TOSA

Vos compétences. Votre différence.

Référentiel pédagogique

CyberCitizen

contact@isograd.com

Table des matières

Introduction au référentiel pédagogique

Pour l'évaluation et la certification Tosa

Le Tosa®

Les tests d'évaluation et de certification Tosa® permettent de déterminer le niveau des compétences et les aptitudes d'un candidat sur les logiciels bureautiques et les outils digitaux utilisés dans un environnement professionnel.

Les tests Tosa® sont ainsi conçus pour valider les compétences professionnelles des candidats souhaitant améliorer leur employabilité (salariés, étudiants, demandeurs d'emploi, personnes en reconversion).

Les évaluations et certifications Tosa® sont des tests adaptatifs, élaborés selon des méthodologies scientifiques (la détermination du score est basée sur l'Item Response Theory (IRT)). Elles délivrent ainsi un diagnostic détaillé sur les compétences de chaque candidat.

La robustesse et la fiabilité des tests Tosa® tiennent donc à l'association d'un modèle mathématique d'analyse de la difficulté et de la pertinence des questions (IRT). C'est un modèle très proche de celui utilisé par le GMAT.

Objet du référentiel pédagogique

Ce référentiel pédagogique présente l'ensemble des compétences évaluées dans les domaines et sous-domaines des tests d'évaluation et de certification Tosa® CyberCitizen.

Il précise les compétences techniques attendues pour chaque niveau, et cela dans chacun des quatre domaines de compétences de la cybersécurité. Il s'agit donc d'un outil d'accompagnement dans l'élaboration de programmes d'enseignement ou de formation adaptés au niveau visé par chaque candidat.

Une échelle de score unique

L'évaluation et la certification Tosa® reposent sur une échelle de score unique, traduite en cinq niveaux :

- D'Initial à Expert, pour l'évaluation ;
- De 1 à 1000 pour la certification.

Niveaux Tosa®	Scores Tosa®
Expert	876 - 1000
Avancé	726 – 875
Opérationnel	551 – 725
Basique	351 – 550
Initial	1 – 350

Domaines et sous-domaines de compétences

Le monde de la cybersécurité	▪ Les acteurs de la cybersécurité ▪ Cibles et impacts d'une attaque ▪ Réagir en cas d'attaque ▪ Identité numérique et authentification
Sécurité au bureau	▪ La sécurité du poste de travail ▪ L'ingénierie sociale ▪ Les périphériques amovibles ▪ Versions de logiciel et mises à jour
Sécurité en déplacement	▪ La sécurité physique des terminaux ▪ Smartphones et sécurité ▪ Les réseaux sans fils ▪ La surexposition des données
Sécurité à la maison	▪ Le phishing ▪ Cloud et sauvegarde de fichiers ▪ Les fichiers externes ▪ Vie privée et protection personnelle

À propos de la certification Cybercitizen

La certification CyberCitizen de Tosa s'appuie sur une base de données de plus de 150 questions. Elle est composée de 35 questions et dure 1 heure. L'algorithme s'adapte à chaque réponse des candidats pour ajuster le niveau de difficulté des questions jusqu'à atteindre la définition exacte du niveau des candidats en calculant la limite haute de leurs compétences.

Le test étant adaptatif, la série de questions que reçoit chaque candidat est par conséquent unique pour chaque test. Cette unicité permet une évaluation plus précise du niveau de chaque candidat. Elle limite également la tricherie et la mémorisation de questions sur différents passages.

Notre plateforme permet aux candidats de passer la certification en classe, dans un centre d'examen agréé ou à distance grâce à nos solutions intégrées de surveillance en ligne asynchrone.

Nos solutions de surveillance à distance offrent une flexibilité supplémentaire à l'administrateur et au candidat, en permettant de passer la certification n'importe où et à n'importe quel moment. Le candidat n'a besoin que d'une connexion Internet, d'un ordinateur équipé d'une webcam et d'un microphone en état de marche.

