



Une formation
Alphorm.com

Formation

Hacking & Sécurité

Acquérir les fondamentaux

Les techniques d'OSINT (Open Source Intelligence)



Hamza KONDAH



Une formation
Alphorm.com

Introduction

OSINT : Open Source Intelligence

Une des pratiques de recherche passive

Identification d'informations **stratégiques**
sur une cible

Renseignement obtenu par une source
d'information publique



Plan de la formation

Présentation de la formation

Introduire la notion d'OSINT

Maîtriser l'OSINT pour la découverte d'information
sur les organismes

Découvrir l'analyse des métadonnées

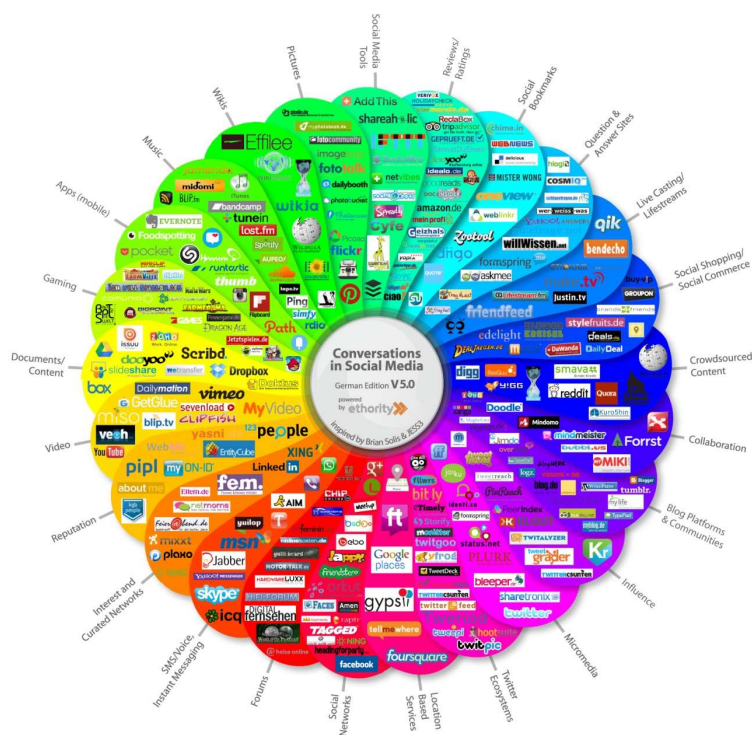
Maîtriser le threat Hunting pour l'OSINT

Maîtriser l'OSINT au niveau des Réseaux sociaux

Découvrir des techniques d'OSINT complémentaires

Conclusion et perspectives de la formation

Une formation
Alphorm
.com



Conversations in Social Media - Version 5.0 - 09.2012 by eThorty | <http://social-media-prisma.eThorty.de> | <http://www.twitter.com/ethorty> | Contact us for updates: prisma@ethorty.de



OSINT & OSINFO



Public concerné

Pentesteurs

Responsables DSI

Responsables sécurité du SI

Chefs de projets IT

Techniciens et administrateurs systèmes et réseaux

Consultants en sécurité de l'information

Journalistes



Connaissances requises

Bonnes connaissances en systèmes
d'exploitation et réseau

Connaissance de base en sécurité des
systèmes d'information

Optionnel : Connaitre le C, Python,
HTML et JS

Une formation
Alphorm.com





AVERTISSEMENT

Ni le **formateur** Ni **Alphorm** ne sont responsables de la mauvaise utilisation du contenu de cette formation

L'utilisation des outils doit être réalisée uniquement au sein d'un environnement virtuel ou avec une autorisation préalable de l'entreprise



Préparer son lab



Hamza KONDAH

Une formation
Alphorm.com



Composants du LAB

Hyperviseur : VMWare Workstation Pro 15 ou plus



Trace Labs OSINT VM
CPU : i3 ou plus
8 GB RAM
Stockage
40 GB

Windows 10 64Bits

Une formation
Alphorm.com



Composants du LAB

Une bonne connexion internet

Un Bloc-notes

Customiser son processus !

