

## Q1LABS « DÉMOCRATISE » LES TECHNOLOGIES SIEM

*Q1Labs « démocratise » les technologies SIEM et Risk Management, souligne Agostinho Rodrigues, Directeur des nouvelles technologies Interdata. Avec son offre QRadar, les entreprises disposent d'une meilleure visibilité sur leur SI et sont en mesure de détecter les écarts de « comportement » par rapport à leur politique de sécurité.*



Agostinho Rodrigues

### **GS Mag : Quels impacts aurait cette législation sur la corrélation de logs et la gestion de risque ?**

**Agostinho Rodrigues :** Face aux nouvelles contraintes imposées par la proposition de loi, les entreprises doivent renforcer la protection des données traitées par des systèmes capables de détecter les fuites de données et notifier toute vulnérabilité connue, présentant un risque de divulgation ou d'utilisation frauduleuse des données personnelles.

En pratique, pour les entreprises, cela se traduit par une capacité à :

- Mesurer le niveau de risque (résiduel) associé aux données personnelles, et l'impact des vulnérabilités sur le SI.
- Assurer une protection dynamique des données sensibles contre d'éventuelles malveillances.
- Rechercher tous les événements associés à une attaque ou fuite de données, et fournir des rapports détaillés sur le contexte et circonstances d'un tel événement.
- Conserver les traces des événements concernés, en assurant leur intégrité.

### **GS Mag : Ainsi, comment se positionne votre offre ?**

**Agostinho Rodrigues :** La solution Q1Labs s'articule autour de 3 fonctions clés :

- Gestion centralisée et corrélation des événements de sécurité (SIEM), basée sur l'analyse des logs sur l'ensemble du système d'information,
  - Traçabilité des activités sur le réseau et accès aux applications, basée sur l'analyse des « flows » jusqu'au niveau 7,
  - Gestion des risques et identification des failles au niveau des équipements de sécurité, basée sur l'audit et l'analyse des configurations et règles (firewall, routeurs...).
- Elle se caractérise par une intégration unique des fonctions d'analyse et corrélation des événements et des « flows » dans sa configuration SIEM, qui sont capables de coopérer avec l'application « Risk Manager ».

### **GS Mag : Comment répond-elle techniquement aux attentes des RSSI ?**

**Agostinho Rodrigues :** L'offre Qradar apporte de nombreux bénéfices aux entreprises soucieuses de mieux contrôler la sécurité et la protection des données. La philosophie de Q1Labs a toujours été de développer des produits « clés-en-main », à la fois performants, efficaces mais surtout simples et rapides à déployer. Cela contraste avec les solutions SIEM traditionnelles, qui ont souvent été perçues comme des « usines à gaz » complexes à configurer.

Les appliances QRadar sont livrées en standard avec de très nombreuses règles de corrélation, adaptées à tous les environnements, capables d'identifier et prioriser les menaces en temps-réel. Elles incluent également une bibliothèque de plusieurs milliers de rapports prédéfinis, entièrement personnalisables pour coller à la politique de l'entreprise. L'« intelligence sécurité » n'est pas une option, mais bien la caractéristique essentielle de la technologie QRadar.

### **GS Mag : Quels sont vos conseils en termes de déploiement ?**

**Agostinho Rodrigues :** Il est judicieux de déployer une solution dans un périmètre limité aux actifs sensibles, intégrant nativement toutes les fonctions requises (SIEM « tout-en-un »), rapidement opérationnelle, et qui requiert peu de ressources et compétences en interne.

La souplesse de la solution QRadar permet ensuite d'évoluer facilement vers une architecture distribuée, pour une gestion de la sécurité de bout-en-bout, via la même console centralisée.

### **GS Mag : Pour conclure, quel serait votre message à nos lecteurs ?**

**Agostinho Rodrigues :** Pour les PME comme pour les grandes entreprises, il faut privilégier une solution intégrée et « prête à l'emploi », facilement appropriable par les équipes réseau et sécurité, renforçant ainsi leur synergie. En réduisant significativement les coûts d'investissement et de possession, QRadar « démocratise » les technologies SIEM et Risk Management, permettant aux entreprises de toute taille de se doter dès maintenant d'un outil de surveillance et de protection efficace. ■■■

### FICHE TECHNIQUE

#### Solutions phares :

Appliances QRadar de Q1Labs (SIEM, Risk Manager)

Contact : Agostinho Rodrigues (Interdata)

Tél. : +33 (0) 1 64 86 86 00

E-mail : [contact@interdata.fr](mailto:contact@interdata.fr)

Web : [www.interdata.fr](http://www.interdata.fr) / [www.q1labs.com](http://www.q1labs.com)

