Change Auditor Threat Detection

Détection proactive des menaces en environnement Microsoft

La plupart des organisations utilisent Active Directory comme source principale d'authentification et d'autorisation, ce qui en fait une cible de choix pour les pirates, les cyberterroristes et les anciens collaborateurs mécontents. Les organisations ne savent pas toujours que la sécurité d'Active Directory peut être mise en péril de l'intérieur, par des utilisateurs agissant sciemment ou involontairement. De plus, la complexité d'Active Directory rend extrêmement difficile l'identification des menaces qui surviennent. Les méthodes classiques de détection des menaces basées sur des règles génèrent tant d'alertes qu'il est impossible de toutes les analyser : vous risquez de passer à côté des véritables menaces et de laisser l'entreprise à la merci de failles de sécurité des données. Comment analysez-vous en temps réel toutes les activités des utilisateurs de votre environnement pour protéger votre entreprise contre les interruptions et les pannes ?

Change Auditor Threat Detection est une méthode unique de détection des menaces liées aux utilisateurs : la modélisation du comportement individuel des utilisateurs permet de détecter les activités anormales qui peuvent indiquer des utilisateurs suspects ou le piratage de comptes. Change Auditor Threat Detection analyse les activités des utilisateurs en utilisant l'apprentissage automatique avancé, l'analyse des comportements des utilisateurs et des entités (UEBA), et des algorithmes d'évaluation complexes. Ainsi il classe les utilisateurs de l'organisation en fonction des risques qu'ils présentent, identifie les menaces potentielles liées aux utilisateurs et réduit les faux positifs. Vous allez enfin pouvoir combler les lacunes laissées par les outils d'audit natifs et protéger l'ensemble de votre environnement.

FONCTIONNALITÉS

Analyse des journaux d'audit en temps réel

Analysez efficacement un volume élevé de données d'audit en temps réel, notamment les modifications d'Active Directory,

Change Auditor Threat Detection permet de détecter rapidement et facilement les activités suspectes des utilisateurs pour assurer la sécurité de votre environnement et des utilisateurs.

AVANTAGES :

- Détection proactive des menaces en fonction de modèles de référence des comportements des utilisateurs
- Réduction du nombre d'alertes associées à la détection des menaces basée sur des règles
- Visualisation des alertes de sécurité en contexte pour déterminer rapidement et facilement leur gravité
- Détecter facilement les actions anormales d'un utilisateur par rapport à la base de référence de son comportement habituel
- Identifier les menaces à partir de vos données d'audit existantes pour limiter l'impact sur votre infrastructure

CAS D'UTILISATION :

Change Auditor Threat Detection permet de découvrir rapidement et facilement les menaces, notamment :

- Activité anormale dans Active Directory
- Utilisation détournée de comptes à privilèges
- Attaques par force brute
- Exfiltration de données
- Accès inapproprié au système ou aux ressources
- Logiciels malveillants
- Élévation des privilèges
- Mouvement latéral

CONFIGURATION SYSTÈME REQUISE

CHANGE AUDITOR COORDINATEUR

(composant côté serveur)

Processeur : équivalent ou supérieur à un processeur quatre cœurs Intel Core i7

Mémoire : minimum 8 Go de RAM (recommandé : 32 Go ou plus)

CHANGE AUDITOR CLIENT

(composant côté client)

Processeur : équivalent ou supérieur à un processeur double cœur Intel Core i5

Mémoire : minimum 4 Go de RAM (recommandé : 8 Go ou plus)

CHANGE AUDITOR AGENT

(composant côté serveur)

Processeur : équivalent ou supérieur à un processeur double cœur Intel Core i5

Mémoire : minimum 4 Go de RAM (recommandé : 8 Go ou plus)

Pour obtenir la liste détaillée à jour des configurations requises, consultez le site support.quest.com/change-auditor

les authentifications et les activités effectuées sur les fichiers. Créez des bases de référence sur les utilisateurs à partir de ces données d'activités brutes afin de détecter de manière proactive les comportements inhabituels des utilisateurs et identifier immédiatement des activités suspectes potentielles.

