

Le XDR de StreamScan

Un enjeu critique pour les entreprises

Les organisations font face à une hausse constante de cyberattaques sophistiquées, rendant la détection et la réponse aux menaces plus complexes que jamais. L'utilisation de multiples outils de sécurité crée souvent des silos d'information, ce qui complique la gestion efficace des incidents.

Le XDR de StreamScan

StreamScan propose une **solution XDR (Extended Detection and Response)** qui centralise et corrèle les alertes de sécurité provenant de différentes sources. Cette approche unifiée permet une surveillance proactive et une protection renforcée des infrastructures réseau, tout en éliminant les silos et en optimisant la réactivité face aux menaces.

En complément, notre service **MDR (Managed Detection and Response)** assure une surveillance 24/7, avec des experts qui analysent et réagissent rapidement aux menaces.

Principales caractéristiques

- IDS/IPS/NDR : détection et prévention des intrusions et des cybermenaces
- Protection des terminaux (EDR & Antivirus)
- Gestion des journaux (SIEM)
- Gestion des alertes de sécurité O365
- Investigation pour la réponse aux incidents
- Scan de vulnérabilités

Principaux avantages

- **Vitesse de détection :**
réduction du temps de détection de 99 %.
- **Visibilité totale :**
couverture complète des menaces sur l'ensemble du réseau, sans angles morts.
- **Consolidation des outils :**
centralise plusieurs solutions de sécurité au sein d'une seule plateforme.
- **Réduction des alertes :**
identification et hiérarchisation automatisée des incidents.
- **Flexibilité :**
s'adapte à l'évolution des besoins des entreprises sans perte d'efficacité.
- **Développée au Canada :**
technologie de pointe breveté, conçue et maintenue au Québec.

Caractéristiques

IDS/IPS/NDR : visibilité sur le réseau

Notre solution XDR repose sur une technologie propriétaire de pointe : le CDS (système de détection des intrusions - Cyberthreat Detection System). Basé sur l'intelligence artificielle, il assure une détection et une prévention avancées des intrusions (IDS /IPS /NDR), offrant une couverture complète et en temps réel de votre réseau, sans angles morts.

Cette technologie analyse l'ensemble du trafic entrant et sortant, vous donnant une visibilité complète sur la sécurité du réseau, tout en détectant et bloquant les comportements suspects ainsi que les cyberattaques.

- Surveillance en temps réel des activités suspectes
- Détection par signatures d'attaques connues
- Détection d'anomalies pour identifier les attaques Zero-Day
- Réponse et prévention automatisées
- Extensible via API sur mesure pour besoins complexes
- Efficace même sur les systèmes où les EDR ne peuvent pas être déployés

Surveillance 24/7 par notre SOC

Notre XDR génère des alertes automatisées, renforcées par **l'expertise humaine** pour analyser les anomalies et comportements suspects. Notre équipe assure une surveillance continue et une réponse rapide aux menaces.

EDR : visibilité sur les terminaux

Notre solution EDR collecte des informations des appareils surveillés, comme les fichiers créés ou modifiés, les processus en cours, les connexions réseau ou les journaux d'événements, afin de détecter et bloquer les activités malveillantes sur les terminaux.

Notre EDR inclut un antivirus et un pare-feu et, lorsqu'elle est intégrée au CDS, elle permet l'isolement immédiat des machines infectées ainsi qu'une communication rapide entre machines pour limiter la propagation.

SIEM : Collecte des journaux

Le module de type SIEM intégré à notre XDR collecte et analyse les journaux (logs) de divers composants de votre réseau, comme les pare-feu, machines, contrôleurs de domaine (ex : Active Directory), serveurs et routeurs, en utilisant le protocole SYSLOG ou via un agent.

Gestion des alertes de O365

Les événements de sécurité O365 peuvent être intégrés à notre XDR pour une meilleure corrélation avec d'autres alertes, assurant une réponse rapide face aux attaques complexes ou distribuées. Configurez votre serveur de messagerie pour transférer les courriels à notre CDS pour une analyse approfondie. Notre système détectera les courriels malveillants, le hameçonnage (phishing) et d'autres menaces.

Caractéristiques

Alertes

Lorsque le XDR de StreamScan détecte une activité malveillante, il envoie des alertes aux équipes de sécurité pour une intervention rapide. En cas d'attaque ou d'activités malveillantes, les notifications peuvent également être envoyées par courriel ou par SMS.

Réponse automatisée

Notre XDR propose des réponses automatisées en cas de menace, telles que :

- Mise en quarantaine des fichiers infectés.
- Désactivation des processus malveillants.
- Blocage des attaques via le pare-feu centralisé ou directement sur les terminaux avec l'EDR de StreamScan, si installé.

Les paramètres de réponse peuvent être ajustés selon vos besoins spécifiques, garantissant une protection sur mesure et réactive.

Intelligence Artificielle (IA)

L'IA est au cœur de notre solution XDR :

- Algorithmes d'apprentissage automatique pour une détection proactive.
- Analyse comportementale des menaces pour repérer les anomalies.
- Analyse prédictive des menaces évolutives.
- Apprentissage continu pour s'adapter aux nouveaux vecteurs d'attaque.

Isolation des ordinateurs compromis

Lorsqu'une menace est détectée, notre XDR scanne l'ensemble du parc informatique pour identifier les IOC (Indicateurs de compromission) associés, isolant les ordinateurs compromis pour limiter la propagation.

Il assure également une communication rapide et une coordination en temps réel entre les machines lors de la détection et de la réponse aux menaces.

