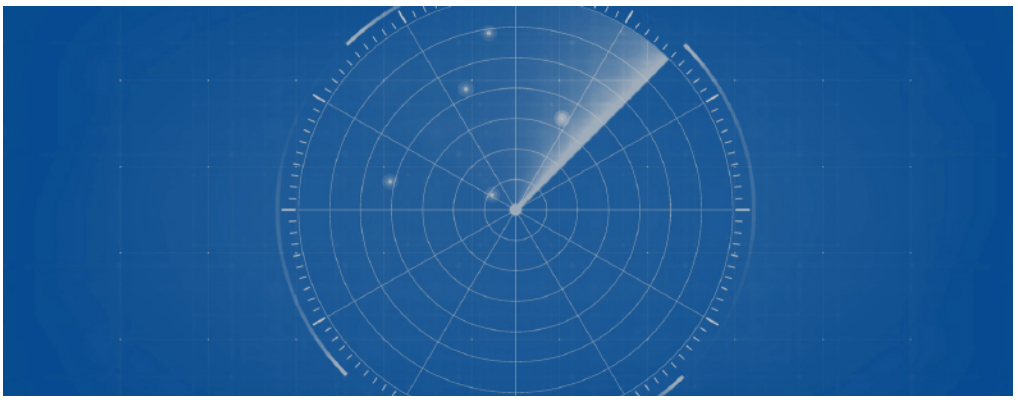
SIEM OKIOK

LA SURVEILLANCE SIMPLIFIÉE

Mettez en œuvre une solution gérée de surveillance et de réponse aux incidents sans tracas



Aujourd'hui, toutes les organisations, grandes et petites, doivent mettre en œuvre une surveillance efficace de leurs actifs informationnels afin de détecter toute activité suspecte le plus tôt possible. De plus, il ne suffit pas de détecter des activités suspectes, il faut pouvoir rapidement les analyser afin de prendre des décisions rapides et appliquer des mesures préventives efficaces le plus rapidement possible.

Un des problèmes souvent rapportés par nos clients est que leur fournisseur de service de surveillance ne réagit pas assez rapidement aux situations suspectes, alors que tout délai peut entraîner des impacts catastrophiques.

Les solutions SIEM traditionnelles requièrent une expertise pointue et une attention soutenue afin d'atteindre et de maintenir leur capacité de détection à la fine pointe et requièrent une équipe d'analystes spécialisés capables de faire évoluer la solution pour la garder efficace ainsi que pour l'exploiter au quotidien.

Malheureusement, le défi d'embaucher et de maintenir une équipe spécialisée rend quasi impossible la mise en œuvre de telles solutions pour la grande majorité des entreprises.

Une solution simple et efficace

La solution SIEM OKIOK est une solution gérée de détection et de réponse aux incidents offerte en mode service, qui mets à votre portée une technologie ultra performante, en constante évolution, qui prend pleinement avantage de l'expérience et de l'expertise de l'équipe de tests d'intrusion d'OKIOK.

Protection en continu, tous les jours, 24 heures par jour

Les journaux en provenance de vos sources sont ingérés, consolidés, normalisés, stockés et analysés 24h sur 24h.

Les situations à risque sont détectées automatiquement par l'application d'algorithmes d'analyse sophistiqués, appuyés sur des cas d'usage tirés de notre expérience ainsi que du cadre de référence MITRE ATT&CK.

Les alertes résultantes sont priorisées et enrichies pour inclure l'information contextuelle nécessaire pour une résolution rapide et efficace et transmises automatiquement à votre équipe technique selon les canaux convenus.

La solution peut prendre action automatiquement sur vos diverses plates-formes pour limiter l'impact d'une attaque.

L'expertise d'OKIOK à votre service

L'équipe d'OKIOK développe et fait évoluer les cas de surveillance en fonction des connaissances concrètes gagnées sur le terrain au cours des centaines de tests intrusion et mandats de réponse aux incidents effectués annuellement.

De plus, vous pouvez compter sur des services professionnels complémentaires fournis par les meilleurs experts de l'industrie pour appuyer votre équipe et vous aider à prendre des décisions éclairées. Ces services se déclinent en une gamme complète allant de l'analyse approfondie des événements jusqu'à la prise en charge de votre stratégie de réponse en cas d'incident majeur.

Éliminer le facteur humain

Analyser rapidement les activités suspectes, prendre les bonnes décisions et initier les actions critiques ne sont pas des tâches faciles même pour les analystes les plus aguerris. Les logiciels malicieux deviennent de plus en plus sophistiqués et efficaces pour camoufler leurs traces et confondre les analystes.

A cet égard, nous croyons qu'il faut viser à éliminer le facteur humain au niveau de l'analyse des événements en plus d'automatiser les réponses qui peuvent aider à réduire les risques en éliminant les délais de réaction.

L'élimination du facteur humain dans la chaîne d'analyse, de décision et de réponse permet de réduire les erreurs et d'initier les actions critiques dans les meilleurs délais.

OKIOK SIEM

Automatiser pour répondre rapidement

La solution SIEM OKIOK inclus des fonctionnalités de type « Security Orchestration, Automation and Response » (SOAR) qui permettent d'automatiser les réponses aux alertes et aux événements afin de réduire les risques et garder le contrôle face au déluge potentiel d'alertes.

Éliminez les coûts et les tracas liés à l'embauche et à la rétention de personnel

La solution SIEM OKIOK permet à votre entreprise de réaliser des bénéfices encore plus grands en vous permettant de canaliser votre ressource la plus précieuse, le capital humain, sur des tâches à valeur ajoutée en lien avec votre mission.

Robustesse et capacité d'ingestion quasi illimitée

La solution SIEM OKIOK est une solution infonuagique pure qui prend avantage de la robustesse et de la capacité quasi illimitée de l'infrastructure infonuagique AWS. En effet, la solution s'adapte au flux de données de votre entreprise qu'ils soient modestes ou énormes.

De plus, la solution est conçue pour ne perdre aucune information, même en cas de panne de réseau ou des composantes technologiques.

Conformité et sécurité de vos données

Dormez en paix, vos données sont adéquatement protégées en transit et au repos lorsqu'elles sont prises en charge par SIEM OKIOK. De plus, les données sont stockées dans des dépôts de données situés dans votre pays ou dans la zone de votre de choix afin d'assurer la conformité aux cadres normatifs et requis d'hébergement.

Obtenez des résultats rapidement

La solution SIEM OKIOK peut être mise en œuvre très rapidement par l'intégration, par nos experts, de vos actifs citriques et de vos infrastructures au service de collecte et de consolidation des journaux.

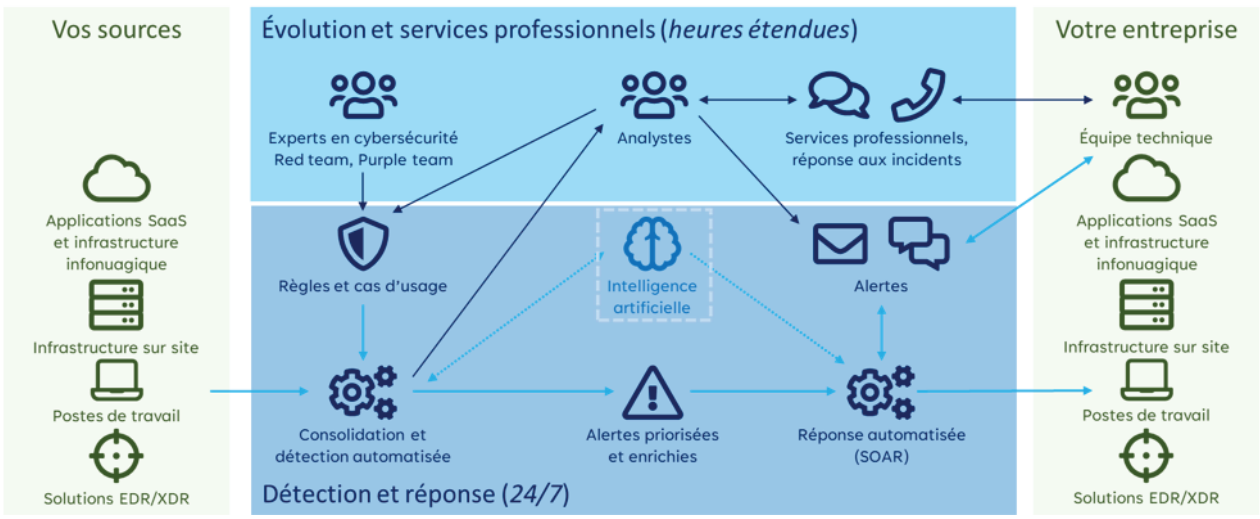
Capacité d'intégration

SIEM OKIOK™ s'intègre facilement à pratiquement n'importe quel système d'information et composante d'infrastructure. La solution peut ingérer tous les formats standards et non-standards de journaux, incluant les journaux produits par les systèmes patrimoniaux, les garde-barrières et les composantes d'infrastructures telles qu'Active Directory (AD), les annuaires LDAP, les bases de données SQL, ainsi que pour les applications et infrastructures infonuagiques telles que Office 365, Microsoft Azure, Google Cloud Platform, AWS, etc.

Cette architecture flexible permet au SIEM OKIOKTM de s'adapter facilement à tout environnement technique existant et futur.

Solutions EDR, XDR

SIEM OKIOK s'intègre aux solutions de type EDR / XDR telles que Sentinel One et prend avantage de leur capacité de détection locale ainsi que de leur capacité de réponse automatisée.



OKIOK est un chef de file en matière de sécurité informatique. Depuis 1973, OKIOK se démarque par l'excellence de ses produits et la qualité de ses services. OKIOK offre une vaste gamme de solutions intégrées conçues pour répondre aux besoins des entreprises de toutes tailles.

www.okiok.com | info@okiok.com | 1 877 561-1681

Dernière mise à jour: Décembre 2022