ALEPH SEARCH DARK

Fuite de données par rançongiciel, l'étendu des dégâts par rebond et conformité NIS2

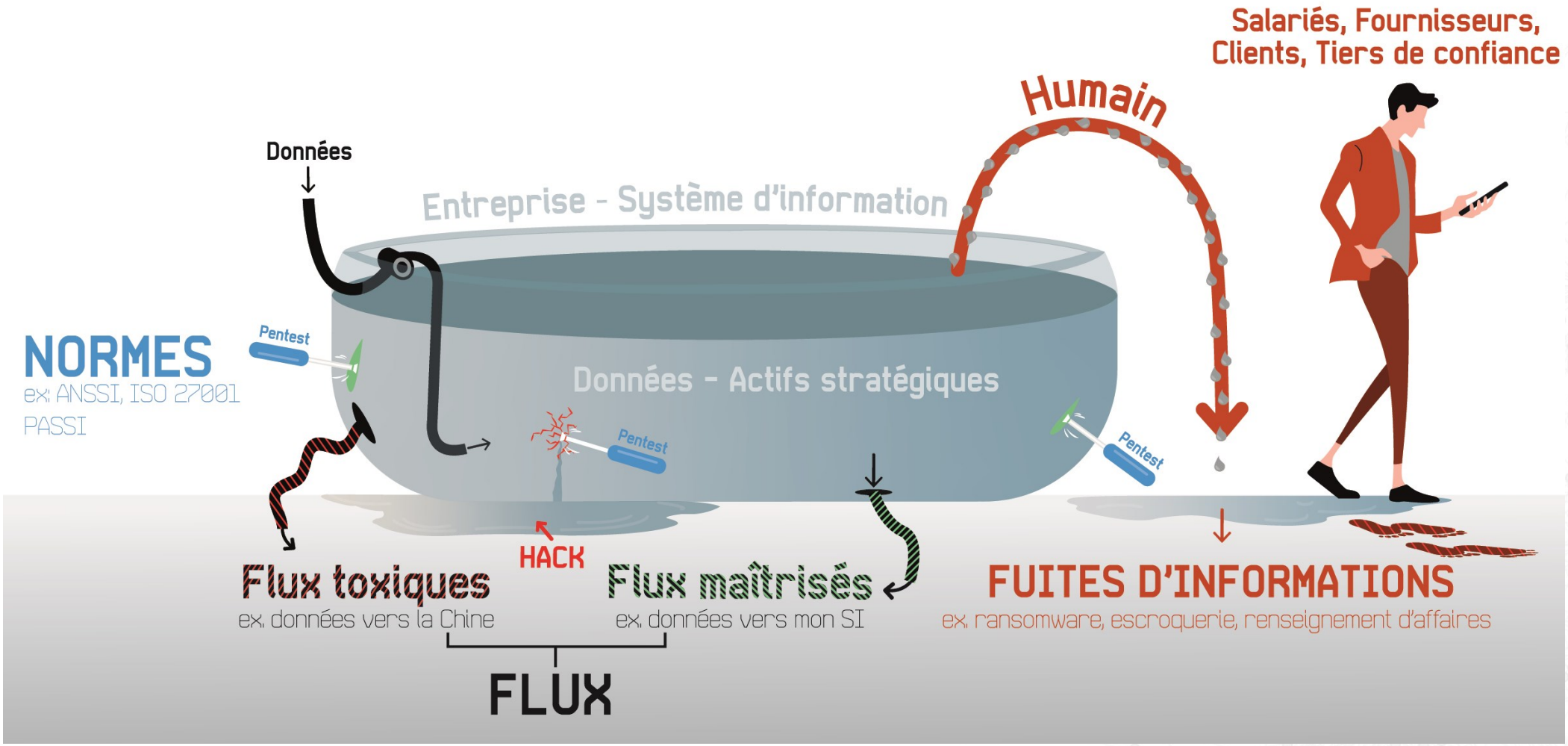
JUIN 2023

ALEPH

Présentation pour

OSSIR

L'HUMAIN, AU CŒUR DE VOTRE SYSTÈME D'INFORMATION

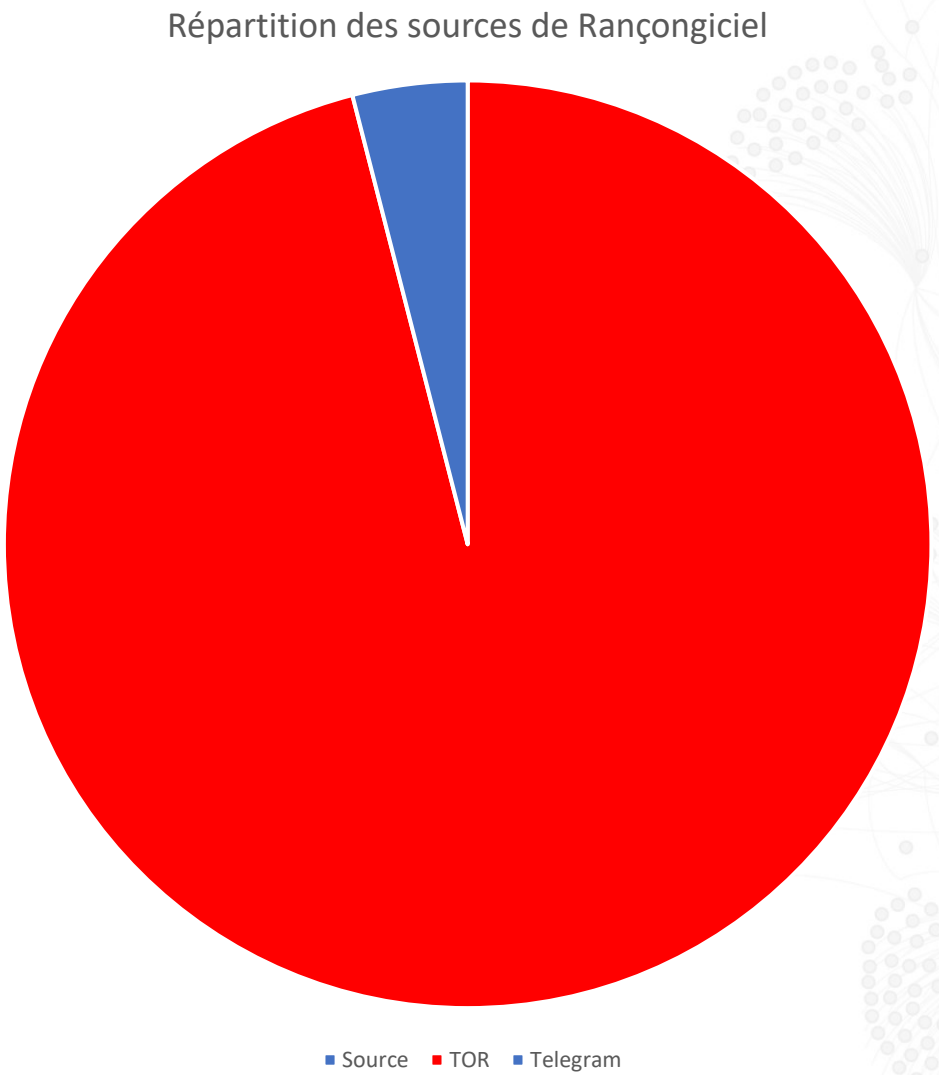


De la norme à la pratique : l'humain, exclu jusqu'à présent du SI , est devenu en réalité le principal risque du SI.

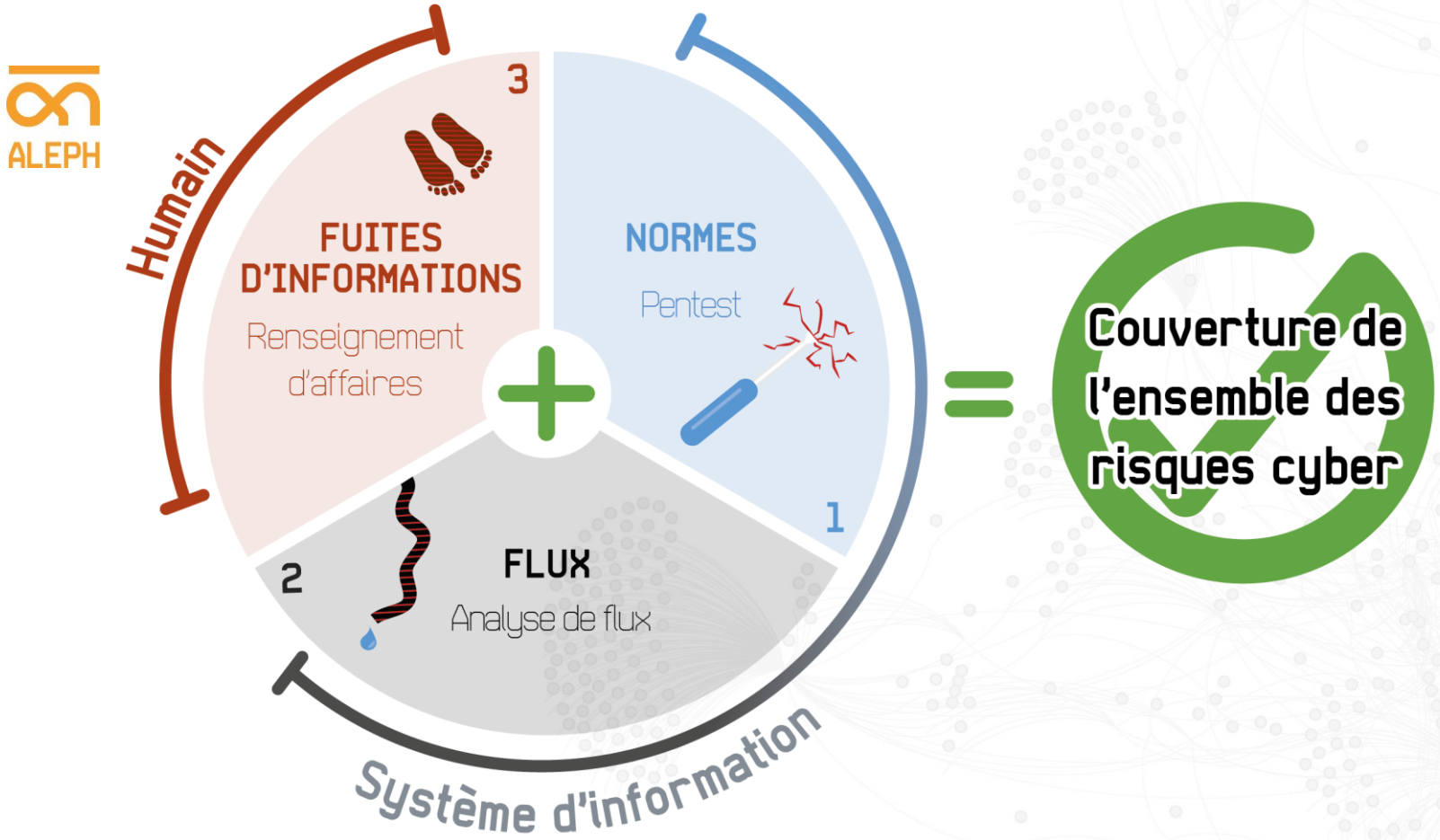
Pour cette raison, **Aleph prend en compte l'humain dans votre protection du SI**, pour une garantie complète du continuum de sécurité.

ALEPH

REPARTITION DES SOURCES DE RANCONGICIEL



UN PÉRIMÈTRE CYBER 360° : LA GARANTIE DE VOTRE CONFORMITÉ



Aleph propose une offre de **protection cyber complète**, vous permettant d'avoir la meilleure des couvertures et de **garantir votre conformité.**

Aleph met à votre disposition **la meilleure des technologies d'indexation du marché** pour surveiller votre environnement informationnel.

L'INDEXATION LA PLUS PUISSANTE DU MARCHÉ SUR LES CLEAR / DEEP / DARK WEBS

Clear Web

2 à 20% du Web (centralisé) – Contenus indexés par les moteurs de recherche
Sites publics, médias sociaux (données publiques et accessibles)

Deep Web

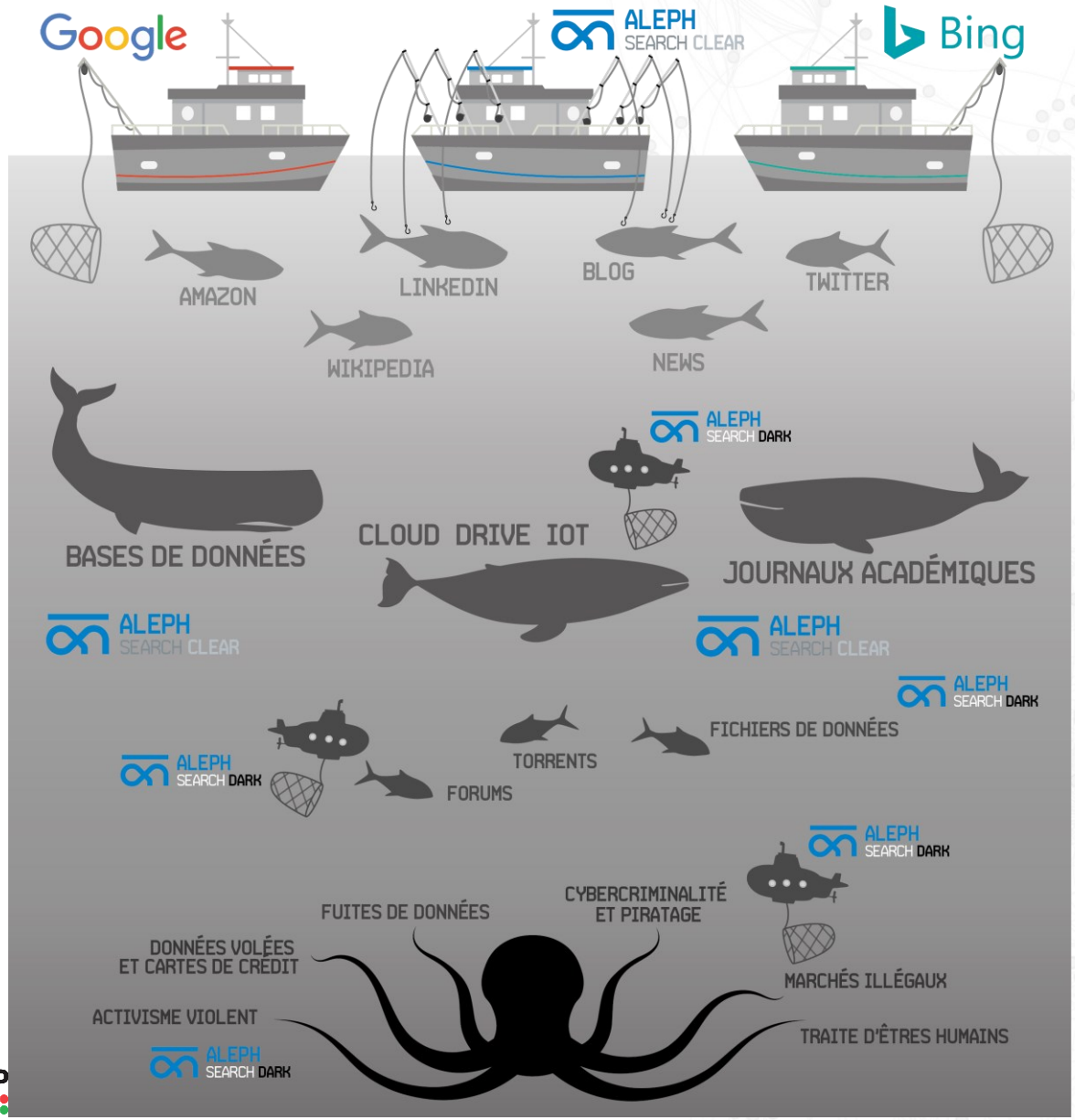
80 à 98% du web accessible non ou mal indexé (centralisé)
Forums, sites ne souhaitant pas être indexés

Stockages en ligne :

Bases de données (cloud computing, drives) connectées à Internet, objets connectés (IoT, domotique, etc.)

Dark Web

Web non accessible à travers des protocoles standards (décentralisé). Environ 350 000 domaines, dont 30 000 actifs



ALEPH

DES CONTRAINTES NORMATIVES RÉCENTES

NORME NIS2 (UE)

Entrée en vigueur en **2024**

Nouvel ensemble d'obligations de cybersécurité pour les organisations de nombreux secteurs jugés critiques pour l'économie.

A l'échelle nationale, NIS 2 s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs : parmi eux des **administrations** de toutes tailles et des entreprises allant des **PME** aux **groupes du CAC40** et leurs **sous-traitants**.

Sanctions :

7 à 10 M€ ou 1,4 à 2% du chiffre d'affaire total

Sanctions pénales

Mesures de réparation

NORME DORA (UE)

Entrée en vigueur en **2025** , renforcement de NIS2

Le règlement DORA vise à assurer une résilience opérationnelle numérique au sein de l'UE. Il concerne l'ensemble des **établissements financiers**, ainsi que des **tiers critiques** qui leur fournissent des services liés aux technologies de l'information et de la communication.

Résilience = capacité à **résister** à un évènement qui menacerait la poursuite de leur activité (panne informatique, attaque informatique ...), à y **répondre** et à **s'en remettre**.

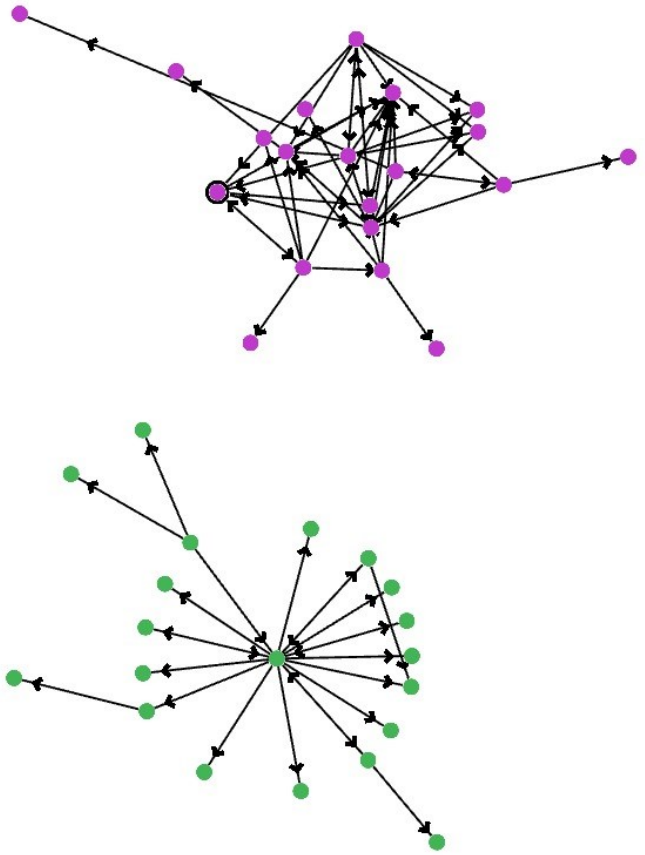
Sanctions :

Pas de plafond défini

ANALYSE COMPARATIVE SOCIETE DE LOGISTIQUE : EXPOSITION CLEAR WEB (VOLONTAIRE … OU PAS)

Violet : sites web de BETA

Vert : sites web de ALPHA



BETA

→ 20 domaines, sous domaines et domaines externes exposés
→ Pattern médiocre
→ Email leaks : 48 227

ALPHA

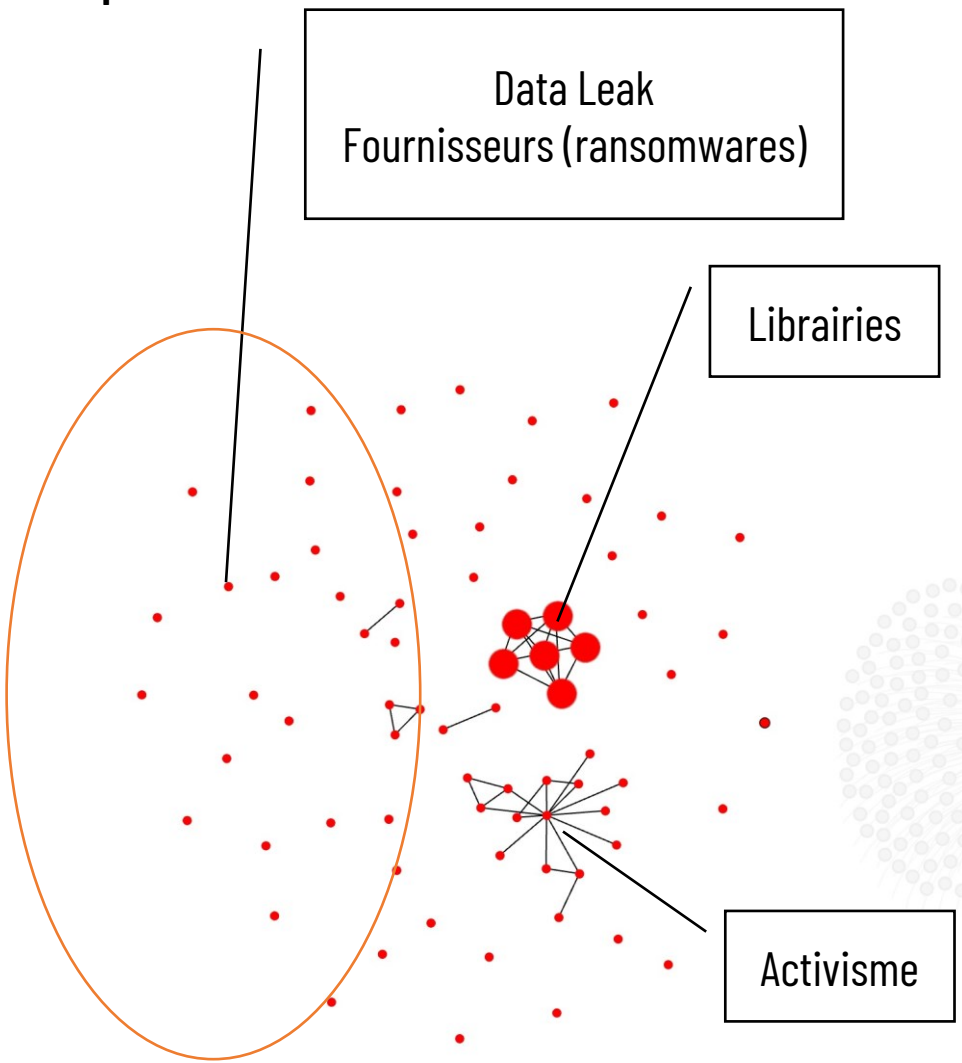
→ 20 domaines, sous domaines et domaines externes exposés
→ Excellent Pattern, maitrise du parcours

Certains domaines ne devraient cependant pas être exposés
Ex: alpha.prod.acquia-sites.com
Email leaks : 1 241

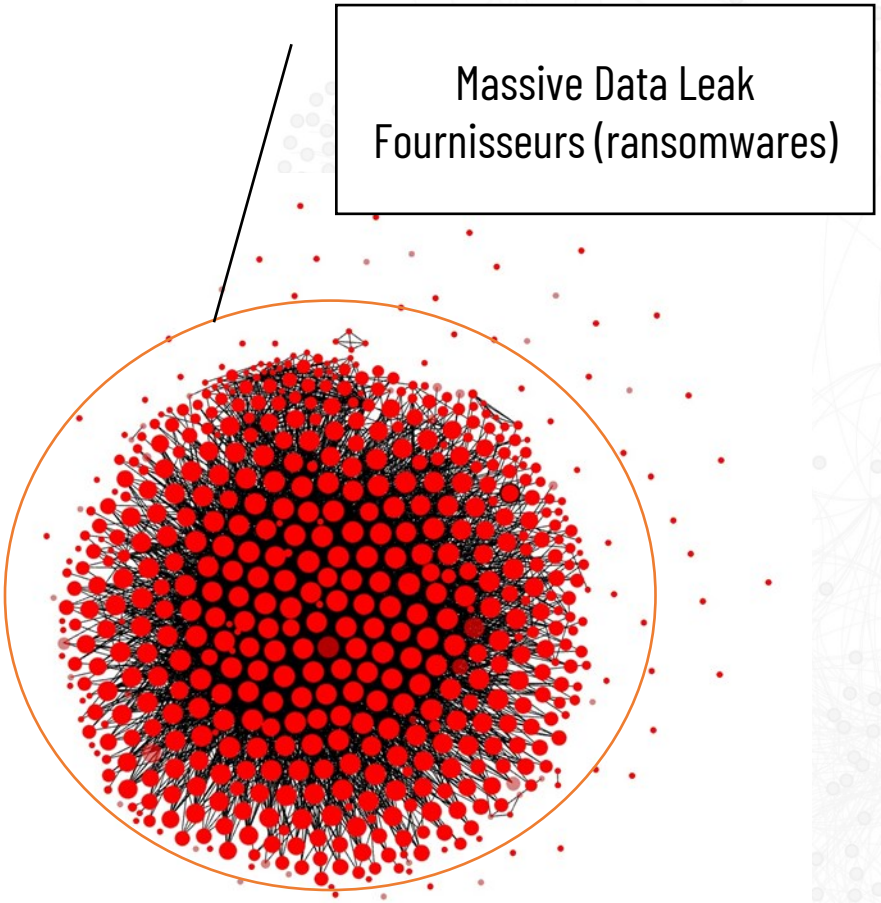
ANALYSE COMPARATIVE SOCIETE DE LOGISTIQUE : EXPOSITION DARK WEB (INVOLONTAIRE)

ALEPH SEARCH DARK

Exposition ALPHA



Exposition BETA



Chaque point rouge est un site du Dark Web

ALEPH

LOCKBIT : UNE EXEMPLE CRIANT

DEMO LOCKBIT

ALEPH SEARCH DARK

DONNÉES COLLECTÉES

Accès libre

Information blanche _ Accès libre

ALEPH SEARCH CLEAR

Légale et partagée par tous
Données publiques et référencées
Accessible via des outils standards

Presse, sites identifiés comme influents par les moteurs de recherche standards, réseaux sociaux publics...

Яндекс Baidu 百度 DuckDuckGo Qwant yahoo! 360搜索 NAVER Google Sogou搜狗 Microsoft Bing

Résultat d'investigations

Information grise _ Résultat d'investigations

ALEPH SEARCH CLEAR ALEPH SEARCH DARK ALEPH SERVICES

Légale dans un cadre défini (recherche de vos propres données)
Pas d'authentification
Disponible avec un effort mineur
Pas accessible via un moteur de recherche classique
API des réseaux sociaux ou de partenaires Aleph (en option)

Réseaux ouverts et discrets, réseaux sociaux alternatifs, forums ouverts, blogs privés...

Information noire
Pratiques illégales

Accès avec fausse authentification
Usurpation d'identité sur les forums
Hacking
Hackback

Réseaux fermés web, réseaux sociaux, forums fermés...

ALEPH

ALEPH SEARCH DARK

MAÎTRISEZ VOS RISQUES & SURVEILLEZ VOS ACTIFS STRATÉGIQUES

VOUS POURREZ :

- **Monitorer vos actifs physiques** (sites de vente, production, stockage, siège social...).
- **Monitorer vos actifs stratégiques et les accès à votre infrastructure IT.**
- **Protéger les données sensibles des personnes clés de votre entreprise.**
- **Protéger vos marques, produits, brevets et votre e-réputation.**
- **Gérer votre due diligence cyber et votre conformité** (directive NIS 2, règlement DORA, assurances...).
- **Détecter des fuites de documents internes ou externes** (fournisseurs, clients, partenaires).

SUR LES DARK & DEEP WEBS :

- **Forums et blogs de hackers 'black hats' :** échange de données et pratiques de hack.
- **Sites marchands :** vente de données et documents volés.
- **Sites d'actualité :** désinformation et diffamation, atteinte à l'image, activisme violent.
- **Sites de dépôt de code :** diffusion de codes sources de logiciels malveillants pour l'organisation de cyber attaques.
- **Sites d'hébergement de fichiers :** dépôt de fichiers issus de fuites de données et cyberattaques.

CONÇU ET HÉBERGÉ EN FRANCE

CONFORME CADRE LÉGAL OSINT FRANCE

Conforme **RGPD**

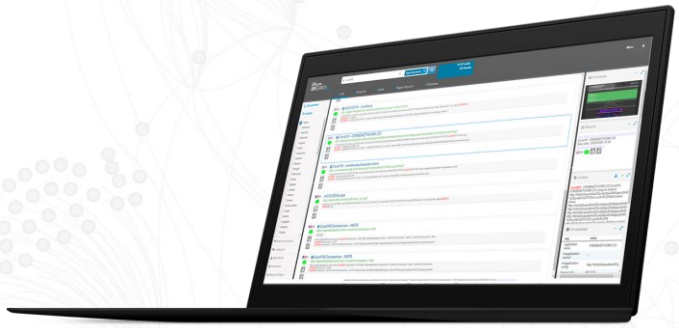
ALEPH

SOLUTION ‘ALEPH SEARCH DARK’

SaaS

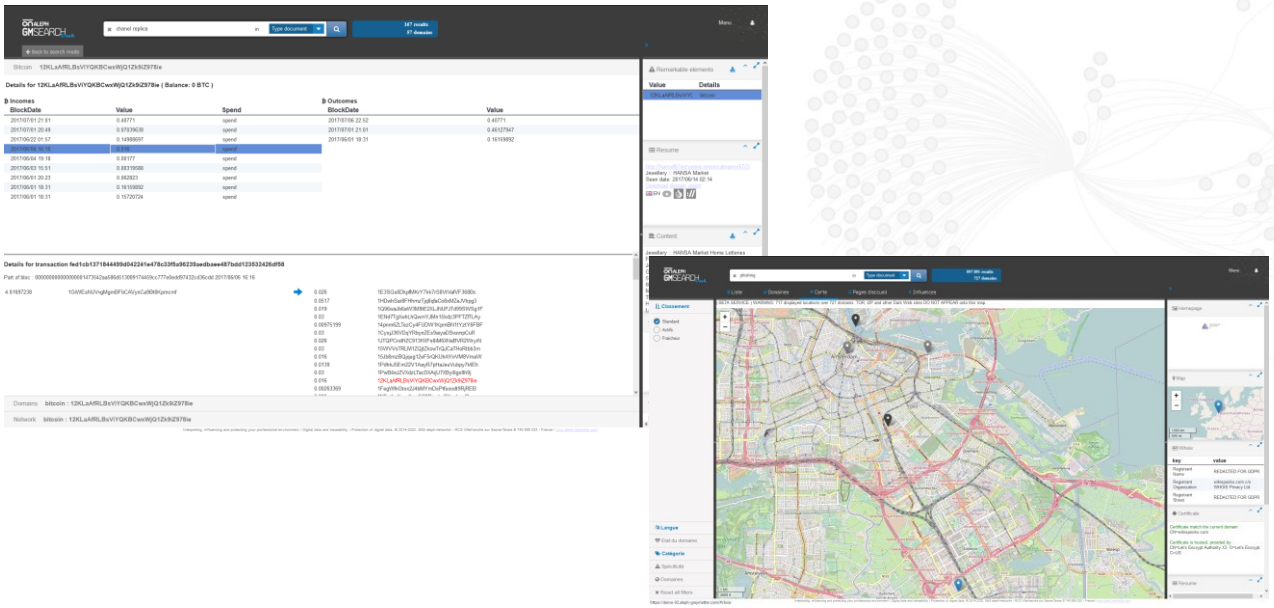
Moteur de recherche et d'analyse sur les Deep & Dark webs,

spécialisé, non intrusif et totalement indépendants de toute API.



Aleph Search Dark est aujourd’hui le moteur de recherche et d’analyse de référence des Dark & Deep Webs. Le **périmètre et les fonctionnalités d’analyse proposés sont uniques.**

Aleph Search Dark permet la recherche de traces et de données illicites sur les Dark & Deep Webs, la cartographie de ces zones du web, l’identification de clusters d’influence et la recherche de certains éléments remarquables.



- **Cyber Sûreté et analyse des risques** des entreprises et acteurs publics
- **Besoins métier :**

- surveillance des fuites de données,

- risques sur les infrastructures logique (SI…) et physique (bâtiments, objets connectés…),

- risques géopolitiques,

- VIP et personnel à risque,

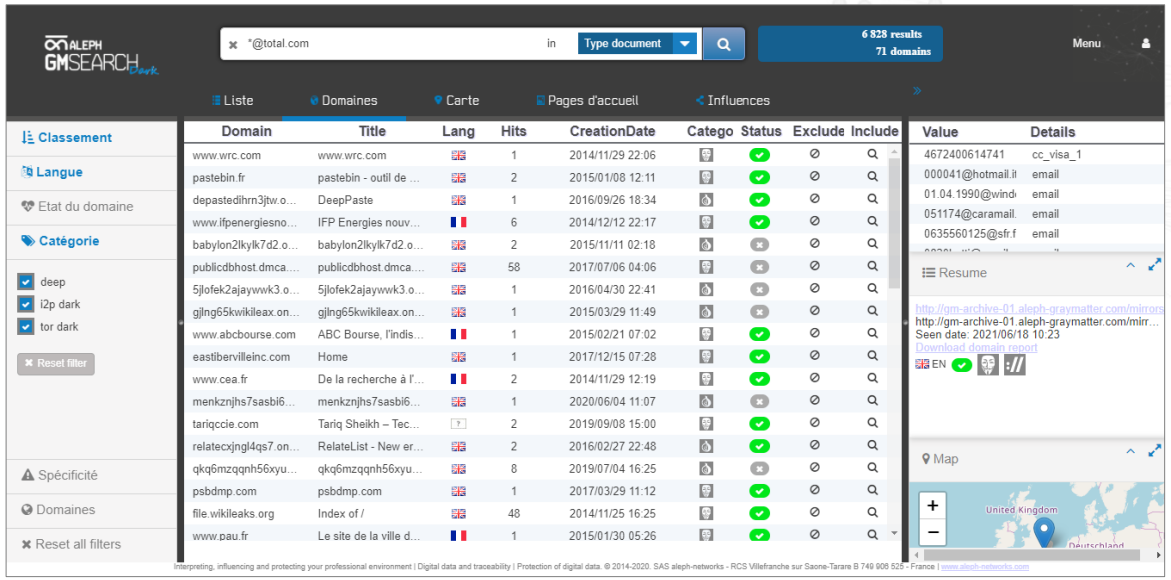
- actifs stratégiques et financiers…

SOLUTION ‘ALEPH SEARCH DARK’

SaaS

MANAGEMENT DES RISQUES / THREAT INTELLIGENCE :

- Protection des données sensibles des personnes clés de votre entreprise.
- Protection de vos marques, produits, brevets et de votre e-réputation.
- Surveillance des actifs physiques (sites de vente, production, stockage, siège social…).
- Surveillance des actifs stratégiques et des accès à votre infrastructure IT.
- Détection des fuites de documents internes ou externes (fournisseurs, clients, partenaires).
- Due diligence cyber.



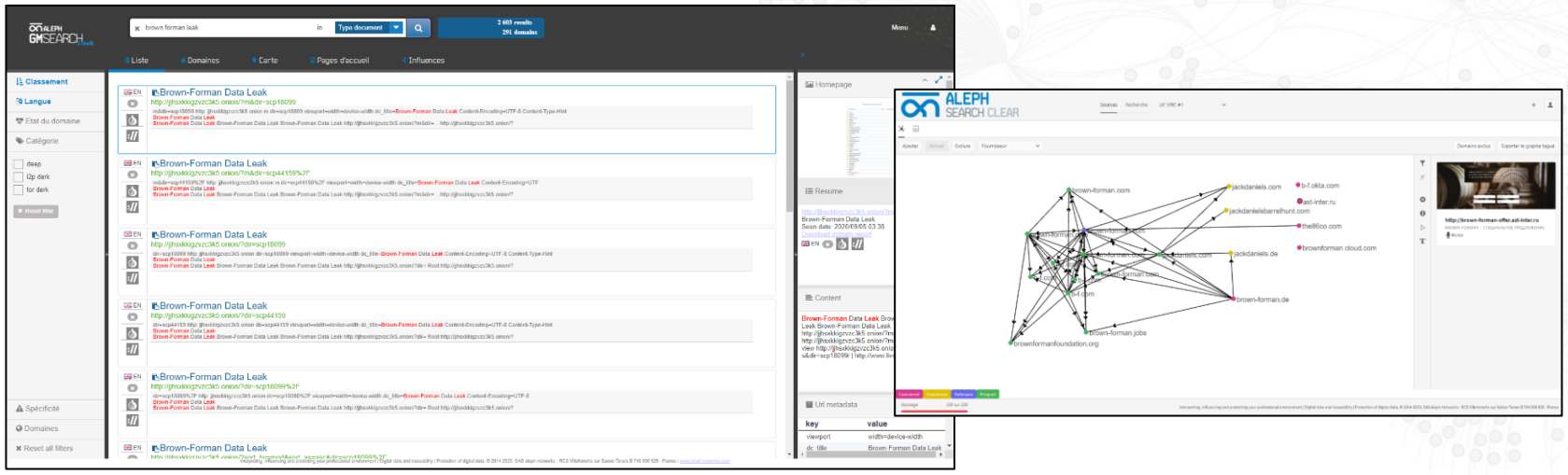
- *« Je veux surveiller les fuites de mails avec mots de passe de toute mon entreprise. »*
- *« Je souhaite surveiller les données personnelles des VIP de mon entreprise qui seraient disponibles sur le web caché. »*
- *« Je veux vérifier que mes noms de domaines ne soient pas utilisés frauduleusement. »*
- *« Je veux avoir une vision objective de mon exposition sur le dark web et de celle de mes fournisseurs. »*

AU DELA DU MOTEUR DE RECHERCHE

L'ANALYSE ET LA VISUALISATION :

- Détection des langues
- Détection d'éléments remarquables
- Détection de patterns significatifs
- Analyse des métadonnées
- Graphes d'influence
- Géolocalisation
- Alerting
- Travail collaboratif
- Aide à la restitution des données

- *« Je veux cartographier la concurrence chinoise. »*
- *« Je souhaite identifier tous les comptes de réseaux sociaux de mes concurrents. »*
- *« Je veux voir apparaître au plus vite les écosystèmes menaçant mon business. »*
- *« Je veux identifier les filiales de mes concurrents russes et de mes fournisseurs turcs. »*
- *« Je souhaite être alerté par l'arrivée d'un nouvel acteur dans mon écosystème. »*
- *« Je souhaite localiser les lieux de stockage de donnée de mes fournisseurs. »*



NOS 2 MOTEURS DE RECHERCHE ET D'ANALYSE

Google Custom Search

Clear Web

Sourcing imposé et limité

- Règle d'affichage des résultats inconnue et non paramétrable
- Représentation des résultats sous forme de liste
- Alertes

ALEPH SEARCH DARK

Dark & Deep Webs

DEEP WEB · Tor · I2P

- Règles d'affichages des résultats proposées et paramétrables
- Représentation des résultats multimodale, avec graphes dynamiques
- Partage d'alertes et export de données

ALEPH SEARCH CLEAR

SaaS

Clear & Deep Webs

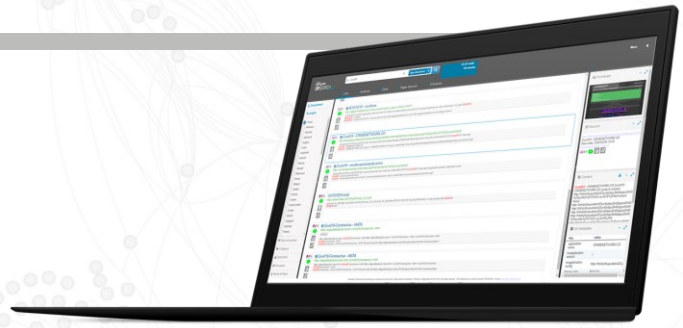
Sourcing personnalisé et illimité

ANALYSE & VISUALISATION :

- Détection des langues
- Détection d'éléments remarquables
- Détection de patterns significatifs
- Analyse des métadonnées
- Graphes d'influence
- Géolocalisation
- Alerting
- Travail collaboratif
- Aide à la restitution des données

ALEPH

LES SOLUTIONS ALEPH



Vous voulez maîtriser totalement votre Lutte Informatique et votre Renseignement Numérique :

Aleph met à disposition sa technologie et ses outils en mode SAAS pour construire votre propre plateforme de surveillance et d'analyse sur mesure.

ALEPH SEARCH DARK

Moteur de recherche et d'analyse sur les Deep & Dark Webs

ALEPH SEARCH CLEAR

BETA TESTING

Moteur de recherche et d'analyse sur les Clear & Deep Webs

ALEPH THREAT INTELLIGENCE

Flux techniques à destination de SOC CERT, plateformes & cabinets de conseil cyber

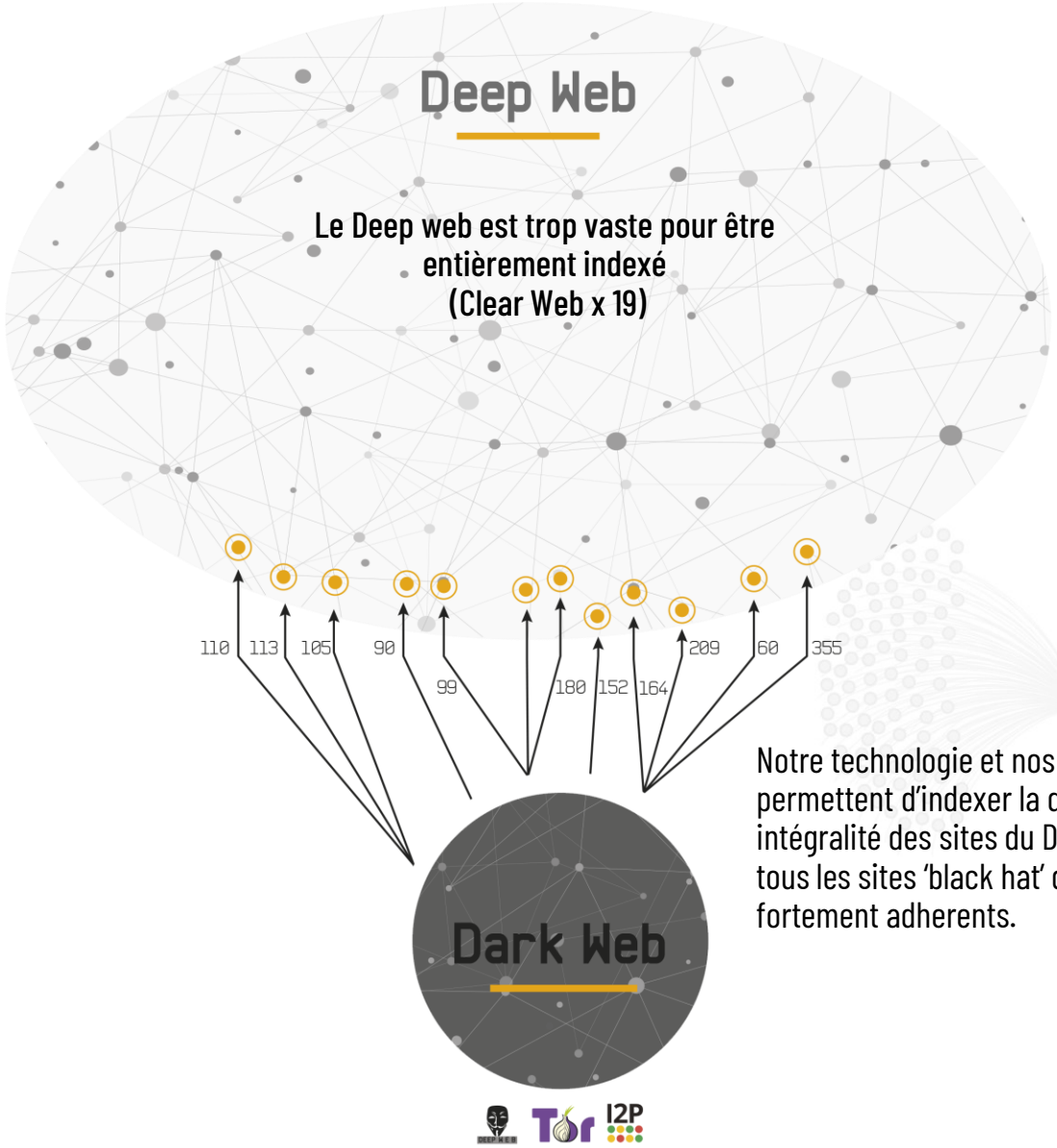
ALEPH SERVICES

Service de surveillance de vos actifs stratégiques (documents, e-reputation, actifs physiques, personnes clés, actifs logiques , nom de domaines, due diligence Cyber)

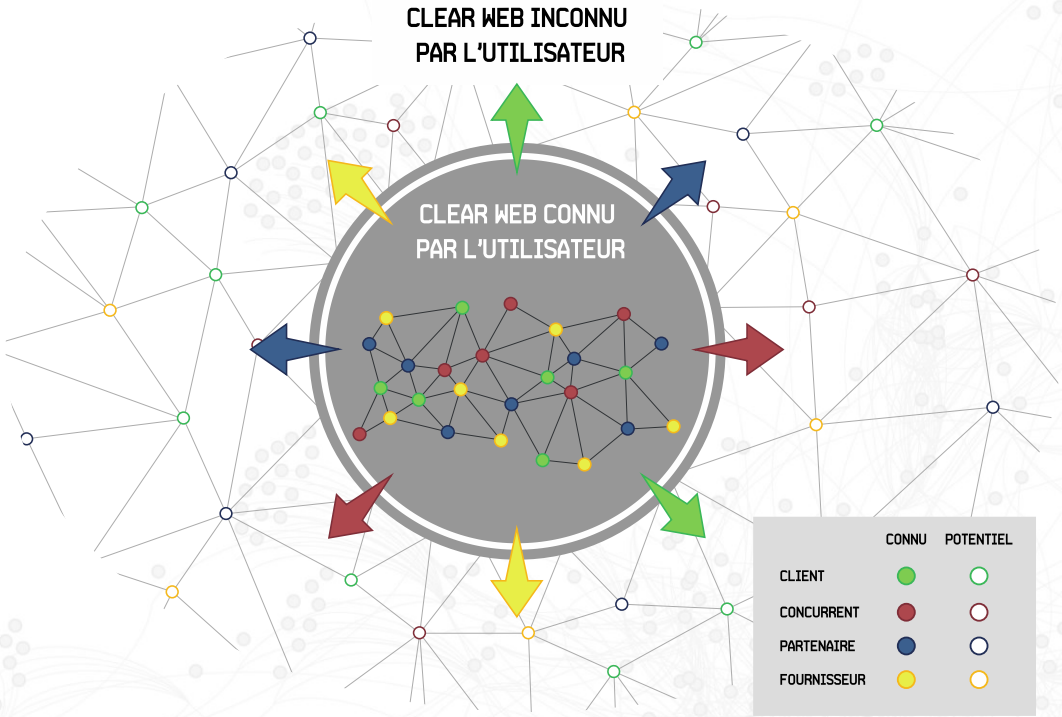
ALEPH

ALEPH GRAYMATTER®
DONNÉES NUMÉRIQUES ET TRAÇABILITÉ

NOTRE TECHNOLOGIE BREVETEE



Notre technologie et nos solutions permettent d'indexer la quasi intégralité des sites du Dark Web et tous les sites 'black hat' du Deep Web fortement adherents.

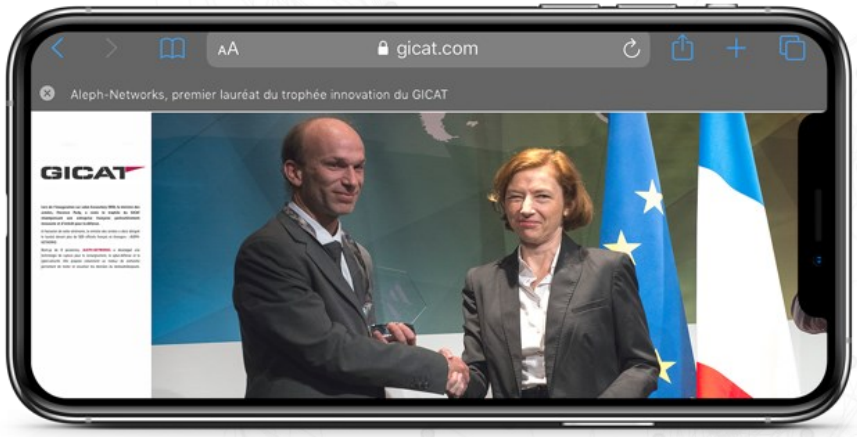


Notre technologie et nos solutions permettent la constitution d'une infosphère de travail personnalisée, intégrant n'importe quelle source des Clear et Deep Webs, selon les choix de l'utilisateur.

ALEPH

NOS RÉFÉRENCES

Clients confidentiels

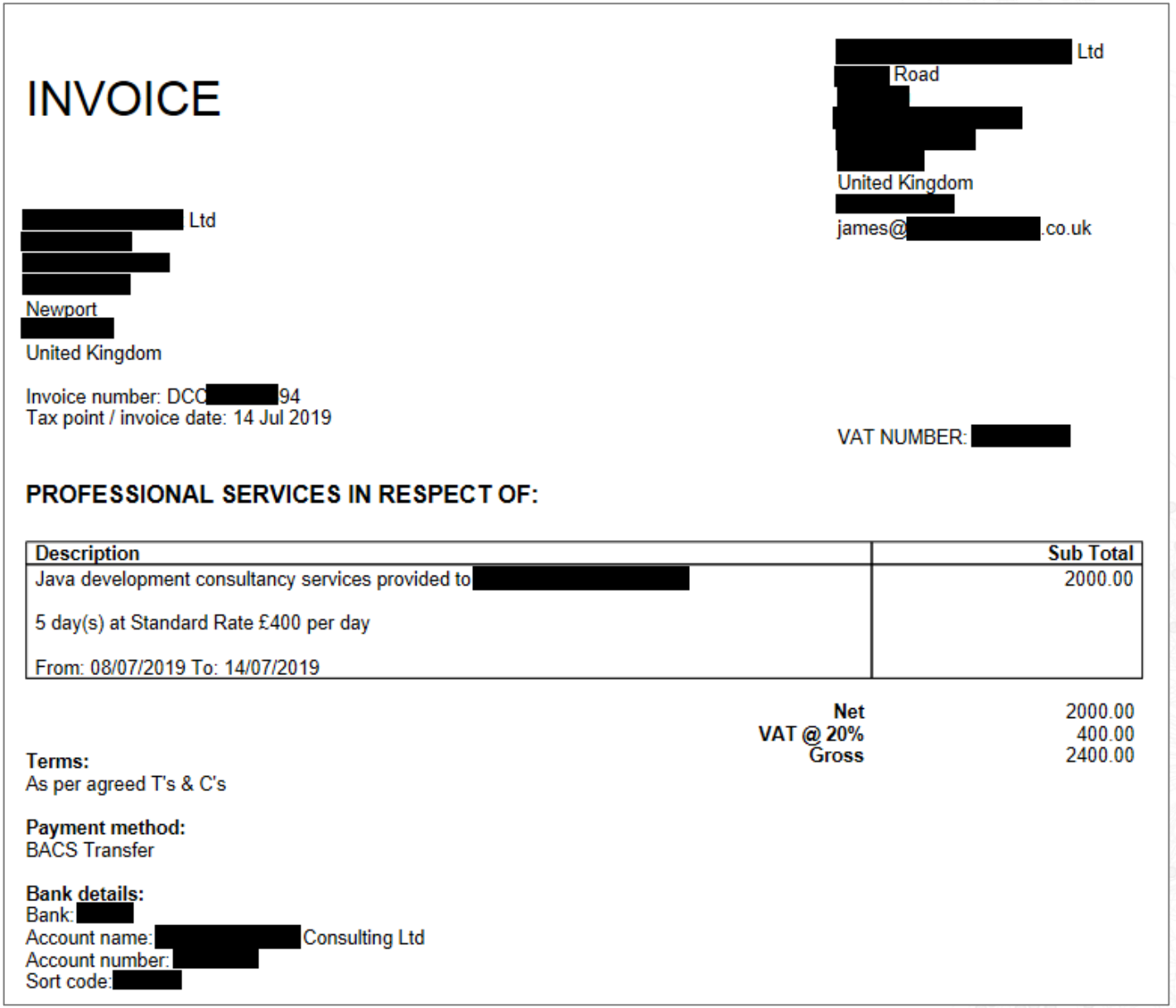


Remise du Prix de l'Innovation du GICAT lors d'Eurosatory 2018, remis par Florence Parly, Ministre des Armées,

pour sa technologie brevetée.

TECHNOLOGIE BREVETÉE

FUITES DE DONNÉES – LES VULNÉRABILITÉS VIA LES FOURNISSEURS



INVOICE

[redacted] Ltd
[redacted] Road
[redacted]
United Kingdom
[redacted]
james@[redacted].co.uk

[redacted] Ltd
[redacted]
Newport
[redacted]
United Kingdom

Invoice number: DCC[redacted]94
Tax point / invoice date: 14 Jul 2019

VAT NUMBER: [redacted]

PROFESSIONAL SERVICES IN RESPECT OF:

Description	Sub Total
Java development consultancy services provided to [redacted] 5 day(s) at Standard Rate £400 per day From: 08/07/2019 To: 14/07/2019	2000.00

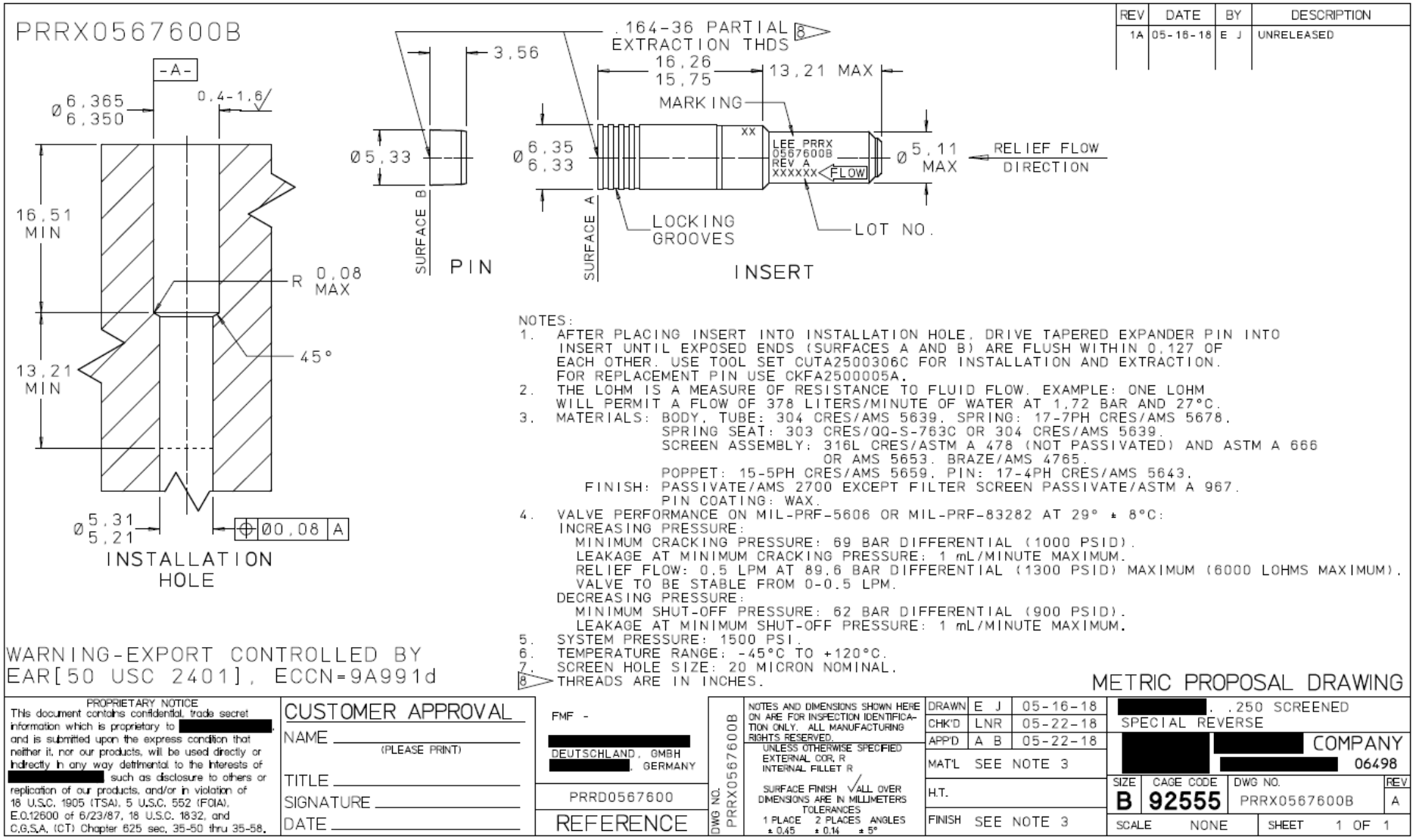
Net	2000.00
VAT @ 20%	400.00
Gross	2400.00

Terms:
As per agreed T's & C's

Payment method:
BACS Transfer

Bank details:
Bank: [redacted]
Account name: [redacted] Consulting Ltd
Account number: [redacted]
Sort code: [redacted]

FUITES DE DONNÉES – LES VULNÉRABILITÉS VIA LES FOURNISSEURS



FUITES DE DONNÉES – LES VULNÉRABILITÉS VIA LES PARTENAIRES

MUTUAL NON-DISCLOSURE AGREEMENT

THIS AGREEMENT (the "Agreement") is made and entered into as of 12 July 2020 (the "**Effective Date**") by and between [redacted] Systems, Ltd., a corporation duly organized and existing under the laws of Israel with its principal place of business at [redacted], Israel and [redacted] Ltd., Reg. No: [redacted], a company incorporated under the laws of Israel and whose principal place of business is at: 2 [redacted], Israel.

1. As used herein:

1.1. "**Confidential Information**" shall mean any and all information provided by either party to the other, including, but not limited to: (a) patent and patent applications; (b) trade secrets; (c) proprietary information, such as mask works, ideas, samples, media, techniques, sketches, drawings, works of authorship, models, inventions, know-how, processes, apparatuses, equipment, algorithms, software programs, software source documents, and formulae related to the current, future, and proposed products and services of each of the parties; (d) their respective information concerning research and development, experimental work, design details and specifications, engineering; (e) financial information and other information relating to either party's financial condition; (f) information regarding procurement requirements, purchasing, manufacturing; and (g) lists and information of present or prospective customers, investors, employees, and information regarding business and contractual relationships and/ or opportunities with customers, investors, employees, business forecasts, sales and merchandising, marketing plans and information.

1.2. "**Disclosing Party**" means that Party which directly or indirectly provides or makes available Confidential Information to the other in connection with this Agreement.

1.3. "**Receiving Party**" means that Party which receives or obtains Confidential Information directly or indirectly from the Disclosing Party in connection with this Agreement.

FUITES DE DONNÉES – LES VULNÉRABILITÉS VIA LES CLIENTS

[redacted]

Avis d'opération de virement

Compte-rendu de votre ordre n° [redacted]269
enregistré le 09/04/2022 à 10:16

Imprimé le 09/04/2022 à 10:16

Montant	**8 753,69 EUR**
Date demandée	**09/04/2022**
Etat	**Exécuté**

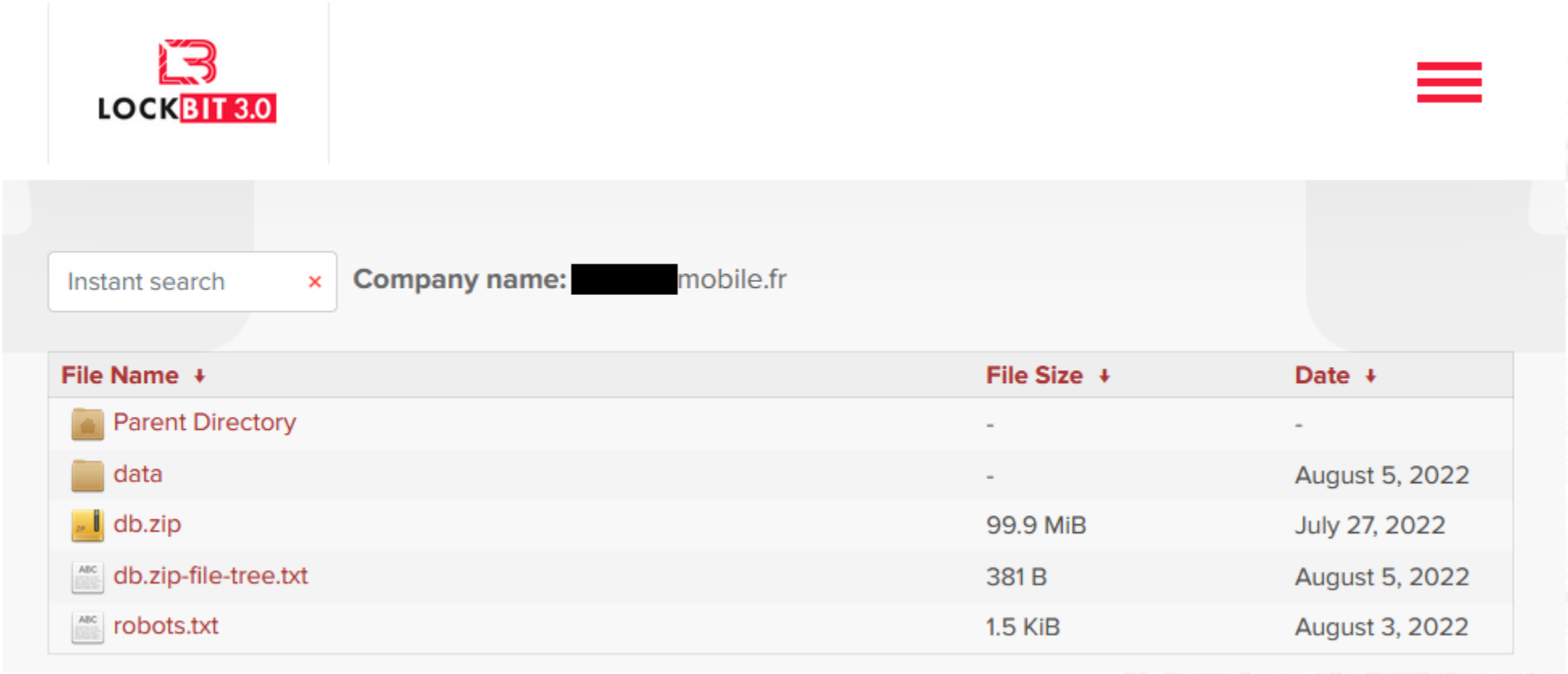
COMPTE A DEBITER	
Compte	[redacted] **COMPTE COURANT ENTREPRISE** **EUR** [redacted] [redacted] **CENTRE ENTREPRISES**
Intitulé	**VIR** [redacted] **232** [redacted]

BENEFICIAIRE A CREDITER	
Compte	[redacted] **FR** [redacted] [redacted] **BIC :** [redacted]
Motif	[redacted]
Référence	[redacted]

Cet ordre de virement a été traité selon vos conditions tarifaires habituelles.
Les informations incluses dans le présent compte-rendu sont de nature confidentielle et sont à l'usage exclusif du donneur d'ordre.
Toute reproduction partielle ou totale de quelque manière ou procédé que ce soit ne saurait engager la responsabilité de la banque.

FUITES DE DONNÉES – LES VULNÉRABILITÉS VIA LES SALARIÉS

Fuite de la base de données clients d'un opérateur de téléphonie mobile :



FUITES DE DONNÉES – LES VULNÉRABILITÉS VIA LES SALARIÉS

Nom, prénom, adresse

Adresse mail professionnelle

[redacted]|PASCAL|18|RUE [redacted]|||75013|PARIS|France|pascal.[redacted]@[redacted].com|False|
0686[redacted]||a|23|23|6|-1|PASCAL|2013-10-13 00:00:00|AXABFRPPXXX|11412[redacted]|
12548[redacted]|FR|76|axa banque|False|False|False|False|False|False|False|||||||||75|1
|M|1967-10-06 00:00:00|45|280|320|.0000|2022-05-23 00:00:00|2009-07-16 17:01:02|13|3
||0|0|False|False||False|False|||||||2022-05-25 00:20:05|2022-06-28
14:38:30.490000000

Date de naissance

Leader européen de l'OSINT sur toutes les couches du web.

-

contact@aleph-networks.com
www.aleph-networks.com

413, rue Héron
69400 Villefranche s/Saône
France

ALEPH