

COURS OSINT

26.01.2023



PROGRAMME

Description du Cours

Ce cours d'Open Source Intelligence (OSINT) fournira aux étudiants la capacité à rassembler des informations sur des personnes, des groupes ou des entreprises à partir de sources diverses. Il fournira une série de compétences allant de la préservation de l'anonymat à la création de fausses identités en ligne, en passant par la compréhension du besoin, la collecte, le traitement, la diffusion et la capitalisation de l'information. Les étudiants se verront présenter les méthodologies et les outils les plus utilisés en renseignement cyber de sources ouvertes, au travers de modules théoriques, techniques et d'ateliers pratiques.

OBJECTIFS DES ATELIERS

- Donner à l'étudiant les compétences nécessaires pour réaliser des techniques d'investigation tout en restant anonyme ;
- Permettre à l'étudiant de se familiariser avec des outils spécialisés et d'en comprendre les résultats ;
- Présenter des ressources en ligne peu connues ;
- Formaliser les résultats d'une investigation.

Admission

Semestre A2S1, A2S2

Pré-requis : Aucun

Règles de savoir vivre





















L'assiduité au cours est la base d'un apprentissage réussi.

Si vous ne pouvez pas assister au cours pour des raisons personnelles ou liées à votre alternance, il est de bon ton de prévenir à l'avance l'enseignant.

Un registre des présents sera tenu sur toute la durée du cours.

Compétences à acquérir en 2ème Année

 Table

Aa Code_compétence...	Description	Ref_RNCP_Competence	Ref_RNCP_Activite	Ref_RNCP_Block	Année	Syllabus
SEC-OSI_2_01	Employer des opérateurs de recherche avancés	 RNCP_CO13	 RNCP_AC04	 RNCP_BLK03	2	 OSINT
SEC-OSI_2_02	Concevoir une investigation numérique à base de source ouverte ciblant un acteur ou une organisation.	 RNCP_CO04	 RNCP_AC02	 RNCP_BLK01	2	 OSINT
SEC-OSI_2_03	Évaluer les différents outils en source ouverte à des fins d'investigations numériques.	 RNCP_CO07	 RNCP_AC03	 RNCP_BLK02	2	 OSINT
SEC-OSI_2_04	Formaliser les résultats d'une investigation	 RNCP_CO03	 RNCP_AC01	 RNCP_BLK01	2	 OSINT
SEC-OSI_2_05	Restituer oralement les résultats d'une investigation	 RNCP_CO03	 RNCP_AC01	 RNCP_BLK01	2	 OSINT

Agenda du cours

Table

Aa Intitulé	Type	Semestre	Promo	Date	Matière
OSINT n°1	Cours Magistral	A2S1	2024	23 janvier 2023 9:30-11:30	! OSINT
Exercices d'OSINT n°1	TP	A2S1	2024	23 janvier 2023 12:30-17:30	! OSINT
OSINT n°2	Cours Magistral	A2S1	2024	24 janvier 2023 9:30-11:30	! OSINT
Exercices d'OSINT n°2	TP	A2S1	2024	24 janvier 2023 12:30-17:30	! OSINT
OSINT n°3	Cours Magistral	A2S1	2024	25 janvier 2023 10:30-11:30	! OSINT
Exercices d'OSINT n°3	TP	A2S1	2024	25 janvier 2023 12:30-17:30	! OSINT
OSINT n 4	Cours Magistral	A2S1	2024	26 janvier 2023 9:30-11:30	! OSINT
Exercices d'OSINT n 4	TP	A2S1	2024	26 janvier 2023 12:30-17:30	! OSINT
OSINT Projet	Suivi	A2S2	2024	6 mars 2023 17:00-17:30	! OSINT
OSINT Devoir	Devoir	A2S2	2024	16 avril 2023 23:59	! OSINT
OSINT Soutenance 1	Soutenance	A2S2	2024	17 avril 2023 9:30-11:30	! OSINT
OSINT Soutenance 2	Soutenance	A2S2	2024	17 avril 2023 12:30-15:30	! OSINT



Évaluation

La session de cours de A2S1 sera évaluée par la réalisation de mini défis individuels. Les réponses seront transmises via un questionnaire interactif en ligne. Un temps imparti sera défini au début de chaque défi.

