COMPTE RENDU – ATELIER 10 : TP2 SÉCURITÉ INFORMATIQUE

BTS SIO – Semestre 1
Baptiste Gaillard
Date : 26 novembre 2025

PHASE 1 : INTRODUCTION ET CONTEXTE

L'atelier 10 est un travail pratique (TP2) portant sur la sécurité informatique appliquée à un cas réel : Galaxy Swiss Bourdin (GSB), une entreprise pharmaceutique de recherche. L'objectif pédagogique est de sensibiliser les étudiants aux risques informatiques et aux mesures de prévention nécessaires dans un environnement professionnel exigeant des protocoles de sécurité stricts.

Cet atelier combine théorie et simulation pratique via un jeu de rôle professionnel, permettant aux participants de développer des compétences en communication, négociation, argumentation et gestion de conflits autour des enjeux de sécurité.

Le contexte de l'atelier s'articule autour d'un incident réel : une clé USB non sécurisée a été branchée sur un poste de travail en R&D, révélant une faille majeure dans la gestion des périphériques amovibles et risquant de compromettre les données sensibles (brevets, données d'essais cliniques, secret industriel).

PHASE 2 : ANALYSE ET PREPARATION

2.1 Objectifs visés

L'atelier vise les objectifs d'apprentissage suivants :
• Comprendre les fondamentaux de la sécurité informatique (confidentialité, intégrité, disponibilité, traçabilité, preuve)
• Identifier les risques spécifiques au secteur pharmaceutique
• Proposer des mesures de prévention et de mitigation adaptées
• Développer une argumentation professionnelle autour de la sécurité
• Défendre son point de vue face à des intérêts divergents
• Animer une réunion ou participer activement à un débat professionnel
• Développer ses compétences en communication, négociation et gestion de conflits

2.2 Contexte métier (Galaxy Swiss Bourdin)

Galaxy Swiss Bourdin (GSB) est une entreprise de recherche et développement pharmaceutique fonctionnant sous des régulations strictes :
• Normalisation : FDA (Food and Drug Administration), EMA (European Medicines Agency), Bonnes Pratiques de Fabrication (BPF)
• Réglementation : RGPD (Règlement Général sur la Protection des Données), protection des données sensibles
• Enjeux stratégiques : Protection de la propriété intellectuelle, prévention du vol de données, continuité d'activité
• Risque de réputation : Dans le secteur pharmaceutique, la confiance est cruciale

2.3 Livrables attendus

Le compte rendu doit intégrer les éléments suivants :
• Analyse du cahier des charges et des risques identifiés
• Fiche préparatoire du personnage / rôle joué (obligatoire pour les participants actifs)
• Résumé de la participation au jeu de rôle ou fiche d'évaluation (si observateur)
• Synthèse personnelle et apprentissages
• Recommandations stratégiques de sécurité

3. ANALYSE DES RISQUES INFORMATIQUES

3.1 Risques majeurs identifiés pour GSB

Pour une entreprise pharmaceutique comme GSB, les risques informatiques incluent :

3.1.1 Risques d'accès non autorisé et d'intrusion
• Intrusion via moyens externes (USB non sécurisés, réseaux VPN non sécurisés)
• Vol d'identifiants de connexion (phishing, ingénierie sociale)
• Escalade de privilèges et accès non autorisés à des données critiques
• Malwares et rancongiciels ciblant les données de recherche
Impact : Compromission de la confidentialité et de l'intégrité des données

3.1.2 Risques de fuites de données sensibles

• Exfiltration de propriété intellectuelle (brevets, formules secrètes)
• Vol de données d'essais cliniques et de résultats de recherche
• Compromission du secret industriel et avantage concurrentiel
• Violation du RGPD (si données personnelles de sujets d'essais)
Impact : Dommages financiers, réputationnel et réglementaire considérables

