SIMULIS

TESTS DE SIMULATIONS SYSTEMES, DE BASES DE DONNEES ET D'APPLICATIONS

FICHE D'IDENTITÉ — SIMULIS

Nom du certificat	SIMULIS — TESTS DE SIMULATIONS SYSTEMES, DE BASES DE DONNEES ET D'APPLICATIONS
Code CRC	SMU00220FS112026
Code fiche (RCI)	**RICC1717**
Domaine(s)	CYBERSECURITE | TESTS ET SIMULATIONS | BASES DE DONNEES | APPLICATIONS | QA | PENTESTING
Entité concernée	Cybersécurité, Éditeurs logiciels, ESN, DSI, Cabinets d'audit IT, Institutions financières
Niveau de qualification	Niveau 6 (Bac + 3 et Bac + 4)
État	Active
Date d'échéance	22.10.2030
Organisme certificateur	Mobile Sharing
Régulateur	RICC – Régulation Internationale des Compétences et des Certifications Professionnelles
Base légale	Arrêté du 22 mars 2023, BO RICC n°1549 du 22 mars 2023
Date de décision	22.10.2026
Date de publication de la fiche	22.11.2026
Date de début des parcours	22.11.2026
Date de dernière délivrance	22.10.2030

APERÇU ET DESCRIPTION DE LA CERTIFICATION SIMULIS

La certification SIMULIS — TESTS DE SIMULATIONS SYSTEMES, DE BASES DE DONNEES ET D'APPLICATIONS est délivrée par Mobile Sharing, accrédité FAIF.

Elle certifie les experts en tests de sécurité et en simulation des systèmes d'information.

Elle valide la maîtrise des techniques de pentesting, de fuzzing et de simulation des systèmes, bases de données et applications dans le cadre de la sécurité informatique. Domaines de compétence : Tests de pénétration (pentesting) : Méthodologies de pentesting (PTES, OWASP), reconnaissance et scanning, exploitation des vulnérabilités, post-

exploitation, rapport de pentesting ; Simulation de systèmes : Tests de charge et de performance, simulation des pannes et de la résilience, chaos engineering, disaster recovery testing ; Sécurité des bases de données : Injections SQL, audit de sécurité des SGBD, chiffrement des données, contrôle d'accès aux bases, test de conformité RGPD des BDD ; Sécurité des applications : OWASP Top 10, tests d'applications web et mobiles, analyse statique et dynamique du code (SAST/DAST), security code review.

Activités et secteurs visés	Types d'emploi ciblés
Cybersécurité | Éditeurs logiciels | ESN | DSI | Cabinets d'audit IT | Institutions financières	Expert Cybersécurité, Pentester, QA Engineer, Responsable Tests, Auditeur Sécurité SI, Consultant en Tests d'Intrusion

RÉFÉRENTIELS ET SOUS-CERTIFICATIONS — SIMULIS

Code	Sous-certification	Type	Profils cibles
`SIMULIS-CERT`	**SIMULIS — CERTIFIED SKILLS**	Niveau Base	Expert Cybersécurité, Pentester, QA Engineer, Responsable Tests, Auditeur Sécurité SI, Consultant en Tests d'Intrusion
`SIMULIS-PROF`	**SIMULIS — PROFESSIONAL SKILLS**	Niveau Expert	Expert Cybersécurité, Pentester, QA Engineer, Responsable Tests, Auditeur Sécurité SI, Consultant en Tests d'Intrusion

CLIENTS POTENTIELS ET MARCHÉS CIBLES — SIMULIS

Segment	Description	Profils potentiels ciblés
Entreprises et Organisations	PME, ETI, grandes entreprises, multinationales, groupements professionnels cherchant à certifier et valoriser les compétences de leurs collaborateurs.	
Professionnels en Activité	Cadres, managers et techniciens souhaitant valider, renforcer et faire reconnaître officiellement leurs compétences dans leur domaine d'expertise.	
Demandeurs d'Emploi & Reconversion	Personnes en recherche d'emploi ou en reconversion professionnelle souhaitant acquérir une certification reconnue pour accélérer leur retour à l'emploi.	

Segment	Description	Profils potentiels ciblés
Établissements de Formation	Écoles, universités, centres de formation agréés FAIF intégrant la certification dans leurs cursus comme débouché professionnel certifié.	

SIMULIS — CERTIFIED SKILLS (NIVEAU BASE)

APERÇU ET PROFILS VISÉS

Les modules et compétences suivants constituent le référentiel de la certification CERTIFIED SKILLS. La maîtrise de ces éléments est validée par des évaluations théoriques et pratiques dans le contexte professionnel du domaine.

COMPÉTENCES MÉTIERS — SIMULIS — CERTIFIED SKILLS

Code	Compétence	Niveau
M1	Tests de pénétration et pentesting : Méthodologies de tests de pénétration (PTES, OWASP Testing Guide, NIST), phases du pentest (reconnaissance, scan, exploitation, post-exploitation, reporting), outils de pentesting (Kali Linux, Metasploit, Burp Suite, Nmap, Wireshark), cadre légal et éthique du pentest.	Basique
M2	Sécurité des applications web : Vulnérabilités des applications web (OWASP Top 10 : injection SQL, XSS, CSRF, SSRF, XXE), tests de pénétration web, analyse des APIs REST/GraphQL, sécurité des applications mobiles.	Basique
M3	Sécurité des réseaux et infrastructures : Tests de pénétration des réseaux (LAN, WAN, WiFi, VPN), analyse des protocoles réseau, sécurité des systèmes (Linux, Windows, Active Directory), attaques et contre-mesures (MITM, ARP poisoning, escalade de privilèges).	Intermédiaire
M4	Forensique numérique et réponse aux incidents : Investigation numérique légale (forensique), analyse des incidents de sécurité, gestion des crises cyber, analyse des malwares, threat intelligence, outils forensiques (Autopsy, Volatility, FTK).	Intermédiaire
Total		**4**

COMPÉTENCES COMPORTEMENTALES — SIMULIS — CERTIFIED SKILLS

Code	Compétence	Niveau
C1	Analyse et évaluation des risques de sécurité : Capacité à analyser les vulnérabilités d'un système, évaluer les risques de sécurité, réaliser les tests de pénétration.	Tous niveaux
C2	Communication des rapports de sécurité : Rédaction des rapports de pentest, communication des vulnérabilités aux équipes techniques et aux directions, recommandations de remédiation.	Tous niveaux
C3	Travail en équipe sécurité : Collaboration avec les équipes de développement (DevSecOps), les administrateurs systèmes et les directions SI.	Tous niveaux
C4	Adaptabilité aux nouvelles menaces : Veille sur les nouvelles vulnérabilités et techniques d'attaque, adaptation des méthodologies de pentest aux nouvelles technologies.	Intermédiaire
Total		**4**

VOIES D'ACCÈS À LA CERTIFICATION

Voie d'accès	Oui	Non	Jury
Après un parcours de formation sous statut d'élève ou d'étudiant		NON	
En contrat d'apprentissage		NON	
Après un parcours de formation continue	OUI		Oui
En contrat de professionnalisation ou d'alternance		NON	
Par candidature individuelle		NON	
Par Validation des Acquis de l'Expérience (VAE)	OUI		Oui

Prérequis : Bac+3 en informatique. 2 ans d'expérience IT ou cybersécurité. Certifications techniques recommandées (CEH, CompTIA Security+).

MODALITÉS D'ÉVALUATION

Bloc de compétences	Modalité d'évaluation
Bloc 1 — Fondamentaux métier	Évaluation des connaissances fondamentales du domaine, des concepts clés, de la réglementation applicable et du contexte professionnel.
Bloc 2 — Application professionnelle	Mise en pratique des compétences sur des situations professionnelles réelles ou simulées, cas pratiques et exercices d'application.
Bloc 3 — Performance et résultats	Évaluation de la capacité à produire des résultats mesurables, à optimiser les processus et à démontrer une maîtrise opérationnelle avancée.
Bloc 4 — Compétences comportementales	Évaluation des postures professionnelles, de la communication, du travail en équipe, du leadership et des comportements éthiques.

Score global >= 90/100 — Seuil minimal >= 65/100 par bloc (en dessous, reprise de l'examen du bloc) — Validité : 3 ans, renouvellement possible — Jury paritaire FAIF composé de professionnels du secteur et d'experts pédagogiques — Examen en présentiel, à distance sécurisé ou mixte.

SIMULIS — PROFESSIONAL SKILLS (NIVEAU EXPERT)

APERÇU ET PROFILS VISÉS

Les modules et compétences suivants constituent le référentiel de la certification PROFESSIONAL SKILLS. Ce niveau valide une maîtrise approfondie et stratégique du domaine, intégrant des dimensions managériales, de leadership et de transformation organisationnelle.

