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

Mis à jour le 05/06/2026

S'inscrire

Formation Tetragon

3 jours (21 heures)

Présentation

Tetragon est une solution de sécurité runtime basée sur eBPF pour les environnements Kubernetes, Linux et cloud native.

Cette plateforme d'observabilité sécurité permet de surveiller les processus, les accès fichiers, l'activité réseau et les appels système directement au niveau du kernel.

Notre formation Tetragon vous permettra de maîtriser la détection des menaces et l'enforcement runtime en exploitant les événements enrichis par le contexte Kubernetes.

Vous apprendrez à installer Tetragon, configurer ses composants, analyser les événements processus et créer vos propres Tracing Policies pour détecter des comportements suspects.

À l'issue de la formation, vous serez en mesure de déployer Tetragon dans un cluster Kubernetes, d'exporter ses événements vers vos outils sécurité, d'appliquer des règles de réponse et de construire une stratégie d'observabilité sécurité cloud native.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le fonctionnement de Tetragon et son usage avec eBPF
- Installer et configurer Tetragon dans un environnement Kubernetes
- Analyser les événements processus, fichiers, réseau et syscalls
- Créer des Tracing Policies adaptées aux cas d'usage sécurité
- Mettre en place des règles de détection et d'enforcement runtime
- Intégrer les événements Tetragon dans une chaîne SOC, SIEM ou observabilité

Public visé

- Ingénieurs sécurité et DevSecOps
- Administrateurs Kubernetes
- Ingénieurs SRE et plateformes
- Analystes SOC orientés cloud native
- Architectes cloud et infrastructure

Pré-requis

- Connaissances de base en Kubernetes
- Notions d'administration Linux
- Compréhension générale de la cybersécurité et des environnements cloud native
- Des bases sur les conteneurs et Docker sont recommandées

Pré-requis techniques

- Disposer d'un poste avec Linux, macOS ou Windows avec WSL2
- Avoir les droits d'installation nécessaires sur son poste
- Installer Docker ou un runtime conteneur équivalent
- Disposer d'un cluster Kubernetes local ou distant, par exemple kind, minikube ou un cluster managé
- Installer kubectl, Helm et un éditeur de code
- Prévoir une connexion Internet stable

Formation Tetragon

[Jour 1 - Matin]

Comprendre Tetragon, eBPF et la sécurité runtime

- Comprendre le rôle de Tetragon dans une stratégie de sécurité runtime
- Identifier les limites des approches classiques : logs applicatifs, agents userspace, SIEM seul
- Découvrir les apports d'eBPF pour l'observabilité kernel et la détection temps réel
- Comprendre les événements surveillés : process_exec, syscalls, fichiers, réseau et privilèges
- Positionner Tetragon dans un environnement Kubernetes, cloud native et DevSecOps
- Atelier pratique : installer Tetragon sur un cluster de test et observer les premiers événements

[Jour 1 - Après-midi]

Architecture, installation et premiers événements

- Comprendre l’architecture de Tetragon : agent, capteurs, export, gRPC et CLI tetra
- Installer Tetragon avec Helm dans un cluster Kubernetes
- Configurer les composants, namespaces, DaemonSet et paramètres de base
- Manipuler les événements JSON et les formats de sortie compact ou détaillé
- Identifier les métadonnées Kubernetes : namespace, pod, conteneur, labels et node
- Diagnostiquer les erreurs d’installation et valider le bon fonctionnement du déploiement

Observation des processus et activités système

- Analyser les événements de cycle de vie des processus avec process_exec et process_exit
- Suivre les commandes exécutées dans les conteneurs et sur les nœuds
- Repérer les comportements suspects : shells interactifs, exécutions depuis /tmp, outils réseau
- Corréler les événements processus avec les workloads Kubernetes
- Définir une première grille de lecture pour les signaux faibles de compromission
- Atelier pratique : détecter des exécutions anormales dans un pod Kubernetes

[Jour 2 - Matin]

Tracing Policies et détection personnalisée

- Comprendre la structure des Tracing Policies Tetragon
- Définir des règles de détection sur événements kernel, fichiers, processus et arguments
- Utiliser le filtrage in-kernel pour réduire le bruit et améliorer les performances
- Construire des politiques adaptées aux workloads critiques
- Tester, versionner et déboguer les politiques de détection
- Atelier pratique : écrire une Tracing Policy pour détecter l’accès à un fichier sensible

[Jour 2 - Après-midi]

Détection de menaces cloud native

- Identifier les scénarios d’attaque courants dans Kubernetes : shell, escape, reconnaissance, exfiltration
- Détecter les changements de privilèges, capabilities et namespaces Linux
- Observer les accès réseau suspects et les outils utilisés en post-exploitation
- Mettre en relation les événements Tetragon avec les tactiques MITRE ATT&CK
- Prioriser les alertes selon criticité, contexte Kubernetes et exposition du workload
- Atelier pratique : simuler un comportement d’attaque et produire une alerte exploitable

Runtime enforcement et réponses immédiates

- Comprendre les capacités d’enforcement runtime de Tetragon
- Différencier observation, filtrage, alerte, blocage et action de réponse
- Configurer des politiques pour restreindre certaines exécutions ou accès sensibles
- Réduire le risque de TOCTOU grâce à l’application de règles au niveau kernel
- Définir une stratégie progressive entre mode audit et mode enforcement
- Atelier pratique : bloquer l’exécution d’un binaire non autorisé dans un conteneur

[Jour 3 - Matin]

Export, observabilité et intégration SOC

- Comprendre les formats d’export : JSON, fichiers, gRPC et intégrations externes
- Envoyer les événements vers des outils d’observabilité ou de centralisation
- Structurer les événements pour une exploitation par un SIEM ou un SOC
- Construire des dashboards de suivi : processus, fichiers, réseau, workloads et alertes
- Réduire le bruit avec des filtres, labels Kubernetes et règles de priorisation
- Atelier pratique : exporter les événements Tetragon vers une chaîne d’analyse sécurité

[Jour 3 - Après-midi]

Performance, durcissement et exploitation

- Comprendre l’impact des politiques sur la performance et le volume d’événements
- Appliquer les bonnes pratiques de filtrage pour limiter la surcharge
- Surveiller l’état de Tetragon, les métriques, les logs et les erreurs runtime
- Sécuriser le déploiement : RBAC, namespaces, accès gRPC et séparation des rôles
- Mettre en place une stratégie de maintenance, upgrade et validation des policies
- Élaborer une checklist de mise en production pour un cluster Kubernetes

Gouvernance, cas final et industrialisation

- Définir une gouvernance des politiques de détection et d’enforcement
- Intégrer Tetragon dans un workflow DevSecOps et GitOps
- Organiser la collaboration entre équipes sécurité, SRE, plateforme et SOC
- Documenter les cas d’usage : investigation, détection, blocage et conformité
- Construire une trajectoire d’adoption progressive sur plusieurs clusters
- Atelier pratique : créer un scénario complet de détection, alerte, enforcement et reporting

Pour aller plus loin

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.