Présentiel/distanciel | Cours Officiel | Formation certifiante

NOUVEAUTÉ

Microsoft Azure Implémenter des contrôles de sécurité de bout en bout pour les charges de travail cloud et IA

Objectifs pédagogiques

- Configurer les mécanismes d'identité, d'authentification, d'autorisation et de gestion des privilèges avec Microsoft Entra ID
- Mettre en oeuvre la protection des secrets, des données et des ressources Azure avec Azure Key Vault, Azure Policy et les contrôles de sécurité natifs
- Sécuriser les réseaux, bases de données, machines virtuelles, conteneurs et services applicatifs Azure
- Appliquer des contrôles de sécurité adaptés aux charges de travail et agents IA avec Microsoft Foundry, Microsoft Entra, Microsoft Agent 365, Microsoft Purview et Microsoft Defender
- Analyser et améliorer la posture de sécurité d'environnements Azure, hybrides et multicloud avec Microsoft Defender for Cloud
- Collecter, analyser et automatiser le traitement des événements de sécurité avec Microsoft Sentinel
- Exploiter Microsoft Security Copilot et ses agents pour accompagner les activités d'analyse et d'administration de la sécurité

Prérequis

- Disposer d'une expérience pratique de l'administration Microsoft Azure et d'environnements hybrides, notamment sur les services de calcul, de réseau et de stockage
- Maîtriser les principes de gestion des identités et des accès avec Microsoft Entra ID
- Connaître les fondamentaux de l'administration Microsoft 365
- Des connaissances générales en sécurité Cloud, RBAC et réseau IP sont recommandées

Certification

Cette formation prépare au passage à l'examen SC-500 Implementing End-to-End Security Controls for Cloud and AI Workloads qui permet d'obtenir la certification Microsoft Certified: Cloud and AI Security Engineer Associate.

Public concerné

Ingénieurs sécurité, ingénieurs Cloud Security, administrateurs Azure expérimentés et professionnels de l'infrastructure Cloud ayant la responsabilité de sécuriser des environnements Azure, hybrides ou intégrant des charges de travail IA.
Bénéfices pour les participants :

- Disposer d'une vision cohérente de la sécurisation d'un environnement Azure de bout en bout
- Renforcer la protection des identités, privilèges, secrets et données sensibles
- Réduire l'exposition des ressources Cloud grâce aux mécanismes d'isolation réseau et de contrôle des accès
- Intégrer la sécurité aux charges de travail IA et à la gouvernance des agents
- Exploiter les capacités de Microsoft Defender for Cloud pour identifier et hiérarchiser les risques
- Centraliser les événements de sécurité et automatiser certaines opérations avec Microsoft Sentinel
- Intégrer Microsoft Security Copilot aux activités quotidiennes des équipes de sécurité

Programme détaillé

Sécuriser l'accès aux ressources à l'aide de Microsoft Entra (1h20)

- Gérer et implémenter des méthodes d'authentification dans Microsoft Entra ID
  - Explorer les méthodes d'authentification Microsoft Entra ID
  - Configurer l'authentification multifacteur dans l'ID Microsoft Entra
  - Implémenter l'authentification sans mot de passe dans l'ID Microsoft Entra
  - Configurer la réinitialisation de mot de passe en libre-service dans l'ID Microsoft Entra
  - Travail pratique : Configurer des méthodes d'authentification dans l'ID Microsoft Entra
- Implémenter et configurer Privileged Identity Management (PIM)
  - Pourquoi Privileged Identity Management et l'accès juste-à-temps (JIT) sont importants
  - Fonctionnalités principales de Privileged Identity Management (PIM)
  - Implémenter l'accès JIT pour les rôles Microsoft Entra
  - Implémenter un accès JIT pour les rôles et ressources Azure
  - Mise à l'échelle avec PIM pour les groupes
  - Application de l'accès JIT aux charges de travail, agents et applications IA
  - Modèles de conception JIT et bonnes pratiques
- Authentifier votre plug-in d'API pour les agents déclaratifs avec des API sécurisées
  - Intégrer un plug-in d'API à une API sécurisée avec une clé
  - Travail pratique : Intégrer un plug-in d'API à une API sécurisée avec une clé
  - Intégrer un plug-in d'API à une API sécurisée avec OAuth
  - Travail pratique : Intégrer un plug-in d'API à une API sécurisée avec OAuth

