RÈGLEMENT DES ÉTUDES
Diplôme de Sciences Po Saint-Germain-en-Laye
Analyste en gouvernance et sécurité du numérique (DAGSEN)
2025-2026

Préambule

Le diplôme d'Analyste en gouvernance et sécurité du numérique (DAGSEN) est un diplôme délivré par Sciences Po Saint-Germain-en Laye, accessible aux professionnels et aux étudiants justifiant un niveau bac +4 (Master 1 ou Maîtrise).
Il peut être suivi en même temps que la deuxième année d'un master proposé à Sciences Po Saint-Germain-en-Laye ou dans un autre établissement d'enseignement supérieur ou indépendamment de toute autre inscription sous réserve de la compatibilité des créneaux horaires.
Ce diplôme propose une formation visant à donner une compréhension approfondie des risques et des défis numériques qui affectent l'ensemble des secteurs et activités professionnelles.
Il aborde la cybersécurité sur les aspects techniques, humains et sociaux, ceux-ci sont analysés sous l'angle des connaissances et de l'expertise issues des recherches en sciences sociales, en mobilisant des approches issues des sciences sociales, des sciences et technologies.
La formation permet d'acquérir des connaissances théoriques et pratiques nécessaires pour appréhender les enjeux globaux de conflictualité et de menace dans le champ numérique. Elle comprend également des mises en situation professionnelle afin de favoriser l'appropriation de méthodes et de pratiques opérationnelles dans le domaine de la cybersécurité.

1 – Accès au DAGSEN

La formation est ouverte aux candidats titulaires ou en cours d'acquisition d'un diplôme d'Etat égal ou supérieur au niveau Bac+4 (240 ECTS).
La sélection se fait par l'étude de dossier (CV, lettre de motivation, relevés de notes, attestation de diplôme ou d'ECTS).

2 – Validation des Acquis Personnels et Professionnels (VAPP)

Une procédure de validation des acquis professionnels et personnels est possible pour les candidats ne bénéficiant pas d'un niveau académique suffisant, mais ayant eu une expérience professionnelle importante. Le processus de validation - dit VAPP - se fait conformément aux exigences de l'IEP.
Sur la base des informations contenues dans le dossier de candidature, le directeur de l'IEP, en concertation avec la direction du DAGSEN, valide l'accès au diplôme.
La demande de VAPP doit se faire avant de candidater à la formation.
Deux conditions réglementaires sont requises pour pouvoir faire une demande de VAPP, avoir au moins 20 ans et avoir interrompu ses études initiales depuis au moins 2 ans.
Une demande de VAPP n'est valable que pour le diplôme et l'année universitaire choisie.
Le dispositif de VAPP ne dispense pas du processus de sélection des candidats.

3 – Modalités et jury de sélection
Les dossiers de candidatures sont examinés par un jury de sélection composé d'au moins deux personnes dont le directeur du diplôme.
Le jury de sélection évalue chaque candidature – niveau requis atteint, objectif professionnel, motivations personnelles, avant d'accepter ou refuser une candidature au DAGSEN.
L'acceptation est communiquée aux candidats admis, assortie des conditions administratives d'inscription au DAGSEN émises par le service de la formation continue de Sciences Po Saint-Germain-en-Laye.

4 - Statut des apprenants
Le DAGSEN est un diplôme qui est ouvert à la fois aux professionnels et aux étudiants en formation initiale. Les apprenants du DAGSEN relèvent donc de l'un de ces deux statuts : stagiaire de la formation continue ou étudiant en formation initiale.

Le statut des stagiaires de la formation continue se caractérise par les éléments suivants :
- Un conventionnement avec Sciences Po Saint-Germain-en-Laye (convention dans le cas d'une personne morale de droit public ou privé et contrat à titre individuel dans le cas d'une personne physique),
- Une possibilité de financement par un organisme public ou privé.

Les étudiants en formation initiale sont inscrits dans un cursus universitaire diplômant. Leur statut comprend :
- Une inscription administrative au sein de leur université ou école d'origine,
- L'accès aux dispositifs pédagogiques,

- Une intégration du DAGSEN dans leur parcours académique, avec un encadrement universitaire.

5 – L'inscription administrative

L'inscription administrative et les droits afférents sont annuels.

Les droits d'inscription sont fixés et votés par le Conseil de Sciences Po Saint-Germain-en-Laye.

L'inscription est obligatoire et intervient une fois la candidature acceptée. Elle consiste à remplir un dossier d'inscription ainsi qu'un dossier de prise en charge du coût de la formation, le cas échéant. A la suite de la réception du dossier d'inscription, un certificat de scolarité ainsi qu'une carte étudiante/stagiaire seront établis.

