BIG DATA APPLIQUÉES À LA SÉCURITÉ

Emmanuel MACÉ – Akamai Technologies

Akamai
FASTER FORWARD

DÉFINITIONS

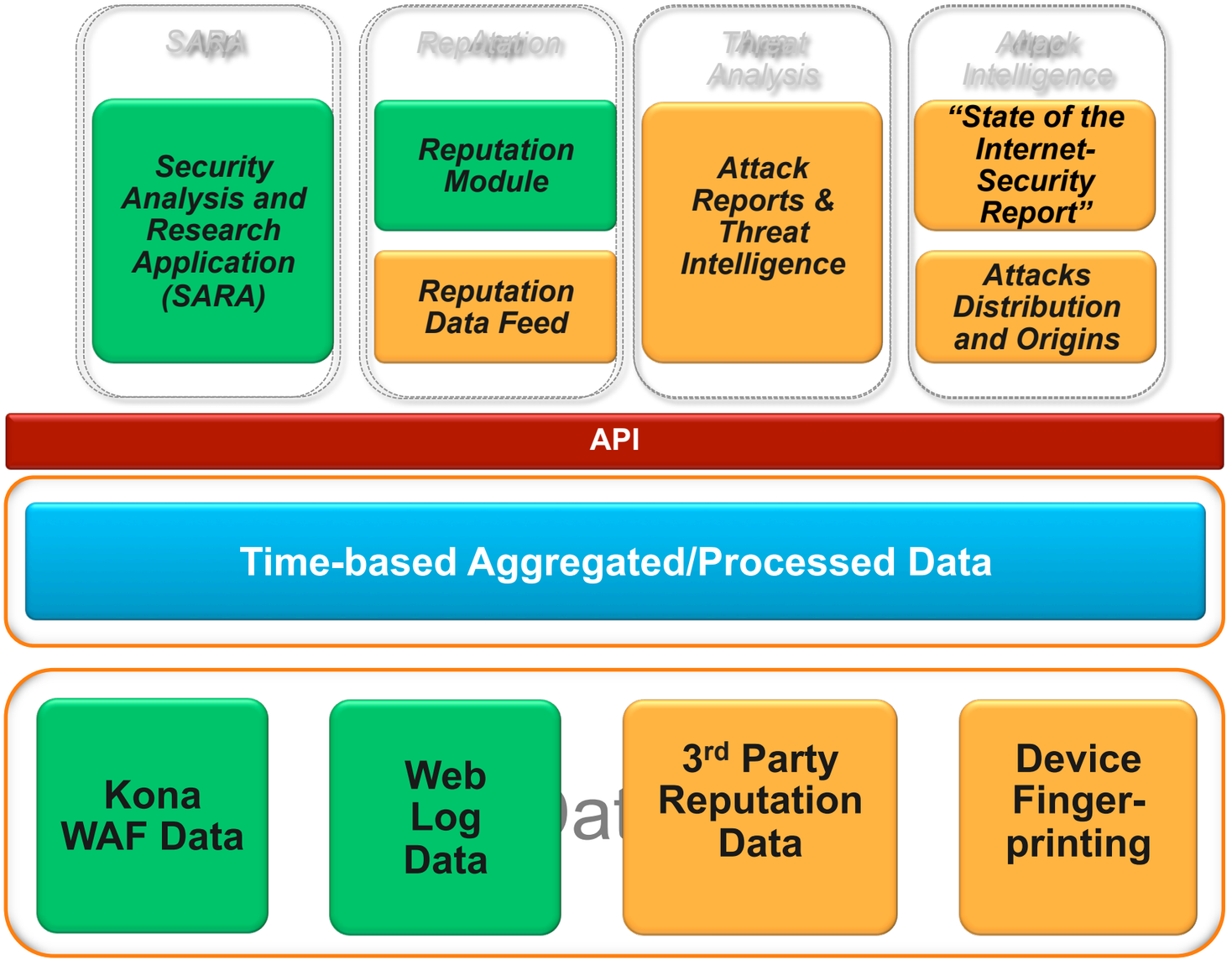
Définitions

Les big data désignent des ensembles de données qui deviennent tellement volumineux qu'elles en deviennent difficiles à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information.

Big Data, c'est comme le sexe chez les ados:

- *Tout le monde en parle*
- *Personne ne sait vraiment comment faire*
- *Tout le monde pense que les autres en font*
- *Donc tout le monde prétent qu'il le fait…*

Architecture du Big Data chez Akamai



Le Big Data en quelques chiffres

20 Terabytes de données relatives aux attaques

2 Petabytes de données “sécurité” stockées

45 jours de retention

140K connexions simultanées (données entrantes)

600K log lines / sec. indexées en 30 dimensions

8000 requètes journalières scannant des terabytes de données

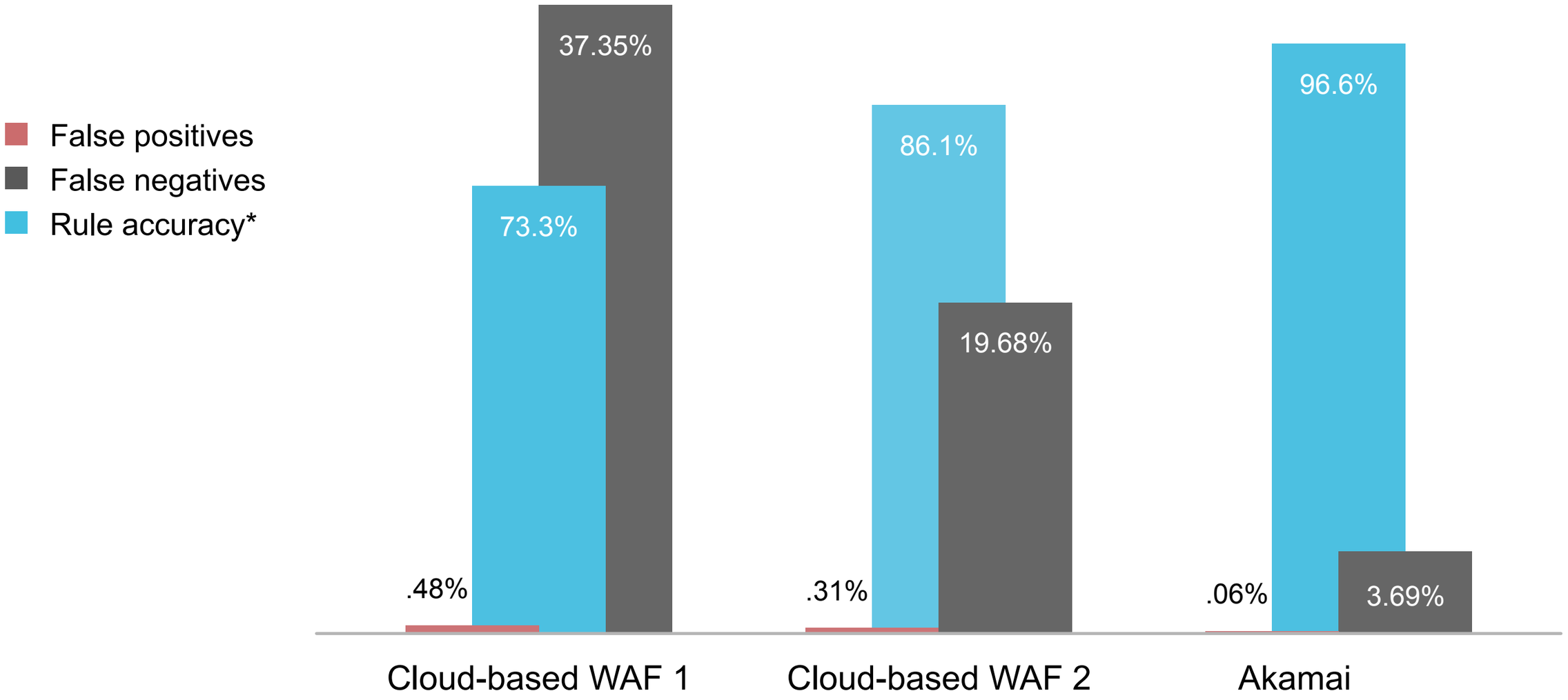
Bénéfices

Visibilité hors normes

- Amélioration des règles du pare-feu applicatif
- Détection de nouvelles attaques,
- Corrélation & apprentissage, cross-client

- Un puissant outil de recherche
- Création de nouvelles règles de filtrage
- Réputation client

Utilisation des Big Data pour améliorer le firewall applicatif



CAS CLIENT

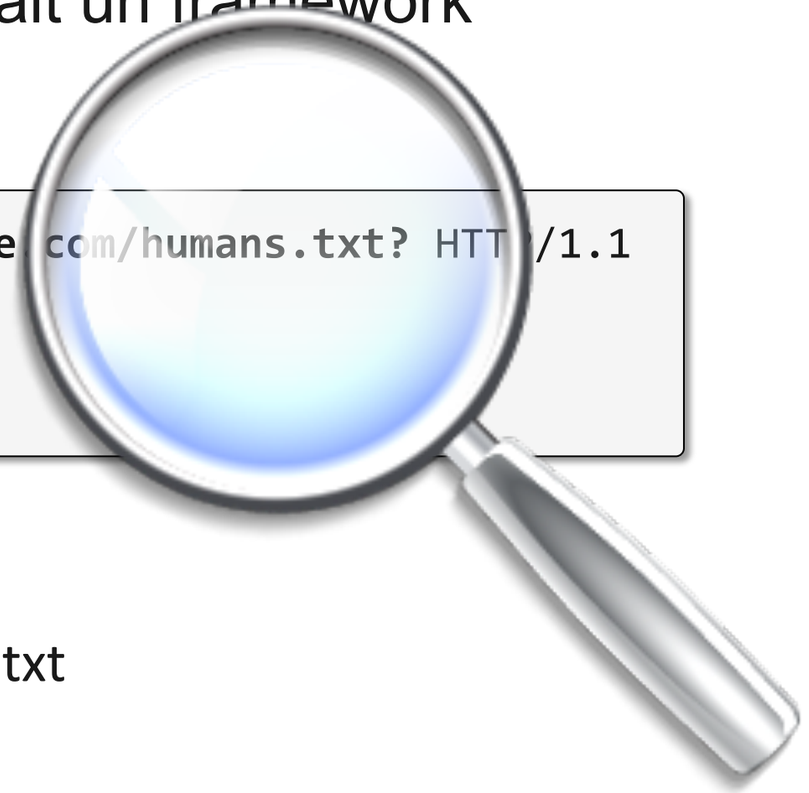
Utilisation des Big Data pour comprendre les attaques

The following slides are based on a real events on January 5th 2014….

Utilisation des Big Data pour comprendre les attaques

Une tentative d'exploitation d'une ancienne vulnérabilité dans Wordpress permettant une attaque de type RFI. La Victime utilisait un framework ASP.NET

```
GET /wp-content/wordtube-button.php?wpPATH=http://www.google.com/humans.txt? HTTP/1.1
Host: www.vulnerable.site
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4)
```

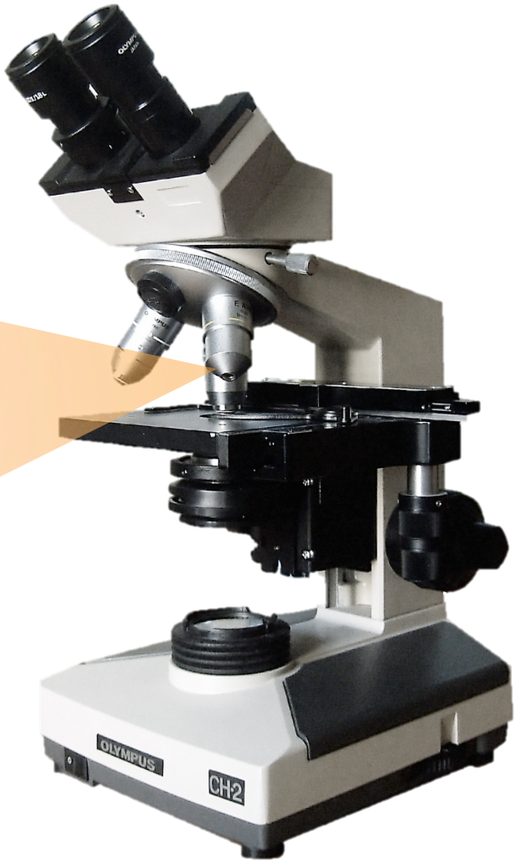


Attacked parameter : wpPATH

Malicious payload: http://www.google.com/humans.txt

Utilisation des Big Data pour comprendre les attaques

Le même attaquant a envoyé 2122 tentative de RFI



34 sites furent attaqués par le même personne

Cumulant un total de 24,301 attaques

Utilisation des Big Data pour comprendre les attaques

L'origine de l'attaque provenait d'un botnet contenant un set de 272 machines d'attaques

1696 applications furent visées

1,358,980 attaques furent lancées durant cette camapagne

La campagne dura 2 semaines

EVERYONE
AND EVERYTHING IS
GETTING **CONNECTED**

Questions & Answers