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

Mis à jour le 12/06/2026

S'inscrire

Formation Watchguard Endpoint Security Essential

2 jours (14 heures)

Présentation

WatchGuard Endpoint Security est une solution de protection des postes et serveurs permettant de prévenir, détecter, investiguer et remédier aux menaces ciblant les endpoints. Elle combine protection antivirus, détection comportementale, EDR, contrôle applicatif, supervision et réponse aux incidents.

Notre formation WatchGuard Endpoint Security Essentials vous permettra de maîtriser les fondamentaux du déploiement, de la configuration et de l'exploitation d'une solution de sécurité endpoint WatchGuard.

Vous apprendrez à administrer la console cloud, organiser les machines, déployer les agents, configurer les politiques de sécurité et adapter les protections aux postes utilisateurs, serveurs et profils sensibles.

À l'issue de cette formation, vous serez en mesure d'analyser les alertes, d'investiguer un incident endpoint, d'isoler une machine compromise, de mettre en œuvre des actions de remédiation et d'exploiter les tableaux de bord de supervision.

Cette formation aborde également les bonnes pratiques de durcissement endpoint, de contrôle applicatif, de gestion des exclusions, de reporting, d'exploitation quotidienne et de collaboration avec les équipes SOC ou cybersécurité.

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

Objectifs

- Comprendre l'architecture et les usages de WatchGuard Endpoint Security

- Déployer les agents et organiser les machines, groupes et politiques
- Configurer les protections antivirus, EDR, contrôle applicatif et sécurité web
- Analyser les alertes, événements, comportements suspects et incidents endpoint
- Mettre en œuvre les actions de réponse : quarantaine, blocage, isolation et remédiation
- Exploiter les tableaux de bord, rapports et bonnes pratiques d’administration

Public visé

- Administrateurs systèmes
- Administrateurs sécurité
- Analystes cybersécurité
- Analystes SOC
- Responsables sécurité
- Équipes IT chargées de la protection des postes et serveurs

Pré-requis

- Connaissances générales en administration systèmes
- Notions de base en cybersécurité et protection endpoint
- Compréhension générale des malwares, alertes de sécurité et incidents IT

Pré-requis techniques

- Disposer d’un ordinateur avec navigateur web récent
- Prévoir une connexion Internet stable

Programme de notre formation WatchGuard Endpoint Security Essentials

[Jour 1 - Matin]

Découvrir WatchGuard Endpoint Security

- Comprendre le rôle de WatchGuard Endpoint Security dans une stratégie de protection des postes et serveurs
- Différencier les approches EPP, EDR, EPDR et Advanced EPDR
- Identifier les menaces ciblant les endpoints : malwares, ransomwares, scripts, phishing et comportements suspects
- Découvrir la console d’administration cloud, les tableaux de bord et les principaux modules de sécurité
- Comprendre le cycle de protection : prévention, détection, investigation, containment et remédiation
- Atelier pratique : explorer la console WatchGuard Endpoint Security, identifier les protections actives et analyser l’état du parc

[Jour 1 - Après-midi]

Déploiement des agents et politiques de sécurité

- Préparer le déploiement des agents sur postes utilisateurs et serveurs
- Organiser les groupes, profils, machines, utilisateurs et politiques de sécurité
- Configurer les protections antivirus, antimalware, anti-exploit et protection comportementale
- Mettre en place le contrôle des applications, périphériques, scripts et accès web
- Adapter les politiques selon les profils : postes bureautiques, serveurs, utilisateurs sensibles et télétravail
- Atelier pratique : créer une politique de sécurité endpoint, l'appliquer à un groupe de machines et vérifier son déploiement

Prévention des menaces et durcissement endpoint

- Comprendre les mécanismes de prévention contre les ransomwares, malwares inconnus et attaques fileless
- Configurer les exclusions, listes d'autorisation, blocages et règles de contrôle applicatif
- Réduire la surface d'attaque sur les postes et serveurs
- Gérer les mises à jour, signatures, moteurs de détection et paramètres de protection
- Éviter les erreurs fréquentes : politiques trop permissives, exclusions excessives et absence de segmentation des profils
- Appliquer une checklist de durcissement pour les endpoints critiques

[Jour 2 - Matin]

Détection, alertes et investigation EDR

- Comprendre le fonctionnement de la détection EDR et de l'analyse comportementale
- Analyser les alertes, événements, processus, fichiers, connexions réseau et actions suspectes
- Prioriser les incidents selon leur criticité, leur contexte et les actifs impactés
- Investiguer une alerte endpoint : chronologie, indicateurs, machine concernée et actions utilisateur
- Identifier les signaux d'attaque : exécution inhabituelle, persistance, élévation de privilèges et mouvement latéral
- Atelier pratique : analyser une alerte de sécurité, reconstituer la chronologie d'un incident et qualifier son niveau de risque

[Jour 2 - Après-midi]

Réponse aux incidents et remédiation

- Mettre en œuvre les actions de réponse : quarantaine, suppression, blocage, isolation et restauration
- Isoler un poste compromis pour limiter la propagation d'une menace

- Gérer les faux positifs, exceptions, éléments restaurés et décisions de remédiation
- Documenter un incident endpoint et préparer les éléments utiles aux équipes sécurité
- Définir un processus de réponse adapté aux environnements postes, serveurs et télétravail
- Atelier pratique : traiter un incident endpoint de bout en bout, depuis l’alerte jusqu’à la remédiation

Supervision, reporting et bonnes pratiques d’exploitation

- Exploiter les tableaux de bord pour suivre l’état de sécurité du parc endpoint
- Créer des rapports sur les menaces, incidents, machines vulnérables et actions de remédiation
- Mettre en place une routine d’exploitation : revue des alertes, exceptions, politiques et postes non conformes
- Aligner WatchGuard Endpoint Security avec les pratiques SOC, ITSM et réponse aux incidents
- Définir les bonnes pratiques d’administration : rôles, accès, journalisation, mises à jour et gouvernance
- Atelier pratique : construire un tableau de suivi endpoint et définir une checklist d’exploitation quotidienne

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.