DDoS Mitigation avancée : architectures de protection et scrubbing

Lien : https://innov-systems.com/formation/ddos-mitigation-avancee-architectures-de-protection-et-scrubbing

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**RT63**	**Sécurité Du Réseau**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les mécanismes des attaques DDoS modernes
- Maîtriser les architectures de protection DDoS avancées
- Concevoir des stratégies de mitigation efficaces
- Utiliser les scrubbing centers pour nettoyer le trafic
- Protéger les applications web et API contre les attaques
- Mettre en place des architectures résilientes
- Intégrer la mitigation DDoS dans un SOC
- Optimiser les performances des systèmes de défense
- Réduire l’impact des attaques sur les services critiques
- Développer des plans de réponse aux incidents DDoS
- Analyser et améliorer les dispositifs de protection
- Étudier des cas concrets d’attaques et de défense

POUR QUI ?

- Ingénieurs cybersécurité
- Network security engineers
- SOC analysts
- Architectes sécurité réseau
- Administrateurs systèmes et réseaux
- DevSecOps engineers
- Consultants cybersécurité
- CISO et responsables sécurité
- Ingénieurs infrastructure cloud
- Ingénieurs télécoms
- Chefs de projet IT sécurité
- Toute personne impliquée dans la protection des infrastructures réseau

Innov Systems

Programme détaillé

1 / Introduction aux attaques DDoS modernes

- Typologie des attaques DDoS (volumétriques, protocolaires, applicatives)
- Évolution des menaces et automatisation des attaques
- Impact sur les infrastructures critiques

2 / Principes de la mitigation DDoS

- Détection précoce des anomalies de trafic
- Filtrage et absorption des flux malveillants
- Stratégies de résilience réseau

3 / Architectures de protection DDoS

- Protection on-premise vs cloud-based
- Architectures hybrides de défense
- Redondance et haute disponibilité

4 / Scrubbing centers et nettoyage du trafic

- Fonctionnement des centres de scrubbing
- Redirection du trafic vers des infrastructures de nettoyage
- Filtrage avancé des paquets

5 / Protection réseau en amont (upstream protection)

- Collaboration avec les ISP et fournisseurs cloud
- Blackholing contrôlé et reroutage BGP
- Anycast et distribution du trafic

Innov Systems

6 / Protection des applications (Layer 7)

- Attaques HTTP/S et API abuse
- WAF et mitigation applicative
- Détection des comportements utilisateurs anormaux

7 / Outils et solutions de mitigation DDoS

- Solutions cloud (Cloudflare, Akamai, AWS Shield)
- Appliances dédiées et services managés
- Intégration avec SOC et SIEM

8 / Détection et réponse en temps réel

- Monitoring du trafic réseau
- Systèmes d’alerte et auto-remédiation
- Orchestration des réponses (SOAR)

9 / Optimisation et tuning des protections

- Réduction des faux positifs
- Ajustement des seuils de détection
- Analyse post-incident

10 / Études de cas et simulations d’attaques

- Scénarios de DDoS réels
- Retours d’expérience industriels
- Exercices de mitigation en conditions réelles

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

30 Nov. au 04 Déc. 2026	Distanciel
04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 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