Référentiel de Compétition Métier

CYBER SECURITE

N°54

Soumis par :

BOUAISSI Foued, Expert National WorldSkills France

Date de publication (par WorldSkills France) : 29/10/2026

© WorldSkills France (WSFR) se réserve tous les droits relatifs aux documents rédigés pour ou au nom de WSFR et comprenant leur traduction et leur envoi par voie électronique. Ce matériel peut être reproduit à des fins professionnelles et pédagogiques non commerciales, à la condition que le logo de WorldSkills France et la déclaration concernant les droits d'auteur restent en place

1. DESCRIPTION DU METIER

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) définit la cybersécurité ainsi : « Etat recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données ». Il existe différents métiers dans le domaine de la cybersécurité, cependant chacun de ces métiers nécessite de s'approprier un socle de connaissances théoriques et pratique dans les domaines de l'administration des systèmes et réseaux, en développement applicatif, en gestion des bases de données.

On distinguera en particulier :

• **Les métiers d'analyste :** Agissant généralement dans un SOC (Security Office Center), ces acteurs ont pour principales missions de détecter tout évènement anormal dans le système d'information, le qualifier et y remédier

• **Les métiers d'auditeur en sécurité :** Souvent appelés pentesteurs, ces acteurs ont des compétences offensives et leurs principales missions ont pour objectif de tester la robustesse d'un système d'information aux tentatives d'intrusion et préconiser des solutions adéquates.

• **Les métiers de l'informatique légale :** Ce domaine, souvent intitulé « forensic » demande la mise en œuvre de protocoles d'investigation en phase avec la législation, et ont pour objet d'apporter des preuves numériques dans le cadre d'enquêtes judiciaires, ou internes à l'entreprise.

• Enfin, la mise en œuvre de politiques de sécurité dans l'entreprise est encadrée par des préconisations de l'ANSII, des normes ISO, leur mise en œuvre et application doit respecter la législation du pays dans lequel exerce une entreprise.

2. COMPETENCES EVALUEES EN COMPETITION

À compter de la 49e édition, la compétition s'organise autour de deux dominantes — Offensive et Défensive — dans lesquelles chaque candidat s'inscrit (orientation confirmée par le prestataire). Les compétences du métier restent évaluées dans leur ensemble : un socle commun de cybersécurité est attendu de tous les candidats, quelle que soit la dominante choisie, afin de préserver un profil polyvalent. Les compétences ci-dessous reprennent et actualisent celles du référentiel précédent (épreuves Enterprise, Analyse SOC, Forensic et RedTeam), réorganisées selon ces deux dominantes et un socle transversal.

SOCLE COMMUN — Compétences transversales évaluées quelle que soit la dominante

	Régional	Qualification	Finale
Configurer, administrer et sécuriser des systèmes d'exploitation Windows et GNU/Linux	X	X	X
Comprendre et exploiter une infrastructure réseau et virtualisée (segmentation, services, flux)	X	X	X
Comprendre les services d'entreprise et l'annuaire (Active Directory, LDAP, DNS, DHCP, messagerie)	X	X	X
Exploiter et analyser des journaux, y compris à l'aide d'expressions régulières	X	X	X
Automatiser des tâches de sécurité par le scripting (Python, Bash, PowerShell)	X	X	X
Situer un événement dans une chaîne d'attaque (Cyber Kill Chain, MITRE ATT&CK)	X	X	X
Appliquer une méthodologie rigoureuse, gérer son temps et respecter le périmètre d'intervention	X	X	X
Documenter, justifier techniquement et restituer ses travaux	X	X	X

DOMINANTE OFFENSIVE — Pentest et Red Team (environ 60 à 70 % de l'épreuve)

	Régional	Qualification	Finale
Domaine : Reconnaissance et collecte d'informations			
Mener une reconnaissance passive et active et cartographier l'environnement cible	X	X	X
Énumérer les services, applications et annuaires ; réaliser du fingerprinting	X	X	X
Domaine : Analyse de vulnérabilités			
Identifier et qualifier des vulnérabilités techniques et logiques	X	X	X
Prioriser les vecteurs d'attaque selon leur faisabilité et leur impact	X	X	X
Domaine : Exploitation			
Exploiter des vulnérabilités Web (référence OWASP Top 10, édition 2025)	X	X	X
Exploiter des systèmes GNU/Linux et Windows	X	X	X
Auditer et compromettre un environnement Active Directory	X	X	X
Réaliser une élévation de privilèges et des mouvements latéraux	X	X	X
Domaine : Post-exploitation et restitution			
Démontrer l'impact dans le respect du périmètre (preuves, données factices)	X	X	X
Construire et documenter une chaîne d'attaque complète	X	X	X
Domaine : Compétences défensives transverses (part minoritaire)			
Comprendre les mécanismes de détection, lire des journaux et interpréter une alerte	X	X	X

Comprendre les démarches d'investigation et d'analyse de traces	X	X	X

DOMINANTE DÉFENSIVE — SOC, Analyse et Forensic (environ 60 à 70 % de l'épreuve)