COMPÉTENCES MÉTIERS — SIMULIS — PROFESSIONAL SKILLS

Code	Compétence	Niveau
M1	Tests de pénétration et pentesting : Méthodologies de pentest, phases, outils (Kali Linux, Metasploit), cadre légal.	Basique
M2	Sécurité des applications web : OWASP Top 10, tests de pénétration web, sécurité des APIs et applications mobiles.	Basique
M3	Sécurité des réseaux et infrastructures : Pentest réseau, protocols, Active Directory, escalade de privilèges.	Intermédiaire
M4	Forensique numérique et réponse aux incidents : Investigation numérique, gestion des incidents, analyse malwares, threat intelligence.	Intermédiaire
M5	Stratégie de cybersécurité offensive et défensive : Stratégie de cybersécurité (Red Team/Blue Team/Purple Team), gestion des risques cyber, SOC et SIEM, Zero Trust architecture.	Avancé
M6	Innovation en cybersécurité : Intelligence artificielle pour la cybersécurité (détection d'anomalies, threat hunting), cybersécurité de l'IoT, blockchain et sécurité, cybersécurité des systèmes industriels (ICS/SCADA).	Avancé
M7	Leadership en cybersécurité : Direction des équipes de cybersécurité (CISO, responsable sécurité), management des SOC, relations avec les autorités et les CERT.	Expert
M8	Excellence en cybersécurité africaine : Développement de la cybersécurité africaine, contribution aux CERT nationaux africains, formation des experts en sécurité informatique.	Expert
Total		**8**

COMPÉTENCES COMPORTEMENTALES — SIMULIS — PROFESSIONAL SKILLS

Code	Compétence	Niveau
C1	Expertise en tests de pénétration avancés : Expertise avancée en pentesting et en évaluation de la sécurité des systèmes complexes.	Tous niveaux
C2	Communication cybersécurité stratégique : Présentation des rapports de sécurité aux comités de direction, communication sur les risques cyber.	Tous niveaux

Code	Compétence	Niveau
C3	Leadership des équipes de sécurité : Direction des équipes de cybersécurité (Red Team, SOC), management du CISO.	Tous niveaux
C4	Adaptabilité aux nouvelles menaces cyber : Anticipation des nouvelles formes de cyberattaques, développement des capacités de réponse.	Intermédiaire
C5	Influence sur la cybersécurité africaine : Contribution aux politiques de cybersécurité nationales, développement des CERT africains.	Intermédiaire
C6	Vision stratégique de la cybersécurité africaine : Stratégie de développement de la résilience cyber africaine, souveraineté numérique.	Avancé
C7	Gestion du changement sécurité : Transformation des cultures organisationnelles vers la cybersécurité, adoption du Zero Trust.	Avancé
Total		**7**

VOIES D'ACCÈS À LA CERTIFICATION

Voie d'accès	Oui	Non	Jury
Après un parcours de formation sous statut d'élève ou d'étudiant		NON	
En contrat d'apprentissage		NON	
Après un parcours de formation continue	OUI		Oui
En contrat de professionnalisation ou d'alternance		NON	
Par candidature individuelle		NON	
Par Validation des Acquis de l'Expérience (VAE)	OUI		Oui

Prérequis : Bac+3 en informatique. 2 ans d'expérience IT ou cybersécurité. Certifications techniques recommandées (CEH, CompTIA Security+).

MODALITÉS D'ÉVALUATION

Bloc de compétences	Modalité d'évaluation
Bloc 1 — Fondamentaux métier	Évaluation des connaissances fondamentales du domaine, des concepts clés, de la réglementation applicable et du contexte professionnel.
Bloc 2 — Application professionnelle	Mise en pratique des compétences sur des situations professionnelles réelles ou simulées, cas pratiques et exercices d'application.
Bloc 3 — Performance et résultats	Évaluation de la capacité à produire des résultats mesurables, à optimiser les processus et à démontrer une maîtrise opérationnelle avancée.
Bloc 4 — Compétences comportementales	Évaluation des postures professionnelles, de la communication, du travail en équipe, du leadership et des comportements éthiques.

Score global >= 90/100 — Seuil minimal >= 65/100 par bloc (en dessous, reprise de l'examen du bloc) — Validité : 3 ans, renouvellement possible — Jury paritaire FAIF composé de professionnels du secteur et d'experts pédagogiques — Examen en présentiel, à distance sécurisé ou mixte.

Vérifier cette certification

Cette fiche fait foi telle qu'elle est publiée au répertoire de la RICC. Scannez le code ou ouvrez : **https://ricc.in/repertoire/RICC1717**