Date version document : 22/03/2024

Programme de Formation

RS6062 – TOSA DIGCOMP

Objectifs finaux

Objectifs professionnels :

À l'issue de la formation, le stagiaire sera capable de :

- ✓ Mettre en œuvre des recherches sur le Web de manière sécurisée
- ✓ Communiquer sur le Web de manière sécurisée
- ✓ Corriger les erreurs communes en systèmes et réseaux
- ✓ Gérer les risques en cas de cyberattaque et mettre le réseau en sécurité
- ✓ Créer du contenu digital
- ✓ Organiser le travail collaboratif sur le Cloud

Aptitudes :

À l'issue de la formation, le stagiaire sera capable de :

- ✓ Connaitre les risques d'une cyberattaque
- ✓ Comprendre les enjeux sécurité du Web
- ✓ Connaitre les méthodes de sécurisation

Catégorie

La catégorie prévue à l'article L.6313-1 est : Action de formation

Public

Le public concerné est : tout public / personnes souhaitant développer leurs compétences professionnelles dans le numérique et la cybersécurité

Prérequis

Les conditions d'accès sont :

Prérequis : aucun

Niveau exigé : aucun

Durée

Cette formation se déroulera en 35 heures sur un durée totale de 1 mois.

Horaires : flexibles – cette formation se déroule en 100% distanciel

Lieu

Cette formation est accessible en ligne sur la plateforme cyberini.com – identifiants individuels pour suivi d'exécution de l'action

Tarif

Cette formation est dispensée pour un coût de 1500 euros HT soit 1500 TTC (taux de tva 0% au titre de l'Art. 261.4.4 a du CGI).

Cyberini

Michel KARTNER (Cyberini)
128 rue la Boétie, 75008 Paris
SIRET 79333268500023 - TVA Intracommunautaire FR53793332685
Déclaration d'activité de formation enregistrée sous le n°11756144875 du préfet de région de la Région Ile-de-France

Programme de Formation

Modalités et délais d'accès

L'inscription est réputée acquise lorsque : le candidat a validé son inscription et reçu le mail de bienvenue.
Les délais d'accès à l'action sont : entre 11 et 30 jours ouvrés.

Moyens pédagogiques, techniques et d'encadrement

Méthodes et outils pédagogiques

Méthodes pédagogiques : Pédagogie active basée sur des séances vidéo, des supports de cours, des QCM, et des travaux pratiques organisés à distance de façon asynchrone que le stagiaire devra réaliser et remettre lorsqu'il termine chaque module.
Outils pédagogiques : La plateforme pédagogique est proposée sous forme de Learning Management System (LMS) accessible au moyen d'une connexion internet
Supports pédagogiques : livret d'accueil et supports accessibles en ligne via la plateforme e-learning 24/7
Prise en compte du handicap : nous proposons des compensations et un accompagnement individualisé pour les PSH – la durée de la formation est adaptable. Tous nos supports de cours peuvent être modifiés pour répondre aux besoins et contraintes. Merci de nous contacter à l'adresse e-mail : support@cyberini.com - pour la certification, des modalités d'évaluation adaptées peuvent être proposées – notre référent handicap M. Michel KARTNER vous accompagne dans les démarches.

Éléments matériels de la formation

Supports techniques : plateforme e-learning - Un compte Cyberini dédié permettra au stagiaire de suivre la formation dans son intégralité et d'effectuer le suivi individualisé. Accessibilité 24/7 à la plateforme en ligne (système LMS LearnDash). Le bénéficiaire doit être muni du matériel informatique répondant aux exigences de cette action : connexion Internet, micro et webcam (pour l'examen).
Documentation : supports de cours consultables 24/7 sur la plateforme.

Compétences des formateurs

La formation est réalisée par M. Michel KARTNER et l'assistance pédagogique et technique sont assurées par M. MICHEL KARTNER, formateur IT depuis 2013, diplômé d'un master en informatique et assurant des formations informatiques depuis 10 années.

