# Atelier S5 — Diagnostic cyber et plan d'action

**DOSSIER ÉTUDIANT • NOVACHIPS**

| Atelier | Évaluation finale | Organisation |
|---|---|---|
| S5.3 : 40 min | E2 : 80 min après l'atelier | Groupes de 3 à 4 |

## Contexte et mission

Novachips est une entreprise fictive qui personnalise des chips avec photos et messages. Elle dispose d'un site commercial, d'un intranet, d'outils IA et d'un SOC de simulation. La direction souhaite une vision claire des principaux risques liés à ses usages numériques et IA, ainsi qu'un plan de traitement réaliste. Votre équipe intervient comme cellule conseil en cybersécurité.

## Environnements et dossier de référence

- Site commercial — https://novachips.portail-cyber.akademiedudigital.com/site-accueil.html
- Intranet — https://novachips-intranet.portail-cyber.akademiedudigital.com/intranet-accueil.html
- SOC de simulation — https://novachips-soc.portail-cyber.akademiedudigital.com/plateforme-soc.html

Capitaliser sur vos traces des ateliers S1 à S4 : actifs et données (S1), fraude et phishing (S2), protection des données et outils IA (S3), investigation des alertes (S4). Aucune vulnérabilité ou compromission ne doit être présentée comme confirmée sans preuve.

## Objectifs opérationnels

- Formuler des risques concrets en distinguant actifs, événements redoutés, causes et conséquences.
- Évaluer la priorité des risques avec une échelle simple, explicite et argumentée.
- Préconiser des contrôles proportionnés, des responsables et des échéances.
- Mettre en place une veille documentée et rendre compte à une direction non technique.

## Déroulement S5.3 — 40 minutes

| Phase | Temps | Livrable intermédiaire |
|---|---|---|
| 1. Synthèse | 5 min | Sélectionner 4 à 5 risques en réutilisant les éléments établis lors des ateliers précédents. |
| 2. Registre | 15 min | Renseigner actif, scénario de risque, impact, vraisemblance, criticité et justification. |
| 3. Plan d'action | 15 min | Définir 3 actions prioritaires, responsables, délai et trace de suivi. |
| 4. Restitution | 5 min | Préparer la présentation et répartir les interventions |

| | | |
|---|---|---|
| | | individuelles. |

## Méthode de priorisation (exercice pédagogique simplifié)

Impact (I) : 1 faible, 2 significatif, 3 majeur. Vraisemblance (V) : 1 peu probable, 2 plausible, 3 probable. Score indicatif : I × V, de 1 à 9 ; 1–2 faible, 3–4 modéré, 6–9 élevé. Les scores ne remplacent pas la justification des hypothèses ni une analyse de risques professionnelle complète.

## Risques à examiner — pistes, pas des constats

- Usage d'un assistant IA avec un dossier de commande contenant images et coordonnées client.
- Fraude par e-mail usurpant un fournisseur ou un dirigeant.
- Accès non autorisé à l'intranet ou divulgation accidentelle de documents.
- Mauvaise interprétation d'une alerte SOC et mesure de réponse inadaptée.
- Perte de disponibilité du site public ou fuite d'informations liées aux commandes.

## Livrables et restitution E2 — distincte de l'atelier

Remettre : (1) diagnostic court de Novachips, (2) registre priorisé de 4 à 5 risques, (3) plan d'action de 3 mesures, (4) fiche de veille sourcée. Pendant E2 (80 minutes pour l'ensemble des groupes), présenter la synthèse et répondre individuellement aux questions. La répartition des temps de passage sera annoncée par le formateur en fonction du nombre de groupes.

## Règles et documentation

Travail exclusivement sur les plateformes pédagogiques. Ne pas tester d'attaque, ne pas exploiter de données personnelles réelles. Sources : ANSSI https://cyber.gouv.fr/ ; CNIL https://www.cnil.fr/fr/intelligence-artificielle ; NIST AI RMF https://www.nist.gov/itl/ai-risk-management-framework ; AI Act https://eur-lex.europa.eu/eli/reg/2024/1689/oj