

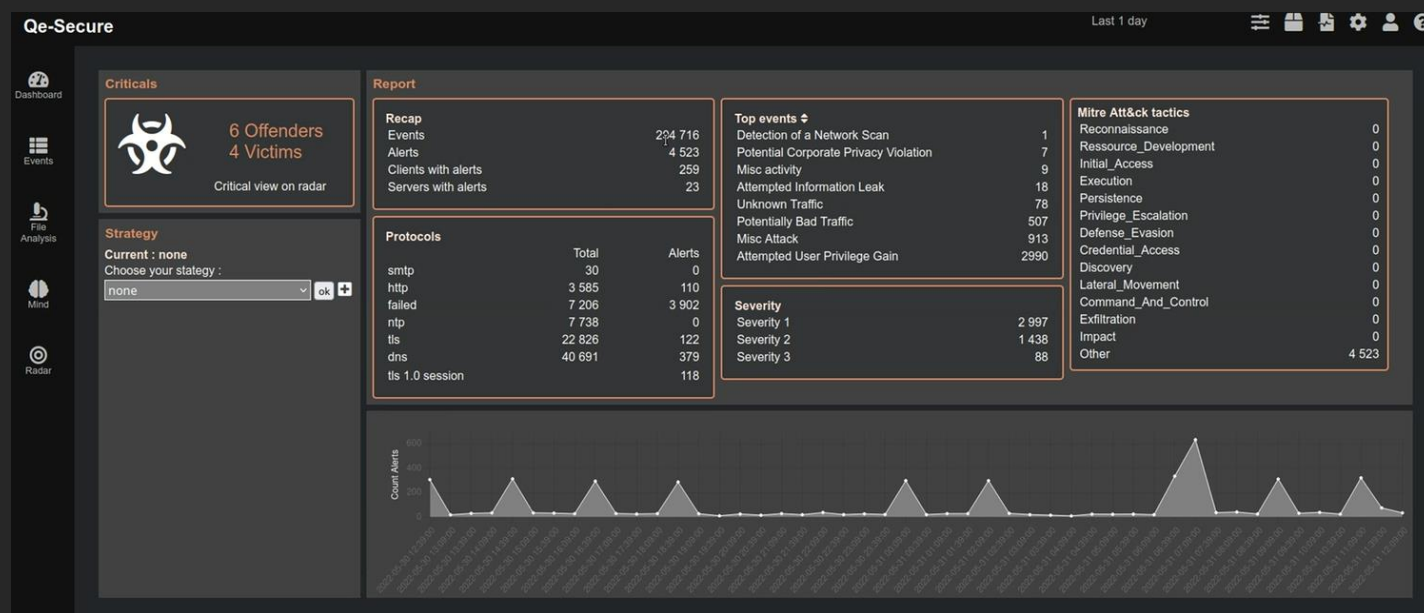
# Qe-Secure

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-NG. 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-NG.

## Accélérer la recherche et la compréhension

Le manager OEMAN-NG dispose d'un mécanisme de gestion de stratégies de détection. Ce procédé permet de concentrer le travail d'analyse en fonction de besoins et contextes particuliers. Avec OEMAN-NG la mise en évidence des événements les plus critiques est instantanée et leur compréhension est tout aussi rapide. Le module d'intelligence artificielle Qe-Mind permet de générer des événements de sécurité même en cas de signaux faibles non détectés par les moteurs de règles. La présentation graphique des schémas d'attaque permet un gain de temps important dans l'analyse des situations.

## 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 événements filtrés 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 OEMAN-NG permettent aux équipes de sécurité d'atteindre un haut niveau d'efficacité même en l'absence de SIEM.

## Labellisation France Cyber Security

La solution Qe-Secure a obtenu la qualification élémentaire de l'ANSSI pour la version 2.1.X, ainsi que le label France Cyber Security, afin de permettre notamment 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) 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 la 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 e évolutive Manager et Sondes	✓
Manager et Sondes livrées clés en main matériel + logiciel intégré + règles de détection	✓
IHM intuitive - Filtrage d'affichage par forage sur toutes les données présentées (évite l'utilisation de menus)	✓
Sécurisation des rôles (opérateur, administrateur distant, administrateur local)	✓
Gestion complète des règles et des sources depuis IHM	✓
Gestion des règles par opérateur autorisé depuis IHM	✓
Support débit jusqu'à 10 G	✓
Gestion de stratégies de détection	✓
Module d'intelligence artificielle Qe-Mind	✓
Présentation graphique des schémas d'attaque	✓
Traitement intelligent des événements évitant l'utilisation d'un SIEM	✓

## A PROPOS D'ALLENIS

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 fabriqué 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 WAN, SD-WAN et LAN, 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**