

Formation Concevoir une Architecture Réseau Sécurisée

Présentation

Cette formation de 5 jours couvre les fondamentaux réseau, les protocoles clés et les principes de sécurité.

Elle aborde la conception d'architectures sécurisées (VLAN, DMZ, pare-feux), le contrôle des accès (NAC, VPN) et la sécurisation des flux.

Les participants apprennent à superviser un réseau, détecter les incidents et y répondre efficacement.

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

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

- Comprendre les menaces et vulnérabilités des infrastructures réseau
- Concevoir une architecture réseau sécurisée (zoning, DMZ, VLAN, filtrage)
- Mettre en œuvre des solutions de sécurité : pare-feu, VPN, IDS/IPS, proxies
- Appliquer les principes de défense en profondeur
- Contrôler les accès et gérer les flux réseau de manière sécurisée
- Détecter, prévenir et réagir face aux attaques réseau

Prérequis

- Maîtrise des bases du réseau : TCP/IP, routage, commutation
- Connaissances en administration système (Linux ou Windows)
- Notions en cybersécurité recommandées (pare-feu, VPN, chiffrement)

Public

- Administrateurs et ingénieurs réseaux et sécurité
- RSSI, techniciens IT, architectes systèmes
- Consultants ou chefs de projet infrastructure
- Toute personne impliquée dans la conception, la sécurisation ou la supervision d'architectures réseau



Programme de la formation

Jour 1 : Fondamentaux réseau et principes de sécurité

- Rappels sur les architectures réseau (OSI, TCP/IP)
- Protocoles clés : ARP, DNS, DHCP, HTTP/S, ICMP
- Cartographie réseau, typologies courantes
- Introduction à la sécurité des réseaux
- Mode infrastructure vs ad-hoc
- Menaces, typologies d'attaques, modèles d'attaquants
- Principes de défense en profondeur
- Règles d'or d'un réseau sécurisé
- TP : Analyse de flux avec Wireshark / Scans avec Nmap / Simulation d'attaques simples

Jour 2 : Conception d'une architecture réseau sécurisée

- Modèles d'architecture sécurisée
- Zoning : interne / DMZ / externe / admin
- VLAN, routage inter-VLAN sécurisé
- Réseau segmenté vs à plat
- Pare-feux (firewalls)
- Fonctionnement, politiques, types (stateful, UTM, NGFW)
- Filtres IP, ports, protocole, Deep Packet Inspection
- DMZ : principes, déploiement d'un service exposé
- TP : Conception d'un réseau en zoning avec DMZ et VLAN ; configuration de pare-feu iptables ou pfSense

Jour 3 : Contrôle des accès et sécurisation des flux

- Contrôle d'accès réseau (NAC)
- 802.1X, RADIUS, politiques d'accès
- Segmentation dynamique selon le niveau de confiance
- VPN
- IPsec, SSL VPN, tunnels site-to-site et client-to-site
- Sécurisation des flux : chiffrement, authentification, filtrage
- Proxies, reverse proxies, inspection HTTPS
- IDS/IPS : détection/prévention des intrusions (Snort, Suricata)

- TP : Déploiement d'un VPN IPsec ; simulation d'un IDS avec alertes Snort ; mise en place d'un proxy Squid

Jour 4 : Supervision, détection et réponse aux incidents

- Supervision de la sécurité réseau
- Logs, SIEM, alertes, corrélation
- Outils : ELK, Grafana, Wazuh, Nagios
- Analyse de trafic anormal, détection d'attaque
- Réponse à incident : méthodologie, isolation, remédiation
- Rétention et exploitation des journaux
- TP : Analyse d'un scénario d'attaque (scan, exfiltration), détection via journaux et réponse simulée

Jour 5 : Normes, bonnes pratiques et étude de cas finale

- Normes et cadres de sécurité
- ISO 27001, NIST CSF, recommandations ANSSI
- RGPD : sécurité des données personnelles
- Bonnes pratiques d'architecture
- Zero Trust, principe du moindre privilège
- Bastion, segmentation par usage, cloud sécurisé
- Étude de cas finale
- Conception d'une architecture réseau sécurisée pour une PME ou collectivité
- Présentation des choix techniques, zoning, sécurité, flux, supervision
- TP / Projet : Élaboration d'un schéma d'architecture sécurisé complet avec contraintes de sécurité, budget et conformité

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**En amont de la formation** *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.