Christopher THIEFIN (Processus)

Ingénieur Sécurité Offensive / Red Team

• Reims (51) • christopher@thiefin.fr • https://github.com/ProcessusT

▼ CONFERENCES

Mars 2026 : Conférence de niveau Avancé sur le **contournement d'EDR à l'aide d'outils d'analyse forensique** lors du HackDay organisé par l'ESIEE de Paris

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)

▼ CERTIFICATIONS

Sécurité offensive / Red Team

- OSCP + OSEP
- RTO I/II
- CRTP/CRTE
- PNPT
- C-ADPenX
- CEH

Expertise en compromission Active Directory, contournement EDR/AV, opérations Red Team complètes

Sécurité Cloud

- CARTP
- Azure Security Specialist

Attaques et audit d'environnements Entra ID (Azure AD), contournement des protections Conditional Access

Gouvernance & Gestion des risques

- ISO 27001 Lead Implementor

Mise en place et pilotage d'un SMSI, analyse et mise en place de traitements de risques (ISO 27005)

▼ RECONNAISSANCE & CONTRIBUTIONS

Depuis Décembre 2022 :

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

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

Depuis Avril 2015 :

Création d'une **chaîne YouTube orientée Cybersécurité** qui cumule aujourd'hui plus de 55 000 abonnés :

https://www.youtube.com/c/processusthief

Depuis Septembre 2022 :

Développement d'un outil d'exploitation du gestionnaire d'identifiants de Windows pour déchiffrer les masterkeys et les blobs à l'aide de la clé privée du domaine Active Directory (via DPAPI)

+500 stars sur GitHub

▼ EXPERIENCES

[CONFIDENTIEL] – Ingénieur sécurité
Avril 2024 – Actuellement en poste
Tests d'intrusion et missions Red team :

- Intrusion physique réussie dans un aéroport français
- Ingénierie sociale, contournement EDR et d'antivirus

[CONFIDENTIEL] – Analyste SOC
Juillet 2022 – Février 2024
Surveillance et maintien des outils du SOC interne et de ses clients managés

[CONFIDENTIEL] – Administrateur systèmes et réseaux
Novembre 2015 – Juin 2022
MEP et MCO Systèmes (Active Directory, Exchange) et Réseaux (Accès VPN, NAT) des clients

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