Les défis de l'écosystème cyber

Former, innover et fédérer

CAMPUS CYBER

CAMPUS CYBER

YANN

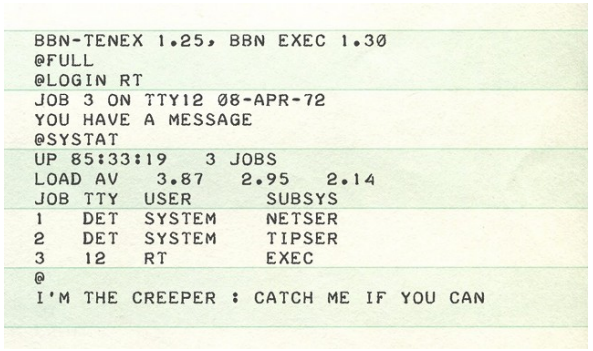
DIRECTEUR GENERAL DELEGUE

SOMMAIRE

- Historique de la cybersécurité
- Panorama des enjeux économiques et sociétaux
- Le défi de la formation
- Le défi de l’innovation
- Le défi de la fédération d’écosystème

Historique de la cybersécurité

De la fiction des risques cyber…



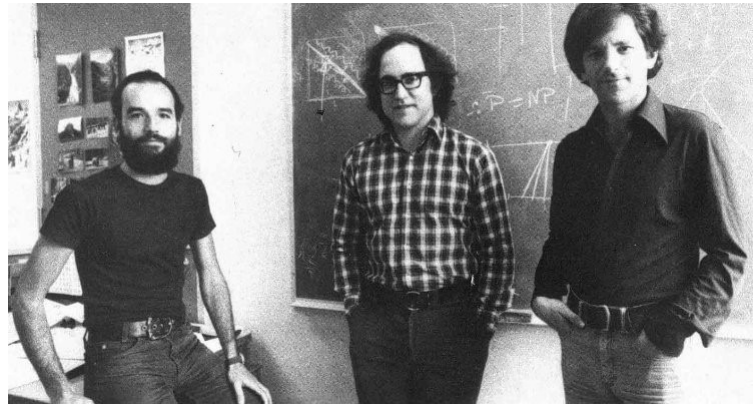
1971

Creeper & Reaper

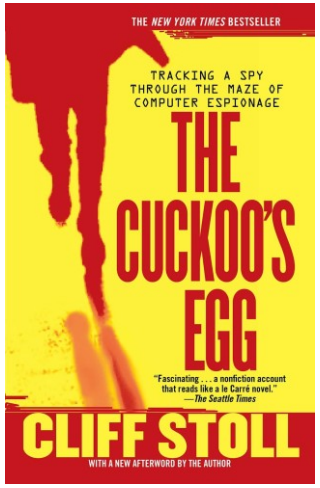
Creeper : premier programme autorépliquant
Reaper : premier anti-virus

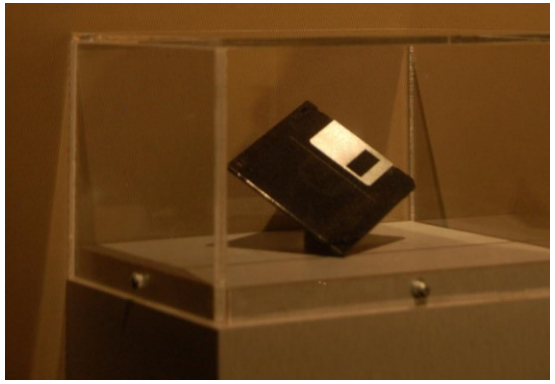
1983

War Game et RSA



War game : film américain mettant en scène des intrusions dans d'autres systèmes générant un risque de guerre nucléaire
RSA : algorithme utilisé pour sécuriser les données confidentielles





1986-1988

The Cuckoo's Egget et Morris Worm

The Cuckoo's Egget : film américain mettant en scène un hack d'ordinateur
Morris Worm : attaque informatique d'une université ralentissant des fonctions centrales

…à la réalité et leur médiatisation !

