Concevoir et Mettre en Œuvre la Sécurité des Infrastructures Cisco (SDSI)

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**RST317**	**Cisco Entreprise**

OBJECTIFS DE LA FORMATION

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

- Comprendre l’architecture de sécurité Cisco et les bonnes pratiques de conception
- Déployer des mécanismes avancés de sécurisation des réseaux et des applications
- Mettre en place des politiques de gestion des risques et de réponse aux incidents
- Exploiter l’automatisation et l’IA pour renforcer la cybersécurité
- Acquérir une approche pragmatique permettant d’intégrer sécurité et performance dans l’infrastructure réseau

POUR QUI ?

- Responsables techniques réseau et sécurité
- Ingénieurs systèmes et réseaux en charge de l’exploitation et de la sécurité des infrastructures Cisco
- Administrateurs réseau souhaitant renforcer leurs compétences en sécurité avancée

Programme détaillé

1/ INTRODUCTION AUX PRINCIPES DE SÉCURITÉ

- Concepts de base : CIA (Confidentialité, Intégrité, Disponibilité)
- Menaces modernes et évolutives sur les infrastructures
- Rôle des normes et référentiels (ISO 27001, NIST, CIS Controls)

2/ ARCHITECTURE DE SÉCURITÉ CISCO

- Présentation des solutions Cisco de sécurité réseau
- Positionnement dans une architecture d'entreprise
- Intégration avec les environnements multicloud et hybrides

3/ POLITIQUES ET GOUVERNANCE

- Définition des politiques de sécurité réseau
- Gouvernance et conformité réglementaire
- Gestion des accès et identités (IAM)

4/ SÉCURISATION DE L'INFRASTRUCTURE RÉSEAU

- Protection du plan de contrôle, du plan de données et du plan de gestion
- Sécurisation des protocoles de routage
- Configuration sécurisée des équipements Cisco IOS et NX-OS

5/ SÉCURITÉ DES APPLICATIONS ET DES SERVICES

- Sécurisation des services critiques (DNS, DHCP, NTP)
- Protection des environnements applicatifs dans le Data Center
- Intégration des firewalls Cisco (NGFW, ASA, FTD)

6/ VISIBILITÉ ET CONTRÔLE

- Segmentation réseau et micro-segmentation
- Cisco ISE : gestion centralisée des identités et des accès
- Monitoring et journalisation sécurisée

7/ ANALYSE DES VULNÉRABILITÉS

- Identification et évaluation des vulnérabilités
- Outils Cisco pour la détection (Stealthwatch, Talos)
- Mise en place d’un processus de patch management

8/ RÉPONSE AUX INCIDENTS

- Cycle de vie d’un incident de sécurité
- Méthodologie de gestion des incidents (NIST, SANS)
- Mise en pratique avec des scénarios d’attaques simulées

9/ GESTION DES RISQUES

- Identification des risques liés à l’infrastructure
- Matrice de criticité et hiérarchisation
- Élaboration d’un plan de continuité et reprise d’activité (PCA/PRA)

10/ AUTOMATISATION DE LA SÉCURITÉ

- Automatisation des configurations de sécurité avec Ansible et Python
- Cisco DNA Center et Catalyst Center pour la sécurité réseau
- Orchestration des politiques de sécurité

11/ IA ET ANALYTIQUE DE SÉCURITÉ

- Introduction aux concepts d’AIOps appliqués à la cybersécurité
- Détection d’anomalies et comportements suspects via l’IA

- Cas pratiques avec Cisco SecureX et Cisco AI Endpoint Analytics

12/ INTÉGRATION AVEC LES ÉCOSYSTÈMES TIERS

- Connecteurs et API de sécurité Cisco
- Intégration avec SIEM (Splunk, QRadar, Elastic)
- Automatisation des flux de réponse via SOAR

13/ BONNES PRATIQUES DE CONCEPTION

- Patterns d’architecture sécurisée
- Zero Trust avec Cisco
- Intégration sécurité-performance

14/ ATELIERS PRATIQUES

- Configuration sécurisée d’un environnement Cisco simulé
- Mise en œuvre d’un scénario de segmentation avec Cisco ISE
- Détection et remédiation d’une attaque simulée

15/ SYNTHÈSE ET PLAN D’ACTION

- Bilan des acquis et QCM de validation
- Élaboration d’un plan d’action personnalisé
- Recommandations pour l’implémentation 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

20 au 24 Juil. 2026	Casablanca - Maroc
14 au 18 Sep. 2026	Casablanca - Maroc
09 au 13 Nov. 2026	Casablanca - Maroc

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

Scannez pour accéder à la fiche en ligne