La session de cours de A2S2 sera évaluée par la réalisation d'un projet en groupe de 6-7 étudiants (même groupe que Forensic) donnant lieu au rendu d'un rapport et à une soutenance de projet 20 minutes (15 minutes de présentation, 5 minutes de questions).



Notation

Pondération

Mini défis (30%)

Rapport (40%)

Soutenance (30%)

Échelle de notation

0 Compétence non constatée

1 Compétence non acquise

2 Compétence en cours
d'acquisition

3 Compétence acquise

4 Maîtrise

5 Expertise

Correspondance sur 20

0 devoir non rendu

1 $1 \leq \text{note} < 7.5$

2 $7.5 \leq \text{note} < 11.5$

3 $11.5 \leq \text{note} < 13.5$

4 $13.5 \leq \text{note} < 20$

5 $\text{note} \geq 20$

Rendu des devoirs

Les mini défis de A2S1 seront à rendre sous la forme d'un questionnaire interactif en ligne.

Les rapports de A2S2 seront envoyés à l'adresse pierre.blondel.ext@ecole2600.com par le chef de projet de chaque groupe au plus tard le 16 avril 2022 à 23h59.

La soutenance se déroulera le 17 avril 2022 et fera l'objet d'une présentation.

Devoirs non rendus ou rendus en retard

Tout devoir non rendu se verra attribuer la note minimale (zéro).

Tout devoir rendu au-delà des délais impartis se verra sanctionné par une pénalité d'1 niveau dans l'échelle de notation avec pour minimal le niveau 1.

OBJECTIFS

DEFI 1, 2, 3, 4, 5, 6
(OSINT)

6# 34 (23h59)

5# 42 (23h57)

4# 40 (1h05)

DEFINITIONS

OSINT

COMMUNAUTE

MÉTHODOLOGIE

SECOPS

MACHINE VIRTUELLE

DISTRIBUTIONS

OSINT

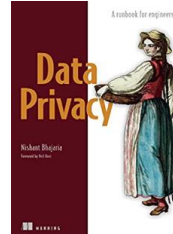
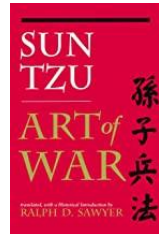
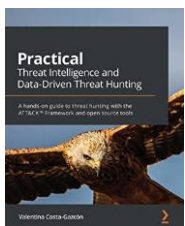
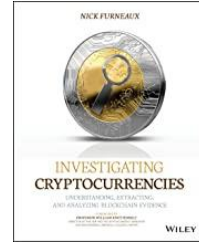
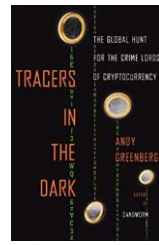
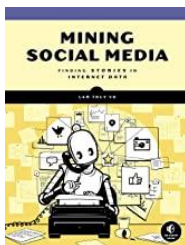
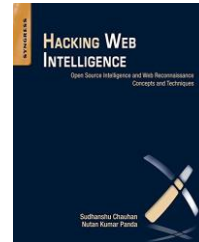
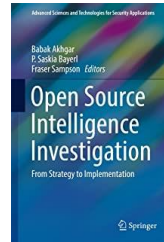
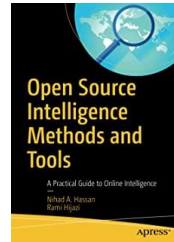
OUTILS

SOURCING

RAPPORT

POUR ALLER PLUS LOIN

LIVRES



PODCAST



BLOG

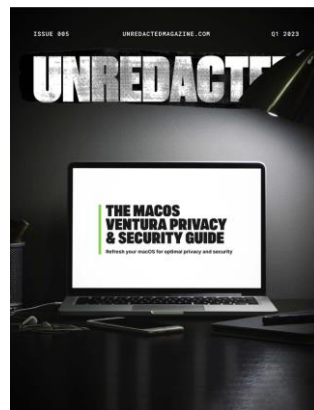
- sector035.nl/articles
- skopenow.com/news
- offensiveosint.io
- hatless1der.com
- osintme.com
- secjuice.com/tag/osint
- nixintel.info/category/osint
- webbreacher.com/category/osint
- blog.sociallinks.io/tag/osint
- socradar.io/category/osint
- espysys.com/osint-blog
- osinteditor.com
- osintcurio.us
- portswigger.net/daily-swig/osint
- maltego.com/categories/osint
- ...



Inoreader



MAGAZINE



CTF OSINT

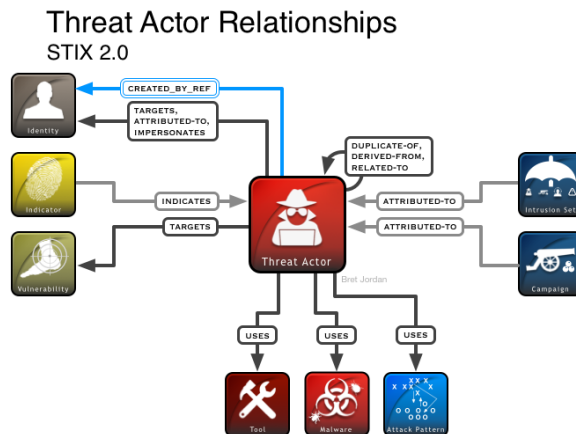
- **OSINT Games** : osint.games
- **OSINT Dojo CTF** : osintdojo.com
- **Cyber Training Force Académie** : ctfacademy.github.io/osint/index.htm
- **Spying Challenge** : spyingchallenge.com
- **OhSINT** : tryhackme.com
- **OSINT-CHALLENGE** : github.com/dataretriever/OSINT-CHALLENGE
- **Hexa OSINT** : discord.gg/tGVJEJ97kc
- **Search Party - Trace Labs** : tracelabs.org
- **NahamCon CTF OSINT Challenge** : twitter.com/NahamSec
- **Stranger Case CTF (OSINT)** : strangercase.fr
- **OZINT** : ozint.eu
- **Hacktoria CTF OSINT** : hacktoria.com
- **EC2 du FIC** : forum-fic.com

DEVOIR + SOUTENANCE

DEVOIR

Date de rendu du rapport : 16 avril 2023 avant 23h59

Rédaction d'un rapport d'investigation OSINT de maximum 15 pages en groupe, au sujet d'un acteur de la menace (Threat actor).



Liste des acteurs de la menace :

- [3/11] **Aurora Stealer** : blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar
- [3/11] **Eternity Stealer** : blog.sekoia.io/eternityteam-a-new-prominent-threat-group-on-underground-forums
- [5/11] **Killnet** : cybershafarat.com/category/all/russia/killnet/

DEVOIR

Exemples plan :

- Executive summary
- Historique du Threat actor
- Description générale de l'acteur ou du groupe
- Victimologie et motivations
- Compétences et expertises affichées
- Remarques de l'analyste
- Moyens de communication
- Fréquences de communication
- Analyse des heures de publications ou d'interactions
- Identification des pseudonymes associés
- Technologies utilisée
- Autres acteurs en lien avec le Threat actor
- Situer le Threat actor dans une campagne ou des campagnes d'attaques
- Evènements particuliers
- Analyse syntaxique
- Identification de sélecteurs (IP, NS, MX, domaines, adresse électronique, ID, numéro de téléphone, BTC, LTC, NFT, ...)
- Descriptions des outils et services utilisés pour l'identification des informations, ou la collecte et le traitement des données
- Business model
- Infrastructure
- ...

Ne pas oublier de sourcer l'intégralité des informations, des captures d'écran et des données présentent dans votre rapport.

DEVOIR

Exemples de sources à monitorer et analyser :

Source forums :

xss.is > xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion
exploit.in > exploitivzcm5dawzhe6c32bbylyggbjvh5dyvsyb5lkuz5ptmunkmqd.onion
github.com/fastfire/deepdarkCTI/blob/main/forum.md
ransomlook.io/markets

Sources Telegram :

ransomlook.io/telegrams
github.com/fastfire/deepdarkCTI/blob/main/telegram.md
telemetr.io/en/channels
tgstat.ru

SOUTENANCE

Date de la soutenance : le 17 AVRIL 2023

- Soutenance orale de 20 minutes par groupe de 6 à 7.
- Chaque groupe présentera le résultat de ses recherches durant 15 minutes +5 minutes de questions.
- Le groupe abordera sa méthodologie de recherche, ainsi que le résultat de ses recherches.
- La soutenance orale sera accompagnée d'un support numérique de présentation libre.
- La prise de parole peut se faire à plusieurs au sein d'un même groupe.

FORMAT DU RAPPORT



Type de rapport	
Source	CERT - OWN
Date de création	09/12/2022
Date de mise à jour	n/a
Reference	

OWN CERT TEAM

OWN-SECURITY
(SEKOA Services)

TIP: AMBER: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TIP: AMBER+DIRECT restricts sharing to the organization only. Recipients may use TIP: AMBER when information requires support to be effectively called upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TIP: AMBER.

PAP: AMBER: Recipients may use PAP: AMBER information for conducting online checks, like using services provided by third parties (e.g., VirusTotal), or set up a monitoring loopback.



- **Texte enrichi** (couleur de premier plan, couleur d'arrière-plan, gras, italique, souligné, barré, petit, h1, h2, h3, indice, exposant, espace fixe)
- **Coloration syntaxique** prenant en charge plusieurs langages de programmation
- **Gestion des images** : insertion dans le texte, édition (redimensionnement/rotation), enregistrement en fichier png
- **Gestion des fichiers embarqués** : insertion dans le texte, sauvegarde sur disque
- Gestion des listes multi-niveaux (à puces, numérotées, à faire et basculer entre elles, multilignes avec SHIFT+ENTER)
- **Gestion simple des tableaux** (cellules avec texte brut), couper/copier/coller une ligne, importer/exporter en tant que fichier csv
- **Gestion des hyperliens** associés à du texte et des images (liens vers des pages web)
- **Vérification orthographique** (avec pygtkspellcheck et pyenchant)
- **Imprimer et enregistrer** en fichier pdf / un nœud / des sous-nœuds / l'ensemble de l'arbre
- **Export en html** d'une sélection / nœud / sous-nœuds / toute l'arborescence
- **Export en texte brut** d'une sélection / nœud / sous-nœuds / toute l'arborescence
- **Génération de data structure** pour un nœud / sous-nœuds / l'arbre entier, basé sur h1, h2 et h3
- **Protection par mot de passe** via 7-zip

github.com/giuspen/cherrytree



File Edit Formatting Tree Search Replace View Bookmarks Import Export Help

Introduction

Cherrytree 0.33.3

Cherrytree is what's referred to as an "hierarchal" note taking application, meaning it's designed to store your entries in containers, which some programs call "notes" or "pages" and Cherrytree calls "nodes". If you envision the Cherrytree document as the root of a tree, and each "node" as a branch in that tree, sub-nodes as branches off that branch, you will start to get the idea. If you have ever used outlining programs like OmniNote, Kjots, Keepnote and others, then Cherrytree will feel very familiar. However, Cherrytree is not just about having a place to write notes and to-do items and keeping them organized, it's also a place you can store links, pictures, tables, even entire documents. It can be your one program for all the miscellaneous information you have and want to keep. All those little bits of information you have scattered around your hard drive can be conveniently placed into a Cherrytree document where you can easily find it.

Just having a place to put notes and bits of information would not be much help if you had to go through a lot of trouble finding a particular piece of it. This is where Cherrytree really excels. It's powerful search functions help you easily and quickly find anything you have put in it. If you can do no more than remember one word of what you're looking for, Cherrytree can find it, fast. As you become more familiar with some of Cherrytree's advanced functions, you will also be able to link related information and make better use of it.

So go ahead, give Cherrytree a try. In the next few pages we'll go over how to get started with some of the basic uses. People already familiar with outlining software may want to jump ahead to the more advanced features. However you start, we believe you're going to love Cherrytree!

Explore! Have fun!

next- [About this Manual](#)

Node Type: Rich Text



CherryTree

File Edit Formatting Tree Search Replace View Bookmarks Import Export Help

COFFEE
SACME
VILLA
GIEMME
ATM
network
pc server
samba
remote export xorg
asterisk
default
django 1.3
admin
views
views-templates
views-urls
views-forms
apache
remote authentication
hg

views

```
urlpatterns = patterns('',
    ...url(r'^polls/$',, 'polls.views.index'),
    ...url(r'^polls/(?P<poll_id>\d+)/$',, 'polls.views.detail'),
    ...url(r'^polls/(?P<poll_id>\d+)/results/$',, 'polls.views.results'),
    ...url(r'^polls/(?P<poll_id>\d+)/vote/$',, 'polls.views.vote'),
    ...url(r'^admin/',, include(admin.site.urls)),
)
#
# let's write the code for the views
nano polls/views.py
#
from django.http import HttpResponse

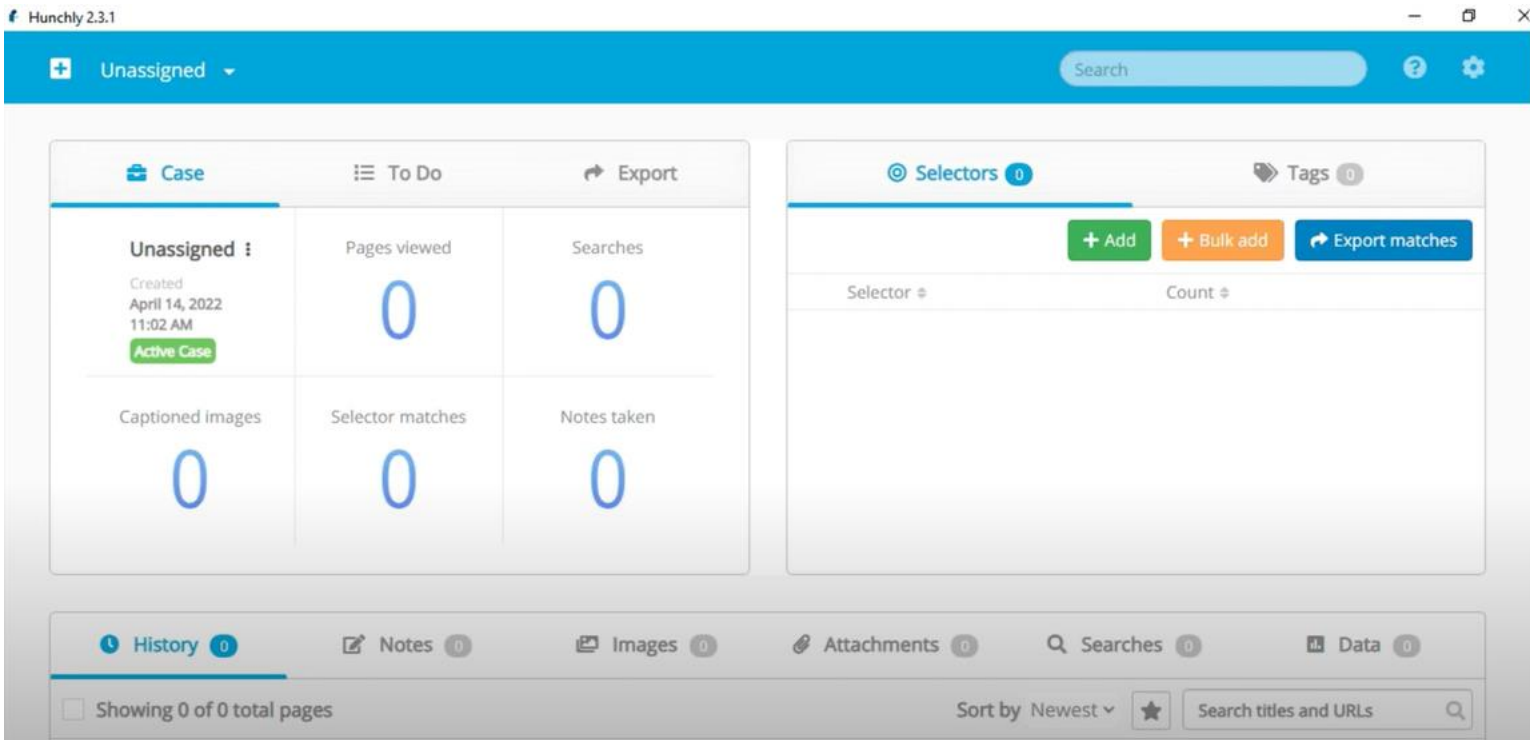
def index(request):
    ...return HttpResponse("Hello, world..You're at the poll index.")

def detail(request, poll_id):
    ...return HttpResponse("You're looking at poll.%s." % poll_id)

def results(request, poll_id):
    ...return HttpResponse("You're looking at the results of poll.%s." % poll_id)

def vote(request, poll_id):
    ...return HttpResponse("You're voting on poll.%s." % poll_id)
```

Node Type: python



Source : hunch.ly



Hunchly 2.3.1

Created
April 14, 2022
12:03 PM

Active Case

17

2

Captioned images

0

Selector matches

14

Notes taken

0

Tag

Tagged Pages

Social Media

1

Imagery of Weapons

0

History 17

Notes 0

Images 0

Attachments 0

Searches 2

Data 80

☐ Showing 17 of 17 total pages

Sort by Newest



Search titles and URLs



Justin Seitz (@jms_dot_py) / Twitter

https://twitter.com/jms_dot_py?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

April 14, 2022 12:25 PM

Justin Seitz, jms_dot_py

Social Media



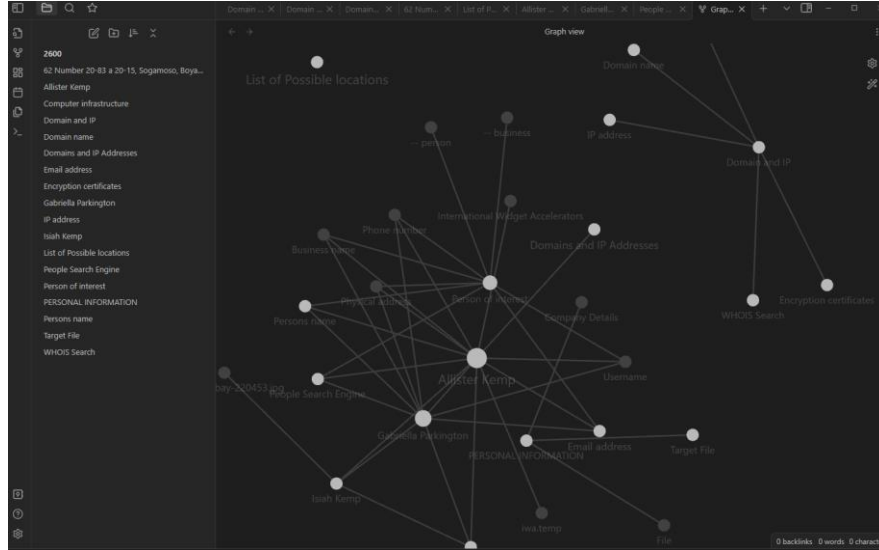
justin seitz - Google Search

https://www.google.com/search?q=justin+seitz&source=hp&ei=zFdYYr2BLeGu0PEpm8Oy0Ac&ifsig=AHkkrS4AAAAAYIH3EoSj0lpzQtP_oU61YEnlrkGKypH&ved=0ahUKEwi9I9...

www.hunch.ly



- Editeur de texte en Markdown.
- Application de base de connaissances
- Stocker vos propres fichiers sur votre ordinateur.
- Le cerveau humain n'est pas linéaire
- Toutes les informations sont stockées dans un répertoire au format Markdown
- disponible MacOs, Windows, Linux mais aussi pour les smartphones via l'App Store (IOS) ou le Play Store (Android)



Source : obsidian.md



td-architecture - Obsidian v0.12.12

Graph view

The graph view displays a complex network of nodes and edges. Nodes are represented by small circles in various colors (blue, white, orange, red) and are connected by thin lines. The background is dark with a subtle pattern of small blue dots.

td-architecture

- Architecture
- Capability-Groups
- Cloud-Management
- FAQ
- Icons
- Models
 - Archi User Guide
- Architecture-Models
- Obsidian-Settings
- OS-Values
- Partners
- Patterns
- Principles-Policies-and-Standards
- References
- Scripts
- Systems-and-Services
- Technology
- Templates
- Architecture
- Capability-Groups
- Cloud-Management
- FAQ
- Hello-World

Architecture-Models

Archi

The Open Group Modeling tool used to create Models in Architecture is called Archi and is available to download from the OS App Portal which is [here](https://osappportal.esd/items/Details?PackageId=2258)(<https://osappportal.esd/items/Details?PackageId=2258>).

****Please Note:**** *_You will need to connect to the VPN to gain access to the OS App Portal_*

coArchi Plug in

Installation of the coArchi Plug in ****is required**** to allow Archi access to Git compatible change control, ie the T&D Repository where our models are stored, allowing for multi-user collaboration on these models.

Aug 2021 < TODAY >

MON	TUE	WED	THU	FRI	SAT	SUN
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Type to start search...

1 backlink 480 words 3638 characters

MERCI POUR VOTRE ATTENTION