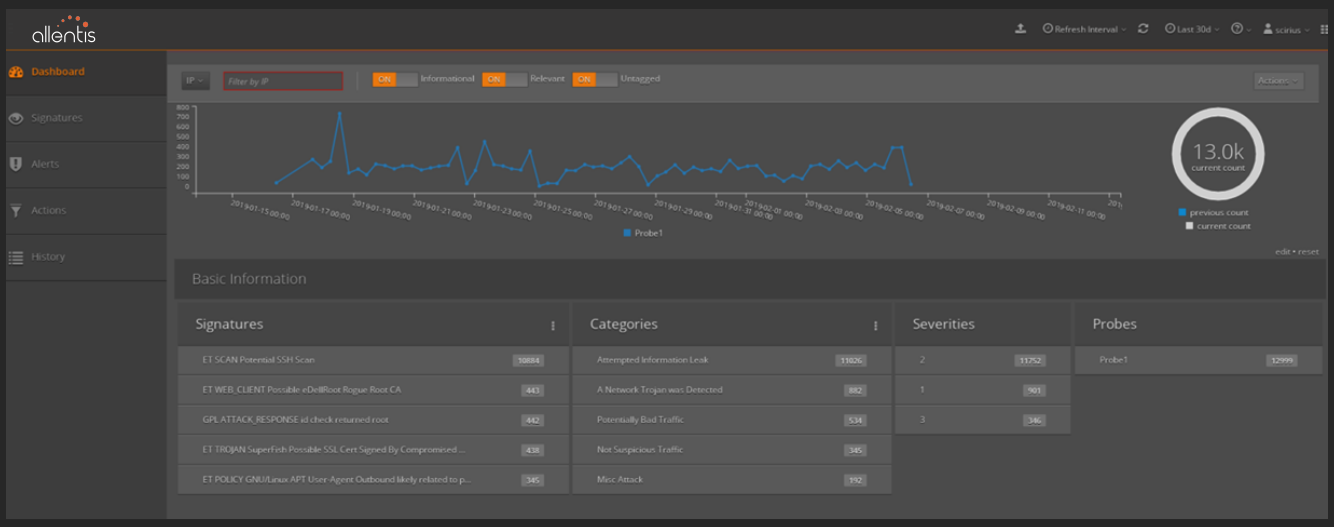
Qe-Secure

La gestion des évènements de sécurité en toute simplicité

Qe-Secure est un système de détection de menaces développé en France par allentis afin de répondre aux besoins exprimés par la Loi de programmation militaire (LPM) aussi bien qu'aux attentes des entreprises et organismes souhaitant se protéger de manière simple et performante des attaques en réseau.

La solution bénéficie de l'expérience d'allentis dans la conception des sondes d'analyse. Elle se distingue notamment par une ergonomie optimale, une interface utilisateur intuitive permettant un gain de temps élevé dans la compréhension des évènements de sécurité.



Une solution évolutive

Qe-Secure comporte une ou plusieurs sondes QESEC en communication avec un serveur QEMAN. Cette architecture permet de centraliser en un point la gestion des évènements de sécurité générés par plusieurs sondes réparties sur l'infrastructure, et d'adapter la configuration de surveillance en fonction des évolutions du réseau.

Traquer les menaces sur leurs chemins d'accès habituels

Les sondes QESEC sont connectées via des systèmes de réplication de trafic aux artères critiques de l'infrastructure de réseau. Elles voient et décodent le trafic dans lequel les menaces se dissimulent, puis elles génèrent des évènements de sécurité issus de l'application de règles d'analyse. Elles procèdent à l'extraction sélective des fichiers pour leur analyse par le manager QEMAN.

Accélérer la recherche et la compréhension

Le manager QEMAN dispose d'un mécanisme exclusif de *tagging* et de filtrage des évènements. Avec QEMAN la mise en évidence des évènements les plus critiques est instantanée et leur compréhension est tout aussi rapide.

Les fonctions intégrées de transformation des règles d'analyse permettent l'optimisation de ces dernières en les adaptant au mieux à l'environnement surveillé.

Support natif des SIEM

Qe-Secure s'interface en quelques clics à IBM QRadar ou à Splunk ainsi qu'à la plupart des outils tiers du marché. Les évènements taggés ou non par Qe-Secure sont transmis au SIEM permettant ainsi un post-traitement différencié. Cependant l'ergonomie et les moyens de recherche offerts par QEMAN permettent aux équipes de sécurité d'atteindre un haut niveau d'efficacité même en l'absence de SIEM.

Qualification élémentaire de l'ANSSI

La solution Qe-Secure a obtenu la qualification élémentaire à l'ANSSI pour la version 2.1.X, 100 Mb/s, 500 Mb/s et 1Gb/s afin de permettre aux Opérateurs d'Importance Vitale de s'équiper dans le cadre de leur mise en conformité avec la LPM. Elle pourra ainsi être mise en œuvre notamment avec les produits de réplication (boîtiers TAP Tapics™) d'allentis déjà qualifiés élémentaire par l'ANSSI et avec les agrégateurs de trafic proposés par allentis.

Accompagner dans la durée

L'expérience unique d'allentis dans le déploiement et le support de vastes configurations de sondes permet de bénéficier d'un accompagnement complet des projets. Depuis leur phase d'étude et d'architecture, puis de déploiement, de configuration et d'optimisation jusqu'à la maintenance et au support H24 7/7, allentis fait bénéficier ses clients du plus haut standard de niveau de service. Chaque utilisateur de Qe-Secure bénéficie d'un accès direct à l'assistance allentis.

PRINCIPALES CARACTERISTIQUES DE QE-SECURE

Architecture modulaire et évolutive Manager et Sondes	√
Manager et Sondes livrées clé en main matériel + logiciel intégré + règles de détection	√
Interface intuitive	√
Sécurisation des rôles (opérateur, administrateur distant, administrateur local)	√
Gestion complète des *ruleset* et des sources depuis IHM intuitive	√
Gestion des règles par opérateur autorisé depuis IHM intuitive	√
Support débit jusquà 10 G	√
Tagging configurable et temps réel des évènements (*informational*, *relevant*, *untagged*)	√
Filtrage d'affichage par forage sur toutes les données présentées (évite l'utilisation de menus)	√
Extraction sélective des fichiers pour analyse	√
Traitement intelligent des évènements évitant l'utilisation d'un SIEM	√

A PROPOS D'ALLENTIS

allentis est une PME française spécialisée dans les systèmes de contrôle de la performance et de la sécurité des échanges en réseau de flux de données. Elle a conçu et fabrique les systèmes QE d'analyse de flux (Qe-Secure pour la détection de menaces, Qe-Streams et Qe-Flows pour l'analyse de performances et la cartographie des flux, Qe-Packets pour la capture massive de données, Qualevent pour l'hypervision métier), et la gamme TAPICS de composants réseau pour la réplication et l'isolation de trafic.

allentis
info@allentis.eu
www.allentis.eu