Pour un stagiaire de la formation continue, l'entrée en formation est confirmée par l'un ou l'autre des documents suivants :

- Une convention de formation, conforme aux dispositions des articles L. 6353-1 du code du travail si l'action de formation fait l'objet d'une prise en charge par un tiers.
- Un contrat de formation, conforme aux dispositions de l'article L. 6353-3 du code du travail, si le stagiaire entreprend à titre individuel une formation et/ou finance personnellement tout ou partie de sa formation.
- Une convention de partenariat spécifique

Sciences Po Saint-Germain-en-Laye doit être avisé des modalités spécifiques de prise en charge des frais de formation au moment de l'inscription administrative, et en tout état de cause, avant le démarrage de la formation.

Aucun apprenant ne peut être diplômé avant paiement intégral de ses droits d'inscription.

6 - Organisation de la formation et obligations

6.1 - Comité de pilotage

Le comité de pilotage du DAGSEN a pour vocation l'évaluation interne de la formation dans une démarche d'amélioration continue, en réunissant la direction du diplôme. Il a pour mission d'éclairer les objectifs de la formation, de contribuer à en faire évoluer les contenus ainsi que les modalités d'enseignement et permet d'en améliorer le contenu, afin de faciliter l'appropriation des connaissances et des compétences.

Il se réunit au moins une fois par an par tout moyen afin de dresser un bilan de la formation et émet des recommandations.

Le comité de pilotage prend, notamment appui sur les bilans pédagogiques établis par l'équipe enseignante.

Il est rattaché au conseil de perfectionnement. À ce titre, il lui présente annuellement ses analyses, conclusions et propositions d'évolution relatives aux objectifs pédagogiques, aux contenus de formation et aux modalités d'enseignement.

6.2 - Déroulé de la formation

La formation, d'une durée de 98 heures se répartit en sessions de formation en présentiel d'une à trois journées par mois.
Un QCM et un cas pratique testeront les connaissances apprises.
Les apprenants devront également rédiger un mémoire d'étude de cas et le soutenir devant un jury composé de spécialistes de la cybersécurité.

6.3 - Suivi de la formation

Le suivi de la formation est assuré par la direction du diplôme, l'administration du service de la formation continue ainsi que par le secrétariat général de Sciences Po Saint-Germain-en-Laye.

6.4 – Assiduité

Les apprenants sont dans l'obligation de respecter le planning pédagogique communiqué et d'être assidu. Ils doivent attester régulièrement de leur présence par la signature de feuilles d'émargement qui leur seront remises. Elles sont exigées par les organismes financeurs et permettent aux stagiaires de percevoir leur salaire ou indemnité selon leur situation.
Les feuilles d'émargement doivent être rendues sans retard, en fonction des consignes qui seront données par la direction du diplôme et/ou le secrétariat pédagogique de la formation continue.
La direction du DAGSEN se réserve le droit de considérer comme défaillant un apprenant qui aurait été absent à plus de 30% du total des enseignements.

6.5 - Dispense d'assiduité

Un aménagement du parcours de formation peut être proposé aux stagiaires pour prendre en compte la comptabilité de la formation avec leur activité professionnelle et/ou l'individualisation de leur parcours de formation contenu de leur expérience professionnelle.
Cet aménagement peut prendre la formation d'une dispense d'assiduité pouvant aller jusqu'à deux séminaires.
Cet aménagement est pensé par la direction de la formation et peut être modifié en fonction du profil des inscrits.

Un aménagement peut également être accordé, à titre exceptionnel, aux étudiants en formation initiale répondant aux critères définis à l'article 12 de l'arrêté du 22 janvier 2014, relatif à l'organisation des études dans l'enseignement supérieur, notamment en cas de double cursus, d'activité salariée régulière, de responsabilités particulières (familiales, électives, etc.) ou de situation de handicap. Toute demande devra être justifiée et validée par la direction du diplôme.

6.6 - Campus numérique

Le DAGSEN propose un accès aux supports de cours par le biais d'une plateforme pédagogique dénommée Campus numérique.
Cette plateforme dispose de l'ensemble des outils nécessaires pour suivre un enseignement à distance : dépôt et stockage de ressources, classe virtuelle, forum, QCM, calendrier, messagerie interne, relevés de connexion et registres d'utilisation.
Pour accéder au campus numérique, chaque apprenant reçoit par courriel un identifiant et un mot de passe. Les utilisateurs de la plateforme sont seuls responsables de la préservation et de la confidentialité de leur identifiant et s'engagent à ne pas communiquer, céder ou vendre leur identifiant à un tiers.
Le non-respect de ces engagements entrainera la suppression du compte de l'apprenant.
L'accès au campus numérique est possible pendant toute la durée de la formation. Les modalités d'utilisation du campus numérique sont précisées dans le protocole individuel communiqué à l'apprenant à l'issue de son inscription administrative au DAGSEN.