La certification Tosa CyberCitizen est délivrée avec un score (entre 1 et 1000), correspondant à un niveau (Initial, Basique, Opérationnel, Avancé, ou Expert). Il n'y a pas d'exigence pour être éligible à la certification, mais nos recommandations pour être bien préparé le jour de l'examen sont les suivantes :

- Passer au moins une évaluation adaptative Tosa CyberCitizen pour estimer votre niveau et vous familiariser avec le format du test.
- Utiliser les tests d'entraînement gratuits sur notre site web pour vous entraîner
- Suivre des cours d'e-learning ou de formation (la durée moyenne par niveau est de 10 à 15 heures par certification).

Parce que le niveau de compétences d'un candidat évolue en fonction de l'utilisation qui est faite du logiciel, les diplômes de certification Tosa sont valables trois ans à compter de leur date d'émission. Par ailleurs, de nouveaux logiciels et de nouvelles versions de logiciels sortent chaque année, et les compétences doivent par conséquent être mises à jour. Pour cette raison, on ne peut légitimement certifier un niveau de compétences numériques pour plus de trois ans. Limiter la validité de la certification renforce la nécessité de l'apprentissage tout au long de la vie et du développement professionnel.

Les certifications Tosa peuvent être repassées lorsqu'elles sont expirées. Les candidats désireux d'améliorer leur score et leur niveau peuvent également repasser l'examen à tout moment.

Niveau 1 - Initial

Entre 1 et 350 points

Le niveau initial pour un test d'évaluation, ou un score compris entre 1 et 350 pour la certification, est le niveau le moins élevé sur l'échelle de score Tosa®. Il correspond au niveau d'un candidat qui n'est que très peu sensibilisé à la cybersécurité ou qui n'a que des notions très parcellaires et limitées du monde de la sécurité numérique.

L'obtention du niveau initial signifie que le candidat connaît peu, voire pas du tout, les aspects même simples de la cybersécurité, et qu'il ne peut les appliquer dans un environnement professionnel.

Synthèse

Domaines	Compétences
Le monde de la cybersécurité	Connaitre l'intérêt d'un mot de passe Définir une attaque informatique
Sécurité au bureau	Connaître l'importance des mises à jour
Sécurité en déplacement	Nommer les risques induits par les déplacements (vol, exposition des données) Reconnaitre une connexion en HTTPS
Sécurité à la maison	Connaître l'utilité des cookies Reconnaitre un captcha

Niveau 2 - Basique

Entre 351 et 550 points

Préalablement à l'acquisition des compétences du niveau Basique, le candidat aura maîtrisé les compétences du niveau Initial

Le monde de la cybersécurité

Les mots de passe

Créer des mots de passes forts et connaître les caractéristiques d'un mot de passe robuste.

Application métier : créer des accès sécurisés sur tous les services professionnels dès l'arrivée en entreprise.

Les acteurs de la cybersécurité

Identifier les contacts principaux de la cybersécurité privé ou public, interne ou externe à l'entreprise.

Application métier : savoir rapidement vers qui se tourner ou où chercher de l'information en cas de besoin sur des questions de cybersécurité, afin d'accélérer la transmission d'information.

Sécurité au bureau

L'accès à ses terminaux

Sécuriser physiquement et informatiquement l'accès aux terminaux électroniques.

Application métier : garantir la sécurité des données et accès des terminaux en cas d'absence du poste du travail, quelle qu'en soit la durée.

Sécurité en déplacement

Le vol de terminal en déplacement

Limiter le risque de vol du terminal ou des données lors des transports.

Application métier (*ex : Commercial)* : pouvoir partir en déplacement professionnel en réduisant le risque de vol de terminal, ou l'exposition trop évidentes des données.

Sécurité à la maison

Le phishing par email

Vérifier l'absence d'éléments d'hameçonnage lors de l’ouverture d’un courriel.

Application métier : pouvoir traiter ses mails sans exposer son entreprise aux risques d’une attaque par phishing.

