03 20 61 95 06
formation@access-it.fr

Formation Cloudflare - Sécurité et gestion des menaces

Durée de la formation : 5 jour(s) / 35 heure(s)

OBJECTIFS

À l'issue de cette formation de 5 jours, les participants seront capables de comprendre l'architecture et les avantages de Cloudflare, configurer les services de base (DNS, SSL/TLS, cache), mettre en place des protections contre les menaces classiques (WAF, DDoS) et avancées (injections, XSS, bots, API), développer des règles personnalisées via Cloudflare Workers, analyser les métriques et les logs pour assurer la surveillance et les alertes, conduire une réponse efficace aux incidents, adapter les configurations à des contextes réels (e-commerce, SaaS), et valider le tout à travers des tests pratiques et un QCM final avec un seuil de réussite à 80 %.

PREREQUIS

Un entretien en amont avec notre expert permet de prendre en compte le profil de chaque participant (niveau, objectifs et résultats attendus, contexte professionnel, enjeux...) et d'adapter le contenu de la formation si besoin. Cette formation ne peut être financée que dans le cadre d'un projet d'entreprise (prise en charge entreprise ou OPCO). Les dossiers à financement personnel et CPF ne sont pas pris en compte.

CONNAISSANCES :

- Bases des réseaux (DNS, HTTP/HTTPS)
- Notions de sécurité web (optionnel, sera revu)
- Utilisation d'un navigateur web et d'interfaces d'admin

MATÉRIEL :

- Ordinateur avec accès internet
- Navigateur moderne (Chrome, Firefox)
- Possibilité d'installer extensions navigateur
- Compte email pour notifications

PUBLIC

Professionnels intervenant sur sites clients (niveaux mixtes)

03 20 61 95 06
formation@access-it.fr

Formation Cloudflare - Sécurité et gestion des menaces

Durée de la formation : 5 jour(s) / 35 heure(s)

PROGRAMME

JOUR 1 - FONDAMENTAUX ET MISE EN PLACE (7h)

MODULE 1.1 : Introduction à Cloudflare (2h)
• Qu'est-ce que Cloudflare et pourquoi l'utiliser
• Architecture et fonctionnement du CDN/WAF
• Types de comptes et plans disponibles
• Interface d'administration : tour d'horizon
• Différences avec les autres solutions (AWS CloudFront, Azure CDN)
Pause (15min)
MODULE 1.2 : Configuration de base (2h30)
• Création et configuration d'un compte
• Ajout d'un domaine (DNS setup)
• Configuration SSL/TLS (modes et certificats)
• Paramètres de base du cache
• Configuration des redirections
Pause Déjeuner (2h)
MODULE 1.3 : DNS et réseau (2h)
• Gestion DNS avancée dans Cloudflare
• Types d'enregistrements et bonnes pratiques
• Load Balancing et Health Checks
• Géolocalisation et restrictions par pays
• Exercice pratique : Configuration complète d'un site
ÉVALUATION JOUR 1 : QCM (15min)

JOUR 2 - SÉCURITÉ DE BASE ET WAF (7h)

MODULE 2.1 : Web Application Firewall (WAF) (2h30)
• Principe de fonctionnement du WAF Cloudflare
• Règles prédéfinies vs règles personnalisées
• Managed Rules et OWASP Core Rule Set
• Configuration et personnalisation
• Modes : Block, Challenge, Log, Allow
Pause (15min)
MODULE 2.2 : Protection DDoS (2h)
• Types d'attaques DDoS (L3/L4, L7)
• Protection automatique Cloudflare
• Rate Limiting et configuration
• Challenge pages et JS Challenge
• Exercice : Simulation d'attaque DDoS
Pause Déjeuner (2h)
MODULE 2.3 : Première approche des menaces (2h)
• Détection des menaces courantes
• Lecture des logs de sécurité
• Tableau de bord Security Events
• Actions à prendre selon les types d'alertes
• Exercice pratique : Analyse de logs d'attaque
ÉVALUATION JOUR 2 : QCM + Exercice pratique (15min)

JOUR 3 - MENACES AVANCÉES ET DÉTECTION (7h)

03 20 61 95 06
formation@access-it.fr

Formation Cloudflare - Sécurité et gestion des menaces

Durée de la formation : 5 jour(s) / 35 heure(s)

MODULE 3.1 : Injection et XSS (2h30)
• Comprendre les attaques par injection SQL
• Cross-Site Scripting (XSS) : types et détection
• Configuration WAF pour bloquer les injections
• Règles personnalisées anti-injection
• Exercice : Créer des Workers pour tester les vulnérabilités
Pause (15min)
MODULE 3.2 : Attaques applicatives avancées (2h)
• CSRF, XXE, et autres vulnérabilités OWASP
• Bot Management et détection de bots malveillants
• API Security et protection des endpoints
• Content Security Policy (CSP) via Headers
• Exercice : Configuration anti-bot avancée
Pause Déjeuner (2h)
MODULE 3.3 : Workers et sécurité personnalisée (2h)
• Introduction aux Cloudflare Workers
• Création de règles de sécurité personnalisées
• Workers pour la détection de menaces
• Intégration avec des API externes
• Exercice : Développer un Worker de sécurité
ÉVALUATION JOUR 3 : Exercice pratique Workers (15min)

