

# Cybersécurité

---

Domaine 2 · EPSO/AD/430/26 · grade AD 8

**254**

lauréats recherchés

**AD 8**

grade de recrutement

**30 / 40 min**

épreuve du domaine

**13 oct. 2026**

clôture des candidatures

[eu-now.com](https://eu-now.com)

Dossier de préparation · 19 blocs d'étude avec leurs sources officielles

D'après l'avis de concours JO C/2026/4668 et les textes officiels qui couvrent son annexe II

[EU-now.com](https://eu-now.com)

## 1 · Le concours en un coup d'œil

EPSO/AD/430/26 est un concours général sur titres et épreuves pour des **administrateurs de grade AD 8** dans les institutions, organes et organismes de l'Union. Deux domaines, et **vous ne pouvez postuler qu'à un seul** : intelligence artificielle (240 lauréats recherchés) et cybersécurité (254). Vous visez la cybersécurité : 254 places sur la liste de réserve.



**Ce qui décide vraiment** : les trois tests de raisonnement et l'essai EUFTE sont des portes — on passe ou on sort. **Seule la note du QCM du domaine classe les candidats**, et seuls les meilleurs voient leur EUFTE corrigé et leur admissibilité vérifiée. Deux tiers de votre temps d'étude appartiennent au domaine.



Les cinq phases. Seule la note du QCM du domaine classe les candidats ; tout le reste est une porte à franchir.

## 2 · Les cinq épreuves

| Épreuve                | Langue   | Questions | Durée         | Points      | Seuil                                      |
|------------------------|----------|-----------|---------------|-------------|--------------------------------------------|
| Raisonnement verbal    | 1        | 20        | 35 min        | 0-20        | <b>10/20</b>                               |
| Raisonnement numérique | 1        | 10        | 20 min        | 0-10        | 10/20 avec l'abstrait                      |
| Raisonnement abstrait  | 1        | 10        | 10 min        | 0-10        | 10/20 avec le numérique                    |
| <b>QCM du domaine</b>  | <b>2</b> | <b>30</b> | <b>40 min</b> | <b>0-30</b> | <b>15/30 et parmi les meilleures notes</b> |
| EUFTE                  | 2        | —         | 40 min        | 0-10        | 5/10                                       |

La **langue 1** est l'une des 24 langues officielles. La **langue 2** est celle du QCM du domaine et de l'EUFTE. Il faut un C1 dans l'une et un B2 dans l'autre, et vous les choisissez dans l'acte de candidature. Les épreuves se passent à distance avec surveillance à distance, et l'ordre des sessions peut différer de celui de l'avis.

L'EUFTE n'est ni un test de langue ni un test de connaissances : EPSO publie avant l'épreuve une documentation sur des sujets européens — la même que vous recevez pendant l'épreuve — et vous traitez un exercice à partir d'elle. La correction se fait selon des grilles publiées.

### La plateforme d'examen

Les épreuves se déroulent sur TAO, la plateforme qu'EPSO utilise pour tous ses examens. Arrivez en sachant où se trouve chaque chose : vous perdez moins de temps et rien ne vous surprend le jour J.

EU Careers - Sample Test / Part I / Verbal Reasoning  
Probe 47a

Clock

All cells in the body have a specific structure and perform a specialised function, apart from stem cells. Stem cells have a number of remarkable properties. Unlike most specialised cells they are capable of replicating themselves many times. They can also develop into different types of specialised cells, such as muscle cells or red blood cells. These properties, in theory, mean that stem cells could repair the body, by multiplying and then replacing badly damaged tissue. It is believed that, in time, stem cell research could revolutionise medicine, as stem cells could be used to repair tissues or even to grow replacement organs.

Which of the following statements is correct?

☐ A. The only difference between stem cells and other cells is that stem cells do not perform a specialised function.

☐ B. A muscle cell that originated from a stem cell may transform back into a stem cell.

☐ C. Stem cells are the only cells that have the ability to repair themselves.

☐ D. Stem cells could repair damaged tissues by multiplying and then replacing damaged cells.

1. Elimination tool  
2. Calculator  
3. Scratchpad

Answered Answered and bookmarked Bookmarked

Back 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 OVERVIEW (16) Next

Bookmark tool

Écran de question : navigateur de questions en bas, signet, horloge et outils en haut.

Verbal Reasoning

Test Configuration

Set

Verbal Reasoning

1013x2

2026

AC ± % ÷

Élimination de réponses : barrez ce que vous avez écarté.

Surligner et règle de lecture pour les énoncés longs.

Calculatrice et brouillon lorsque l'épreuve les autorise.

Captures d'écran de la plateforme TAO utilisée lors des épreuves EPSO.

La liste de réserve est publiée par ordre alphabétique, non par note ; tous les candidats à égalité à la dernière place y figurent ; et y figurer ne garantit aucun recrutement.

Sources : avis de concours JO C/2026/4668, sections 1, 4.2, 4.3.1, 4.3.2 (tableaux 3 à 5), 4.3.3 et 4.3.4.

### 3 · À quoi ressemblent les 30 questions

L'avis ne publie ni programme ni bibliographie. Le contrat, c'est l'**annexe II**, « **fonctions types** » : tout ce qui est interrogeable en vient, et c'est pourquoi ce dossier la décortique en entier. Trente questions en 40 minutes, en langue 2 : **80 secondes par question**. Pas le temps de reconstruire quoi que ce soit — on répond avec ce que l'on reconnaît.

Une situation tirée de votre travail  
Une autorité nationale détecte un incident important dans une entité essentielle...

- A · Notifier le CSIRT sous 72 heures
- B · Alerte précoce au CSIRT sous 24 heures
- C · Rapport final à la Commission sous un mois
- D · Notifier le groupe de coopération

#### Ce qui décide de la réponse

- 1 QUI est compétent  
CSIRT, autorité, Commission...
- 2 QUELLE obligation exacte  
alerte, notification, rapport
- 3 LE CHIFFRE  
24 h · 72 h · un mois

Les distracteurs visent l'un des trois :  
le délai voisin, l'organe d'à côté,  
l'obligation d'une autre phase.

Anatomie d'une question du domaine : 80 secondes pour reconnaître trois données.

## Les cinq pièges du format

- **L'option la plus longue.** Dans les épreuves officielles, la bonne réponse n'est la plus longue qu'environ 4 fois sur 10 : choisir à la longueur ne fait pas réussir.
- **L'absolu.** « Toujours », « jamais », « dans tous les cas » signalent en général l'option fausse : le droit de l'Union vit d'exceptions.
- **L'acteur interverti.** L'obligation est correctement décrite, mais attribuée au mauvais organe. Lisez le sujet avant le verbe.
- **L'instrument voisin.** L'affirmation est vraie, mais elle appartient à une autre norme, qui ne régit pas ce cas.
- **Le texte dépassé.** Une rédaction antérieure à une modification. Étudiez toujours le texte consolidé.

## La fiche qui fonctionne

| A qui cela s'applique | Ce que cela impose    | Délais et chiffres  | Qui contrôle      |
|-----------------------|-----------------------|---------------------|-------------------|
| entités · produits    | le comportement exact | 24 h · 72 h · seuil | et qui sanctionne |

Une fiche par instrument : quatre colonnes, rien de plus. C'est ce qui répond en 80 secondes.

## 4 · Le programme, bloc par bloc

L'annexe II décrit des fonctions, pas des matières. Les voici transformées en blocs d'étude : ce qui entre, ce que l'on confond et où c'est écrit. Ce qui ne figure pas dans un texte officiel n'est pas interrogé.



Le domaine 2 est affaire de décisions : quelle mesure, quel délai et qui répond quand quelque chose arrive.

## 1 - Gestion des risques et assurance de sécurité

Cadres de risque (RMF, CSF 2.0)

Mesures et surveillance

Vulnérabilités et tests

Certification européenne

## 2 - Architecture, conception et technologie

Confiance zéro, nuage et virtualisation

Identité et accès

Cryptographie et post-quantique

Développement sécurisé et DevSecOps

Technologies émergentes

## 3 - Opérations de sécurité et réponse aux incidents

Opérations et détection

Réponse et investigation

Continuité et assainissement

## 4 - Gouvernance, politique et coordination

Institutions de l'Union (2023/2841)

NIS2 et exécution

Cyberrésilience

Cybersolidarité

DORA

Politique et droit pénal

## 5 - Sensibilisation, compétences et conseil

Formation et profils ECSF

L'annexe II transformée en blocs d'étude.

### 1 Cybersécurité des institutions de l'Union — règlement 2023/2841

Le cadre de la maison où vous travaillerez. Il revient souvent et se confond systématiquement avec NIS2.

#### Ce qui entre

- Le cadre de l'article 6 : approuvé au plus haut niveau de direction avant le 8 avril 2025, couvrant l'infrastructure sur site, l'informatique en nuage, les technologies opérationnelles et le mobile, révisé au moins tous les quatre ans.
- L'évaluation de maturité de l'article 7 : avant le 8 juillet 2025, puis au moins tous les deux ans.
- Les mesures de l'article 8 et le plan de cybersécurité de l'article 9, révisé tous les deux ans.
- Le responsable local de la cybersécurité : missions et rattachement.
- Le signalement au CERT-UE prévu à l'article 21 : alerte précoce sous 24 heures, notification sous 72 heures, rapport final sous un mois.
- L'IICB (articles 10 à 12) décide et publie des orientations ; le CERT-UE (article 13) fournit des services.

