Cybersécurité

Threat Intelligence

A l'issue de la formation, le stagiaire sera capable de mettre en place un service de renseignement sur les menaces de cyber-attaques grâce à la CTI (Cyber Threat Intelligence).

Public visé

- RSSI,
- SOC Manager,
- Analystes SOC,
- Consultant en cybersécurité ou toute personne en charge de la sécurité d'un système d'information d'entreprise.

Les objectifs de la formation

- Comprendre les fondamentaux de la CTI (Cyber Threat Intelligence)
- Savoir collecter et analyser les informations sur les menaces
- Utiliser l'intelligence artificielle (IA) pour automatiser la collecte, l'analyse et la corrélation d'informations liées aux menaces
- Transformer les données en données exploitables
- Intégrer les outils et méthodes de la CTI dans le processus de sécurité de son organisation.

Les prérequis de la formation

- Connaissances de base dans le fonctionnement des systèmes d'information et en cyber sécurité.

Méthodes pédagogiques

- Apports théoriques structurés, illustrés par des exemples concrets et adaptés au contexte professionnel des participants.
- Exercices pratiques et ateliers à chaque étape pour favoriser l'appropriation des connaissances.
- Étude de cas permettant de relier les différents blocs de compétences.
- Forte interaction entre les formateurs et les stagiaires permettant de rendre les échanges plus concrets, en corrélation avec les attentes des stagiaires.
- Documentation pédagogique complète, fournie au format numérique.
- Questionnaire d'évaluation du cours en fin de formation, analysé par notre équipe pédagogique.
- Attestation des compétences acquises transmise au stagiaire à l'issue de la formation.
- Attestation de fin de formation adressée en même temps que la facture à l'entreprise ou à l'organisme financeur,

Programme de la formation

Jour 1 :

- **Matin :** Introduction à la CTI / Concepts & modèles (MITRE ATT&CK, Diamond, Kill Chain) / Typologies de menaces
- **Après-midi :** CTI dans l'organisation (SOC, CERT, RSSI) / Cas pratiques & classification des menaces

Jour 2 :

- **Matin :** Collecte (OSINT, Dark Web, SIEM, EDR) / IoC & IoA
- **Après-midi :** Analyse des TTP / Outils CTI (MISP, YARA, Sigma) / Atelier pratique

Jour 3 :

- **Matin :** Automatisation & IA / Transformation des données / Rapports CTI (RSSI, COMEX, SOC)
- **Après-midi :** Mise en place d'un service CTI / Simulation & restitution / Clôture & attestations