Sécuriser Azure Key Vault avec la défense en profondeur pour les charges de travail Cloud et IA (1h40)

- Configurer et sécuriser les Azure Key Vault
  - Déployer Azure Key Vault avec des contrôles de sécurité
  - Configurer l'accès à Azure Key Vault
  - Configurer Key Vault paramètres de pare-feu et de réseau
- Gérer les clés et les secrets dans Azure Key Vault
  - Gérer les clés de chiffrement dans Azure Key Vault
  - Gérer les secrets dans Azure Key Vault
- Gérer les certificats et surveiller les Azure Key Vault
  - Gérer les certificats dans Azure Key Vault
  - Activer la journalisation d'audit pour Key Vault
- Protéger Azure Key Vault avec Microsoft Defender for Cloud
  - Analyser les secrets exposés à l'aide de Defender Cloud Security Posture Management (CSPM)
  - Activer Microsoft Defender pour Key Vault
  - Examiner et répondre aux alertes de Defender pour Key Vault

Appliquer la gouvernance de la sécurité et la conformité réglementaire (2h10)

- Appliquer la gouvernance avec des Azure Policy et des verrous de ressources
  - Attribuer des définitions de Azure Policy intégrées
  - Créer et déployer des définitions de stratégie personnalisées
  - Implémenter des verrous de ressources
- Configurer les contrôles de sécurité et corriger les recommandations dans Defender for Cloud
  - Configurer Defender for Cloud et gérer les normes de sécurité
  - Déployer des contrôles de correction à grande échelle
- Evaluer la conformité réglementaire dans Defender for Cloud
  - Comprendre les normes et les contrôles de conformité dans Defender for Cloud
  - Naviguer dans le tableau de bord de conformité réglementaire et examiner les lacunes de contrôle
  - Affecter des normes et communiquer la posture de conformité
- Gérer et dimensionner correctement les attributions de rôles RBAC selon le principe du moindre privilège
  - Attribuer et gérer des rôles intégrés Azure
  - Créer des rôles Azure personnalisés et des rôles de Microsoft Entra
  - Évaluer et corriger l'accès privilégié
- Protéger les données de sauvegarde avec des fonctionnalités de sécurité Sauvegarde Azure
  - Activer la suppression douce et les voûtes immuables
  - Configurer l'autorisation multi-utilisateur et RBAC pour la sauvegarde
- Implémenter des contrôles de sécurité dans l'infrastructure en tant que code
  - Analyser des modèles IaC à l'aide de Microsoft Defender pour DevOps
  - Assurer la conformité aux politiques dans les déploiements IaC

Implémenter la sécurité pour le stockage Azure (1h30)

- Décrire les services de stockage Azure
  - Décrire les comptes de stockage Azure
  - Décrire la redondance du stockage Azure
  - Décrire les services de stockage Azure
  - Identifier les options de migration des données Azure
  - Identifier les options de déplacement de fichiers Azure
- Implémenter la sécurité et gérer l'accès pour le stockage Azure
  - Configurer les paramètres de sécurité du compte de stockage
  - Sélectionner un modèle d'autorisation pour le stockage Azure
  - Gérer l'accès avec des stratégies d'accès stockées
  - Désactiver l'autorisation par clé partagée et l'imposer via Azure Policy

