinstalle l'OS de chaque poste. Comptes et objets machines sont désactivés, et les mots de passe des comptes de services et des 3500 utilisateurs changés.

- **Joindre les utilisateurs sans messagerie** : vacances, six sites, une partie du personnel pas encore au courant ; les utilisateurs doivent contacter l'école eux-mêmes.
- **Ingénierie sociale** : l'annuaire volé sert à de faux appels pour se faire passer pour des utilisateurs, d'où une réinitialisation des comptes en personne uniquement, sur présentation d'une carte d'identité.
- **Priorités de remise en service** : l'infrastructure de base passe avant les besoins métiers. La direction ne comprend pas toujours cet ordre, ce qui crée des tensions.
- **Facteur humain** : personnel épuisé en pleine période de vacances, enseignants stressés pour préparer la rentrée. La direction accepte un rythme soutenable pour garder le personnel efficace. Le service informatique n'a aucune expérience de la MFA pour accompagner les utilisateurs : documentation interne et FAQ à créer.

4.2.2.5. Conséquences / Défis

- Réinstallation d'un annuaire (Active Directory), importation d'une sauvegarde
- Tous les comptes et objets machines ont été désactivés
- Réactivation des comptes utilisateurs et de services après l'identification de l'utilisateur et d'un changement de mdp
- Réactivation des serveurs et services. Modif. des mdp.
- Réinstallation de tous les postes de travail (>1000 ordinateurs + ordinateurs étudiants)
- Interruption des services durant plusieurs semaines -> perte de productivité
- Accumulation de retard sur le traitement des dossiers
- Augmentation des heures travaillées -> épuisement du personnel (vacances)
- Comm avec les utilisateurs >3500 comptes
- Informations et gestion médiatique
- Difficultés liées aux nouvelles mesures mises en place, à l'incompréhension de la situation
- Manque de communication et documentation utilisateur

4.2.2.6. Finalité

- Exports de données mais on ne sait pas lesquelles
- Suivi des IP: connexions VPN
- Déclaration police + FedPol
- Analyse du disque
- Pas d'encryption
- Pas de publication
- Classe d'attaque: attaque non ciblée, par opportunité (moins de moyens des attaquants)

4.2.2.7. Nouvelles mesures - technique

- Déplacement de certains services dans le cloud (messagerie, MFA)
- On-premise / cloud, limiter la synchro des comptes, séparer les comptes à privilèges
- Mise en place de gestion des accès à privilèges
- Déploiement d'un EDR aussi sur les serveurs
- Limiter l'accès à internet (par zone)

- Engagement d'un EPT dédié à la sécurité informatique

4.2.2.8. Nouvelles mesures - utilisateur

- Limiter les accès VPN (zones géographiques) -> aujourd'hui retiré, car trop limitant en pratique
- Implémentation d'un filtre DNS (Cisco Umbrella)
- Limiter les postes de travail dans notre domaine (Active Directory), privilégier Intune
- Séparer la zone dédiée aux étudiants (services)
- Mise en place du SRP avec MFA
- Enlever les droits administrateurs locaux sur les postes de travail
- Bandeau d'avertissement des mails externes

4.2.2.9. Conclusion

- Erreur humaine impossible à éliminer
- Utilisation du MFA partout où possible
- Former les utilisateurs !

4.2.2.10. Vocabulaire

- **EDR** : Endpoint Detection and Response.
- **SWITCH CERT** : CERT national suisse, l'organisme à alerter.
- **SRP** : Secure Remote Password.
- **EPT** : équivalent plein temps (un poste à 100 %).
- **VPN** : Virtual Private Network.
- **MFA** : Multi-Factor Authentication.
- **DNS** : Domain Name System.
- **NCSC** : centre national de cyber-sécurité suisse.
- **SI** : Systèmes d'information.
- **SQL** : Structured Query Language.
- **IP** : Internet Protocol.

4.2.3. Résultats

L'intrusion vient d'un utilisateur, pas d'une faille technique. Le 9 juin, un poste télécharge un malware en voulant installer un logiciel ; le 10 juin, l'hébergeur alerte sur des connexions suspectes. Aucun exploit, aucune campagne ciblée : une opportunité saisie.