La gestion électronique des documents

Utiliser des outils de gestion électronique des documents.

Application métier : garantir la sauvegarde de tous ses fichiers de travail, même en cas de perte ou changement de poste de travail.

Synthèse

Domaines	Compétences
Le monde de la cybersécurité	Créer des mots de passes robustes Identifier les rôles clés au sein d'une entreprise (RSSI, DPO, SOC) Identifier les acteurs publics de la sécurité (ANSSI, CERT FR/EU) Nommer les champs d'actions d'un SOC
Sécurité au bureau	Sécuriser son poste de travail lors de son absence Transférer des données publiques de façon sécurisée
Sécurité en déplacement	Identifier l'augmentation des risques de cybersécurité lors d'un déplacement Connaître les risques d'une connexion sur un Wi-Fi public (aéroport ou gare par exemple) Utiliser le mode avion pour sécuriser ses appareils contenant des données sensibles
Sécurité à la maison	Nommer les éléments à vérifier pour s'assurer du caractère de confiance d'un email Reconnaître une potentielle tentative de phishing par email Stocker sur le cloud des fichiers professionnels Télécharger un document externe ou une pièce jointe de mail Distinguer les principaux champs d'action du RGPD

Niveau 3 - Opérationnel

Entre 551 et 725 points

Préalablement à l'acquisition des compétences du niveau Opérationnel, le candidat aura maîtrisé les compétences du niveau Basique

Le monde de la cybersécurité

Les profils d'attaquants

Citer différents profils d'attaquants, qu'il s'agisse de groupes ou d'individus, et reconnaître des exemples pour chaque profil.

Application métier : facilité la prise de conscience et l'identification du risque en reconnaissant les différents objectifs d'attaquants.

Les gestionnaires de mots de passe

Utiliser un gestionnaire de mots de passe (Keepass est utilisé comme exemple dans le test).

Application métier : garantir un niveau de sécurité élevé sur tous ses accès à des services professionnels

Sécurité au bureau

L'ingénierie sociale

Reconnaître une tentative de manipulation potentielle.

Application métier (*ex : Commercial)* : éviter l'intrusion d'une personne malveillante ou la fuite d'information due à la présence d'un intrus dans les locaux.

Les mises à jour logicielles

Mettre à jour les logiciels et les systèmes d'exploitation.

Application métier : garantir l'installation des dernières versions des logiciels et OS afin de garantir l'application des correctifs de sécurité dès leur publication.

Sécurité en déplacement

Les réseaux sans fil

Reconnaître et utiliser un réseau sans fil sécurisé (Wi-Fi, Bluetooth).

Application métier : pouvoir continuer à travailler sur internet même en déplacement dans un lieu public ou depuis des locaux d'une autre entreprise.

La sécurité des smartphones

Compétence : Sécuriser l'accès aux données et aux services sur un smartphone.

Application métier : pouvoir utiliser son smartphone professionnel en déplacement sans s'exposer à des fuites de données.

Sécurité à la maison

Les fichiers dangereux

Appliquer les précautions requises avec les fichiers inconnus et reconnaître un fichier potentiellement dangereux.

Application métier : limiter le risque lors de l'ouverture de fichiers envoyés par pièce jointe.

Le phishing

Détecter des tentatives de phishing sur différents canaux (mail, SMS, appel)

Application métier : pouvoir utiliser l'intégralité des canaux de communication professionnels sur des documents ou données sensibles, en limitant leur exposition à un risque de fuite ou une attaque.

