FORMATION - SIMULATEUR D'ATTAQUE INFORMATIONNELLE : COMPRENDRE ET CONTRER LA DÉSINFORMATION

Public et pré-requis
Secteur médias & information : journalistes, pigistes, fact-checkers, responsables de rédactions.
Communication & institutionnel : directeurs de la communication, responsables de la communication de crise, conseillers politiques et agents des collectivités territoriales.
Intelligence & cybersécurité : analystes OSINT (débutants à intermédiaires), veilleurs stratégiques et spécialistes de la menace informationnelle.
Enseignement & recherche : étudiants et chercheurs en sciences politiques, relations internationales, journalisme ou cybersécurité.

Durée et modalités pédagogiques
Formation Présentiel de 3h30min

Moyens pédagogiques
Le support numérique de formation vous est transmis pendant ou après la session.

Accessibilité
Nous mettons tout en œuvre pour vous accueillir toutes et tous dans les meilleures conditions. Notre charte handicap détaille nos engagements pour l'accessibilité de nos formations. Contactez notre référent handicap si vous avez des besoins spécifiques d'accompagnement avant, pendant et après la formation: handicap@samsa.fr

Evaluation
1- Positionnement
Un questionnaire en ligne ou un tour de table en début de session permettra d'évaluer votre niveau initial, vos besoins et vos attentes.
2-Evaluation des acquis
Au cours de la formation, les exercices réalisés permettent au formateur ou à la formatrice d'évaluer l'acquisition des compétences.
3- Attestation
Une attestation des acquis de fin de formation vous sera adressé suite à la session

Dernière modification contenu formation - 02/10/2026

Objectifs

- Comprendre les schémas d'attaques informationnelles
- Analyser une opération d'influence coordonnée multi-plateforme dans un contexte électoral français
- Détecter et caractériser les comportements inauthentiques coordonnés
- Identifier l'origine d'une attaque et repérer les signatures des commanditaires

Programme

- Présentation du formateur et tour de table pour identifier les attentes des participants
- Histoire de la propagande et évolution des attaques informationnelles
- Typologie des attaques informationnelles contemporaines
- Atelier immersif collaboratif avec le simulateur d'attaque informationnelle développé par Checkfirst : les participants sont invités dans une interface qui propose un flux ininterrompu de contenus en simulant les outils quotidiens :
  - Réseaux sociaux (déferlantes de Tweets, posts Tiktok, Instagram et fils d'actualité)
  - Messageries instantanées (alertes sur boucles Telegram)
  - Communications directes (emails de sources, de lecteurs et de pressions externes)
- Identification des contenus manipulés en individuel ou en petits groupes
- Debrief de l'atelier et ancrage des notions clés
- Évaluation à chaud de la formation par les participants