Formations
Règles de l'Art

certilience
EXPERTS EN SÉCURITÉ INFORMATIQUE

3 allée des Séquoias - 69760 LIMONEST
04 28 29 72 50 - contact@certilience.fr

www.certilience.fr

Nos formations

ART01	14 heures	*Authentification*
ART02	14 heures	*Durcissement des Systèmes*
ART03	14 heures	*Firewall*
ART04	14 heures	*Logs*
ART05	7 heures	*Le Monitoring – Supervision et Administration*
ART06	7 heures	*Sécurisation des Applications Web sur Apache*
ART07	14 heures	*Sécurité WIFI*
ART08	14 heures	*Sécurité du Cloud Computing*

ORDINATEUR PORTABLE NON FOURNI

ART01 Authentification

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau, Connaissances en systèmes	Niveau Bac+2 en informatique	locaux Certilience / vos locaux	14 heures (2 jours)

La Formation Authentification permet de **comprendre les mécanismes généraux de l'authentification**, et d'étudier les **méthodes**, les **protocoles** et les **usages**.

OBJECTIFS DE LA FORMATION

- Adapter le moyen d'authentification au besoin
- Comprendre comment fédérer l'authentification
- Sécuriser son infrastructure

PROGRAMME

1/. Introduction

- Cryptographie
- Les techniques de chiffrement (Symétrique / Asymétrique)
- Faiblesses des solutions traditionnelles d'authentification

2/. Les bases

- LDAP, DB
- PKI, CAS, SAML

3/. Théorie

- Le concept AAA (Authentication, Authorization and Accounting)
- Le SSO

4/. Les protocoles

- Radius
- Tacacs
- 802.1x
- 802.11x
- EAP

5/. Les implémentations

- En OpenSource
- Présentation de produits

6/. Travaux pratiques

ART02 Durcissement des Systèmes

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau, Connaissances en systèmes	Administrateur Réseau Administrateur Sécurité	locaux Certilience / vos locaux	14 heures (2 jours)

La Formation Durcissement des Systèmes permet d'apprendre à **optimiser son système d'information** au niveau de la performance et de l'administration en activant le minimum de services et en réduisant les permissions inutiles.

OBJECTIFS DE LA FORMATION

- Maîtriser les techniques de durcissement et comprendre l'intérêt des techniques
- Se protéger contre des vulnérabilités non publiées

PROGRAMME

1/. Systèmes Linux

- Les bases
- Durcissement général
- Durcissement SSH
- Durcissement PAM
- Tripwire / Iwatch : outils test d'intégrité sur les fichiers
- Externalisation des logs
- Focus Sécurité serveur Web / Reverse proxy :
  - Apache
  - Durcissement (header, cache, compression, XFF, …)
  - Fail2ban
  - Dos_evasion

2/. Systèmes Windows

- Sécurisation des services
- Sécurisation des comptes utilisateurs
- Gestion des mises à jour

3/. Travaux pratiques

- Attaques
- Contre-mesures

ART03 Firewall

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau, Connaissances en systèmes	Niveau Bac+2 en informatique	locaux Certilience / vos locaux	14 heures (2 jours)

La formation Firewall permet de **comprendre tous les aspects d'un pare-feu d'infrastructure**.

OBJECTIFS DE LA FORMATION

- Savoir créer une architecture réseau sécurisée
- Implémenter et maintenir efficacement une politique de filtrage
- Choisir les technologies adaptées à ses besoins

PROGRAMME

1/. Introduction

2/. Le cloisonnement réseau
- Usages et limites

3/. Comment construire une stratégie de filtrage
- Création des DMZ
- Les règles à ne pas oublier
- Processus de création

4/. Les composants d'un pare feu
- Filtrage
- Translation
- VPN
- Prévention d'intrusion : IPS
- Dénie de Service : Dos
- Gestion de la qualité de service : QoS

5/. Travaux pratiques

ART04 Logs

Niveau	Prérequis	Public	Lieu	Durée
Débutant	Bonnes connaissances des systèmes et des réseaux	Niveau Bac+2 en informatique	locaux Certilience / vos locaux	14 heures (2 jours)

Le but de la Formation Logs est de donner une **vision d'ensemble** des problématiques de la **supervision** et de la **gestion des logs**.

OBJECTIFS DE LA FORMATION

- Savoir installer une solution de gestion des logs,
- Configurer la remontée des logs,
- Comment exploiter la solution au quotidien

PROGRAMME

1/. Introduction aux logs

2/. Présentation des différents formats et protocoles
- le format Propriétaire
- le format « Cleartext »
- Syslog

3/. Installation et configuration d'un serveur type syslog
- Architecture
- Configuration type

4/. Comment configurer les équipements
- Firewall
- Serveurs
- Solutions

5/. Architecture LogStash
- Installation
- Configuration
- Exploitation

6/. Les SIEM
- Concept
- Implémentation
- Produits du Marché

7/. La législation française

ART05 Monitoring – Supervision et Administration

Niveau	Prérequis	Public	Lieu	Durée
Débutant	Bonnes connaissances des systèmes et des réseaux	Administrateur réseaux / Ingénieur en sécurité et réseaux / Responsable de la sécurité des systèmes d'informations	locaux Certilience / vos locaux	7 heures (1 jour)

La Formation Monitoring – Supervision et Administration permet **d'acquérir les compétences nécessaires à l'administration d'une solution de monitoring.**

Elle aborde également l'aspect **production** et **contrainte de supervision.**

OBJECTIFS DE LA FORMATION

- Savoir installer un système Linux,
- Configurer une solution de monitoring,
- et Exploiter la solution de monitoring

PROGRAMME

1/. Introduction à Linux
- L'historique
- Le noyau Linux
- Les distributions

2/. Introduction au Monitoring
- Les objectifs
- Les architectures
- Les services

3/. Configuration
- Les protocoles de supervision
- Les services supervisés
- Les notifications

4/. Administration
- La gestion des alertes
- Le reporting
- La sauvegarde et la restauration

5/. Travaux pratiques
- Installation, configuration et administration d'une solution

ART06 Sécurisation des Applications Web sur Apache

Niveau	Prérequis	Public	Lieu	Durée
Débutant	Connaissances en réseau, Connaissances en systèmes	Administrateur réseaux / Ingénieur en sécurité et réseaux / Responsable de la sécurité des systèmes d'informations	locaux Certilience / vos locaux	7 heures (1 jour)

La Formation Sécurisation des Applications Web sur Apache permet **l'apprentissage de la mise en place de solutions simples pour se protéger des attaques les plus répandues**.

Elle permet également d'apprendre à **installer un système Linux.**

OBJECTIFS DE LA FORMATION

- Durcir la configuration d'apache
- Ajouter les bons composants pour protéger votre site web

PROGRAMME

1/. Introduction à Apache

- Installation
- Configuration
- Utilisation de SSL

2/. Hardening Apache

- Directives à repositionner sur une installation standard
- Les directives à éviter

3/. Hardening PHP

- Le fichier php.ini
- suPHP

4/. Ajout de briques

- Utilisation de mod Evasive
- Activation de modsecurity
  - Présentation de modsecurity
  - Activation des règles
  - Création des règles
  - Gestion des alertes

5/. Utilisation de fail2ban

- Écriture de règles

6/. Interconnecter modsecurity et fail2ban

ART07 Sécurité WIFI

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau	RSSI / Responsable Système et Réseau / Consultant Sécurité / Agence gouvernementale / Informaticien averti	locaux Certilience / vos locaux	14 heures (2 jours)

La Formation Sécurité WIFI a pour but de vous faire **découvrir les principes d'une infrastructure sécurisée** et de vous apprendre **les mettre en œuvre.**

OBJECTIFS DE LA FORMATION

- Configurer une infrastructure wifi et l'exploiter
- Administrer ses accès invité

PROGRAMME

1/. Introduction

- Le wifi 802.11…
- Les Protocoles et bases : RADIUS, PKI, etc.

2/. Sécurisation du WIFI

- Faire le point sur les problèmes liés au Réseau sans fil
- La base : WEP / WPA
- 802.11x et les protocoles associés (EAP-xxx, …)
- Authentification AD / Certificat

3/. Sécurisation d'un accès public (Hotspot)

- Les attaques
- Les bonnes pratiques

4/. Travaux pratiques

- Services RADIUS, AD et PKI de Microsoft
- les Technologies Aruba et Fortinet

ART08 Sécurité du Cloud Computing

Niveau	Prérequis	Public	Lieu	Durée
Intermédiaire	Connaissances en réseau et système	RSSI / Responsable Système et Réseau / Consultant Sécurité / Consultant Cloud	locaux Certilience / vos locaux	14 heures (2 jours)

L'objectif de la Formation Sécurité du Cloud Computing est de **comprendre les nouveaux défis de Sécurité** liés à l'utilisation du cloud.

OBJECTIFS DE LA FORMATION

- Comprendre la sécurité pour chaque modèle Cloud (Saas, PaaS, IaaS)
- Mettre en place une Politique de Sécurité, Évaluation des risques, Gouvernance et Réversibilité du Cloud Computing
- Évaluation globale de la Sécurité d'un modèle de Cloud Computing
- Protection des données dans le Cloud le long de leur cycle de vie

PROGRAMME

1/. Introduction au cloud computing
- Modèles : SaaS, PaaS, IaaS
- Types : public, privé, hybride

2/. Sécurité : défis dans le nuage
- Présentation du sujet – Pourquoi est-ce difficile ?
- Virtualisation et multi-location
- L'évaluation des risques pour la migration

3/. La sécurité des infrastructures dans le nuage
- La gestion de patch et de configuration
- La sécurité des réseaux et la virtualisation
- La sécurité et l'impact pour les applications
- La sécurité des données

4/. Les risques et la gouvernance pour le cloud computing
- La nécessité des politiques internes et des exigences
- Service Level Agreements (SLA)
- Les modèles de gouvernance pour le nuage et la gestion des risques
- La réversibilité

ART08 Sécurité du Cloud Computing

Niveau	Prérequis	Public	Lieu	Durée
Intermédiaire	Connaissances en réseau et système	RSSI / Responsable Système et Réseau / Consultant Sécurité / Consultant Cloud	locaux Certilience / vos locaux	14 heures (2 jours)

PROGRAMME (suite)

5/. Audit et évaluation du cloud

- Audit du cloud à distance et sur place
- Les évaluations pour le nuage
- Cloud Security Alliance et A6 CloudAudit [2]
- Pen-tester le nuage

6/. La sécurité des données dans le cloud

- Types de chiffrement et disponibilité
- Les données et leur cycle de vie
- La gestion des clés de chiffrement

7/. Gestion des Identités et des Accès (IAM)

- Architecture IAM et sa pertinence dans le "cloud"
- Normes d'authentification et d'autorisation
- La gestion des comptes, la fédération et le provisionnement