



Christopher THIEFFIN (Processus) INGÉNIEUR SÉCURITÉ

CONTACT

christopher@thieffin.fr

SITE WEB

<https://processus.site>

GITHUB

<https://github.com/ProcessusT>

YOUTUBE

Création d'une chaîne YouTube orientée Cybersécurité en Avril 2015 qui cumule aujourd'hui plus de 55 000 abonnés

CONFERENCES

Décembre 2024 : Conférence de niveau Avancé sur la détection d'une opération Red team à la convention DFIR 212 à Rabat (Maroc)

Juillet 2024 : Conférence de niveau Avancé sur le contournement des Antivirus et des EDR à la nuit du hack (LeHack)

Juillet 2023 : Conférence de niveau Expérimenté sur le contournement des Antivirus et des EDR à la nuit du hack (LeHack)

Mars 2023 : Conférence sur la Data Protection API (HackSécuReims)

CONTRIBUTIONS

Mai 2023 : Participation au podcast de Les Numériques en live pour la journée mondiale du mot de passe

Septembre 2022 : Contribution au projet Pypykatz (clone de Mimikatz en python) pour l'ajout du déchiffrement des masterkey avec la clé privée du contrôleur de domaine dans le module DPAPI

PARCOURS PROFESSIONNEL

[CONFIDENTIEL] – Ingénieur sécurité

Avril 2024 – Actuellement en poste

Tests d'intrusion et missions Red team :

- Intrusion physique réussie dans un aéroport français
- Obtention d'accès initiaux via ingénierie sociale par téléphone

Mise en place et maintien des outils du SOC :

- EDRs HarfangLab et Defender for Endpoints
- SIEM Sekoia

[CONFIDENTIEL] – Analyste SOC

Juillet 2022 – Février 2024

Surveillance et maintien des outils du SOC interne et de ses clients managés

ESGI – Enseignant vacataire (Bachelor et Master)

Juin 2022 – Actuellement en poste

Intrusion Red team / Sécurité offensive / Analyse de malwares / Analyse forensique / Gestion des exploits / Audit des applications Android

DISTINCTIONS HONORIFIQUES

Obtention du titre Microsoft® Security Most Valuable Professional (MVP)

Décembre 2022

Titre récompensant les experts en sécurité qui partagent bénévolement leur savoir avec la communauté



CERTIFICATIONS

OffSec Experienced Penetration Tester (OSEP)

Février 2025

Exécution de code côté client (VBA, JScript), évasion antivirus avancée, pivoting et post-exploitation Linux & Windows

Certified Azure Red Team Professional (CARTP)

Janvier 2025

Compromission d'une infrastructure Entra ID
Contournement de protection Conditional Access

Azure Cloud Security Specialist

Novembre 2024

Audit de sécurité d'une infrastructure Entra ID
Techniques de détection et approche défensive

Red Team Operator (RTO I) + Red Team Lead (RTO II)

Septembre 2023 et Octobre 2024

Exploitation Active directory avancée (Applocker, CLM, ADCS)
Création d'une infrastructure C2 sécurisée, mise en place de redirecteurs et contournement d'antivirus et EDR
Expertise de Cobalt Strike

Certified Ethical Hacker (CEH)

Juillet 2023

Connaissance de l'évaluation de la sécurité des systèmes informatiques

Practical Network Penetration Tester (PNPT)

Juin 2023

Pentest réel en environnement Active Directory
Remise d'un rapport et débrief oral en anglais devant un jury

Offensive Security Certified Professional (OSCP)

Avril 2023

Exploitation de vulnérabilités / Maîtrise de Kali Linux
Remise d'un rapport de pentest

Certified Red Team Professional + Expert (CRTP + CRTE)

Août 2022

Pentest réel en environnement Active Directory et évasion d'antivirus
Fourniture d'un rapport détaillé avec remédiations