+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 03/10/2024

S'inscrire

Formation OpenCTI

2 jours (14 heures)

Présentation

OpenCTI est une plateforme open-source dédiée au renseignement sur les cybermenaces. Elle permet la collecte, l'analyse et la visualisation des menaces. Grâce à cette technologie, les organisations peuvent comprendre et anticiper les cyberattaques.

Pendant ce cours, vous apprendrez à utiliser OpenCTI pour centraliser et structurer des informations sur les cybermenaces, créer des liens entre différentes sources, visualiser les relations entre les menaces et automatiser l'intégration avec d'autres outils de sécurité.

Vous découvrirez aussi les concepts clés de la Threat Intelligence, tels que les indicateurs de compromission (IoCs), les tactiques, techniques et procédures (TTPs), et la gestion des incidents en utilisant OpenCTI. Vous verrez comment structurer et enrichir les données de menaces.

Grâce à cette formation, vous maîtriserez la gestion du renseignement sur les cybermenaces, l'automatisation des processus de sécurité et l'analyse des cyberattaques. Vous développerez des compétences en visualisation des données, en collaboration entre équipes et en anticipation des risques.

Cette formation vous sera animée avec les dernières nouveautés concernant l'outil OpenCTI.

Objectifs

- Comprendre les bases de la Cyber Threat Intelligence (CTI) avec OpenCTI
- Utiliser les tableaux de bord et fonctionnalités de recherche sur OpenCTI
- Analyser et pivoter entre les données pour découvrir des menaces et relations
- Gérer et configurer OpenCTI pour une haute disponibilité et performance
- Appliquer des techniques de troubleshooting pour résoudre les problèmes

Public visé

- Administrateurs réseau
- **Développeurs**
- Professionnels de la sécurité informatique

Pré-requis

- Connaissance de Linux
- Une bonne compréhension des concepts réseau (TCP/IP, DNS, DHCP, etc.) est nécessaire
- Connaissance de langages comme Python, Bash ou PowerShell
- Expérience en sécurité informatique

PROGRAMME DE NOTRE FORMATION OpenCTI

INTRODUCTION à OpenCTI

- Qu'est-ce qu'OpenCTI ?
- Initiation aux bases de la CTI (Cyber Threat Intelligence)
- Approche et utilisation
- Modèle de données
- Discussion sur l'importance de l'intelligence de menaces cybernétiques

EN-TÊTE DE PLATEFORME

- Recherche d'informations spécifiques
- Tableaux de bord personnalisés
- Aperçu de l'enquête
- Profil de l'utilisateur et abonnements

EXPLORATION DES DONNÉES ET PIVOTS

- Tableau de bord de l'organisation
- Analyse
  - Rapports
  - Regroupement
- Évènements
  - Relations et pivots de la connaissance
  - Observations
  - Données observées
- Observations
  - Observables
  - Artéfacts
  - Infrastructures

- Menaces
  - Acteurs de la menace
  - Déductions des connaissances
  - Ensembles d'intrusions
  - Campagnes
- Arsenal
  - Malwares
  - Outils
  - Vulnérabilités

GESTION AVANCÉE DE LA PLATEFORME

- Techniques avancées pour la gestion et la surveillance d'OpenCTI
- Configuration et gestion d'un environnement clusterisé pour la haute disponibilité
- Optimisation des indices Elasticsearch et gestion du rollover
- Installation et configuration d'un serveur de cartographie local pour les données géospatiales
- Surveillance de la performance et ajustements en temps réel

RÉSOLUTION DE PROBLÈMES

- Méthodologies de troubleshooting pour identifier et résoudre les problèmes courants
- Gestion des incidents et récupération après erreur
- Analyse des logs pour le diagnostic des problèmes
- Conseils pour maintenir la stabilité et la performance de la plateforme
- Utilisation des forums, de la documentation et du support d'OpenCTI pour résoudre les problèmes

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.