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

Mis à jour le 26/06/2025

S'inscrire

Formation Falco

3 jours (21 heures)

Présentation

Notre formation Falco vous permettra de sécuriser efficacement vos environnements Linux et Kubernetes en mettant en œuvre une surveillance comportementale en temps réel. Vous apprendrez à détecter et à réagir aux intrusions ou comportements suspects grâce à un moteur de règles puissant et personnalisable, intégré nativement dans les workflows DevSecOps modernes.

Vous découvrirez les fondements de la sécurité runtime, le fonctionnement de Falco, ses différents drivers et sa capacité à intercepter les appels système critiques pour générer des alertes contextuelles et précises. La sécurité s'adapte dynamiquement à vos workloads, sans les alourdir.

La formation vous initiera également à l'écosystème Falco étendu : intégration des alertes via Falcosidekick, visualisation dans Grafana ou ELK, gestion centralisée avec falcoctl, et surveillance avancée via des plugins.

Vous serez formé au packaging natif avec GraalVM, au déploiement Docker/K8s, et à l'observabilité via Prometheus, Grafana et OpenTelemetry.

Comme pour toutes nos formations, elle se déroulera sur ma toute dernière version de Falco

Objectifs

- Savoir installer et configurer Falco sur un système Linux ou un cluster Kubernetes en choisissant le driver adapté
- Comprendre l'architecture de Falco, le rôle du moteur de règles, et le fonctionnement de la capture d'événements système en temps réel
- Maîtriser l'écriture, la personnalisation et l'optimisation de règles Falco pour détecter des comportements suspects dans un environnement cloud-native
- Intégrer Falco avec des outils d'alerte et d'observabilité comme Falcosidekick, Slack, Prometheus, Grafana ou Elasticsearch, pour une supervision unifiée

- Mettre en œuvre une stratégie de sécurité runtime dans Kubernetes, incluant la détection d’intrusions, la réduction des faux positifs et l’analyse post-incident
- Automatiser la gestion des règles et plugins via falcoctl et valider la robustesse de la configuration à travers un atelier pratique en environnement simulé d’attaque

Public visé

- Ingénieurs DevOps
- Administrateurs système
- Analystes sécurité

Pré-requis

- Connaissances de base en ligne de commande Linux

Programme de la formation Falco

Introduction à Falco et à la Sécurité Runtime

- Définitions : sécurité pré-déploiement vs post-déploiement
- Limites des solutions traditionnelles dans Kubernetes
- Pourquoi la surveillance en temps réel est critique
- Historique : de Sysdig à la CNCF
- Positionnement par rapport à d’autres outils
- Cas d’usage concrets

Architecture et Fonctionnement de Falco

- Falco Engine
- Falco Rules
- Kernel Driver
- Falcosidekick
- Interception des appels système
- Pipeline d’analyse
- Génération d’alertes

Installation de Falco

- Via packages, Docker, ou compilation

- Vérification du support du noyau
- Helm chart officiel
- Mode DaemonSet
- Pré-requis
- Avantages / Inconvénients de chaque approche
- Vérification de compatibilité avec votre distribution

Règles Falco – Écriture, Compréhension, Personnalisation

- Structure YAML d’une règle
- Champs rule, desc, condition, output, priority
- Champs disponibles : proc.name, fd.name, user.name, etc.
- Opérateurs logiques et expressions personnalisées
- Niveaux : EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFO, DEBUG
- Mapping avec des politiques de sécurité
- Héritage de règles
- Création de règles spécifiques à un environnement
- Validation des règles personnalisées

Cas pratiques de règles et détections

- Ouverture de shell dans un conteneur
- Accès à des fichiers sensibles
- Utilisation de commandes réseau
- Escalade de privilèges suspecte
- Génération d'événements manuellement
- Visualisation des logs
- Debug des règles

Intégration de Falco dans un SI

- Présentation de l’outil
- Configuration de la redirection des alertes
- Intégration avec :
- Slack / Discord / Teams
- Webhook
- Prometheus / Grafana
- Elasticsearch / Logstash / Kibana
- Meilleures pratiques pour l’export
- Structuration des messages JSON
- Interprétation dans Kibana ou Grafana Loki

Utilisation avancée de Falco

- Cas d’usage : capture S3, audit logs Kubernetes, etc.
- Gestion via falcoctl
- Impact des règles sur les performances
- Filtrage avancé pour éviter les faux positifs
- Alertes "silencieuses"

Bonnes pratiques et sécurité

- Analyse comportementale
- Affinage progressif des règles
- Tests sur environnements de préprod
- Mise à jour du noyau et impact sur Falco
- Maintenance des règles
- Utilisation de sources communautaires
- OPA / Kyverno / PodSecurityPolicies
- Sécurité réseau
- Journalisation complète avec Falco + AuditD

Détection d'une attaque en environnement Kubernetes

- Déploiement d’un cluster vulnérable
- Simulation d’attaque
- Identifier les règles qui ont détecté l’attaque
- Comprendre la chaîne de détection et d’alerte
- Corriger ou renforcer les règles en conséquence

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.