FICHE TECHNIQUE

CLOUDFLARE

Security Operations Center (SOC)-as-a-Service par Cloudflare

+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

L’environnement des menaces

Dans le monde numérique actuel, où les cyberattaques sont devenues courantes et les réseaux sont devenus complexes, même les organisations les plus attentives peuvent peiner à détecter les menaces. Quelles alertes et quels incidents sont des faux positifs, et lesquels nécessitent d’être examinés ? Quels nouveaux aspects de l’environnement des menaces en perpétuelle évolution constituent le plus grand risque pour l’organisation ?

La complexité des réseaux résultant d’environnements hétérogènes et d’un modèle d’infrastructure « périmétrique » obsolète laisse aujourd’hui les organisations face à un amoncellement d’outils cloisonnés de sécurité et de performance. Les équipes de sécurité et informatiques passent beaucoup de temps à traduire les logs, les alertes et les politiques entre les différents environnements. Ceci rend les opérations coûteuses, inefficaces et sujettes aux erreurs.

En plus d’augmenter la surface d’attaque et le risque d’exposition des organisations, cette complexité empêche les entreprises de se concentrer sur leurs nouvelles opportunités de croissance.

Aller à l'essentiel : SOC-as-a-Service par Cloudflare

La solution SOC-as-a-Service de Cloudflare intègre nos produits de sécurité et et fait appel à notre équipe d’experts de la cybersécurité, qui surveille l’environnement de votre entreprise 24x7x365 afin d’identifier les menaces de sécurité et les perturbations des opérations, exécute des analyses approfondies afin d’identifier les vecteurs d’attaque et déploie des contremesures afin d’atténuer les incidents.

La solution SOC-as-a-Service de Cloudflare est conçue pour répondre aux besoins de surveillance de la sécurité, de détection des menaces et de réponse aux incidents pour les entreprises de toute taille, sur les couches 3, 4 et 7. Dans la mesure où les premiers indicateurs d’incidents de sécurité peuvent parfois apparaître sous la forme d’une dégradation de l’intégrité des applications ou du réseau, des alertes proactives concernant l’accessibilité, la disponibilité et la latence des serveurs d’origine sont diffusées. Cette approche offre non seulement une visibilité de l’intégrité globale du réseau, mais assure également une défense proactive contre les perturbations et les défaillances du réseau.

La technologie d’alerte de Cloudflare repose sur des algorithmes propriétaires avancés, plutôt que sur de simples déclencheurs basés sur des « seuils d’alerte ». Ces alertes permettent à l’équipe SOC de réagir et prendre les bonnes décisions en quasi-temps réel. Les experts de la solution SOC-as-a-Service de Cloudflare veillent à ce que les incidents urgents soient correctement triés, examinés et résolus. L’équipe SOC Cloudflare communique de manière proactive au sujet des événements et fournit régulièrement des rapports détaillés sur les attaques et les incidents sur le réseau.

Le réseau Cloudflare s’étend à plus de 200 villes dans le monde entier, et plus d’un milliard d’adresses IP uniques y transitent chaque jour. Cette diversité et cette ampleur fournissent des connaissances uniques, qui permettent à l’équipe SOC Cloudflare d’identifier les activités suspectes sur le réseau.

Avantages de la solution SOC-as-a-Service de Cloudflare

Protection 24x7x365

Les experts Cloudflare surveillent en permanence les menaces de sécurité et réagissent à celles-ci avant qu’elles ne deviennent des événements critiques.

Détection et résolution plus rapides

L’atténuation et la configuration personnalisées par l’équipe SOC contribuent à réduire le délai entre l’instant où un incident se produit, sa détection et son atténuation.

Communication et rapports proactifs

Communications proactives sur différents canaux (téléphone, e-mail et webhook) en cas d’anomalie du trafic ou d’attaque sur le réseau. Rapports périodiques détaillant les règles créées et les attaques arrêtées, avec des recommandations relatives aux modifications de la configuration.

Réduction des coûts globaux de sécurité

La solution SOC Cloudflare réduit la nécessité d’employer et de former des spécialistes de la sécurité en interne pour surveiller les alertes et y réagir, réduisant ainsi les dépenses globales de sécurité.

Démarrage rapide et facile

La mise en œuvre d’une configuration de base de la solution SOC est simple et rapide. L’activation du service SOC ne nécessite pas le déploiement d’agents ou d’outils supplémentaires sur les terminaux

Sécurité assurée par les experts Cloudflare

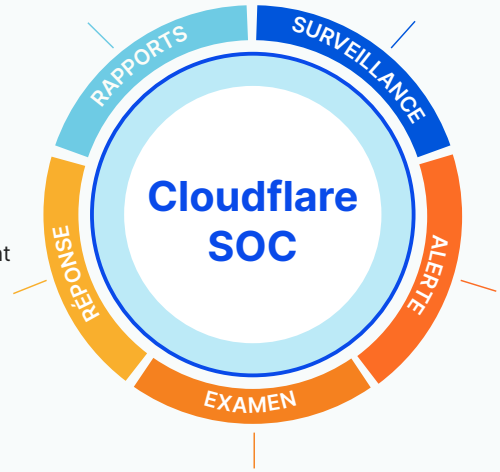
Votre équipe de sécurité ne perd plus son temps à examiner un flot de faux positifs et peut se concentrer sur d’autres projets prioritaires. Les experts de la sécurité de Cloudflare identifient immédiatement toute activité suspecte et réagissent rapidement, en recommandant des solutions.

Rapports mensuels/trimestriels

Notre équipe SOC fournit des rapports réguliers pour partager des informations sur les protections Cloudflare permettant d’atténuer les menaces de sécurité.

- Publication régulière de rapports sur les attaques atténuées et les politiques configurées
- Conservation des logs aux fins de l'analyse a posteriori et de la conformité

- Surveillance 24x7x365 des alertes par l'équipe SOC
- Détection basée sur les divergences par rapport à la ligne de base des seuils de trafic



- Atténuation automatique conformément aux politiques configurées
- Atténuation mise en œuvre conformément au processus/runbook approuvé par le client
- Configuration précise des règles de détection

- Notification en cas d'atténuation automatique d'événements
- Alertes en cas d'événements non atténués nécessitant une analyse approfondie

- Triage et examen des alertes
- Diffusion d'analyses et de recommandations au client

Options de service

	SOC for Core Applications	SOC for Network
Surveillance proactive et alerte en cas d'événements anormaux	✔	✔
Règles personnalisées pour atténuer les attaques actives	✔	✔
Rapports	✔	✔
Analyse et atténuation des attaques en couche 7	✔	✘
Détection précoce/alertes concernant le serveur d'origine Problèmes d'accessibilité, de disponibilité et de latence	✔	✘
Analyse et atténuation des attaques sur le réseau en couches 3 et 4	✘	✔
Surveillance de l'intégrité des tunnels GRE	✘	✔
Produits pris en charge	DDoS Limitation de débit Pare-feu WAF	Magic Transit

Pour commencer : contactez dès aujourd'hui votre chargé de compte Cloudflare pour vous lancer.