7 - Modalités d'évaluation des enseignements et conditions d'obtention du diplôme

Les modalités d'appréciation de l'acquisition des compétences et des connaissances précisent le nombre d'épreuves, leur nature (répartition entre épreuves écrites et orales) et les coefficients affectés à celles-ci.
Ces modalités sont obligatoirement portées à la connaissance des apprenants.

7.1 - Convocation aux examens

La convocation des apprenants aux épreuves écrites et orales est faite par e-mail à leur adresse institutionnelle, communiquée lors de l'inscription administrative, au plus tard 15 jours avant le début des épreuves. Il appartient à chaque apprenant de consulter régulièrement cette messagerie.

La convocation précise la date, l'heure, le lieu de l'examen et les modalités de celui-ci, le cas échéant.

7.2 - Déroulement des épreuves

Le contrôle des connaissances est effectué par une session d'examens portant sur les enseignements de l'année écoulée. Les examens peuvent être dématérialisés.
L'évaluation des séminaires s'effectue sous la forme d'un QCM, d'un cas pratique et de la soutenance d'un mémoire. Le mode d'évaluation choisi ainsi que les solutions techniques retenus sont portés à la connaissance des apprenants via le campus numérique ou via messagerie électronique au plus tard un mois avant l'examen.

7.3 - Conditions techniques

L'apprenant doit disposer d'un outil de communication numérique lui permettant de pouvoir éventuellement passer l'examen dans de bonnes conditions (navigateur à jour, connexion Internet suffisante et stable, vérification de ses codes d'accès).
L'apprenant est seul responsable de son matériel et du bon fonctionnement de celui-ci. Tout apprenant ne disposant pas du matériel adéquat est tenu de se signaler au secrétariat pédagogique de la formation continue au plus tard 10 jours avant l'examen.

7.3 - Ponctualité

Le respect de l'heure de convocation à l'examen ou de rendu des travaux est obligatoire. Il est conseillé à l'apprenant de se connecter à l'espace d'examen quelques minutes avant le début de l'épreuve afin d'éviter tout retard lié à un problème de connexion. Tout retard devra être justifié.

7.4 - Déroulement de l'épreuve

L'apprenant s'engage à composer seul et personnellement, à ne pas communiquer avec ses pairs pendant toute la durée de l'épreuve, à ne pas s'absenter et à ne pas consulter d'autres documents ou ressources que ceux explicitement autorisés par l'enseignant et mentionnés sur le sujet de l'épreuve.

7.5 - Dispositifs de surveillance

Des logiciels de surveillance d'examen, de détection de plagiat, rapports de connexion et d'activité sur le campus numérique pourront être utilisés par les correcteurs, y compris dans le cadre d'examen avec correction automatique.

7.6 - Notation des séminaires

Le contrôle des connaissances est effectué par une session d'examen unique portant sur les enseignements dispensés durant la formation.

Il n'est pas prévu de seconde session. En cas d'impossibilité d'être présent aux épreuves (maladie, mission professionnelle, incident technique…), le stagiaire ou l'étudiant devra en informer dans les 48h qui suivent la tenue de l'épreuve, le directeur de la formation qui proposera une nouvelle épreuve du même type.

Un nombre déterminé de séminaires, défini en début d'année en fonction de leur nature, pourra ne pas être soumis à évaluation.

L'évaluation de ces connaissances s'effectue sous la forme d'un QCM. L'épreuve dure entre 1 et 2 heures selon le nombre de questions du QCM.

La notation se fait sur l'ensemble des séminaires avec une note sur 20 valant 25% de la note finale.

L'évaluation des connaissances prend également la forme d'un cas pratique**.** La notation de cette épreuve est également sur 20 et représente 25 % de la note finale**.**

Les apprenants sont également tenus de réaliser un mémoire d'étude de cas qui donne lieu à une soutenance devant un jury (comme précisé à l'article 10). Ce mémoire et sa soutenance sont notés sur 20 et constituent 50% de la note finale. Chaque apprenant bénéficie d'un tuteur/tutrice de mémoire, choisi parmi l'un ou l'une des enseignants des séminaires et d'un encadrement sous la forme de l'envoi en début de formation d'un conducteur méthodologique de recherche par le directeur du DAGSEN, puis d'une ou deux réunions avec le(a) tuteur/tutrice.

La soutenance se tient en présence du responsable de la formation ou de son représentant et d'au moins un professionnel de la cybersécurité.

Elle a lieu soit dans les locaux de Sciences Po Saint-Germain-en-Laye, soit dans tout autre lieu adéquat à l'exercice.

Le DAGSEN, est un diplôme d'établissement ne donnant pas lieu à la délivrance d'ECTS.

