Network Flow Analysis avancé : NetFlow, IPFIX, sFlow et détection d'anomalies

Lien : https://innov-systems.com/formation/network-flow-analysis-avance-netflow-ipfix-sflow-et-detection-danomalies

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**RT79**	**Surveillance Réseaux**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes de l’analyse des flux réseau
- Maîtriser NetFlow, IPFIX et sFlow
- Concevoir des architectures de collecte de flux
- Analyser les performances réseau en temps réel
- Détecter les anomalies et comportements suspects
- Améliorer la visibilité sur les infrastructures réseau
- Optimiser les performances des réseaux complexes
- Intégrer l’analyse de flux dans les outils SOC
- Réduire les risques de sécurité réseau
- Exploiter les données de flux pour la prise de décision
- Déployer des solutions de monitoring avancées
- Étudier des cas concrets d’analyse réseau

POUR QUI ?

- Ingénieurs réseau
- Architectes réseau
- SOC analysts
- Ingénieurs cybersécurité
- SRE (Site Reliability Engineers)
- DevOps engineers
- Administrateurs systèmes et réseaux
- Data engineers réseau
- Consultants cybersécurité
- Ingénieurs infrastructure IT
- Chefs de projet réseau
- Toute personne impliquée dans l’observabilité et la sécurité réseau

Innov Systems

Programme détaillé

1 / Introduction à l’analyse des flux réseau

- Importance de la visibilité réseau
- Différence entre paquets et flux
- Cas d’usage en sécurité et performance

2 / Fondamentaux des flow technologies

- Définition des flux réseau
- Comparaison NetFlow, IPFIX et sFlow
- Avantages et limites de chaque technologie

3 / NetFlow : architecture et fonctionnement

- Principe de collecte des flux Cisco NetFlow
- Exportateurs et collecteurs
- Cas d’usage opérationnels

4 / IPFIX : standardisation des flux

- Extension normalisée de NetFlow
- Flexibilité des templates
- Interopérabilité multi-vendeurs

5 / sFlow : échantillonnage réseau

- Principe du sampling statistique
- Avantages en environnements haute vitesse
- Cas d’usage data centers et cloud

Innov Systems

6 / Collecte et traitement des données de flux

- Infrastructure de collecte centralisée
- Stockage et gestion des volumes massifs
- Normalisation et enrichissement des données

7 / Analyse des performances réseau

- Détection de congestion et latence
- Analyse des patterns de trafic
- Optimisation des ressources réseau

8 / Détection d’anomalies et sécurité

- Identification de comportements suspects
- Détection d’attaques réseau (DDoS, scans)
- Corrélation avec les systèmes SIEM

9 / Outils et plateformes d’analyse de flux

- Solutions open source et commerciales
- Dashboards et visualisation des flux
- Intégration avec les outils SOC

10 / Études de cas et monitoring avancé

- Analyse de trafic en environnement réel
- Détection d’incidents réseau
- Bonnes pratiques d’exploitation

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

01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca
13 au 17 Sep. 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