FICHE SOLUTION

Détecter et répondre aux menaces internes : FortiSIEM de Fortinet avec fonction UEBA

Synthèse

L'identification et la prise en charge des menaces résultant de collaborateurs internes, négligents ou malveillants, constituent un défi complexe pour les entreprises. Les risques associés aux utilisateurs au sein d'une organisation peuvent créer une zone d'ombre importante en termes de cybersécurité et de conformité. La transition vers des applications cloud et la migration rapide vers le télétravail suite à la pandémie du COVID-19 ont réduit la visibilité et pèsent sur la capacité des fonctions de sécurité traditionnelles à repérer les activités suspectes des collaborateurs.

"Le coût total moyen d'une menace interne ressort à $11,45 millions. La fréquence des menaces internes a triplé depuis 2016."[1]

FortiSIEM de Fortinet répond à ces défis qui pèsent sur les centres opérationnels de sécurité (SOC). Notre plateforme SIEM (security information and event management) offre une visibilité en temps réel sur l'ensemble de l'écosystème IT. De plus, la fonction UEBA (user and entity behavior analytics ou traitement analytique des données comportementales des utilisateurs et entités) assure la recherche des menaces avancées. Grâce au monitoring des terminaux (endpoints) et au traitement analytique des données comportementales, les entreprises sont outillées pour détecter et gérer les comportements utilisateurs à risque, ceux susceptibles de nuire aux données métiers.

Une visibilité précise

Les entreprises doivent relever un certain nombre de défis pour bénéficier d'une visibilité sur l'activité des stations de travail des utilisateurs et identifier les comportements utilisateurs indésirables. FortiSIEM UEBA, basé sur la technologie éprouvée et mature FortiInsight, répond à ces défis de manière efficace et non intrusive.

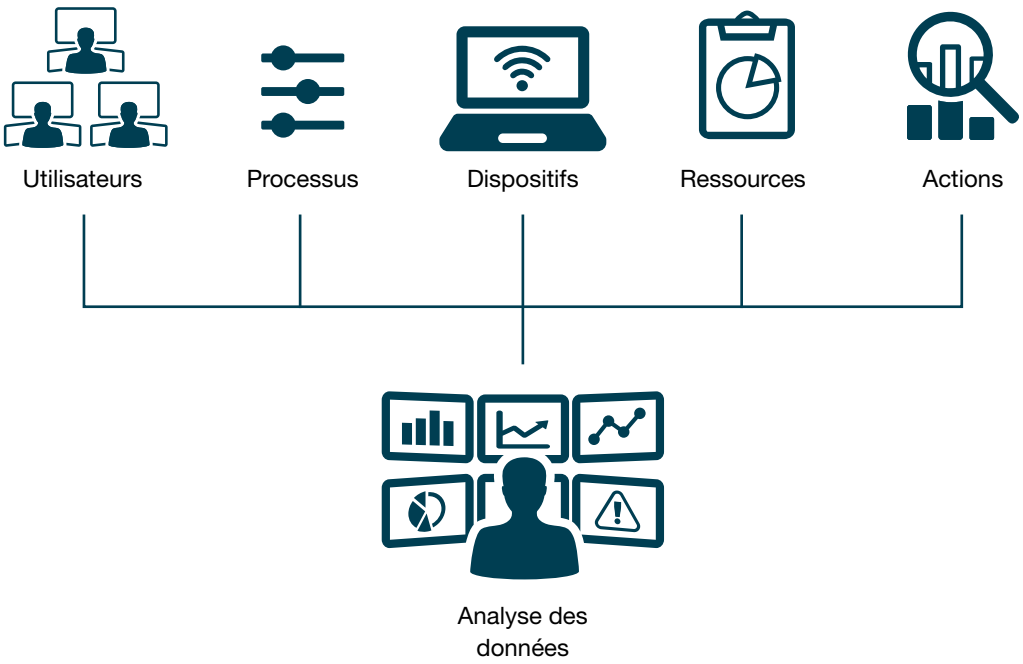
FortiSIEM UEBA, simple à utiliser, collabore avec FortiSIEM pour assurer un monitoring de bout en bout des activités des serveurs, du réseau et des services cloud. FortiSIEM propose une visibilité en temps réel et décisionnelle sur les comportements utilisateurs suspects, vis-à-vis des données critiques. Ceci permet un profiling pertinent des utilisateurs, des applications, des fichiers, des terminaux et des réseaux. Nombre d'avantages sont au rendez-vous, parmi lesquels :

- **Une visibilité sur les terminaux.** Bénéficiez d'une visibilité intégrale sur les flux de données (sur et hors du réseau), grâce à des informations essentielles sur les comportements des utilisateurs mais aussi des terminaux.
- **Une sécurité fédérée.** Attribuez des identifiants et des mots de passe spécifiques à chaque collaborateur, pour faciliter les tâches d'alertes et de réponse aux incidents.
- **Reporting de conformité.** Tirez parti d'un reporting qui assure votre conformité réglementaire, avec le RGPD (Règlement Général sur la Protection des Données) notamment.
- **Visualisation et tableaux de bord.** Visualisez les données essentielles associées aux utilisateurs, processus, terminaux, types de ressources (fichiers, bases de données, applications) et comportements.
- **Analyses post-incident.** Suivez l'ensemble des activités des utilisateurs et des terminaux pour accélérer et affiner la prise en charge des incidents de sécurité potentiels ou avérés. Ceci est essentiel à la réponse aux incidents et pour faciliter le respect de certaines contraintes réglementaires, à l'instar de la notification des incidents de sécurité sous 72 heures, comme le stipule le RGPD.