8 - Fraudes, plagiat, usage abusif de l'intelligence artificielle

Dans le cadre des évaluations et de la rédaction du mémoire d'étude de cas, les apprenants sont tenus de respecter strictement les règles en matière de prévention de la fraude et du plagiat.

Toute production soumise à évaluation doit être personnelle. Le recours à des sources externes, y compris à des outils de génération de texte par intelligence artificielle, n'est autorisé que s'il est explicitement mentionné, conformément aux exigences de citation académique. L'omission de cette mention constitue un acte de plagiat.
L'équipe pédagogique de Sciences Po Saint-Germain-en-Laye se réserve la possibilité de vérifier, via l'utilisation de logiciels adaptés, la régularité des travaux réalisés par les apprenants.
Présenter comme sien un contenu généré par une tierce personne ou un outil d'intelligence artificielle, sans mention explicite, est considéré comme une fraude.
Conformément aux dispositions du Règlement Intérieur de Sciences Po Saint-Germain-en-Laye, en cas de fraude ou tentative de fraude, un procès-verbal est établi et transmis au Président de l'université, qui peut engager des poursuites disciplinaires. L'apprenant concerné poursuit l'épreuve normalement, sa copie est corrigée mais la note reste confidentielle jusqu'à décision de la section disciplinaire.
Aucune sanction ni note zéro ne peut être appliquée sans décision disciplinaire. L'admission éventuelle est provisoire et aucun document officiel ne peut être délivré avant le jugement. En cas de sanction affectant les résultats, le jury se réunit à nouveau.

9 - Défaillance et redoublement

Le DAGSEN ne donne pas lieu à un droit au redoublement.
Toute absence aux épreuves qu'il s'agisse du QCM, du cas pratique ou de la soutenance du mémoire d'étude de cas devra être justifiée dans un délai maximum de 48 heures.
Toute absence non justifiée à l'un des examens entraîne la déclaration de défaillance de l'apprenant.
En cas d'absence à une épreuve, et sous condition de l'avoir justifié, il sera envisagé par le jury du DAGSEN de proposer une autre date d'épreuve à titre exceptionnel.

10. Composition du jury de délibération

Le jury est composé d'au moins deux personnes, du tuteur/tutrice de mémoire et du directeur du DAGSEN.
La composition du jury fait l'objet d'un arrêté de la direction de Sciences Po Saint-Germain-en-Laye.

Il se réunit en juillet de chaque année pour délibérer sur le respect des conditions d'obtention du diplôme.
Le jury est garant du respect des modalités de contrôle, d'évaluation des connaissances et d'acquisition des compétences (programme, règlement, déroulement correct des épreuves, égalités des candidats) prévues par le règlement et la maquette de la formation.
Il s'appuiera sur les notes obtenues au QCM, au cas pratique ainsi qu'à la soutenance du mémoire.

Le jury délibère souverainement à partir de l'ensemble des résultats obtenus par les apprenants. Les délibérations du jury sont strictement confidentielles, et aucun de ses membres n'est habilité à en divulguer les résultats. Les décisions du jury sont définitives et sans appel, à l'exclusion d'erreurs matérielles, dont la correction doit être effectuée par le directeur de la formation.
A l'issue de la délibération, sont établis :
- Un procès-verbal récapitulatif des résultats auquel est annexé une feuille d'émargement comportant la signature des membres présents,
- Un relevé de notes pour chaque apprenant conforme au procès-verbal.

Aucune modification ne peut être apportée sur les procès-verbaux après délibération du jury.

11. Délivrance du Diplôme

Pour valider le DAGSEN, l'apprenant doit obtenir une moyenne supérieure ou égale à 10/20. La réussite du DAGSEN donne lieu à un diplôme décerné par Sciences Po Saint-Germain-en-Laye. Aucun ECTS n'est attribué. Un relevé de notes pourra accompagner ce diplôme sur demande des apprenants auprès de l'administration de Sciences Po Saint-Germain-en- Laye. En outre, trois mentions sont dispensées : « assez bien » pour les apprenants obtenant une note moyenne finale allant de 12/20 à 13,99/20, « bien » de 14/20 à 15,99/20 et « très bien » à partir de 16/20. Le diplôme sera remis aux apprenants lors de la cérémonie de diplomation. Si celle-ci ne peut avoir lieu dans un délai de six (6) mois suivant la décision finale du jury de délibération, le diplôme est remis aux lauréats avant l'expiration de ce délai.