#### Ce que l'on confond

- Le CERT-UE ne surveille pas, ne sanctionne pas et n'est le CSIRT national de personne : il sert les entités de l'Union.
- Les entités de l'Union ne relèvent PAS de NIS2 : si le cas cite une institution européenne, la norme est le règlement 2023/2841.

- Les informations classifiées relèvent d'un régime distinct, la décision 2015/444, avec ses marquages, ses zones et ses bureaux d'ordre.

**Sources** : Règlement (UE, Euratom) 2023/2841, articles 6 à 13 et 21 · Décision (UE, Euratom) 2015/444

## 2 NIS2 et le règlement d'exécution 2024/2690

La norme de référence du secteur et la source la plus riche en questions de délais et de seuils.

### Ce qui entre

- Les dix domaines de mesures de l'article 21, paragraphe 2 : analyse des risques, gestion des incidents, continuité des activités, sécurité de la chaîne d'approvisionnement, acquisition et développement, évaluation de l'efficacité, cyberhygiène et formation, cryptographie, ressources humaines et contrôle d'accès, authentification à plusieurs facteurs.
- Les entités couvertes par le règlement d'exécution : DNS, registres de noms de domaine de premier niveau, informatique en nuage, centres de données, réseaux de diffusion de contenu, fournisseurs de services gérés et de services gérés de sécurité, places de marché en ligne, moteurs de recherche, réseaux sociaux et prestataires de services de confiance.
- Les critères d'importance de l'article 3 : perte directe supérieure à 500 000 EUR ou à 5 % du chiffre d'affaires, le montant le plus faible étant retenu ; exfiltration de secrets d'affaires ; décès ou atteinte grave à la santé ; accès non autorisé.
- Le signalement par étapes de l'article 23 : alerte précoce sous 24 heures, notification d'incident sous 72 heures, rapport final sous un mois.
- La responsabilité de l'organe de direction (article 20) et la formation obligatoire.
- Les seuils propres à chaque service, aux articles 5 à 14 du règlement d'exécution, et les treize sections de son annexe.

### Ce que l'on confond

- L'ENISA ne surveille pas les entités : ce sont les autorités nationales compétentes qui le font.
- Les mesures de l'article 21 ne sont pas les obligations de sécurité du RGPD, si semblables paraissent-elles.
- Entités essentielles et importantes diffèrent surtout par la surveillance et les sanctions, non par les mesures elles-mêmes.

**Sources** : Directive (UE) 2022/2555, articles 20, 21 et 23 · Règlement d'exécution (UE) 2024/2690 · Orientations techniques de l'ENISA 2025

### 3 Règlement sur la cyberrésilience — règlement 2024/2847

Produits comportant des éléments numériques : classification, échéances et répartition des responsabilités.

#### Ce qui entre

- La classification : produit par défaut, produit important de classe I ou II (article 7 et annexe III) et produit critique (article 8 et annexe IV).
- Les procédures d'évaluation de la conformité de l'article 32, selon la classe.
- Les obligations du fabricant : traitement des vulnérabilités et période d'assistance de l'article 13, d'au moins cinq ans sauf durée de vie plus courte.
- Le signalement prévu à l'article 14 pour les vulnérabilités activement exploitées et les incidents graves : alerte précoce sous 24 heures, notification sous 72 heures, rapport final sous 14 jours, via la plateforme unique de signalement de l'article 16.
- Le rôle de dépositaire de logiciels libres (article 24).
- Les dates : application générale le 11 décembre 2027, obligations de signalement à partir du 11 septembre 2026, dispositions relatives aux organismes notifiés à partir du 11 juin 2026.

#### Ce que l'on confond

- Le rapport final du règlement sur la cyberrésilience est dû en 14 jours ; celui de NIS2, en un mois. C'est le piège le plus fréquent.
- La plateforme unique de signalement est créée par l'article 16, mais l'obligation de signaler figure à l'article 14.
- Un service interne d'une institution n'est pas un produit mis sur le marché.

**Sources** : Règlement (UE) 2024/2847, articles 7, 8, 13, 14, 16, 24 et 32 ; annexes I, III et IV

### 4 Règlement sur la cybersolidarité et plan directeur de l'Union

Réponse européenne aux incidents de grande ampleur : trois volets et trois niveaux.

#### Ce qui entre

- Le système européen d'alerte à la cybersécurité, avec des pôles cyber nationaux et transfrontières (articles 3 à 9).
- Le mécanisme d'urgence en matière de cybersécurité : préparation coordonnée, réserve de cybersécurité de l'UE et assistance mutuelle (articles 10 à 19).
- Le mécanisme européen d'examen des incidents de cybersécurité, conduit par l'ENISA à la demande de la Commission ou d'EU-CyCLONe (article 21).
- Qui peut demander le déploiement de la réserve : les États membres, les institutions, organes et organismes de l'Union et les pays tiers associés au programme pour une Europe numérique.
- Les niveaux du plan directeur (recommandation (UE) 2025/3445) : technique dans le réseau des CSIRT, opérationnel dans EU-CyCLONe, politique par l'activation de l'IPCR par la présidence du Conseil.

