Formations Intégration

- Produits et Applications -

certilience
EXPERTS EN SÉCURITÉ INFORMATIQUE

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

www.certilience.fr

Nos formations

PAP01	14 heures	*Antivirus McAfee Endpoint*
PAP02	7 heures	*Antivirus Eset NOD32*
PAP03	28 heures	*Firewall CheckPoint*
PAP04	21 heures	*Firewall pfSense*
PAP05	14 heures	*Fortinet FortiGate - Initial*
PAP06	21 heures	*Monitoring – Centreon*
PAP07	21 heures	*VPN SSL – Juniper – Junos Pulse*
PAP08	28 heures	*Proxy Squid*
PAP09	14 heures	*Virtualisation – VMware*
PAP10	21 heures	*Firewall Sophos UTM, solution de sécurité*

ORDINATEUR PORTABLE NON FOURNI

PAP01 Antivirus McAfee Endpoint

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau, en matière de gestion du système Windows (PC et serveur) et Connaissances des Réseaux et de l'Internet	Administrateur Réseau / Admin Sécurité / Admin de la solution antivirale de l'entreprise (solution globale de sécurité McAfee EPO)	locaux Certilience / vos locaux	14 heures (2 jours)

La Formation Antivirus McAfee Endpoint permet d'appréhender **toutes les utilisations de cet un antivirus**, qui est également un **outil de détection d'intrusion** (HIPS), de **détection des fuites d'information** (DLP) et de **blocage des flux réseau** (Firewall).

OBJECTIFS DE LA FORMATION

- Savoir installer, utiliser efficacement et administrer l'antivirus McAfee Endpoint
- Comprendre la politique antivirale
- Connaître l'installation et le déploiement des composants de sécurité McAfee Endpoint

PROGRAMME

1/. Principes
- Mécanismes de protection antivirale
- Architecture de gestion

2/. Architecture de déploiement
- Les composants logiciels
- Les tâches serveur
- Les politiques
- Les tâches clientes

3/. Configuration avancée
- Les tags
- L'héritage
- Mise à jour des composants clients

4/. Composants additionnels
- Le HIPS : principe et méthode
- Le DLP : principe et méthode

5/. Maintien en conditions opérationnelles
- Mise à jour
- Surveillance
- Sauvegarde / Restauration

6/. Base de données

7/. Travaux pratiques

PAP02 Antivirus Eset NOD32

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau, en matière de gestion du système Windows (PC et serveur) et Connaissances des Réseaux et de l'Internet	Administrateur Réseau / Admin Sécurité / Admin de la solution antivirale de l'entreprise	locaux Certilience / vos locaux	7 heures (1 jour)

La formation Antivirus Eset Nod32 permet d'apprendre **l'utilisation complète** de ce logiciel d'antivirus de poste : version pour Windows, Mac, Linux, Android et d'autres plateformes.

OBJECTIFS DE LA FORMATION

- Savoir installer, utiliser efficacement et administrer l'antivirus NOD32
- Comprendre les architectures des plateformes antivirales (client / serveur)
- Comprendre les mécanismes de distribution, de mise à jour et de remontée d'informations

PROGRAMME

1/. Principes
- Architecture
- Composants logiciels (antivirus, pare-feu)

2/. Déploiement
- Contexte ActiveDirectory
- OCS Inventory
- Autres méthodes

3/. Politique de sécurité
- Antivirale
- Pare-feu

4/. Reporting et alertes

5/. Maintien en conditions opérationnelles
- Mise à jour
- Surveillance
- Sauvegarde / Restauration
- Licences

6/. Travaux pratiques

PAP03 Firewall CheckPoint

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau	Administrateur Réseau / Administrateur Sécurité / Responsable informatique	locaux Certilience / vos locaux	28 heures (4 jours)

L'objectif de la Formation Firewall Checkpoint est **l'apprentissage de cette solution**, leader mondial des pare-feu d'infrastructure.