De la motivation et persévérance 😊

Une formation
Alphorm.com



Découvrir la définition de l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Plan

Intelligence stratégique

OSINT

OSINFO vs OSINT

Une formation
Alphorm.com



Intelligence stratégique

Le processus de la veille stratégique
est très proche de celui du
renseignement

Il est naturel d'observer un
rapprochement entre les deux
disciplines

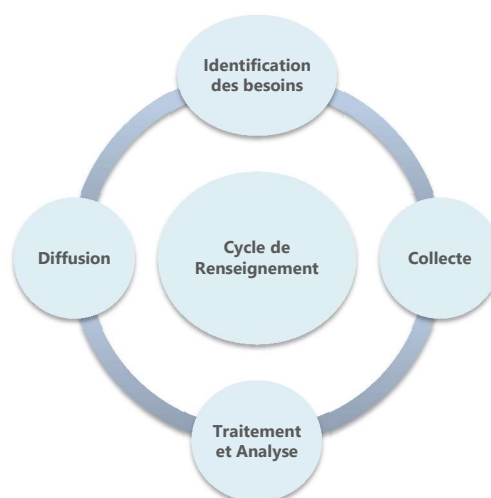
Une formation
Alphorm.com

Intelligence stratégique et cycle de renseignement

Une formation
Alphorm.com



Intelligence stratégique et cycle de renseignement



Une formation
Alphorm.com



OSINT

Open Source Inteligence, OSINT

Le renseignement de sources ouvertes ou renseignement d'origine source ouverte est un renseignement obtenu par une source d'information publique .

Une formation
Alphorm.com



OSINT

C'est une discipline à part entière qui consiste à collecter ces information ouvertes mais également à les analyser pour produire des connaissances actionnable pour les décideurs

Une formation
Alphorm.com



Une formation
Alphorm.com

OSINFO vs OSINT

Collecter de l'information ne veut pas dire créer des connaissances actionnable

Il y a une multiplication des moyens techniques qui permettent de récolter de l'information de façon automatisée



Une formation
Alphorm.com

OSINFO vs OSINT

Il est nécessaire de traiter cette information et de l'analyser pour conter l'infobésité générée par l'amélioration des moyens techniques
La règle du 10/90





Démystifier les différentes catégories de l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Plan

Open Source Intelligence
Défi de vérification de l'information

Une formation
Alphorm.com



Open Source Intelligence

Human IntellHUMINTigence	SIGINT Signal Intelligence	IMINT Imagery Intelligence	CYBERINT Cyber - Intelligence
• Informations obtenus à partir de sources humaines • EX : <i>Mystery Shopper Rapports d'etonnements , Sondages , Interviews</i>	• Informations obtenues à partir de signaux • EX : Analyse du trafic internet , Surveillance de fréquence radio...	• Informations obtenues à partir d'imagerie • EX : Imagerie satellite commerciale , Google Street View , Enregistremen t par des drones...	• Information obtenues à partir d'internet • EX : Social Media , Blogs , PDF , API...



Défi de vérification de l'information

Fiabilité	Crédibilité
A : Source d'information jugée très fiable	1 : Information jugée très crédible
B : Source d'information jugée fiable	2 : Information jugée crédible
C : Source d'information jugée relativement fiable	3 : Information jugée relativement crédible
D : Source d'information jugée peu fiable	4 : Information jugée peu crédible
E : Source d'information jugée non fiable	5 : Information jugée non fiable
F : Impossible de juger de la fiabilité de la source	6 : Impossible de juger de la crédibilité

La fiabilité est jugée sur le temps . Une source qui fournit de l'information qui est jugée fiable à répétition ou qui dispose d'une réputation certaine doit se voir accorder un meilleur classement au fil du temps

La crédibilité est jugée par comparaison avec le corpus de connaissance déjà établi . Une information est jugée crédible si elle est logiquement acceptée par ce corpus . Une information peut être contradictoire tout en restant logiquement valide



Une formation
Alphorm.com

Appréhender les approches et méthodologies relatives à l'OSINT



Hamza KONDAH



Une formation
Alphorm.com

Plan

Intelligence stratégique et cycle de renseignement

Framwork OSINT

Intelligence stratégique et cycle de renseignement

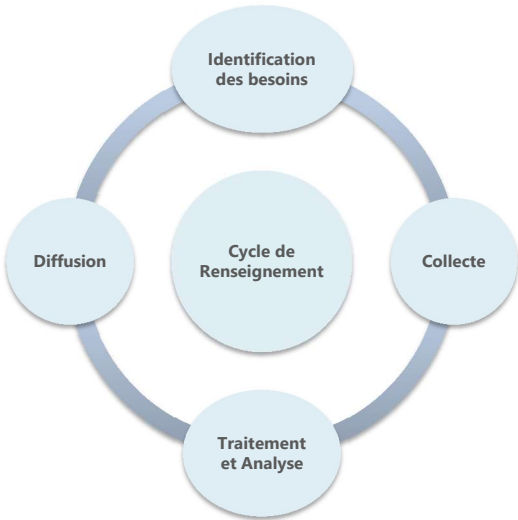
Méthodologie OSINT

Approches OSINT



Une formation
Alphorm.com

Intelligence stratégique et cycle de renseignement



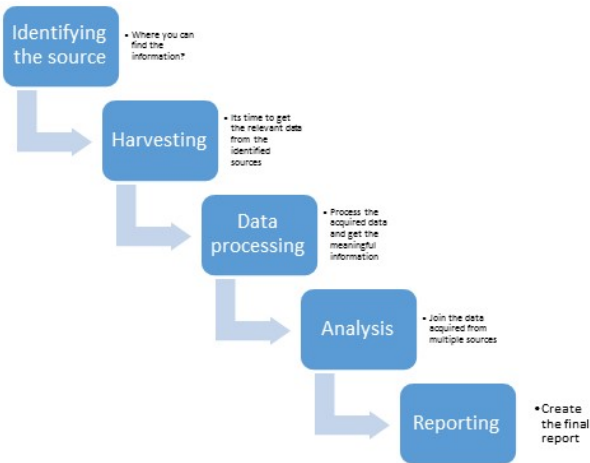
Une formation
Alphorm.com

Framwork OSINT

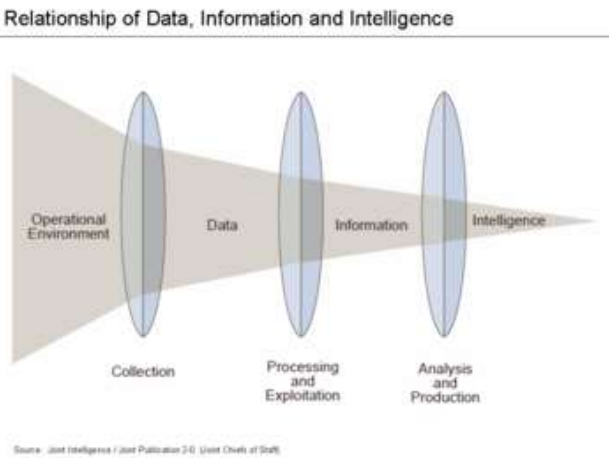




Intelligence stratégique et cycle de renseignement

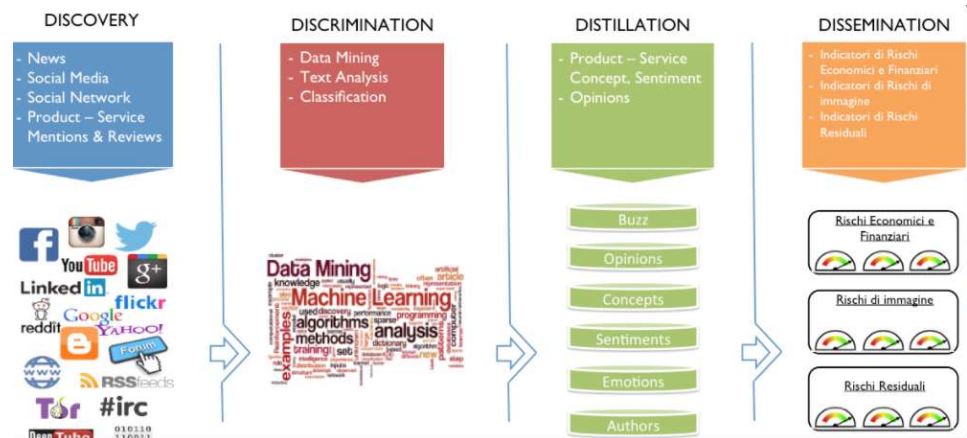


Méthodologie OSINT





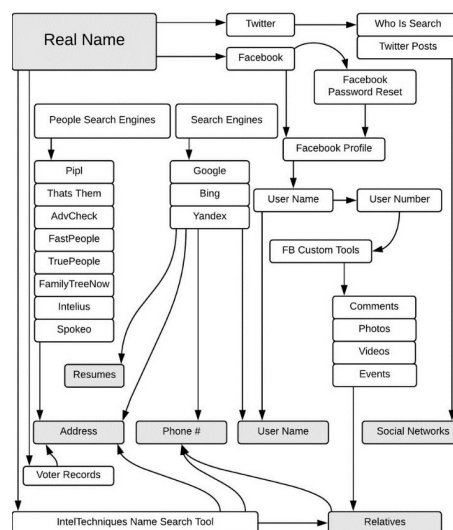
Méthodologie OSINT



Une formation
Alphorm
com



Méthodologie OSINT

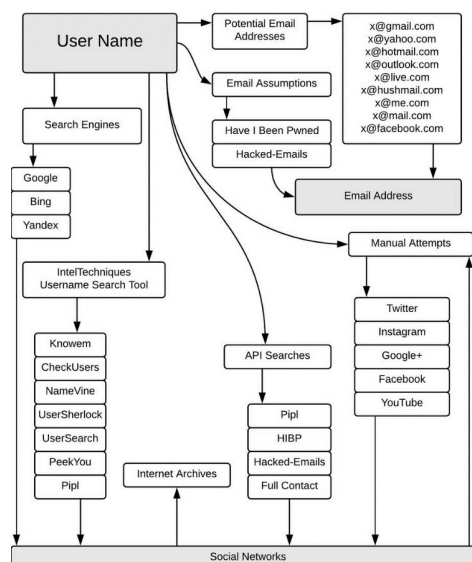


Une formation
Alphorm
com



Une formation
Alphorm.com

Méthodologie OSINT



Une formation
Alphorm.com

Approches OSINT

- Base de données publiques
- Google Dorks
- Maltego (ou autres corrélateurs...)
- Réseaux sociaux et Doxing
- Darknet
- Crawlers intelligents
- Approches avancées



Une formation
Alphorm.com

Retenir les meilleures pratiques relatives à l'OSINT



Hamza KONDAH



Une formation
Alphorm.com

Meilleures pratiques

Utiliser des sources d'informations
variées

Corréler les résultats

Organiser son processus

Prendre des notes (Tools)



Une formation
Alphorm.com

Structurer ses résultats d'analyse



Hamza KONDAH

Start.me

Maltego casefile



Introduire les techniques de récoltes d'informations



Hamza KONDAH



Plan

Introduction

Techniques d'OSINT

Une formation
Alphorm.com



Introduction

Exploiter l'OSINT peut passer par différentes approches

Chaque approche doit être customisé selon la situation

Il n'existe pas d'outils/source mieux que d'autres, il faut :

Structurer → Filtrer → Choisir → Améliorer

Une formation
Alphorm.com



Techniques d'OSINT

Manuellement

Ressources
publics

Outils
automatisés

Tiers

Une formation
Alphorm.com



Découvrir les outils de récoltes d'informations



Hamza KONDAH

Une formation
Alphorm.com

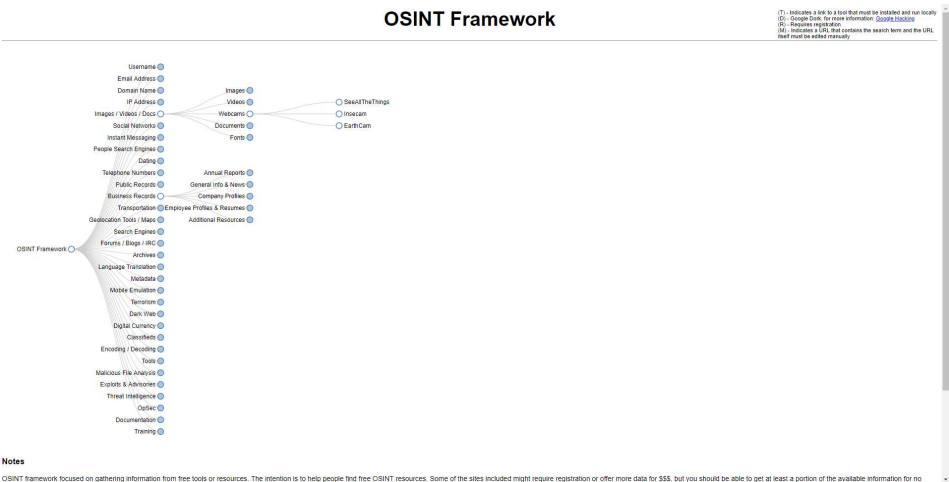


Le tenant Intune

Plateforme Intune dans le cloud
Contient un nom de domaine
Plusieurs plateformes sur le tenant :
Office 365, Azure, Intune
Une seule base de compte

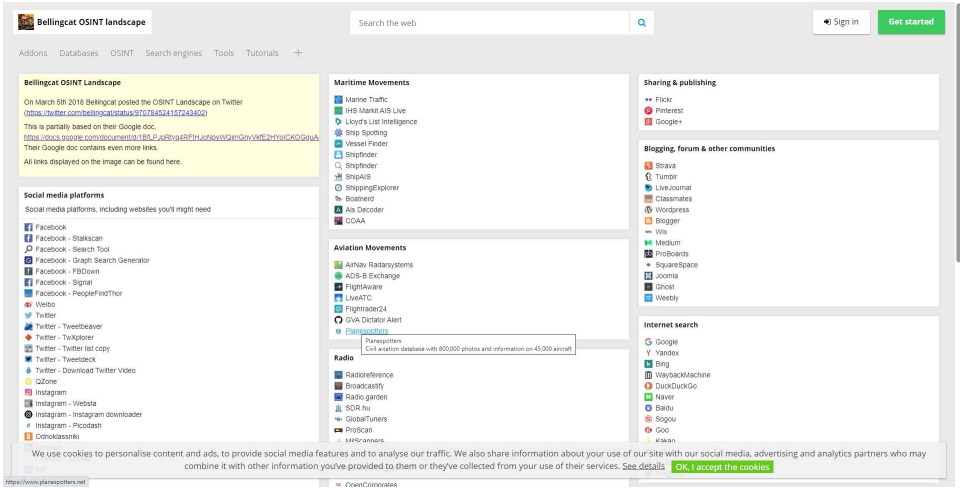


OSINT FRAMEWORK





START.ME



Outils de récolte d'informations



Découvrir l'outil LAMPYRE pour de l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Plan