### Ce que l'on confond

- Le niveau politique ne conduit pas la réponse technique : l'IPCR coordonne des décisions, il n'endigue pas les incidents.
- EU-CyCLONe est opérationnel, non politique, et ne remplace pas le réseau des CSIRT.

**Sources** : Règlement (UE) 2025/38 · Recommandation (UE) 2025/3445 du Conseil

## 5 Certification européenne — règlement sur la cybersécurité et schéma EUCC

Le cadre de certification : niveaux, caractère volontaire et répartition des rôles.

### Ce qui entre

- Les niveaux d'assurance de l'article 52 — élémentaire, substantiel et élevé — et l'évaluation qu'exige chacun.
- Le caractère volontaire posé à l'article 56, sauf disposition contraire du droit de l'Union ou national.
- Les rôles : l'ENISA prépare les schémas candidats (article 49), les organismes d'évaluation de la conformité certifient (article 60), les autorités nationales surveillent (article 58) et l'ECCG conseille (article 62).
- Le schéma EUCC (règlement d'exécution 2024/482) : critères communs et CEM, le niveau substantiel correspondant à AVA\_VAN 1-2 et le niveau élevé à AVA\_VAN 3-5, sans auto-évaluation, certificats valables jusqu'à cinq ans.
- Les obligations du titulaire en matière de gestion des vulnérabilités et les motifs de retrait.

### Ce que l'on confond

- L'ENISA ne délivre pas de certificats : elle prépare les schémas.
- La certification n'est pas obligatoire par défaut ; l'affirmer est un distracteur classique.
- L'EUCC n'admet aucune auto-évaluation, contrairement à certains schémas de niveau élémentaire.

**Sources** : Règlement (UE) 2019/881, articles 49, 52, 56, 58, 60 et 62 · Règlement d'exécution (UE) 2024/482

## 6 DORA et le secteur financier

Il apparaît comme cadre sectoriel : retenez la carte et la frontière avec NIS2, pas le détail.

### Ce qui entre

- Les cinq piliers : gestion du risque informatique (chapitre II), gestion et notification des incidents (III), tests de résilience opérationnelle numérique, y compris les tests de pénétration fondés sur la menace (IV), risque lié aux tiers avec un superviseur principal pour les prestataires critiques (V) et partage d'informations (VI).
- La responsabilité de l'organe de direction au titre de l'article 5.
- Le règlement délégué 2024/1774 précise le cadre de gestion du risque informatique.
- Le rapport avec NIS2 : DORA est la lex specialis des entités financières.

## Ce que l'on confond

- Les autorités européennes de surveillance ne supervisent pas une banque déterminée : ce sont les autorités nationales compétentes.
- Un rapport d'incident majeur au titre de DORA n'est pas une notification NIS2, et les délais diffèrent.

**Sources** : Règlement (UE) 2022/2554, article 5 et chapitres II à VI · Règlement délégué (UE) 2024/1774

## 7 Politique de l'Union et droit pénal

Questions d'attribution : ce que dit chaque instrument et de qui relève la compétence.

### Ce qui entre

- La stratégie de cybersécurité de 2020 : résilience et souveraineté technologique ; capacité opérationnelle de prévenir, dissuader et réagir ; un cyberspace mondial et ouvert.
- Le régime de sanctions cyber du règlement (UE) 2019/796 : cyberattaques ayant un effet important, inscription sur la liste par le Conseil, gel mis en œuvre par les États membres.
- La directive 2013/40 : accès illégal, atteinte à l'intégrité d'un système et de données, interception, outils ; circonstances aggravantes telles que les réseaux de zombies ou les infrastructures critiques ; points de contact 24 heures sur 24.
- L'académie des compétences en cybersécurité (COM(2023) 207) et ses quatre piliers.

### Ce que l'on confond

- Les sanctions sont décidées par le Conseil ; le droit pénal est appliqué par les États membres. Les deux ne se mélangent pas.
- L'académie n'est pas un organe doté de pouvoirs : c'est une initiative politique.

**Sources** : JOIN(2020) 18 · Règlement (UE) 2019/796 · Directive 2013/40/UE · COM(2023) 207

## 8 Cadres de gestion des risques — RMF, SP 800-30 et CSF 2.0

L'ossature technique. L'épreuve demande l'ordre des étapes et le produit de chacune.

### Ce qui entre

- Les sept étapes du RMF (SP 800-37r2) : préparer, catégoriser, sélectionner, mettre en œuvre, évaluer, autoriser et surveiller, avec le produit de chaque étape.
- L'appréciation des risques selon la SP 800-30r1 : sources de menace, événements de menace, vulnérabilités et conditions prédisposantes, vraisemblance et impact ; le processus préparer-conduire-communiquer-maintenir ; les trois niveaux organisationnels.
- Le CSF 2.0 (CSWP 29) : six fonctions, dont Govern, catégories et sous-catégories, profils actuel et cible, et niveaux 1 à 4.
- Les modèles de maturité : à quoi ils servent et en quoi ils diffèrent d'une appréciation des risques.

### Ce que l'on confond

- Les fonctions du CSF ne sont pas les étapes du RMF, ni les articles de l'ISO 27001.

- Les niveaux du CSF décrivent la rigueur de la gouvernance, pas une note de sécurité.

Sources : NIST SP 800-37r2 · NIST SP 800-30r1 · NIST CSWP 29

## 9 Mesures de sécurité, évaluation et surveillance continue

Ce que l'annexe II appelle opérations et indicateurs d'évaluation de la sécurité.

### Ce qui entre

- Les familles de mesures de la SP 800-53r5 et la différence entre une mesure de base et son amélioration.
- Les socles et les orientations d'adaptation sont passés dans la SP 800-53B ; la r5 en garde les concepts : périmètre, mesures compensatoires et paramètres définis par l'organisation.
- Les méthodes d'évaluation de la SP 800-53A : examiner, s'entretenir et tester, et la preuve que chacune produit.
- La surveillance continue (SP 800-137) : définir la stratégie, établir, mettre en œuvre, analyser et rendre compte, réagir, réviser et mettre à jour ; trois niveaux ; ce qui détermine la fréquence.
- La mesure (SP 800-55) : indicateurs de mise en œuvre, d'efficacité et d'impact.

### Ce que l'on confond

- Un audit annuel n'est pas une surveillance continue.
- Un indicateur qui ne déclenche aucune décision n'est pas un indicateur de sécurité, seulement un chiffre.

Sources : NIST SP 800-53r5 · SP 800-53A r5 · SP 800-137 · SP 800-55

## 10 Gestion des vulnérabilités et tests de sécurité

Distinguez les techniques par l'objectif, le périmètre et la preuve — et sachez quelle règle les impose.

### Ce qui entre

- Analyse de vulnérabilités, test de pénétration et équipe rouge : ce que chacun cherche et ce qu'il livre.
- Les phases de la SP 800-115 : planification, découverte, attaque et rapport ; techniques d'examen, identification et analyse des cibles, validation des vulnérabilités.
- La gestion des correctifs en entreprise (SP 800-40r4) : réponses au risque — accepter, atténuer, transférer ou éviter ; groupes de maintenance ; cycle de vie du correctif.
- Les niveaux de l'OWASP ASVS 5.0 et les catégories de tests du WSTG 4.2.
- Le déclencheur juridique : annexes 6.5 et 6.10 du règlement d'exécution 2024/2690.

### Ce que l'on confond

- Une analyse n'est pas un test de pénétration : l'objectif et la preuve diffèrent.
- Le règlement d'exécution fonde les tests sur le risque, il ne les impose pas inconditionnellement.

Sources : NIST SP 800-115 · SP 800-40r4 · OWASP ASVS 5.0 et WSTG 4.2 · Règlement d'exécution (UE) 2024/2690

## 11 Architecture de sécurité — confiance zéro, nuage et virtualisation

Des concepts d'architecture au vocabulaire très précis.

### Ce qui entre

- Les principes et les composants logiques de la SP 800-207 : le moteur de politique décide, l'administrateur de politique établit et le point d'application de la politique applique.
- Les sources qui alimentent l'algorithme de confiance : diagnostics continus, conformité sectorielle, renseignement sur la menace, journaux d'activité et SIEM.
- Les approches : gouvernance renforcée de l'identité, micro-segmentation et périmètre défini par logiciel ; les variantes de déploiement : agent et passerelle, passerelle d'enclave, portail de ressources et mise en bac à sable des applications.
- Les menaces propres à une architecture de confiance zéro (section 5).
- Nuage et virtualisation : SP 800-145 pour les modèles, SP 800-144 pour la responsabilité partagée et SP 800-125 pour l'hyperviseur.

### Ce que l'on confond

- La confiance zéro n'est ni un produit ni un périmètre réseau : c'est une stratégie de décision à chaque accès.
- La transition est progressive et commence par les actifs les plus précieux ; tout remplacer d'un coup est la fausse option typique.

Sources : NIST SP 800-207 · SP 800-145, 800-144 et 800-125

## 12 Gestion des identités et des accès

Les niveaux d'assurance sont le terrain favori des distracteurs.