- Configurer la sécurité réseau pour le stockage Azure
  - Décrire les contrôles de sécurité réseau du stockage Azure
  - Configurer des règles de réseau virtuel et d'adresse IP
  - Configurer des règles d'instance de ressource et des services approuvés
  - Implémenter des points de terminaison privés pour les comptes de stockage
- Implémenter Microsoft Defender pour le stockage
  - Explorer Microsoft Defender pour les fonctionnalités de stockage
  - Activer et déployer Defender pour le stockage
  - Configurer l'analyse des programmes malveillants et la détection des données sensibles
  - Configurer le routage des alertes et valider la couverture Defender

Implémenter la sécurité pour les bases de données Azure SQL (0h50)

- Configurer la sécurité au niveau de la plateforme pour Azure SQL
  - Configurer l'authentification et l'accès aux identités managées
  - Implémenter l'isolement réseau
  - Chiffrer et protéger les données en transit et au repos
  - Appliquer le masquage des données et la sécurité au niveau des lignes
- Configurer l'audit pour Azure SQL Database et SQL Managed Instance
  - Décrire les fonctionnalités d'audit Azure SQL
  - Configurer des destinations d'audit pour Azure SQL Database
  - Configurer l'audit pour SQL Managed Instance
  - Concevoir une stratégie d'audit conforme
- Implémenter Microsoft Defender pour les bases de données
  - Explorer Microsoft Defender pour les fonctionnalités des bases de données
  - Activer Defender pour les bases de données Azure SQL au niveau de l'étendue de l'abonnement
  - Activer Defender pour les bases de données relationnelles open source
  - Configurer l'évaluation des vulnérabilités
  - Configurer le routage des alertes et valider la couverture

Implémenter des contrôles de sécurité réseau dans Azure (2h50)

- Segmenter et isoler les charges de travail Azure à l'aide de contrôles de sécurité réseau
  - Évaluer les lacunes de segmentation du réseau
  - Contrôler le trafic avec des groupes de sécurité réseau (NSG)
  - Simplifier la gestion des règles avec des groupes de sécurité d'application
  - Appliquer une stratégie cohérente avec Azure Virtual Network Manager
  - Vérifier les règles de sécurité réseau effectives avec Network Watcher
- Centraliser et appliquer l'inspection du trafic à l'aide de Pare-feu Azure
  - Déterminer quand l'inspection centralisée du trafic est requise
  - Configurer des règles et des stratégies Pare-feu Azure
  - Sécuriser un hub Virtual WAN avec Pare-feu Azure
- Sécuriser la connectivité distante et hybride à l'aide de passerelles VPN et de Accès privé Microsoft Entra
  - Évaluer les risques de sécurité dans la connectivité hybride
  - Renforcer la sécurité de la passerelle VPN
  - Remplacez l'accès VPN étendu par Accès privé Microsoft Entra
- Eliminer l'exposition du réseau public aux services PaaS Azure
  - Évaluer le risque d'exposition des points de terminaison PaaS publics
  - Configurer des points de terminaison privés pour éliminer l'exposition PaaS publique
  - Exposer des services internes en toute sécurité à l'aide du service Azure Private Link
  - Appliquer et auditer l'adoption du point de terminaison privé

Implémenter la sécurité pour l'IA (3h50)

- Accès sécurisé pour l'Identité de l'agent Microsoft Entra
  - Mapper les flux d'authentification et l'étendue d'accès conditionnel
  - Configurer des stratégies d'accès conditionnel pour les agents
  - Contrôler l'accès et le cycle de vie d'un agent
- Analyser les risques liés aux identités IA à l'aide de Microsoft Defender XDR
  - Découvrir des agents IA dans le portail Microsoft Defender
  - Évaluer le rayon d'explosion et les chemins d'attaque
- Activer la protection en temps réel pour les agents Copilot Studio
  - Explorer la protection de l'agent IA de Copilot Studio
  - Activer la protection dans Microsoft Defender
  - Passer en revue les résultats de protection de l'agent d'IA
- Configurer la sécurité de la passerelle AI dans Microsoft Foundry
  - Examiner l'architecture de la passerelle IA
  - Créer et configurer une passerelle AI
  - Sécuriser et surveiller l'accès à la passerelle IA
- Configurer et gérer des garde-fous dans Microsoft Foundry
  - Comprendre les garde-fous et la sécurité du contenu Microsoft
  - Comprendre les contrôles de sécurité dans Microsoft Foundry
  - Essayer des garde-fous intégrés
  - Créer et gérer des listes de blocs dans Microsoft Foundry
  - Configurer et appliquer des garde-fous dans Microsoft Foundry
  - Choisir et affiner les garde-fous appropriés pour vos charges de travail d'IA
- Protéger les charges de travail IA avec Microsoft Defender for Cloud
  - Activer le plan des charges de travail IA