Annexe 1 - Résumé de la notation des épreuves

<table>
<tr><th>Compétences attendues</th><th>Exercice d'évaluation

Modalités d'appréciation de l'acquisition des compétences
(1 exercice pratique par promotion)</th><th>Critères de validation</th></tr>
<tr><td>I. Maitriser des connaissances appliquées en sécurité du numérique à partir de cas pratiques :

1. Connaitre et savoir mettre en œuvre les réglementations françaises et européennes dans des situations professionnelles concrètes

2. Maîtriser les fondamentaux humains et techniques pour sécuriser un réseau informatique

3. Apprendre les fondamentaux de la science des données aux fins d'usage en contexte cyber : statistiques, traitement des données et interprétation des résultats d'analyse

4. Analyser les stratégies cyber des grandes puissances internationales afin de comprendre le contexte de l'insécurité numérique</td><td>Exemple de cas pratique :

Exercice : Dans un contexte fictif vous devez produire une analyse structurée et proposer des actions concrètes autour de 4 axes correspondant aux 4 éléments du module.
NB : L'exercice pourra être rédigé sous la forme d'un rapport professionnel ou présenté oralement.

1. Réglementation française et européenne (RGPD, NIS2, etc.)
Travail attendu :
• Identifier les obligations de l'entreprise en cas de violation de données (délai, notification, DPO…).
• Déterminer si le cadre de la directive NIS2 s'applique à cette entreprise.
• Proposer des actions de mise en conformité avec le RGPD (minimisation, registre des traitements, audit…).

2. Sécurisation du réseau informatique
Travail attendu :
• Identifier les vulnérabilités techniques et humaines possibles (phishing, shadow IT, absence de segmentation réseau…).
• Proposer un plan de sécurisation de l'infrastructure (authentification forte, segmentation, gestion des droits, sensibilisation…).
• Recommander des outils de supervision ou d'analyse réseau (SIEM, IDS/IPS…).

3. Science des données appliquée à la cybersécurité
Travail attendu :
À partir d'un jeu de données fictif fourni (ex. logs d'accès, tentatives de connexion), réalisez une analyse statistique de base (anomalies, pics d'activités, corrélations).</td><td>1. Réglementation française et européenne
Objectif évalué : compréhension et application des cadres juridiques
<table><tr><th>Critères</th><th>Description</th></tr><tr><td>Identification des textes applicables</td><td>L'étudiant(e) identifie correctement le RGPD, la directive NIS2, et autres textes pertinents.</td></tr><tr><td>Application concrète aux faits</td><td>Les obligations (notification CNIL, registre, DPO…) sont bien reliées à la situation.</td></tr><tr><td>Propositions de conformité</td><td>Des recommandations précises, pertinentes, réalistes (DPIA, revue des traitements, etc.).</td></tr></table>
2. Sécurisation du réseau informatique
Objectif évalué : capacité à évaluer et proposer des solutions de sécurité technique et humaine.
<table><tr><th>Critères</th><th>Description</th></tr><tr><td>Identification des vulnérabilités</td><td>Analyse pertinente des risques (techniques et humains).</td></tr><tr><td>Proposition de contre-mesures</td><td>Solutions adaptées au contexte (plan de sécurisation, bonnes pratiques…).</td></tr><tr><td>Pertinence des outils recommandés</td><td>Outils (SIEM, firewall, MFA…) bien choisis et justifiés.</td></tr></table>
3. Science des données appliquée à la cybersécurité
Objectif évalué : Lecture et traitement de données de sécurité.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>

Interpréter les résultats pour identifier des signes de compromission potentiels.
Proposer une visualisation simple (histogramme, heatmap, etc.)

<u>4. Analyse géopolitique et cyberstratégie</u>
<u>Travail attendu</u> :
Présenter une synthèse des stratégies cyber des grandes puissances (ex : États-Unis, Chine, Russie, Europe).

Mettre en relation ces stratégies avec les risques
Proposer des mesures de sécurité ou de gouvernance pour limiter la dépendance ou les risques de compromission par des puissances étrangères.

</td>
<td>
<table>
<tr><th>Critères</th><th>Description</th></tr>
<tr><td>Traitement statistique de base</td><td>Moyennes, écarts, détection d’anomalies bien exécutés.</td></tr>
<tr><td>Interprétation des résultats</td><td>Les conclusions tirées sont logiques, cohérentes avec les données.</td></tr>
<tr><td>Visualisation claire</td><td>Graphique/visualisation utile, lisible et pertinente.</td></tr>
</table>
<u>4. Analyse géopolitique et stratégie cyber</u>
<u>Objectif évalué</u> : Mise en perspective internationale des enjeux de cybersécurité.
<table>
<tr><th>Critères</th><th>Description</th></tr>
<tr><td>Connaissance des stratégies cyber</td><td>L’étudiant(e) démontre une bonne compréhension des doctrines cyber (USA, Chine, Russie, etc.).</td></tr>
<tr><td>Lien avec la situation de l’entreprise</td><td>Les risques géopolitiques sont reliés au contexte donné.</td></tr>
<tr><td>Propositions concrètes</td><td>Idées concrètes pour limiter l’exposition aux risques (clauses contractuelles, souveraineté, audit tiers…).</td></tr>
</table>
+
<u>Compétences transversales</u>
<u>Objectif évalué :</u> Qualité du travail rendu (sur le fond et la forme).
<table>
<tr><th>Critères</th><th>Description</th></tr>
<tr><td>Clarté et structuration du rapport</td><td>Plan logique, titres, introduction/conclusion claires.</td></tr>
<tr><td>Esprit critique et prise de recul</td><td>Capacité à aller au-delà du descriptif, à prioriser ou nuancer.</td></tr>
<tr><td>Pertinence globale et réalisme</td><td>Propositions en lien avec le réel, faisables dans une PME.</td></tr>
</table>
</td>
</tr>
<tr>
<td>II. Savoir anticiper les menaces et opportunités dans le cyberespace :

