riverbed

DESCRIPTION DE LA SOLUTION

# Alluvio IQ automatise les analyses forensiques de la sécurité

## Améliore l'efficacité des outils SIEM et SOAR classiques grâce à l'accès à des données NPM haute fidélité.

La sécurité intelligente est une préoccupation constante pour tous les réseaux hybrides aujourd'hui. Au fur et à mesure que les entreprises s'étendent au-delà du data center, l'exposition du réseau étendu aux menaces concerne désormais les bureaux distants, les campus et les ressources cloud. Pour faire face aux menaces omniprésentes, les équipes SecOps doivent appliquer une automatisation intelligente tout en ayant accès à des données d'analyse réseau enrichies pour la détection active et la chasse aux menaces. Les outils de sécurité classiques sont souvent insuffisants en raison d'une télémétrie peu fiable ou échantillonnée et de l'incapacité à automatiser la réponse aux incidents. Il en résulte des investigations manuelles fastidieuses et laborieuses qui sont souvent moins précises. Les équipes de sécurité sont donc confrontées à des défis importants, car elles doivent constamment réduire les risques liés à la sécurité tout en maintenant une expérience digitale fiable pour les employés et les clients.

### Enrichir les outils de sécurité classiques par des investigations automatisées

Alluvio™ IQ, le SaaS d'observabilité unifiée de Riverbed, favorise la collaboration entre les équipes NetOps et SecOps en soutenant l'investigation des menaces omniprésentes à l'aide d'une automatisation intelligente basée sur des données réseau haute fidélité, notamment des mesures associées aux flux, aux paquets et à l'infrastructure. Alluvio IQ examine les menaces trouvées dans les outils de sécurité classiques, tels que la gestion des informations et des événements de sécurité (SIEM) ou l'orchestration de la sécurité, l'automatisation et la réponse (SOAR), et s'appuie sur de puissants runbooks low-code pour automatiser la collecte de données forensiques justificatives dans l'ensemble du portefeuille de gestion des performances réseau (NPM) Alluvio™. Alluvio IQ distille les données forensiques pour fournir des informations exploitables qui aident les équipes SecOps à se concentrer sur la résolution des menaces réelles, au lieu de chasser manuellement les faux positifs. Les analyses forensiques automatisées de la sécurité ne fournissent que les données les plus pertinentes en appliquant des runbooks hautement personnalisables et spécifiques à la sécurité, donnant aux équipes SecOps les données dont elles ont besoin pour mener des investigations de sécurité intelligentes et atténuer les cybermenaces.

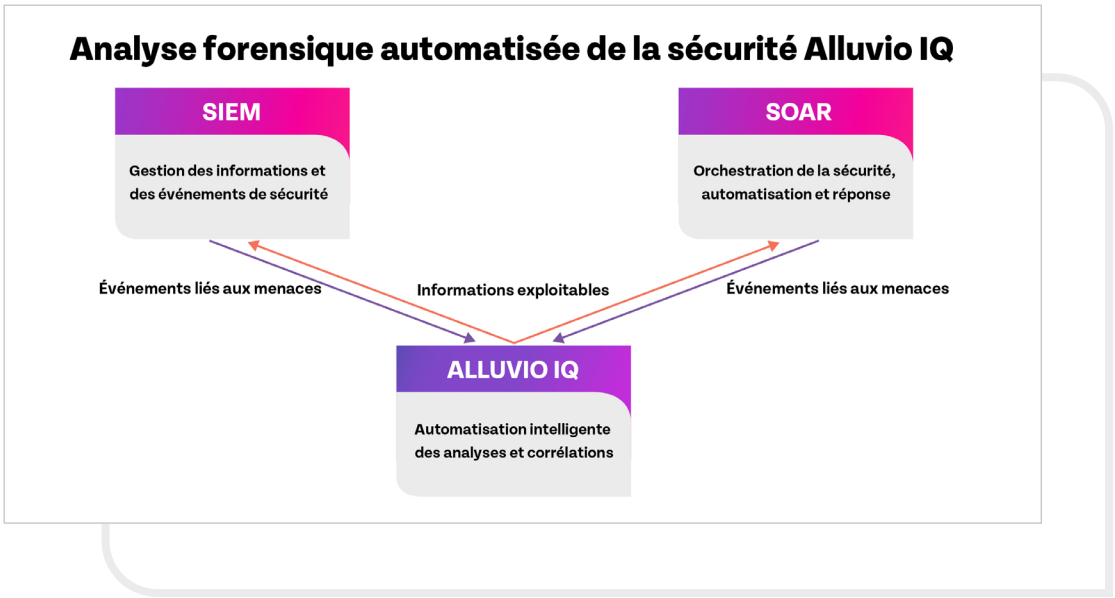



**Figure 1 :** Alluvio IQ étudie les menaces détectées par les outils de sécurité classiques, tels que SIEM ou SOAR, et s'appuie sur de puissants runbooks low-code pour recueillir des données forensiques dans l'ensemble du portefeuille Alluvio NPM.

