

Network Detection & Response (NDR) : Vectra, Darktrace, ExtraHop

Lien :
https://innov-maroc.com/formation/network-detection-response-ndr-vectra-darktrace-extrahop

DURÉE
5 jours (35h)

RÉFÉRENCE
RT65

CATÉGORIE
Sécurité Du Réseau

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- ✔ Comprendre les principes du Network Detection & Response
- ✔ Maîtriser les solutions Vectra, Darktrace et ExtraHop
- ✔ Déployer une architecture NDR en environnement entreprise
- ✔ Détecter les comportements réseau anormaux
- ✔ Améliorer la visibilité du trafic réseau
- ✔ Identifier les attaques avancées et zero-day
- ✔ Intégrer NDR dans un SOC moderne
- ✔ Automatiser la réponse aux incidents
- ✔ Réduire le temps de détection des menaces
- ✔ Optimiser les capacités de threat hunting
- ✔ Corréler les données réseau avec les outils SIEM/SOAR
- ✔ Étudier des cas concrets de cyberattaques

INOV MAROC

👥 POUR QUI ?

- ✔ Ingénieurs cybersécurité
- ✔ SOC analysts
- ✔ Network security engineers
- ✔ Architectes sécurité
- ✔ Consultants cybersécurité
- ✔ DevSecOps engineers
- ✔ Administrateurs réseau et sécurité
- ✔ Responsables SOC
- ✔ Threat hunters
- ✔ CISO et responsables sécurité
- ✔ Ingénieurs infrastructure IT
- ✔ Toute personne impliquée dans la détection et la réponse aux menaces réseau



Programme détaillé

1 / Introduction au NDR (Network Detection & Response)

- Définition et rôle du NDR dans la cybersécurité moderne
- Différences entre NDR, IDS/IPS et SIEM
- Cas d’usage en détection avancée des menaces

2 / Panorama des solutions NDR

- Présentation de Vectra AI
- Présentation de Darktrace
- Présentation d’ExtraHop
- Comparaison des approches et technologies

3 / Architecture d’un système NDR

- Collecte des données réseau (packets, flows, metadata)
- Analyse comportementale et IA
- Intégration dans le SOC

4 / Déploiement des solutions NDR

- Modes de déploiement (on-premise, cloud, hybride)
- Positionnement des sondes réseau
- Intégration avec l’infrastructure existante

INNOV MAROC

5 / Détection basée sur l’intelligence artificielle

- Machine learning appliqué au trafic réseau
- Détection d’anomalies comportementales
- Identification des attaques zero-day

6 / Threat hunting et investigation

- Analyse des alertes NDR
- Corrélation des événements réseau
- Investigation des incidents de sécurité

7 / Réponse aux incidents (NDR-driven response)

- Automatisation des actions de réponse
- Isolation des machines compromises
- Intégration avec SOAR

8 / Intégration avec l’écosystème cybersécurité

- SIEM, SOAR et EDR
- Corrélation multi-sources
- Centralisation des alertes

9 / Monitoring et optimisation des performances NDR

- Réduction du bruit d’alertes
- Ajustement des modèles de détection
- KPI et tableaux de bord SOC

10 / Cas d’usage industriels et études de cas

- Détection de ransomware et mouvements latéraux
- Protection des environnements cloud et SaaS

INOV MAROC

- Retours d’expérience en entreprise

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

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
06 au 10 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-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC — Tous droits réservés