INTRA

INTER

CYBERSÉCURITÉ DES RÉSEAUX

DÉVELOPPER UNE APPROCHE OFFENSIVE ET DÉFENSIVE POUR ANALYSER, DURCIR ET PROTÉGER LES RÉSEAUX FACE AUX ATTAQUES

OBJECTIFS

1. **Comprendre les principes essentiels de la cybersécurité des réseaux** et leur rôle dans la protection et la résilience des infrastructures face aux menaces.
2. **Identifier les faiblesses et leviers de durcissement** d'une architecture réseau en intégrant une vision à la fois offensive et défensive.
3. **Acquérir une compréhension claire des bonnes pratiques,** standards et approches techniques permettant de renforcer la sécurité et la supervision des environnements réseau.
4. **Savoir proposer et prioriser des recommandations opérationnelles** adaptées au contexte technique et aux contraintes métiers de l'entreprise.

MOYENS PÉDAGOGIQUES

Projection du cours, support de cours papier, clés USB
Chaque point de la formation sera illustré par des exemples concrets afin que les participants puisse s'approprier le sujet.

MÉTHODES UTILISÉES

La progression pédagogique du participant est évaluée tout au long de la formation au moyen de QCM.

PUBLIC

> Responsables SSI, administrateurs réseaux et systèmes, ingénieurs en sécurité ou exploitants d'infrastructures, Professionnels de l'IT
> Chefs de projet, techniciens ou auditeurs impliqués dans la protection, le durcissement et l'amélioration continue des environnements réseau.

PRIX HT
1 300 € par personne

DATES
28 et 29 avril 2026

DURÉE
2 jours (14 heures)

LIEU
LCIE Moirans

INTERVENANT
Expert en cybersécurité

PRÉ-REQUIS
Bases en réseaux (modèle TCP/IP, adressage, routage, protocoles courants)
Notions générales en cybersécurité et en administration systèmes et réseaux
Expérience ou familiarité avec la gestion ou la configuration d'équipements réseaux

PARCOURS DE FORMATION

> Introduction à la cybersécurité des réseaux
- Rappels et enjeux du hardening systèmes et réseau.
- Principes de défense en profondeur et réduction de la surface d'attaque

> Sécurisation et contrôle des flux réseau
- Bonnes pratiques de configuration et de filtrage (firewalls, ACL, NAT).
- Segmentation et cloisonnement des environnements, gestion des zones de confiance.
- Supervision, analyse des journaux et gestion des flux critiques.

> Protection et prévention des attaques
- Introduction aux UTM et NGFW
- Mise en œuvre et ajustement des mécanismes de protection (IDS/IPS, DNS filtering, etc.).
- Stratégies de détection, blocage et durcissement face aux menaces courantes.

> Sécurisation de la couche 2
- Bonnes pratiques de commutation : protection des ports, DHCP snooping, BPDU guard, etc.
- Prévention des attaques internes et dérives de configuration.

> Outils, retours d'expérience et recommandations
- Présentation d'outils et d'exemples concrets issus d'audits réseau.
- Élaboration de recommandations adaptées et hiérarchisées.