



SEC101 Sécurité des Systèmes d'Information

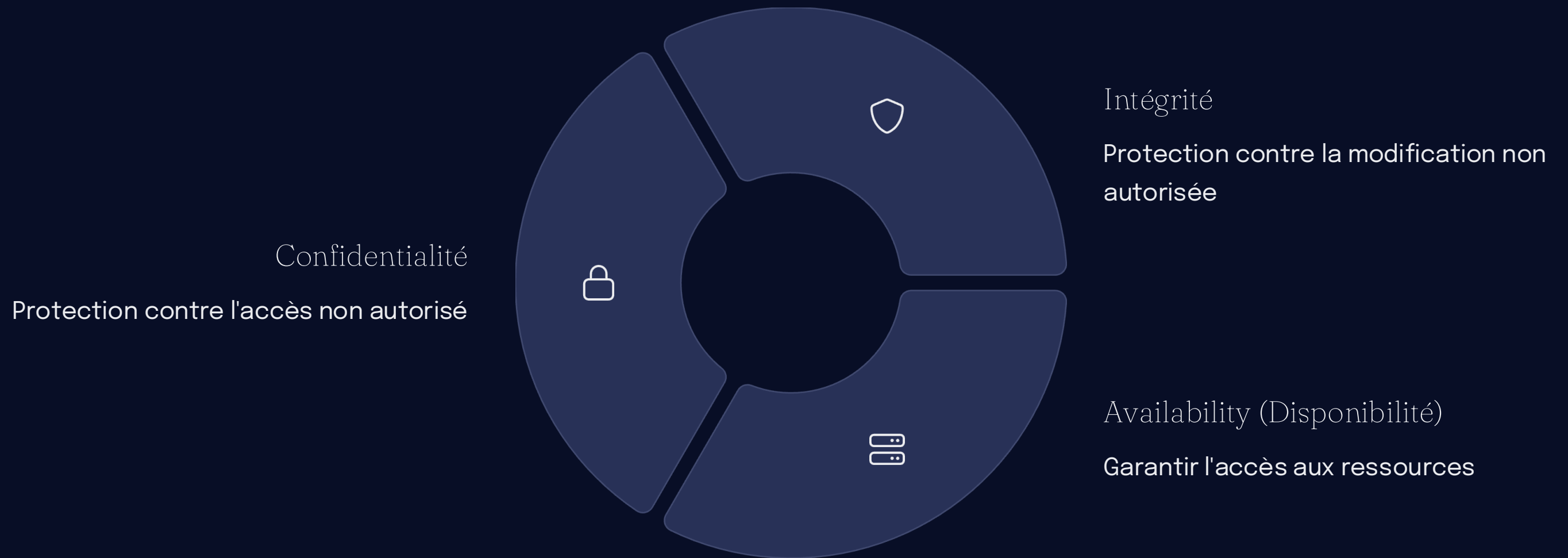
Structure de l'examen



Conseils généraux

- Réponses structurées et concises
- Justifier vos choix avec des arguments techniques

