MODULE MENACES HYBRIDES : RISQUE DRONE/RISQUE CYBER

Objectif :

Risque terroriste, espionnage économique, guerre électronique, risque industriel, etc. Les applications malveillantes des drones ne sont plus une fiction mais une réalité. La menace potentielle posée par les drones doit désormais être pleinement appréhendée par les responsables sécurité/sûreté dans leur analyse de risques. Ce module de sensibilisation vise à conduire un état de l'art complet des menaces induites par la dronotique et des contremesures existantes afin de s'en protéger. Il est d'un intérêt particulièrement pour les directions et chefs de sites sensibles.

Pré requis :

Aucun

Public visé :

Directions sites sensibles OIV/PIV
Responsables de sites sensibles
Chefs d'équipe sûreté/sécurité

Validation :

Attestation de formation délivrée par l'ESSE

Contenu pédagogique :

Module 1 : Approche technologique, IA et guerre électronique
Typologie et limites des drones face à la météo et aux charges utiles.
Cyber & Électronique : Étude des liaisons de données, des vulnérabilités électromagnétiques (EM), de l'automatisation par l'IA et de la guerre algorithmique.
Module 2 : Systèmes de détection et capteurs électroniques
Analyse des capteurs : radars (actifs/passifs), optronique, acoustique et laser.
Cyber & Électronique : Principes de la détection Radiofréquence (RF) (et ses limites face aux drones autonomes), détection NLJD des composants électroniques, et fusion informatique des données via les systèmes C2.
Module 3 : Contre-mesures, Hacking et neutralisation
Méthodes physiques : armes cinétiques, captures par filet, et protections passives.
Cyber & Électronique : Brouillage EM, spoofing (falsification GNSS), impulsions micro-ondes (HPM) pour griller l'électronique, et cyber-prise de contrôle (hacking) du drone.
Module 4 : Concepts d'Opérations (CONOPS) et Menaces Hybrides
Déploiement d'architectures de sécurité adaptées par secteur (aéroports, OIV, armées, prisons).
Cyber & Électronique : Protection des sites d'entreprises contre les cyberattaques par drone (intrusion de réseau, espionnage), et articulation du risque avec le cyber-renseignement (CYBINT, SIGINT).

Moyens pédagogiques :

Contenu théorique & illustrations multimédias / Exercices & Etudes de cas : Mises en situations professionnelles / Questions / Réponses et partage d'expérience

CALENDRIER DE FORMATION

PARIS

204 boulevard Raspail
75014 PARIS

Calendrier sur le site internet www.ess-e.fr

*Tous nos centres sont en mesure d'accueillir des personnes en situation de handicap et d'effectuer un accompagnement pédagogique adapté

Durée :
7 heures – 1 journée

Nombre de stagiaires :
12 personnes maximum en formation

Lieu :
Formation à l'ESSE 204 boulevard Raspail 75014 PARIS

Tarif :
450 € H.T. (entreprise)
350 € H.T. (individuel)

Numéro de déclaration d'activité: 11751048975

contact@ess-e.fr