aDvens

SECURITY FOR THE DIGITAL AGE

COMMENT FAIRE FACE À LA MENACE CYBER ?

1ER PURE-PLAYER FRANÇAIS DE LA CYBERSÉCURITÉ

Depuis près de 20 ans, nous accompagnons nos clients pour les aider à prendre de l'avance et faire de la sécurité un actif différentiateur.

200
Collaborateurs
Paris, Lille, Lyon, Bordeaux & Nantes

30%
Croissance annuelle

+300
Clients actifs
En France et à l'international

PALMARÈS Capital MEILLEUR CABINET DE CONSEIL 2019

silicon Cybersecurity Awards

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

VISA DE SÉCURITÉ ANSSI

Happy AT WORK

choose Happy 2019 FRANCE

CESIN

Ensemble… …en avance

« L'ère numérique transforme nos horizons et ouvre des voies innombrables pour développer nos entreprises, améliorer nos modes de vie et apporter des solutions concrètes aux défis de notre société …à condition de créer le halo de confiance qui favorise son essor. »

Ensemble, faisons du numérique une opportunité pour un monde meilleur !

UNE MENACE CROISSANTE

Avant, la question était…

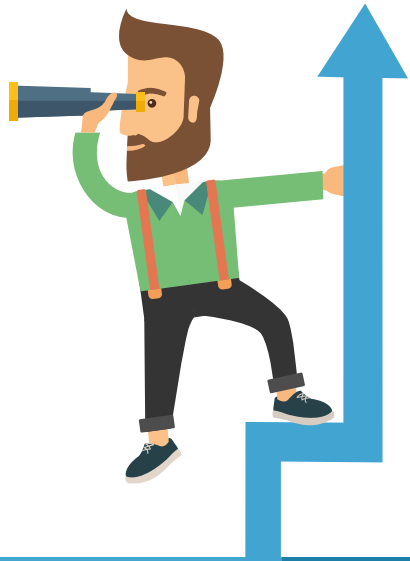
« Sera-t-on un jour attaqué ? »

Puis la question a été…

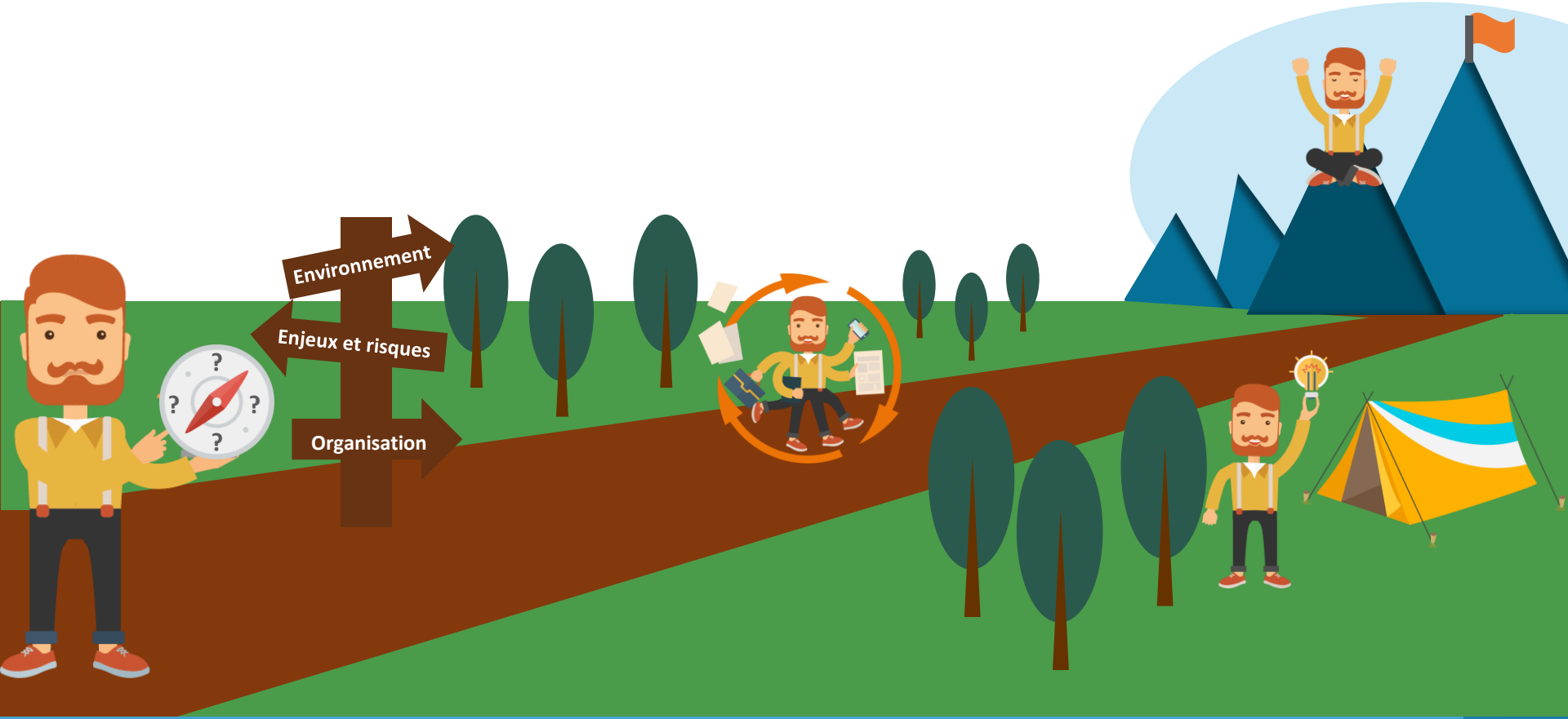
« Quand va-t-on être attaqué ? »

Maintenant la question est…

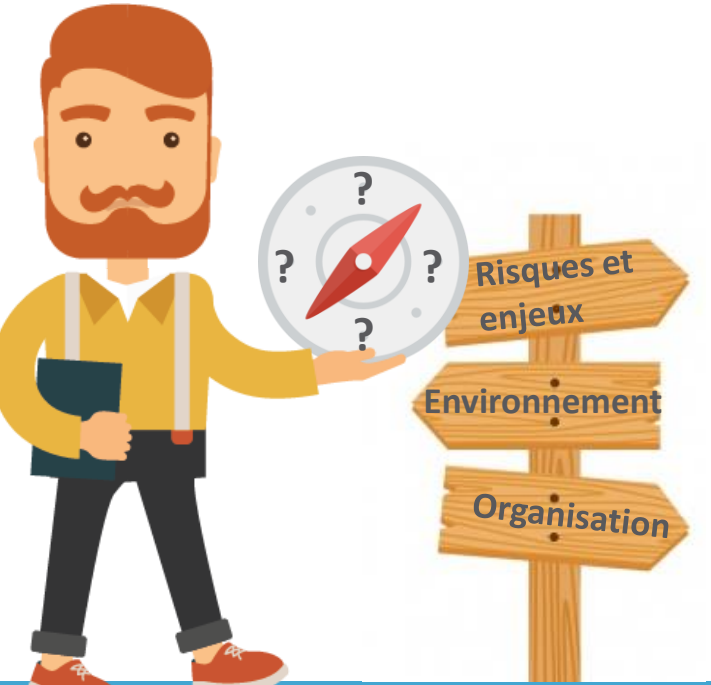
« Va-t-on se relever après la prochaine attaque ? »



QUELLE FEUILLE DE ROUTE SÉCURITÉ ?



QUELLE FEUILLE DE ROUTE SÉCURITÉ ?



Prévention

Mesures de sécurité, techniques et organisationnelles, prévues pour faire en sorte d'éviter les incidents ou d'en réduire les impacts

EXEMPLE : sensibilisation, formation, firewall, proxy

Détection

Dispositifs de surveillance et d'observation permettant de détecter les comportements à risque ou les incidents

EXEMPLE : antivirus, IDS, SOC

Réaction

Processus, méthodes et outils permettant de faire face à une crise et de remettre l'activité en état

EXEMPLE : CERT, cellule de crise, site de secours, antivirus

COMMENT PRÉVENIR ET DÉTECTER LES INCIDENTS?

SOC : Security Operations Center

- Dispositif de sécurité regroupant technologies, processus et experts visant à superviser la sécurité d'un périmètre sensible

Collecter → Analyser → Qualifier → Alerter → Traiter

LE RECOURS À L'INTELLIGENCE ARTIFICIELLE

Détection à base de règles

Reconnaitre un modèle (pattern matching) dans un jeu de données

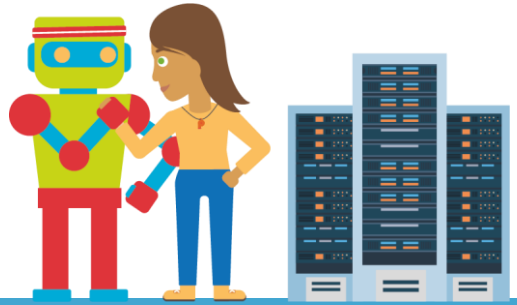
Analyse mathématique

Faire appel aux statistiques, probabilités, variations et régression pour corréler

Machine learning et algorithmes dédiés

Apprendre des évènements passés pour anticiper le futur

Régression logique, machine à vecteurs de support, forêts aléatoires, arbres décisionnels



« J'ai détecté le virus XYZ »

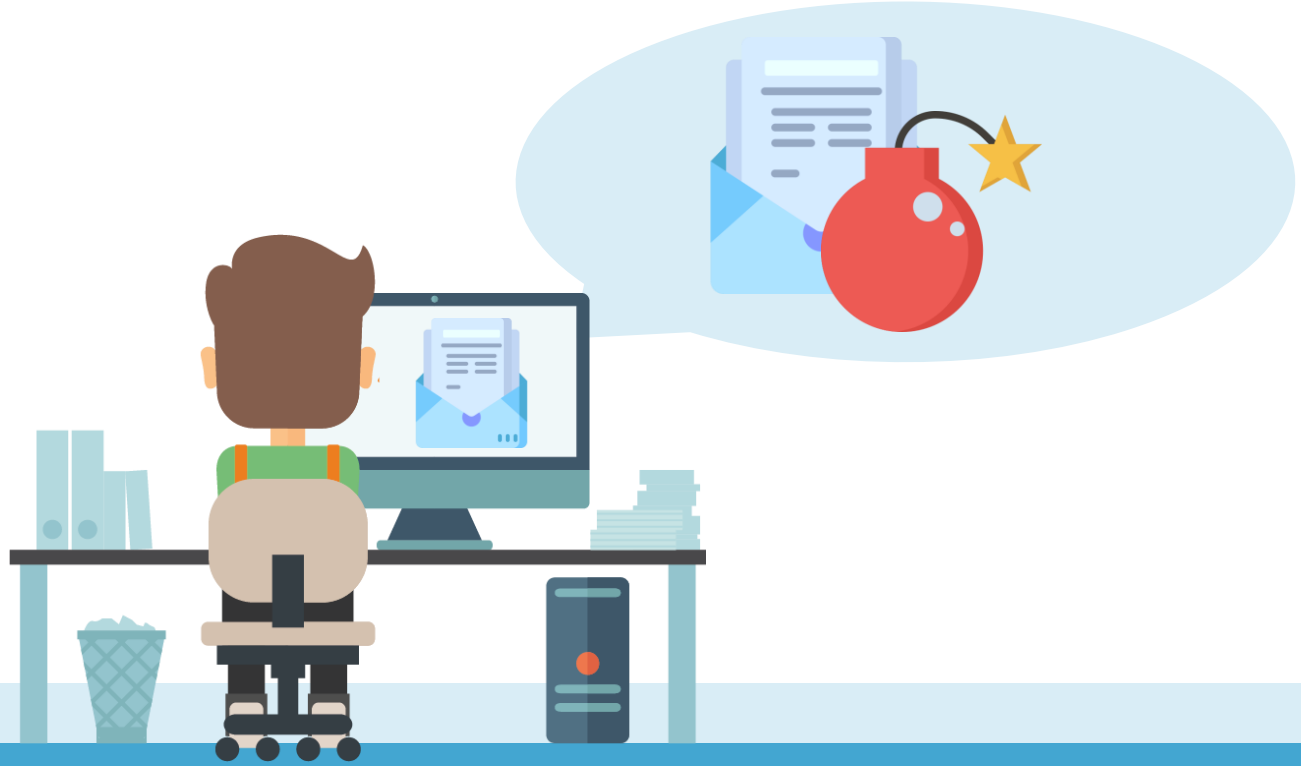
« L'accès en lecture à ces fichiers est plus important que d'habitude, est-ce grave ? »

« Si un utilisateur réalise 1000 virements de 50 € entre 3h et 4h du matin, il commet une fraude »

« Le comportement de ce poste montre une connexion vers le C&C d'un malware. »

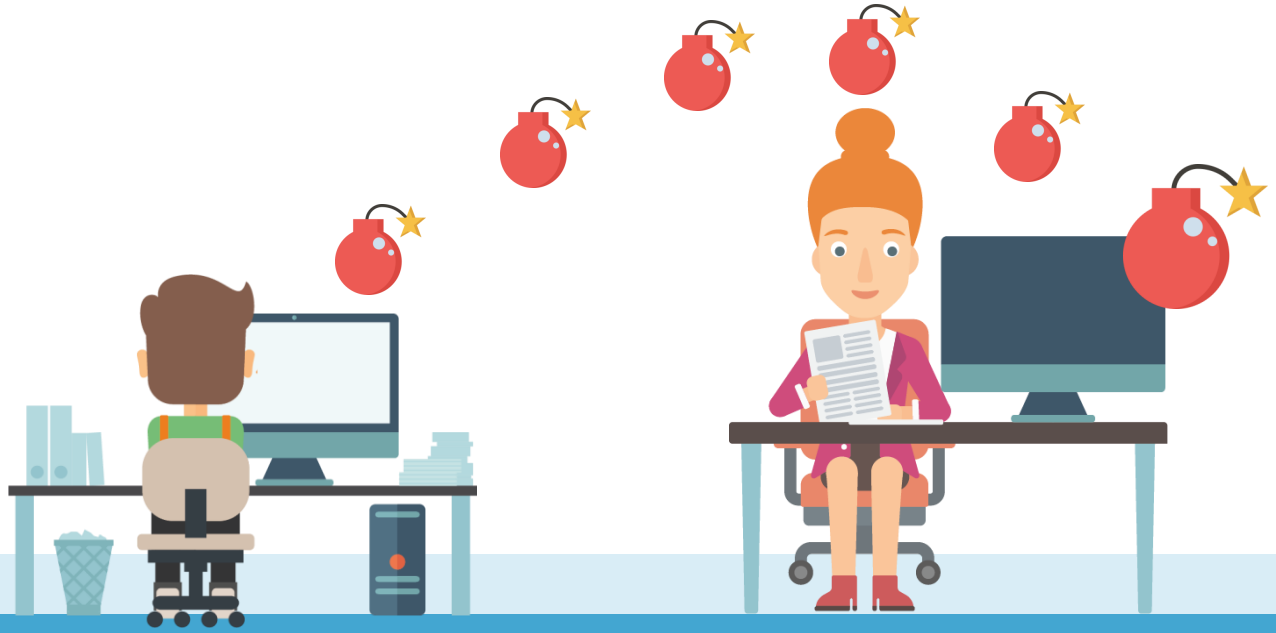
CAS D'USAGE : DÉTECTION DGA

Un mail ciblé, une pièce jointe malicieuse et un malware …



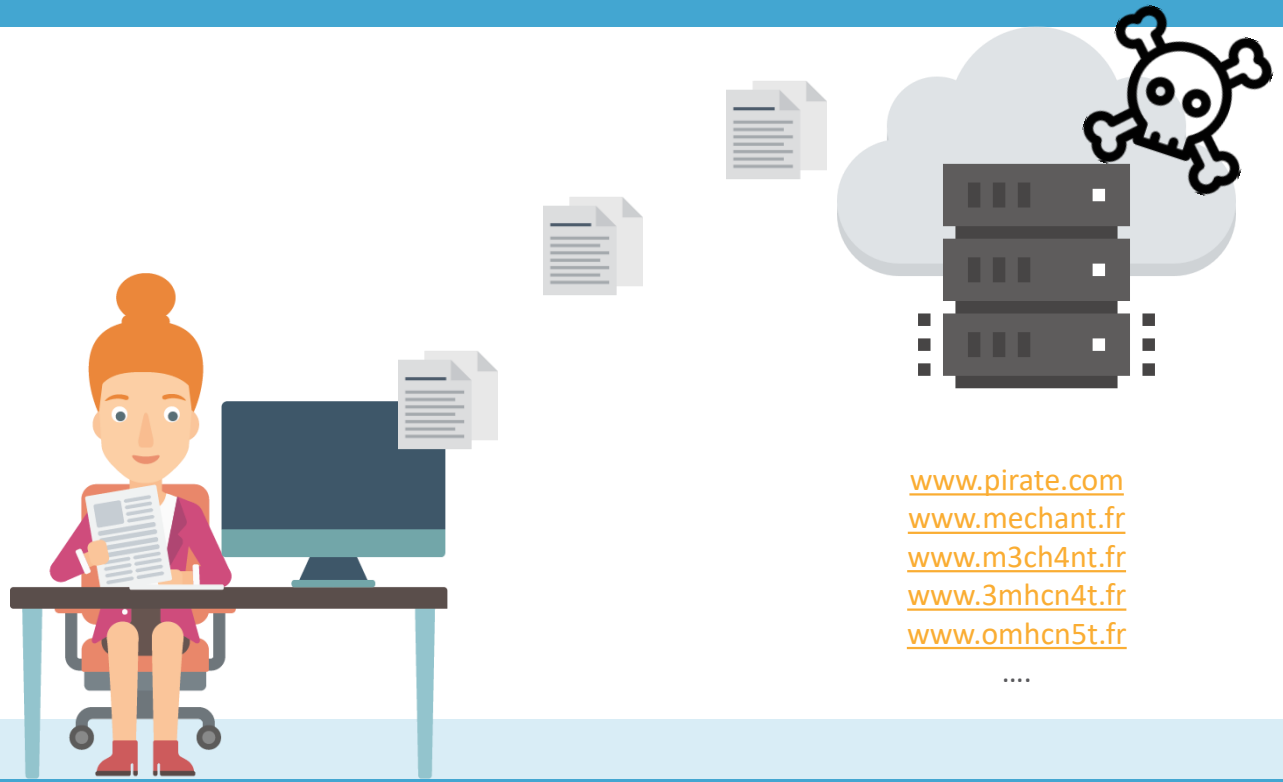
CAS D'USAGE : DÉTECTION DGA

Le malware se propage vers des postes VIP en vue de voler des données sensibles.



CAS D'USAGE : DÉTECTION DGA

Le malware tente d'exfiltrer des données sensibles vers un C&C.

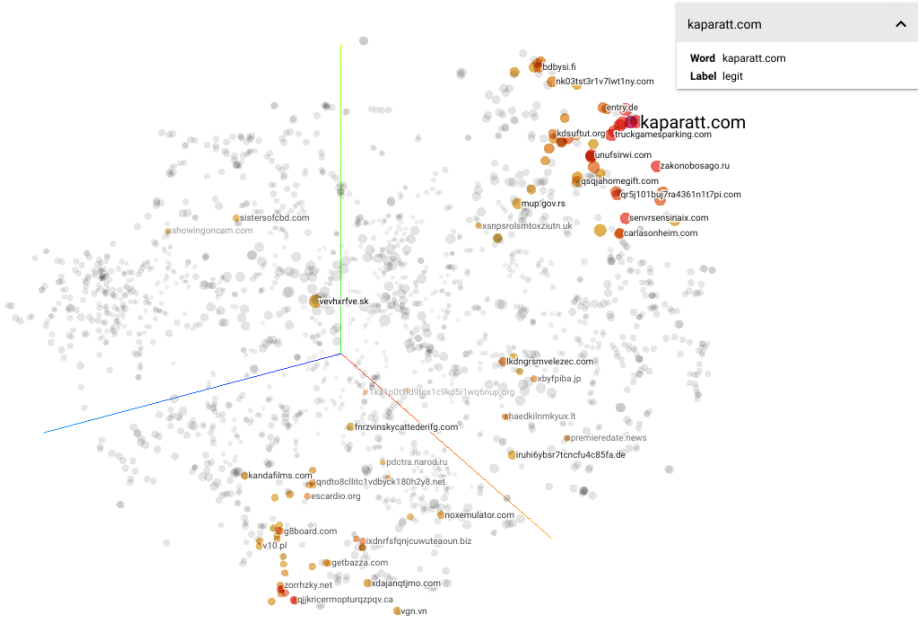


www.pirate.com
www.mechant.fr
www.m3ch4nt.fr
www.3mhcn4t.fr
www.omhcn5t.fr
....

CAS D'USAGE : DÉTECTION DGA

Les DGA (Domain Generation Algorithms) sont des algorithmes qui créent ou mettent à jour régulièrement un grand nombre de noms de domaines. Ils sont souvent utilisés par des malwares ou des botnets pour faire le lien avec leur centre de contrôle (Command & control servers).

- Détecter un DGA permet de détecter une infection de votre système par un malware ou l'utilisation de vos ressources dans un botnet.
- La détection d'un DGA par une règle ne fonctionne par car on ne connait pas les noms de domaine qui seront utilisés par l'attaquant. Il faut une approche plus… intelligente !
- Les blacklists sont utiles, mais par définition elles ne sont jamais à jour. Il faut une approche plus… intelligente ?
- **mySOC utilise le deep learning, en particulier un réseau de neurones récurrent, pour détecter les DGA.** L'algorithme « reconnaît » automatiquement et en temps réel tout nom de domaine qui n'est pas un nom légitime, avec une précision > 97%.



advens

SECURITY FOR THE DIGITAL AGE

advens.fr

Paris +33 1 84 16 30 25
Lille +33 3 20 68 41 81
Lyon +33 4 28 29 08 29
Bordeaux +33 5 35 54 82 84