STREAMSCAN
Votre partenaire de cybersécurité

FICHE EDR

L'EDR de StreamScan

L'adoption des solutions nuagiques, le télétravail et l'usage d'appareils personnels en entreprise, combinés à la montée des cybermenaces, ont transformé l'approche de la sécurité des terminaux. Face à des attaques sophistiquées contournant les protections classiques, les organisations recherchent un système de sécurité unifié offrant prévention, détection et réponse, tout en respectant leurs contraintes budgétaires.

Grâce à l'analyse comportementale et à l'intelligence artificielle, l'EDR de StreamScan réduit les vecteurs d'attaque, créant des barrières supplémentaires contre les intrusions potentielles. Il est conçu pour offrir une détection en temps réel, des capacités de réponse automatisée, la priorisation des alertes, l'intégration avec d'autres outils de cybersécurité, une visibilité complète, des outils d'enquête et des capacités de rapports détaillés.

L'EDR de StreamScan permet aux organisations de se défendre contre des cyberadversaires sophistiqués et de gérer des cycles de vie d'attaque complets grâce à :

- La minimisation de la surface de menace via un pare-feu, un antivirus et un filtrage web intégrés.
- L'élimination des menaces avant exécution grâce à l'apprentissage automatique adaptatif et à l'analyse comportementale.
- Le blocage en temps réel des activités malveillantes, des charges utiles et des activités de rançongiciels.
- La détection et le blocage des communications informatiques malveillantes, ainsi que des mouvements latéraux.
- Une communication inter-machines rapide et un scan des indicateurs de compromission (IOC) de l'ensemble du réseau.

Applications

Pour les organisations qui ne disposent pas encore de solution pour protéger leurs ordinateurs et serveurs.

▾

Pour celles qui ont déjà un antivirus mais qui souhaitent une couche de protection supplémentaire sur leurs terminaux contre les menaces « zero-day » et sophistiquées.

▾

Pour celles qui n'ont pas de réseau mais qui souhaitent quand même protéger leur ordinateur contre les tentatives d'intrusion.

▾

Pour celles qui disposent d'un outil de détection réseau et qui souhaitent une meilleure protection de leurs terminaux.

STREAMSCAN
Votre partenaire de cybersécurité

FICHE EDR

Fonctionnement

Protection antivirale complète dès l'installation

Dès l'installation votre ordinateur bénéficie automatiquement d'une protection antivirale complète via l'antivirus Avira, l'un des plus réputés du marché.

Collecte de données

L'EDR de StreamScan récupère les informations de télémétrie des appareils surveillés, comme les fichiers créés ou modifiés, les processus en cours, les connexions réseau et les journaux d'événements.

Analyse des données

Les données sont examinées en temps réel par le serveur EDR, qui utilise des algorithmes pour identifier tout comportement suspect ou menace potentielle.

Détection des menaces

Basé sur des algorithmes et des règles, l'EDR identifie des menaces telles que les attaques de logiciels malveillants, les rançongiciels, les fuites de données, les tentatives d'exploitation des failles et les tentatives d'intrusion.

Réponses automatisées

En cas de problème de sécurité, l'EDR peut automatiser certaines réponses, comme la mise en quarantaine des fichiers infectés, la désactivation des processus malveillants ou le blocage d'une attaque.

Alertes

Lorsqu'une activité malveillante est détectée, l'EDR envoie des alertes aux équipes de sécurité afin qu'elles puissent prendre les mesures nécessaires. L'alerte s'affiche également sur l'ordinateur concerné, informant l'utilisateur qu'une activité malveillante est en cours.

Pourquoi choisir l'EDR de StreamScan

Fait au Canada

- Périmètre d'action et surface d'attaque réduits sur les terminaux.
- Visibilité centralisée sur tous vos appareils.
- Faible consommation de ressources.
- Intégration facile avec vos outils de sécurité existants.
- Facilité d'utilisation et automatisation des tâches.
- Compatibilité avec les systèmes d'exploitation Windows modernes et prise en charge des systèmes hérités.
- Aucune expérience en cybersécurité n'est requise pour l'installation.
- Mise à jour continue des définitions de virus, des renseignements sur les menaces et des améliorations du produit.
- Conçu pour convenir aux entreprises de toutes tailles.
- Gestion basée sur le cloud pour une évolutivité flexible.
- Possibilité d'avoir la console EDR dans votre réseau local.
- Possibilité de configurer les EDR avec des politiques de sécurité sur mesure, en fonction des besoins de l'entreprise.

STREAMSCAN
Votre partenaire de cybersécurité

FICHE EDR

Spécifications

Protection antivirus

‣ Notre EDR dispose d'une couche antivirus complète fournie par l'antivirus Avira, reconnu comme l'un des leaders du marché. Vous pouvez donc remplacer votre antivirus existant par notre EDR.
‣ Analyse en temps réel des fichiers, des documents et des pièces jointes.
‣ Détection proactive des menaces à l'aide d'une analyse basée sur les signatures et d'une analyse heuristique avancée.
‣ Détection des menaces en temps réel.
‣ Détection instantanée des programmes malveillants et des rançongiciels.
‣ Mises à jour automatiques des définitions de virus.
‣ Suppression automatique des outils malveillants.

Intelligence artificielle (IA)

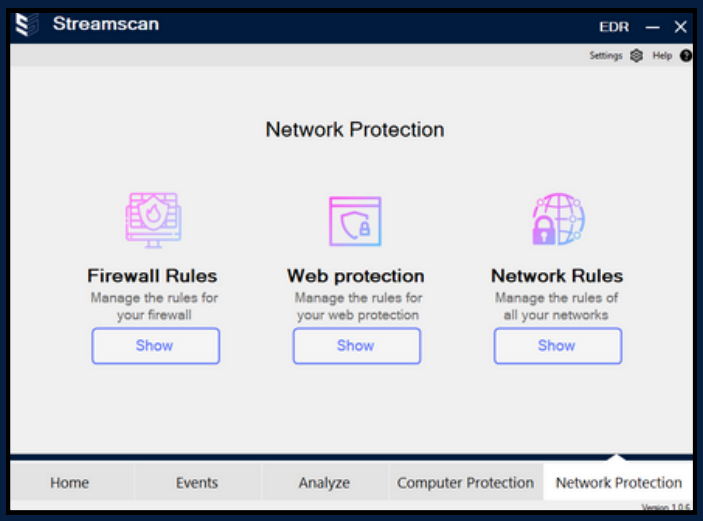
‣ Algorithmes d'apprentissage automatique pour la détection proactive des menaces.
‣ Analyse comportementale pour la détection des anomalies.
‣ Analyse prédictive pour identifier les menaces en constante évolution.
‣ Apprentissage continu et adaptation aux nouveaux vecteurs d'attaque.

Blocage des attaques et des logiciels malveillants

‣ Heuristique avancée pour identifier et bloquer les logiciels malveillants sophistiqués.
‣ Analyse comportementale pour contrecarrer les tactiques d'attaque en constante évolution.
‣ Blocage en temps réel des activités et charges utiles malveillantes.
‣ Blocage adaptatif basé sur les renseignements sur les menaces.
‣ Détection et blocage de scripts malveillants (powershell, shellcode, webshell et autres.)

Pare-feu intégré

‣ Blocage des communications malveillantes entrantes et sortantes de l'ordinateur.
‣ Blocage des mouvements latéraux malveillants.
‣ Inspection et filtrage HTTPS.
‣ Contrôle granulaire des politiques d'accès au web.



Détection et blocage des rançongiciels

‣ Analyse comportementale pour identifier les schémas de rançongiciels.
‣ Analyse heuristique du comportement de chiffrement des fichiers.
‣ Blocage en temps réel des activités des rançongiciels.
‣ Réponse rapide et remédiation aux attaques de rançongiciels.

Détection et blocage des communications réseaux malveillantes

‣ Détection et blocage des communications malveillantes entrantes et sortantes de l'ordinateur.
‣ Détection et blocage des mouvements latéraux malveillants.

STREAMSCAN
Votre partenaire de cybersécurité

FICHE EDR

Spécifications

Sécurité web

- Catégorisation des URL et analyse de la réputation.
- Blocage des sites web malveillants.
- Protection contre les contenus web dangereux classés dans la catégorie phishing, malware, spam ou fraude.
- Inspection et filtrage HTTPS.
- Contrôle granulaire des politiques d'accès au web.
- Contrôle des fichiers téléchargés (blocage des fichiers malveillants).
- Blocage des sites web associés à la distribution de PUAs (Potentially Unwanted Program).
- Blocage des sites web redirigés à partir de sources malveillantes (malware/PUA).