	Régional	Qualification	Finale
Domaine : Supervision et détection			
Collecter et exploiter la télémétrie (journaux Windows, Sysmon, journaux Linux, flux réseau)	X	X	X
Exploiter une plateforme SIEM et construire des requêtes de filtrage	X	X	X
Qualifier et corréler des alertes de sécurité	X	X	X
Mener une activité de threat hunting ciblée (IOC, TTP, MITRE ATT&CK)	X	X	X
Domaine : Analyse réseau			
Analyser une capture de trafic réseau (PCAP) afin d'identifier une activité malveillante	X	X	X
Domaine : Investigation numérique (forensic)			
Investiguer un système Windows compromis et exploiter les artefacts	X	X	X
Réaliser une analyse de la mémoire vive	X	X	X
Analyser une campagne de phishing et un corpus de messages	X	X	X
Conduire une investigation forensic mobile lorsqu'elle est au programme	X	X	X
Domaine : Reconstitution d'incident			
Reconstituer une chronologie (timeline) et rechercher des indicateurs de compromission	X	X	X
Identifier la chaîne d'attaque et les techniques employées par l'attaquant	X	X	X
Domaine : Compétences offensives transverses (part minoritaire)			
Comprendre les techniques de reconnaissance et d'exploitation d'un attaquant	X	X	X
Comprendre et caractériser une vulnérabilité à partir de son exploitation	X	X	X

3. MODALITES DES EPREUVES

3.1 Organisation générale

L'épreuve est individuelle. Chaque sélection représente environ 6 heures d'épreuve et se compose de plusieurs challenges de difficulté progressive (orientation confirmée par le prestataire). Avant la compétition, chaque candidat s'inscrit dans une dominante : Offensive ou Défensive.

La répartition envisagée est d'environ 60 à 70 % de l'épreuve sur la dominante choisie et d'environ 30 à 40 % sur les autres domaines de la cybersécurité. Il ne s'agit pas de créer deux profils cloisonnés : le candidat doit conserver un profil polyvalent et démontrer, même dans sa dominante, une compréhension des mécanismes de l'autre spécialité.

Le découpage précis de la journée, notamment la répartition des challenges entre le matin et l'après-midi, est à définir avec le prestataire / l'équipe métier.

3.2 Dominante Offensive

OBJECTIF : former un profil principalement offensif (pentest et Red Team), capable de comprendre les mécanismes de défense, de détection et d'investigation.

DOMAINES ÉVALUÉS : reconnaissance et collecte d'informations, découverte de l'environnement cible, identification de vulnérabilités, vulnérabilités Web, exploitation, compromission de systèmes, élévation de privilèges, attaques système, post-exploitation. Une part minoritaire porte sur le SOC, le forensic, l'analyse réseau et l'investigation.

ACTIVITÉS POSSIBLES : cartographier et énumérer une cible, identifier et valider des vulnérabilités, exploiter une application Web ou une infrastructure, auditer et compromettre un domaine Active Directory, progresser sur une chaîne d'attaque jusqu'à l'objectif fixé.

COMPÉTENCES ATTENDUES : identifier les services exposés d'un système cible et déterminer les vecteurs d'attaque potentiels ; exploiter une vulnérabilité de manière contrôlée et démontrer son impact ; justifier chaque étape techniquement et rester dans le périmètre autorisé.

LIVRABLES POSSIBLES : preuves de compromission (par exemple au format « flag »), traces d'exploitation, éléments de restitution. La nature exacte des livrables est à définir avec le prestataire / l'équipe métier.

EXEMPLES DE TECHNOLOGIES / OUTILS : distribution d'audit (par exemple Kali Linux), outils d'énumération et de cartographie réseau, outils de test d'intrusion Web et d'audit Active Directory. Ces exemples sont cités à titre indicatif et ne constituent pas une liste imposée.

3.3 Dominante Défensive

OBJECTIF : former un profil principalement Blue Team / DFIR, capable de comprendre concrètement les méthodes utilisées par un attaquant.

DOMAINES ÉVALUÉS : SOC, analyse de journaux, détection et qualification d'incidents, investigation, analyse réseau et analyse PCAP, forensic, analyse mémoire, phishing, reconstitution d'incidents, recherche d'indicateurs de compromission. Une part minoritaire intègre des challenges offensifs ou système : exploitation, compréhension d'une vulnérabilité, reconnaissance.

ACTIVITÉS POSSIBLES : exploiter un SIEM, analyser des journaux et des captures réseau, qualifier et corréler des alertes, investiguer un système compromis, analyser la mémoire, examiner une campagne de phishing, reconstituer la chronologie et la chaîne d'une attaque.

COMPÉTENCES ATTENDUES : corréler plusieurs événements de sécurité afin de reconstituer une séquence d'attaque ; identifier les indicateurs de compromission et les techniques employées ; appuyer chaque conclusion sur des artefacts vérifiables.

LIVRABLES POSSIBLES : réponses d'investigation (par exemple au format « flag »), chronologie d'incident, indicateurs de compromission identifiés, éléments de restitution. La nature exacte des livrables est à définir avec le prestataire / l'équipe métier.

EXEMPLES DE TECHNOLOGIES / OUTILS : plateforme SIEM open source, outils d'analyse réseau, outils d'investigation système et mémoire, outils d'analyse forensic. Ces exemples sont cités à titre indicatif et ne constituent pas une liste imposée.

3.4 Compétences transversales

Quelle que soit la dominante, l'épreuve mobilise des compétences transversales évaluées en continu :

- Analyse et raisonnement structuré
- Méthodologie d'intervention
- Gestion du temps
- Compréhension du réseau et des systèmes
- Scripting et automatisation
- Documentation, restitution et justification technique
- Respect du périmètre d'intervention et du cadre éthique

3.5 Format des challenges

L'épreuve peut être constituée de plusieurs challenges indépendants ou liés, de difficulté croissante. À titre de proposition de structuration (et non de décision actée du prestataire), trois niveaux peuvent être distingués :

- Niveau 1 — identification, observation, analyse simple.
- Niveau 2 — investigation ou exploitation nécessitant plusieurs étapes.
- Niveau 3 — corrélation, exploitation avancée ou chaîne d'attaque / d'investigation complète.

Le nombre exact de challenges, leur pondération et la répartition par niveau sont à définir avec le prestataire / l'équipe métier.

4. EVALUATION

4.1 Répartition des points par dominante (proposition, à ± 5 %)

La répartition fixe de l'édition précédente (Enterprise 35 %, BlueTeam 25 %, Forensic Android 15 %, RedTeam 25 %) n'est plus compatible avec l'organisation par dominante. Elle est remplacée par une logique alignée sur l'orientation du prestataire : la dominante choisie représente la majorité des points, les autres domaines le complément.

Domaine de compétences	Régional	Qualification	Finale
Dominante choisie (Offensive ou Défensive)	60 à 70 %	60 à 70 %	60 à 70 %
Autres domaines de cybersécurité (compétences transversales)	30 à 40 %	30 à 40 %	30 à 40 %
TOTAL	**100 %**	**100 %**	**100 %**

La pondération définitive sera arrêtée pour chaque niveau de compétition, dans le respect d'une dominante représentant environ 60 à 70 % des points. Le choix d'un ratio précis (par exemple 60/40, 65/35 ou 70/30) est à valider par le prestataire / l'équipe métier.

4.2 Notation mesurable et notation jugée

L'évaluation privilégie une notation objective et reproductible (type Measurement), appuyée sur des preuves techniques, des artefacts, des journaux ou des livrables vérifiables. Une part de notation jugée (type Judgement) peut porter sur la méthode, la qualité et la pertinence professionnelle de la restitution. La proportion exacte Measurement / Judgement est à définir avec le prestataire / l'équipe métier.

4.3 Description des critères de notation, des attendus et des tolérances applicables

Le barème de notation détaillé sera établi par le prestataire pour chaque sujet et dévoilé en amont des épreuves, dans la continuité du modèle de la précédente CNAT. Il précisera, par challenge, les critères, sous-critères et aspects de notation ainsi que les tolérances applicables.

5. EQUIPEMENT ET MATERIAUX

LISTE D'INFRASTRUCTURES

La liste des infrastructures reprend tous les équipements courants, matériaux et installations mis à disposition des compétiteurs sur les espaces de concours en général.

MATÉRIAUX, ÉQUIPEMENTS ET OUTILS QUE LES COMPÉTITEURS APPORTERONT DANS LEUR CAISSE À OUTILS

Aucune caisse à outil n'est nécessaire pour ce métier.

MATÉRIAUX ET ÉQUIPEMENTS INTERDITS SUR L'ESPACE DE CONCOURS

Aucun système de communication numérique synchrone ou asynchrone n'est autorisé durant la compétition.Exemple : téléphones, ordinateurs, objet connecté).

Aucun appareil électronique appartenant au candidat ne sera accepté (exception ; matériel nécessaire pourles personnes en situation de handicap, dont la demande devra être produite en amont par le candidat).

EXIGENCES DE SÉCURITÉ LIÉES AU MÉTIER

Aucune exigence particulière n'est imposée pour ce métier.

6. REGLES SPECIFIQUES AU METIER

Par principe et pour s'orienter au plus près de l'épreuve internationale, l'utilisation d'internet en dehors des plateformes mises en place et de tout outil IA est strictement interdite sauf évolution du règlement de compétition.

DOCUMENTS COMPLEMENTAIRES AU REFERENTIEL DE COMPETITION

Le Référentiel de Compétition Métier ne contient que des informations relatives au métier. Il doit donc être utilisé en association avec le règlement de la Compétition Nationale des Métiers et ne peut contredire ce Règlement. En cas de contradiction qui resterait dans le présent document, c'est le Règlement de la Compétition qui prime.