2007/2008

Estonie et **Géorgie**

Cyberattaques en Estonie à la suite d'un désaccord avec la Russie

2010

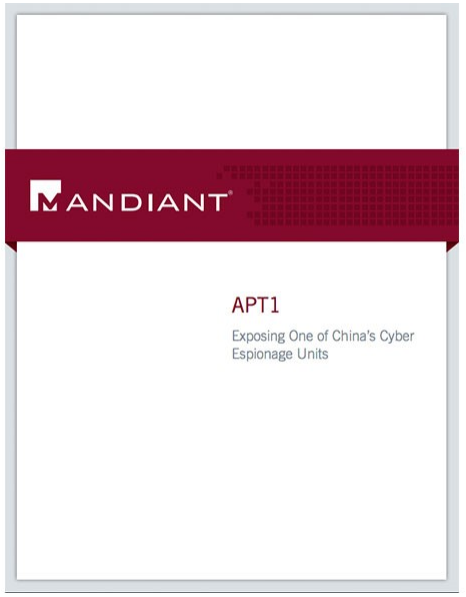
Stuxnet

Ver informatique créé par la NSA et Israël s'attaquant aux centrifugeuses iraniennes d'uranium (45 000 systèmes affectés)

2013

Mandiant « ATP1 report » et révélations Snowden

ATP1 : rapport sur l'espionnage chinois
Snowden : publication d'information top secrètes de la NSA dans les médias concernant des captations et surveillances illégales



Toujours au coeur des actualités

Brèves Energies

La compagnie italienne Eni, victime d'une cyberattaque

En Italie, le **contexte des élections législatives** anticipées semble avoir eu des répercussions sur le niveau de cybermenace dans le pays.

PIXELS

L'Ukraine et la Russie au bord de la cyberguerre

Entre sites attaqués et ordinateurs espionnés, le conflit entre la Russie et l'Ukraine se traduit aussi en ligne, avec la menace d'une cyberguerre.

Depuis le début du conflit, l'Ukraine a recensé **plus de 60 cyberattaques.**

C dans l'air

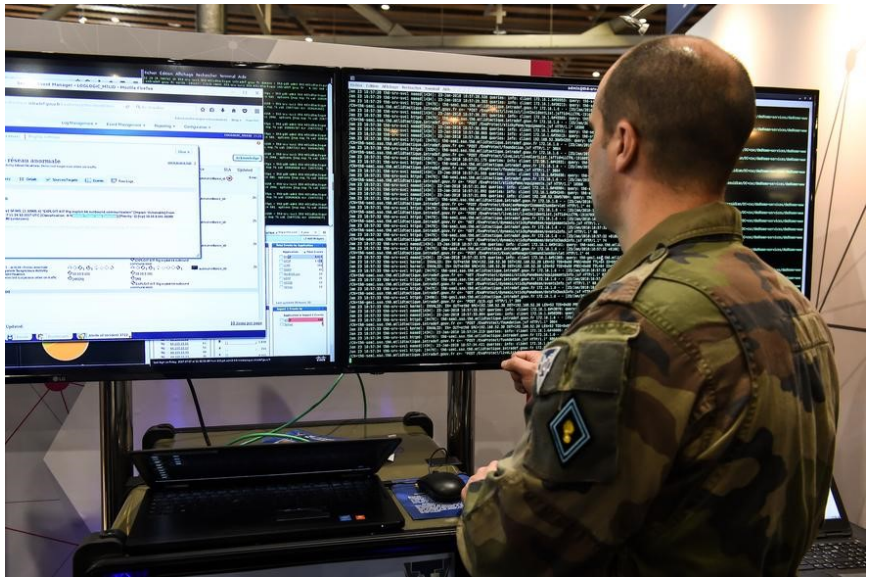
Cyber : la guerre est déclarée

•5 magazines • 130 min

tous publics

Le cyberespace est devenu le nouveau terrain d'affrontement mondial. C'est l'autre facette de la guerre
sans chars ni avions de chasse, où les virus informatiques ont remplacé les bombes et où les soldats s'ap
adversaires et semer le chaos à travers les réseaux. En 2020, les capacités des pirates du net ont augmen

Ne pas confondre cybersécurité et cyberdéfense



La **CYBERDÉFENSE** est l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

La **CYBERSÉCURITÉ** est un état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Enjeux économiques et sociétaux

Des enjeux économiques…

X4 des attaques

par rançonlogiciels entre 2019 et 2020

Des pertes financières…

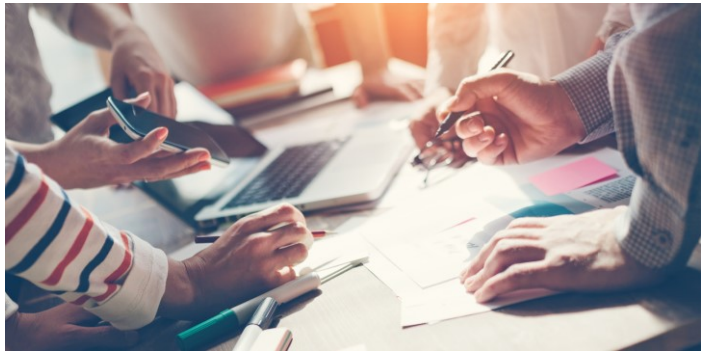
TOP 10

des risques business *(forum économique mondial)*

6 000 milliards

d'euros de pertes financières

DES ENTREPRISES AU CŒUR DES ATTAQUES



… qui touchent particulièrement les petites entreprises

80%

des cyberattaques touchent les PME

60%

de faillites dans les 6 mois

...aux enjeux sociétaux !

Les écoles et universités également touchées

- Il y a quelques jours, le Pôle universitaire Léonard de Vinci était victime d'une cyberattaque
- L'université de Neuchâtel, en Suisse, a été victime d'un rançongiciel en février 2022
- L'ENT des lycées franciliens a été touché en mars par une cyberattaque.

.00%

de services publics dématérialisés en 2022.

DES SERVICES PUBLICS TOUCHES PAR LES ATTAQUES CAR INSUFFISAMMENT PROTEGES : LES DONNEES DES CITOYENS A RISQUE

1 attaque sur un hôpital chaque semaine

en France en 2022

.9%

des cibles, en 2021, sont des collectivités territoriales. C'est plus que les entreprises stratégiques ou les hôpitaux.

Paradoxalement, un secteur en forte pénurie de ressources humaines.

15 000

postes non pourvus en France

46%

de ces postes sont à pourvoir en Île-De-France.

UN CRUEL MANQUE DE TALENTS FEMININS

89%

des professionnels actuels sont des hommes

4%

Des filles choisissent le vœu de spécialité NSI en fin de seconde, contre presque 21% des garçons (en 2022).

métiers particulièrement en tension

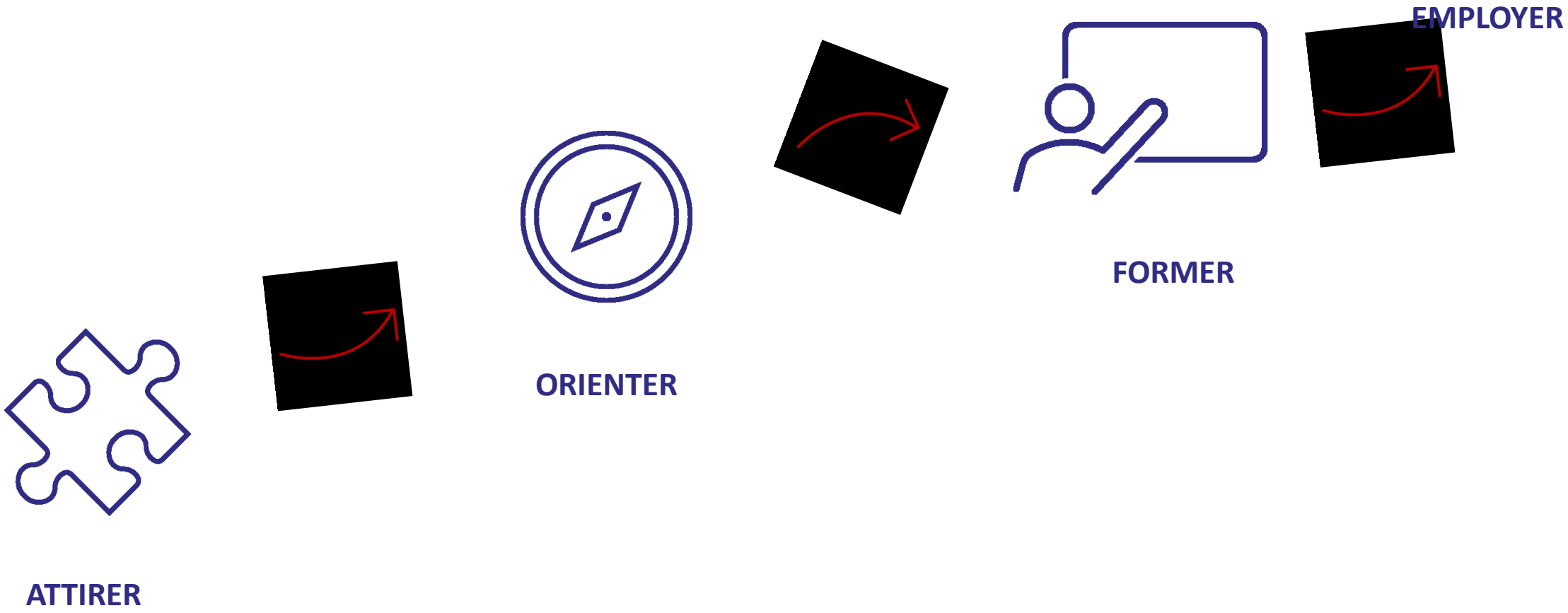
- Architecte cybersécurité
- Ingénieur analyste

89%

d'augmentation des effectifs cyber pour faire face aux besoins en défense des organismes publics et privés

Le défi de la formation des talents

Adresser la pénurie des talents en 3 étapes clefs.



Une image erronée…

… qui ne reflète pas la diversité des métiers !

GESTION DE LA SÉCURITÉ ET PILOTAGE DES PROJETS DE SÉCURITÉ

- *Directeur Cybersécurité*
- *Responsable de la Sécurité des Systèmes d'Information (RSSI)*
- *Déclinaison pour le Responsable de sécurité des SI au sein d'une PME / TPE*
- *Coordinateur sécurité*
- *Directeur de programme de sécurité*
- *Responsable de projet de sécurité*

CONCEPTION ET MAINTIEN D'UN SI SÉCURISÉ

- *Chef sécurité de projet*
- *Architecte sécurité*
- *Spécialiste sécurité d'un domaine technique*
- *Spécialiste en développement sécurisé*
- *Cryptologue*
- *Administrateur de solutions de sécurité*
- *Auditeur de sécurité organisationnelle*
- *Auditeur de sécurité technique*

MÉTIERS CONNEXES

- *Métiers contribuant à la démarche de cybersécurité*
- *Métiers pouvant se spécialiser en cybersécurité*

GESTION DES INCIDENTS ET DES CRISES DE SÉCURITÉ

- *Responsable du SOC*
- *Opérateur analyste SOC*
- *Responsable du CSIRT*
- *Analyste réponse aux incidents de sécurité*
- *Gestionnaire de crise de cybersécurité*
- *Analyste de la menace cybersécurité*

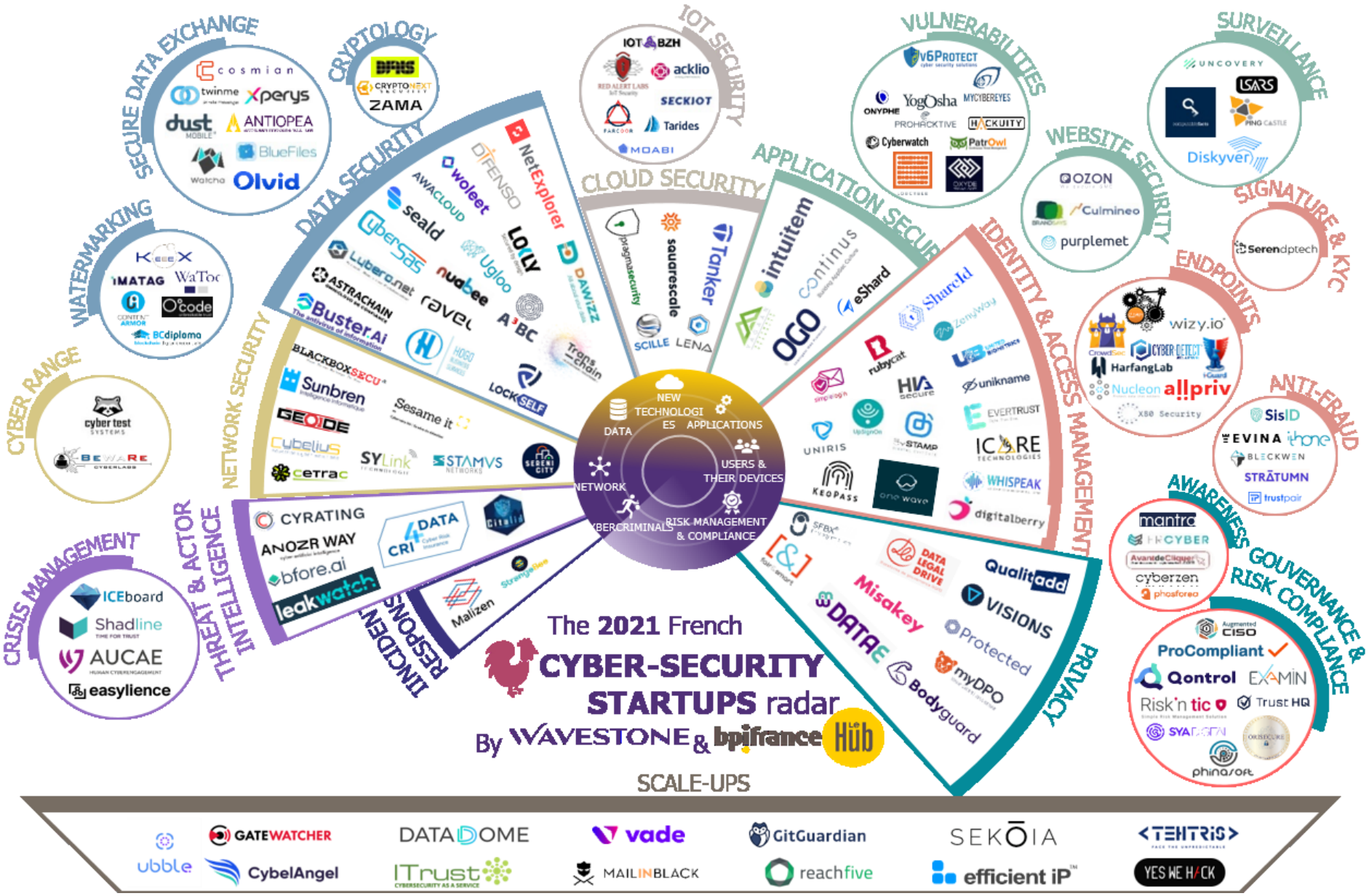
CONSEIL, SERVICES ET RECHERCHE

- *Consultant en cybersécurité*
- *Formateur en cybersécurité*
- *Évaluateur de la sécurité des technologies de l'information*
- *Développeur de solutions de sécurité*
- *Intégrateur de solutions de sécurité*
- *Chercheur en sécurité des systèmes d'information*

Des métiers avec beaucoup de sens : les cyberpompiers.

Le défi de l’innovation

Plus de 160 startups en cybersécurité



Continuer de développer des solutions françaises souveraines !

+de 75%

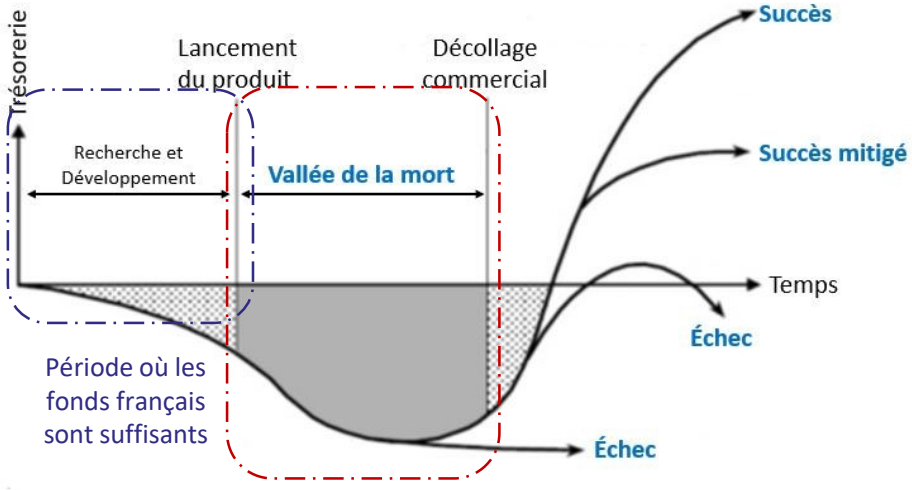
des investissements en cybersécurité
sont destination des Etats-Unis

2 OBJECTIFS

Faciliter l'émergence de projets

Trouver des financements

UN FORT RISQUE DE RACHAT ETRANGER



Période où les fonds français sont suffisants

Période de rachat par une entreprise étrangère

2 PROGRAMMES

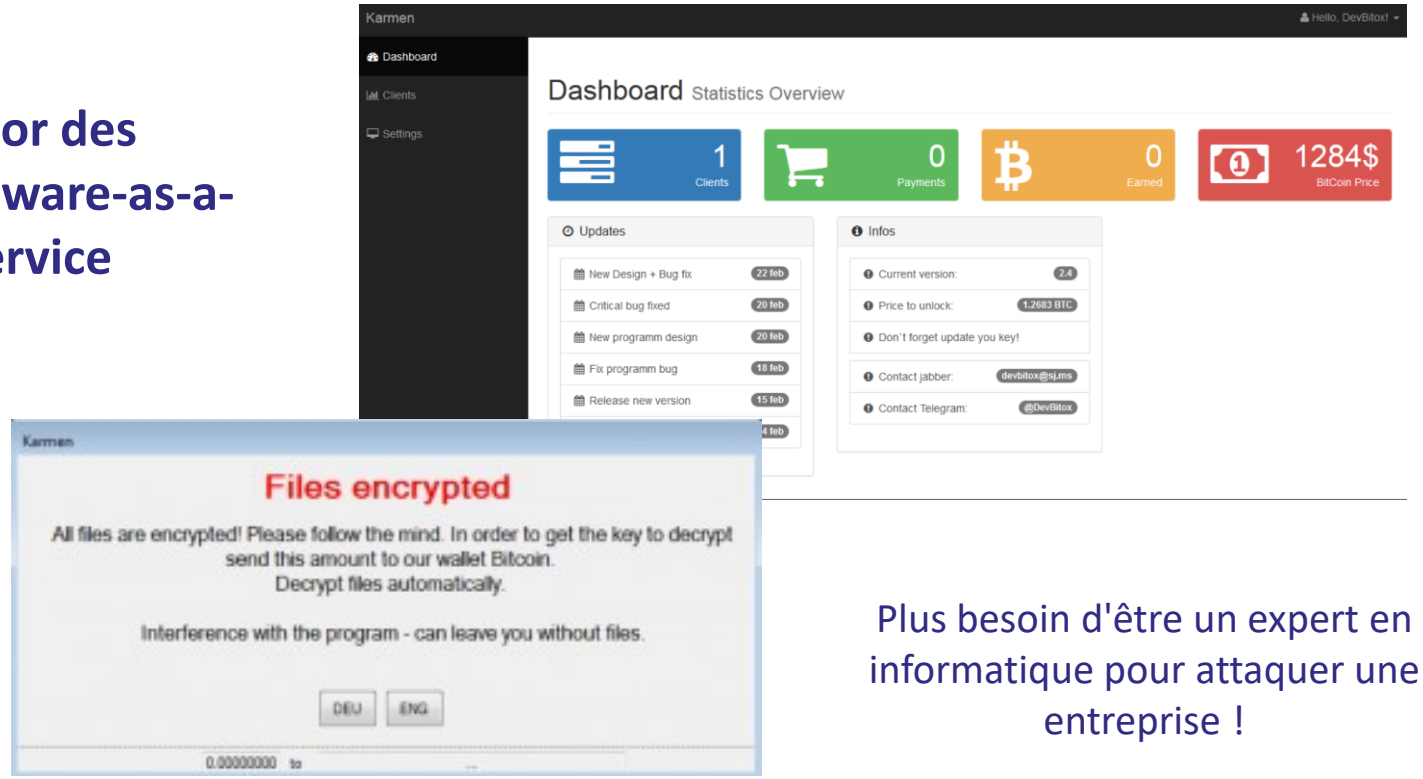
Programme de transfert recherche / industriels

Programme de pré-incubation et incubation / accélération

Le défi de la fédération de l’écosystème

Côté cyberattaquants, une industrialisation de la menace.

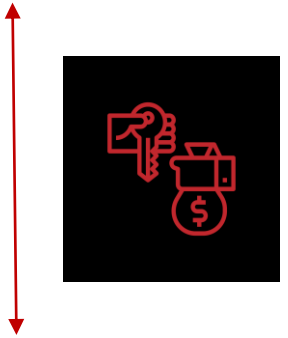
Essor des ransomware-as-a-service



Plus besoin d'être un expert en informatique pour attaquer une entreprise !

De 40 à quelques milliers de dollars

Prix d'un kit

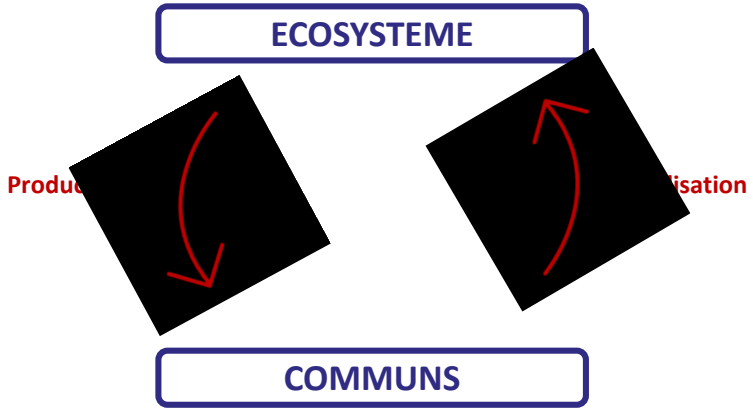


6 millions de dollars

Rançon moyenne en 2021

Fédérer pour mutualiser les forces : mieux faire face à la menace.

Objectif :
générer des effets levier
- Renforcer la notoriété et l'expertise des acteurs français sur la scène internationale
- Mieux répondre à la menace



Challenge :
changement d'état d'esprit et de mode de travail pour dépasser les concurrences économiques

RETOMBEES POUR L'ECOSYSTEME

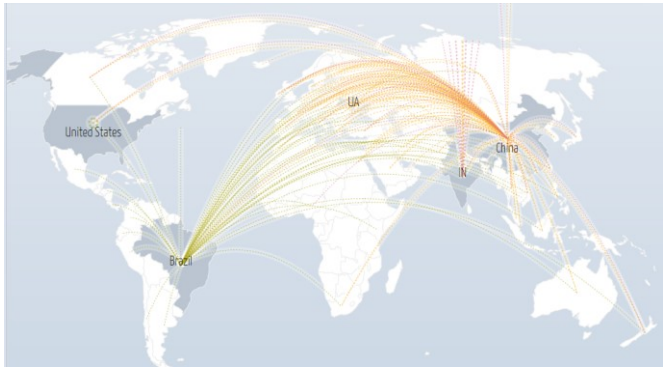
Réduction des coûts de développement et R&D

Interopérabilité des solutions

Développement de standards internationaux

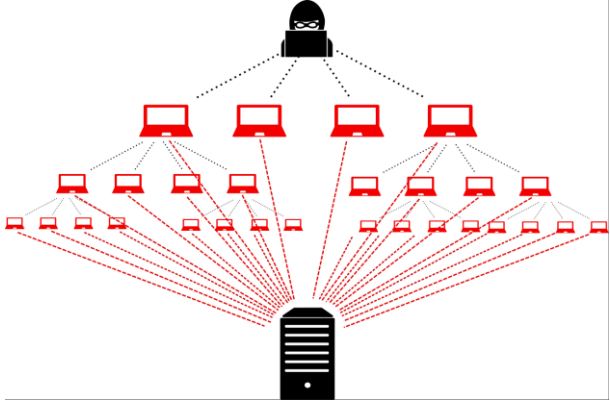
Quelques exemples :
- Travail de la communauté bancaire
- Développement d'une base de renseignement sur l'état de la menace cyber
- Mise en œuvre d'une plateforme d'échange de données utilisant l'IA

Quelques notions de vocabulaire…

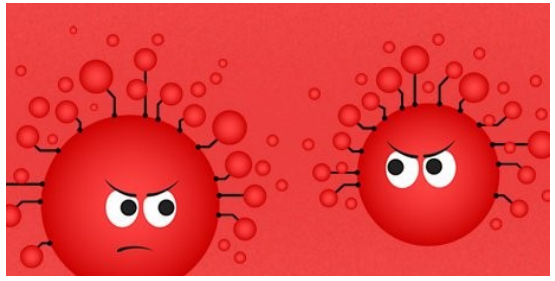


Un **BOTNET** est un réseau de machines compromises à la disposition d'un individu malveillant. Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise.

Une **BACKDOOR** est un accès dissimulé qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive.



Un **DDoS** (distributed denial of service) empêche ou limite fortement la capacité d'un système à fournir le service attendu. Ce type d'attaques est souvent réalisé à l'aide de botnets.



Un **MALWARE**, ou code/ logiciel malveillant caractérise tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau.

Un **RANSOMWARE**, est un programme malveillant dont le but est d'obtenir le paiement d'une rançon, la plupart du temps en chiffrant les données de victime.

Un **APT** (Advanced Persistent Threat) désigne principalement des acteurs étatiques ou sponsorisés par des Etats capables de conduire des cyberattaques sophistiquées, notamment pénétrer dans des systèmes d'information et y rester durablement sans être détectés.