BGP Security & RPKI : sécuriser le routage Internet et prévenir les BGP hijacks

Lien : https://innov-systems.com/formation/bgp-security-rpki-securiser-le-routage-internet-et-prevenir-les-bgp-hijacks

DURÉE
5 jours (35h)

RÉFÉRENCE
RT93

CATÉGORIE
Protocoles Réseau Avancés et Évolutions IP

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre le fonctionnement du protocole BGP et du routage Internet
- Identifier les vulnérabilités liées au BGP et aux route leaks
- Comprendre et implémenter RPKI pour sécuriser le routage
- Prévenir les attaques de type BGP hijacking
- Configurer des politiques de filtrage de routes sécurisées
- Mettre en place une surveillance des annonces BGP
- Renforcer la résilience des infrastructures réseau globales
- Participer aux initiatives de sécurité du routage Internet
- Réagir efficacement en cas d’incident de routage
- Améliorer la coordination entre opérateurs réseau
- Appliquer les bonnes pratiques MANRS et RPKI
- Étudier des cas réels d’incidents de sécurité Internet

POUR QUI ?

- Ingénieurs réseaux
- Network architects
- Opérateurs télécoms
- Ingénieurs ISP (Internet Service Providers)
- Ingénieurs cybersécurité réseau
- Administrateurs systèmes et réseaux
- Consultants réseau et sécurité Internet
- SOC engineers réseau
- Responsables infrastructure IT
- Ingénieurs backbone et opérateurs BGP
- Responsables NOC (Network Operations Center)
- Toute personne impliquée dans la gestion ou la sécurité du routage Internet

Innov Systems

Programme détaillé

1 / Introduction au protocole BGP et à l'Internet global

- Rôle du BGP dans l'architecture d'Internet
- Fonctionnement du routage inter-domaine (AS)
- Enjeux de stabilité et de sécurité du routage

2 / Vulnérabilités du routage BGP

- Absence de mécanismes natifs de sécurité
- Fuites de routes et erreurs de configuration
- Attaques de type BGP hijacking et route leaks

3 / Principes du BGP hijacking

- Détournement de préfixes IP
- Interception et redirection de trafic
- Cas réels d'incidents Internet majeurs

4 / Introduction à RPKI (Resource Public Key Infrastructure)

- Concepts de cryptographie appliqués au routage
- Rôle des ROA (Route Origin Authorization)
- Validation des annonces BGP

5 / Mise en œuvre de RPKI

- Publication et gestion des ROA
- Validation côté routeurs (Origin Validation)
- Intégration avec les politiques BGP

Innov Systems

6 / Sécurisation avancée du routage BGP

- Filtrage des routes et prefix-lists
- Best practices d’AS-path filtering
- Coordination entre opérateurs (IRR, RPKI, MANRS)

7 / Surveillance et détection des incidents BGP

- Monitoring du trafic inter-AS
- Détection des anomalies de routage
- Outils de visibilité Internet (RIPE, BGPStream)

8 / Gouvernance et initiatives de sécurité Internet

- Initiative MANRS (Mutually Agreed Norms for Routing Security)
- Rôle des RIR (RIPE, ARIN, AFRINIC, etc.)
- Collaboration entre opérateurs réseau

9 / Résilience et réponse aux incidents

- Plans de mitigation en cas de hijack
- Re-routage et correction rapide des annonces
- Communication entre opérateurs et CERT

10 / Cas pratiques et analyse d’incidents BGP

- Étude de cas de détournement de trafic réel
- Mise en place d’une infrastructure RPKI
- Bonnes pratiques pour opérateurs réseau

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

15 au 19 Fév. 2027	Présentiel - Casablanca
12 au 16 Avr. 2027	Présentiel - Casablanca
07 au 11 Juin 2027	Présentiel - Casablanca
02 au 06 Août 2027	Présentiel - Casablanca
27 Sep. au 01 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