3.1.3 Risques humains et organisationnels

• Manque de sensibilisation du personnel aux menaces
• Non-respect des protocoles de sécurité par négligence
• Partage de mots de passe ou utilisation de clés faibles
• Ingénierie sociale et tentatives de phishing efficaces
• Erreurs humaines dans le traitement des données
Impact : Crée des vulnérabilités que les attaquants peuvent exploiter

3.1.4 Risques technologiques

• Absence de chiffrement des données en stockage et en transit
• Absence de contrôle des périphériques amovibles (USB, disques externes)
• Faible gestion des sauvegardes et récupération après sinistre
• Absence de journalisation et d'audit trail complets
• Systèmes d'information obsolètes ou non maintenus
Impact : Augmente la surface d'attaque et limite la récupérabilité

3.1.5 Risques réglementaires et légaux

• Non-conformité FDA/EMA (risque de suspension d'autorisation)
• Violation du RGPD (amende jusqu'à 4% du chiffre d'affaires)
• Responsabilité civile et pénale de l'entreprise
• Audit régulateur découvert suite à un incident
• Perte de certifications et de crédibilité auprès des partenaires
Impact : Amendes massives, réputation endommagée, limitations d'activité

4. RECOMMANDATIONS STRATÉGIQUES DE SÉCURITÉ

4.1 Mesure 1 : Contrôle strict des périphériques amovibles

Problématique : L'incident USB démontre que les clés USB personnelles non sécurisées constituent un vecteur d'attaque critique.

Actions proposées :
• Interdiction totale des supports personnels (clés USB, disques durs externes)
• Distribution de clés USB d'entreprise chiffrées (AES-256)
• Mise en œuvre de politiques GPO (Group Policy Object) pour désactiver les ports USB non autorisés
• Journalisation de tous les transferts de données vers des périphériques
• Exceptions documentées et validées pour collaborateurs externes

Justification : Elimine directement le vecteur d'attaque et réduit drastiquement le risque de fuite de données sensibles.

Bénéfices : Conformité FDA/EMA, protection de la propriété intellectuelle, audit trail complet.

Défis et compromis : Peut générer de la friction avec les utilisateurs ; solution = accompagnement pédagogique, altérnatifs sécurisés (plateformes de transfert de fichiers), phase pilote en R&D d'abord.

4.2 Mesure 2 : Authentification forte et gestion des identifiants

Problématique : Les accès non autorisés peuvent résulter de mots de passe faibles ou vol d'identifiants.

Actions proposées :
• Authentification multi-facteur (MFA) obligatoire pour tous les accès distants et sensibles
• Politiques de mots de passe stricts (15+ caractères, complexité, rotation tous les 90 jours)
• Gestionnaire de mots de passe d'entreprise (Dashlane, Bitwarden, ou 1Password)
• Formation à la reconnaissance du phishing et de l'ingénierie sociale

Justification : Réduit significativement les risques de compromission de compte et d'escalade de privilèges.

Bénéfices : Sécurité renforcée sans impact majeur sur la productivité.

Défis : Résistance initiale du personnel ; solution = support utilisateur réactif, formation progressive.

4.3 Mesure 3 : Chiffrement et protection des données

Problématique : Les données en vol ou en stockage doivent être protégées contre l'accès non autorisé.

Actions proposées :
• Chiffrement de tous les portables (BitLocker pour Windows, FileVault pour macOS)
• Chiffrement des données en transit (TLS 1.3, VPN avec chiffrement fort)
• Chiffrement des données sensibles en base de données
• Politique de destruction sécurisée des données en fin de vie

Justification : Protège les données en cas de vol ou de perte de matériel.

Bénéfices : Conformité RGPD, preuve de diligence raisonnable, réduction de l'impact potentiel d'une violation.

Défis : Surcharge de système (léger) ; solution = optimisation progressive.

4.4 Mesure 4 : Formation et sensibilisation continue

Problématique : Le facteur humain reste la vulnérabilité la plus exploitée.

Actions proposées :
• Module annuel obligatoire pour tous les employés (min. 1 heure, tousô et contrôle)
• Tests de phishing réalistes (min. 2x par an)
• Ateliers thématiques mensuels : risques pharmaceutiques, ingénierie sociale, outils de sécurité
• Ressources en ligne et série de « bonnes pratiques » affichage
• Incidents d'entraînement « simulation de crise » trimestriels

Justification : Renforce la vigilance collective et crée une culture de sécurité.

Bénéfices : Augmente à elle seule l'efficacité de toutes les autres mesures techniques (multiplier par 5 l'impact).

Défis : Coûts de formation ; solution = investissement à long terme, ROI clé (réduction de risque de fuite massif).

4.5 Mesure 5 : Audit, journalisation et continuité d'activité

Problématique : Absence de visibilité sur les menaces et capacité de récupération limitée.

Actions proposées :
• Mise en place de journalisation centralisée (SIEM : ELK Stack, Splunk)
• Audit trail complet sur accès données sensibles
• Sauvegarde synchronisée et chiffrée (3-2-1 : 3 copies, 2 supports, 1 hors site)
• Test trimestriel du plan de récupération après sinistre (PRA)
• Documentation des problématiques et création d'une base de connaissances d'incidents

Justification : Traçabilité complète des accès, capacité de récupération en cas de sinistre.

Bénéfices : Support aux enquêtes régulatoires, conformité FDA/RGPD, résilience opérationnelle.

Défis : Coût initial d'infrastructure ; solution = déploiement progressif, cloud hybride.

PHASE 3 : PRÉPARATION ET DÉROULEMENT DU JEU DE RÔLE

5.1 Rôle choisi : Animateur de la réunion

Contexte : Nouvellement intégré au service informatique de GSB suite à l'incident USB, chargé de présenter un plan d'action au comité de direction.

5.2 Objectifs personnels du rôle

• Présenter une analyse crédible et professionnelle des risques identifiés
• Convaincre les directeurs de l'urgence d'agir et de l'importance stratégique
• Gérer les objections et les conflit potentiels avec diplomatie
• Proposer des compromis réalistes et des phases pilotes
• Aboutir à un plan d'action décidé avec responsables et calendrier défini
• Animer la réunion de manière constructive et conclure positivement

5.3 Arguments clés à développer

Argument 1 - Urgence réglementaire
"GSB est soumise à la FDA, l'EMA et aux BPF. Une faille de sécurité peut entraîner une non-conformité majeure, la suspension d'une autorisation de mise sur le marché, et des amendes de millions d'euros. L'incident USB n'est qu'un symptôme visible du problème systémique."

Argument 2 - Propriété intellectuelle
"Notre valeur réside dans nos brevets et nos données d'essais. Une fuite compromise nos avantages concurrentiels et nos investissements en R&D. Un seul incident peut coûter plus cher que 5 ans de sensibilisation à la sécurité."

Argument 3 - Risque réputationnel
"Dans le secteur pharmaceutique, la confiance est cruciale. Un scandale de sécurité endommage notre réputation auprès des patients, des agences, et des partenaires. Nous n'avons qu'une chance de bien faire."

Argument 4 - Mesures graduelles et acceptées
"Les mesures proposées ne visent pas à entraver l'innovation, mais à la sécuriser. Phase pilote en R&D, formation progressive, outils intuitifs. Nous écoutons les équipes et nous adaptons."

5.4 Profils et contrearguments anticipés

Profil	Priorité	Crainte possible	Réponse proposée
Directeur R&D	Innovation sans frein	Ralentissement, bureaucratisation	"Données protégées = liberté d'innover sans risque. Outils simples. Support DSI réactif 24/7."
Directeur Qualité	Conformité réglementaire	Audit découvrant des failles	"Plan d'action tracé, tests réguliers, documentation complète. Couvert en cas d'audit."
Directeur Opérations	Continuité et efficacité	Surcharge de travail IT	"Impact minimal sur les opérations. Automatisation des contrôles. Déploiement progressif."
Resp. Conformité RGPD	RGPD, responsabilité légale	Non-conformité RGPD	"Chiffrement, audit trail, politique de rétention claire. Couvert légalement."
Chercheurs/Techniciens	Liberté d'accès aux données	Ralentissement, frustration	"Accès rapide via VPN sécurisé. Formation dédiée. Escalade DSI réactive."

