

2024
2025

Atelier n°4

SEC101 – Cybersécurité : référentiel, objectifs et déploiement
STÉPHANE LARCHER

Implémentation de la sécurité

Atelier n°4

Atelier n°4 Implémentation de la sécurité

Table des matières

Phase 1 : Panorama des méthodes d'analyse de risque	3
Activité 1.1 : Cartographie des méthodes.....	3
Activité 1.2 : Étude de cas - Choix de méthode	3
Phase 2 : De l'analyse de risque à la PSSI.....	4
Activité 2.1 : Construction d'une PSSI	4
Activité 2.2 : Validation de cohérence.....	4
Phase 3 : Approfondissement EBIOS et fiche FEROS.....	5
Activité 3.1 : Application pratique d'EBIOS.....	5
Activité 3.2 : Élaboration de la fiche FEROS	5
Phase 4 : Déploiement et projets de sécurité	7
Activité 4.1 : Plan de déploiement	7
Activité 4.2 : Indicateurs de réussite	7
Phase 5 : Maintien en condition de sécurité	8
Activité 5.1 : Rôles RSSI et SECOPS.....	8
Activité 5.2 : Procédures opérationnelles.....	8
Livrables de l'atelier	9

Module SEC101

- i. Comparer et choisir une méthode d'analyse de risque adaptée à un contexte
- ii. Élaborer une PSSI à partir d'une analyse de risque
- iii. Appliquer la méthode EBIOS pour préparer une fiche FEROS
- iv. Définir un plan de déploiement sécurité
- v. Concevoir des procédures opérationnelles SECOPS

Phase 1 : Panorama des méthodes d'analyse de risque

Activité 1.1 : Cartographie des méthodes

En binômes :

Vous disposez de 4 méthodes d'analyse de risque. Pour chacune, identifiez :

- i. **Contexte d'utilisation optimal**
- ii. **Avantages principaux**
- iii. **Limitations**

Méthodes à analyser :

- i. **EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)**
 - a. Méthode française de l'ANSSI
 - b. Approche par scénarios de risque
 - c. 5 modules : Cadrage → Événements redoutés → Scénarios stratégiques → Scénarios opérationnels → Traitement
- ii. **ISO 27005 (Gestion des risques de sécurité de l'information)**
 - a. Standard international
 - b. Cycle : Identification → Analyse → Évaluation → Traitement → Surveillance
- iii. **MEHARI (Méthode Harmonisée d'Analyse de Risques)**
 - a. Méthode du CLUSIF
 - b. Base de connaissances intégrée
 - c. Approche quantitative et qualitative
- iv. **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**
 - a. Méthode américaine (SEI/CMU)
 - b. Focus sur les actifs critiques
 - c. Approche collaborative interne

Activité 1.2 : Étude de cas - Choix de méthode

Scénario : Une PME de 150 salariés dans le secteur de la santé digitale souhaite obtenir l'homologation ANSSI pour son nouveau système de télémedecine. L'entreprise a peu d'expertise en sécurité interne.

Questions :

- i. Quelle méthode recommandez-vous et pourquoi ?
- ii. Quels sont les 3 premiers éléments à identifier ?
- iii. Qui devrait participer à l'analyse ?

Phase 2 : De l'analyse de risque à la PSSI

Activité 2.1 : Construction d'une PSSI

Contexte : À partir de l'analyse EBIOS précédente, vous devez élaborer les grandes lignes de la PSSI.

Livrables attendus :

- i. Structure de la PSSI**
 - a. Objectifs de sécurité
 - b. Périmètre d'application
 - c. Rôles et responsabilités
 - d. Règles de sécurité principales
- ii. Cartographie des mesures organisationnelles**
 - a. Gouvernance de la sécurité
 - b. Gestion des accès et habilitations
 - c. Gestion des incidents
 - d. Sensibilisation et formation
- iii. Schéma de sécurité technique**
 - a. Architecture sécurisée
 - b. Mesures de protection technique
 - c. Mesures de détection
 - d. Mesures de réaction

Activité 2.2 : Validation de cohérence

Checklist de validation :

- i. ☐ Les mesures couvrent-elles tous les risques identifiés ?
- ii. ☐ Les responsabilités sont-elles clairement définies ?
- iii. ☐ Les mesures sont-elles proportionnées aux enjeux ?
- iv. ☐ Le schéma technique est-il cohérent avec l'organisation ?

Phase 3 : Approfondissement EBIOS et fiche FEROS

Activité 3.1 : Application pratique d'EBIOS

Cas d'étude : Système de gestion des dossiers patients

- i. **Module 1 - Cadrage et biens essentiels :**
 - a. Identifiez 5 biens essentiels
 - b. Définissez leurs critères de sécurité (DICPN)
 - c. Cartographiez leurs relations
- ii. **Module 2 - Événements redoutés :**
 - a. Listez 3 événements redoutés prioritaires
 - b. Évaluez leur impact (Faible/Limité/Important/Critique)
- iii. **Module 3 - Scénarios stratégiques :**
 - a. Identifiez les sources de risque
 - b. Associez-les aux objectifs visés
 - c. Évaluez la pertinence de chaque couple
- iv. **Module 4 - Scénarios opérationnels :**
 - a. Détaillez un scénario d'attaque complet
 - b. Identifiez les vulnérabilités exploitées
 - c. Évaluez la vraisemblance

Activité 3.2 : Élaboration de la fiche FEROS

Structure de la fiche FEROS :

- i. **Identification du système**
 - a. Nom et version
 - b. Périmètre d'homologation
 - c. Classification
- ii. **Contexte sécuritaire**
 - a. Enjeux métier
 - b. Environnement d'utilisation
 - c. Menaces principales
- iii. **Objectifs de sécurité**
 - a. Fonction de sécurité requises
 - b. Niveau de robustesse attendu
 - c. Critères d'évaluation
- iv. **Architecture de sécurité**
 - a. Composants de sécurité
 - b. Mécanismes de protection
 - c. Points de contrôle

Livrable : Remplir les sections 1 et 2 pour votre cas d'étude

Phase 4 : Déploiement et projets de sécurité

Activité 4.1 : Plan de déploiement

Objectif : Définir un plan de déploiement des mesures de sécurité

Template de planning :

Phase	Mesures	Durée	Prérequis	Ressources	Indicateurs
Phase 1 : Socle					
Phase 2 : Spécialisé					
Phase 3 : Avancé					

Critères de priorisation :

- i. Criticité du risque couvert
- ii. Facilité de mise en œuvre
- iii. Coût d'implémentation
- iv. Dépendances techniques

Activité 4.2 : Indicateurs de réussite

Définissez 5 KPI pour mesurer l'efficacité du déploiement :

- i. **Indicateur de conformité** (ex: % de mesures déployées)
- ii. **Indicateur de performance** (ex: temps de détection d'incident)
- iii. **Indicateur de couverture** (ex: % d'actifs sécurisés)
- iv. **Indicateur d'efficacité** (ex: réduction du nombre d'incidents)
- v. **Indicateur de maturité** (ex: niveau de sensibilisation)

Phase 5 : Maintien en condition de sécurité

Activité 5.1 : Rôles RSSI et SECOPS

Matrice RACI à compléter :

Activité	RSSI	SECOPS	DSI	Métier
Définition de la politique				
Surveillance 24/7				
Réponse à incident				
Mise à jour sécuritaire				
Formation utilisateurs				
Audit de conformité				

Légende : R=Responsable, A=Autorité, C=Consulté, I=Informé

Activité 5.2 : Procédures opérationnelles

Rédigez une procédure type pour la gestion d'incident :

- i. Détection et signalement**
 - a. Canaux de remontée
 - b. Critères de qualification
 - c. Délais de signalement
- ii. Qualification et classification**
 - a. Grille de criticité
 - b. Processus d'escalade
 - c. Notification des parties prenantes
- iii. Containment et investigation**
 - a. Mesures de confinement
 - b. Collecte de preuves
 - c. Analyse forensique
- iv. Résolution et communication**
 - a. Plan de remédiation
 - b. Communication externe
 - c. Retour d'expérience

Livrables de l'atelier

Document de synthèse (3-4 pages) contenant :

- i. **Analyse comparative** des méthodes d'analyse de risque
- ii. **Ébauche de PSSI** avec schéma de sécurité
- iii. **Extrait de fiche FEROS** (sections 1 et 2)
- iv. **Plan de déploiement** avec indicateurs
- v. **Procédure opérationnelle** de gestion d'incident