

Q1LABS

Description de la solution :

QRadar est un outil évolué et complet de surveillance de la sécurité et de protection des réseaux basé sur l'analyse comportementale temps réel des trafics. Développé par la société Q1 Labs, le nom « Qradar » est un acronyme de Q1 Labs Real-time Anomalie Détection and Résolution. Qradar est un « écran radar » de surveillance, d'analyse et de contrôle des infrastructures réseaux.

Les produits Q1LABS :

-

QRADAR

Les besoins :

QRADAR permet de suivre le comportement des systèmes, applications et utilisateurs, et, de détecter instantanément les anomalies engendrées par des failles de sécurité, des violations de règles, des usages illicites des réseaux et des dysfonctionnements d'équipements.

Les atouts de la solution :

Le mécanisme de détection temps réel d'anomalies est basé sur la comparaison entre la matrice dynamique des trafics et le profil comportemental « normal » de cette matrice. En parallèle QRadar collecte les événements (Logs) provenant de tous types d'équipements (composants réseau, produits de sécurité, serveurs et applications). Il normalise ces événements et les corrèle avec les trafics.

Couplé au module optionnel QRadar-ICX, QRadar agit en tant que système de Détection et de Prévention des intrusions couvrant l'ensemble du réseau de l'entreprise et s'affranchissant de tout délai entre la naissance d'une faille et la mise en oeuvre de sa détection.