<u>1. Cartographier les menaces cyber pour son organisation</u>

<u>2. Réaliser des études prospectives des menaces et des risques cyber pour</u></td>
<td>
<u>Exemple de cas pratique</u> (pour les stagiaires du DReSeN) :

<u>Exercice</u> : Dans un contexte fictif vous êtes mandaté(e) pour analyser les menaces cyber auxquelles une collectivité est exposée et pour anticiper les risques émergents liés à cette transition numérique.

<u>1. Cartographier les menaces cyber pour l'organisation</u>
Compétence visée : identifier, qualifier et prioriser les menaces existantes et spécifiques à l’environnement de l’organisation.
</td>
<td>
<u>1. Cartographier les menaces cyber pour l’organisation</u>
<u>Objectif évalué</u> : Savoir identifier, qualifier et prioriser les menaces actuelles.
<table>
<tr><th>Critères</th><th>Description attendue</th></tr>
<tr><td>Identification des menaces</td><td>L’étudiant(e) identifie les menaces pertinentes pour l'organisation</td></tr>
</table>
</td>
</tr>
</table>

l'organisation afin d'identifier les vulnérabilités	Travail attendu : • Identifier les acteurs de la menace (cybercriminels, hacktivistes, États, insiders, etc.). • Décrire les types d'attaques possibles (phishing, ransomware, défiguration, DDoS, fuites de données, altération d'algorithmes d'IA…). • Analyser les vecteurs d'attaque (portails web, email, failles humaines, partenaires…). • Construire une matrice de risque (verbatim ou visuel) avec : probabilité × impact. • Proposer une typologie structurée des menaces en fonction des actifs numériques à protéger. **2. Réaliser une étude prospective des menaces et des risques cyber** Compétence visée : réfléchir à l'évolution du contexte cyber et identifier des vulnérabilités futures. Travail attendu : • Réaliser une analyse prospective à 3-5 ans : quelles évolutions technologiques, politiques ou criminelles peuvent aggraver ou modifier le risque ? • Identifier les vulnérabilités systémiques : dépendance à des prestataires, IA non maîtrisée, centralisation des données, manque de formation, etc. • Proposer un ou deux scénarios prospectifs : un pessimiste, un réaliste • Formuler des recommandations stratégiques à mettre en œuvre maintenant pour se préparer à ces risques (veille, gouvernance, architecture résiliente, etc.)	<table><tr><td></td><td>(ransomware, DDoS, hameçonnage, etc.)</td></tr><tr><td>**Caractérisation des acteurs**</td><td>Les types d'acteurs sont différenciés (États, groupes cybercriminels, insiders...) et adaptés au contexte</td></tr><tr><td>**Analyse des vecteurs d'attaque**</td><td>Les portes d'entrée possibles sont bien décrites (emails, services en ligne, partenaires...)</td></tr><tr><td>**Matrice de risque ou typologie claire**</td><td>Une représentation synthétique (tableau, graphique, diagramme) est fournie avec pertinence et logique</td></tr></table> **2. Réaliser des études prospectives des menaces et des risques cyber** Objectif évalué **:** Analyser les évolutions possibles des menaces et anticiper les risques à moyen terme. <table><tr><th>Critères</th><th>Description attendue</th></tr><tr><td>**Vision prospective claire**</td><td>Des tendances futures sont identifiées (technologiques, géopolitiques, criminelles…)</td></tr><tr><td>**Construction de scénarios**</td><td>Au moins un scénario prospectif (réaliste/pessimiste) est construit de manière argumentée</td></tr><tr><td>**Identification des vulnérabilités futures**</td><td>L'analyse inclut les failles anticipées du système ou de la gouvernance</td></tr><tr><td>**Préconisations stratégiques pertinentes**</td><td>Les recommandations sont concrètes, applicables et cohérentes avec les scénarios</td></tr></table> **+** **Compétences transversales** Objectif évalué : Qualité du travail rendu (sur le fond et la forme). <table><tr><th>Critères</th><th>Description</th></tr><tr><td>**Clarté et structuration du rapport**</td><td>Plan logique, titres, introduction/conclusion claires.</td></tr><tr><td>**Esprit critique et prise de recul**</td><td>Capacité à aller au-delà du descriptif, à prioriser ou nuancer.</td></tr><tr><td>**Pertinence globale et réalisme**</td><td>Propositions en lien avec le réel, faisables dans une PME.</td></tr></table>