Formation ouverte ou à distance FOAD

Nature des travaux et durée estimée : QCM et travaux pratiques à rendre à la fin de chaque module : durée estimée de 3 heures.
Modalités de suivi de l'action de formation : temps de connexion sur la plateforme, QCM, travaux réalisés, accompagnement pédagogique et technique.

Modalités d'évaluation : test de positionnement**,** évaluations pendant le parcours de formation, évaluation de fin de formation.

Évaluation finale : certification TOSA DIGCOMP RS6062

Accompagnement / assistance pédagogique : accompagnement réalisé par MICHEL KARTNER, formateur IT depuis 2013, diplômé d'un master en informatique et assurant des formations informatiques depuis 10 années. L'assistance pédagogique se fait par mail, par téléphone ou bien directement sur la plateforme pédagogique e-learning. Les réponses sont apportées soit en instantané dès que possible ou dans un délai de 24h les jours ouvrés.

Accompagnement / assistance technique : accompagnement réalisé par MICHEL KARTNER, formateur IT depuis 2013, diplômé d'un master en informatique et assurant des formations informatiques depuis 10 années. L'assistance pédagogique se fait par mail, par téléphone ou bien directement sur la plateforme pédagogique e-learning. Les réponses sont apportées soit en instantané dès que possible ou dans un délai de 24h les jours ouvrés.

Contenu de la formation

MODULE 1 : GERER LES INFORMATIONS ET AMELIORER SA CULTURE DES DONNÉES (4h45)

- *Rechercher des informations sur le Web*
- *Gérer l'historique de navigation et la navigation privée*
- *Créer et organiser les favoris et les notes*
- *Identifier les risques d'une navigation non sécurisée et des extensions*
- *Gérer les fichiers cookie et les caches*
- *Evaluer la crédibilité d'une source et d'une information*
- *Mettre en place des outils de veille sur Internet*
- *Créer son propre outil de recherche d'emploi*
  TP : trouver les informations d'un document en recherchant sur le Web (temps estimé 45min

MODULE 2 : COMMUNIQUER ET COLLABORER SUR INTERNET (4h45)

- *Gérer, classer et trier ses mails sur Outlook et Gmail*
- *Exploiter les paramètres avancés des e-mails et gérer les spams*
- *Créer et Gérer les listes de diffusion*
- *Sélectionner un prestataire cloud en fonction des besoins et contraintes*
- *Stocker des données en sécurité*
- *Gérer les réseaux sociaux en protégeant ses données*
- *Gérer son identité numérique et sa e-réputation*
- *Réaliser un travail collaboratif en ligne*
- *Vérifier la véracité des commentaires en ligne*
  TP : retrouver un CV caché dans un cloud (temps estimé 45min)

MODULE 3 : CREER DU CONTENU DIGITAL (4h30)

- *Créer un CV sur Word*
- *Identifier les outils de PAO pour produire du contenu*
- *Sélectionner des outils alternatifs à Microsoft Office*
- *Utiliser des banques d'image pour créer du contenu*
- *Administrer un site Wordpress*
- *Exploiter des lignes de code pour créer du contenu*

TP : Mettre en forme un contenu digital selon les consignes (temps estimé 30min)

MODULE 4 : RESOUDRE DES PROBLEMES SUR INTERNET(4h30)

- *Évaluer la gravité d'un incident en adoptant les bons réflexes*
- *Optimiser l'accessibilité sur Internet*
- *Utiliser les chats et forums pour résoudre un problème*
- *Exploiter l'intelligence Artificielle pour trouver des solutions*
- *Dépanner les erreurs système et réseaux*
- *Choisir au mieux son équipement*
  TP : Déboguer un blue screen (temps estimé 30min)

MODULE 5 : ASSURER LES BASES DE LA CYBERSECURITE (5h45)

- *Assurer la confidentialité, l'intégrité et la disponibilité d'une donnée sur Internet*
- *Exploiter le pare-feu Windows*
- *Protéger sa connexion Wi-Fi*
- *Exploiter les ressources pour éviter des vulnérabilités dans un système*
- *Protéger sa vie privée en ligne*
- *Repérer les techniques d'influence en ligne*
- *Évaluer les risques et les impacts de la cybersécurité*
- *Gérer ses mots de passe pour sécuriser l'accès aux données informatiques*
- *Mettre en place un agrégateur d'actualités de cybersécurité*
  TP : Mettre en place un plan d'action pour sécuriser un réseau local (temps estimé 45min)

