

« CHARGÉ(E) DE CYBERSÉCURITÉ »

Durée à définir

CHARGÉ DE CYBERSÉCURITÉ

Public : Cette formation s'adresse à toute personne souhaitant acquérir des compétences professionnelles dans le domaine de la sécurité des personnes et des biens.
Elle est particulièrement adaptée aux personnes en reconversion professionnelle, demandeurs d'emploi, ou salariés souhaitant évoluer vers les métiers de la sécurité privée, de la surveillance ou de la prévention des risques.
Accessibilité handicap : Cette formation est accessible aux personnes en situation de handicap. Pour tout besoin d'aménagement spécifique, merci de nous contacter avant le début de la formation afin que nous puissions étudier ensemble les dispositions adaptées.
Modalité de la formation : présentiel, face à face pédagogique formateurs et distanciel.
Délai d'inscription : 2 semaines avant le début d'une session
Délai d'accès à la formation : toute l'année en continu.
Durée à définir.
Tarifs à définir.

▪ OBJECTIFS DE LA FORMATION

Cette formation vise à transformer l'expérience du stagiaire en support technique et ses compétences en "Cybersécurité (débutant)" en une expertise opérationnelle de Chargé de Cybersécurité. Elle répond aux besoins en compétences relatives à la transformation numérique et la sécurisation des systèmes d'information, exigeant de nouveaux professionnels polyvalents, opérationnels et rigoureux.
Les objectifs sont de préparer du stagiaire à l'immersion directe à un poste opérationnel salarié lui permettant de :
• **Garantir la sécurité des services informatiques :** Assurer la disponibilité, l'intégrité et la confidentialité des services informatiques face aux cyberattaques, en identifiant les menaces et en mettant en œuvre les défenses appropriées.
• **Maîtriser le cadre légal et la conformité :** Protéger les données à caractère personnel et appliquer la réglementation (ex : RGPD).
• **Opérationnaliser les infrastructures :** Aller au-delà des notions pour exploiter un réseau informatique et analyser une structure matérielle et logicielle.
• **Gérer et prévenir les incidents :** Caractériser les risques, analyser des incidents de sécurité et proposer des contre-mesures.
• **Intégrer la sécurité dans le développement :** Coder et prendre en compte la sécurité dans un projet de développement d'une solution applicative.

▪ COMPÉTENCES VISÉES

Compétences Techniques Opérationnelles (Réseau et Analyse)
• Exploiter un réseau informatique et maîtriser la connectivité et les architectures de sécurité.
• Analyser une structure matérielle et logicielle.
• Sécuriser les équipements et les usages des utilisateurs.
• Coder (Scripting) pour l'automatisation des tâches de sécurité.
• Mobiliser des savoirs hautement spécialisés dans un domaine en constante évolution.

Compétences Spécifiques Cybersécurité et Conformité
• Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques.
• Identifier les menaces et mettre en œuvre les défenses appropriées.
• Analyser des incidents de sécurité (logs) et proposer des contre-mesures
• Protéger les données à caractère personnel et appliquer la réglementation.
• Prendre en compte la sécurité dans un projet de développement (DevSecOps).
Compétences Transversales (Gestion et Qualité)
• Analyser ses actions en situation professionnelle, s'autoévaluer pour améliorer sa pratique dans le cadre d'une démarche qualité.
• Gérer des contextes professionnels complexes, imprévisibles.
• Conduire un projet (conception, pilotage, mise en œuvre, évaluation).
• Communiquer à des fins de transfert de connaissances, par oral et par écrit, en français et dans au moins une langue étrangère.
• Respecter les principes d'éthique, de déontologie et de responsabilité environnementale.
• Mettre en œuvre des règles, des normes et des démarches qualité (appliquées aux référentiels de sécurité)

▪ PRÉ-REQUIS

Niveau BAC

▪ CONTENU DE LA FORMATION

Module 1 : Ingénierie Réseau et Sécurité des Systèmes d'Exploitation

• Exploitation d'un réseau informatique (approfondissement TCP/IP, VPN) ;
• Administration et durcissement des systèmes (Windows/Linux Server) ;
• Maîtrise d'Active Directory du point de vue de la sécurité (au-delà des notions) ;
• Installation et validation de la conformité d'une infrastructure.

Module 2 : Analyse de la Menace et Développement Sécurisé

• Analyse d'une structure matérielle et logicielle ;
• Initiation au Coder (Scripting Python pour l'automatisation et l'analyse de logs) ;
• Gestion des vulnérabilités (scans et corrections) ;
• Préparation à la prise de responsabilité et au leadership.

Module 3 : Cybersécurité Opérationnelle, Gestion d'Incidents et Conformité

• Gestion des Incidents et Logs (Analyse des connexions, proposition de contre-mesures) ;
• Mise en œuvre des défenses appropriées et gestion des privilèges (évolution du "contrôle d'accès") ;
• Protection des données à caractère personnel (RGPD) ;
• Intégration de la sécurité dans le cycle de vie du développement applicatif

▪ ÉVALUATION

Exercices Techniques, QCM et mise en situation

▪ MÉTHODES ET MOYENS PÉDAGOGIQUES

Exposés, études de cas, échanges, coaching…
Au cours de la formation, une documentation est remise à chaque stagiaire. Les stagiaires auront accès à l'ensemble de leur cours et le suivi de leur évolution sur la PROGISUITE
Des évaluations seront réalisées à plusieurs étapes de la formation.
Des fiches de séances individuelles seront réalisé pour une formation personnalisée par stagiaire.
Des formateurs qualifiés et/ou expérimenté conformément aux dispositions académiques interviendront tout au long de la formation. Ils interviendront en salle, sur leur poste de travail, et aussi en visio-conférence avec l'application « ZOOM ».

▪ VALIDATION

Bilan complété par le tuteur, le président et le stagiaire.

Nombre de stagiaires ayant terminé ce cursus : 1

Taux d'achèvement : 100 %
Mis à jour le 4 juin 2026

Contact : contact@techinfrance.com - Tel : 07 50 50 21 31