Analyse automatisée du comportement des utilisateurs (UEBA)

Modélisez les activités des utilisateurs automatiquement, sans besoin de saisie ou de configuration de la part de l'administrateur. Les bases de référence des comportements des utilisateurs sont automatiquement créées via un apprentissage machine avancé non supervisé, en modélisant tous les aspects des activités de chaque utilisateur, notamment ses modèles de connexion, ses activités d'administration et ses accès aux dossiers.

Détection sophistiquée des comportements inhabituels

Identifiez les activités anormales des utilisateurs en comparant automatiquement chaque action de l'utilisateur avec la base de référence de son comportement. La détection sophistiquée d'indicateurs de menaces et la notation des risques à plusieurs niveaux permettent de signaler uniquement les anomalies flagrantes qui représentant des comportements risqués des utilisateurs.

Détection des menaces basée sur des modèles

Les alertes SMART relatives aux menaces liées aux utilisateurs sont déclenchées uniquement en cas de détection d'un modèle corrélé de comportement anormal d'un utilisateur. Au lieu d'utiliser des règles pour détecter des activités particulières, analysez automatiquement toutes les activités des utilisateurs au fur et à mesure qu'elles se produisent et identifiez les utilisateurs suspects de l'environnement au moyen d'une détection sophistiquée. La modélisation globale sophistiquée permet de signaler uniquement les comportements inhabituels et inquiétants des utilisateurs, et ainsi de réduire de manière significative les faux positifs et les activités isolées normales.

Analyse précise des comportements des utilisateurs

Change Auditor crée les journaux d'audit qui alimentent les analyses. Ainsi, toutes les données d'événements brutes utilisées pour la détection proactive des menaces dans votre environnement fournissent des informations essentielles et pertinentes, notamment :

- Qui a effectué la modification ?
- Qu'est-ce qui a été modifié ?
- Quand a été effectuée la modification ?
- Où a été effectuée la modification ?
- Adresse IP ou station de travail d'où provient la modification

Contrairement aux journaux d'événements natifs de Windows, Change Auditor permet de détecter toutes les actions importantes des utilisateurs et donc d'éviter les lacunes dans l'analyse des comportements des utilisateurs.

Alertes de sécurité en contexte

Visualisez toutes les alertes liées aux activités suspectes des utilisateurs dans le contexte des indicateurs de menaces découverts dans le cadre de l'alerte. Chaque comportement inhabituel est présenté dans le contexte de l'activité de la base de référence de l'utilisateur et avec tous les événements bruts qui ont déclenché l'alerte, pour indiquer clairement la raison du déclenchement de l'alerte et simplifier l'enquête et le suivi.

Outil léger de détection des menaces liées aux utilisateurs

Exploitez votre infrastructure Change Auditor existante et les données d'audit pour modéliser le comportement des utilisateurs, et ainsi éviter le déploiement d'agents et de serveurs supplémentaires inutilement lourds. La seule infrastructure supplémentaire requise pour permettre l'analyse avancée des menaces liées aux utilisateurs est une simple appliance virtuelle.

PROFIL DE QUEST

L'objectif de Quest est de résoudre des problèmes complexes avec des solutions simples. Nous y parvenons en restant fidèles à notre philosophie qui repose sur l'excellence de nos produits, un service de qualité et un objectif global de simplicité dans nos interactions. Notre vision est de proposer une technologie qui apporte à la fois efficacité et résultats concrets afin de permettre à votre entreprise de libérer du temps en gestion informatique pour se consacrer davantage à l'innovation.

Quest
www.quest.com/fr
Si vous n'êtes pas situé en Amérique du Nord, vous trouverez des informations concernant notre bureau local sur notre site Web.

DataSheet-ChangeAuditorThreatDetection-US-KS-FR-WL-32855