La persistance passe par le VPN, puis par les comptes à privilèges. Du 13 au 23 juin, l'attaquant utilise le VPN, scanne les ports et tente un mouvement latéral. Le point de bascule survient les 29-30 juin avec l'accès à un compte à privilèges. C'est ce passage qui élargit réellement la portée de l'incident, pas l'intrusion initiale.

La réponse est tenue, mais elle se paie cher. La procédure est suivie : cellule de crise, isolement du réseau, alerte du NCSC et de SWITCH CERT, saisines police et FedPol. Le prix : des semaines d'interruption, plus de 1000 postes réinstallés, 3500 comptes repris un par un.

L'attaquant n'a pas utilisé son levier. Il n'y a eu ni chiffrement ni publication, et les données exportées restent non identifiées. Cette absence de chiffrement ne rassure pas : le compte à privilèges lui en ouvrait la voie.

4.2.4. Interprétation des résultats

Que faut-il absolument réussir pour progresser en cybersécurité ? Ni un outil, ni une certification, mais trois choses, dans cet ordre :

1. **Savoir ce que l'on protège et où** : sans inventaire fiable, reconstruire le domaine et réinstaller plus de 1000 postes ne peut être ni planifié ni chiffré.
2. **Détecter tôt et rétablir vite** : ces deux durées sont les seules qui comptent vraiment. Ici, la compromission est restée invisible en interne pendant trois semaines (du 9 juin au 1er juillet), puis le rétablissement a pris des semaines.
3. **Savoir dire ce que l'on ne sait pas** : l'export est confirmé mais non caractérisé ; c'est le risque que je retiens comme le plus sérieux.

Ce que je critique :

- **Le changement de mot de passe du 10 juin n'a rien arrêté** : l'attaquant entre par le VPN le 13. Changer un mot de passe sans révoquer les sessions actives ne referme rien si les identifiants sont déjà exfiltrés ; c'est la MFA qui traite ce cas, pas le changement de secret.
- **Limitation géographique du VPN retirée, trop limitante** : la mesure théoriquement excellente et la mesure effectivement déployable ne sont pas la même chose.
- **Sauvegardes** : l'absence de chiffrage a tenu les données hors de portée de l'attaquant, mais la copie des sauvegardes sur support externe au début de la crise n'a, elle, jamais été cartonnée.

Ce que je voudrais approfondir :

- **L'obligation de déclaration** : ce qui déclenche l'alerte du NCSC et la saisine de FedPol, et dans quel délai ; mes notes donnent la chronologie, pas la règle.
- **Le périmètre de la reconstruction** : tout réinitialiser (proposition de SWITCH CERT) ou réparer chirurgicalement ? La décision repose sur des critères de coût et de risque que je ne sais pas encore évaluer.
- **Le volet forensique** : identifier les données exportées suppose des méthodes que je n'ai jamais pratiquées.

Ce que cela change pour moi : cet incident relie mon futur travail de dev et d'admin à celui du RSSI. Mes correctifs et mon inventaire déterminent si la reconstitution est possible, et le temps de rétablissement se mesure sur ce que j'ai produit. J'en tire deux réflexes : tenir l'inventaire à jour, et traiter la MFA et la restauration testée comme des prérequis, pas comme des améliorations.

4.3. Activité 9 : Que faire dans Concevoir, Valider et Opérer (cas : une entreprise) ?

Objectifs

- Donner des pistes, pour une entreprise et non un projet spécifique, sur les activités de Concevoir, Valider et Opérer.
- Ajouter des liens spécifiques d'amélioration continue.

4.3.1. Métiers pertinents

- **RSSI/CISO** : tient le fil entre les trois étapes, arbitre ce qui entre dans le cycle.
- **Auditeur sécurité** : intervient sur la validation, seul regard extérieur non biaisé.

- **SOC Analyst, GRC Analyst** : exploitation et indicateurs qui ferment la boucle.

4.3.2. Résultats

Activités étape par étape, de la conception à l'exploitation :

4.3.2.1. Concevoir

- **Cadrer** : périmètre, valeurs métier, classification des actifs, selon la chaîne actifs → menaces et vulnérabilités → risques → mesures.
- **Analyser les risques** : EBIOS RM au niveau stratégique, STRIDE-LM au niveau technique, puis hiérarchiser et traiter (éviter, réduire, transférer, accepter).
- **Choisir le référentiel** : ISO 27001/27002, NIST CSF, CIS Controls, ou la MCSR de l'OFCS. Ce choix détermine les contrôles, donc les preuves exigées en Valider.
- **Formaliser** : stratégie alignée sur les objectifs métiers → PSSI → procédures (SOP : acteurs, décisions, escalade), avec des objectifs SMART et une organisation claire (qui décide, qui applique, qui contrôle).

4.3.2.2. Valider

- **Tests d'intrusion par un externe** : l'équipe qui a conçu ne cherchera pas ce qui l'inquiète.
- **Contrôle des preuves, pas des intentions** : exemple du cours, la revue des habilitations suit la chaîne exigence → contrôle → indicateur → résultat → preuve, puis analyse les 2 % restés non conformes.
- **Tests de continuité et de reprise** : un PCA se drill, il ne se rédige pas.
- **Revue des KPI** : MTDD, MTTR, correctifs appliqués dans le délai ; revue de direction.

4.3.2.3. Opérer

- **Supervision** : journalisation centralisée, SIEM, EDR. Un SIEM sans tri des alertes ne sert à rien.
- **Vulnérabilités en continu** : priorisées par exploitabilité réelle, pas par le seul score CVSS. Exemple : le variant Akira a tenu en Suisse grâce à une SonicWall non patchée.
- **Identités** : MFA, moindre privilège, revue des habilitations, révocation aux départs.
- **Réponse et environnement** : IRP (plan de réponse aux incidents), veille, sensibilisation continue, relations externes (assistance DDoS, signalement à l'OFCS et au PFPDT).

4.3.3. Interprétation des résultats

Ces étapes forment une boucle, pas une feuille de route : Améliorer renvoie à Gouverner, Gouverner à Concevoir. Valider est l'étape que je garderais en priorité : elle ne produit rien mais exige des preuves, donc elle engage la responsabilité de celui qui les exige.

L'activité 4 rappelle que les biais font le plus de dégâts dans Gouverner, qui tranche avec des données incomplètes. Une organisation très bien opérée, mais dont la priorisation penche vers le spectaculaire, aura un bon niveau de maturité et une posture médiocre.

Séance du 9 octobre 2026

5.1. Activité 10 : Qu'est-ce qui alimente la veille cybersécurité et technologique ?

Objectifs

- Distinguer les canaux (comment on capte) des sources (ce qui fait autorité).
- Montrer que les signaux rapides (réseaux sociaux, forums, fuites) ne deviennent de la veille qu'après validation et exploitation.
- Relier chaque aliment à une décision : Identifier / Détecter vers SoA et playbook (prépare l'activité 11).

5.1.1. Métiers pertinents

- **Analyste CTI / SOC** : capte, trie et recoupe les signaux.
- **RSSI / risk manager** : arbitre ce qui entre dans la SoA et les priorités C/I/A.
- **Admin / développeur** : applique le correctif issu de la veille.
- **DPO** : suit les fuites et la notification en cas de données exposées.
- **Auditeur** : vérifie que la veille est tracée et rejouable.

5.1.2. Déroulement

Je pars de ma pratique réelle (réseaux, blogs), puis je la confronte aux exigences d'une veille défendable. La question impose deux temps : d'abord les canaux, où je croise l'info ; ensuite les sources, qui permettent de la valider et de l'exploiter.

5.1.2.1. 1. Les canaux : comment l'info arrive

- **Réseaux sociaux et blogs** : X/Twitter, YouTube, LinkedIn, Reddit, Hacker News, blogs techniques et newsletters. Leur atout est la vitesse et les signaux faibles (0-day, PoC, retour d'outil) ; leur limite, le bruit, les rumeurs et les manipulations, sans aucune autorité seule.
- **Forums cyber et zones de fuites** : forums spécialisés, leak sites et pages de rançongiciels (DLS), places de revente de bases. Ils montrent l'exposition réelle (victimes citées, bases en circulation, TTP du moment), mais l'accès est borderline, les faux et intoxications fréquents, et le cadre légal suisse à respecter. Règle : ne pas y aller seul, passer par un relais (OFCS, fournisseur CTI, SOC).
- **Collectif et direct** : communautés, conférences, intervenants (ex. séance 03), échanges entre pairs, retours d'incidents internes. Ils apportent le contexte et la validation par l'expérience.

