Les technologies de cybersécurité émergentes

Karim Ganame, PhD, GCIA, GCIH, CISSP

Traqueur de cybermenaces

Qui suis-je

- Dr en cybersécurité, chercheur AI & Cybersecurité
- Expert en détection d'intrusions & réponse aux incidents
- Enseignant en cybersécurité à l'Ecole Polytechnique de Montréal
- Fondateur de StreamScan

STREAMSCAN

Streamscan

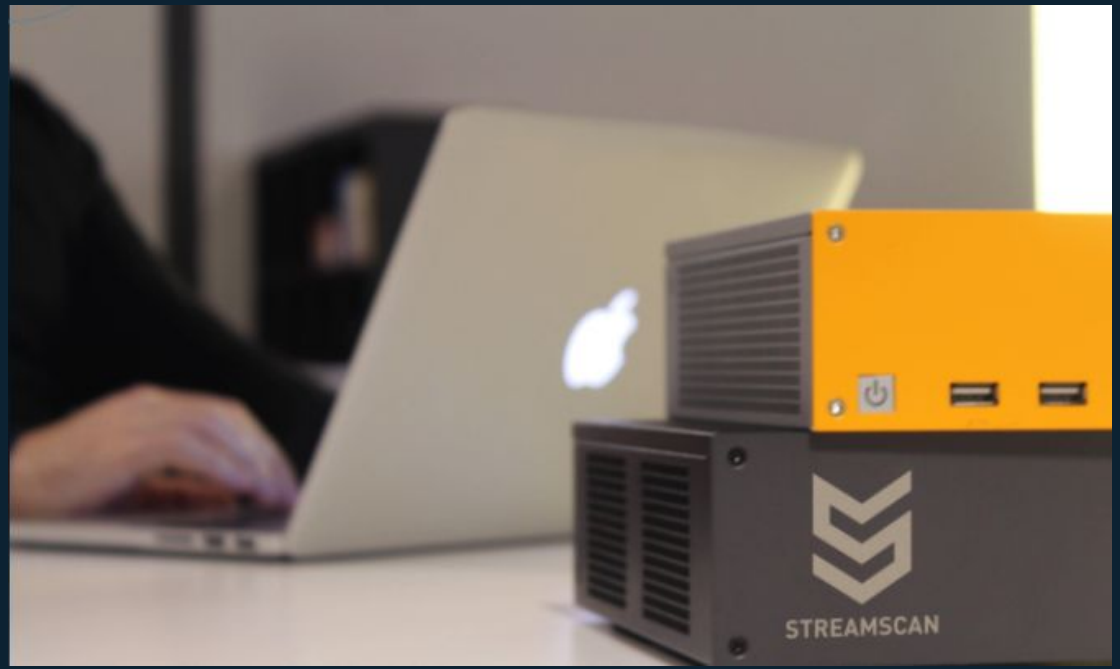
Montréal / Canada

R&D en cybersécurité & AI

- Détection d'intrusions
- Détection de malwares
- Réponse aux incidents

Technologie Cyber Threat Detection System (CDS)

- Système de détection d'intrusions (IDS) basé sur l'IA
- 1er IDS développé au Québec
- Brevet Américain sur la technologie CDS
- Sélection par le gouvernement fédéral comme innovation. Projets avec:
  - Défense Canada
  - Centre Sécurité Télécoms / CST
- Utilisée par plusieurs entreprises: manufacturières, pharmaceutiques, gouvernements, éducation, Défense, TI, etc.



Appliances CDS

- Serveurs physiques
- Serveurs virtuels
- Cloud

Centre de surveillance de cybersécurité (SOC)

Couverture 24/7

- Equipe de réponses aux incidents de sécurité
- Mise en place de SOC/CERT au Canada à l'international (Togo, Burkina)

Projet IDS avec Defence Canada (Armée de l’air)

- Détection des cyberattaques ciblant les avions de chasse
- AI & Cybersécurité

StreamScan a été sélectionné pour son expertise afin de sécuriser les avions militaires canadiens contre les cyberattaques.