### Ce qui entre

- IAL, AAL et FAL, de 1 à 3 : ce qu'exige chaque niveau en matière de vérification d'identité, d'authentification et de fédération.
- Les règles d'authentificateur de la SP 800-63B-4 : authentification à plusieurs facteurs, résistance à l'hameçonnage, authentificateurs synchronisables et réauthentification.
- Les accès à privilèges avec la SP 800-53r5 : AC-2 gestion des comptes, AC-5 séparation des tâches et AC-6 moindre privilège ; annexe 11.3 du règlement d'exécution 2024/2690.
- Les services de confiance eIDAS : signature électronique avancée et qualifiée, cachet et horodatage qualifiés, portefeuille européen d'identité numérique, et leurs effets juridiques.

### Ce que l'on confond

- AAL2 n'est pas AAL3 : la résistance à l'hameçonnage et le type d'authentificateur changent.
- Une signature avancée n'est pas qualifiée : seule la qualifiée a l'effet d'une signature manuscrite.

Sources : NIST SP 800-63-4 (A, B et C) · SP 800-53r5 · Règlement (UE) 910/2014 consolidé

### 13 Cryptographie, gestion des clés et transition post-quantique

Chiffres, états et processus : très interrogeable et facile à confondre.

#### Ce qui entre

- Le cycle de vie et les états d'une clé ; les facteurs qui fixent une cryptopériode (SP 800-57 partie 1, section 5.3).
- Les types de clés et la protection que chacun exige.
- La force de sécurité et les orientations de transition entre algorithmes (section 5.6).
- Les normes post-quantiques : FIPS 203 ML-KEM pour l'encapsulation de clés, FIPS 204 ML-DSA et FIPS 205 SLH-DSA pour les signatures.
- Ce que demande réellement la recommandation (UE) 2024/1101 : un sous-groupe du groupe de coopération NIS, une feuille de route de mise en œuvre coordonnée sous deux ans, des plans nationaux de transition, des schémas hybrides et un réexamen sous trois ans.

#### Ce que l'on confond

- Un mécanisme d'encapsulation de clés n'est pas un schéma de signature : ML-KEM et ML-DSA ne sont pas interchangeables.
- La recommandation de l'Union ne fixe aucune échéance de migration : les inventer est l'erreur la plus répétée.

**Sources** : NIST SP 800-57 partie 1 r5 · FIPS 203, 204 et 205 · Recommandation (UE) 2024/1101

### 14 Développement sécurisé et DevSecOps

L'annexe II parle de développement sécurisé ; la source est le SSDF.

#### Ce qui entre

- Les quatre groupes du SSDF (SP 800-218) : préparer l'organisation, protéger le logiciel, produire un logiciel bien sécurisé et répondre aux vulnérabilités.
- La sécurité dans la chaîne d'intégration et de déploiement continu (SP 800-204C) et les cinq types de code : applicatif, services applicatifs, infrastructure en tant que code, politique en tant que code et observabilité en tant que code.
- Les contrôles du maillage de services et leur emplacement.
- L'ingénierie de la sécurité des systèmes (SP 800-160 vol. 1 r1) : processus de l'ISO 15288, fiabilité et dossier d'assurance.
- Les ancres juridiques : annexes 6.2 et 6.3 du règlement d'exécution 2024/2690 et exigences du règlement sur la cyberrésilience.

#### Ce que l'on confond

- Une seule analyse en fin de cycle n'est pas du DevSecOps.
- L'infrastructure en tant que code et la politique en tant que code sont aussi du code à protéger : c'est l'oubli habituel.

**Sources** : NIST SP 800-218 · SP 800-204C · SP 800-160 vol. 1 r1

## 15 Opérations de sécurité — journaux, détection et renseignement sur la menace

SOC, surveillance et paysage des menaces.

### Ce qui entre

- La gestion des journaux (SP 800-92) : production, conservation et analyse ; les rôles de syslog et du SIEM ; des politiques par environnement ; les difficultés courantes.
- Le partage d'informations sur la menace (SP 800-150) : indicateurs contre tactiques, techniques et procédures ; consommer, utiliser, organiser et produire ; validation et priorisation.
- Le protocole des feux de circulation pour la diffusion : rouge, orange, vert et blanc.
- Le paysage des menaces de l'ENISA et sa méthodologie : acteurs, techniques et secteurs les plus touchés.

### Ce que l'on confond

- Un indicateur de compromission n'est pas une tactique : le premier se périmé, la seconde décrit un comportement.
- Le SIEM ne produit pas les journaux : il les reçoit. Confondre cela change la réponse.

**Sources** : NIST SP 800-92 · SP 800-150 · Paysage des menaces de l'ENISA 2025 et méthodologie CTL

## 16 Réponse aux incidents et investigation numérique

C'est là que l'on confond le plus les phases et l'ordre des gestes.