MODULE 6 : ASSURER LA SECURITE RESEAU ET SYSTÈME ET ATTEINDRE LE NIVEAU EXPERT À L'EXAMEN DE CERTIFICATION (7h45)

- *Comprendre la Cyber kill chain (chaîne de frappe)*
- *Mettre en place la « Défense en profondeur »*
- *Classifier et définir les cyberattaques*
- *Gérer et traiter des cyber risques*
- *Mobiliser les acteurs pour détecter et gérer des incidents cybersécurité*
- *Faire du renseignement et de l'investigation numérique*
- *Connaître les acteurs et les métiers de la cybersécurité*
- *Améliorer son CV en participant à des événements*
- *Reconnaître les standards industriels et métiers*
- *Identifier les enjeux d'une Politique de sécurité et d'un Plan d'Assurance*
- *Comprendre les lois du numérique et le RGPD*
- *Faire des projets pour améliorer son CV*
- *Comprendre les failles de sécurité par la pratique*
- *Mener un test d'intrusion en pratique*
- *TP : Faire du renseignement numérique avec MITRE ATT&CK (45min)*

Programme de Formation

Suivi et évaluation

Exécution de l'action

Les moyens permettant de suivre l'exécution de l'action sont :

☑ *Relevés de connexion de la plateforme*
☑ *QCM et évaluations formatives*
☑ *Évaluation des acquis en fin de session*

Les résultats, les relevés de connexions et le suivi pédagogique et technique sont enregistrés nominativement.

Modalités d'évaluation des résultats (ou d'acquisition des compétences)

Les moyens mis en place pour déterminer si le stagiaire a acquis les connaissances ou les gestes professionnels précisés dans les objectifs sont :

☑ *Questions orales ou écrites (QCM)*
☑ *Travaux à rendre sur la plateforme*
☑ *Evaluation finale*

Évaluation finale :

Certification TOSA Digcomp enregistrée à France Compétences sous le numéro RS6062. À l'issue de l'examen, le candidat se voit attribuer un score (de 0 à 1000), correspondant à un niveau (Initial, Basique, Opérationnel, Avancé ou Expert), qui lui permettra de faire valoir ses compétences sur le marché du travail. La certification est délivrée si le score est supérieur à 551 sous 5 jours ouvrés. Équivalences, passerelles et suite de parcours : N/A.

Sanction de la formation :

Certification TOSA Digcomp enregistrée à France Compétences sous le numéro RS6062.

La certification TOSA® DigiComp (RS6062) atteste pour une durée de 3 ans des compétences de l'apprenant sur une échelle de 1 000 points. L'examen de certification est inclus dans la formation, il se déroule sur la plateforme de l'organisme certificateur Isograd. Le stagiaire s'engage à le réaliser en ligne lorsqu'il a terminé sa formation. La planification à l'examen s'effectue à partir du démarrage de la formation (délai examen prévisionnel: 30 jours). L'examen dure 75min et se présente sous la forme de 45 questions alternant entre des manipulations sur le logiciel et des QCM, dont la difficulté s'adapte selon les réponses du candidat. Le système d'évaluation emploie pour cela un scoring mathématique dit « IRT » (Item Response Theory). Sans demande spécifique, il est dispensé par défaut en français et sur la version logicielle la plus récente. La surveillance est faite par un logiciel et est enregistrée à des fins de contrôle de conformité. Un accès à Internet ainsi qu'un ordinateur équipé d'une webcam et d'un micro sont requis. Une fois l'examen réalisé, le candidat peut consulter en direct ses résultats et reçoit par e-mail une attestation, une restitution détaillée de ses compétences ainsi que son diplôme. La certification TOSA® DigComp évalue 5 compétences digitales : informations et données, communication et collaboration, création de contenu digital, résolution de problèmes et sécurité numérique. Le résultat atteste du niveau de compétences du stagiaire dans chacun de ces domaines.

