DAWAN

Plan de la formation

www.dawan.fr

Formation Threat Intelligence (Cyber Threat Intelligence)

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 475,00 CHF HT (standard) 1 980,00 CHF HT (remisé)
Public :	RSSI, SOC Manager, analystes SOC, consultants en cybersécurité, toute personne en charge de la sécurité d'un SI
Pré-requis :	Connaissances de base en systèmes d'information et en cybersécurité
Objectifs :	Comprendre les fondamentaux de la Cyber Threat Intelligence (CTI) - Savoir collecter, enrichir et analyser les informations liées aux menaces- Utiliser l'intelligence artificielle et des outils spécialisés pour automatiser la CTI- Transformer les données en renseignement exploitable et actionnable- Intégrer la CTI dans les processus de sécurité de l'organisation
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102769-F

Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre les fondamentaux de la Cyber Threat Intelligence

Définir la CTI et ses objectifs : anticiper, détecter, qualifier et contextualiser les menaces
Identifier les types de CTI : stratégique, tactique, opérationnelle, technique
Comprendre la typologie des menaces et des acteurs malveillants (étatiques, cybercriminalité, hacktivisme, insiders)
Situer la CTI dans l'écosystème SOC, SIEM, gestion des incidents et gestion des risques
Atelier fil rouge : analyser un rapport public de CTI et en extraire les éléments clés pour son organisation

Collecter et enrichir la donnée CTI

Identifier les sources de données : open source, commerciales, communautaires, internes
Comprendre le rôle des IOC (indicateurs de compromission) et des IOA (indicateurs d'attaque)
Mettre en place des flux de collecte : flux de menaces, RSS, API, plateformes de partage (ISAC, MISP, etc.)
Enrichir les données collectées : contexte, relations, pertinence, fiabilité
Atelier fil rouge : construire un flux de collecte simple et enrichir des IOC à partir de sources publiques

Automatiser la CTI avec l'IA et les outils spécialisés

Découvrir les principales plateformes et outils de CTI (TIP, MISP, intégrations SIEM, etc.)
Utiliser l'IA pour automatiser la collecte, la classification et le tri des informations de menace

Mettre en place des workflows d’enrichissement automatique (recherches WHOIS, géolocalisation, réputation IP/domaines)
Relier la CTI aux outils de détection et de réponse (SIEM, EDR, SOAR)
Atelier fil rouge : définir un scénario d’automatisation CTI incluant IA, enrichissement et intégration dans un SIEM ou SOAR

Transformer les données CTI en renseignement exploitable

Analyser et corréler les données de menaces avec les actifs et les vulnérabilités de l’organisation
Élaborer des rapports de CTI adaptés aux différents publics (direction, SOC, équipes réseau/applicatif)
Définir des priorités d’action : durcissement, surveillance ciblée, règles de détection, chasse aux menaces
Mesurer l’impact de la CTI sur la posture de sécurité et la réduction des risques
Atelier fil rouge : produire une fiche de renseignement CTI actionnable à partir d’un jeu de données de menaces

Intégrer la CTI dans les processus de sécurité de l’organisation

Articuler CTI, gestion des incidents, gestion des vulnérabilités et gestion des risques
Mettre en place une boucle d’amélioration continue : collecte, analyse, action, retour d’expérience
Définir les rôles, responsabilités et compétences nécessaires au sein de l’équipe CTI / SOC
Construire un plan de montée en maturité de la CTI pour l’organisation
Atelier fil rouge final : définir une feuille de route CTI sur 12 à 24 mois pour son organisation ou un cas d’école