Atelier S4 — Investigation cyber assistée par IA

DOSSIER ÉTUDIANT • NOVACHIPS

Durée	Organisation	Positionnement
50 minutes	Groupes de 3 à 4	S4.3 — Investigation assistée par IA, après S4.2

Mission professionnelle

Novachips, entreprise fictive spécialisée dans les chips personnalisées, dispose d'un SOC de simulation. Votre équipe est sollicitée pour étudier une alerte, déterminer ce qui est établi, construire des hypothèses et comparer votre analyse à une aide produite par IA. La mission est exclusivement défensive : aucune intrusion ni modification d'un système réel.

Plateformes à consulter

- SOC Novachips — https://novachips-soc.portail-cyber.akademiedudigital.com/plateforme-soc.html
- Intranet Novachips — https://novachips-intranet.portail-cyber.akademiedudigital.com/intranet-accueil.html
- Plateforme formateur (contexte uniquement) — https://novachips-trainer.portail-cyber.akademiedudigital.com/accueil-formateur.html
- Site Novachips — https://novachips.portail-cyber.akademiedudigital.com/site-accueil.html

Les modules SOC peuvent présenter des alertes, des flux réseau, des événements EDR, des incidents corrélés et des signalements issus de la messagerie. Les données disponibles varient selon le scénario de simulation. N'inventez ni identifiant ni événement absent de l'interface.

Objectifs de l'atelier

- Lire une alerte et relier plusieurs traces (horodatage, hôte, compte, source, sévérité).
- Distinguer fait observé, hypothèse d'incident et conclusion vérifiée.
- Mesurer l'intérêt et les limites d'une assistance IA pour résumer et interpréter des journaux.
- Proposer une action de traitement proportionnée sans assimiler une anomalie à une attaque confirmée.

Déroulement — 50 minutes

Phase	Durée	Action
1. Repérage	5 min	Ouvrir le SOC, identifier les sources visibles et sélectionner une alerte ou un incident.
2. Investigation humaine	15 min	Collecter au moins 3 traces compatibles ; renseigner chronologie, observations et hypothèses.

3. Assistance IA	15 min	Comparer une synthèse IA fournie en séance ou solliciter un assistant autorisé sur des données fictives nettoyées.
4. Vérification	10 min	Contrôler chaque affirmation IA contre les traces, relever les erreurs, proposer des contrôles adaptés.
5. Restitution	5 min	Présenter une conclusion argumentée et une incertitude.

Pièce de secours — Jeu de données pédagogique fictif

À utiliser uniquement si le SOC est indisponible ou si aucune alerte exploitable n'est présentée. Ces lignes sont créées pour cet atelier et ne proviennent pas des plateformes.

Heure	Source	Événement simulé
09:12	Messagerie	Signalement d'un e-mail demandant une connexion urgente depuis un lien inattendu.
09:18	Authentification	Cinq échecs de connexion sur le compte atelier.compta depuis une adresse inconnue.
09:21	Authentification	Connexion réussie du même compte ; second facteur : non renseigné dans ce journal.
09:23	Flux réseau	Connexion sortante de 145 Mo depuis poste-C07 ; destination et motif non qualifiés.
09:25	EDR	Aucun événement malveillant confirmé dans les données fournies.

Synthèse IA fictive à vérifier (si pas d'assistant disponible)

« Une cyberattaque est confirmée : l'e-mail a permis de compromettre le compte comptable puis d'exfiltrer 145 Mo. L'EDR confirme l'installation d'un malware. Il faut bloquer immédiatement tout le réseau. »

Cette synthèse contient volontairement des conclusions qui ne sont pas démontrées par les traces. Identifiez les affirmations non étayées et précisez les vérifications nécessaires.

Travail attendu

- Choisir un événement de départ et citer son horodatage, sa source et sa sévérité si elle est affichée.
- Relever trois observations vérifiables et produire une chronologie courte.

- Formuler deux hypothèses, les informations manquantes et les contrôles permettant de trancher.
- Comparer l'analyse IA aux faits : vrai, plausible non confirmé, faux / non étayé.
- Préconiser trois actions de défense (vérifier, signaler, contenir de façon proportionnée) en précisant les limites.

Livrable et règles

Compléter la fiche de réponse S4. N'utiliser que des données fictives ; ne pas copier de données personnelles ou d'identifiants réels dans une IA externe. Aucune action de réponse simulée sur la plateforme ne doit être assimilée à une action sur un SI réel.

Références

ANSSI : https://cyber.gouv.fr/ • NIST CSF : https://www.nist.gov/cyberframework • MITRE ATT&CK : https://attack.mitre.org/