Programme de Formation

Compétences attestées :

Niveau Opérationnel (score Tosa 551 à 725)

• Filtrer et analyser les différentes sources d'information sur Internet, afin de fiabiliser la collecte de données
• Créer une méthodologie permettant de trier et ranger ses données numériques pour optimiser leur restitution (recherches ciblées sur internet, gestion de son courriel...)
• Diffuser et partager des fichiers numériques en respectant les bonnes pratiques des réseaux sociaux
• Adapter ses communications aux bons interlocuteurs internes et externes à l'entreprise en sélectionnant le canal de diffusion approprié
• Créer ou modifier du contenu numérique, l'enrichir et exploiter différents formats de contenus
• Gérer son style d'écriture et la mise en page de ses documents numériques
• Choisir l'outil, le logiciel ou le service numérique le mieux adapté à ses besoins, dans le but d'optimiser son environnement de travail (boîtes mails, Internet, tableur, logiciel de traitement de texte...)
• Résoudre des problèmes de routines sur un appareil connecté
• Protéger ses données et celles de l'entreprise en renforçant les mesures de sécurité numérique, en vue d'assurer la continuité d'activité (prévention des attaques potentielles sur le réseau)

Niveau Avancé (score Tosa 726 à 875)

• Sélectionner les informations pertinentes et fiables sur Internet correspondant à des recherches ciblées
• Travailler à plusieurs personnes sur un même fichier en conservant les précautions de sécurité personnelle, afin d'optimiser l'efficacité collective : savoir mettre en place des stratégies de communication sur les réseaux sociaux pour fédérer et animer les échanges
• Maîtriser la création de contenus numériques en utilisant les différents outils bureautiques (blogs, fiches produit, posts sur les réseaux sociaux, etc.) et en respectant les licences relatives aux contenus
• Gérer la plupart des problèmes rencontrés lors de l'utilisation des technologies numériques : savoir organiser des serveurs, des systèmes d'exploitation, des ordinateurs, des logiciels, etc.
• Mettre à jour régulièrement ses connaissances en matière de protection des données et transmettre ces compétences à autrui, afin de diffuser les meilleures pratiques de sécurité au sein de son équipe ou de son entreprise

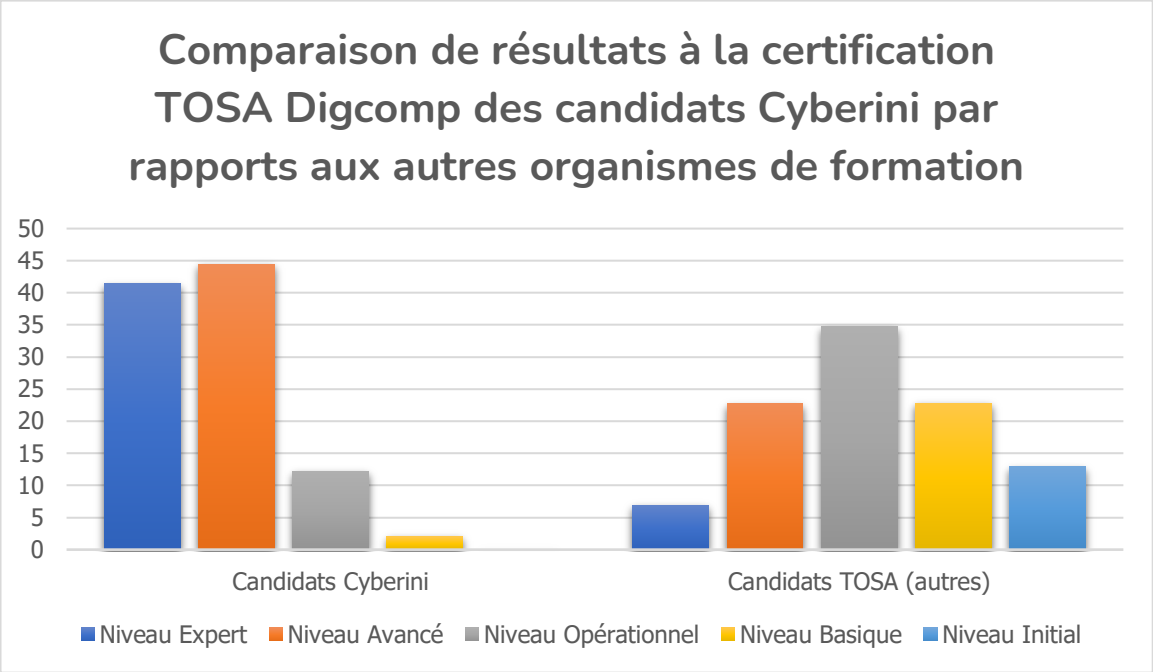
Niveau Expert (score Tosa 876 à 1000)

