STREAMSCAN
Votre partenaire de cybersécurité



StreamStop - Forfait de réponse aux incidents

Attaque neutralisée. Contrôle restauré. En avant, plus fort.

StreamStop est un fortait de réponse aux incidents qui donne à votre entreprise un accès prioritaire 24h/24 et 7j/7 à notre équipe d'experts en réponse aux incidents, vous offrant la tranquillité d'esprit.

Qu'est-ce qu'un fortait de réponse aux incidents

Un fortait de réponse aux incidents est un accord proactif avec un partenaire de confiance en cybersécurité qui assure un soutien rapide et expert lors d'une violation de sécurité ou d'un autre incident cybernétique. Avec un tel fortait en place, les organisations peuvent compter sur une mobilisation plus rapide de l'équipe de réponse aux incidents, des processus prévisibles et un accès prioritaire à une expertise spécialisée.

Pourquoi obtenir un forfait de réponse aux incidents

Avec la fréquence et la complexité croissantes des cyber attaques, un forfait de réponse aux incidents n'est plus seulement une protection, c'est un élément critique d'une stratégie de cybersécurité résiliante et proactive.

Les forfaits de réponse aux incidents de StreamScan combinent une réponse rapide avec une expertise technique approfondie, donnant aux organisations la confiance nécessaire pour contenir rapidement les menaces et se rétablir avec un minimum de perturbations.

Avantages de StreamStop

- Accès 24h/24 et 7j/7 à nos experts en réponse aux incidents
- Analyse, confinement et rétablissement rapides des incidents par une équipe qui connaît votre environnement
- Meilleure gestion des coûts grâce à des modalités et tarifs préétablis
- Atténuation des risques en suivant les meilleures pratiques en cybersécurité
- Peut améliorer votre assurabilité et diminuer vos primes d'assurance
- Aide à la conformité réglementaire pertinente à votre secteur d'activité

StreamStop. Quand chaque minute compte.

Processus de réponse aux incidents

1. Diagnostic initial et confinement

Lorsqu'un incident survient, la priorité est d'évaluer rapidement la situation pour cerner sa portée, sa nature et son impact potentiel sur l'entreprise. Plus un diagnostic est précis et complet, plus le risque des pertes sera minimisé et le retour en production sera rapide.

Une fois le diagnostic confirmé, un plan d'action est élaboré et des mesures de confinement sont mises en place afin d'éviter que l'incident ne se propager davantage.

Les mesures de confinement courantes comprennent :

- Déconnexion des appareils infectés
- Ajout de règles aux pare-feu
- Désactivation de comptes d'utilisateurs
- Changement de mots de passe

2. Enquête et reconstruction

Lors de la gestion de l'incident, il est essentiel de prendre le contrôle du réseau et de confirmer qu'aucune autre attaque n'est en cours. Le XDR de StreamScan peut être déployé pour fournir une visibilité complète du réseau, permettant à nos experts d'analyser tout activité en temps réel. En travaillant étroitement avec votre équipe informatique, notre équipe restaure le contrôle et supprime toute menace active de l'environnement.

Dans les cas complexes tels que les rançongiciels ou les intrusions avancées, une enquête plus approfondie est menée pour déterminer exactement ce qui s'est passé. Cela peut inclure la rétro-ingénierie d'outils malveillants pour comprendre leur objectif, leurs méthodes de propagation et leurs points d'entrée.

L'équipe d'experts StreamScan sera en mesure de :

- Reconstruire le scénario de l'attaque
- Déterminer comment l'incident s'est produit et identifier les vulnérabilités
- Identifier le « patient zéro », le premier système infecté
- Définir et prioriser les mesures de réponse

3. Éradication, recouvrement et analyse

Une fois l'incident confiné et l'investigation complétée, la phase d'éradication consiste à mettre en place des mesures pour éliminer la cause de l'incident ou de nettoyer les systèmes impactés.

Lors de la phase de recouvrement nous aidons votre équipe à remettre les systèmes en production.

Voici quelques-unes des actions qui pourraient être réalisées durant cette phase :

- Réinstallation des systèmes impactés
- Endurcissement des systèmes afin de rehausser leur niveau de sécurité
- Activation de fonctions ou outils de sécurité sur les systèmes
- Restauration des données via des sauvegardes
- Retour graduel en production

Si nécessaire, une **analyse forensique** pourrait être réalisée par StreamScan afin de collecter et de préserver les éléments de preuve requises si l'entreprise désire initier une poursuite judiciaire contre l'auteur d'une intrusion ou d'une malversation.

Une fois l'incident résolu, un examen final est effectué pour comprendre l'événement et prévenir de futures occurrences. Un rapport complet de gestion d'incident est livré, couvrant :

- Les méthodes de l'attaquant et les vulnérabilités exploitées
- La portée et l'impact de l'incident
- Les mesures de réponse prises
- Les conclusions de toute rétro-ingénierie
- Les forces et faiblesses de l'intervention
- Les recommandations pour prévenir la récurrence

Mise en service de StreamStop

La mise en service de StreamStop est un processus simple conçu pour mettre la protection en place rapidement et sans perturber les opérations.

- **Réunion de démarrage :** L'équipe rencontre les parties prenantes clés pour confirmer les objectifs, clarifier les rôles et recueillir les informations essentielles telles que les diagrammes de réseau, une liste des actifs critiques, les outils de sécurité actuels et tout plan de réponse aux incidents existant.
- **Établissement des règles de communication :** L'équipe de StreamScan se familiarisera avec votre réseau et pourra déterminer le meilleur moyen de connecter notre outil de détection d'intrusion, si nécessaire. Nous établirons également les règles de communication, y compris une liste d'escalade et un protocole à suivre en cas d'incident.
- **Validation de l'accès :** Lors de cette étape, nous effectuerons un test d'accès à votre réseau via VPN. Cela nous permettra d'installer à distance des outils de sécurité en cas d'intervention.
- **Équipe prête à intervenir :** Une fois l'accès confirmé et tous les documents requis en notre possession, l'équipe StreamScan sera prête à intervenir en cas d'incident.

Forfaits

Standard - 5 000 $ / an

Idéal pour les entreprises qui recherchent un accès prioritaire et des économies.

- Réponse garantie en 4 heures
- Processus d'intégration complet
- Rabais de 20 % sur les frais d'intervention standards

Plus populaire

Pro - 9 000 $ / an

Pour les équipes qui veulent plus de couverture, sans le plein engagement.

- Comprend tout ce qui est inclus dans le forfait Standard, plus :
- Rabais de 30 % sur les frais d'intervention standards
- Jusqu'à 15 heures de services d'intervention incluses
- 2 000 $ crédités à d'autres services si aucun incident ne survient

Complet - 30 000 $ / an

Pour les organisations qui recherchent une couverture et une flexibilité maximales.

- Comprend tout ce qui est inclus dans le forfait Pro, plus:
- Rabais de 40 % sur les frais d'intervention standards
- Jusqu'à 100 heures de services d'intervention incluses
- 7 500 $ crédités à d'autres services si aucun incident ne survient
- Optionnel : Intégration de notre NDR dans votre réseau*

Avantages supplémentaires sur tous les forfaits :

- 15 % sur les analyses de vulnérabilités
- 15 % sur la révision (ou aide à la préparation) du plan de réponse aux incidents
- 15 % sur simulations d'incident (tabletop)

* Sur serveur virtuel dans l'infrastructure client. Frais d'installation et configuration de 5 000$ par site.