Sans filtre, ces canaux informent mais ne protègent pas : ils surchargent (biais d'alerte, activité 4).

5.1.2.2. 2. Les sources : ce qui valide et rend exploitable

- **Institutionnel** : OFCS/BACS, CISA, ANSSI, Cybermalveillance.gouv.fr — doctrine, réflexes, ne pas payer, notification.

- **Technique et vulnérabilités** : CVE/NVD, bulletins éditeurs, correctifs et durcissements.
- **Renseignement structuré** : IoC, TTP, rapports CTI et CERT, filtres SOC.
- **Interne** : journaux, alertes hiérarchisées, post-mortems sans blâme, résultats de pentests et d'audits.
- **Normatif et techno** : ISO 27001, NIST CSF 2.0, évolutions DevSecOps, chiffrement, IA.

Canal rapide	Source qui valide	Décision alimentée
Post X / Hacker News sur faille	CVE/NVD + bulletin éditeur	Patch priorisé selon C/I/A, tracé en SoA.
Vidéo YT sur nouvel outil d'attaque	Rapport CTI / OFCS	Règle de détection, test des protections.
Rumeur de fuite sur forum	Fournisseur CTI / OFCS, vérification d'exposition	Blocage d'IoC, notification PFPDT si avéré.

Ordre imposé : capter vite, recouper, puis seulement verser au plan d'action.

5.1.3. Résultats

Les canaux se répartissent les rôles : sociaux et blogs pour la vitesse, forums et fuites pour l'exposition, collectif pour le contexte. Les sources d'autorité sont institutionnelles, techniques (CVE, éditeurs), CTI structurée, internes et normatives. La règle de passage est stricte : aucun signal brut ne déclenche seul une action ; il faut un recoupement, puis un rattachement à un actif C/I/A et à une fonction Identifier / Détecter. Les trois cas tracés l'illustrent : patch priorisé, détection ajoutée, fuite vérifiée et notifiée.

5.1.4. Interprétation des résultats

S'informer n'est pas faire de la veille. La veille commence au tri (faux positifs écartés), à la validation (deux sources indépendantes) et à la traçabilité (SoA, playbook).

Comme en défense en profondeur (activité 2), chaque aliment couvre un angle mort des autres : les canaux rapides rattrapent la lenteur institutionnelle, l'institutionnel rattrape le bruit des canaux. Le facteur humain (activité 4) reste décisif : alertes hiérarchisées, procédures écrites et post-mortems rendent le flux tenable.

Cette chaîne capter → valider → décider est l'entrée du schéma conception et opération de la sécurité (activité 11). Un flux subi devient ainsi une posture pilotée, défendable devant la direction et l'auditeur.

5.1.5. Références

- CVE Program et NVD : vulnérabilités et scores
- Hacker News : signaux techniques rapides, à recouper

5.2. Activité 11 : Schéma général conception et opération de la sécurité

5.2.1. Résultats

Schéma au niveau de l'entreprise, donc très global : il cadre le pilotage, pas l'implémentation.



Boucle d'amélioration continue : **Revoir** → **Planifier**.

- **Gouverner** : la direction oriente, arbitre les risques et alloue les budgets.
- **Planifier** : périmètre, analyse de risques, PSSI, programme et priorités.
- **Déployer** : organisation, rôles, ressources et conduite du changement.
- **Piloter** : indicateurs, audits, conformité et suivi des décisions.
- **Revoir** : revue de direction, enseignements, nouvelle ambition.

5.2.2. Interprétation des résultats

La sécurité se pilote comme un programme d'entreprise, pas comme un chantier technique : chaque bloc engage la direction avant les outils. Planifier sans piloter reste une intention, et piloter sans revoir fige le système ; la boucle de retour porte donc l'amélioration continue. L'implémentation (SIEM, patch, IRP) n'est qu'un moyen au service du plan : elle se décide en Déployer et se mesure en Piloter.