• Définir et suivre une veille stratégique (veille sociétale, veille en entreprise, veille concurrentielle, veille commerciale, veille fournisseur, veille image, veille juridique ou encore veille technologique), afin d'assurer ou de participer à l'évolution de son secteur professionnel ou son entreprise.
• Participer activement aux espaces en ligne, par exemple les forums ou les réseaux sociaux, en vue de renforcer une présence et une identité d'entreprise (site internet, campagnes d'emailings, réseaux sociaux, webinaires/séminaires, etc.)
• Produire du contenu multimédia complexe, adapté aux différents formats de restitution, afin de correspondre aux attentes des utilisateurs
• Concevoir et mettre en place des pratiques d'apprentissage fondées sur une veille technologique adaptée, afin de renforcer ses compétences numériques
• Crypter ses données personnelles ou professionnelles afin de les protéger des attaques
• Appréhender les risques et facteurs de dépendance au numérique et les transmettre à autrui, en vue de prévenir les phénomènes d'addiction et d'isolement

Date version document : 22/03/2024

Programme de Formation

UNE FORMATION ET DES RÉSULTATS



Source : Cyberini & Isograd – Ensemble de candidats ayant passé la certification sur l'année 2023 (en %)

- La moyenne des notes obtenues par les candidats Cyberini à l'examen de **certification** TOSA® Digcomp est de **848/1000 (taux d'obtention de la certification : 99%)**
- + de **85% des candidats** obtiennent le Niveau « **Avancé** » ou « **Expert** » (score de **725/1000 et +**)
- Le plus haut score est **1000/1000** et le plus bas est **506/1000 (aucun** candidat n'a eu le Niveau « Initial » inférieur à 350/1000)
- Les examens blanc et officiel sont **inclus sans frais supplémentaires avec la formation**
- **88%** des étudiants certifiés affirment que le TOSA® leur permet de faire la différence en entretien

☑ **REJOINDRE CYBERINI C'EST OPTER POUR DES RÉSULTATS ET DES DÉBOUCHÉS**

Michel KARTNER (Cyberini)
128 rue la Boétie, 75008 Paris
SIRET 79333268500023 - TVA Intracommunautaire FR53793332685
Déclaration d'activité de formation enregistrée sous le n°11756144875 du préfet de région de la Région Ile-de-France

Date version document : 22/03/2024

Programme de Formation

CRITÈRES QUALITÉ

Cyberini© dispose d'une charte qualité avec **4 engagements** :

1. L'adaptation de la formation au stagiaire
2. L'application des compétences dans le monde réel
3. La satisfaction du client
4. L'amélioration continue

Cyberini© est un centre de formation **certifié Qualiopi**© n°746 OF Ind 0 (référentiel national sur la qualité des actions concourant au développement des compétences), afin de montrer son engagement dans l'amélioration permanente de ses actions de formation, et de faciliter ses référencements auprès des financeurs.

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

ACN Alliance pour la confiance numérique

TOSA® Centre Agréé

Michel KARTNER (Cyberini)
128 rue la Boétie, 75008 Paris
SIRET 79333268500023 - TVA Intracommunautaire FR53793332685
Déclaration d'activité de formation enregistrée sous le n°11756144875 du préfet de région de la Région Ile-de-France