III. Savoir gérer une crise cyber :

1. Gérer efficacement une attaque cyber à l'échelle de son organisation,

2. Utiliser les diagnostics de crise afin de mettre en œuvre un plan d'action préventif,

3. Savoir maîtriser une communication influente sur les enjeux de sécurité numérique avant et après une crise

Exemple de cas pratique :

Exercice :
Dans un contexte fictif :

1. Gérer efficacement une attaque cyber à l'échelle de son organisation
Travail attendu :

- Décrire les mesures immédiates à prendre (containment, coupure réseau, alertes internes…).
- Définir une cellule de crise (acteurs clés, rôles, coordination).
- Identifier les points critiques à sécuriser en priorité (infrastructures, données…).
- Proposer un plan d'action opérationnel pour les 24 premières heures.

2. Utiliser les diagnostics de crise afin de mettre en œuvre un plan d'action préventif
Travail attendu :

- Identifier les causes probables de l'attaque (techniques, humaines, organisationnelles).
- Produire un diagnostic post-crise synthétique : comment l'attaque a été possible.
- Proposer des actions correctives et préventives (audit de sécurité, PRA/PCA, segmentation, sauvegardes…).
- Élaborer une feuille de route à 6 mois pour éviter une nouvelle crise.

3. Savoir maîtriser une communication influente sur les enjeux de sécurité numérique avant et après une crise
Travail attendu :

- Rédiger un communiqué de presse destiné au public (voix rassurante, transparente, sans détails techniques).
- Élaborer un message interne pour les employés.
- Identifier les messages à diffuser en amont d'une crise pour renforcer la culture de sécurité (affiches, campagnes de sensibilisation…).

1. Gérer efficacement une attaque cyber à l'échelle de son organisation
Objectif évalué : Savoir gérer la temporalité et convaincre

Critères	Description
Réactivité	Capacité à détecter rapidement l'incident et à enclencher les premières actions sans délai excessif
Logique des actions	Cohérence et pertinence des mesures prises selon la nature de l'attaque et les étapes de la gestion de crise
Mobilisation des acteurs	Capacité à impliquer les parties prenantes internes et externes pertinentes de manière efficace
Priorisation des actions	Capacité à identifier et traiter en priorité les éléments critiques de l'organisation

2. Utiliser les diagnostics de crise afin de mettre en œuvre un plan d'action préventif
Objectif évalué : capacité à gérer les outils de diagnostic de manière proactive

Critères	Description
Capacité à analyser un diagnostic de crise	Comprendre, interpréter et extraire les enseignements clés d'un diagnostic de crise
Identification des leviers d'action préventive	Repérer les axes d'amélioration pour prévenir une nouvelle crise.
Élaboration d'un plan d'action structuré	Concevoir un plan d'action concret, cohérent et réaliste.
Prise en compte de l'organisation et de son contexte	S'adapter aux contraintes, à la culture, aux ressources et à la maturité de l'organisation.

3. Savoir maîtriser une communication influente sur les enjeux de sécurité numérique avant et après une crise
Objectif évalué : capacité à communiquer en vue de produire des effets

Critères	Description
Clarté et pédagogie du message	Formuler des messages clairs, compréhensibles et adaptés à différents publics
Adaptation du discours selon les publics cibles	Savoir adapter contenu, ton et objectifs
Maîtrise de la communication en situation sensible	Gérer une communication post-incident

<table>
<tr>
<td></td>
<td>

- Proposer une stratégie de communication multicanal post-crise (RS, site, médias…).

</td>
<td>

<table>
<tr><td>Valorisation proactive des enjeux de sécurité en amont</td><td>Porter un discours influent avant la crise, pour ancrer la cybersécurité comme enjeu stratégique.</td></tr>
</table>

+

<u>Compétences transversales</u>

<u>Objectif évalué :</u> Qualité du travail rendu (sur le fond et la forme).

