Sécurité du plan de contrôle réseau : BGP hijacking, DNS abuse et RPKI

Lien : https://innov-systems.com/formation/securite-du-plan-de-controle-reseau-bgp-hijacking-dns-abuse-et-rpki

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**RT66**	**Sécurité Du Réseau**

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les bases du plan de contrôle réseau
- Maîtriser le fonctionnement de BGP et DNS
- Identifier les attaques de type hijacking et abuse
- Comprendre le rôle de RPKI dans la sécurité Internet
- Détecter les anomalies de routage
- Réagir aux incidents de sécurité réseau
- Mettre en place des mécanismes de protection BGP
- Améliorer la résilience des infrastructures réseau
- Appliquer les bonnes pratiques opérateurs
- Comprendre les enjeux globaux de sécurité Internet
- Étudier des cas concrets d’attaques réseau

POUR QUI ?

- Ingénieurs réseau
- Ingénieurs cybersécurité
- Network security engineers
- Opérateurs télécoms
- Administrateurs systèmes et réseaux
- SOC analysts
- Architectes réseaux
- Consultants en cybersécurité
- Ingénieurs cloud networking
- Responsables infrastructure IT
- Étudiants en réseaux et télécommunications

Innov Systems

Programme détaillé

1 / Introduction à la sécurité du plan de contrôle

- Plan de contrôle vs plan de données
- Rôle critique du routage Internet
- Surface d’attaque des protocoles réseau

2 / Fonctionnement de BGP

- Principe du protocole BGP
- Échanges inter-opérateurs
- Logique de propagation des routes

3 / Vulnérabilités de BGP

- Absence de mécanisme natif de confiance
- Propagation d’annonces erronées
- Risques systémiques Internet

4 / BGP Hijacking

- Détournement de préfixes IP
- Usurpation de routes
- Impacts sur la connectivité mondiale

5 / DNS abuse

- Empoisonnement de cache DNS
- Usurpation de résolution
- Détournement de trafic utilisateur

Innov Systems

6 / Attaques combinées DNS + BGP

- Scénarios d’attaques hybrides
- Redirection massive de trafic
- Impact sur la sécurité globale

7 / RPKI et sécurisation du routage

- Validation cryptographique des routes
- Certification des origines de préfixes
- Réduction des annonces malveillantes

8 / Détection et monitoring

- Outils de surveillance BGP
- Détection d’anomalies de routage
- Alertes en temps réel

9 / Réponse aux incidents réseau

- Mitigation des hijacks BGP
- Coordination inter-opérateurs
- Rétablissement du routage

10 / Bonnes pratiques et gouvernance

- Filtrage et politiques BGP
- Adoption de RPKI
- Standards de sécurité Internet

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

22 au 26 Fév. 2027	Présentiel - Casablanca
19 au 23 Avr. 2027	Présentiel - Casablanca
14 au 18 Juin 2027	Présentiel - Casablanca
09 au 13 Août 2027	Présentiel - Casablanca
04 au 08 Oct. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés