Cybersécurité des systèmes électoraux et d'identité numérique

Lien : https://innov-systems.com/formation/cybersecurite-des-systemes-electoraux-et-didentite-numerique

DURÉE
8 jours (56h)

RÉFÉRENCE
SI92

CATÉGORIE
Cybersécurité Sectorielle

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les enjeux critiques des systèmes électoraux et d’identité numérique
- Identifier les menaces pesant sur les infrastructures démocratiques numériques
- Concevoir des architectures sécurisées et résilientes
- Mettre en œuvre des mécanismes cryptographiques de confiance
- Renforcer l’authentification et le contrôle d’accès des systèmes sensibles
- Garantir l’intégrité, la transparence et la vérifiabilité des processus
- Assurer la continuité des opérations électorales en cas de crise
- Déployer des systèmes d’identité numérique sécurisés et fiables
- Intégrer les bonnes pratiques de cybersécurité dans les systèmes publics
- Mettre en place des dispositifs de détection et de réponse aux incidents
- Réduire les risques de fraude, manipulation et compromission
- Étudier des cas concrets de sécurisation de systèmes électoraux

POUR QUI ?

- Ingénieurs cybersécurité
- Architectes systèmes critiques
- Experts en identité numérique
- Responsables systèmes d’information gouvernementaux
- RSSI / CISO du secteur public
- Consultants en cybersécurité
- Administrateurs systèmes et réseaux
- Ingénieurs cryptographie
- Responsables infrastructures critiques
- Analystes SOC
- Responsables transformation digitale de l’administration publique
- Toute personne impliquée dans la conception ou la sécurisation de systèmes électoraux ou d’identité numérique

Innov Systems

Programme détaillé

1 / Introduction aux systèmes électoraux et d’identité numérique

- Typologie des systèmes électoraux modernes (papier, électronique, hybride)
- Rôle de l’identité numérique dans les services publics
- Enjeux de confiance, souveraineté et intégrité démocratique

2 / Architecture des systèmes électoraux numériques

- Infrastructures de vote électronique et plateformes de dépouillement
- Systèmes centralisés vs distribués
- Chaîne de confiance de bout en bout

3 / Architecture des systèmes d’identité numérique

- Registres d’état civil et bases d’identités nationales
- Systèmes d’authentification et fédération d’identité
- Intégration avec services publics numériques

4 / Menaces sur les systèmes électoraux

- Attaques de manipulation de votes et altération des résultats
- Déni de service et perturbation des scrutins
- Désinformation et attaques hybrides

5 / Menaces sur les systèmes d’identité numérique

- Vol d’identité et compromission de comptes citoyens
- Attaques sur bases de données d’identité
- Fraude documentaire et falsification numérique

Innov Systems

6 / Cryptographie et intégrité des systèmes

- Signature numérique des bulletins et transactions
- Chaînes de blocs et mécanismes d’audit
- Preuves cryptographiques de l’intégrité des votes

7 / Authentification forte et contrôle d’accès

- MFA et identité numérique sécurisée
- Gestion des rôles électeurs et administrateurs
- Séparation des privilèges et moindre accès

8 / Auditabilité et transparence des systèmes

- Journalisation sécurisée des opérations
- Vérifiabilité individuelle et publique des votes
- Mécanismes de traçabilité sans compromission de l’anonymat

9 / Résilience et continuité des opérations électorales

- Redondance des infrastructures critiques
- Plans de continuité et scénarios de crise
- Protection contre les attaques DDoS et sabotage

10 / Gouvernance et cadre réglementaire

- Normes internationales des systèmes électoraux
- Protection des données personnelles (RGPD et équivalents)
- Gouvernance des infrastructures d’identité nationale

11 / Détection et réponse aux incidents

- Surveillance des systèmes électoraux en temps réel
- Détection des anomalies et tentatives de fraude

Innov Systems

- Gestion de crise électorale

12 / Cas pratiques et retours d’expérience

- Analyse de systèmes électoraux existants
- Études de cas de cyberattaques et incidents
- Bonnes pratiques de conception sécurisée

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

16 au 25 Nov. 2026	Distanciel
18 au 27 Jan. 2027	Présentiel - Casablanca
15 au 24 Mars 2027	Présentiel - Casablanca
10 au 19 Mai 2027	Présentiel - Casablanca
05 au 14 Juil. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Innov Systems

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés