STREAMSCAN

Le XDR de StreamScan

Cybersécurité : un défi pour les entreprises

Les entreprises font face à une augmentation constante des cyberattaques sophistiquées, rendant la détection et la réponse aux menaces plus complexes que jamais. L'utilisation de divers outils de sécurité peut entraîner des silos d'information, compliquant ainsi la gestion efficace des incidents.

CDS de StreamScan

StreamScan propose une solution XDR (Extended Detection and Response) qui centralise et corrèle les alertes de sécurité provenant de différentes sources, permettant ainsi une surveillance proactive et une protection renforcée des infrastructures réseau. Grâce à cette approche unifiée, nous éliminons les silos et optimisons la réactivité face 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 (en développement)

- ➤ **Vitesse de détection :** réduction du temps de détection de 99%
- ➤ **Visibilité totale :** vue complète des menaces sur tout le réseau, sans angles morts
- ➤ **Consolidation des outils :** centralise plusieurs solutions de sécurité en une seule plateforme.
- ➤ **Réduction de la charge d'alertes :** Identification et hiérarchisation automatisée des incidents.
- ➤ **Flexibilité :** s'adapte aux besoins grandissants des entreprises sans perte d'efficacité.
- ➤ **Développée au Canada :** Technologie de pointe breveté développée et maintenue au Québec.

Charactéristiques

Cyberthreat Detection System (CDS)

Notre solution XDR intègre CDS une technologie propriétaire de fine-pointe de détection et prévention d'intrusions (IDS/IPS) basée sur l'intelligence artificielle.

Cette technologie surveille tout le trafic entrant et sortant de votre réseau vous donnant un visibilité totale sur la sécurité du réseau et pouvant détecter et bloquer les comportements suspects ainsi que les cyber attaques.

- Surveillance en temps réel des activités suspectes.
- Détection basée sur les signatures des modèles d'attaque connus.
- Détection des anomalies pour identifier les attaques Zero-Day.
- Mécanismes automatisés de réponse et de prévention.
- Extensible avec des API sur mesure pour répondre à des exigences complexes.
- Efficace sur les anciennes technologies où les EDR ne peuvent pas être installés.

Endpoint Detection & Response (EDR)

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, pour détecter et bloquer les activités malveillantes sur les terminaux. Notre EDR vient avec un anti-virus et pare-feu et quant intégré à la CDS, permet un isolement immédiat des machines infectées et communication rapide inter-machines pour limiter la propagation.

Collecte des journaux (SIEM)

Le module 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 phishing et d'autres menaces.
Note : ce module est en cours de développement

Charactéristiques

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 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 coeur de notre solution IPS/IDS:

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

Isolation rapide 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.

Communication rapide et 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 autres

- 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.

STREAMSCAN

Charactéristiques

Détection des attaques TI et OT

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

Gestion des incidents et vérification de sites internet

Notre XDR intègre un module complet pour la gestion des incidents, centralisant la réponse aux menaces. Vous pouvez directement vérifier dans notre XDR si une adresse IP ou un nom de domaine est répertorié comme malveillant.

Visualisation graphique des attaques

Affichage du flux d'attaque en temps réel, avec la possibilité de télécharger des fichiers PCAP et de créer des tickets d'incidents associés aux activités malveillantes.

Sources de données multiples

- Réseau : collecte du trafic entrant et sortant en format PCAP (full packet capture), avec surveillance des protocoles des couches 2 à 7 et détection d'attaques sur le réseau.
- Logs : les journaux générés par les systèmes du réseau sont analysés par le XDR pour détecter les cybermenaces
- Courriels/SMTP : intégration O365 en cours
- Pare-feu : compatibilité avec les principaux pare-feu (PFSENSE, SOPHOS, FORTINET, SONICWALL, etc.).

Scans de vulnérabilité et tests d'intrusion

- Possibilité de scanner votre réseau pour identifier les vulnérabilités critiques.
- Scans sur mesure selon des paramètres personnalisés (sur terminaux ou de certains fichiers, etc.).
- Possibilité de lancer des tests d'intrusions automatisés sur votre réseau.

Gestion des accès et authentification multi-facteurs (MFA)

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

Profilage d'utilisation réseau (UBEA)

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

Audit Active Directory (AD)

- Visibilité sur les groupes et utilisateurs créés dans AD.
- Collecte d'informations telles que la date de création, les groupes associés, et les 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 divers rapports de sécurité, avec des options de rapports périodiques automatisés selon les besoins.

STREAMSCAN

Déploiement, évolotivité, assistance et maintenance

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

Nous sommes ravis de partager notre expérience positive avec StreamScan, dont nous sommes clients en utilisant leur solution MDR et CDS. L'équipe se distingue par sa disponibilité sans faille et son efficacité prouvée. Leurs points de contrôle réguliers nous permettent de rester proactifs face aux menaces émergentes, tandis que leur capacité à filtrer les faux positifs nous fait gagner un temps précieux pour nous concentrer sur les vrais défis de sécurité.
- Jérémy Merlin, Chef d'équipe, Département TI LeddarTech

Déploiement

Déploiement possible dans le cloud ou sur site (VM ou serveur physique), 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 : Une équipe experte disponible en continu pour vous assister, avec un support bilingue (français et anglais).
- Mises à jour régulières des définitions de virus, des renseignements sur les menaces et des améliorations logicielles pour rester à jour face aux menaces émergentes.

STREAMSCAN