Sujet d'examen

Intitulé	Cas pratique – Sensibilisation et Orientation dans le paysage cyber		
Référence	ECSI3-Evaluation-01	Durée	1 jour

- Type d'évaluation : **Individuelle**
- Ressources autorisées : Cours, Ordinateur, Internet, LLM[1]

Objectifs pédagogiques

Évaluer les compétences du module d'enseignement du bloc 1 suivant :

- CYBER-100 Introduction à la sécurité
- CYBER-101 Comprendre les enjeux de sécurité et les facteurs de risques associés
- CYBER-103 Connaître le marché de la sécurité, les acteurs et les outils

Compétences évaluées

- C16 : Identifier les enjeux cyber auxquels l'entreprise est confrontée, en distinguant les différents types d'attaquants, en appréhendant la diversité des motivations, en identifiant les diverses sortes d'attaques et leurs conséquences et en reconnaissant les fragilités les plus courantes des systèmes d'information pour inscrire la démarche de sécurité dans le contexte global.
- C20 : Identifier les différents acteurs de l'écosystème de la cybersécurité étatiques ou industriels, en comprenant les rôles respectifs des acteurs étatiques et en évaluant les solutions technologiques proposées par différents fournisseurs, afin de solliciter les acteurs appropriés et de choisir les solutions de sécurité pertinentes et adaptées à la structure.

[1] Utilisation pertinente et judicieuses des LLM, vous serez sanctionné en cas d'abus.

Évaluation du bloc

Cas pratique - Plateforme d'orientation cyber pour entreprises débutantes

En 2026, l'offre d'informations en cybersécurité est abondante, mais reste difficile à exploiter pour une entreprise qui débute. Les sources sont nombreuses, hétérogènes, et il est rarement évident de savoir par où commencer. Grâce aux modules suivis, vous disposez désormais des connaissances et d'une vision d'ensemble du marché de la cybersécurité, ce qui vous permet de jouer un rôle de guide et de médiateur pour aider une organisation à structurer ses premiers pas.

Objectif :

Votre mission est de concevoir une plateforme sous forme de site internet qui aide une organisation à démarrer son parcours de sécurisation en :

1. sensibilisant les publics internes (employés, IT, dirigeants)
2. orientant l'entreprise vers les bonnes démarches, bonnes sources, bonnes obligations, bons interlocuteurs, et bonnes catégories d'outils, selon son contexte

Le site doit fonctionner comme un guide, à la manière d'une plateforme d'orientation, avec une logique proche de "je réponds à quelques questions et j'obtiens une trajectoire claire".

Livrables attendus

- 1 site internet
- 1 rapport PDF

Vous remettrez un rapport PDF contenant obligatoirement :

1. Le lien du site publié (livrable principal noté)
2. Une note de démarche de 10 à 20 lignes maximum expliquant vos choix (structure, logique de parcours, comment vous avez sélectionné et organisé l'information)
3. Des captures d'écran de vos pages (screenshots) pour figer le contenu en cas d'indisponibilité du site

Le site doit être accessible publiquement via un lien. Le rapport doit permettre l'évaluation même si le site devient indisponible via les captures des écrans du site.

Contraintes de réalisation

- Le rendu doit être un site publié (obligatoire pour avoir tous les points)
- Le site doit être navigable (menus, liens, parcours) et compréhensible
- Le design, le responsive, l'esthétique ne sont pas notés
- Aucune pénalité liée au style graphique, aux couleurs, à la mise en forme
- L'évaluation porte sur l'organisation de l'information, la qualité pédagogique, et la pertinence de l'orientation

Indications de réalisation

- L'essentiel c'est le contenu pas la technologie derrière. Ne perdez pas de temps à déployer votre plateforme.
- Contentez-vous d'outils et de plateforme gratuite.
- Outils possibles :
  - Framer ou Wix (recommandé)
  - Figma / Penpot (maquette cliquable)
  - Vibe-coding
  - No-code
- Organisez vos idées et structurez-les avant de démarrer la création du site.
- Pour les images, utilisez du contenu gratuit (https://unsplash.com/) ou du contenu généré gratuitement par IA (ChatGPT ou Google Gemini)
- Utilisez les LLMs à bon escient, sans quoi vous serez pénalisé.
- Si vous êtes dans l'incapacité de créer une plateforme Web, vous pouvez utiliser un logiciel de présentation comme PowerPoint.

Contenu attendu

Général

Dans votre plateforme vous devez permettre à une entreprise de se reconnaître selon son contexte :

- au moins 4 secteurs ou contextes au choix (ex : e-commerce, industrie/OT, collectivité, santé, SaaS/IT, association, éducation, finance)
- actifs critiques typiques
- menaces dominantes et conséquences prévisibles (arrêt d'activité, pertes financières, sanctions, atteinte réputationnelle, risques humains)
- distinguer IT et OT quand pertinent

Expliquez-votre démarche et pourquoi votre plateforme existe.

Espace de sensibilisation (multi profils)

Créer un espace qui parle au minimum à 3 profils :

- Employé
- Équipe IT
- Dirigeant

Exemples de notions attendues (liste non exhaustive) :

- vocabulaire et notions clés (risque, menace, vulnérabilité, impact, surface d'attaque…)
- menaces actuelles illustrées par des exemples concrets (phishing, rançongiciel, fuite de données, compromission de comptes, perte de matériel, erreurs humaines)
- bonnes pratiques et premières mesures actionnables (hygiène numérique, MFA, mises à jour, sauvegarde, gestion des accès)
- au moins un contenu "action" : checklist, quiz, scénario, fiche réflexe

Orientation réglementaire et normative

Pour la partie orientation réglementaire et normative, vous mettrez en place un dispositif simple permettant d'associer un contexte d'entreprise à des textes, obligations ou référentiels pertinents. Vous pouvez, par exemple, utiliser un questionnaire court, une arborescence de choix, ou un parcours par profils et secteurs. Le résultat attendu est une restitution lisible qui liste les réglementations et référentiels applicables ou probables selon le cas, en expliquant brièvement le périmètre, les implications concrètes à haut niveau et quelques premières actions raisonnables à initier. Les informations doivent être sourcées à partir de ressources publiques récentes.

Orientation vers acteurs, prestataires, outils

Le site doit proposer une orientation structurée vers :

- acteurs étatiques et ressources (ANSSI, CERT-FR, Cybermalveillance.gouv.fr, CNIL, etc.)
- prestataires (ex : MSSP/SOC, réponse à incident, audit, pentest, sensibilisation) avec leurs noms
- catégories d'outils (EDR/XDR, IAM, sauvegarde, CTI, scan vulnérabilités, MDM, segmentation, supervision…) avec le nom des éditeurs et les technologies

Attendus :

- une logique "qui contacter selon la situation" et "quoi prioriser"
- une articulation simple entre : niveau de menace, impact, urgence, et interlocuteurs adaptés
- Vous devez mentionner au mininum 5 acteurs, 5 prestataires et 5 catégories, et chaque catégorie doit posséder aux moins 3 éléments.

Barème de notation (indicatif)

Critère	Points
• Qualité de la présentation de la démarche aux visiteurs du site. • Prise en comptes des divers contextes et environnements métier. • Pertinence des sources utilisées	/4
Couverture complète et navigable des 4 domaines : 1. Sensibilisation 2. Normes et réglementations 3. Prestataires 4. Outils	/8
Site publié et accessible via lien (livrable principal)	/2
Qualité de rédaction et de structuration de l'information (pédagogie, lisibilité, orientation)	/4
Respect des consignes et fourniture d'un rapport PDF expliquant la démarche de réflexion	/2

Modalités d'organisation

- Mode : Présentiel
- Surveillance : Personnel administratif Epita / SecureSphere
- Horaires :
  - 09h30 – 12h30
  - 13h45 – 17h30
- Pauses :
  - A votre convenance

Versions du document

Action	Nom	Version	Date
Création du document	LPE	1.0	2026-01-27