### Ce qui entre

- Le cycle de vie de la SP 800-61r3 construit sur le CSF 2.0 : préparation (Govern, Identify, Protect) et enseignements tirés, face aux phases de réponse (Detect, Respond, Recover), avec le tableau de correspondance vers l'ancien modèle en quatre phases.
- Le processus d'investigation de la SP 800-86 : collecte, examen, analyse et rapport ; données volatiles d'abord ; intégrité et chaîne de conservation.
- Les sources de données : fichiers, systèmes d'exploitation, trafic réseau et applications.
- Les délais de signalement au CERT-UE prévus à l'article 21 du règlement 2023/2841 et la coordination de l'article 22.

### Ce que l'on confond

- Éradiquer avant de recueillir les preuves détruit le dossier : l'ordre compte et il est interrogé.
- Le rétablissement n'est pas la clôture : les enseignements tirés préparent l'incident suivant.

**Sources** : NIST SP 800-61r3 · SP 800-86 · Règlement (UE, Euratom) 2023/2841

## 17 Continuité, plans d'urgence et assainissement des supports

Des listes fermées et des paramètres : des points rapides si on les connaît.

### Ce qui entre

- Les types de plans de la SP 800-34r1 : continuité des activités, continuité des opérations, communication de crise, protection des infrastructures critiques, réponse aux cyberincidents, reprise après sinistre, plan d'urgence du système d'information et plan d'urgence pour les occupants.
- RTO, RPO et durée d'interruption maximale tolérable, déduits de l'analyse d'impact sur l'activité.
- Les stratégies de reprise : méthodes de sauvegarde et sites froids, tièdes, chauds, mobiles et en miroir.
- L'assainissement des supports (SP 800-88r2) : effacer, purger et détruire ; effacement cryptographique et ses conditions ; l'arbre de décision de la section 4.3 selon le support, la réutilisation et la catégorisation de confidentialité FIPS 199.

### Ce que l'on confond

- Le RTO n'est pas le RPO : l'un mesure le temps de retour, l'autre la quantité de données que l'on peut perdre.
- Effacer n'est pas purger, et la démagnétisation ne fonctionne pas sur la mémoire flash, qui ne stocke rien magnétiquement.

Sources : NIST SP 800-34r1 · SP 800-88r2

## 18 Sensibilisation, formation et métiers de la cybersécurité

Ce bloc clôt l'annexe II et se traite vite quand on connaît les listes.

### Ce qui entre

- Le programme d'apprentissage de la SP 800-50r1 : analyse des besoins ; plan et stratégie ; analyse et conception ; développement et mise en œuvre ; évaluation et amélioration.
- Sensibilisation contre formation par rôle : objectif différent, mesure différente.
- Les douze profils de rôle de l'ECSF de l'ENISA et le cadre NICE (SP 800-181r1) avec ses rôles professionnels et ses énoncés de tâches, de connaissances et de compétences.
- Les déclencheurs juridiques : article 20, paragraphe 2, de NIS2, annexe 8 du règlement d'exécution 2024/2690 et article 8, paragraphe 1, point p), du règlement 2023/2841.

### Ce que l'on confond

- Un module en ligne une fois par an n'est pas un programme : il manque l'analyse des besoins et la mesure.
- N'inventez pas de profils ECSF : la liste est fermée et les distracteurs en ajoutent souvent un faux.

Sources : NIST SP 800-50r1 · SP 800-181r1 · ECSF de l'ENISA

## 19 Technologies émergentes — IA en sécurité et préparation quantique

Le pont vers l'autre domaine de ce concours.

### Ce qui entre

- Les trois couches du cadre multicouche de l'ENISA : fondements de cybersécurité, fondamentaux de l'IA et couche sectorielle.
- Les classes d'attaque du NIST AI 100-2 qui comptent quand un SOC adopte l'apprentissage automatique ou des outils fondés sur des grands modèles de langage.
- Les entrées du Top 10 OWASP LLM à contrôler en premier dans une organisation.
- La préparation quantique : inventaire cryptographique, agilité, schémas hybrides et processus de la recommandation (UE) 2024/1101.

### Ce que l'on confond

- Un outil d'apprentissage automatique ne remplace pas une mesure de sécurité : il la complète.
- Il n'existe pas d'échéance européenne de migration post-quantique : il existe un processus assorti de jalons de planification.

**Sources** : Cadre multicouche de l'ENISA · NIST AI 100-2 · OWASP LLM Top 10 · Recommandation (UE) 2024/1101

## 5 · Comment l'étudier en huit semaines



Huit semaines permettent deux passages sur le programme si l'on répond à des questions dès le premier jour.

| semaine                   | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |  |
|---------------------------|---|---|---|---|---|---|---|---|--|
| Carte et fiches           |   |   |   |   |   |   |   |   |  |
| Étude bloc par bloc       |   |   |   |   |   |   |   |   |  |
| Blocs faibles et chiffres |   |   |   |   |   |   |   |   |  |
| Simulations chronométrées |   |   |   |   |   |   |   |   |  |
| Révision et raisonnement  |   |   |   |   |   |   |   |   |  |

**Répartition** : deux tiers pour le domaine, un tiers pour le raisonnement. Le domaine vous classe ; le raisonnement ne fait qu'éliminer. Et à partir de la semaine 3, répondez à des questions le jour même où vous étudiez le bloc : lire sans répondre ne fixe rien.

