GUIDE PROFESSIONNEL

Réussir son entretien pour un poste de RSSI/CISO

Comprendre le rôle, démontrer sa valeur et convaincre sans nécessairement posséder le CISSP

Audience	Objectif	Approche
Professionnels IT et cybersécurité en transition vers un rôle de direction	Préparer et réussir un entretien pour un poste de RSSI ou CISO	Méthode structurée, exemples concrets et posture professionnelle

Comprendre ce que l'entreprise recherche réellement

Une entreprise ne recrute pas uniquement un expert technique. Elle recherche une personne capable d'assumer des responsabilités transversales à l'intersection de la technique, du management et de la stratégie.

Compétences stratégiques

- Comprendre les risques métiers
- Définir une stratégie de sécurité
- Prioriser les actions
- Conseiller la direction

Compétences opérationnelles et relationnelles

- Coordonner plusieurs équipes
- Piloter les incidents majeurs
- Faire respecter les exigences réglementaires
- Communiquer avec des interlocuteurs techniques et non techniques

Le recruteur évalue avant tout la capacité du candidat à créer de la valeur pour l'organisation — pas uniquement son niveau de maîtrise technique.

RSSI et CISO : quelle mission ?

Le RSSI/CISO est le responsable de la gouvernance de la sécurité de l'information. Son périmètre couvre l'ensemble des dimensions stratégiques, organisationnelles, réglementaires et opérationnelles de la sécurité.

Stratégie & Gouvernance

- Définir la stratégie de cybersécurité
- Élaborer les politiques de sécurité
- Présenter les risques à la direction

Risques & Conformité

- Identifier et traiter les risques
- Piloter les audits et plans d'amélioration
- Suivre la conformité réglementaire

Coordination & Sensibilisation

- Organiser la gestion de crise
- Sensibiliser les collaborateurs
- Coordonner les équipes internes et les prestataires

Le niveau d'implication opérationnelle dépend de la taille et de l'organisation de l'entreprise.

Ce que le RSSI n'est pas

Le RSSI doit comprendre les enjeux techniques, mais sa valeur principale consiste à transformer ces enjeux en décisions, priorités et plans d'action pour l'entreprise.

Fonction	Responsabilité principale
RSSI/CISO	Gouvernance, risques, stratégie, conformité et coordination
Pentester	Recherche et exploitation contrôlée des vulnérabilités
Support IT	Assistance aux utilisateurs et résolution des incidents courants
Administrateur système	Exploitation, configuration et maintien des infrastructures
Ingénieur sécurité	Conception et déploiement des solutions techniques de sécurité

Chaque fonction a sa propre légitimité. Le RSSI ne remplace aucune d'entre elles — il les pilote, les oriente et les coordonne dans un cadre de gouvernance cohérent.

Expliquer les limites du rôle sans paraître rigide

Comment expliquer avec diplomatie que le RSSI n'est pas destiné à remplacer les équipes opérationnelles :

> « Mon rôle est de définir le niveau de sécurité attendu, d'évaluer les risques, de prioriser les mesures et de vérifier leur mise en œuvre. Je travaille étroitement avec les équipes IT, les administrateurs, les ingénieurs et les prestataires, qui assurent l'exécution technique. Dans une situation critique, je peux naturellement contribuer à l'analyse et à la coordination, tout en conservant une vision globale du risque. »

Complémentarité

Le RSSI s'appuie sur les équipes techniques sans les court-circuiter ni les remplacer.

Coordination

Il orchestre les acteurs, aligne les priorités et garantit la cohérence du dispositif.

Responsabilités

Chaque partie prenante dispose d'un périmètre clair, documenté et assumé.

Il faut parler de **complémentarité**, de **coordination** et de **responsabilités** — et non dire simplement : « Ce n'est pas mon travail. »

Les compétences évaluées pendant l'entretien

Le jury d'entretien évalue un spectre large de compétences, allant de la maîtrise des référentiels à la capacité de leadership et de communication. Voici les dix dimensions clés :

1	Gouvernance de la sécurité
2	Analyse et gestion des risques
3	Communication avec la direction
4	Leadership et capacité d'influence
5	Gestion de crise

Préparer son entretien

Étudier avant l'entretien

- Le secteur d'activité de l'entreprise et ses données sensibles
- Ses obligations réglementaires et ses principales menaces
- Son organisation informatique et son exposition aux fournisseurs et au cloud
- Ses incidents ou actualités publiques éventuels
- La maturité probable de son dispositif de sécurité
- Les missions exactes indiquées dans l'offre

Questions pertinentes à poser au recruteur

- À qui le RSSI est-il rattaché ?
- Dispose-t-il d'un budget et d'une équipe ?
- Quelles sont les priorités des douze prochains mois ?
- Quel est le niveau de maturité actuel ?
- Comment sont réparties les responsabilités entre le RSSI et la DSI ?
- Quelle est la fréquence des échanges avec la direction ?
- Quels sont les principaux enjeux réglementaires et métiers ?

Poser des questions pertinentes démontre une compréhension du rôle et une posture de futur décideur — pas seulement de candidat.

Répondre aux questions techniques

Ce qu'un RSSI doit démontrer

Un RSSI n'a pas besoin de connaître chaque commande ou chaque produit par cœur. Il doit démontrer :

- Une méthode d'analyse et une compréhension des risques
- La capacité à poser les bonnes questions et à mobiliser les bons experts
- Une prise de décision proportionnée
- Une connaissance des principes de défense en profondeur
- Une compréhension des dépendances entre identité, réseau, postes, cloud, données et continuité d'activité

Structure de réponse recommandée

01

Identifier le contexte

02

Évaluer le risque et l'impact métier

03

Définir les priorités

04

Mobiliser les équipes compétentes

05

Décider des mesures immédiates

06

Contrôler la mise en œuvre

07

Informer la direction

08

Capitaliser après l'incident

Présenter ses expériences avec la méthode STAR

La méthode STAR

S — Situation

Contexte et problème rencontré

T — Tâche

Responsabilité du candidat

A — Actions

Décisions et mesures prises

R — Résultats

Impacts obtenus et enseignements

Résultats mesurables à mettre en avant

Privilégier des indicateurs quantifiables et des réalisations concrètes :

- Réduction du nombre d'incidents
- Amélioration du délai de réaction
- Fermeture de vulnérabilités critiques
- Mise en conformité réglementaire
- Réduction du risque résiduel
- Amélioration du taux de sensibilisation
- Mise en place d'indicateurs présentés à la direction

Pas de CISSP : est-ce éliminatoire ?

Le CISSP peut faciliter l'accès à certains postes, mais il ne remplace pas les compétences fondamentales attendues d'un RSSI :

Expérience concrète

Les réalisations terrain priment sur les certifications dans la majorité des processus de recrutement.

Compréhension de l'entreprise

Aligner la sécurité sur les enjeux métiers est une compétence que nulle certification ne peut certifier seule.

Leadership et jugement

La capacité à décider, à influencer et à obtenir des résultats est au cœur du rôle.

Gestion des risques

Identifier, évaluer et prioriser les risques est une compétence pratique avant d'être académique.

> « Je ne possède pas encore la certification CISSP, mais j'ai développé des compétences directement applicables en gestion des risques, sécurité opérationnelle, coordination et communication. Je connais les référentiels du secteur et je poursuis activement le développement structuré de mes compétences. »

Ne pas prétendre qu'une certification est inutile. Reconnaître sa valeur tout en valorisant ses propres atouts est la posture la plus crédible.

Comment compenser l'absence de certification ou d'ancienneté ?

Preuves concrètes à apporter lors de l'entretien :

Réalisations documentées

Cartographie des risques, politiques ou procédures rédigées, tableaux de bord et indicateurs de pilotage présentés à la direction.

Participation active aux processus clés

Audits, gestion ou coordination d'incidents, plans de continuité ou de reprise d'activité.

Sensibilisation et veille

Actions de sensibilisation menées, veille réglementaire et technologique structurée et documentée.

Maîtrise des référentiels

ISO 27001, ISO 27005, NIST CSF, EBIOS Risk Manager, DORA, NIS2 et RGPD.

Plan de progression et recommandations

Plan de formation réaliste et recommandations professionnelles vérifiables.

⚠ Important : ne présenter aucun document confidentiel appartenant à un ancien employeur.

Convaincre sans avoir dix ans d'expérience

Démontrer sa capacité à exercer la fonction — et non essayer de dissimuler son niveau d'expérience. Mettre en avant :

Compétences transférables et progression

Mettre en lumière l'évolution du parcours et les responsabilités croissantes assumées.

Prise de responsabilités concrètes

Identifier les situations où le candidat a pris des initiatives et des décisions à fort impact.

Maturité et capacité d'apprentissage

Démontrer la capacité à reconnaître ses limites, à s'entourer d'experts et à apprendre rapidement.

Vision claire des priorités

Articuler une vision structurée des priorités de sécurité adaptée au contexte de l'entreprise.

> « Je ne prétends pas avoir rencontré toutes les situations possibles. En revanche, je dispose d'une méthode structurée, d'une expérience opérationnelle utile et de la capacité à identifier rapidement les risques, mobiliser les experts et rendre compte à la direction. »

Questions difficiles et réponses recommandées

Anticiper les questions déstabilisantes est une étape essentielle de la préparation. Voici les formulations recommandées pour les situations les plus fréquentes :

Question	Réponse synthétique recommandée
Pourquoi vous recruter sans CISSP ?	Mes compétences opérationnelles, ma méthode et mes résultats concrets compensent l'absence de certification. Je poursuis activement ma montée en compétences.
Vous n'avez jamais occupé officiellement un poste de RSSI : pourquoi êtes-vous prêt ?	J'ai exercé des responsabilités équivalentes dans mes fonctions précédentes. Je dispose d'une méthode, d'une vision et de la maturité nécessaires.
Êtes-vous capable de réaliser un test d'intrusion ?	Ce n'est pas le cœur du rôle RSSI. Je sais piloter et interpréter les résultats d'un pentest, et je m'appuie sur des experts pour l'exécution.
Pouvez-vous intervenir directement sur les serveurs ?	Je peux contribuer à l'analyse en situation critique, mais mon rôle est de coordonner et de décider, pas de remplacer les équipes techniques.
Que faites-vous en cas de ransomware ?	J'active le plan de réponse à incident, isole les systèmes affectés, mobilise les équipes, informe la direction et pilote la communication.
Comment convaincre une direction qui refuse votre budget ?	Je traduis les risques en impacts métiers chiffrés, je priorise les mesures à fort ROI et je propose des arbitrages documentés.
Comment arbitrer entre sécurité et contraintes métiers ?	Je recherche le niveau de risque acceptable avec la direction, je propose des mesures proportionnées et je documente les décisions.
Que faites-vous lorsque l'équipe IT refuse une mesure ?	Je comprends les contraintes, j'explique le risque, je cherche un compromis et, si nécessaire, j'escalade à la direction avec les éléments factuels.
Quel serait votre premier chantier en arrivant ?	Comprendre l'existant, identifier les risques critiques et proposer un plan de 90 jours réaliste et priorisé.

Plan des 90 premiers jours

Proposer un plan structuré pour les 90 premiers jours démontre une posture de décideur, une méthode rigoureuse et une compréhension réaliste des enjeux d'une prise de poste.

Période	Objectif	Actions clés
Jours 1–30	**Comprendre**	Rencontrer les parties prenantes · Identifier les actifs critiques · Examiner les incidents récents · Étudier les audits et obligations réglementaires · Comprendre les responsabilités et processus existants
Jours 31–60	**Évaluer et prioriser**	Établir une première vision des risques · Identifier les mesures urgentes · Évaluer la maturité · Définir des indicateurs · Proposer des actions rapides et réalistes
Jours 61–90	**Structurer et engager**	Présenter une feuille de route · Définir les responsabilités · Faire valider les priorités · Lancer les premiers chantiers · Organiser le suivi avec la direction

Comprendre

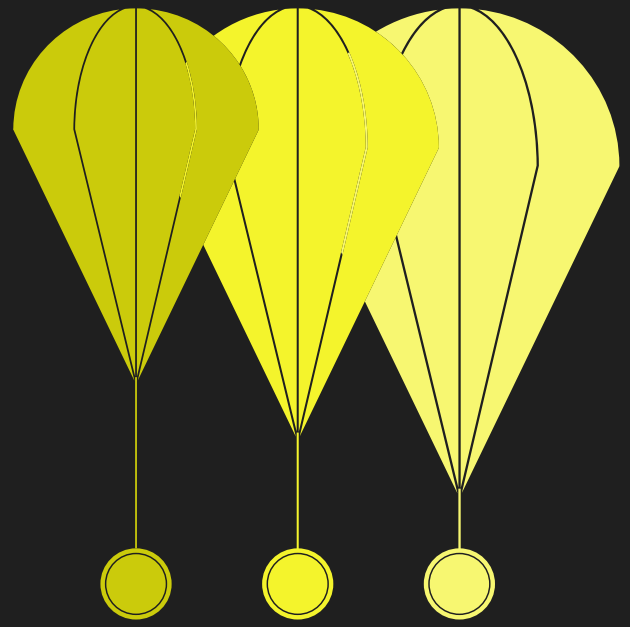
Jour 1-30: audits et rencontres clés

Évaluer et prioriser

Jour 31-60: risques et actions prioritaires

Structurer et engager

Jour 61-90: plan gouvernance et mobilisation



Conclusion : les clés pour obtenir le poste

Comprendre le rôle réel du RSSI/CISO

Gouvernance, risques, stratégie et coordination — pas uniquement expertise technique.

Relier la cybersécurité aux enjeux métiers

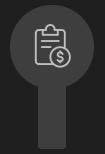
Traduire chaque risque technique en impact compréhensible pour la direction.

Démontrer une méthode et des résultats

Utiliser la méthode STAR et des indicateurs mesurables pour valoriser son parcours.

Expliquer les limites du rôle avec diplomatie

Complémentarité, coordination et responsabilités partagées — pas de refus catégorique.



Transformer l'absence de certification en plan de progression

Présenter un plan de montée en compétences crédible et structuré.

> « Un bon RSSI n'est pas celui qui prétend tout savoir ou tout exécuter seul. C'est celui qui sait identifier les risques, prendre les bonnes décisions, mobiliser les bonnes compétences et rendre la cybersécurité compréhensible par toute l'entreprise. »