OBJECTIFS DE LA FORMATION

- Construire et maintenir une politique de Firewall
- Mettre en œuvre une architecture VPN
- Utiliser au mieux les fonctionnalités offertes

PROGRAMME

1/. Présentation
- Bases : Réseaux / Firewall
- Architecture Checkpoint
- Système GAIA

2/. Installation
- Software Firewall / Appliance
- Configuration Réseau
- Clustering

3/. Firewalling
- Politique de sécurité Checkpoint
- Checkpoint : règles implicites, filtrage, authentification, audit
- Translation : types de translation

4/. Les VPN IPSEC
- Les bases du protocole
- Configuration VPN site à site, VPN routing
- Création de VPN & Diagnostic sur les VPN

5/. Les VPN nomades
- Endpoint et MobileAccess
- La gestion des domaines de chiffrement

6/. Fonctionnalités supplémentaires
- Qualité de service
- Identity Awareness

7/. Maintien en conditions opérationnelles
- Mise à jour
- Surveillance
- Sauvegarde / Restauration

8/. Configuration avancée
- Multi-liens
- Liaison Radius, AD, PKI

9/. Travaux pratiques

PAP04 Firewall pfSense

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau	Administrateur Réseau / Administrateur Sécurité	locaux Certilience / vos locaux	21 heures (3 jours)

Cette Formation Firewall pfSense permet **l'apprentissage de cette solution Open Source de pare-feu.**
Cette solution peut être installée sur un ordinateur ou un serveur.

OBJECTIFS DE LA FORMATION

- Savoir installer un firewall adapté au monde de l'entreprise
- Savoir configurer correctement un firewall
- Savoir exploiter un firewall

PROGRAMME

1/. Présentation de pfSense
- Origine du produit
- Évolutions
- Configuration requise

2/. Installation de pfSense

3/. Gestion du réseau : Interfaces / VLAN / Bridge / Routage

4/. Gestion du filtrage

5/. Gestion de la NAT

6/. Les technologies VPN
- IPSE C/ L2TP / OPENVPN / PPTP / LAN2LAN

7/. Gestion des utilisateurs
- Utilisateurs locaux avec certificat
- Interconnexion annuaire / Radius / PKI

8/. Les services de base
- DHCP (server/relay) / DNS (server/forwarder)

9/. Gestion de la QOS

10/. Gestion de la HA

11/. Fonctions avancées
- Gestion multi-opérateurs
- Load balancing
- Intégration SQUID
- Intégration IDS/IPS (Snort)
- Portail captif
- Gestion des traces

12/. Maintien en conditions opérationnelles
- Mise à jour
- Surveillance
- Sauvegarde / Restauration

13/. Travaux pratiques

PAP05 Fortinet FortiGate – Initial

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

La Formation Fortinet FortiGate – Initial permet l'**apprentissage de ce produit de sécurité** intégrant les fonctionnalités suivantes : Pare-feu, Antivirus, Système de prévention d'intrusion, VPN, Filtrage Web, Antispam, et compression de flux.

OBJECTIFS DE LA FORMATION

- Savoir installer, utiliser et administrer le pare-feu Fortinet Fortigate
- Comprendre les architectures de sécurité, ainsi que les mécanismes de filtrage, de translation d'adresse et de routage
- Connaître les règles de bonne utilisation des composants UTM

PROGRAMME

1/. Principes

- Architecture matérielle, logicielle
- Réseau : Zone, Interface, routage
- Politique de Sécurité
- Filtrage / Translation
- VPN IPSEC / VPN SSL

2/. Fonctions UTM

- Politique DoS
- Filtrage d'URL
- Antivirus / Antispam

3/. Fonctionnalités avancées

- Optimisation WAN
- Contrôleur Wifi
- Routage PBR et Multi-liens
- Qualité de service
- Prévention d'intrusions

4/. Maintien en conditions opérationnelles

- Mise à jour
- Surveillance
- Sauvegarde / Restauration

5/. Travaux pratiques

PAP06 Monitoring – Centreon

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau, Connaissances en internet, Connaissances des systèmes Unix	Administrateur Réseau / Administrateur Sécurité / Responsables de la sécurité des systèmes d'informations	locaux Certilience / vos locaux	21 heures (3 jours)

La finalité de la Formation Monitoring – Centreon est de **savoir mettre en œuvre une architecture complète** de monitoring.

OBJECTIFS DE LA FORMATION

- Surveiller ses systèmes
- Être alerté de manière proactive
- Anticiper les évolutions d'infrastructure
- Vérifier ses processus applicatifs

PROGRAMME

1/. Présentation

- Principes
- Architecture logicielle
- Architecture de supervision
  - Les dépendances
  - Les pollers
- Bonnes pratiques – qualité et performance

2/. Utiliser les sondes

- Protocoles utilisés (SNMP, WMI, IPMI, TCP, …)
- Méthodes
- Exemples avancés

3/. Le système d'alertes

- Les modes d'alertes (SMS, Email, autres)

4/. Le reporting

- Construction des graphes
- Externalisation du reporting

5/. Travaux pratiques

PAP07 VPN SSL – Juniper – Junos Pulse

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau, en matière de gestion du système Windows (PC et serveur) et Connaissances des Réseaux et de l'Internet	Administrateur Réseau / Ingénieur en sécurité et Réseaux / Responsable de la sécurité des systèmes d'informations	locaux Certilience / vos locaux	21 heures (3 jours)

La Formation VPN SSL Juniper – Junos Pulse vise l'apprentissage de cette solution qui à pour objectif de **rendre accessible les données de l'entreprise à ses utilisateurs nomades** de manière sécurisée.

OBJECTIFS DE LA FORMATION

- Installer des appliances Junos Pulse
- Exploiter et maintenir la solution dans les règles de l'art
- Publier de nouveaux portails nouvelles ressources
- Publier de nouvelles ressources

PROGRAMME

1/. Présentation
- Qu'est-ce qu'un VPN SSL
- Architecture matérielle
- Notions : Portails, Royaumes, Ressources, Profils, Politiques
- Clients compatibles
- Usages

2/. Gestion de l'authentification
- Radius, LDAP, PKI, SAML
- SSO

3/. Sécurisation du client
- Vérification du Host
- Virtualisation de l'espace de travail
- Remédiation
- Nettoyage du client

4/. Publication
- Portails et Royaume
- Ressources
- Politiques

5/. Configuration avancée
- Reverse proxy (rewriting, proxy passthrough, etc.)

6/. Maintien en conditions opérationnelles
- Mise à jour
- Surveillance
- Sauvegarde / Restauration

7/. Travaux pratiques

PAP08 Proxy - Squid

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en réseau	Administrateur Réseau / Administrateur Sécurité / Administrateur Système	locaux Certilience / vos locaux	28 heures (4 jours)

La Formation Proxy Squid vise l'apprentissage de ce **proxy performant et Open Source**.

Vous découvrirez la gestion des requêtes en un seul processus d'entrée/sortie non bloquant, l'enregistrement des données les plus fréquemment utilisées ainsi que des requêtes DNS. Vous mettrez également en pratique la hiérarchisation des données pour utiliser moins de bande passante.

OBJECTIFS DE LA FORMATION

- Comprendre les architectures Web
- Savoir installer, configurer, sécuriser et superviser un proxy en production

PROGRAMME

1/. Concepts réseau

- Les protocoles HTTP, ICAP, WCCP
- et les architectures WEB

2/. Le Web Caching

- Intérêts
- Fonctionnement

3/. Installation et Configuration

- Mise en place de l'Installation
- Gestion des ACL et du cache
- Utilisation de parent proxy
- Authentification : LDAP, NTLM, …
- et enfin Gestion de la QoS

4/. Configuration avancée

- Mode transparent
- Proxyfication SSL
- et également Architectures complètes (HAVP, squidguard, Dansguardian

5/. Trace et supervision

- Analyse des logs
- Statistiques
- Sarg (installation et configuration)

6/. Utilisation en reverse proxy

- Principe,
- Configuration

7/. Travaux pratiques

PAP09 Virtualisation – VMware

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en matière d'architecture matérielle et de systèmes d'exploitation	Administrateur Réseau / Administrateur Système	locaux Certilience / vos locaux	14 heures (2 jours)

La Formation Virtualisation – VMware vise l'apprentissage de cette solution qui permet de **mutualiser les ressources au niveau des serveurs, de simplifier l'exploitation et de réduire les coûts.**

OBJECTIFS DE LA FORMATION

- Apprentissage de l'utilisation de la solution de virtualisation VMware ESXi
- Gestion des ressources
- Installation et exploitation du produit
- Devenir autonome sur l'environnement

PROGRAMME

1/. Principes

- La virtualisation : avantages et inconvénients
- La virtualisation au sens VMware
- Architectures types
- La gestion des ressources matérielles

2/. La couche d'abstraction

- Le prérequis
- L'administration
- La maintenance
- La gestion du réseau
- La gestion du CPU
- La gestion de la RAM
- La gestion de l'espace de stockage

3/. Le système hôte

- Prérequis
- Calcul des ressources à affecter
- Clonage d'une machine
- Snapshots

4/. Architecture Vsphere

- Présentation de la haute disponibilité
- Gestion des hyperviseurs
- Gestion du stockage

5/. Maintien en conditions opérationnelles

- Mise à jour
- Surveillance
- Sauvegarde / Restauration

6/. Travaux pratiques

PAP10 Firewall Sophos UTM, solution de sécurité

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en matière d'architecture matérielle et de systèmes d'exploitation	Administrateur Réseau / Administrateur Système	locaux Certilience / vos locaux	21 heures (3 jours)

La Formation Sophos UTM V9 permet l'apprentissage de ce produit de sécurité intégrant les fonctionnalités suivantes : **Pare-feu, Antivirus, Système de prévention d'intrusion, VPN, Filtrage Web, et Antispam**.

OBJECTIFS DE LA FORMATION

- Administrer un pare-feu / VPN
- Études de cas : plusieurs scénarios de mise en œuvre
- Déploiement de VPN
- Mise en fonction de la haute disponibilité
- Sensibilisation aux faiblesses inhérentes au protocole TCP/IP et aux stratégies pour compenser ces éventuelles lacunes

PROGRAMME

Formation Architect

- Intégrer Sophos UTM dans les VLAN et configurer les fonctionnalités réseau telles que l'agrégation des liens, les stratégies de routage ou le protocole OSPF
- Allouer de la bande passante en utilisant des fonctions de QoS et configurer l'équilibrage des charges sur les serveurs, utiliser des proxys génériques et assurer la sécurité VoIP
- Utiliser les systèmes d'authentification Sophos UTM pour l'authentification LDAP et l'assignation des profils de sécurité des contenus, configuration et maintenance du chiffrement des e-mails S/MIME et PGP
- Distribuer la sécurité des contenus aux utilisateurs, filtrer les URL, bloquer les données Web douteuses, proposer des capacités d'audit et des rapports détaillés
- Protéger les organisations des attaques connues et de catégories entières d'attaques émergentes ou inconnues avec sophos UTM IPS

PAP10 Firewall Sophos UTM, solution de sécurité

Niveau	Prérequis	Public	Lieu	Durée
Perfectionnement	Connaissances en matière d'architecture matérielle et de systèmes d'exploitation	Administrateur Réseau / Administrateur Système	locaux Certilience / vos locaux	21 heures (3 jours)

PROGRAMME (suite)

- Configurer les VPN avec l'authentification à certificats X509V3, identifier les fonctionnalités des options de haute disponibilité de Sophos
- Assimiler la Gestion des points d'accès Wifi et des portails captifs associés
- Apprendre la Gestion des sites distants (Red) et configurations réseaux complexes
- Comprendre la Gestion de la publication de sites et applications au travers du reverse proxy (WAF)
- Cours sur le Troubleshooting