Synthèse

Domaines	Compétences
Le monde de la cybersécurité	Connaître l'utilité d'un gestionnaire de mots de passe Ajouter un mot de passe dans un gestionnaire (Keepass) Sécuriser son identité numérique avec des mots de passes variés Identifier les cibles privilégiées de potentielles attaques Nommer les motivations habituelles des attaquants
Sécurité au bureau	Appliquer les mises à jour automatiques de logiciels Appliquer les mises à jour automatiques de systèmes d'exploitation Détecter une tentative de manipulation par un agent externe à l'entreprise Réagir de façon appropriée à la présence de personnes inconnues dans les bureaux
Sécurité en déplacement	Classer la sécurité des différents protocoles de sécurité Wi-Fi Ajouter un code d'accès sur son téléphone Reconnaître un certificat SSL Retrouver l'autorité de certification d'un certificat SSL
Sécurité à la maison	Réagir en cas de suspicion de phishing Vérifier l'extension d'un fichier externe Manipuler des fichiers envoyés par pièce jointe Envoyer numériquement des fichiers volumineux publics

Niveau 4 - Avancé

Entre 726 et 875 points

Préalablement à l'acquisition des compétences du niveau Avancé, le candidat aura maîtrisé les compétences du niveau Opérationnel

Le monde de la cybersécurité

Les vulnérabilités

Distinguer les principaux types de vulnérabilités.

Application métier : identifier efficacement des potentielles expositions aux risques de cybersécurité dès la prise de poste, afin d'en mitiger les potentiels impacts.

Les contacts de la cybersécurité

Identifier le contact et le canal pour alerter en cas d'attaque avérée.

Application métier : être un élément fort de la transmission de l'information en cas d'attaque de l'entreprise.

Sécurité au bureau

Le stockage externe

Manipuler en toute sécurité des dispositifs de stockage externes.

Application métier : pouvoir se servir de façon sécurisée de documents transmis par un autre membre de l'entreprise ou un partenaire externe stocké sur une clé USB ou un disque dur, ou en transmettre par ce biais.

L'installation de logiciels

Distinguer les sources de logiciels dignes de confiance.

Application métier : installer de façon sécurisée les logiciels nécessaires au travail mais non fourni par l'entreprise.

Sécurité en déplacement

L'exposition des données en déplacement

Limiter l'exposition des données sensibles par écrit, oralement ou sur écran à l'extérieur.

Application métier : pouvoir travailler sur des documents sensibles depuis les transports ou dans des lieux publics. Organiser des réunions à l'extérieurs des locaux de l'entreprises traitant de sujets sensibles.

Les VPN

Connaître l'utilité et l'utilisation d'un VPN.

Application métier : pouvoir garantir une connexion sécurisée aux services et application de l'entreprise d'où que l'employé se trouve.

Sécurité à la maison

Les documents externes

Manipuler de manière sécurisée tout type de document externe, et savoir faire une analyse antivirus sur un fichier (VirusTotal est utilisé dans le test)

Application métier : pouvoir utiliser en toute sécurité un document envoyé par un partenaire ou une personne inconnue.

Les sphères personnelles et professionnelles

Séparer les usages numériques personnels et professionnels sur les terminaux et applications (réseaux sociaux en particulier)

Application métier : limiter l'exposition de données professionnelles par l'utilisation personnelle de terminaux, outils, ou réseaux sociaux professionnels de l'employé.

Synthèse

Domaines	Compétences
Le monde de la cybersécurité	S'authentifier à un service via une authentification multi-facteurs Savoir quand et pourquoi effectuer un test d'intrusion Appliquer les procédures de sécurité sur son poste de travail en cas d'attaque (déconnexion en particulier) Modifier un mot de passe dans un gestionnaire (Keepass)
Sécurité au bureau	Nommer les risques d'installer un logiciel cracké ou d'une source inconnue Trouver une source de confiance pour télécharger un logiciel Faire une analyse antivirus (avec VirusTotal par exemple) Retrouver la version d'un logiciel donné Manipuler des périphériques de stockages inconnus
Sécurité en déplacement	Utiliser un filtre de confidentialité Sécuriser ses cartes d'accès (transport, carte d'accès hôtel par exemple) Savoir quand utiliser un VPN Distinguer les bénéfices d'utiliser un VPN pour la sécurité Limiter les données laissées par une équipe après son passage dans un nouvel environnement : documents papier, écrits, traces électroniques
Sécurité à la maison	Utiliser ses principaux droits sur ses données personnelles (rectification, suppression) Nommer les éléments à vérifier pour s'assurer du caractère de confiance d'un appel ou d'un SMS Connaître les caractéristiques de sécurité d'un fichier joint Connaître et appliquer les fonctionnalités de sécurité des données personnelles sur les réseaux sociaux

Niveau 5 - Expert

Entre 876 et 1000 points

Préalablement à l'acquisition des compétences du niveau Expert, le candidat aura maîtrisé les compétences du niveau Avancé

Le monde de la cybersécurité

La criticité des attaques

Evaluer les différents potentiels impacts d'une attaque sur une entreprise.

Application métier : prioriser les prises d'actions et de sensibilisation au sein d'une équipe ou d'une entreprise. À ce niveau, le candidat peut former sur la sensibilisation à la cybersécurité.

La collecte de preuves

Reproduire une procédure de collecte de preuve d'intrusion.

Application métier : être un soutien actif à tout employé de l'entreprise afin de faciliter le travail de mitigation et d'investigation des équipes d'experts.

Sécurité au bureau

L'exposition de données sensibles

Limiter l'exposition de documents ou d'informations sensibles.

Application métier : Garantir un niveau d'exposition faible des données de l'entreprise au sein des locaux, pour en limiter la diffusion à des personnels externes, ou interne non concernés.

Le stockage externe chiffré

Sécuriser les informations sur tous les périphériques amovibles.

Application métier : être en mesure de transférer tout type de document, de public à classifié, en utilisant le bon support, chiffré ou non.

Sécurité en déplacement

Sécuriser un nouvel environnement

Sécuriser les terminaux dans un nouvel environnement (hôtel, salle de réunion).

Application métier : pouvoir préparer un environnement sécurisé pour une équipe, pour l'organisation d'une réunion ou un séjour de longue durée à l'hôtel par exemple.

La MDM

Connaître les principes et l'utilité d'un service professionnel de gestion des appareils mobiles (MDM).

Application métier : être un maillon fort de la couverture de sécurité de la flotte mobile de l'entreprise, en étant le référent sur les applications et les données contrôlées par la MDM.

Sécurité à la maison

La continuité d'activité

Maîtriser les principes de la sauvegarde des données et de la stabilité de l'entreprise.

Application métier : garantir un niveau de continuité de l'activité même en cas d'attaque avérée grâce à la disponibilité des fichiers de l'équipe.

Le télétravail d'équipe

Protéger ses informations personnelles et sa vie privée en étant chez soi ou en travaillant à distance.

Application métier : limiter l'exposition de données professionnelles par l'utilisation personnelle de terminaux, outils, ou réseaux sociaux professionnels de l'équipe.

Synthèse

Domaines	Compétences
Le monde de la cybersécurité	• Évaluer la criticité de potentielles attaques pour différentes entreprises • Nommer la norme ISO27001 • Identifier les risques de différents types d'attaques (phishing, ransomware, DDoS) au sein d'une entreprise ou institution donnée
Sécurité au bureau	• Transférer des données sensibles de façon sécurisée • Retrouver la version du système d'exploitation • Traiter de façon sécurisée des documents papier • Désactiver un processus Windows
Sécurité en déplacement	• Identifier les potentiels risques dans un nouvel environnement • Distinguer les avantages et limites d'un service professionnel de gestion des appareils mobiles (MDM) • Distinguer les bénéfices d'utiliser un proxy pour la sécurité
Sécurité à la maison	• Séparer les stockages des documents personnels et professionnels • Prévenir la fuite de données professionnelles sur les réseaux sociaux personnels ou professionnels • Extraire les métadonnées d'un fichier • Envoyer numériquement des fichiers sensibles

TOSA

Vos compétences. Votre différence.

contact@isograd.com
www.tosa.org