

Mis à jour le 29/09/2026

S'inscrire

Formation Strategy One : création de tableaux de bord

2 jours (14 heures)

Présentation

SentinelOne Singularity Endpoint est une plateforme de protection des postes de travail et serveurs combinant EPP, EDR, détection comportementale et réponse automatisée. Elle permet de détecter, analyser et contenir les menaces tout en centralisant la supervision des endpoints depuis une console unique.

Notre formation SentinelOne vous permettra de maîtriser les mécanismes essentiels de déploiement, d'administration et d'investigation avec SentinelOne Singularity Endpoint.

Vous apprendrez à déployer et configurer les agents SentinelOne, à organiser les endpoints, à définir les politiques de protection et à superviser l'état de sécurité des postes de travail et serveurs.

Vous saurez analyser les menaces avec Storyline, appliquer des actions de confinement et de remédiation, puis exploiter Deep Visibility pour mener des investigations avancées et des opérations de Threat Hunting.

À l'issue de la formation, vous serez en mesure d'administrer un environnement SentinelOne, d'analyser une chaîne d'attaque, de répondre aux incidents et d'améliorer la visibilité sur les actifs grâce à Singularity Network Discovery.

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

Objectifs

- Comprendre l'architecture et les principales fonctionnalités de SentinelOne Singularity Endpoint
- Déployer, configurer et administrer les agents SentinelOne sur les endpoints
- Configurer les politiques de protection et superviser l'état de sécurité du parc
- Analyser les menaces et les chaînes d'attaque avec Storyline
- Mener des investigations et des opérations de Threat Hunting avec Deep Visibility
- Mettre en oeuvre les actions de confinement, de remédiation et de réponse aux incidents

Public visé

- Administrateur système
- Administrateur sécurité
- Analyste SOC
- Ingénieur cybersécurité
- Responsable de la protection des endpoints

Pré-requis

- Connaissances générales en administration des systèmes Windows, Linux ou macOS
- Compréhension des principes fondamentaux de la cybersécurité
- Notions sur les logiciels malveillants, les attaques réseau et la réponse aux incidents

Pré-requis techniques

- Poste sous Windows 11, Linux ou macOS avec droits administrateur
- Au moins 8 Go de RAM, 16 Go recommandés pour les exercices de laboratoire
- Navigateur récent permettant l'accès à la console SentinelOne Singularity
- Connexion Internet stable permettant l'accès à l'environnement de laboratoire fourni

Programme de notre formation SentinelOne

[Jour 1 - Matin]

Déploiement et administration de SentinelOne Singularity Endpoint

- Présentation de la plateforme SentinelOne Singularity et positionnement des fonctions EPP, EDR et de réponse automatisée
- Architecture de Singularity Endpoint, rôle de la console de management et fonctionnement de l'agent SentinelOne
- Organisation des environnements, sites, groupes et endpoints dans la console d'administration
- Déploiement et gestion des agents sur les postes de travail et serveurs Windows, macOS et Linux
- Configuration des politiques de protection, paramètres de sécurité, exclusions et stratégies de mise à jour
- Atelier pratique : prendre en main la console, déployer un agent sur un endpoint et appliquer une politique de protection adaptée.

[Jour 1 - Après-midi]

Détection, analyse et réponse aux menaces

- Comprendre les mécanismes de détection par Static AI et Behavioral AI et leur utilisation face aux logiciels malveillants et attaques sans fichier
- Analyser les alertes, événements et indicateurs de compromission remontés par la plateforme
- Exploiter Storyline pour visualiser les processus, événements et relations constituant une chaîne d'attaque
- Utiliser les actions de réponse : arrêt de processus, quarantaine, remédiation, isolation réseau et résolution des incidents
- Comprendre le fonctionnement du Rollback pour restaurer les modifications provoquées par certaines attaques et ransomwares
- Atelier pratique : analyser une menace détectée avec Storyline, identifier son origine puis appliquer les actions de confinement et de remédiation appropriées.

[Jour 2 - Matin]

Investigation avancée et Threat Hunting avec Deep Visibility

- Découvrir Deep Visibility et les données de télémétrie collectées sur les endpoints
- Construire des recherches pour retrouver processus, fichiers, connexions réseau, utilisateurs et événements suspects
- Utiliser les informations contextuelles de Storyline pour reconstituer le déroulement complet d'une attaque
- Identifier les techniques adverses et exploiter les correspondances avec le référentiel MITRE ATT&CK
- Mettre en œuvre une démarche de Threat Hunting à partir d'indicateurs, comportements et hypothèses de compromission
- Atelier pratique : mener une investigation avec Deep Visibility, reconstruire une chaîne d'attaque et identifier les endpoints potentiellement compromis.

[Jour 2 - Après-midi]

Exploitation, supervision et sécurisation avancée de la plateforme

- Administrer les politiques de sécurité, exclusions, contrôles de périphériques et paramètres opérationnels à l'échelle du parc
- Découvrir Singularity Network Discovery pour identifier les équipements présents sur le réseau et repérer les actifs non protégés
- Utiliser les fonctions de contrôle et d'isolation pour limiter les communications avec des équipements non autorisés
- Superviser l'état des agents, la couverture du parc, les incidents et les événements de sécurité depuis la console
- Découvrir les possibilités d'intégration de SentinelOne avec les outils SIEM, les solutions tierces et l'écosystème Singularity

- Atelier pratique : contrôler la couverture d'un parc, identifier un équipement non protégé et construire un scénario complet de détection, investigation et réponse.

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.