Découvrir Lampyre
Avantages
Découvrir Lampyre
LAB : Lampyre

Une formation
Alphorm.com



Découvrir Lampyre

Obtain, visualize and analyze data in
one place to see what others can't.

Alternative à Maltego

Moins cher surtout ...

Une formation
Alphorm.com



Avantages

The data is easy to visualize in a
schema

No Linux is required

It doesn't require you to mess around
with APIs

Une formation
Alphorm.com



Découvrir Lampyre

More than 100 requests for obtaining and processing data

User ontology for working with the objects of your interest

Importing data from a file for working offline

More than 100 regularly updated data sources

Python API for fulfilling the most challenging tasks

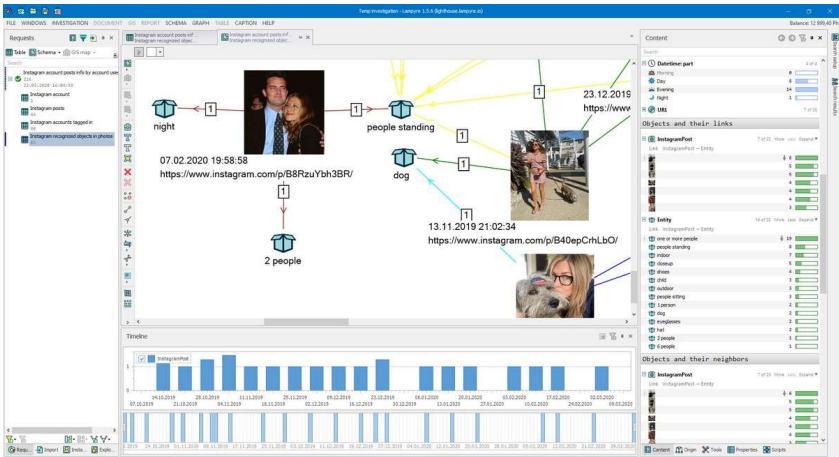
Statistical and time-line data analysis

Obtaining data in one click without registration and additional expenses

Working with data on a map, graph and in a table at the same time



LAB : Lampyre





Maitriser l'outils LAMPYRE pour l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Maitriser l'outils MALTEGO pour l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Le principe du Doxing : Méthodologie

- Les méthodes de recherche utilisent principalement internet
- ✓ Les réseaux sociaux, tels facebook, linkedin, etc...
- ✓ Les moteurs de recherches
- ✓ Les informations récupérées sur les sites par piratage ou en coopération avec les administrateurs du site



Une formation
Alphorm.com

Le principe du Doxing : Méthodologie

- ✓ En piégeant la personne ciblée (hameçonnage par message privé pour l'attirer vers un site dont le pirate est administrateur afin de récupérer son ip, lien de photo en message privé, cheval de troie)
- ✓ Croisement des sources de plusieurs sites pour trouver les différents pseudonymes de la personne ciblée



Une formation
Alphorm.com

Le principe du Doxing : Méthodologie

- Maltego est un outil qui permet de récupérer et agréger des informations dans le but de faire du footprinting.
- Cette technique permet d'obtenir des informations sur des cibles (personnes, machines, réseaux, etc.) uniquement à partir de sources dont l'accès est libre et autorisé (whois, requêtes SNMP, etc.).



Une formation
Alphorm.com

Maltego

- Cette application est disponible par défaut dans Kali, mais, étant implémentée en Java, elle peut fonctionner sur d'autres Linux-like, sur Windows ou encore sur Mac OS.



MALTEGO



Maitriser l'outils SPIDERFOOTFX de l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Maitriser l'outils shodan de l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Plan

Définition

Lab : Test d'exposition

Une formation
Alphorm.com



Définition

*Un test d'exposition consiste à énumérer tous les actifs présents sur le réseau public d'une organisation
Ce qui inclus toute ressources exposées sur internet (Composant SI ou pas)*

Une formation
Alphorm.com



Lab : Test d'exposition



Une formation
Alphorm.com



Maitriser l'outil zoomeye de l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Maitriser les Googles droks



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction
Google : Ami ou ennemi ?
Opérateurs
Labs : Google Dorks

Une formation
Alphorm.com



Une formation
Alphorm.com

Introduction

Technique de recherche :

Seulement inscrire un mot et
effectuer une recherche

Vous devez vérifier votre présence Internet:

Google est une base de données qui
possède presque tout !



Une formation
Alphorm.com

Introduction

Une des plus puissantes bases de données au monde

Les étudiants ...

Les entreprises ...



Introduction

Que peut faire Google pour un pirate ?

Rechercher des informations sensibles

Effectuer des balayages de
vulnérabilités

Proxy transparent

Une formation
Alphorm.com



Google, ami ou ennemi ?

Google est **le meilleur ami** de
chacun (le vôtre et celui des pirates)

La cueillette d'information et
l'identification des vulnérabilités sont
les premières étapes d'un scénario
typique du Hacking ;

La reconnaissance

Une formation
Alphorm.com



Google, ami ou ennemi ?

Passif, furtif et contient une immense collection de données

Google est beaucoup plus qu'un moteur de recherche

Avez-vous utilisé Google pour vérifier votre organisation aujourd'hui ?

Une formation
Alphorm.com

Advanced	What you can do with it	Google this
site:	search only within a specific site	site: www.stanford.edu
filetype:	find a type of file: PDF, DOC, TXT ...	filetype: PDF
define:	find definitions for a word	define: audacity
intitle:	find words in the title of the webpage	intitle: inspirational
..	get ranges of numbers, dates, or prices	presidents 1800 ..1900
word * word	find other combinations of words between words	creative * writing
- word	search for homer, but NOT simpson	homer -simpson
"word"	find exact words—no synonyms or plurals	"peace" "freedom"
"set of words"	search for exact set of words, quotes or phrases	"I have a dream"



Les opérateurs

Opérateurs de Google :

Les opérateurs sont utilisés pour raffiner les résultats et maximiser la valeur d'une recherche. Ils sont vos outils de même que des armes pour les Hackers

Opérateurs de base :

`+`, `-`, `~`, `,`, `.`, `*`, `""`, `&`, `OR`



Les opérateurs

Opérateurs avancées

<code>allintext: ,</code>	<code>allintitle:,</code>	<code>allinurl:,</code>	<code>bphonebo ok:,</code>	<code>cache:,</code>	<code>define:,</code>
<code>filetype:,</code>	<code>info:,</code>	<code>intext:,</code>	<code>intitle:,</code>	<code>inurl:,</code>	<code>link:,</code>
<code>phoneboo k:,</code>	<code>related:,</code>	<code>rphonebo ok:,</code>	<code>site:,</code>	<code>numrange :,</code>	<code>daterange</code>



Découvrir l'OSINT au niveau des réseaux sociaux



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction
Les RS dans le monde

Une formation
Alphorm.com



Introduction

Ressource en or

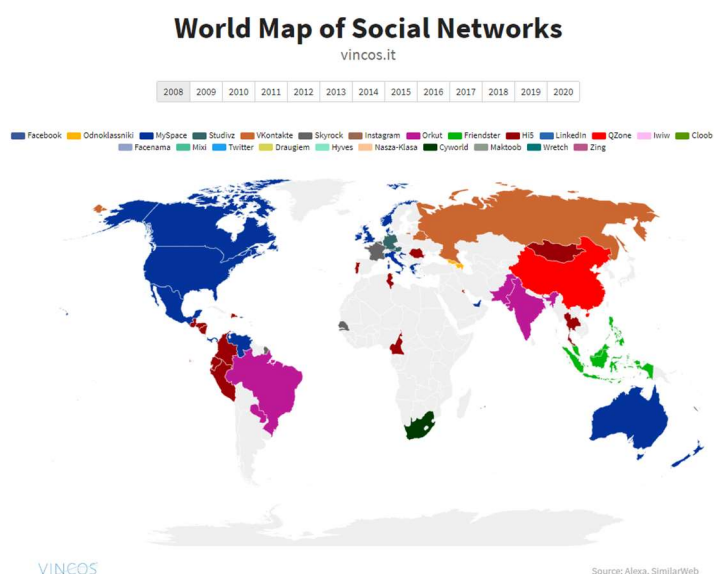
Faire attention à ce qui est exposé
sur vos RS

Chaque réseau social possède une
approche d'analyse spécifique

Une formation
Alphorm.com



Les RS dans le monde



Une formation
Alphorm.com



Une formation
Alphorm.com

Twitter



Une formation
Alphorm.com

Facebook



Maitriser l'analyse des leaks



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction

Plateformes de Leaks

Lab : Maitriser les Leaks

Une formation
Alphorm.com



Introduction

Fuite de données → Leaks

Public ou privé

Collection #1 à 05

Exploitation des données personnelles
dans un contexte de social engineering

Dictionnaire et ré-exploitation de
Credentials

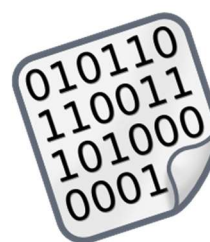
Une formation
Alphorm.com



Plateformes de Leaks

_X

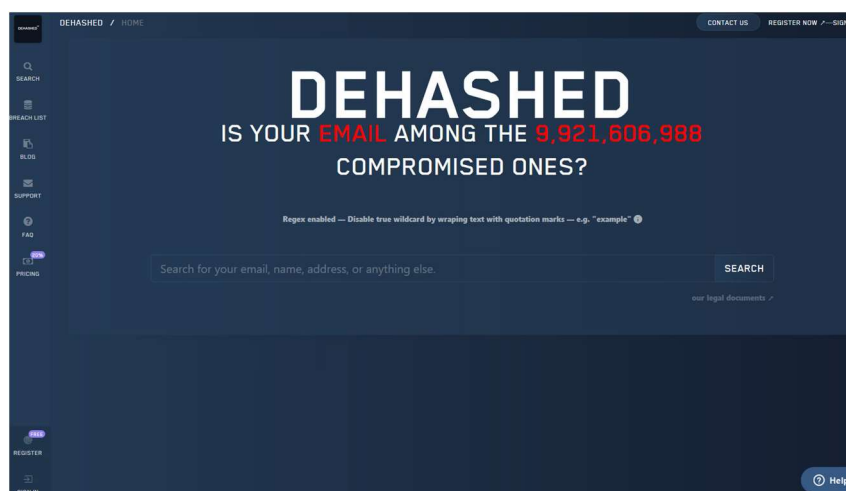
#



Une formation
Alphorm.com



Lab : Maitriser les Leaks



Une formation
Alphorm.com



Introduction la notion de Metadonnées

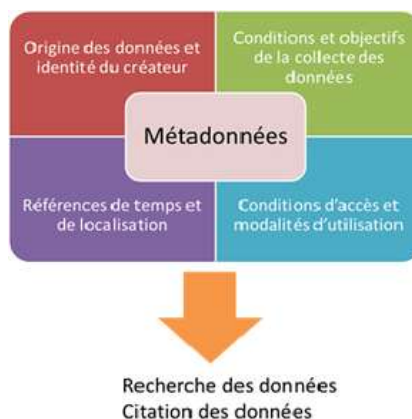


Hamza KONDAH

Une formation
Alphorm.com



Définition



Une formation
Alphorm.com



Maitriser le processus d'analyse des metadonnées



Hamza KONDAH

Une formation
Alphorm.com

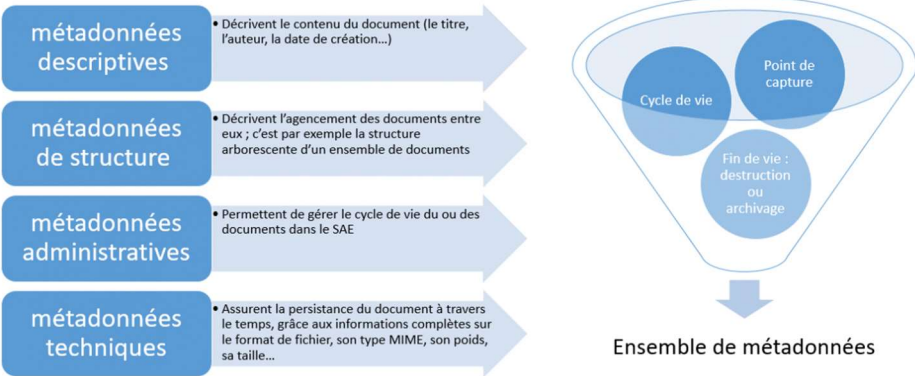


Plan

Types de métadonnées
Exit data



Types de métadonnées





Une formation
Alphorm.com

Exit data

Global Positioning System	
GPS Altitude	31.9 m
GPS Latitude	6deg 14' 7.620"
GPS Longitude	106deg 49' 30.210"
Image Information	
Date and Time	2018:08:24 15:47:27
Manufacturer	Apple
Model	iPhone 6s
Photograph Information	
Aperture	F2.2
Exposure Bias	0 EV
Exposure Mode	Auto
Exposure Program	Auto
Exposure Time	1/874 s
Flash	No, auto
FNumber	F2.2
Focal Length	4.2 mm
ISO Speed Ratings	25
Metering Mode	Multi-segment
Shutter speed	1/874 s
White Balance	Auto



Une formation
Alphorm.com

Exploiter les outils d 'analyse de métadonnées



Hamza KONDAH



Introduire le rôle du threat hunting dans l'OSINT



Hamza KONDAH

Une formation
Alphorm.com



Plan

Introduction et définition
Approche proactive VS Approche
réactive

Une formation
Alphorm.com



Une formation
Alphorm.com

Introduction et definition

Le Threat Hunting est l'art de recherche itérative dans le données (brut ou structurées) afin de pouvoir détecter des menaces (avancées principalement) qui passe entre les mailles du filet .



Une formation
Alphorm.com

Introduction et definition

Un contrastes avec les mesures de détection de menaces traditionnel

Firewalls

Systèmes de détection d'intrusion

Sandbox de détection de Malwares

SIEM (Intéressant ? Really ?)

Une mesure principalement suite à une alerte

Attention : Ce n'est pas de la réponse à incident



Approche proactive VS Approche réactive



Une formation
Alphorm.com



Découvrir le processus de threat hunting



Hamza KONDAH

Une formation
Alphorm.com



Plan

Objectifs

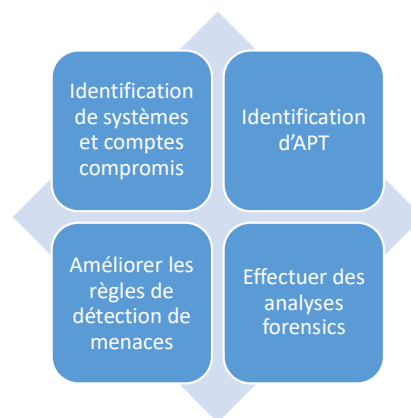
Processus

Méthodologie de threat hunting

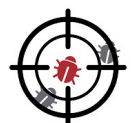
Une formation
Alphorm.com



Objectifs



Une formation
Alphorm.com





Processus

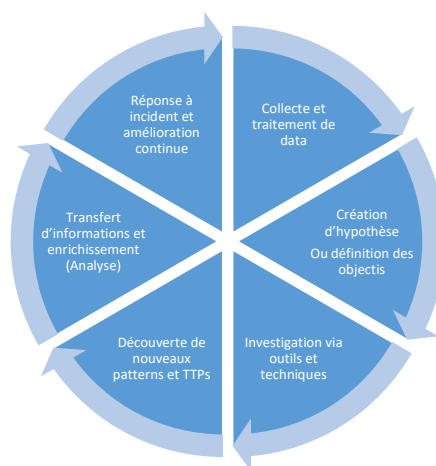
- Mitre Att&ck
- Réseau sociaux
- Conférences
- Blogs
- Rapports APT
- Exercices Red Teaming
- IR/DF
- Monitoring



Une formation
Alphorm.com



Méthodologie de threat Hunting



Une formation
Alphorm.com



Maitriser les outils à exploiter pour du threat hunting



Hamza KONDAH

Une formation
Alphorm.com



Découvrir les techniques de recherches inverse (image et vidéos)



Hamza KONDAH

Une formation
Alphorm.com



Découvrir les techniques d'identification de personnes dans les vidéos



Hamza KONDAH

Une formation
Alphorm.com



Maitriser l'analyse inverse des codes de tracking



Hamza KONDAH

Une formation
Alphorm.com



Maitriser l'OSINT dans la blockchain



Hamza KONDAH

Une formation
Alphorm.com



Apprendre l'Osint de comptes gmail



Hamza KONDAH

Une formation
Alphorm.com



Découvrir les techniques de recherche inverse de telephones



Hamza KONDAH

Une formation
Alphorm.com



Découvrir le tracking des réseaux sans fils



Hamza KONDAH

Une formation
Alphorm.com



Une formation
Alphorm.com

Conclusion et perspectives



Hamza KONDAH

AVERTISSEMENT

Ni le **formateur** Ni **Alphorm** ne sont responsables de la mauvaise utilisation du contenu de cette formation

L'utilisation des outils doit être réalisée uniquement au sein d'un environnement virtuel ou avec une autorisation préalable de l'entreprise



Bilan

1. Découvrir les techniques d'OSINT de reconnaissances passive
2. Maitriser les techniques de reconnaissance active
3. Maitriser les techniques d'OSINT
4. Maitriser les attaques réseaux
5. Découvrir les attaques sur les clients
6. Introduire les attaques AD
7. Découvrir les attaques physiques
8. Découvrir les attaques sur les web

Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com



Hacking et sécurité
2020

Méthodologies de Pentest,
Reconnaissance Passive et Active

Une formation
Alphorm.com





Hacking et sécurité
2020

Méthodologies de Pentest,
Reconnaissance Passive et Active

Une formation
Alphorm.com

Prochainement



PENTESTING
ACTIVE DIRECTORY