CATALOGUE

APPLICATION SECURITY
CATALOGUE DES
FORMATIONS 2024

UBIKA

SOMMAIRE

UBIKA propose à ses clients et partenaires un choix de formations certifiantes couvrant l'ensemble du cycle de mise en œuvre de ses produits Application Security.

Que la mise en œuvre soit assurée par le client lui-même, par un partenaire, ou par UBIKA, il est essentiel que les ingénieurs mettant en œuvre ou exploitant les solutions soient formés et disposent d'un niveau technique suffisant pour assurer une sécurité efficace des applications et services web.

L'ensemble des formations sont animées par un membre de l'équipe professionnel services d'UBIKA, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications. Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés. Les dates indiquées se déroulent dans les locaux de UBIKA SAS à Meudon. Pour répondre aux besoins spécifiques de certains projets, nous proposons également des sessions de formation intra-entreprise personnalisées en fonction des contraintes ainsi que des formations de type e-learning. Enfin, il est possible, sous certaines conditions, de définir un programme dit « custom » sur un périmètre précis et un temps déterminé.

1. Planning

	UBIKA WAAP Gateway	Expert UBIKA WAAP Gateway	Extended API Security	Web Access Manager
Durée	3 jours	3 jours	2 jours	2 jours
Janvier	9-11	-	-	-
Février	12-14 à distance	6-8	20-21	22-23
Mars	12-14	-	-	-
Avril	8-10	-	-	-
Mai	-	14-16	-	-
Juin	12-14	-	18-19	20-21
Juillet	3-5 à distance	-	-	-
Août	-	-	-	-
Septembre	10-12	17-19	-	-
Octobre	7-9 à distance	-	15-16	17-18
Novembre	13-15	-	-	-
Décembre	9-11 à distance	-	-	-

2.UBIKA WAAP Gateway

2.1 Détails de la formation

Durée	**3 jours (~21 heures)**
Audience	**Administrateur, Ingénieurs réseaux et sécurité, chef de projet, RSSI et tous ceux qui administrent régulièrement la solution UBIKA WAAP Gateway.**
Contenu	**50 % théorie / 50 % pratique**
Certification	**oui**

Cette formation se faisant avec la dernière version stable du produit UBIKA WAAP Gateway, son contenu est par conséquent régulièrement mis à jour afin d'y intégrer les dernières fonctionnalités et innovations.

En conséquence, l'agenda décrit ci-dessous peut être amené à être légèrement différent tout en gardant bien entendu les lignes directrices constituant les bases nécessaires à l'exploitation de la solution.

À l'issue de la formation, les participants seront capables de :

- Définir un WAF/WAAP et décrire son rôle dans une architecture sécurisée.
- Installation et configuration initiale de UBIKA WAAP Gateway.
- Décrire comment UBIKA WAAP Gateway protège une application web.
- Définir les paramètres d'apprentissage, d'alerte et de blocage avec le Workflow.
- Configurer le traitement des faux positifs dans une politique de sécurité.
- Déployer une politique de sécurité en utilisant l'apprentissage.
- Administrer la solution manuellement ou avec API.
- Configurer le mode de protection le plus adapté à une application Web.

2.2 AGENDA

Introduction (1h)
- Présentation globale
- Produits et intégration
- Support et espace client

HTTP (1h30)
- Bases HTTP
- Transactions importantes
- Concepts SSL
- Expressions régulières

Installation et configuration basique (2h)
- Basic Concepts •Installation
- Initialisation
- Configuration
- LAB

Gestion basique du workflow (2h30)
- Concept
- Les base du workflow
- Gestion du workflow
- LAB

Gestion avancée du workflow (3h)
- Politique de sécurité ICX
- Composants utiles
- LAB

Gestion avancée de la sécurité (2h)
- Fonctions de sécurité avancées
- Moteurs de sécurité avancée
- LAB

Gestion des faux positifs (2h)
- Concepts de base
- Résolution des faux positifs
- LAB

Haute disponibilité (1h)
- Concepts de base
- Configuration de la haute disponibilité
- LAB

Journalisation, alertes, rapports et surveillance (1h)
- Gestion des logs
- Alerte
- Management
- Reporting
- LAB

Configuration API (1h)
- Configuration
- LAB

Les bonnes pratiques (1h)
- Prérequis d'installation
- Configuration

Troubleshooting (1h)

Certification (2h)

3. Expert UBIKA WAAP Gateway

3.1 Détails de la formation

Durée	**3 jours (~21 heures)**
Audience	**Administrateur, Ingénieurs réseaux et sécurité, chef de projet, RSSI et tous ceux qui administrent régulièrement la solution UBIKAWAAP Gateway.**
Contenu	**50 % théorie / 50 % pratique**
Certification	**oui**

Cette formation se faisant avec la dernière version stable du produit UBIKA WAAP Gateway, son contenu est par conséquent régulièrement mis à jour afin d'y intégrer les dernières fonctionnalités et innovations.

En conséquence, l'agenda décrit ci-dessous peut être amené à être légèrement différent tout en gardant bien entendu les lignes directrices constituant les bases nécessaires à l'exploitation de la solution.

À l'issue de votre formation, les participants seront capables de :

- Utiliser des fonctionnalités avancées du produit (Foreach, Redis, Datastore, URL Mapping …).
- Optimiser la configuration des applications web avec les Workflows Parameters.
- Gérer des timeouts TCP et session SSL de bout en bout.
- Gérer des conteneurs de ressources statiques sur UBIKA WAAP Gateway.
- Publier et sécuriser une application de type Websocket.
- Mettre en œuvre du Load Balancing en amont et aval de la solution UBIKA WAAP Gateway.
- Configurer une authentification simple ou une pré authentification pour les applications.
- Permettre l'utilisation de base externe pour l'authentification des administrateurs sur UBIKA WAAP Gateway.

3.2 AGENDA

Introduction (1h)
- Agenda
- Lab setting

Performance (2h)
- Reverse proxy profile
- Timeout TCP
- Compression
- Caching
- Lab

Websocket (1h)
- Concept
- LAB

Workflow functions (2h)
- Concept
- LAB

Static Content Bundle (2h)
- Concept
- LAB

Foreach (1h)
- Concept
- LAB

Redis (1h)
- Concept
- LAB

Workflow Parameters (2h)
- Concept
- LAB

Datastore (1h)
- Concept
- LAB

URL Mapping (2h)
- Concept
- LAB

SSL advanced (2h)
- SSL Client Authentication
- Outgoing SSL
- Lab

Load Balancing (1h)
- Concept
- LAB

Basic Authentication (2h)
- WAM Perimeter Authentication Standalone
- LDAP Pre-authentication
- External Admin Authentication
- Lab

Antivirus (1h)
- Concept
- LAB

Certification (1h)

4.Extended API Security

4.2 AGENDA

- **Introduction (1h)**
  - Comment sécuriser un web service ?
  - Module EAS du WAAP UBIKA
- **Configuration du Lab (1h30)**
- **XML (6h)**
  - Parsing XML
  - Validation par schéma XML
  - Chiffrement et Déchiffrement XML
  - Signature XML
  - Modification XML
  - XPATH
- **JSON (3h)**
  - JSON to Table
  - Validation par schéma JSON
  - Filtrage ICX pour JSON
  - Attribut JSON
  - SITEMAP
- **JWT (2h)**
  - Génération de token JWT
  - Parsing JWT
- **QCM (1h)**

4.1 Détails de la formation

Durée	**2 jours (~14 heures)**
Audience	**Administrateur, Ingénieurs réseaux et sécurité, chef de projet et tous ceux qui administrent régulièrement la solution UBIKA WAAP Gateway.**
Contenu	**50 % théorie / 50 % pratique**
Certification	**non**

L'objectif de cette formation est l'obtention des connaissances et de l'expérience nécessaires pour mettre en place, maintenir, et diagnostiquer une sécurité portée sur les Web Services.

Cette formation se faisant avec la dernière version stable du produit UBIKA WAAP Gateway, son contenu est par conséquent régulièrement mis à jour afin d'y intégrer les dernières fonctionnalités et innovations.

En conséquence, l'agenda décrit ci-dessous peut être amené à être légèrement différent tout en gardant bien entendu les lignes directrices constituant les bases nécessaires à l'exploitation de la solution.

