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

Mis à jour le 23/01/2025

S'inscrire

Formation Zeek

3 jours (21 heures)

Présentation

Notre formation Zeek vous enseignera la maîtrise du nécessaire pour détecter, identifier et endiguer toutes les intrusions. Notre programme couvre l'ensemble des fonctionnalités de l'outil afin que vous puissiez efficacement analyser et traiter les cyberattaques.

Dans ce cours, vous apprendrez tout d'abord à identifier les intrusions avec Zeek et la sécurisation de votre environnement informatique . À travers une démonstration pratique, vous apprendrez à optimiser, intégrer et gérer Zeek en production.

Vous découvrirez les bonnes pratiques d'usage, la gestion des rôles, des logs, et des flux de travail. L'automatisation et l'orchestration de la réponse aux menaces grâce à Zeek.

Comme pour toutes nos formations, nous vous présenterons la dernière version du logiciel : Zeek V7.1.0

Objectifs

- Comprendre le rôle de Zeek dans la cybersécurité
- Les logs générés par Zeek
- Le langage de script Zeek
- Optimisation des performances dans les environnements à fort trafic
- domaines malveillants
- Création de scripts pour personnaliser les alertes et analyses

Public visé

- **Analystes Cybersécurité**
- Analystes SOC
- Ingénieur en sécurité
- Administrateur Réseau

Pré-requis

Connaissances de base des réseaux et des systèmes.

Programme de la formation Zeek

INTRODUCTION À ZEEK

- Comprendre le rôle de Zeek dans la cybersécurité
- Fonctionnement de Zeek : architecture et composants
- Différences entre Zeek et d'autres IDS comme Snot ou Suricata
- Concepts de base : événements, logs, scripts
- Surveillance des réseaux, détection des menaces

Installation et configuration de Zeek

- Pré-requis système et configurations matérielles
- Installation sur Linux et déploiement sur un réseau
- Configuration initiale et fichiers principaux de Zeek
- Surveillance passive : paramétrage des interfaces réseau
- Vérification et tests post-installation

Analyse des logs générés par Zeek

- Logs générés pas Zeek
  - HTTP
  - DNS
  - SSL
  - Logs de connexion
- Compréhension des champs importants dans les logs
- Extraction d'informations critiques pour la sécurité
- Méthodes d’identification des anomalies dans les logs
- Gestion des volumes de logs

Le scripting avec Zeek

- Le langage de script Zeek
- Syntaxe et logique du scripting pour Zeek
- Création de scripts pour personnaliser les alertes et analyses
- Gestion des événements et détection de menaces spécifiques
- Frameworks intégrés
  - Notice
  - Intel

Détection avancée des menaces

- Surveillance avancée des protocoles réseau
- Détection d’anomalies réseau et d’exfiltrations de données
- Identification des menaces via les connexions chiffrées SSL/TLS
- Utilisation de listes noires d’adresses IP
- domaines malveillants
- Détection des scans de port et d'activités suspectes

Optimisation et intégration de Zeek

- Optimisation des performances dans les environnements à fort trafic
- Tuning des paramètres réseau pour améliorer l'efficacité
- Intégration avec des outils tiers
  - Elastic Stack
  - Splunk
  - SIEMs
- Automatisation avec des scripts externes
  - Python
  - Make
- Export des données Zeek pour des analyses externes

Sécurisation et gestion de Zeek en production

- Gestion des mises à jour et de la maintenance
- Surveiller la disponibilité et la santé des instances Zeek
- Implémentation d’une stratégie de sauvegarde des configurations
- Mise en conformité avec les normes GDPR, ISO 27001

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.