SECURITE

Keenai SOC
L'assistant de vos équipes cyberdéfense

SOFTWARE

LE CONTEXTE

La croissance du Système d'Information de l'entreprise entraîne la génération d'un volume important d'informations d'activité et de sécurité. Ces informations constituent autant de sources de données pour évaluer le niveau de sécurité et détecter tout type de menaces.

Face à l'augmentation exponentielle des informations à analyser pour une équipe SOC, les outils traditionnels n'ont pas les capacités pour traiter ces données en temps réel.

Davantage d'équipements, davantage de données et de flux : **comment faciliter l'analyse et accélérer la prise de décision des experts sécurité au quotidien ?**

Soutenue par l'état francais

SUPERVISION *Temps réel*

CYBERSÉCURITÉ **Réferentiel PDIS**

Correlation *Big Data*

Active Learning

L'OFFRE GFI

Notre pôle cybersécurité conçoit, commercialise et intègre **des solutions de gestion et de supervision de la sécurité du SI de type SIEM.**

Nos solutions permettent, à partir des informations d'activité et de sécurité des équipements et des applications (les logs), d'analyser en temps réel le niveau de sécurité du SI, notamment grâce à la corrélation d'évènements.

Fort de notre expertise et des retours d'expérience d'utilisateurs sur nos solutions, nous avons conçu **Keenaï SOC** pour répondre aux 4 fondamentaux suivants :

- Tirer parti d'un volume croissant de données
- Identifier les comportements suspects
- Optimiser l'analyse en gardant le contrôle
- Adopter les exigences d'un référentiel reconnu

Tirer parti d'un volume croissant de données

Les logs comme les flux échangés constituent les éléments représentatifs de l'activité de votre SI. Afin de faciliter le traitement de ces données et d'anticiper la croissance de votre Système d'Information, **Keenaï SOC** utilise les technologies Big Data optimisées pour l'analyse de log.

Les principaux avantages :

• Des **performances de traitement en temps réel** inégalées : grâce aux traitements parallélisés de cette plateforme, les opérations de recherche et de stockage d'information sont ultra performantes.

• Une **capacité de stockage extensible facilement : Keenaï SOC** stocke les logs dans leur intégralité, vous permettant une traçabilité accrue.

Votre contact : marketing.software@gfi.fr

Gfi Informatique - La Porte du Parc -145 bd Victor Hugo - 93400 Saint-Ouen - RCS : 385 365 713 - Tél. 01 44 04 50 00

Facebook : facebook.com/gfiinformatique | **Twitter** : twitter.com/gfiinformatique | **Linkedin** : linkd.in/gfiinformatique | **Youtube** : bit.ly/youtubeGfi

Identifier les comportements suspects

Les outils de détection d'incidents traditionnels sont performants pour les attaques connues. Pour couvrir les attaques inconnues, **Keenaï SOC** intègre des algorithmes de Machine Learning dédiés à la détection de comportements malveillants. Ces algorithmes analysent le comportement des utilisateurs, qualifient ce comportement par rapport à des métriques définies afin d'identifier des divergences.

Optimiser l'analyse en gardant le contrôle : l'Active Learning

Les divergences de comportement détectées précédemment sont proposées à l'expert sécurité du SIEM pour qu'il qualifie la normalité du comportement.

Keenaï SOC prend en compte le retour de l'expert pour enrichir sa méthodologie d'analyse.

L'expert sécurité se concentre sur les incidents de sécurité, plutôt que sur la configuration d'un outil de détection.

Adopter les exigences d'un référentiel reconnu

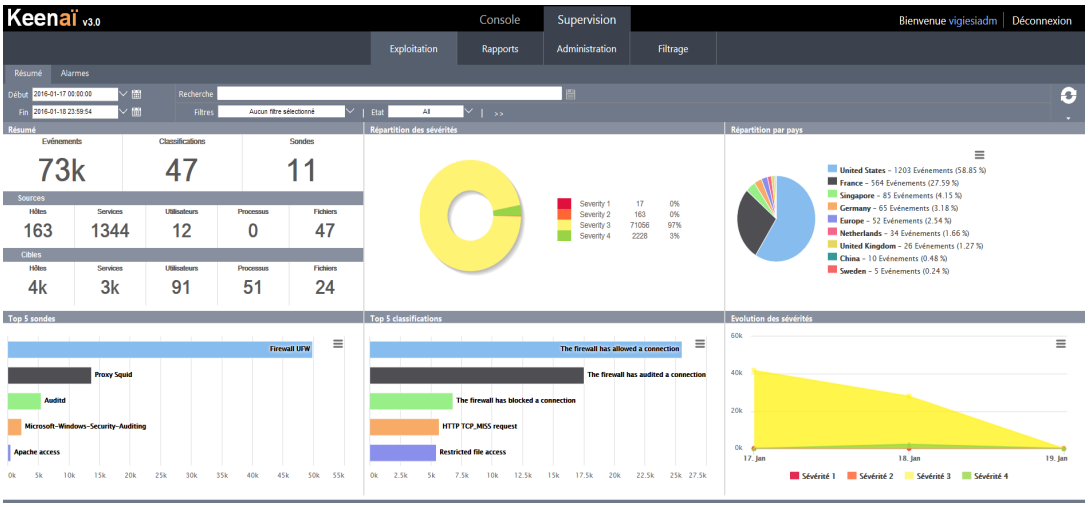
L'ANSSI a défini un cadre concernant les prestataires et prestations de détection d'incidents de sécurité : le référentiel PDIS (Prestataires de Détection d'Incidents de Sécurité).

C'est un modèle de référence pour la supervision de la sécurité des OIV (Opérateurs d'Importance Vitale) qui peut également être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire.

Afin de détecter au plus tôt les tentatives d'attaques, le système de corrélation et d'analyse des logs mis en œuvre dans **Keenaï SOC** s'appuie sur les catégories suivantes du référentiel PDIS :

- Architecture
- Liste des attaques à detecter à minima
- Indicateurs clés

La prise en compte de ces exigences définies par le PDIS vous garantit un haut niveau de qualité des fonctionnalités et de la méthodologie offertes par **Keenaï SOC.**



GFI PRESENT DANS LE TOP 10 DES EDITEURS FRANCAIS

Aujourd'hui, ce sont plus de **3 000 clients** qui nous font confiance et qui bénéficient de notre expertise métier depuis plus de 30 ans. La fiabilité de nos solutions et nos innovations participent à leurs projets de transformation.

Au-delà de l'édition de solutions SIEM, nous offrons des services sur-mesure : audit, conseil, formation, intégration et offres co-managées.

Votre contact : marketing.software@gfi.fr

Gfi Informatique - La Porte du Parc -145 bd Victor Hugo - 93400 Saint-Ouen - RCS : 385 365 713 - Tél. 01 44 04 50 00
Facebook : facebook.com/gfiinformatique | **Twitter** : twitter.com/gfiinformatique | **Linkedin** : linkd.in/gfiinformatique | **Youtube** : bit.ly/youtubeGfi

OCTOBRE 2017