JOUR 4 - ANALYSE ET MONITORING (7h)

MODULE 4.1 : Analytics et monitoring (2h30)
• Dashboard Analytics : lecture et interprétation
• Métriques de performance vs sécurité
• Security Events : analyse approfondie
• Configurtion d'alertes personnalisées
• Integration avec outils externes (Slack, email)
Pause (15min)
MODULE 4.2 : Logs et forensics (2h)
• Export et analyse des logs Cloudflare
• Enterprise Logs vs logs gratuits
• Outils d'analyse (Log Explorer, API)
• Corrélation d'événements de sécurité
• Exercice : Investigation d'incident
Pause Déjeuner (2h)
MODULE 4.3 : Response et mitigation (2h)
• Procédures de réponse aux incidents
• Escalade et communication client
• Mesures d'urgence et blocages temporaires
• Documentation des incidents
• Exercice : Simulation d'incident complet
ÉVALUATION JOUR 4 : Cas pratique d'analyse (15min)

JOUR 5 - SCÉNARIOS RÉELS (7h)

MODULE 5.1 : Cas clients e-commerce (2h)
• Spécificités sécurité e-commerce
• Protection des données de paiement

03 20 61 95 06
formation@access-it.fr

Formation Cloudflare - Sécurité et gestion des menaces

Durée de la formation : 5 jour(s) / 35 heure(s)

• Gestion du trafic en période de pointe
• Configuration pour sites à fort trafic
• Exercice : Configuration e-commerce complète
Pause (15min)
MODULE 5.2 : Cas clients corporate/SaaS (2h)
• Sécurité des applications métier
• Zero Trust et accès utilisateurs
• API Protection avancée
• Conformité et audit trails
• Exercice : Setup corporate avec Zero Trust
Pause Déjeuner (2h)
MODULE 5.3 : Tests de pénétration et validation (1h30)
• Méthodologie de test de la configuration
• Outils pour valider la sécurité
• Tests d'intrusion contrôlés
• Rapport de sécurité client
MODULE 5.4 : Révisions (1h)
• Révision des points clés
• Questions/Réponses
• **QCM final (45min)**

RESSOURCES ET OUTILS FOURNIS

DOMAINE DE TEST :
• 1 domaine fourni par le formateur pour exercices
• Scripts Workers d'exemple pour tests
SUPPORTS PÉDAGOGIQUES :
• Présentations PowerPoint par module
• Guides pratiques étape par étape
• Check-lists de sécurité
EXERCICES PRATIQUES :
• 15+ exercices hands-on
• Simulations d'attaques DDoS
• Tests XSS et injection SQL
• Développement Workers sécurité
• Cas réels anonymisés
ÉVALUATION :
• QCM quotidiens (20 questions/jour)
• Exercices pratiques notés
• QCM final (100 questions)
• Seuil de réussite : 80%

03 20 61 95 06
formation@access-it.fr

Formation Cloudflare - Sécurité et gestion des menaces

Durée de la formation : 5 jour(s) / 35 heure(s)

Prise en compte du handicap
Pour les personnes en situation de handicap, afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous via notre formulaire de contact ou par mail (formation@access-it.fr) ou par téléphone (0320619506). Un entretien avec notre référente handicap pourra être programmé afin d'identifier les besoins et aménagements nécessaires.

Modalités et moyens Pédagogiques, techniques et d'encadrement mis en œuvre
Répartition théorie/pratique : 45%/55%. Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques s'articulant autour d'une application fil rouge, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
Formation accessible à distance de n'importe où et n'importe quand, via un ordinateur type PC disposant d'une connexion à Internet à haut débit (ADSL ou plus).
Pour assurer un démarrage dans les meilleures conditions au premier jour de la formation, notre service logistique se met systématiquement en relation, en amont, avec vous afin de réaliser un test de validation technique et de vous présenter l'environnement de formation.
Pendant toute la durée de la formation, le stagiaire dispose d'une assistance technique et pédagogique illimitée, par e-mail, avec un délai de prise en compte et de traitement qui n'excède pas 24h. En complément, le stagiaire peut planifier un rendez-vous pédagogique avec un formateur expert afin d'échanger sur des éléments de la formation.
La durée de la formation affichée sur cette page est une durée estimée qui peut varier en fonction du profil du stagiaire et de ses objectifs (notamment s'il souhaite valider sa formation par le passage d'un examen de certification).
Durant la formation, le formateur prévoit :
Des démonstrations organisées en modules et en séquences découpées le plus finement possible, en suivant le programme pédagogique détaillé sur cette page ;
Des énoncés et corrigés de travaux pratiques à réaliser tout au long de la formation ;
Des travaux pratiques sont proposés ; la plateforme prévoit l'environnement technique nécessaire à la réalisation de l'ensemble des travaux pratiques ;
Le formateur valide les connaissances acquises après chaque TP ;
Il est proposé un ou plusieurs livres numériques faisant office d'ouvrage(s) de référence sur le thème de la formation.

Validation et sanction de la formation
Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation par courrier électronique.
A la demande, il sera délivré un certificat de réalisation.

Type de formation
Professionnalisante ayant pour objectif le perfectionnement, l'élargissement des compétences

Moyens permettant de suivre l'exécution de l'action
Le contrôle de la présence des stagiaires sera assuré par la vérification de l'assiduité des participants. Le stagiaire signera une feuille de présence par demi-journée de formation. Celle-ci sera également signée par le formateur.

Modalité d'évaluation des acquis
Durant la formation, le participant est amené à mettre en pratique les éléments du cours par la réalisation de travaux pratiques réalisés sur PC.
La validation des acquis du stagiaire est faite par le formateur à la fin de chaque atelier. Cette validation individuelle est possible du fait du faible nombre de participants par session de formation (6 personnes maximum).
A la fin de la formation, le stagiaire a donc atteint les objectifs fixés par la formation.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par l'éditeur en passant un examen de certification.
Access it étant centre d'examen ENI, les examens peuvent être réalisés sur demande à distance ou dans nos locaux de Villeneuve d'Ascq.
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

Assistance Post-Formation
Toute personne ayant suivi une formation avec Access it bénéficie d'une assistance post-formation d'une durée de 1 mois. Ce nouveau service d'accompagnement permet aux stagiaires rencontrant des difficultés dans la mise en oeuvre des connaissances acquises de solliciter l'aide de nos formateurs sur des aspects relatifs aux programmes de formation suivis. Pour en bénéficier, il suffit de se rendre sur la page contact de notre site web et de remplir le formulaire. Une réponse est apportée par mail ou par téléphone dans un délai de 48 heures.

Centre d'Examen
Notre centre de formation agréé Qualiopi bénéficie de l'agrément d'ENI et ICDL pour les certifications informatiques. C'est pour nos clients la garantie de pouvoir suivre des formations préparant à des certifications professionnelles.

Aide à l'orientation
Pour chacune des grandes thématiques couvertes par notre offre de formation, nous proposons via nos spécialistes un rendez-vous physique ou téléphonique qui via un diagnostic permettra aux personnes souhaitant être accompagnées dans le choix d'un programme ou dans la définition d'un parcours de formation une orientation vers les programmes les plus adaptés à leurs besoins et à leur niveau.

Aspects Pratiques
Dès leur inscription, les participants sont contactés par nos services qui s'assurent que les débits internet constatés sur le lieu depuis lequel ils souhaitent se former sont suffisants pour suivre la formation dans des conditions optimales.
À l'occasion de cet appel, nos experts s'assurent également qu'ils disposent du matériel nécessaire pour suivre la formation (PC Portable, webcam, Micro-casque..).
Avant le début de la formation, les participants reçoivent un lien leur permettant d'accéder à la classe virtuelle et leurs identifiants personnels de connexion. Un aide à l'utilisation de la solution de visioconférence utilisée leur est également proposée.
Le jour de la formation, ils se connectent à la classe virtuelle depuis leur navigateur internet. Ils voient et entendent le formateur ainsi que les autres participants et peuvent à tout moment communiquer avec eux.
Ils participent aux échanges et réalisent les ateliers dans les mêmes conditions que s'ils étaient en salle. Grâce à nos outils de prise en main à distance, les formateurs peuvent à tout moment prendre la main sur leurs postes pour les aider ou vérifier leurs TP.
Tout au long de la formation, les participants peuvent bénéficier de l'assistance immédiate de nos experts en composant le numéro qui leur a été communiqué avant la formation.
Des bilans intermédiaires ont lieu en présence des participants du formateur et du référent pédagogique d'Access it afin de vérifier l'état d'avancement de la session, les difficultés rencontrées et permettre d'éventuels actions correctives.

Bénéfices pour les participants
Se former depuis leur lieu de travail ou leur domicile,
Accéder sans se déplacer à la qualité d'une formation délivrée par un formateur consultant ayant une expérience probante sur le sujet animé.
Bénéficier à distance de la richesse d'une formation interentreprises : échanges avec le formateur et les autres participants, partages d'expériences, ateliers pratiques…
Pouvoir se former en toutes circonstances et notamment en cas d'imprévus.

Bénéfices pour l'entreprise
Optimiser ses budgets en limitant les frais de déplacement et d'hébergement.
Proposer à tous ses collaborateurs, quelle que soit leur situation géographique, des formations de qualité (en Inter comme en Intra).
Limiter les temps de déplacement.
Proposer davantage de choix dans les formations à des collaborateurs peu mobiles.
Assurer la montée en compétences de ses collaborateurs quelles que soient les circonstances