Détecter les menaces connues et inconnues

FortiSIEM UEBA identifie les menaces connues et inconnues : erreurs de la part d'utilisateurs, transgression de règles, activité malveillante d'utilisateurs, piratage de compte et détournement de compte par des intrus. La solution tire parti d'un machine learning puissant et flexible et propose un rapport d'audit sur les actions des utilisateurs. Ceci offre une visibilité totale au cœur des activités affectant les données d'une entreprise, grâce à un monitoring du comportement des utilisateurs et du mouvement des données, sur et hors du réseau.

FortiSIEM examine le comportement des utilisateurs vis-à-vis des données (accès inhabituel des utilisateurs à des fichiers) ou les changements dans les méthodes de travail, ainsi que les comptes compromis ou les actions inhabituelles de certains profils d'utilisateurs. Lorsque de tels comportements sont identifiés, des alertes en temps réel sont envoyées aux parties prenantes impliquées pour déclencher une investigation.



Mode opératoire

Le moteur FortiSIEM UEBA s'exécute sur FortiSIEM Supervisor et recueille des données à partir des machines des utilisateurs finaux, via l'agent FortiSIEM UEBA. Cet agent collecte automatiquement des logs fiables et s'assure de la pertinence de ces données, avec un minimum d'impact sur les dispositifs clients. Une solution utilisant un agent offre également une visibilité sur l'utilisation des clés USB et peut recueillir des données même si un client n'est pas connecté au réseau corporate. Cette activité off-net peut être mise en cache en local sur le client à des fins d'analyses ultérieures, ou une fonction de recueil FortiSIEM peut être déployée dans une zone DMZ pour que les agents off-net y téléchargent leurs données dès qu'ils disposent à nouveau d'une connexion à Internet.

Comme illustré ci-dessous, l'agent UEBA FortiSIEM recueille des données fiables, sur et hors du réseau, sur la base de cinq facteurs. Les informations suivantes sont utilisées pour comprendre le comportement des utilisateurs :

- Utilisateurs
- Processus
- Dispositifs
- Ressources
- Actions

Les avantages clés de FortiSIEM :

- Une visibilité en temps réel et décisionnelle
- Une réponse accélérée aux incidents
- Une veille centralisée
- Une maîtrise du nombre de faux-positifs
- Une protection intégrale

Un monitoring qui préserve la confidentialité des collaborateurs

FortiSIEM UEBA n'est pas intrusif. La solution ne permet pas d'enregistrer les frappes au clavier, les copies d'écran ou les logs détaillés d'activité, autant d'actions que certaines entreprises trouveraient problématiques. L'agent enregistre l'interaction des utilisateurs avec les ressources (fichiers) sur la machine, et offre la capacité de :

- Surveiller les utilisateurs, les processus et les accès aux fichiers sur les PC portables, pour faciliter les investigations sur les activités des utilisateurs et assurer l'identification des menaces
- Identifier toute activité liée à une menace interne
- Enregistrer les transferts de données vers des clés USB
- Identifier et surveiller l'utilisation d'applications spécifiques sur les terminaux
- Identifier et surveiller des noms spécifiques de fichiers comme :
  - Des noms de fichiers qui indiqueraient la présence de données confidentielles (DonnéesClients.csv par exemple)
  - Des noms de fichiers associés à des médias potentiellement indésirables (mp3, avi, mpg)
  - Des noms de fichiers présentant un certain risque (passwords.txt)
- Des alertes en cas de détection de comportement utilisateur malveillants

Sécurité intégrale du réseau

FortiSIEM UEBA prévient les menaces internes grâce à un monitoring permanent des utilisateurs et des terminaux et des fonctions automatisées de détection et de réponse aux menaces. La solution identifie automatiquement les comportements non-conformes, suspects ou anormaux (sur et hors du réseau) et lance des alertes le cas échéant. En tirant parti du machine learning et d'un traitement analytique sophistiqué, notre approche proactive à la détection des menaces offre davantage de protection et de visibilité sur l'ensemble du réseau.

[1] Larry Ponemon, "Gaining Insight Into the Ponemon Institute's 2020 Cost of Insider Threats Report," Security Intelligence, 27 janvier 2020.

FORTINET

www.fortinet.fr

mars 2, 2021 11:08 AM

779872-0-1-FR

sb-fortiSIEM-A4_FR