- Passer en revue les insights dans le tableau de bord de sécurité des données et de l'IA
- Évaluer et améliorer la posture de sécurité de l'IA avec Cloud Security Posture Management (CSPM)
- Détecter les menaces IA lors de l'exécution avec Cloud Workload Protection (CWP)
- Examiner les alertes de sécurité IA avec des preuves rapides dans Microsoft Defender XDR

• Activer Defender pour les services d'IA protection des charges de travail dans Microsoft Defender for Cloud
- Activer et configurer le plan de Defender pour les services d'IA
- Surveiller la sécurité de l'IA avec le tableau de bord Données et IA

• Gérer les agents à l'aide de Microsoft Agent 365
- Activer et naviguer dans Microsoft Agent 365
- Inscrire des agents et appliquer des contrôles d'accès
- Surveiller l'activité de l'agent et appliquer la gouvernance

• Identifier les risques liés aux données IA à l'aide de Gestion de la posture de sécurité des données Microsoft Purview
- Configurer la gestion de la posture de sécurité des données (DSPM) pour l'IA
- Évaluer la surexploitation de SharePoint
- Identifier les risques liés aux interactions entre les applications Copilot et l'IA

Implémenter la sécurité pour les serveurs et les machines virtuelles (2h50)

• Implémenter le chiffrement de disque pour les machines virtuelles Azure
- Choisir l'option de chiffrement de disque appropriée pour les machines virtuelles Azure
- Configurer le chiffrement sur l'hôte avec des clés gérées par le client
- Appliquer le chiffrement de disque confidentiel aux machines virtuelles confidentielles

• Configurer les fonctionnalités de sécurité de lancement approuvées pour les machines virtuelles Azure
- Identifier les composants de lancement approuvé et les types de sécurité de machine virtuelle
- Activer le lancement approuvé sur les machines virtuelles Gen2 nouvelles et existantes
- Migrer des machines virtuelles Gen1 et configurer des composants de lancement approuvé
- Imposer l'adoption de Trusted Launch avec Azure Policy

• Planifier et implémenter Azure Bastion
- Planifier le déploiement de Azure Bastion
- Déployer et configurer Azure Bastion
- Se connecter à des machines virtuelles via Azure Bastion

• Gérer la sécurité des serveurs hybrides avec Arc
- Contrôler l'accès et la sécurité des extensions pour les serveurs avec Arc
- Appliquer Azure Policy aux serveurs avec Arc
- Surveiller la posture de sécurité du serveur Arc dans Defender for Cloud

• Implémenter Microsoft Defender pour les serveurs
- Intégrer des serveurs à Defender for Servers
- Configurer l'analyse des vulnérabilités avec Defender Vulnerability Management
- Configurer Defender pour l'intégration des points de terminaison, l'analyse sans agent et la surveillance de l'intégrité des fichiers

• Activer et appliquer l'accès juste-à-temps (JIT) aux machines virtuelles
- Examiner les exigences d'accès JIT aux machines virtuelles et l'éligibilité des machines virtuelles
- Activer et configurer des stratégies d'accès JIT
- Demander l'accès JIT et auditer les activités d'accès

• Appliquer la configuration de sécurité des machines virtuelles avec Azure Machine Configuration
- Explorer les capacités et modes d'extension d'Azure Machine Configuration
- Appliquer des stratégies de base de référence de sécurité intégrées
- Créer et affecter des configurations d'ordinateur personnalisées

Sécuriser les services de plateforme d'applications Azure (2h50)

• Détecter les risques liés aux conteneurs à l'aide de Microsoft Defender for Containers
- Explorer Microsoft Defender for Containers
- Activer et configurer Defender for Containers
- Évaluer les vulnérabilités d'image conteneur
- Détecter les menaces et les erreurs de configuration du runtime de conteneur

• Implémenter des contrôles de sécurité pour Azure Kubernetes Service (AKS)
- Contrôler l'accès au cluster AKS avec Microsoft Entra ID et RBAC
- Sécuriser l'accès réseau AKS
- Implémenter l'identité de charge de travail et la gestion des secrets pour AKS
- Appliquer des règles de sécurité aux pods et aux conteneurs

• Implémenter des contrôles de sécurité pour Azure Container Registry, Container Instances et Container Apps
- Sécuriser les Azure Container Registry
- Implémenter des contrôles de sécurité pour Azure Container Instances
- Implémenter des contrôles de sécurité pour Azure Container Apps

• Implémenter des contrôles de sécurité pour les applications

Azure Function et Logic
- Configurer l'authentification et l'autorisation pour les applications Azure Function
- Sécuriser l'accès réseau pour les applications Azure Function
- Implémenter des contrôles de sécurité pour les applications Azure Logic

- Implémenter des contrôles de sécurité pour Azure App Services et Web Application Firewall
  - Implémenter des contrôles de sécurité pour Azure App Service
  - Configurer des stratégies de Web Application Firewall
  - Protéger App Service avec Web Application Firewall
- Implémenter la sécurité du back-end d'API à l'aide de Gestion des API Azure
  - Configurer les stratégies d'authentification et d'autorisation de l'API
  - Implémenter la sécurité réseau de l'API et la protection contre les menaces
  - Gestion sécurisée des connexions backend d'API
  - Configurer la passerelle AI dans Gestion des API pour Azure AI Foundry

Gérer la posture de sécurité en utilisant Microsoft Defender pour le Cloud (3h20)

- Connecter des environnements hybrides et multiclouds à Microsoft Defender for Cloud
  - Explorer le modèle de connectivité multicloud de Defender for Cloud
  - Planifier une stratégie de connecteur pour les environnements hybrides et multiclouds
  - Connecter des machines locales à l'aide de Azure Arc
  - Connecter des comptes AWS à Defender for Cloud
  - Connecter des projets GCP à Defender for Cloud
  - Vérifier la couverture multicloud et valider la protection
- Identifier les risques de sécurité à l'aide de la gestion de la posture de sécurité cloud
  - Explorer les plans CSPM et la visibilité de la posture
  - Analyser les recommandations de sécurité avec la hiérarchisation des risques
  - Identifier les chemins d'attaque et les points d'étranglement
  - Rechercher les risques avec Cloud Security Explorer
- Découvrir des ressources et des vulnérabilités non protégées à l'aide de Microsoft Defender External Attack Surface Management (EASM)
  - Explorer les caractéristiques et fonctionnalités d'EASM
  - Découvrir des ressources à l'aide de la découverte récursive
  - Analyser votre surface d'attaque avec des tableaux de bord
  - Intégrer EASM Insights à Defender for Cloud
- Evaluer la conformité réglementaire dans Defender for Cloud
  - Comprendre les normes et les contrôles de conformité dans Defender for Cloud
  - Naviguer dans le tableau de bord de conformité réglementaire et examiner les lacunes de contrôle
  - Affecter des normes et communiquer la posture de conformité
- Activer et configurer des plans de protection des charges de travail dans Microsoft Defender for Cloud
  - Comprendre le catalogue de plans Defender for Cloud CWPP

paramètres d'environnement
- Configurer Defender pour le stockage et Defender pour les bases de données
- Déployer des plans à grande échelle et vérifier la couverture

- Configurer les paramètres de Microsoft Defender Vulnerability Management (MDVM) pour les machines virtuelles Azure
  - Explorer l'intégration de Gestion des vulnérabilités Microsoft Defender (MDVM) à Defender for Servers
  - Configurer l'analyse des vulnérabilités pour les machines virtuelles Azure
  - Examiner et gérer les résultats des vulnérabilités
  - Appliquer les fonctionnalités premium du Plan 2 MDVM

Implémenter l'activité et la collecte d'événements dans Microsoft Sentinel (3h20)

- Créer et gérer des espaces de travail Microsoft Sentinel
  - Organisation de l'espace de travail Microsoft Sentinel
  - Créer un espace de travail Microsoft Sentinel
  - Gérer les espaces de travail parmi les locataires avec Azure Lighthouse
  - Présentation des autorisations et des rôles Microsoft Sentinel
  - Gestion des paramètres Microsoft Sentinel
  - Configurer les journaux
- Gérer le contenu dans Microsoft Sentinel
  - Utiliser des solutions à partir du hub de contenu
  - Utiliser des dépôts pour le déploiement
- Connecter les services Microsoft à Microsoft Sentinel
  - Planifier les connecteurs de services Microsoft
  - Connecter le connecteur Microsoft 365
  - Connecter le connecteur Microsoft Entra
  - Connecter le connecteur Microsoft Entra ID Protection
  - Se connecter au connecteur Azure Activity
- Connecter des sources de données Syslog à Microsoft Sentinel
  - Planifier la collecte des données Syslog
  - Collecter des données à partir de sources Linux à l'aide de Syslog
  - Configurer la règle de collecte de données pour les sources de données Syslog
  - Analyser les données Syslog avec KQL
- Connecter des journaux Common Event Format (CEF) à Microsoft Sentinel
  - Planifier un connecteur pour CEF
  - Connectez votre solution externe en utilisant le connecteur CEF
- Connecter des hôtes Windows à Microsoft Sentinel
  - Planifier le connecteur pour les événements de sécurité des hôtes Windows
  - Se connecter en utilisant le connecteur Événements de sécurité Windows via AMA
  - Se connecter en utilisant le connecteur Événements de sécurité via l'agent hérité
  - Collecter les journaux des événements Sysmon
- Implémenter des règles d'automatisation et des playbooks dans Microsoft Sentinel
  - Comprendre les options d'automatisation Microsoft Sentinel
  - Créer des règles d'automatisation dans Microsoft Sentinel
  - Configurer et activer un playbook de Content Hub
  - Créer un playbook personnalisé avec Azure Logic Apps
- Gérer le stockage des données et interroger les journaux d'audit dans Microsoft Sentinel

Implémenter la rétention des données dans Microsoft Sentinel
- Connecter Microsoft Purview Audit à Microsoft Sentinel
- Interroger les journaux d'audit Purview dans Microsoft Defender XDR

Déployer et exploiter Microsoft Security Copilot (1h30)

- Décrire le Microsoft Security Copilot
  - Décrire la terminologie de Microsoft Security Copilot
  - Décrire comment Microsoft Security Copilot traite les demandes faites par prompt
  - Décrire les éléments d'un prompt efficace
  - Décrire comment activer Microsoft Security Copilot
- Configurer des espaces de travail pour Microsoft Security Copilot
  - Planifier un déploiement d'espace de travail
  - Créer un espace de travail Security Copilot
  - Configurer l'accès et les paramètres de l'espace de travail
  - Affecter des espaces de travail pour les agents intégrés
  - Surveiller et gérer la capacité de l'espace de travail
- Gérer les plug-ins et les agents dans Microsoft Security Copilot
  - Configurer les paramètres du plug-in dans Security Copilot
  - Découvrir et configurer des agents intégrés Microsoft
  - Acquérir et configurer des agents partenaires à partir du Magasin de sécurité
  - Gérer les agents Security Copilot

Documentation

Travaux pratiques et/ou Labo en anglais

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation