SYNACKTIV
DIGITAL SECURITY

Journée portes ouvertes chez Synacktiv

Démonstration de quelques outils d'intrusion

Présenté 24 / 01 / 2017

Pour le FIC 2017

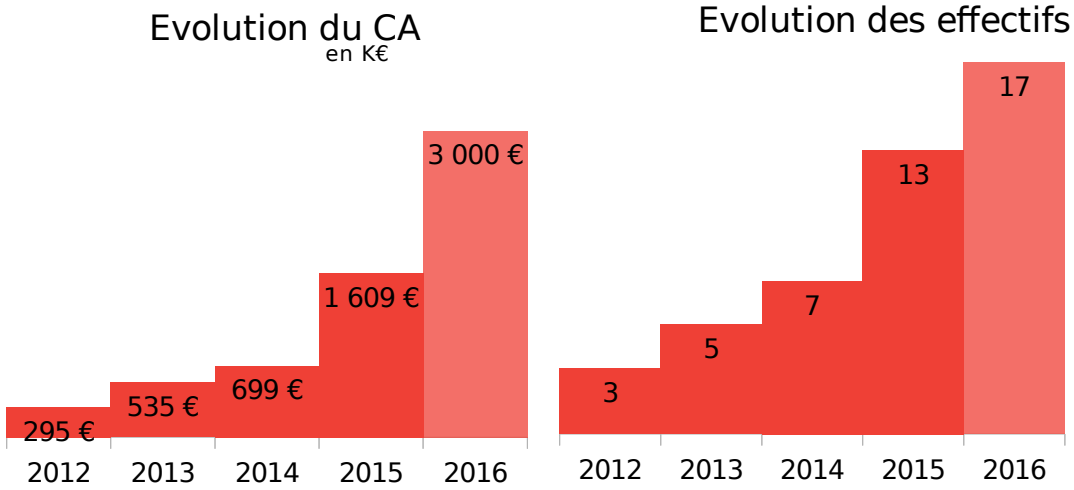
Par Renaud Feil et Nicolas Collignon

Innovation | Expertise

Pertinence | Sécurité

Transparence | Passion

- **Avril 2012 : création de Synacktiv**
- **Expertise en sécurité des systèmes d'information**
  - Tests d'intrusion et audits de sécurité
  - Recherche de vulnérabilités
  - Développements d'outils de sécurité
- **Intervention en France et dans le monde entier**



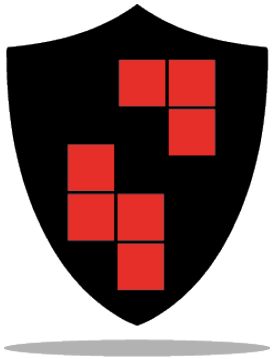
Ambition : Être la référence française en sécurité offensive

Disconet

Plateforme collaborative pour la réalisation de tests d'intrusion

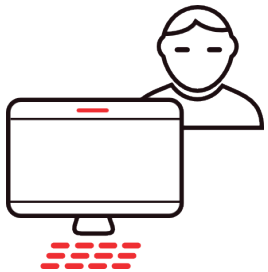
Les objectifs de Disconet

- **Plateforme pour faciliter la réalisation des audits et tests d'intrusion**
  - Automatiser les tâches simples pour se concentrer sur les attaques complexes
  - Simplifier les interactions entre les différents outils
  - Déroulement de séquences d'intrusion pré-définies
  - Faciliter la collaboration entre plusieurs experts sécurité

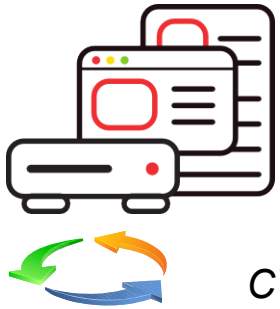


Auditer avec Disconet

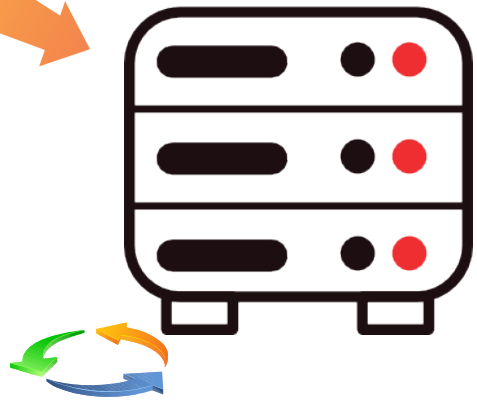
Experts sécurité
Pilotage de l'automate
Étapes d'audit/intrusion avec/sans Disconet
Rédaction collaborative de rapports

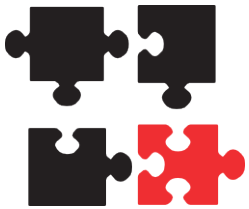


Disconet
Orchestration



Base de connaissance
300 vulnérabilités fr/en
CVSS, ISO-27001, PCI-DSS, etc



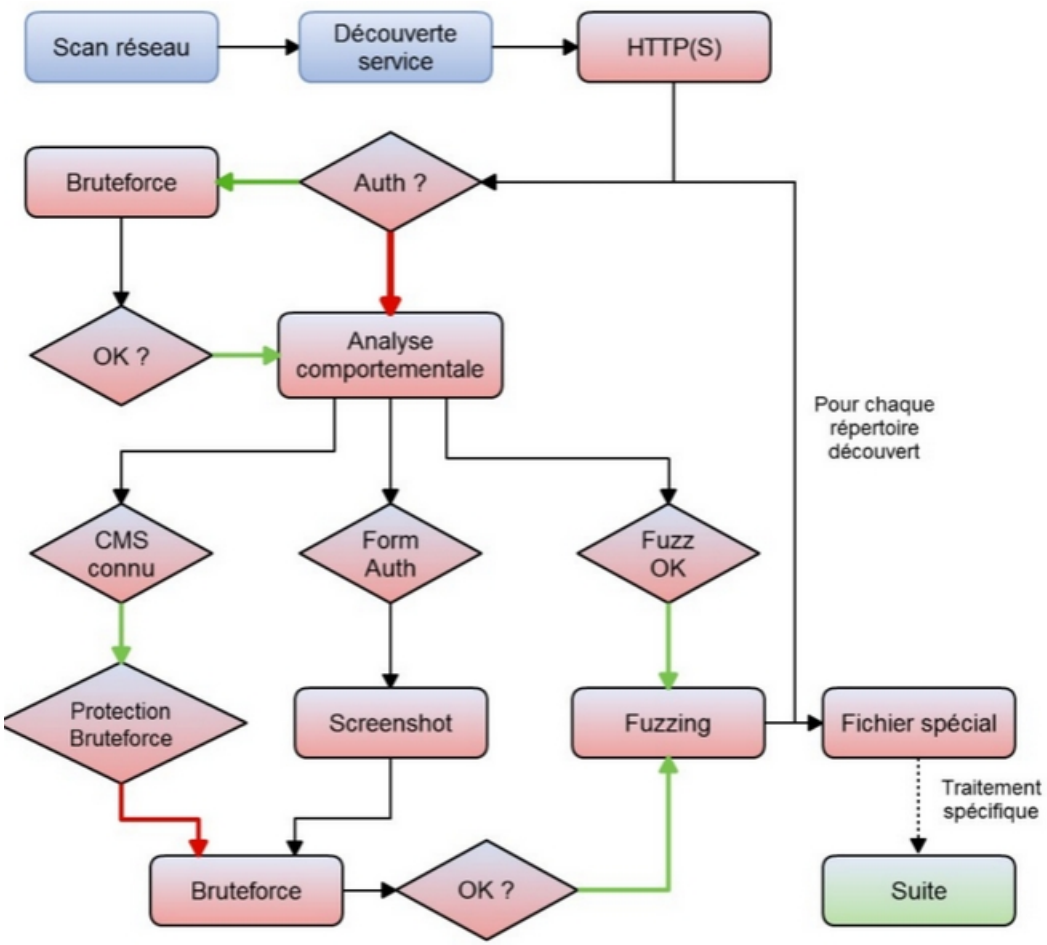


Outils d'intrusion
80 plugins intégrés
Support nmap, Nessus, BurpSuite, etc.

Reporting
Tableaux de bord, rapports Office
Export vers des services tiers

Le cœur Disconet

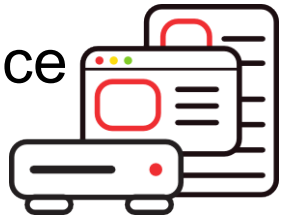
- **Orchestration du test d'intrusion**
  - Agrège, classifie et interprète les informations
  - Génère des tâches en suivant des schémas d'intrusion pré-configurés
  - Adapte l'intrusion en fonction des actions des consultants



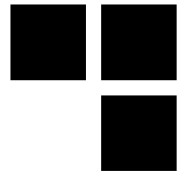
VKB: *Vulnerability Knowledge Base*

- **Modèles de vulnérabilités**
  - 300 vulnérabilités rédigées en français et anglais
  - Structure claire : Titre, Observation, Risque, Recommandations, Références
  - Pré-classification des vulnérabilités
  - Indicateurs *CVSS*, *CWE*, *ISO-27001*, *ARJEL*, *PCI-DSS*

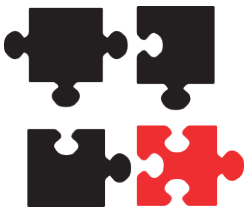
- **Maintien et amélioration dans le temps**
  - Workflow d'approbation de nouvelles vulnérabilités
  - Mécanisme de synchronisation de bases de connaissance inter-serveurs



Plugins d'intrusion sur Disconet



- **30 plugins développés en interne**
  - Analyses comportementales des services
  - Recherche sur des services tiers : *Bing*, *Google*, *Shodan*, etc.
- **50 outils d'intrusion supportés**
  - Scanners de vulnérabilités : *Nessus*
  - Scanners réseau : *masscan*, *nmap*
  - Outils d'audit : *dig*, *ikescan*, *snmpwalk*, *whatweb*
  - Outils d'attaques : *BurpSuite*, *fierce*, *medusa*, *mimikatz*, *responder*, *patator*, *wfuzz*
- **Traitement des entrées/sorties unifié**
  - Tâches exécutées par Disconet
  - Tâches exécutées manuellement sur un poste d'auditeur

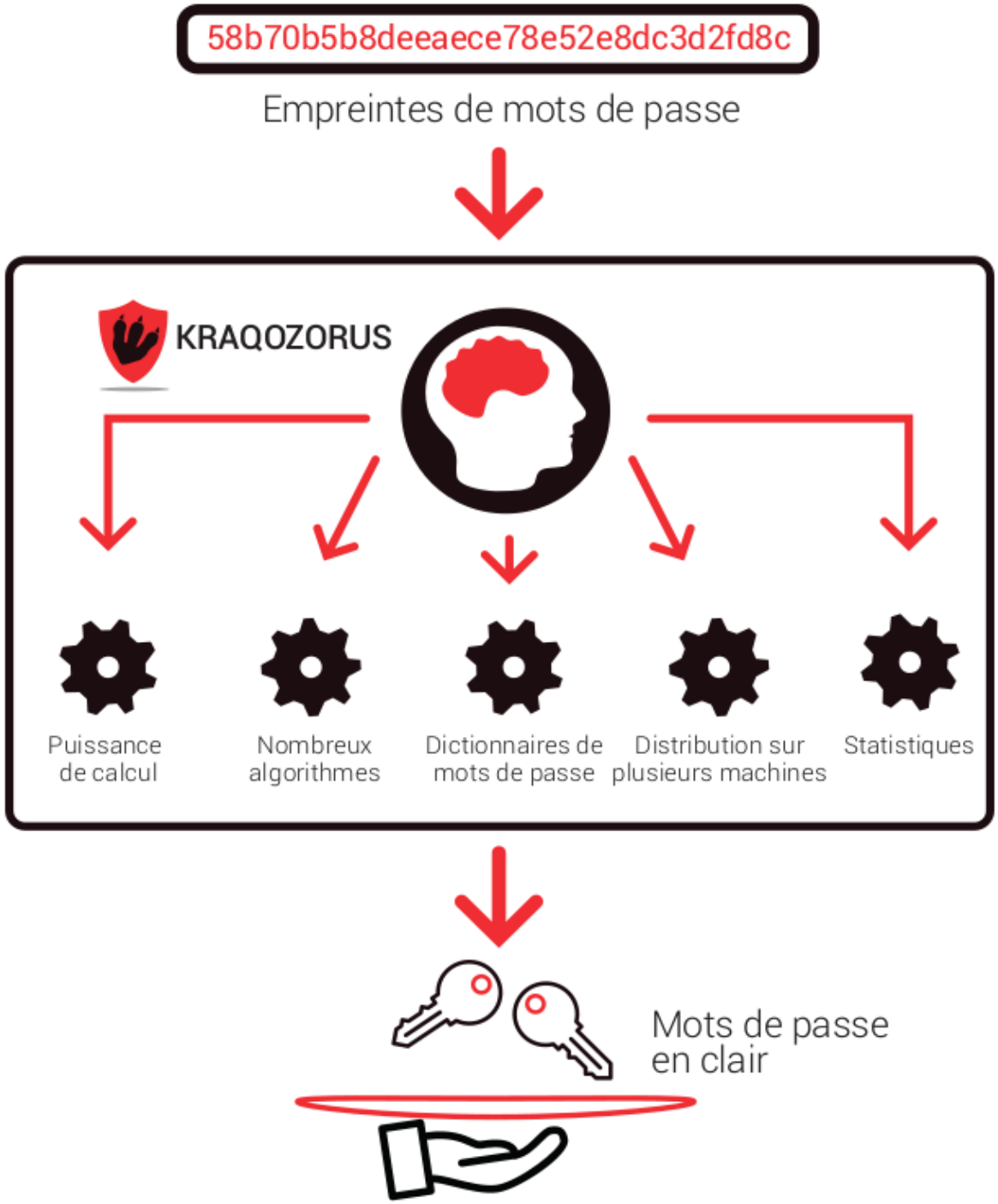


Rapports de vulnérabilités

- **Visualisation sur un *dashboard***
  - Classification et agrégation des vulnérabilités
  - Fonctionnalité de suivi des corrections
- **Rédaction collaborative de rapports**
  - Rapports structurés basés sur des modèles prédéfinis
  - Fonctionnalité de bloc-note collaboratif en temps réel
- **Support multi-formats**
  - Rapports et tableurs classiques : *OpenOffice*, *MS Office*
  - Services tiers : *Redmine*

Kraqozorus

Plateforme de cassage d'empreintes de mots de passe

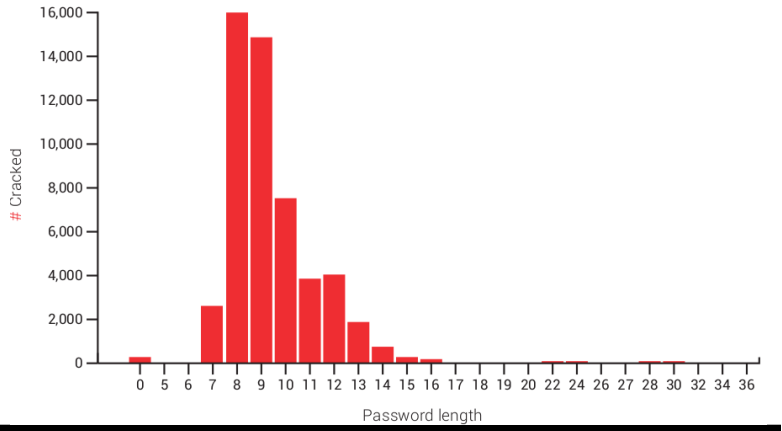

58b70b5b8deeaece78e52e8dc3d2fd8c
Empreintes de mots de passe
KRAQOZORUS
Puissance de calcul
Nombreux algorithmes
Dictionnaires de mots de passe
Distribution sur plusieurs machines
Statistiques
Mots de passe en clair

Kraqozorus : fonctionnalités

- **Puissance de calcul**
  - Jusqu'à 8 cartes graphiques par machine
  - 99% des empreintes de mots de passe cassées sur des fuites publiques
  - Plus de 300 milliards de mots de passe testés par seconde (algorithme Windows)

- **Personnalisation des campagnes de cassage**
  - Création de stratégies
  - Sélection de dictionnaires
  - Configuration de la politique de mots de passe
  - Choix de la priorité des tâches

- ***Dashboard***
  - Statistiques sur les mots de passe trouvés



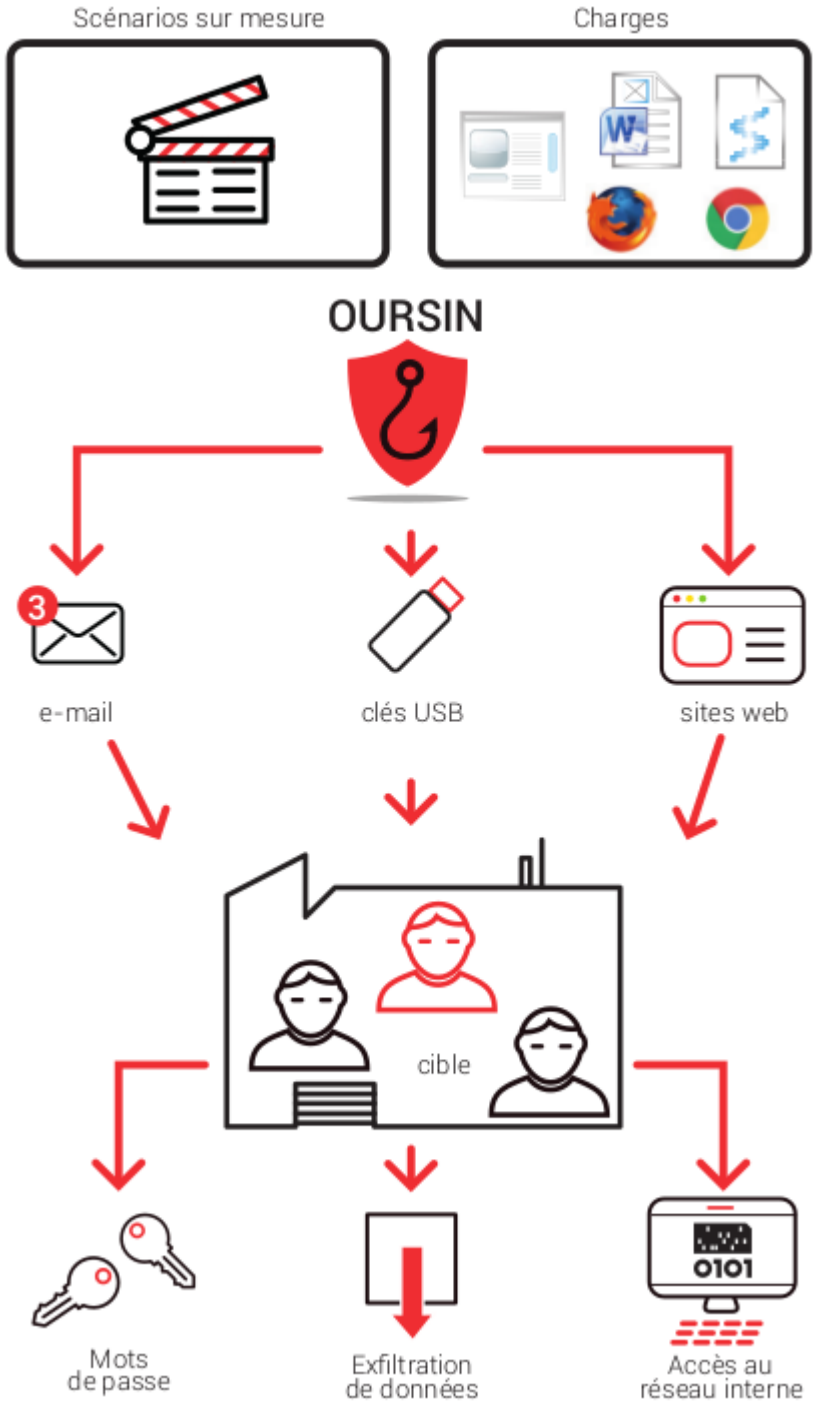
Kraqozorus : fonctionnalités

- **Supports des types d'empreintes**
  - Plus de 60 formats d'empreintes testés
  - Supporte tous les formats *John* et *Hashcat*
  - Possibilité d'ajouter des nouveaux formats

- **Nombreux dictionnaires**
  - 100+ Go de dictionnaires
  - Intégration des dictionnaires provenant de fuites publiques
  - Recyclage automatique des mots de passe cassés pour trouver des dérivations

Oursin

Plateforme d'attaques côté client

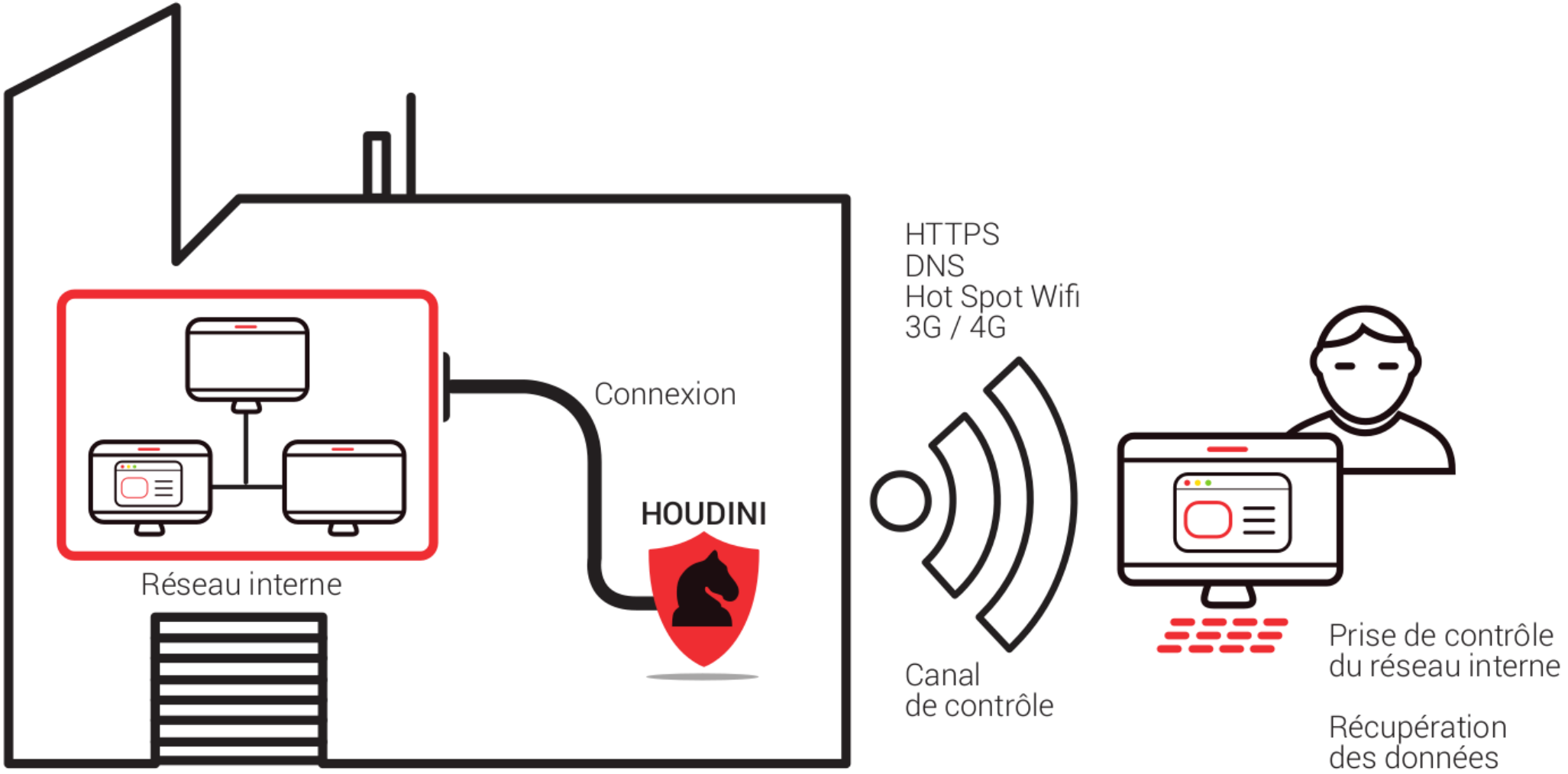

Scénarios sur mesure
Charges
OURSIN
3
e-mail
clés USB
sites web
cible
0101
Mots
de passe
Exfiltration
de données
Accès au
réseau interne

Oursin : fonctionnalités

- **Campagne d'attaques variées**
  - Modèles de *phishing* personnalisables
  - Macros Office permettant d'exécuter du code sur la cible
  - Injection d'exploits et pivot post-intrusion
  - Multi-cibles : *Android*, *iOS*, *Linux*, *Windows*
- **Fonctionnalités des portes dérobées**
  - Évasion des anti-virus
  - Analyse, communique et contourne la politique de sécurité locale

Houdini

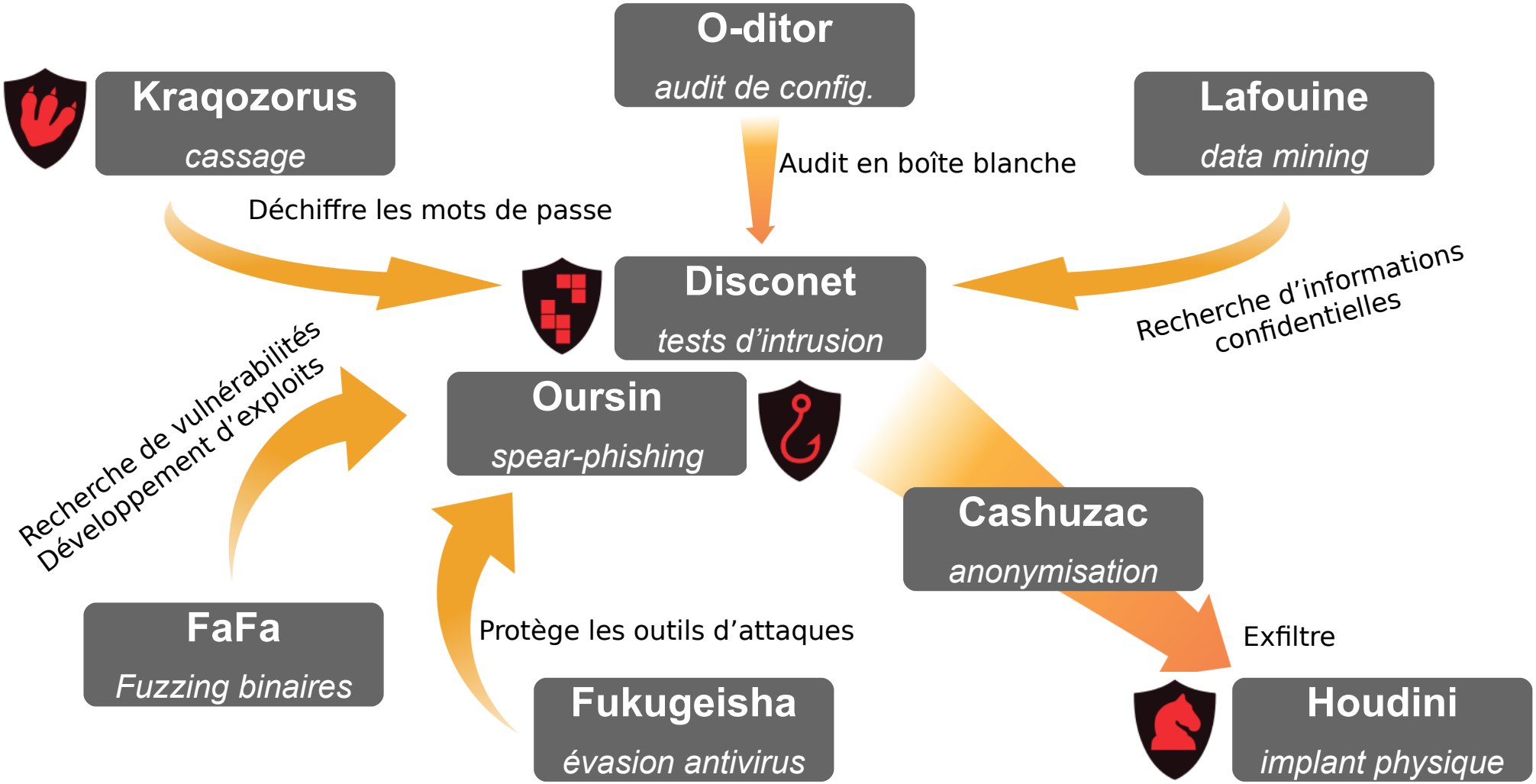
Implant pour intrusion physique


Connexion
HOUDINI
Réseau interne
HTTPS
DNS
Hot Spot Wifi
3G / 4G
Canal
de contrôle
Prise de contrôle
du réseau interne
Récupération
des données

Houdini : fonctionnalités

- **Auto-configuration réseau**
  - Exfiltration vers Internet : *HTTPS*, *HTTP*, *DNS*, *3G/4G*, *SMS*
  - Support mode bridge pour contournement *802.1x*
- **Distribution Debian personnalisée**
  - Pré-installation de 60 outils d'intrusion
  - Plate-forme d'intrusion ou relais d'attaques
- **Fonctionnalités de sécurité**
  - Anonymisation du processus de compilation
  - Déchiffrement *white-box* de la partition racine
  - Brouillage de la configuration
  - Déchiffrement manuel de la partition de données
  - Support ordre de suppression des données

Synergie des outils Synacktiv



AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY