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

Mis à jour le 15/11/2024

S'inscrire

Formation Tracecat

2 jours (14 heures)

Présentation

Tracecat est une technologie open-source qui vise à automatiser la sécurité, la personaliser à l'infini grace à l'intégration au Workflow. Elle permet aux ingenieurs et aux professionels de la sécurité de comprendre et maîtriser l'automatisation de leurs playbooks.

Ce cours couvre les fonctionnalités de Tracecat, telles que l'installation et la configuration de l'outil, l'intégration avec Docker Compose pour créer vos premiers playbooks. Nous aborderons les meilleures pratiques pour déployer les playbooks de manière sécurisée, en tirant parti du YAML pour simplifier le processus de création.

Vous apprendrez à utiliser le Control flow via les conditions du Workflow, comment activer des Workflows à travers des plannings et des Webhooks, et à encadrer les migrations de données en toute sécurité.

À la fin de la formation, vous maîtriserez la création des Playbooks, l'utilisation avancée de Tracecat pour la gestion du Workflow, ainsi que la gestion et la sécurisation des données sensibles.

Notre formation se basera sur la dernière version de la technologie : Tracecat v 0.13.

Objectifs

- Maîtriser les fondamentaux et avantages de Tracecat pour la gestion du Workflow
- Installer et configurer Docker avec Docker Compose en suivant les meilleures pratiques de sécurité
- Intégrer Tracecat et utiliser les Workflow pour la gestion des playbooks
- Personnaliser les playbooks et les intégrer au Workflow
- Configurer Tracecat pour automatiser la gestion de vos playbooks

Public visé

- Développeurs
- Ingénieur en sécurité
- Administrateurs réseau
- Administrateurs système
- DevOps

Pré-requis

- Connaissances premières de docker et Doker Compose
- Familiarité avec le système des playbooks
- Compétences en langage de programmation Python, YAML
- Accès à un environnement Docker pour installer Tracecat

PROGRAMME DE NOTRE FORMATION TRACECAT

INTRODUCTION À TRACECAT

- Qu'est ce Tracecat ?
- Pourquoi l'utiliser ?
- Fonctionnalités de base
  - Actions
  - Secrets
  - Expressions
  - Fonctions

INSTALLATION ET CONFIGURATION

- Étapes détaillées pour l'installation de Tracecat
- Configuration initiale et intégration avec dockers
- Utilisation de Docker Compose pour simplifier le déploiement de Tracecat
- Configuration de l'environnement de développement pour Tracecat
- Bonnes pratiques de sécurité lors de l'installation et de la configuration

INTÉGRATION AVEC DOCKER

- Présentation de DOCKER et du rôle de Tracecat
- Configuration de Tracecat pour travailler avec Docker
- Comprendre les métriques essentielles fournies par Tracecat
- Création et complexification des playbooks grâce aux YAML
- Exercices pratiques de configuration et de visualisation

UTILISATION DE L'INTERFACE UTILISATEUR

- Navigation dans l'interface utilisateur Tracecat
- Comprendre les différents outils et leurs utilisations dans Tracecat
- Créations de différents playbooks selon les besoins spécifiques
- modification et intégration grâce aux pyton et YAML
- Gestion des alertes et notifications

UTILISATION DE TRACECAT

- Apprendre à utiliser le CONTROL FLOW selon les conditions du WORKFLOW
- Utilisation de Tracecat pour combiner un Smaller-WORKFLOW avec un Single-WORKFLOW
- Comprendre comment activer des WORKFLOW à travers des plannings et des webhooks
- Ajouts et intégration personnalisé au registre d'action
- Découvrir comment actualiser et gérer les migrations de données en toute sécurité

COMPRENDRE LA PRINCIPALE FONCTIONNALITÉ DE TRACECAT

- Construction des « blocks » pour une meilleure automatisation du Workflow
- Stocker et récupérer des données sensibles
- Référencement des métadonnées d'action et de résultat dans le Workflow

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.