Des génies d'ici protègent les avions de chasse

PARTAGEZ SUR FACEBOOK PARTAGEZ SUR TWITTER AUTRES

FRANCIS HALIN
Lundi, 9 novembre 2020 00:00
MISE À JOUR Lundi, 9 novembre 2020 00:00

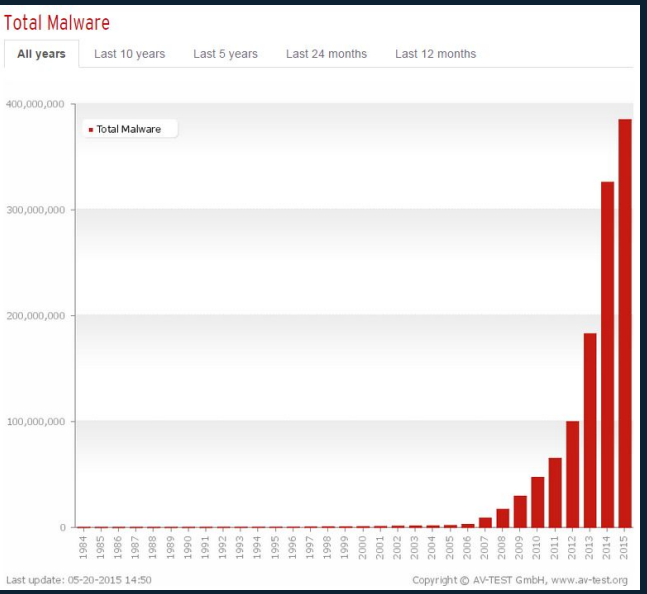
Une équipe québécoise d'élite d'une vingtaine d'employés en cybersécurité a inventé un outil informatique pour protéger les avions de chasse de l'armée.

« Lorsqu'il y a intrusion, les dégâts sont majeurs. Ça peut conduire à des écrasements ou à de l'interception d'information très sensible », explique calmement au bout du fil le PDG de StreamScan, Karim Ganame.

Fondée en 2011, l'entreprise montréalaise compte parmi ses clients de gros noms des secteurs manufacturier et pharmaceutique connus que son grand patron préfère taire pour des raisons de sécurité.

Quelques défis actuels de la cybersécurité

Défi 1- Explosion des cybermenaces



- Explosion des malwares (virus, etc.)
- 1 000 000 nouveaux malwares par jour
- Expansion de possibilités d'attaques (Facebook, sms, téléphone, etc.)
- Création de nouvelles cyberattaques/fraudes à chaque jour
- Campagnes hameçonnage COVID-19
- Cybercriminels mieux organisés

STREAMSCAN

Depuis mars 2020

De plus en plus d'infections par ransomware

- EMOTET
- RYUK
- NETWALKER
- SUNCRYPT
- SODINOKIBI

* Exfiltration de données
* rançons plus élevées: 150K$ US et plus

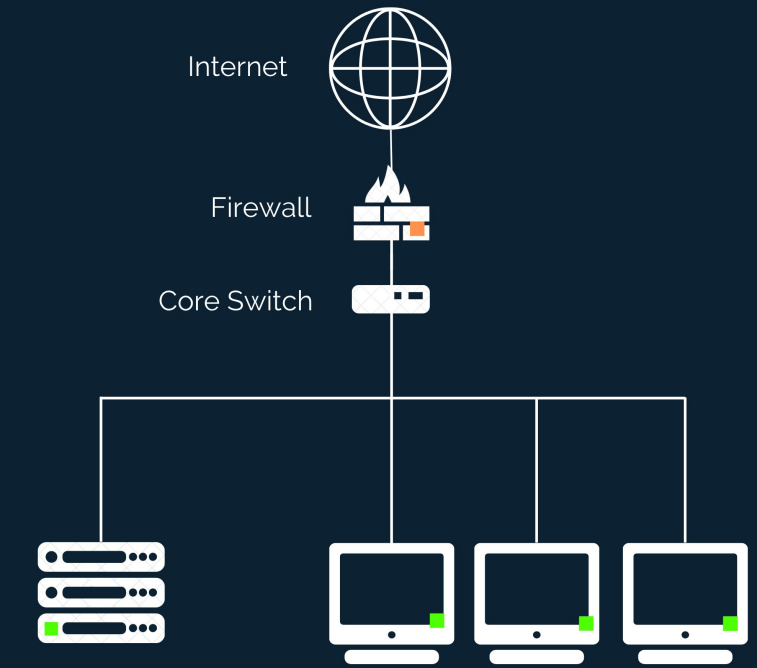
Pics de piratage de comptes Outlook dans le Cloud

- Hameçonnage
- Informations achetées sur le Darkweb

Recrudescence des attaques ciblées

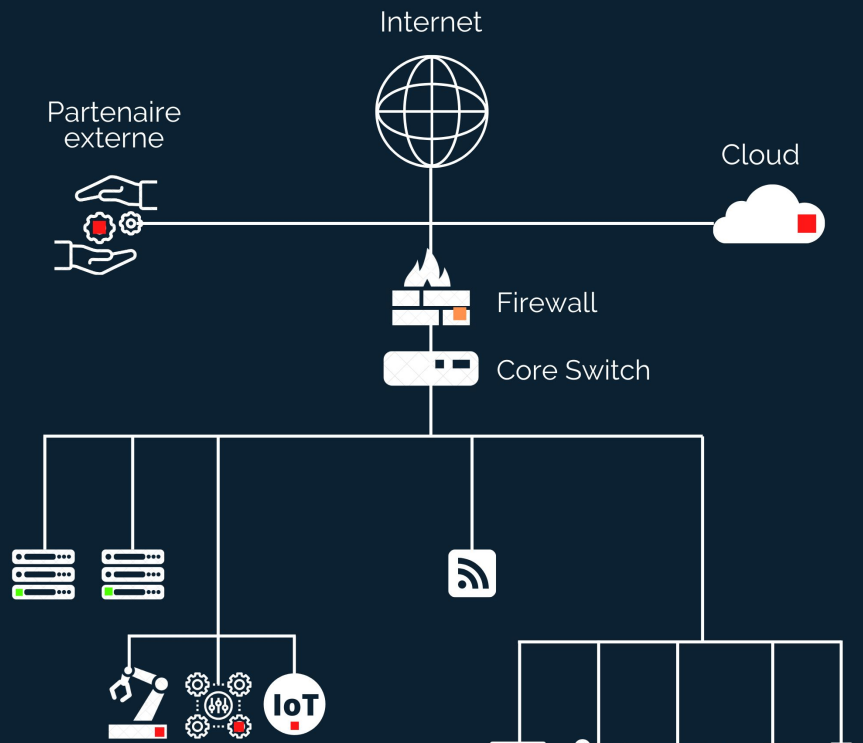
- DDOS + demande de rançon

Défi 2- Les réseaux sont de plus en plus complexes



Sécurité

- Firewall
- Anti-virus



Sécurité

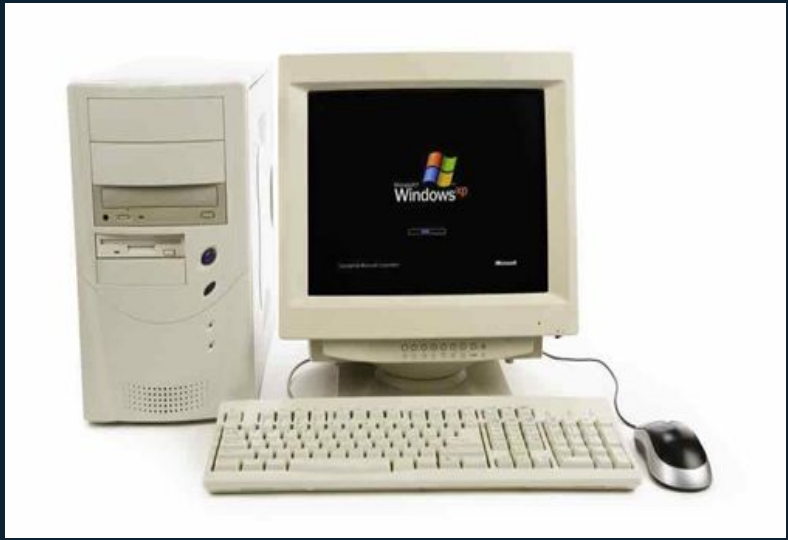
- Firewall
- Anti-virus
- Non sécurisé

Défi 3- Les organisations en savent peu sur les pirates

Cyber défense est un problème d’asymétrie d’information

STREAMSCAN

Défi 4- Pas de gestion des vulnérabilités



La cybersécurité du parc informatique se dégrade continuellement

Défi 4- Pas de visibilité totale sur le réseau

On ne peut se défendre que contre ce qu’on voit.

STREAMSCAN

Défi 5- Manque de ressources qualifiées

- Il manque 20 M d’experts d’ici 2025
- 80% officiers, 20% de soldats

STREAMSCAN

Les technologies émergentes en cybersécurité

Tendance 1:
Détection de cybermenaces:
AI / Automatisation

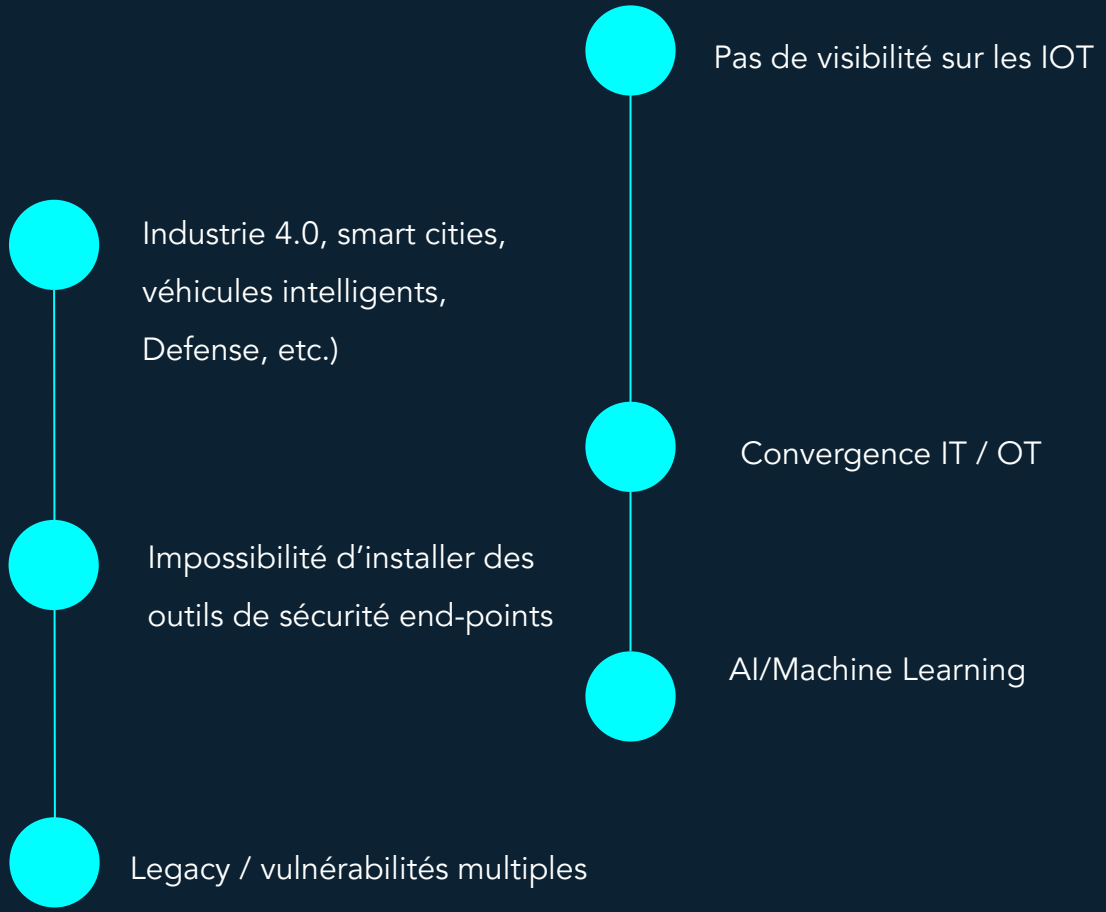
- Détection d'anomalies
- Automatisation de la détection des cybermenaces
- Automatisation de la réponse

- AI & Machine Learning
- Modèles supervisés
  Modèles non supervisés

Tendance 2:
Détection sur du trafic chiffré (5G, etc.)

- Reconnaître des patterns dans du trafic chiffré
- Détection d'intrusions
- Détection d'exfiltration de données DLP
- Vitesse de détection
- Abstraction des méthodes de chiffrement utilisées

Tendance 3: Sécurité IOT



Quelques autres tendances AI

- La détection des cas d'hameçonnage
- Détection comportementale de ransomwares
- Confirmation du caractère ciblé ou non des cyberattaques
- Détection des menaces internes (insider threat)
- Attribution des attaques

Quelques autres tendances

- Threat Intelligence
- Détection de vulnérabilités zero-day
- Zero Trust
- Identité numérique
- Informatique Quantique

Pour plus d’information

ganame@streamscan.ai
abdoul-karim.ganame@polymtl.ca