Console de gestion

- Interface intuitive et conviviale.
- Gestion centralisée des menaces détectées.
- Administration des EDR déployés sur tout le réseau (local, sites distants, utilisateurs VPN).
- Actions administratives via la console centralisée : isolation, arrêt de processus, blocage des communications réseau.
- Contrôle d'accès basé sur les rôles (RBAC).
- Gestion centralisée des politiques de sécurité.



Détection et blocage des rançongiciels et autre

- Analyse comportementale pour identifier les schémas typiques des rançongiciels.
- Analyse heuristique du comportement de chiffrement.
- Blocage en temps réel des activités liées aux rançongiciels.
- Réponse et remédiation rapides aux attaques
- Détection et blocage des communications malveillantes entrantes et sortantes.
- Détection et blocage des mouvements latéraux malveillant.

Caractéristiques

Détection des attaques TI et OT

Identification des attaques ciblant les environnements technologiques de l'information (TI) et opérationnels (OT).

Gestion des incidents et vérification de sites internet

Notre XDR centralise la réponse aux menaces et permet de vérifier directement si une adresse IP ou un nom de domaine est répertorié comme malveillant.

Visualisation graphique des attaques

Affichage en temps réel du flux d'attaque, avec téléchargement possible de fichiers PCAP et création de billets d'incidents associés.

Sources de données multiples

- **Réseau** : collecte du trafic entrant et sortant en PCAP, surveillance des protocoles des couches 2 à 7, détection des attaques réseau
- **Journaux (Logs)** : analyse des journaux système pour identifier les cybermenaces
- **Courriels/SMTP** : intégration O365 en cours
- **Pare-feu** : compatible avec PFSENSE, SOPHOS, FORTINET, SONICWALL, etc.

Profilage d'utilisation réseau (UBEA)

- Analyse des comportements réseau pour détecter toute déviation ou activité suspecte, indiquant une possible cyberattaque.

Scans de vulnérabilité et tests d'intrusion

- Identification des vulnérabilités critiques du réseau
- Scans sur mesure (terminaux, fichiers, etc.)
- Tests d'intrusion automatisés possibles

Gestion des accès et authentification multi-facteurs (MFA)

- Création de rôles (RBAC) pour attribuer des privilèges spécifiques.
- Connexion via Active Directory (AD) avec support de l'authentification multi-facteurs pour renforcer la sécurité.

Audit Active Directory (AD)

- Visibilité sur les groupes et utilisateurs créés dans AD.
- Collecte d'informations telles que la date de création, groupes associés, et événements liés à la sécurité.
- Notifications pour des événements tel que la création de nouveaux utilisateurs.
- Historique des connexions utilisateurs.
- Détection des tentatives de brute force.

Extraction et analyse des fichiers

- Extraction et analyse des fichiers suspects pour déterminer leur caractère malveillant.
- Notification en cas de détection de fichiers malveillants.
- Blocage automatique via le EDR ou le pare-feu en cas de menace confirmée.

Rapports et analyses

- Tableau de bord centralisé pour une surveillance en temps réel.
- Création instantanée de rapports de sécurité, avec des options de rapports périodiques automatisés selon les besoins.

Témoignages

L'équipe de StreamScan se distingue par son offre de service complète, que ce soit leur conseil technique avec leur MDR, leur expertise en cas de cyberattaque ainsi que leurs outils tels que CDS et EDR. Je recommande vivement StreamScan. Leur expertise technique, leur engagement envers l'excellence et leur service client exceptionnel en font un partenaire de confiance pour la protection des actifs numériques les plus précieux.

- Ghislain Gamache, Gestionnaire TI, Atlas Aéronautique

La centralisation de la surveillance de notre réseau et de nos EDR représente un avantage significatif, tant sur le plan financier que pour l'efficacité de la protection. Cela leur donne une vision à 360 degrés de notre réseau et de nos Endpoint. De plus, l'efficacité de leur solution EDR est remarquable. Ce qui distingue particulièrement cette équipe, c'est leur rapidité de réponse, leur professionnalisme ainsi que leur expertise. Leur engagement envers la protection de notre infrastructure est indéniable, et nous sommes extrêmement satisfaits de leur collaboration continue.

- Éric Lambert, GMP Énergie

StreamScan effectue des scans de vulnérabilités trimestrielles, identifiant et atténuant de manière proactive les menaces potentielles. Ses systèmes IPS/IDS se sont révélés essentiels pour la défense contre les tentatives d'attaques, nous permettant ainsi de maintenir la continuité de nos activités en toute confiance. Leur engagement en faveur de l'excellence et leur gestion proactive des risques ont contribué à renforcer notre position en matière de cybersécurité, faisant d'eux un élément essentiel de nos opérations. Nous recommandons vivement StreamScan à toute organisation à la recherche d'un partenaire dévoué et compétent en matière de cybersécurité.

- Anthony Gattas, Chef de l'infrastructure et de la cybersécurité, MI Composites technologie inc.

Déploiement

Sur site (VM ou serveur physique) ou dans le cloud, selon les besoins de l'entreprise.

Évolutivité

Conçu pour s'adapter à des entreprises de toutes tailles, avec une gestion basée sur le cloud offrant une mise à l'échelle flexible.

Intégration possible de la console XDR dans votre réseau local pour une gestion sur site. Possibilité de déployer la console XDR dans le Cloud.

Assistance et maintenance

- Support technique 24/7 par une équipe experte et bilingue (français/anglais)
- Mises à jour régulières des définitions de virus, des renseignements sur les menaces et du logiciel pour rester protégé.

**Pour plus d'informations,
contactez StreamScan :**

info@streamscan.ai

877 208-9040 poste 1

www.streamscan.ai