



# STREAMSCAN

---

GESTION DES INCIDENTS DE SÉCURITÉ:  
DE LA REACTIVITÉ A LA PROACTIVITÉ

Karim Ganame, PhD  
ganame@streamscan.io

18 mai 2017

# Agenda

---



- ✓ Qui suis-je?
- ✓ Réponse aux incidents de sécurité
- ✓ Quelques constats
- ✓ Recommandations

# Karim Ganame

---

- Docteur en cyber sécurité
- Spécialiste en détection d'intrusions et gestion des incidents
- Conseiller sénior en cyber sécurité
- Mise en place de CERT national
- Chercheur en cyber sécurité
- Fondateur de StreamScan inc.
  - Détection comportementale des brèches de sécurité
  - Intelligence artificielle et Machine Learning
- Enseignant à l'Ecole Polytechnique de Montreal

# Centre de reponse aux incidents



# CENTRE DE REPONSE AUX INCIDENTS

---



Computer  
Emergency  
Response  
Team  
ou **SOC**

# Plan de réponse aux incidents

---

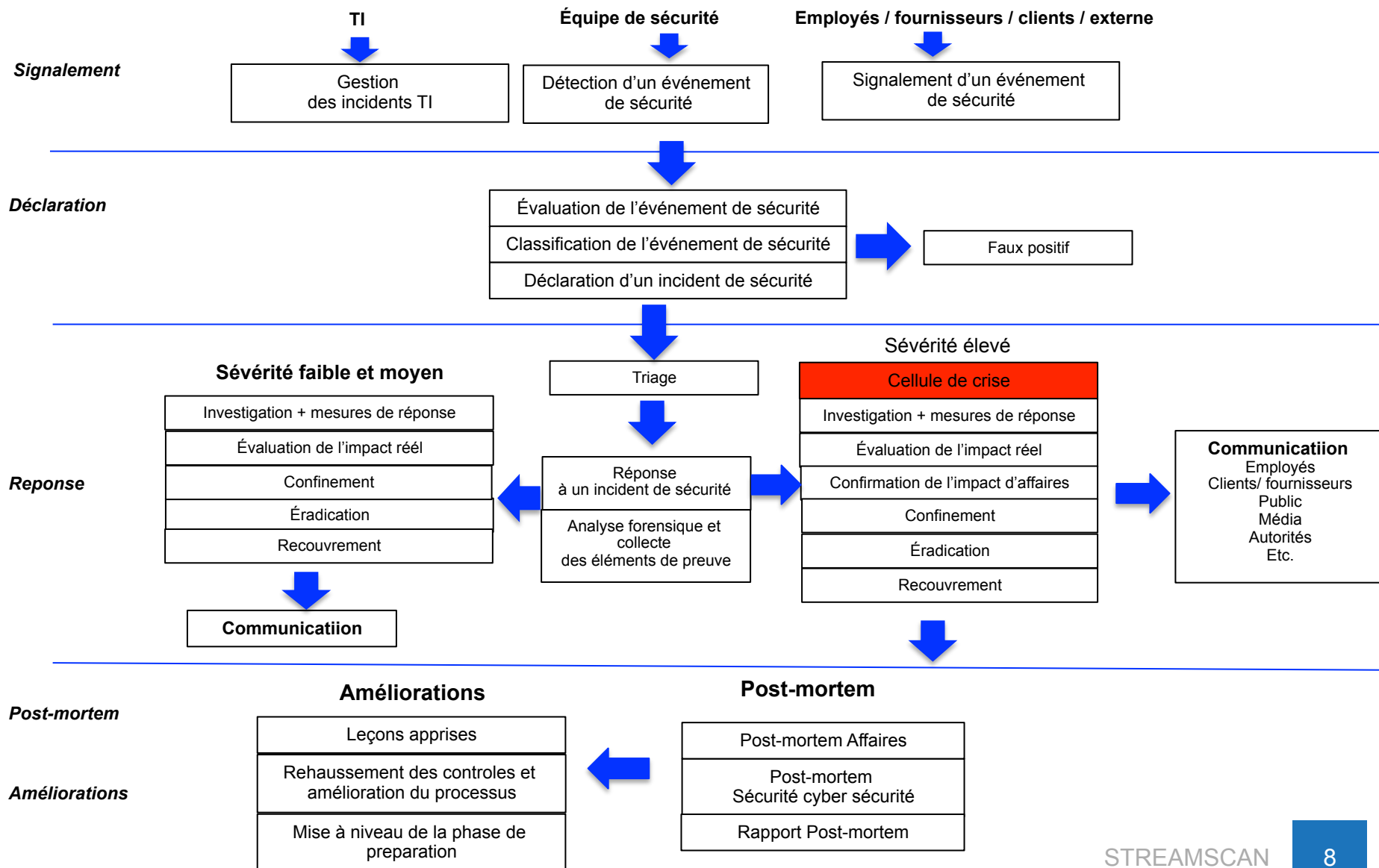
- Structure organisationnelle et équipe de réponse aux incidents (CSIRT)
- Rôles et responsabilités
- Processus de gestion des incidents
- Liste d'escalade
- Procédures opérationnelles de réponse aux incidents
- Outils technologiques

# Phase 1 : Préparation

---

- Définition de la portée
- Identification les types d'incidents et classification
- Définition des guides opérationnels de réponse aux incidents
- Définition de la structure de l'équipe de réponse aux incidents et assignation des ressources
- Formation des ressources
- Simulations et tests périodiques de gestion d'incidents

# Phase 2 : Processus de gestion des incidents





# Constat 1: 2 maillons faibles

---

## La détection

- Plusieurs incidents sont découverts par hasard
- Longs délais de détection des incidents: 205 jours en moyenne en 2015!
- Utilisation exclusive d'outils basés sur des signatures (révolus aujourd'hui!)

## La préparation

- La gestion des incidents connus est généralement efficace
- Malgré la préparation, les délais de réponse sont souvent longs
- La gestion des incidents inconnus est très souvent inefficace
  - Tâtonnement
  - Résignation

# Constat 2: les cyber menaces explosent

---

- Explosion du nombre de malwares
  - 2013: 200 000 nouveaux malwares par jour
  - 2014: 800 000 jour
  - 2016: 1.8 M par jour
- Les outils basés sur la détection par signatures sont de moins en moins efficaces (IDS, SIEM, antivirus, etc.)
  - Impossible de créer une signature pour chaque menace

# Constat 3: les CSIRT sont (trop) conservateurs

---

- Focus sur les incidents connus
- Une procédure de réponses par type d'incidents
  - DDOS
  - Ver
  - Fuite d'information sensible
  - Etc.
- Gestion approximative des incidents dont la procedure de reponse est inexistante

# Constat 4: le focus n'est pas mis sur la détection rapide des incidents

---

- Long délai moyen de détection des incidents
  - 2014: 240 jours
  - 2015: 205 jours
- Impact des incidents plus grand

# Constat 5: gestion des vulnérabilités pas souvent efficace

---

- Focus sur les avis de sécurité des éditeurs et scans de vulnérabilités
- Très peu ou pas d'intelligence sur les menaces
  - Shadow Brokers a publié l'exploit ETHERNALBLUE (exploitation SMB) en avril 2017
  - Microsoft a publié un patch en mars 2017
  - Wannacry: 12 mai 2017, surprise générale!
- Utilisation d'OS non supportés
  - XP, etc.

# Constat 6: gestion approximative des incidents inconnus (zero-day)

---

- Très peu de préparation des équipes opérationnelles
  - Long délai de traitement
    - réponse pas souvent efficace
    - Application de plusieurs signatures pour confiner l'incident
    - Tâtonnement
  - Ces types d'incidents ont le plus d'impact
- Il y aura de plus en plus d'incidents zero-day!**

# Constat 7: Les menaces evoluent plus vite que les bonnes pratiques

---

- Les principales références de gestion des incidents sont peu actualisées
  - **NIST 800-61** (Computer Security Incident Handling Guide, 2008, update 2012!)
  - **ISO 27035** (2011, update 2016)
  - **Gouvernement du Canada Information Technology Incident Management Plan** (mai 2012, update aout 2016)
- La liste des incidents définis peut être en décalage avec la réalité de l'entreprise

# Constat 8: les simulations et cas pratiques de gestion d'incidents ne sont pas exhaustifs

---

- Guides opérationnels inadaptés
- Pas de simulation d'incidents de type zero-day
  - Connus comme étant le plus d'impact



# Cas du zero-day Wannacry

---

- Début de l'infection: vendredi 12 mai 2017
- Environ 100 pays touché en 1 jour
- 150 pays touchés en 3 jours, environ 200 000 ordinateurs infectés
- Ramsonware exploitant une vulnérabilité Windows SMB
  - Patch Windows disponible depuis mars 2017!
  - Peu d'entreprises ont appliqué les correctifs
  - Gestion chaotique (comme tous les zero-day majeurs)

# Cas du zero-day Wannacry



# Wannacry: quelques indicateurs de compromission

---

## Executables

C:\Windows\mssecsvc.exe

C:\Windows\tasksche.exe

## Clés de registre

HKEY\_LOCAL\_MACHINE\Software\WanaCrypt0r

## Domaines

[www.iuqerfsodp9ifjaposdfjhgosurijfae](http://www.iuqerfsodp9ifjaposdfjhgosurijfae)

[wrwergwea.com](http://wrwergwea.com)

Rphjmrpwmfv6v2e.onion

Gx7ekbenv2riucmf.onion

www.oaghpufdjvuoapis2.com

[www.lwjf2u7djhf6ggwz4obt6fm](http://www.lwjf2u7djhf6ggwz4obt6fm)

## Fichiers créés

@Please\_Read\_Me@.txt

@WanaDecryptor@.exe

@WanaDecryptor@.exe.lnk

taskse.exe

taskdl.exe

## IP

197.231.221.221:9001

128.31.0.39:9191

213.61.66.116:9003

79.172.193.32:443

38.229.72.16:443

# Detection via Snort (signature IDS)

(<http://docs.emergingthreats.net/bin/view/Main/2024218>)

```
alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo  
Request (set)"; flow:to_server,established; content:"00 00 00 31 ff|SMB|2b 00 00 00 00 18 07  
c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|" distance:0;  
flowbits:set,ETPRO.ETERNALBLUE; flowbits:noalert; classtype:trojan-activity; sid:2024220; rev:1;)
```

```
alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo  
Response"; flow:from_server,established; content:"00 00 00 31 ff|SMB|2b 00 00 00 00 98 07  
c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|" distance:0;  
flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:1;)
```



# Analyse Wannacry par StreamScan (2)

wannacry-wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.0.186

No.	Time	Source	Destination	Protocol	Length	Info
12472	1169.282310	192.168.0.186	171.25.193.9	TCP	60	49542→80 [ACK]
12625	1192.682294	192.168.0.186	194.109.206.212	TCP	66	49545→443 [SYN]
12626	1192.776617	194.109.206.212	192.168.0.186	TCP	66	443→49545 [SYN]
12627	1192.776750	192.168.0.186	194.109.206.212	TCP	60	49545→443 [ACK]
12628	1192.790959	192.168.0.186	194.109.206.212	TLSv1.2	279	Client Hello
12629	1192.884848	194.109.206.212	192.168.0.186	TCP	60	443→49545 [ACK]
12630	1192.886155	194.109.206.212	192.168.0.186	TLSv1.2	810	Server Hello,
12631	1192.893103	192.168.0.186	194.109.206.212	TLSv1.2	180	Client Key Ex
12632	1192.987693	194.109.206.212	192.168.0.186	TLSv1.2	105	Change Cipher
12633	1192.988106	192.168.0.186	194.109.206.212	TLSv1.2	92	Application Da
12634	1193.090327	194.109.206.212	192.168.0.186	TCP	1514	[TCP segment c
12635	1193.090351	194.109.206.212	192.168.0.186	TLSv1.2	118	Application Da
12636	1193.090484	192.168.0.186	194.109.206.212	TCP	60	49545→443 [ACK]
12637	1193.091840	192.168.0.186	194.109.206.212	TLSv1.2	1111	Application Da
12639	1193.187549	194.109.206.212	192.168.0.186	TLSv1.2	597	Application Da
12640	1193.188212	192.168.0.186	194.109.206.212	TLSv1.2	1111	Application Da
12641	1193.285542	194.109.206.212	192.168.0.186	TLSv1.2	597	Application Da

Frame 12628: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits)

Ethernet II, Src: CompalIn\_69:28:7b (00:26:22:69:28:7b), Dst: ZyxelCom\_57:92:92 (04:bf:6d:57:92:92)

Internet Protocol Version 4, Src: 192.168.0.186, Dst: 194.109.206.212

Transmission Control Protocol, Src Port: 49545, Dst Port: 443, Seq: 1, Ack: 1, Len: 225

Secure Sockets Layer

0000 04 bf 6d 57 92 92 00 26 22 69 28 7b 08 00 45 00 ..mW...& "i({..E.  
0010 01 09 12 88 40 00 00 06 94 c2 c0 a8 00 ba c2 6d ....@... ..m

Wireshark · Packet 12628 · wannacry

- ▶ Cipher Suites (24 suites)
- Compression Methods Length: 1
- ▶ Compression Methods (1 method)
- Extensions Length: 127
- ✦ Extension: server\_name
  - Type: server\_name (0x0000)
  - Length: 38
- ✦ Server Name Indication extension
  - Server Name list length: 36
  - Server Name Type: host\_name (0)
  - Server Name Length: 33
  - Server Name: **www.zjnnqqzkmkyczkug73uq4dtj2y.com**
- ▶ Extension: ec\_point\_formats

0000 04 bf 6d 57 92 92 00 26 22 69 28 7b 08 00 45 00 ..mW...& "i({..E.  
0010 01 09 12 88 40 00 00 06 94 c2 c0 a8 00 ba c2 6d ....@... ..m  
0020 ce d4 c1 89 01 bb 53 db f6 fc 3b 23 c8 22 50 18 .....S. .;#. "P.  
0030 01 00 f7 76 00 00 16 03 01 00 dc 01 00 00 d8 03 ....V... ..  
0040 03 87 d4 e8 cf 48 b7 b1 09 42 ff c7 37 27 57 36 .....H.. .B..7'W6  
0050 a7 cc 9b 00 aa 5e e9 b4 79 1e 2f ef e7 07 26 eb .....^.. y./...&.  
0060 df 00 00 30 c0 2b c0 2f c0 0a c0 09 c0 13 c0 14 ...0.+./ .....  
0070 c0 12 c0 07 c0 11 00 33 00 32 00 45 00 39 00 38 .....3 .2.E.9.8  
0080 00 88 00 16 00 2f 00 41 00 35 00 84 00 0a 00 05 ...../ .A .5.....  
0090 00 04 00 ff 01 00 00 7f 00 00 00 26 00 24 00 00 .....& \$  
00a0 21 77 77 77 2e 7a 6a 6e 71 71 7a 6b 6d 6b 79 63 jwww.zjnn qqzkmkyc  
00b0 7a 6b 75 71 37 33 75 71 34 64 74 6a 32 79 2e 63 zkug73uq 4dtj2y.c  
00c0 6f 6d 00 0b 00 04 03 00 01 02 00 0a 00 1c 00 1a om.....  
00d0 00 17 00 19 00 1c 00 1b 00 18 00 1a 00 16 00 0e .....  
00e0 00 0d 00 0b 00 0c 00 09 00 0a 00 23 00 00 00 0d .....#...  
00f0 00 20 00 1e 06 01 06 02 06 03 05 01 05 02 05 03 .....  
0100 04 01 04 02 04 03 03 01 03 02 03 03 02 01 02 02 .....</p></div>
<div data-bbox="760 937 890 962" data-label="Page-Footer">STREAMSCAN</div>
<div data-bbox="914 939 944 962" data-label="Page-Footer">22</div>

# Pouvait-on detecter Wannacry?

---

- Détection par signatures (antivirus, IDS, SIEM, etc.): **NON**
- Détection comportementale : **OUI**
  - detection de "**random-generated domain**"
    - *Ex: luqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*
  - Comment?: **IA et Machine Learning**, etc.  
→ **Module disponible dans le CDS de StreamScan**
- Toute communication avec un domaine auto-généré est potentiellement suspect

# Recommandation R1 : mieux gérer les vulnérabilités de sécurité

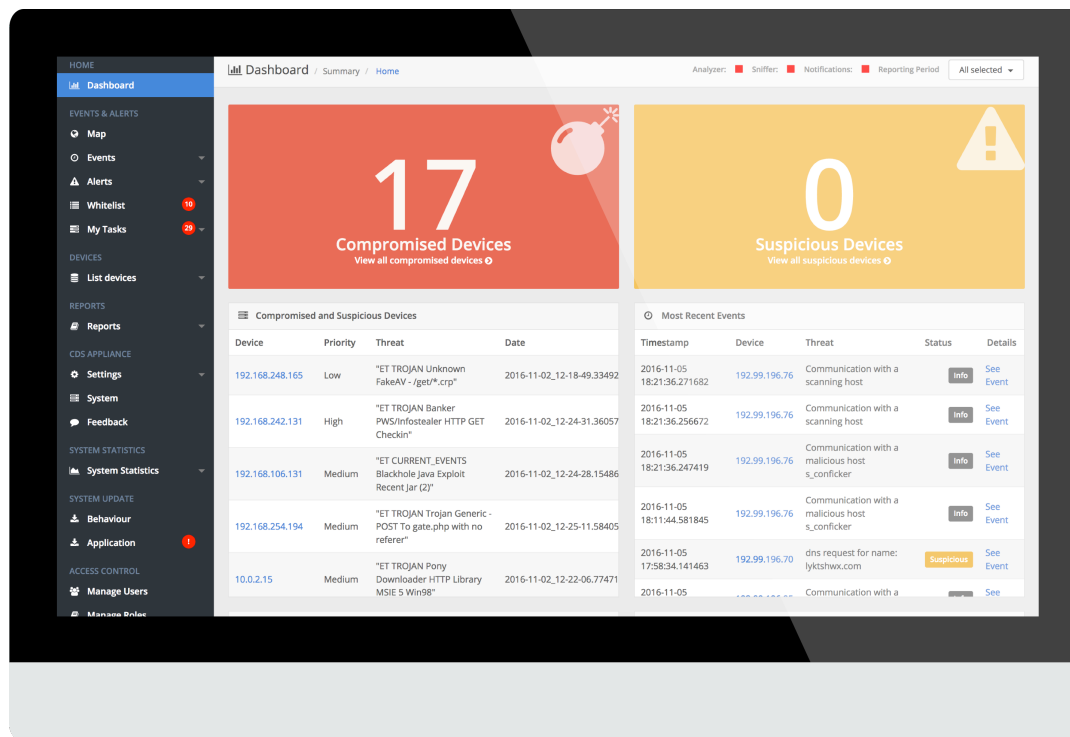
---

- Appliquer les correctifs de sécurité
- Décommissionner les systèmes non supportés (XP, etc.)
- Coupler Intelligence sur les menaces et gestion des vulnérabilités
- Rester alerte

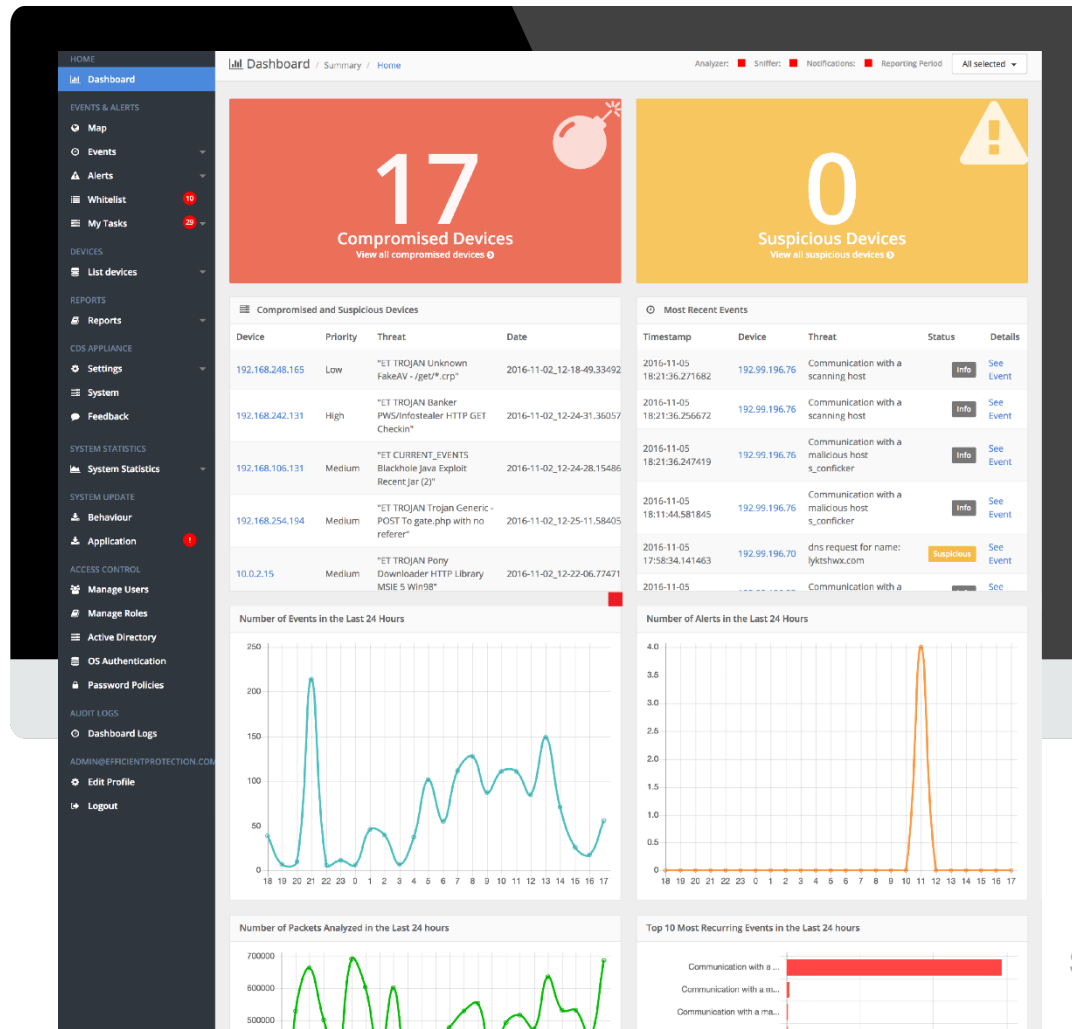


# R2 : connaitre ses risques

- Ne pas se fier uniquement aux types d'incidents identifiés par les références reconnues (NIST, etc.)
- Réaliser périodiquement une cartographie des types de cyber menaces réelles qui ciblent votre réseau. Ex: TOP 10 ou TOP 15

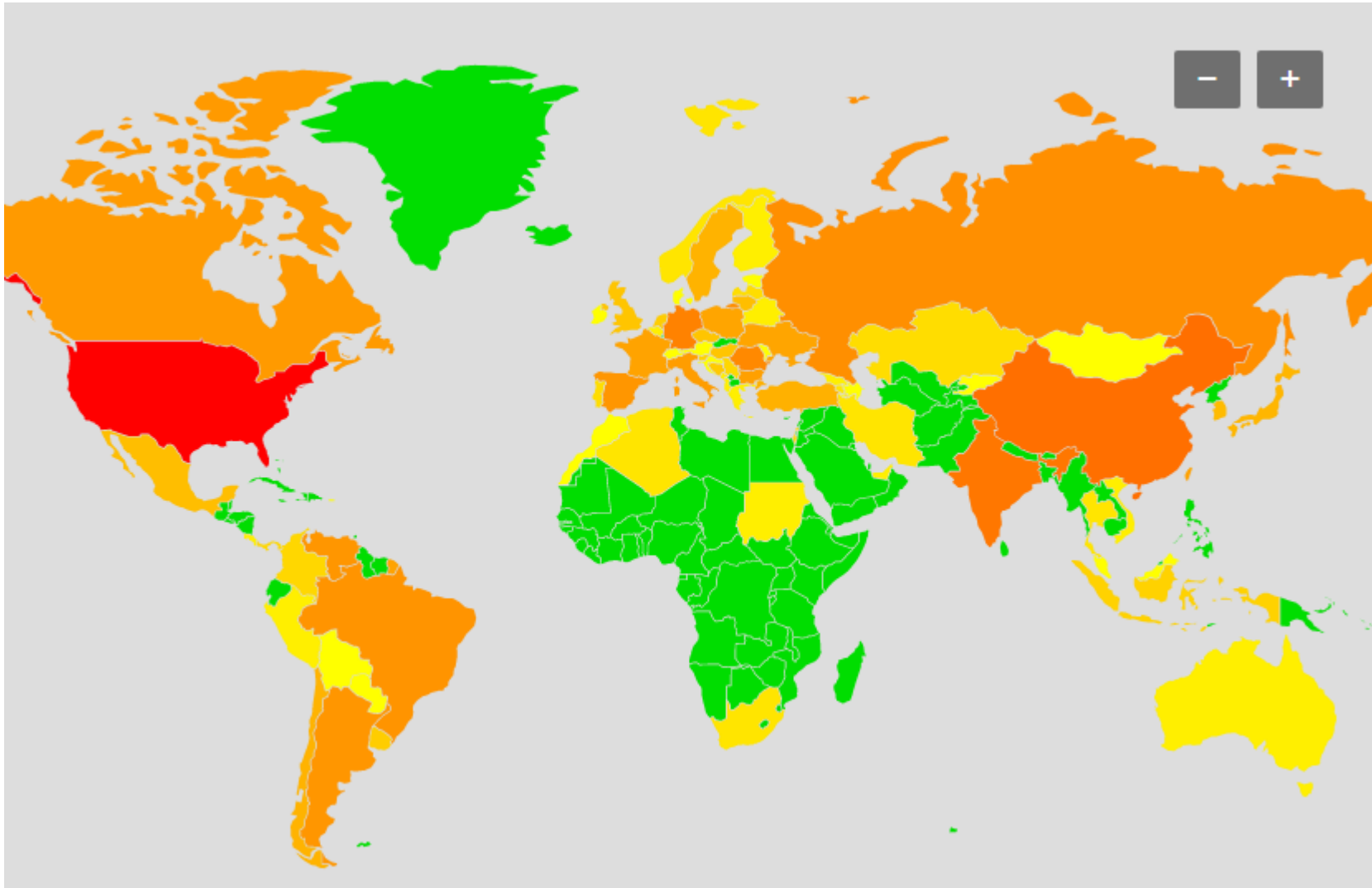


# R3: mieux connaître la sécurité de son réseau (vue du CDS de StreamScan)





## R4 : connaitre les sources des attaques qui vous ciblent (vue du CDS de StreamScan)



# R5 : mettre l'accent sur la detection rapide des incidents

---

- Permet de minimiser les impacts
  - Les délais de detection actuels sont trop longs (205 jours!)
- Les outils basés sur des signatures ne sont plus suffisants
  - Trop grand volume de cyber menaces
- Utiliser des outils comportementaux

# R6 : se preparer à faire face aux incidents zero-day

---

- Déployer un outil de sécurité comportemental et identifier le TOP 10 ou 15 des menaces comportementales
- Développer des procédures opérationnelles de réponse
  - Environ 70% des nouvelles cyber menaces sont des variantes de menaces existants
- Se préparer à faire face aux incidents de type zero-day
  - Simulations

# Evolution des ramsonwares

---

- **Jusqu'en 2016:** encryption disque et demande de rançon
- **2017:** encryption + propagation dans le réseau
  - Wannacry est un ballon d'essai
  - Plusieurs variantes vont apparaitre
    - de plus en plus sophistiqués et difficiles à detecter
- **2018+**
  - Bombe logique + encryption massive dans le réseau
  - Recrudescence des demandes de rançon via DDOS

➔ **Soyez proactifs et anticipez**

# A surveiller: exploits publiés par le groupe Shadow Brokers



GitHub, Inc. [US] | [https://github.com/x0rz/EQGRP\\_Lost\\_in\\_Translation](https://github.com/x0rz/EQGRP_Lost_in_Translation)

3 commits

1 branch

0 releases

1 contributor

Branch: master

New pull request

Find file

Clone or download

x0rz updated README

Latest commit 6692b14 on Apr 14

oddjob	initial upload	a month ago
swift	initial upload	a month ago
windows	initial upload	a month ago
README.md	updated README	a month ago

Decrypted content of odd.tar.xz.gpg, swift.tar.xz.gpg and windows.tar.xz.gpg

Downloaded from [https://yadi.sk/d/NJqzpqo\\_3GxZA4](https://yadi.sk/d/NJqzpqo_3GxZA4) Original post from the #ShadowBrokers  
<https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation>

- windows:** contains Windows exploits, implants and payloads
- swift:** contains operational notes from banking attacks



**QUESTIONS?**

# StreamScan

---

## Adresse

2300 Rue Sherbrooke Est, Suite 1, Montreal, H2K 1E5

## Téléphone

+1 514-600-1136

## Numéro gratuit (Canada et USA)

1 877-208-9040

## Support technique

1-800-601-2802  
+1 438-795-5213

## Email

info@streamscan.io

<https://www.streamscan.io>



@streamscan