Présentiel/distanciel

Cyber Threat Intelligence (CTI) Analyser et anticiper les cybermenaces

Objectifs pédagogiques

- Identifier les principales catégories de cybermenaces et les caractéristiques des acteurs associés
- Distinguer les différents niveaux de Cyber Threat Intelligence : stratégique, tactique, opérationnel et technique
- Organiser les différentes étapes du cycle du renseignement en fonction des besoins des parties prenantes
- Collecter, qualifier et contextualiser des informations provenant de différentes sources de Threat Intelligence
- Analyser des indicateurs de compromission et des tactiques, techniques et procédures afin de caractériser une menace
- Définir les principaux composants organisationnels et techniques nécessaires à la mise en place d'une activité CTI
- Exploiter la Threat Intelligence pour améliorer la détection, la réponse aux incidents et le Threat Hunting
- Utiliser les techniques OSINT et le renseignement sur les menaces pour profiler un acteur et contribuer à l'anticipation des risques

Prérequis

- Connaître les principes généraux de fonctionnement d'un système d'information
- Disposer de connaissances de base en cybersécurité, notamment sur les principakes menaces, les mécanismes de détection et la réponse aux incidents

Public concerné

RSSI et responsables de la sécurité des sytèmes d'information, SOC Managers et responsables d'équipes de détection, Analystes threat Intelligence et Threat Hunting, Consultants en cybersécurité et responsables sécurité et professionnels participant à la protection d'un système d'information.

Bénéfices pour les participants

- Disposer d'une vision structurée de la Cyber Threat Intelligence et de ses principaux cas d'usage
- Mieux comprendre les cybermenaces, les acteurs qui le sportent et leurs modes opératoires
- Transformer des informations techniques ou issues de sources ouvertes en renseignement exploitable
- Enrichir les capacités d'un SOC en matière de détection, de réponse aux indidents et de Threat Hunting
- Identifier les principes d'organisation nécesaires à la mise en place d'une activité CTI
- Exploiter la CTI pour éclairer les activités de sécurité, de gestion des risques et d'anticpations

Programme détaillé

Panorama des Cyber Menaces : groupes, individus et codes malveillant (1h30)

- Evolution et diversité des cybermenaces
- Principales motivations : cybercriminalité, espionnages, sabotage, hacktivisme et recherche de gains financiers
- Typologie des acteurs de la menace et niveaux de sophistication
- Chaînes d'attaque et modes opératoires
- Malware, ransomware, exploitation de vulnérabilités, compromission d'identités et attaques sur la chaîne d'approvisionnement
- Notions d'IOC et de TTP
- Lecture d'une attaque à travers le comportement de l'adversaire
- Travail pratique: A partir d'un scénario de cyberattaque, identifier le type de menace, les objectifs probables de l'attaquant, le sprincipales étapes de l'attaque et les informations qui pourraient être utiles à une équipe de sécurité

Définition et introduction à la Cyber Threat Intelligence (CTI) (1h30)

- Définition et finalités de la Cyber Threat Intelligence
- De la donnée brute au renseignement exploitable
- Différences entre information, indicateur, contexte et renseignement
- CTI stratégique, tactique, opérationnelle et technique
- Prinicpaux consommateurs du renseignement au sein de l'organisation
- Cas d'usage : prévention, détection, réponse, Threat Hunting, gestion des risques et anticipation
- Valeur et limites du renseignement sur les menaces
- Travail pratique : Qualifier un ensemble d'informations relatives à une menace et déterminer leur niveau de CTI, les destinataires concernés et les décisions de sécurité qu'elles peuvent alimenter

Cycle de vie du renseignement et parties prenantes (2h00)

- Identification des besoins en renseignement
- Définition des priorités et des questions auxquelles la CTI doit répondre
- Planification et orientation de la collecte
- Collecte des informations
- Traitement, normalisation et enrichissement
- Analyse et contextualisation
- Production et diffusion du renseignement
- Recueil du retour des utilisateurs et amélioration continue
- Identification des parties prenantes : SOC, CERT, RSSI, direction, équipes risques, Red team et métiers
- Adaptation du niveau d'information au destinataire
- Travail pratique : A partir d'une organisation fictive confrontée à plusieurs menaces, définir ses principaux besoins en renseignement puis construire un cycle CTI permettant d'alimenter le SOC, le RSSI et les équipes de gestion des risques

Les principales Sources de renseignement : Techniques et Stratégiques (2h30)

- Sources internes et externes de Threat Intelligence
- Sources ouvertes et techniques OSINT
- Flux et feeds de Threat Intelligence
- CERT, CSIRT, communautés et sources institutionnelles
- Sources commerciales et services spécialisés
- Informations techniques : adresses IP, domaines, URL, empreintes de fichiers et artefacts
- Informations sur les vulnérabilités, campagnes et groupes d'attaquants
- Evaluation de la fiabilité d'une source et de la crédidibilité d'une information
- Corrélation et enrichissement des données
- Gestion de la fraîcheur, du contexte et du risque de faux positifs
- Travail pratique : Analyser plusieurs sources relatives à une même menace, évaluer leur fiabilité, croiser les informations disponibles puis produire une synthèse exploitable par une équipe de cybersécurité

Mettre en place un programme CTI et une organisation au sein de vos équipes (2h00)

- Définition des objectifs et du périmètre d'un programme CTI
- Identification des consommateurs du renseignement
- Formalisation des besoins et priorités
- Organisation des rôles et responsabilités
- Processus de collecte, qualification, analyse et diffusion
- Choix des sources et des outils
- Articulation entre CTI, SOC, CERT, gestion des vulnérabilités, gestion des risques et équipes offensives
- Production de livrables adaptés aux différents interlocuteurs
- Critères permettant d'évaluer la pertinence et l'utilité du renseignement produit
- Principes d'amélioration continue d'une activité CTI
- Travail pratique : Construire le schéma d'organisation d'une cellule CTI pour une entreprise fictive en définissant ses missions, ses interlocuteurs, ses sources, ses principaux livrables et les circuits de diffusion du renseignement

Architecture CTI et Dissémination des IOCs avec une Threat Intelligence Platform (3h00)

- Rôle d'une Threat Intelligence Platform
- Collecte et centralisation des informations
- Normalisation, enrichissement, corrélation et déduplication
- Gestion du cycle de vie des indicateurs
- Qualification et contextualisation des IOC
- Principes de scoring, confiance et priorité
- Découverte de MISP et de ses principaux usages

- Organisation des événements, attributs, objets, taxonomies et relations
- Principes de partage de l'information entre organisations
- Introduction aux formats structurés de Cyber Threat Intelligence
- Principes de STIX et TAXII
- Interconnexion d'une plateforme CTI avec les outils de sécurité
- Diffusion d'indicateurs vers les solutions de détection et d'analyse
- Travail pratique: À partir d'informations relatives à une campagne malveillante, sélectionner et qualifier les IOC pertinents, les enrichir avec leur contexte, définir les règles de partage puis préparer leur exploitation par les outils du SOC

La CTI appliquée au SOC : Détection, Réponse aux incidents et Threat Hunting (3h30)

- Positionnement de la CTI dans les activités du SOC
- Enrichissement des alertes et événements de sécurité
- Priorisation des alertes à partir du contexte de menace
- Utilisation des IOC pour la détection
- Limites d'une approche reposant uniquement sur les IOC
- Analyse des comportements adverses et des TTP
- Exploitation de MITRE ATT&CK pour structurer l'analyse
- Identification des tactiques et techniques associées à une campagne
- Définition d'hypothèses de Threat Hunting
- Recherche proactive de traces d'activité malveillante
- Apport du renseignement dans la qualification et la réponse aux incidents
- Capitalisation sur les incidents afin d'enrichir la connaissance de la menace
- Travail pratique: Analyser un scénario d'intrusion, associer les comportements observés à des tactiques et techniques MITRE ATT&CK, identifier les éléments exploitables par le SOC puis formuler plusieurs hypothèses de Threat Hunting

La CTI appliquée aux équipes d'anticipation : Red Team, Veille et Gestion des Risques (2h30)

- Passer d'une utilisation réactive à une utilisation proactive du renseignement
- Identification des menaces pertinentes pour l'organisation
- Analyse des capacités et intentions des acteurs
- Surveillance des campagnes et évolutions des modes opératoires
- Utilisation du renseignement pour orienter les activités Red Team
- Construction de scénarios d'attaque réalistes à partir des TTP observées
- Contribution de la CTI à l'évaluation des risques cyber
- Identification des actifs, technologies et populations susceptibles d'être ciblés
- Priorisation des actions de sécurité à partir du contexte de menace
- Production d'éléments d'aide à la décision pour les responsables sécurité
- Travail pratique : À partir du profil d'une organisation fictive et d'informations concernant plusieurs groupes d'attaquants, identifier les menaces les plus pertinentes, sélectionner les scénarios à tester et proposer des priorités de surveillance et de réduction des risques

La CTI appliquée aux investigations OSINT et au profilage d'acteurs de la Menace (2h30)

- Positionnement de l'OSINT dans une démarche de Threat Intelligence
- Méthodologie de recherche et de collecte
- Recherche sur les infrastructures, domaines et ressources Internet
- Recherche d'informations sur les campagnes et les groupes d'attaquants
- Recoupement et validation des informations collectées
- Identification des relations entre infrastructures, outils, campagnes et acteurs
- Analyse des TTP et des récurrences comportementales
- Construction d'un profil d'acteur de la menace
- Gestion des incertitudes et niveaux de confiance
- Limites de l'attribution d'une cyberattaque
- Présentation et restitution des résultats d'une investigation
- Travail pratique : Réaliser une investigation guidée à partir d'un jeu d'informations concernant une campagne fictive, recouper les sources, identifier les relations pertinentes, caractériser les TTP observées et produire une fiche synthétique de profil de menace

Présentiel/distanciel

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes, le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation