



Cycle Veille et Sécurité SI

DURÉE
12 jours (84h)

RÉFÉRENCE
SEC12

CATÉGORIE
Sécurité du SI

OBJECTIFS DE LA FORMATION

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

- ✓ Connaître les différents facteurs et typologies de risques pouvant porter atteinte à la performance d'une organisation
- ✓ Etre capable de mettre en place une veille concurrentielle efficace

POUR QUI ?

- ✓ Toute personne souhaitant apprendre la sécurité des systèmes et des réseaux



Programme détaillé

1/ Introduction à la Sécurité informatique

- Pourquoi la sécurité informatique ?
- Vue d'ensemble de la sécurité du Système d'Information
- Définitions et concepts fondamentaux : confidentialité, intégrité, disponibilité...
- Les composants de la cybersécurité : Que veut-on protéger ? Pourquoi ?
- Principales méthodes et normes pour l'analyse des risques (EBIOS, Mehari, ISO 27001...)
- Qu'est-ce que la cybercriminalité ? Les grandes familles de virus et malwares
- Quelles sont les menaces physiques ?

2/ Vue d'ensemble des architectures de sécurité

- Panorama des architectures de sécurité et leurs besoins
- RFC 1918
- Translation d'adresses
- DMZ
- La virtualisation : son rôle dans sécurité de l'architecture
- Par-feu. Capacités de protection et limites
- VLANs et appliances
- Composant de la sécurité du Cloud : VPC, CASB, VPN...
- Proxy
- Proxy ou firewall
- Reverse proxy
- Relais SMTP

3/ Détection des intrusions

- Les méthodes de détection
- Principaux acteurs du marché
- Les scanners réseaux (Nmap)
- Web applications
- IDS
- Avantages et limites de de ces technologies
- Comment les mettre en place

4/ Les menaces et vulnérabilités du poste de travail

- Les vulnérabilités sur le poste de travail : déni de service, intrusion, injection de code
- Panorama des vulnérabilités les plus courantes du poste de travail
- Poste de travail et les Virus / Hoax ...

5/ Les vulnérabilités des applications web

- Architecture générale et évolutions
- Navigateurs Web, serveurs HTTP : fonctionnement, faiblesses
- Classement des risques majeurs selon l'OWASP et le CWE
- Analyse des vulnérabilités et des conséquences de leur exploitation
- Les principales attaques :
- Les failles PHP
- Les failles XSS(Cross-Site Scripting)
- Commandes injection, SQL injection, LDAP injection...
- Broken Authentication and Session Management
- Cross-Site Request Forgery (CSRF)
- Cookie poisoning, session hijacking...
- HTTP (ver Nimda, faille Unicode...)
- Default password, directory transversal...
- Cross-Site Request Forgery

- Redirections non validées
- Outils de détection et d'exploitation
- Les scanners de vulnérabilités Web
- L'analyse statique de code
- Les outils d'analyse manuelle
- Exploitation SQL
- Brute-force et fuzzing
- Bonnes pratiques et contre-mesures

6/ Les outils documentaires de veille

- Les abonnements : presse, newsletters, flux RSS...
- Types d'informations web recherchées
- Les modalités, les outils de collecte et d'analyse des contenus
- Constitution du référentiel (sites web, blogs, forums)
- Les logiciels de cartographie de l'information
- Panorama des logiciels spécialisés de veille globale

🔗 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

📅 22 Juin au 07 Juil. 2026

📍 Casablanca

📅 17 Août au 01 Sep. 2026



📅 12 au 27 Oct. 2026



📅 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>

▼
Scannez pour accéder
à la fiche en ligne

Document généré le 15/06/2026 — Réf : SEC12
INNOV MAROC — Tous droits réservés