NDR (Network Detection & Response) : détection comportementale des menaces réseau

Lien : https://innov-systems.com/formation/ndr-network-detection-response-detection-comportementale-des-menaces-reseau

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI109**	**Surveillance Réseaux**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes du Network Detection & Response
- Concevoir une architecture de détection réseau efficace
- Mettre en œuvre la détection comportementale des menaces
- Analyser le trafic réseau et les flux suspects
- Détecter les attaques avancées et mouvements latéraux
- Intégrer NDR avec SIEM et SOC
- Améliorer la visibilité sur le réseau interne et cloud
- Réduire les faux positifs grâce à l’analyse comportementale
- Optimiser la réponse aux incidents de sécurité réseau
- Exploiter la threat intelligence dans la détection réseau
- Déployer des solutions NDR en environnement complexe
- Étudier des cas concrets d’attaques réseau avancées

POUR QUI ?

- Analystes SOC
- Ingénieurs cybersécurité
- Architectes sécurité réseau
- Ingénieurs réseau
- Security engineers
- Threat hunters
- Incident responders (IR)
- Consultants cybersécurité
- RSSI / CISO
- Administrateurs systèmes et réseaux
- Ingénieurs sécurité cloud
- Toute personne impliquée dans la surveillance et la sécurité des réseaux

Innov Systems

Programme détaillé

1 / Introduction au NDR et à la détection réseau moderne

- Définition du Network Detection & Response (NDR)
- Évolution des solutions NDR face aux menaces avancées
- Place du NDR dans l’écosystème SOC (SIEM, SOAR, EDR)

2 / Architecture d’une solution NDR

- Capteurs réseau et points de collecte (SPAN, TAP)
- Moteurs d’analyse et plateformes d’investigation
- Intégration avec les systèmes de sécurité existants

3 / Collecte et analyse du trafic réseau

- Inspection des flux (NetFlow, packet capture, metadata)
- Analyse en temps réel et traitement des événements
- Gestion du trafic chiffré et visibilité limitée

4 / Détection comportementale des menaces

- Baselines comportementales du réseau
- Détection d’anomalies et d’écarts de comportement
- Identification des communications suspectes (C2, exfiltration)

5 / Techniques d’analyse avancée

- Machine Learning appliqué au trafic réseau
- Analyse statistique et corrélation d’événements
- Détection d’attaques latérales (lateral movement)

Innov Systems

6 / Cas d’usage de détection NDR

- Détection de ransomware et mouvements internes
- Identification de compromissions de comptes
- Surveillance des environnements cloud et hybrides

7 / Investigation et réponse aux incidents

- Analyse des alertes et triage des incidents
- Forensic réseau et reconstitution des attaques
- Coordination avec les équipes SOC et IR

8 / Intégration avec SIEM et SOAR

- Corrélation des événements de sécurité
- Automatisation des réponses aux incidents
- Enrichissement des alertes avec threat intelligence

9 / Optimisation et réduction des faux positifs

- Ajustement des modèles comportementaux
- Tuning des règles de détection
- Amélioration continue de la précision des alertes

10 / Déploiement et cas pratiques NDR

- Mise en œuvre d’une solution NDR en entreprise
- Analyse de scénarios d’attaques réelles
- Bonnes pratiques d’exploitation en production

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

23 au 27 Nov. 2026	Distanciel
25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 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