## 6 · Bibliothèque officielle

Tout ce qui suit est public et citable. Une préparation sérieuse n'a pas besoin de plus, et aucun manuel commercial ne remplace le texte consolidé.

| Document                                                               | À quoi il sert                                                            |
|------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Règlement (UE, Euratom) 2023/2841 et décision 2015/444                 | Cybersécurité des entités de l'Union et informations classifiées de l'UE. |
| Directive (UE) 2022/2555 et règlement d'exécution 2024/2690            | Mesures, seuils d'importance et délais de signalement.                    |
| Règlement (UE) 2024/2847 — cyberrésilience                             | Produits comportant des éléments numériques, classes et signalement.      |
| Règlement (UE) 2025/38 et recommandation (UE) 2025/3445                | Réserve de cybersécurité et gestion de crise.                             |
| Règlement (UE) 2019/881 et règlement d'exécution 2024/482              | Certification européenne et schéma EUCC.                                  |
| Règlement (UE) 2022/2554 et règlement délégué 2024/1774                | DORA et le cadre de gestion du risque informatique.                       |
| JOIN(2020) 18 · Règlement 2019/796 · Directive 2013/40 · COM(2023) 207 | Stratégie, sanctions, droit pénal et compétences.                         |
| NIST SP 800-37r2 · SP 800-30r1 · CSWP 29                               | Cadre de gestion des risques, appréciation et CSF 2.0.                    |
| NIST SP 800-53r5 · 800-53A r5 · 800-137 · 800-55                       | Mesures, évaluation, surveillance continue et indicateurs.                |
| NIST SP 800-115 · 800-40r4 · OWASP ASVS et WSTG                        | Tests de sécurité et gestion des correctifs.                              |
| NIST SP 800-207 · 800-144/145/146 · 800-125                            | Confiance zéro, nuage et virtualisation.                                  |
| NIST SP 800-63-4 (A, B, C) et règlement 910/2014                       | Identité, authentification et services de confiance.                      |
| NIST SP 800-57 p.1 r5 · FIPS 203/204/205 · Recommandation 2024/1101    | Clés, post-quantique et feuille de route européenne.                      |
| NIST SP 800-218 · 800-204C · 800-160 v1r1                              | Développement sécurisé, CI/CD et ingénierie de la sécurité des systèmes.  |
| NIST SP 800-92 · 800-150 · Paysage des menaces de l'ENISA 2025         | Journaux, renseignement sur la menace et paysage.                         |
| NIST SP 800-61r3 · 800-86 · 800-34r1 · 800-88r2                        | Incidents, investigation, continuité et assainissement.                   |
| NIST SP 800-50r1 · SP 800-181r1 · ECSF de l'ENISA                      | Sensibilisation, formation et profils de métiers.                         |

## 7 · Avant de vous déclarer prêt

- Tenez-vous séparés les délais de NIS2, du règlement sur la cyberrésilience et de 2023/2841, rapport final compris ?
- Savez-vous qui surveille, qui certifie et qui assiste dans chaque cadre européen ?
- Récitez-vous les sept étapes du RMF et les six fonctions du CSF 2.0 avec leur produit ?
- Distinguez-vous analyse, test de pénétration et équipe rouge par l'objectif et la preuve ?
- IAL, AAL et FAL sont-ils clairs, ainsi que les trois normes post-quantiques et leur fonction ?
- Savez-vous pourquoi la démagnétisation n'assainit pas la mémoire flash, et ce qu'exige l'effacement cryptographique ?
- Avez-vous fait trois simulations de 30 questions en 40 minutes, dans votre langue 2 ?

**Entraînez-vous avec des questions de ce domaine, dans les cinq langues de l'examen.**

Banque EPSO/AD/430/26 cybersécurité, avec l'explication et l'article derrière chaque réponse : [eu-now.com/specialist/cybersecurity](https://eu-now.com/specialist/cybersecurity)



**Et quand quelque chose ne passe pas, demandez.** Chez EU-now, EUgenio répond avec la norme sous les yeux et cite l'article d'où vient la réponse : la différence entre savoir que l'on s'est trompé et savoir pourquoi.

Les chiffres et les échéances proviennent de l'avis publié au Journal officiel (C/2026/4668) et des textes officiels cités. En cas de rectificatif publié par EPSO, le Journal officiel prévaut.