Console de gestion EDR

- Interface intuitive et conviviale.
- Gestion des menaces détectées par les EDR
- Gestion centralisée des EDR déployés dans l'ensemble du réseau de l'entreprise (réseau local, siège distant, utilisateurs VPN, etc).
- Contrôle d'accès basé sur les rôles pour les tâches administratives.
- Gestion et déploiement centralisés des politiques.
- Isolation des terminaux à la demande.
- Prise d'actions sur les terminaux via la console centralisée : arrêt de processus douteux, arrêt de communication entrante ou sortante de l'ordinateur, etc.

Rapports et analyses

- Tableau de bord centralisé pour une surveillance en temps réel.
- Rapports personnalisables sur les incidents de sécurité et les tendances.
- Outils d'analyse forensique pour les enquêtes sur les incidents.

Liste blanche d'applications

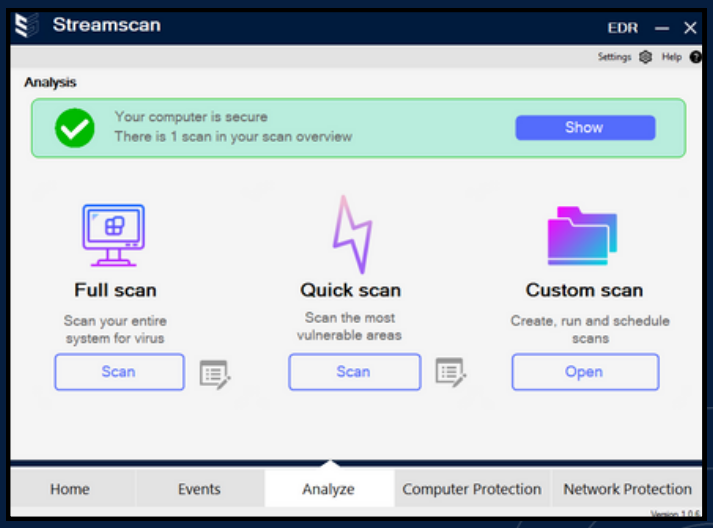
- Contrôle complet des applications.
- Liste d'autorisations et de refus basée sur le comportement de l'application.
- Contrôle précis des fichiers exécutables.
- Intégration avec des bases de données d'applications connues.

Isolation rapide des ordinateurs compromis

- Recherche d'indicateurs de compromissions (IOC) sur l'ensemble du parc informatique : lorsqu'une menace est détectée sur un ordinateur, le parc informatique est balayé à la recherche des IOC de la menace et tous les ordinateurs présentant les symptômes de la menace sont isolés du réseau.
- Rapidité de la communication inter-machines lors de la recherche de la menace dans le parc informatique.

Scan anti-viral

- Scan anti-viral exhaustif de l'ordinateur ou du terminal.
- Scan rapide et ciblé de certains fichiers.
- Scan sur mesure selon des paramètres personnalisés.



STREAMSCAN
Votre partenaire de cybersécurité

FICHE EDR

SURVEILLANCE 24/7

Pendant que les solutions EDR sont excellentes pour signaler les anomalies et les comportements suspects, l'expertise humaine est souvent requise pour l'analyse approfondie de ces alertes.

StreamScan offre cette couche d'expertise cruciale avec une équipe dédiée de professionnels en cybersécurité. Nos experts surveillent les alertes de manière proactive et répondent rapidement aux menaces critiques, garantissant que vos outils de sécurité ne sont jamais une solution de type « configurez et oubliez ».

Basé à Montréal, notre Centre des Opérations de Sécurité (SOC) surveille en permanence des millions de signaux quotidiennement pour une clientèle diversifiée. Le tout est soutenu par un groupe de R&D qui maintient StreamScan à la fine pointe des menaces émergentes.

À propos de StreamScan

StreamScan est une entreprise canadienne spécialisée en cybersécurité opérationnelle englobant entre autres la surveillance de réseau, la chasse aux menaces et la réponse aux incidents.

L'équipe est composée de chercheurs en cybersécurité, de spécialistes de l'IA, d'analystes, de pirates éthiques, et d'experts en accompagnement pour diverses normes.

StreamScan se distingue en étant l'une des premières entreprises à appliquer l'IA à la détection des cybermenaces. Notre technologie a été reconnue par le gouvernement canadien comme une solution innovante en matière de cybersécurité.

Pour plus d'informations:
info@streamscan.ai
1 877 208-9040 poste 1