Le triptyque CIA



Menaces internes

Erreur humaine

Mauvaise manipulation, négligence

Malveillance interne

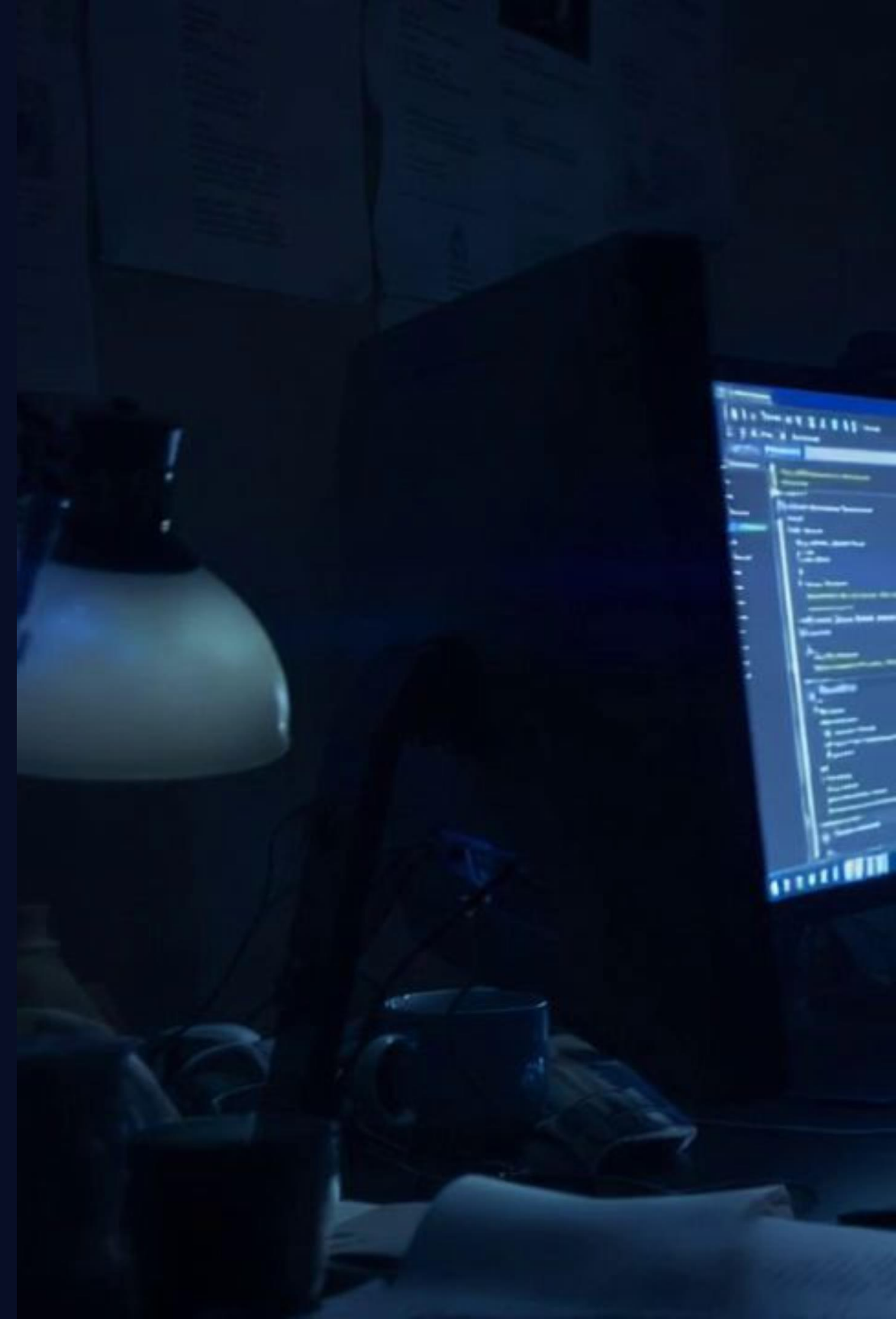
Vol de données, sabotage

Ingénierie sociale

Manipulation des employés

Négligence

Non-respect des procédures



OIV (Opérateur d'Importance Vitale)

Définition : Organisation dont l'activité est indispensable au fonctionnement du pays



