



Surveiller ce qui circule sur vous.

Vous aimeriez savoir si les mots de passe de vos salariés, vos noms de domaine ou vos documents circulent déjà quelque part ? Quatre jours pour monter une surveillance qui tourne toute seule et vous prévient avant que ça serve à quelqu'un.

DURÉE	TARIF INTER	INTRA	NIVEAU
4 jours	3 000 € HT	dès 1 500 € HT/jour	Intermédiaire

À l'issue de la formation

- Comprendre l'écosystème infostealer et ses acteurs
- Mettre en place une veille automatisée multi-sources
- Produire des bulletins CTI opérationnels exploitables
- Construire les fondations d'un CERT/CSIRT interne

Pour qui

- Analystes CTI en montée en compétences
- RSSI voulant structurer une fonction veille
- Consultants en charge de la surveillance de clients
- SOC managers souhaitant créer une capacité CERT

Prérequis

Notions de sécurité, familiarité avec les logs et alertes. MISP recommandé.

Déroulé

Jour 1 Infostealers – comprendre l'écosystème

- Panorama des familles : Lumma, Vidar, RedLine, StealC
- C2, marchés underground et canaux Telegram
- Logs d'infostealer : structure, ce qu'on y trouve
- Identifier une machine compromise dans un log
- Sources publiques : URLhaus, ThreatFox, C2Tracker

Jour 2 CTI opérationnelle

- Cycle du renseignement appliqué à la veille
- MISP - setup, taxonomies, corrélation automatique
- IOC vs IOA - chasse sur les comportements
- Pivots OSINT à partir d'un IOC (domaine → IP → infra → acteur)
- Diamond Model appliqué : profiler un acteur

Jour 3 OSINT & surveillance automatisée

- Surveillance de domaines et d'identités (typosquatting, leaks)
- Automated OSINT : Shodan, Censys, SecurityTrails en API
- Honeytokens et canary tokens - détecter les reconnaissances
- Workflows d'alerte : de la source au ticket SIEM
- TP : pipeline de détection infostealer automatisée

Jour 4 Structurer un CERT / CSIRT

- Gouvernance d'un CERT : périmètre, SLA, escalade
- Playbooks de réponse à incident par type de menace
- Intégration CTI → SOAR → tickets
- Communication de crise - technique et non-technique
- Exercice final : incident infostealer de A à Z

Ce qui est compris

- Accès à des logs d'infostealers réels anonymisés
- Instance MISP préconfigurée (accès lab 30j)
- Playbooks de réponse à incident éditables
- Templates de bulletin CTI

Prochaines sessions inter-entreprises

DATES	LIEU ET FORMAT	PLACES
4 - 7 janvier 2027	Paris · Présentiel ou distanciel	6 places
19 - 22 avril 2027	Paris · Présentiel ou distanciel	8 places
13 - 16 septembre 2027	À distance · Distanciel	8 places

Résistez aux hackers - organisme de formation certifié Qualiopi. Prise en charge OPCO possible, les pièces sont fournies.

Inscription et devis : <https://resistez-aux-hackers.com/contact.html> - formation@resistez-aux-hackers.com

Programme susceptible d'évoluer. Version du 08/10/2026. Accessibilité : nous contacter pour toute situation de handicap, nous étudions les adaptations possibles.