



# Savoir qui vous attaque et comment il s'y prend.

Vos équipes reçoivent des alertes toute la journée sans savoir lesquelles comptent ? On apprend à suivre un attaquant à la trace, à comprendre sa méthode, et surtout à chercher ce qui n'a déclenché aucune alerte.

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

## À l'issue de la formation

- Maîtriser le cycle du renseignement cyber appliqué
- Produire du CTI exploitable par les équipes opérationnelles
- Déployer et alimenter une plateforme MISP
- Chasser proactivement les menaces sur un SIEM

## Pour qui

- Analystes SOC niveaux 2 et 3
- RSSI et responsables sécurité
- Consultants CTI
- Équipes de réponse à incident

### Prérequis

Fondamentaux réseau, notions de sécurité. Expérience SIEM recommandée.

## Déroulé

### Jour 1 Cycle du renseignement & frameworks

- Définition des PIR/RFI, niveaux de CTI
- Sources OSINT, HUMINT, TECHINT
- Frameworks : MITRE ATT&CK, Diamond Model, Kill Chain
- Modélisation des acteurs de menace

### Jour 2 MISP & partage

- Installation et configuration MISP
- Taxonomies, galaxies, IOC vs IOA
- STIX/TAXII - interopérabilité
- Automatisation des flux de menace

### Jour 3 Threat Hunting pratique

- Hypothèses de chasse basées sur ATT&CK
- Hunting sur logs Windows Event Log
- SIEM queries avancées (Elastic/Splunk)
- Visualisation des patterns d'attaque

### Jour 4 CTI opérationnelle & reporting

- Intégration CTI → SIEM → SOAR
- Rédaction d'un bulletin CTI opérationnel
- Exercice complet : du feed brut à l'alerte
- Cas pratique sectoriel

## Ce qui est compris

- Plateforme MISP configurée (accès lab)
- Jeux de données réels anonymisés
- Templates de rapport CTI

## Prochaines sessions inter-entreprises

| DATES                | LIEU ET FORMAT                   | PLACES   |
|----------------------|----------------------------------|----------|
| 15 - 18 mars 2027    | Paris · Présentiel ou distanciel | 8 places |
| 19 - 22 juillet 2027 | À distance · Distanciel          | 8 places |
| 6 - 9 décembre 2027  | Paris · Présentiel ou 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](mailto: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.