Énergie

EDF, Total



Santé

Hôpitaux



Transport

SNCF, aéroports



Télécommunications



Finance

PCA et PRA

1

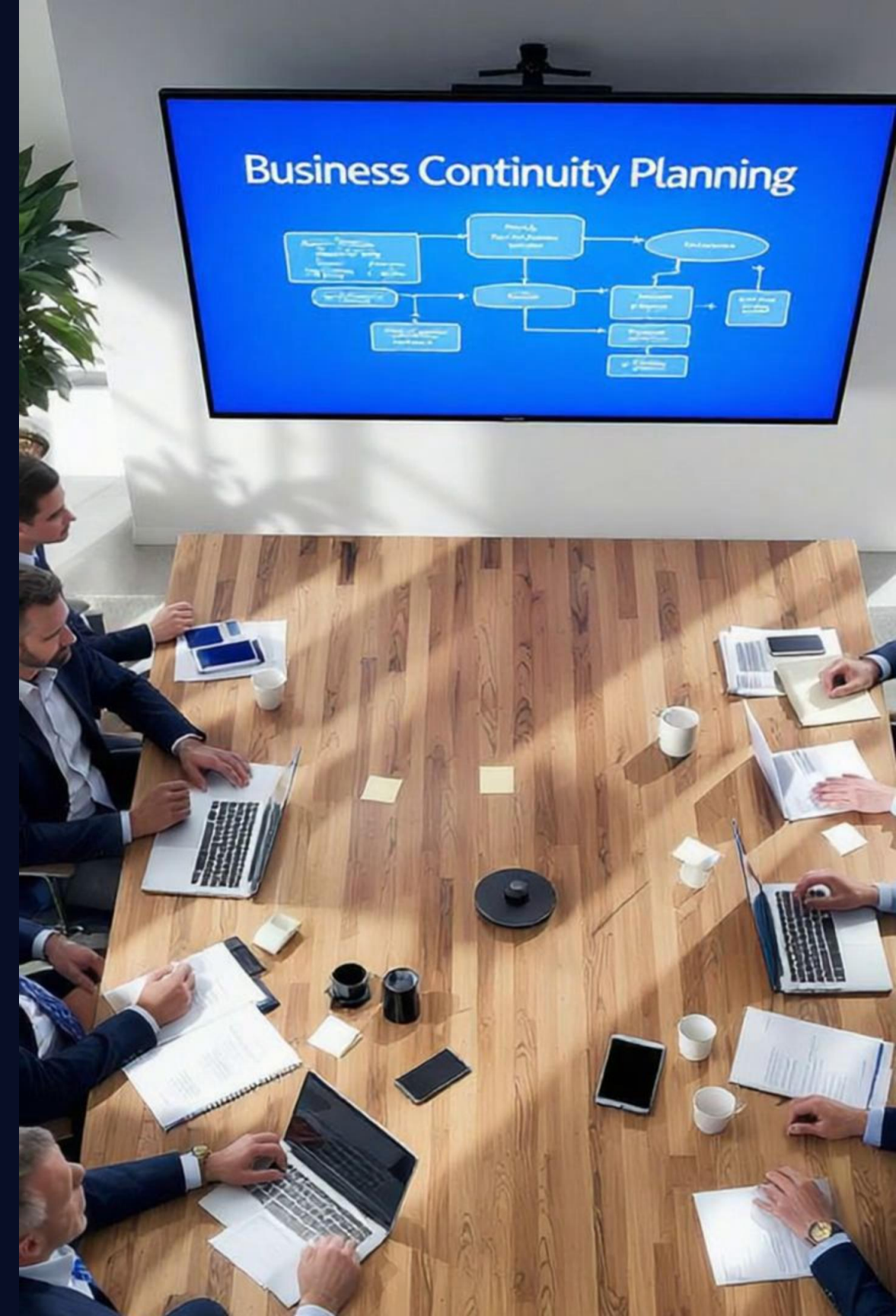
PCA (Plan de Continuité d'Activité)

- Stratégie globale de continuité
- Maintien des activités critiques
- Organisation et procédures

2

PRA (Plan de Reprise d'Activité)

- Volet technique du PCA
- Restauration des systèmes IT
- Procédures de récupération



Cycle de réponse aux incidents

Détection
Identification de l'incident

Retour d'expérience
Analyse post-incident



Confinement
Limitation de la propagation

Éradication
Suppression de la menace

Récupération
Restauration des systèmes

ISO 27001

Nature

Norme internationale de management de la sécurité

Objectif principal

Mise en place d'un SMSI (Système de Management de la Sécurité de l'Information)

Approche

Amélioration continue (PDCA)



SIEM

Définition : Security Information & Event Management

Fonctions

- Collecte centralisée des logs
- Corrélation d'événements
- Détection d'anomalies
- Alertes temps réel

Avantages

- Vision globale de la sécurité
- Détection rapide des incidents
- Conformité réglementaire



APT (Advanced Persistent Threat)

Caractéristiques

- Attaque sophistiquée et ciblée
Utilisation de techniques avancées pour cibler des organisations spécifiques
- Persistance dans le temps
Présence prolongée dans les systèmes compromis
- Objectif : espionnage/vol de données
Extraction discrète d'informations sensibles
- Acteurs : États, groupes organisés
Entités disposant de ressources importantes



Audit interne vs externe

Audit interne

- Réalisé par l'organisation
- Amélioration continue
- Connaissance du contexte

Audit externe

- Tiers indépendant
- Objectivité garantie
- Certification possible

EBIOS

Signification

Expression des Besoins et Identification des Objectifs de Sécurité

Objectif

Méthode d'analyse de risques française (ANSSI)



Contexte



Événements redoutés



Scénarios



Risques



Mesures

Gestion d'incident et obligations légales

Contexte du scénario

- PME e-commerce
- Données bancaires clients
- Service 24/7
- Menace ransomware

Mesures préventives contre ransomware

1

Sauvegarde 3-2-1

- 3 copies des données
- 2 supports différents
- 1 copie hors site/déconnectée

2

Sensibilisation utilisateurs

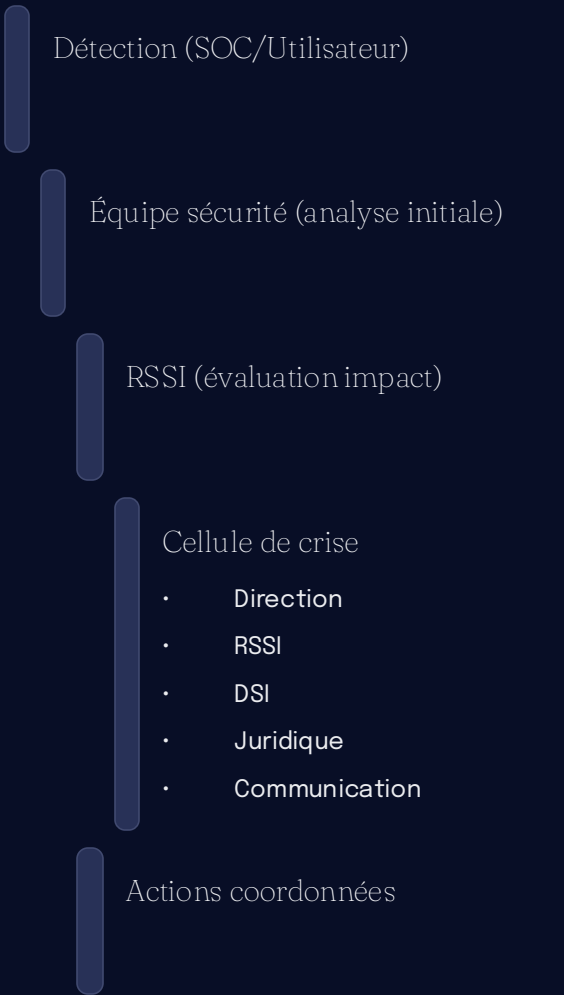
- Formation anti-phishing
- Procédures de signalement
- Tests réguliers



Mesures techniques et plan de réponse

1	2
<div>Mesures techniques</div> <ul style="list-style-type: none">• Antivirus/EDR à jour• Segmentation réseau• Principe du moindre privilège• Patch management rigoureux	<div>Plan de réponse</div> <ul style="list-style-type: none">• Procédures documentées• Équipe de crise identifiée• Tests réguliers

Schéma d'escalade en cas d'incident



Conseils pour l'examen

Structure de réponse type

1. **Contexte** : Reformuler brièvement
2. **Analyse** : Identifier les enjeux
3. **Solutions** : Propositions concrètes
4. **Justification** : Arguments techniques

Points d'attention

- Toujours penser "risque métier"
- Équilibre technique/organisationnel
- Solutions réalistes et budgétées
- Conformité réglementaire

Gestion du temps

- Partie I : 20 minutes (2 min/question)
- Partie II : 30 minutes
- Partie III : 40 minutes
- Relecture : 10 minutes

Conclusion

Les clés du succès :

- Maîtriser les fondamentaux (CIA, ISO, RGPD)
- Penser "RSSI terrain" pas théorique
- Structurer ses réponses
- Justifier ses choix
- Garder une vision globale

Bon courage pour l'examen !