## Obtenir des informations sur le réseau et des analyses forensiques de la sécurité auprès d'un seul fournisseur

Les entreprises doivent souvent utiliser plusieurs produits provenant de différents fournisseurs pour obtenir une visibilité de bout en bout sur leurs réseaux hybrides. Les solutions Alluvio IQ et de gestion des performances réseau (NPM) Alluvio font partie du portefeuille d'observabilité unifiée Alluvio de Riverbed, offrant à la fois une télémétrie haute fidélité et une observabilité unifiée, ce qui rend nos données extrêmement précieuses pour les deux organisations. Riverbed unifie les données, les informations et les actions pour l'ensemble du service IT, y compris les équipes NetOps et SecOps. Grâce à l'observabilité unifiée Alluvio IQ, le service IT peut éliminer les silos de données, les salles de crise et l'accoutumance aux alertes. Le service IT peut prendre des décisions plus efficaces dans tous les domaines, appliquer plus largement les connaissances des experts et améliorer en permanence l'expérience digitale et les performances.

## Améliorer l'efficacité des outils de sécurité

L'efficacité des outils de sécurité classiques, tels que SIEM et SOAR, dépend largement de l'information qu'ils ingèrent. Souvent, les données réseau utilisées par ces outils sont échantillonnées ou difficiles d'accès pour les équipes SecOps. Le choix d'une source de données qui fournit une télémétrie réseau haute fidélité en capturant chaque mesure de paquets, de flux et d'équipement, associée à des informations exploitables provenant de runbooks intelligents et automatisés, accroît l'efficacité des investigations de sécurité.

## Réduire les investigations manuelles sur les faux positifs grâce à l'automatisation intelligente

Alluvio IQ peut ingérer des données provenant de la télémétrie Alluvio ainsi que de solutions tierces et appliquer des scripts d'automatisation personnalisables afin d'identifier les incidents de sécurité à fort impact. Les informations exploitables très précises qui en résultent permettent d'isoler uniquement les incidents les plus pertinents, tout en éliminant les faux positifs. En se concentrant sur les menaces réelles, les équipes SecOps peuvent identifier et remédier aux menaces de sécurité sur le réseau hybride moderne.

## Améliorer la collaboration entre les équipes NetOps et SecOps

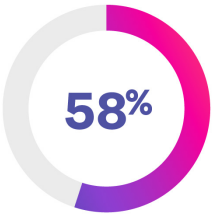
Souvent, ces deux organisations s'opposent sur des priorités opérationnelles concurrentes qui, en fin de compte, ont un impact sur la sécurité et la performance réseau. Les deux équipes ont besoin de données sur le réseau pour accomplir efficacement leur travail. Dans le cas des équipes NetOps, il s'agit de maintenir la performance du réseau et des applications qui le traversent, tandis que les équipes de sécurité ont besoin de données sur le réseau pour éliminer les risques qui pèsent sur le réseau et l'infrastructure.

Grâce aux investigations automatisées d'Alluvio IQ, la collaboration s'installe, car les responsabilités sont clairement délimitées. Les équipes NetOps sont responsables de la télémétrie du réseau tandis que les équipes SecOps sont responsables des outils de sécurité classiques qui ingèrent les données de performance réseau haute fidélité d'Alluvio pour protéger l'entreprise contre les cybermenaces.

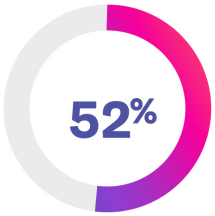
## Bénéfices de l'automatisation de l'analyse forensique de la sécurité d'Alluvio

Outre l'amélioration de la collaboration entre les équipes NetOps et SecOps, l'automatisation de l'analyse forensique de la sécurité peut offrir les bénéfices suivants aux équipes SecOps :

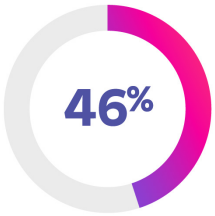
**Les trois principaux bénéfices d'un partenariat NetSecOps réussi :**




Résolution plus rapide des problèmes de sécurité




Réduction des risques de sécurité




Efficacité opérationnelle

Enterprise Management Associates

- **Rapidité et efficacité :** L'automatisation permet de traiter rapidement de grands volumes de données, d'identifier des schémas et de recueillir des données de diagnostic complètes afin de réduire considérablement le temps nécessaire à l'identification, à l'analyse et à l'atténuation des incidents de sécurité.
- **Précision :** Les outils automatisés sont moins sujets aux erreurs humaines et peuvent analyser davantage de données de manière plus cohérente et plus fiable. Ils réduisent considérablement le risque de passer à côté des indicateurs critiques d'une violation de la sécurité ou de signaler à tort des événements non liés à la sécurité.
- **Cohérence :** En combinant l'IA, la mise en corrélation et l'automatisation, Alluvio IQ analyse et hiérarchise de manière cohérente les incidents de sécurité tout en recueillant des données justificatives et de diagnostic connexes pour s'assurer que toutes les menaces liées sont correctement identifiées.
- **Évolutivité :** L'analyse forensique automatisée de la sécurité peut facilement s'adapter à l'analyse de grands volumes de données provenant de plusieurs systèmes et équipements. Elle permet d'identifier les incidents de sécurité et d'y répondre rapidement et efficacement.
- **Économique :** Les outils automatisés réduisent la charge de travail des analystes de la sécurité et leur permettent de se concentrer sur des problèmes de sécurité plus complexes. Ils contribuent ainsi à réduire le coût global de la gestion des incidents de sécurité.

Dans l'ensemble, l'automatisation de l'analyse forensique de la sécurité aide les équipes SecOps à identifier les incidents de sécurité et à y répondre plus rapidement et plus efficacement, tout en réduisant la charge de travail et les coûts associés aux méthodes manuelles.

## À propos d'Alluvio IQ

Alluvio IQ, la solution ouverte, programmable, basée sur le cloud et de type SaaS de Riverbed pour l'observabilité unifiée, permet à l'ensemble du personnel IT et de sécurité d'identifier et de résoudre rapidement les problèmes. Cette solution applique des techniques de machine learning (ML) à l'expérience utilisateur et aux données de performance réseau pour chaque transaction afin d'identifier les événements anormaux. Elle établit ensuite une corrélation contextuelle entre les flux de données afin d'identifier ceux qui ont le plus d'impact sur l'entreprise. Ces informations alimentent les runbooks d'investigation automatisés, qui reproduisent les workflows de diagnostic des experts IT et en sécurité afin de rassembler le contexte, d'éliminer le bruit et de définir les priorités, réduisant ainsi le volume d'alertes à celles qui ont le plus d'impact sur l'entreprise.

Alluvio IQ favorise la collaboration entre les équipes NetOps et SecOps, en favorisant la recherche active de menaces omniprésentes sur le réseau grâce à des investigations de sécurité automatisées. L'analyse forensique automatisée de la sécurité identifie les événements les plus pertinents, en appliquant aux événements identifiés dans les solutions SIEM ou SOAR des runbooks hautement personnalisables et spécifiques à la sécurité. Les équipes SecOps disposent des données réseau dont elles ont besoin pour mener des investigations de sécurité intelligentes.

Pour plus d'informations sur Alluvio IQ, l'analyse forensique automatisée de la sécurité, cliquez ici.

riverbed

### Riverbed — Renforcer l'expérience

Riverbed est la seule entreprise à disposer de la richesse collective de la télémétrie couvrant tout l'écosystème digital, du réseau à l'utilisateur final en passant par les applications, pour éclairer et accélérer chaque interaction afin que les utilisateurs profitent d'une expérience digitale sans faille. Riverbed propose des solutions de pointe dans deux domaines : Alluvio by Riverbed, un portefeuille innovant et différencié d'observabilité unifiée qui unifie les données, les informations et les actions tout au long du parcours IT, afin que les clients puissent offrir des expériences digitales transparentes ; et Riverbed Acceleration, qui fournit une accélération rapide, agile et sécurisée de n'importe quelle application sur n'importe quel réseau aux utilisateurs, qu'ils soient mobiles, distants ou sur site. Avec nos milliers de partenaires et nos clients leaders du marché dans le monde entier, nous favorisons chaque clic, chaque expérience digitale. Pour en savoir plus, visitez le site riverbed.com/fr/.