<table>
<tr><th>Critères</th><th>Description</th></tr>
<tr><td>Clarté et structuration du rapport</td><td>Plan logique, titres, introduction/conclusion claires.</td></tr>
<tr><td>Esprit critique et prise de recul</td><td>Capacité à aller au-delà du descriptif, à prioriser ou nuancer.</td></tr>
<tr><td>Pertinence globale et réalisme</td><td>Propositions en lien avec le réel, faisables dans une PME.</td></tr>
</table>

</td>
</tr>
<tr>
<td>

Faire dialoguer et travailler entre eux les différents acteurs publics et privés du secteur numérique

<u>1. Savoir déterminer le rôle et les missions des membres d'une organisation pour organiser efficacement la gestion agile de projets cyber</u>

<u>2. Comprendre les bases du secteur de l'économie de la sécurité numérique dans l'industrie informatique</u>

<u>3. Diffuser dans l'organisation une culture professionnelle de la sécurité du numérique reposant sur une politique de sensibilisation</u>

</td>
<td>

<u>Exemple de cas pratique</u> :

<u>Contexte fictif :</u>
Vous êtes chargé(e) de coordonner les travaux autour de la sécurité numérique d'un projet.

<u>1. Savoir déterminer le rôle et les missions des membres d'une organisation pour organiser efficacement la gestion agile de projets cyber</u>
<u>Travail attendu :</u>

- Cartographier les différents types d'acteurs impliqués (publics, privés, prestataires, autorités).
- Définir le rôle précis de chaque acteur dans le projet (RSSI, DPO, chef de projet agile, experts cybersécurité, etc.).
- Proposer une organisation agile avec répartition des responsabilités et un schéma de gouvernance (comité de pilotage, gestion de crise, etc.)

<u>2. Comprendre les bases du secteur de l'économie de la sécurité numérique dans l'industrie informatique</u>
<u>Travail attendu :</u>

- Analyser le modèle économique de la cybersécurité : qui paie quoi ? Quels contrats ? Quels coûts ?
- Étudier la chaîne de valeur de la cybersécurité (prestataires, éditeurs, services managés…).

</td>
<td>

<u>1. Organisation et gestion agile des acteurs dans un projet cyber</u>
<u>Objectif évalué :</u> capacité à avoir une vision d'ensemble et à opérer avec souplesse

<table>
<tr><th>Critère</th><th>Description attendue</th></tr>
<tr><td>Identification des acteurs</td><td>Bonne identification et classification des parties prenantes (publics, privés, prestataires, régulateurs…)</td></tr>
<tr><td>Répartition des rôles</td><td>Répartition claire, fonctionnelle, et réaliste des responsabilités dans l'organisation</td></tr>
<tr><td>Structuration du projet</td><td>Mise en place d'une gouvernance agile (comités, coordination, canaux de décision, outils)</td></tr>
</table>

<u>2. Économie de la cybersécurité et relations contractuelles</u>
<u>Objectif évalué :</u> capacité à raisonner en termes économiques et en termes de risques

<table>
<tr><th>Critère</th><th>Description attendue</th></tr>
<tr><td>Analyse des coûts et ROI sécurité</td><td>Compréhension des coûts associés (audit, MSSP, cloud, licences…) et évaluation coût/risque</td></tr>
</table>

</td>
</tr>
</table>

- Évaluer les enjeux liés à l'externalisation (MSSP, cloud souverain, dépendances technologiques, clauses contractuelles).
- Produire un document de cadrage budgétaire ou décisionnel (ex. tableau coûts vs risques, ROI sécurité…)

3. Diffuser dans l'organisation une culture professionnelle de la sécurité du numérique reposant sur une politique de sensibilisation
Travail attendu :

- Identifier les routines à risque dans l'organisation (collaborateurs, agents publics…).
- Élaborer une stratégie de sensibilisation multicanal : formations, phishing simulé, charte de sécurité, affiches…
- Proposer des indicateurs de suivi de l'efficacité de la culture sécurité (ex : taux de clics, taux de participation, amélioration des audits…).

Compréhension des modèles économiques	Bonne vision des modèles (prestataires, services managés, éditeurs…)
Prise en compte des enjeux d'externalisation	Capacité à identifier les risques juridiques, stratégiques et techniques d'une sous-traitance

3. Politique de sensibilisation et culture de sécurité
Objectif évalué : capacité à faire comprendre les risques

Critère	Description attendue
Ciblage des besoins en sensibilisation	Identification pertinente des comportements à risque ou publics cibles internes
Qualité du plan de sensibilisation	Richesse des actions proposées, diversité des supports, réalisme de mise en œuvre
Indicateurs de suivi	Présence et pertinence de KPIs pour mesurer l'impact des actions (ex : taux de clic, audits internes)

+ Compétences transversales
Objectif évalué : Qualité du travail rendu (sur le fond et la forme).

Critères	Description
Clarté et structuration du rapport	Plan logique, titres, introduction/conclusion claires.
Esprit critique et prise de recul	Capacité à aller au-delà du descriptif, à prioriser ou nuancer.
Pertinence globale et réalisme	Propositions en lien avec le réel, faisables dans une PME.