5.5 Éléments de contexte et connaissances métier

• Audit FDA potentiel suite à l'incident de sécurité
• Données critique à GSB : Formules de produits, données PK/PD, résultats d'essais cliniques, secrets de fabrication
• Contraintes opérationnelles : La R&D doit rester productive ; les essais en cours ne doivent pas être ralentis
• Budget estimé : ~100k€ pour infrastructure + 50k€ pour formation (justifier auprès du DG)
• Timeline proposée : Phase 1 (60 jours) = diagnostic + pilote R&D ; Phase 2 (180 jours) = déploiement complet

6. DÉROULEMENT DU JEU DE RÔLE

6.1 Scénario 1 : Réunion du Comité de Direction (durée : 1h30)

Participants attendus :
• Stagiaire DSI (animateur de réunion, présentateur des risques et recommandations)

• Directeur de la Recherche
• Directeur Qualité et Conformité
• Directeur des Opérations
• Responsable Conformité RGPD/Affaires légales

01:00 - Ouverture (5 min)
Rappel du contexte de l'incident USB, ordre du jour, objectif de la réunion.

01:05 - Présentation des risques (10 min)
Analyse de l'incident USB, risques identifiés, enjeux réglementaires (FDA, EMA, RGPD, audit potentiel).

01:15 - Propositions de mesures (15 min)
Présentation des 5 piliers de la solution (USB, authentification, chiffrement, formation, audit).

01:30 - Discussion / Débat (40 min)
Chaque directeur exprime ses préoccupations, échange avec les autres, négociation des compromis.

02:10 - Plan d'action décidé (15 min)
Récapitulation des décisions prises, priorités identifiées, responsables désignés, calendrier défini.

02:25 - Clôture (5 min)
Prochaines étapes, création d'un comité de pilotage, date du prochain point.

Critères de succès :
• ✓ Tous les enjeux majeurs ont été soulevés et discutés
• ✓ Accord sur au moins 3 mesures prioritaires parmi les 5 proposées
• ✓ Calendrier de mise en œuvre défini (Phase 1 : 60 j ; Phase 2 : 180 j)
• ✓ Responsables désignés pour chaque mesure
• ✓ Ressources budgétaires approuvées
• ✓ Comité de pilotage mis en place

Posture adoptée : Pédagogue, bienveillant, à l'écoute des préoccupations pratiques. Montrer que la sécurité est un élément essentiel du travail, non une entrave.

PHASE 4 : SYNTHÈSE, CONCLUSION ET RECOMMANDATIONS

7.1 Participation personnelle au jeu de rôle

Reçu en tant qu'Animateur de réunion, j'ai pu :
• Acqurir une compréhension profonde des enjeux de sécurité dans un contexte pharmaceutique réaliste
• Comprendre comment les différents départements voient la sécurité (R&D, Qualité, Opérations, RGPD)
• Pratiquer des compétences clang : argumentation, négociation, gestion de conflits, communication persuasive
• Apprécier l'importance d'adapter son message à l'audience

7.2 Compétences développées

1. Communication professionnelle
Début : Présentation claire des risques techniques, adaptation au contexte métier.
Améliorations notées : Capacité à vulgariser, à argumenter avec données, à tenir compte des contraintes opérationnelles.

2. Négociation et gestion de conflits
Début : Propose solutions techérales.
Améliorations notées : Recherche active de compromis, écoute active, proposition de phases pilotes pour réduire la résistance.

3. Connaissance métier
Début : Vérifications générale des risques informatiques.
Améliorations notées : Profonde compréhension des régulations FDA/EMA, des enjeux de propriété intellectuelle, de la conformité RGPD.

4. Leadership et animation
Début : Présentation structurée.
Améliorations notées : Capacité à diriger un débat, à s'assurer que tous les avis sont entendus, à conclure sur un accord.

7.3 Points clés retenus

• La sécurité informatique n'est pas un domaine purement technique, mais un élément de stratégie entreprise qui affecte tous les départements.

• Pour convaincre une organisation, il faut comprendre les priorités de chaque partie prenante et adapter le discours en conséquence.

• L'implémentation de mesures de sécurité dur réussir que si elle s'accompagne de sensibilisation, de formation, et de phases pilotes de test.

• La conformité réglementaire (FDA, EMA, RGPD) est un levier puissant pour justifier des investissements en sécurité.

• Le facteur humain reste le plus influent ; une formation continue est aussi importante que les outils techniques.

7.4 Compétences présentables en entretien d'embauche

Cet atelier m'a permis de développer des compétences transversales directement applicables au métier :

• Gestion de projet : Priorisation des actions, planification phasing, allocation des ressources.
• Communication inter-départementale : Création de pont entre IT et métier.
• Gestion du changement : Understanding de la résistance, proposition de solutions progressives.
• Conformité réglementaire : Compréhension des enjeux FDA, EMA, RGPD.
• Cybersecurity awareness : Sensibilisation aux risques et bonnes pratiques.

7.5 Perspectives futures

Ce TP a renforcé mon intérêt pour les domaines suivants :
• Sécurité informatique appliquée au secteur critique/pharmaceutique
• Gestion de crise et incident response
• Conformité et gouvernance IT (ITIL, ISO 27001)
• Leadership technique et gestion d'équipes IT

8. CONCLUSION

L'atelier 10 TP2 Sécurité Informatique a constitué une expérience pédagogique très enrichissante, combinant théorie et simulation pratique pour développer des compétences essentielles en sécurité informatique appliquée.

Par le biais du jeu de rôle et de l'analyse de cas réel (Galaxy Swiss Bourdin), j'ai pu :
• Renforcer ma compréhension des fondamentaux de la sécurité informatique (CIA, menaces, mitigations)
• Appréhender les spécificités du secteur pharmaceutique et ses contraintes réglementaires (FDA, EMA, RGPD)
• Implémenter un plan stratégique de sécurité prenant en compte les enjeux de tous les départements
• Développer mes compétences interpersonnelles essentielles : communication, négociation, persuasion
• Pratiquer l'animation de réunion et la gestion de conflit dans un contexte professionnel simulé

À titre personnel, j'ai apprécié la pertinence du scénario, qui reflète des situations réelles rencontrées dans l'industrie. Cela a rendu l'apprentissage concret et motivé. Les livrables attendus (cahier des charges, fiches de caractère, grille d'évaluation) ont facilité l'organisation et la conduite du jeu de rôle.

9. RECOMMANDATIONS POUR AMÉLIORATION

1. Étoffer les phases d'accompagnement
   Le jeu de rôle gagnerait à s'accompagner de courtes vidéos d'introduction (5-10 min) montrant les bonnes pratiques de négociation et de communication.

2. Ajouter des supports visuels
   Intégrer des diagrammes d'impact, des matrices de risques, des schémas d'attaque USB pour faciliter la compréhension visuelle.

3. Créer un atelier de retour d'expérience
   Prévoir une débriefing collective après le jeu de rôle, permettant une analyse critique des décisions prises et des apprentissages partagés.

4. Intégrer des équivalences avec les normes industrielles
Créer des liens avec ISO 27001, NIST Cybersecurity Framework, ou cadres de conformité existants pour renforcer la crédibilité.

5. Proposer des variantes du scénario
Diversifier les incidents d'amorce (vol de données, attentat par malware, erreur employé) pour couvrir d'autres angles du risque.