À l'issue de la formation, les participants seront capables de :

- Décrire comment UBIKA WAAP Gateway protège un web service.
- Configurer le mode de protection le plus adapté :
- Conformité JSON ou XML
- Validation par schéma (OpenAPI3, Swagger 2, WSDL)
- Manipulation de contenu
- Vérification d'intégrité
- Chiffrement et déchiffrement
- Utiliser le moteur de filtrage ICX pour protéger un web service.
- Déployer une politique de sécurité en utilisant l'apprentissage (Sitemap).
- Manipuler des token de type JWT.

5.Web Access Manager

5.1 Détails de la formation

Durée	**2 jours (~14 heures)**
Audience	**Administrateur, Ingénieurs réseaux et sécurité, chef de projet et tous ceux qui administrent régulièrement la solution UBIKA WAAP Gateway.**
Contenu	**50 % théorie / 50 % pratique**
Certification	**non**

L'objectif de cette formation est l'obtention des connaissances et de l'expérience nécessaires pour mettre en place, maintenir, et diagnostiquer une authentification de type Web SSO.

Cette formation se faisant avec la dernière version stable du produit UBIKA WAAP Gateway, son contenu est par conséquent régulièrement mis à jour afin d'y intégrer les dernières fonctionnalités et innovations.

En conséquence, l'agenda décrit ci-dessous peut être amené à être légèrement différent tout en gardant bien entendu les lignes directrices constituant les bases nécessaires à l'exploitation de la solution.

À l'issue de cette formation, les participants seront capables de :

- Décrire comment UBIKA WAAP Gateway gère une authentification.
- Configurer plusieurs méthodes d'authentification et expliquer comment elles peuvent fonctionner ensemble.
- Déployer une politique d'authentification et d'autorisation pour une application avec UBIKA WAAP Gateway.
- Déployer une configuration de type SSO avec UBIKA WAAP Gateway (SAML, OAuth).

5.2 AGENDA

- **Introduction (1h)**
- **Authentication component (1h30)**
- **Standalone Authentication (1h)**
- **Advanced Authentication (2h)**
- **WebSSO (2h)**
- **Credential Mapping (1h)**
- **Customization (1h)**
- **SAML (2h)**
- **OAuth (2h)**
- **Certification (1h)**

6. E-Learning

6.1 AVANTAGES

- **Des cours en ligne** pour étudier où et quand vous le voulez
- **Un accès 24h/24** à votre Espace Élève personnel
- **Des exercices interactifs** pour tester vos connaissances
- **Des vidéos thématiques** sur des sujets clés du programme

6.2 PÉDAGOGIE

- **Formation qui peut être suivie depuis votre domicile ou votre entreprise.** Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur.
- **Chaque stagiaire dispose d'un poste de travail** adapté aux besoins de la formation, d'un support de cours au format numérique et d'un environnement de lab.
- **Pour une meilleure assimilation, le stagiaire alterne tout au long de la formation** les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul.
- **Des exercices sous forme de QCM** sont proposés après chaque chapitre.
- **Attestation de fin de formation,** remise au stagiaire par courrier électronique.

6.3 E-learning UBIKA WAAP Gateway

AGENDA

La formation contient des informa- tions sur les protocoles (HTTP, SSL, authentifications), une description détaillée des fonctionnalités du produit et leurs configurations avec des exercices pratiques. Pour plus de détail sur les leçons de la formation en ligne, vous pouvez consulter la page suivante de notre site e-learning

Détails de la formation

Durée	**21h, la formation est disponible sur le site e-learnin gpour une durée de 90 jours. L'environnement de Lab est disponible pour une durée de 20 heures.**
Audience	**Ingénieurs et Administrateurs Sécurité**
Contenu	**50 % théorie / 50 % pratique**
Certification	**oui**

7.Accessibilité des formations

Accessibilités aux personnes handicapées : La Loi du 5 septembre 2018 pour la « liberté de choisir son avenir professionnel » a pour objectif de faciliter l'accès à l'emploi des personnes en situation de handicap. UBIKA tente de donner à tous les mêmes chances d'accéder ou de maintenir l'emploi.

C'est pourquoi nous vous invitons, en amont de votre session, à nous indiquer tout besoin spécifique vous permettant de suivre votre formation dans les meilleures conditions. Lors d'un entretien de recueil de vos attentes et besoins avec notre réfèrent handicap Chloé BRISSET (chloe.brisset@ubikasec.com), nous étudierons ensemble la faisabilité de la réalisation de l'action de formation.

8.Prérequis

8.1 MATÉRIEL ET LOGICIEL

Un accès réseau adéquate est fourni à l'ensemble des participants. les démonstrations et la mise en pratique de l'ensemble des formations se font à travers un environnement de lab virtualisé. Chaque stagiaire, afin d'accéder à cet environnement, devra se munir du matériel suivant :

- Un ordinateur **portable architecture 64bits avec 4Go de RAM au minimum**
- Une version récente de **java installé**
- **Un navigateur internet** graphique récent, de type Firefox ou Chrome
- **Adobe Acrobat Reader** ou équivalent
- **Posséder le droit administrateur pour modifier le fichier hosts**
- **Avoir la possibilité de se connecter à un réseau Wifi et d'accéder aux ressources locales**

8.2 CONNAISSANCES TECHNIQUES POUR L'ENSEMBLE DES FORMATIONS

- Connaissances approfondies **des protocoles HTTP / HTTPS et TCP /**
- **IP** Connaissances de base sur **la technologie reverse proxy**
- Connaissances de base sur **les expressions régulières**
- Connaissances de base sur **l'administration système linux**
- Connaissances de base du **top10 de l'OWASP**

8.3 CONNAISSANCES TECHNIQUES SPÉCIFIQUES POUR LA FORMATION EXTENDED API

- **Passer avec succès la formation UBIKA WAAP Gateway**
- Connaissances de base **des standards XML et JSON**
- Connaissances de base de **la terminologie des Web Services**

8.4 CONNAISSANCES TECHNIQUES SPÉCIFIQUES POUR LA FORMATION WEB ACCESS MANAGER

- **Passer avec succès la formation UBIKA WAAP Gateway**
- Connaissances de base sur **les authentifications applicatives web et / ou SAML**
- Connaissances de base sur **LDAP / Active directory / PKI**
- Connaissances de base **du langage HTML**

8.5 CONNAISSANCES TECHNIQUES SPÉCIFIQUES POUR LA FORMATION EXPERT UBIKA WAAP GATEWAY

- **Passer avec succès la formation UBIKA WAAP Gateway**

8.6 Autres prérequis en cas de formation à distance

- La formation et le partage d'écran se fait avec l'outil Teams ou GotoMeeting.
- Le stagiaire accède à un environnement de Lab chez azure avec le protocole RDP (le flux RDP doit être autorisé depuis le PC du stagiaire vers Azure).

9.Pédagogie

Le nombre de stagiaires peut varier de 4 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 support de cours et/ou un manuel de référence au format numérique.

Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise, intra-entreprise ou classe virtuelle qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.
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.

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.
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 d'UBIKA.

Attestation de fin de formation, remise au stagiaire par courrier électronique.

10.Modalités d’inscription et de paiement

Contacter votre commercial ou envoyer un email à info@ubikasec.con pour obtenir un devis.

L’enregistrement se fait directement en prenant contact avec votre responsable commercial au sein de UBIKA. Tout paiement devra se faire par transfert bancaire et déclenchera systématiquement la réservation définitive de votre place, celle-ci n’étant que provisoirement assurée avant cela.

Les inscriptions sont possibles jusqu'à **48 heures** avant le début de la formation.

Toute annulation doit se faire dans un délai de **15 jours** minimum avant le premier jour de la formation. Passé ce délai, la formation sera due.

Le délai de mise en œuvre d'une formation intra-entreprise ou "custom" est de 3 semaines après acceptation du devis.

UBIKA

A propos

UBIKA est l’un des leaders en sécurité informatique qui protège les ressources numériques des entreprises et des les

institutions publiques au niveau mondial contre cyberattaques.

Le pionnier des technologies de chiffrement hautement sécurisées propose un chiffrement réseau à haut débit, une sécurité des terminaux zéro-trust et des solutions innovantes de protection des données pour les environnements cloud et les applications web.

Ces solutions de sécurité de confiance accompagnent les utilisateurs vers un monde sécurisé et numérisé et contribuent ainsi de manière significative à la souveraineté numérique.

Service à valeur ajoutée

- Mondial
- Local et personnalisé
- Spécifique au client et flexible
- Qualité sans compromis
- Fiabilité à long terme

UBIKA SAS
Parc Tertiaire de Meudon
9-11 Rue Jeanne Braconnier
92366 Meudon - France
Info : +33 (0)1 46 20 96 00
Email : sales@ubikasec.com
www.ubikasec.com/FR