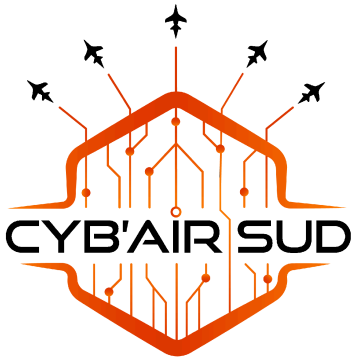


Reverse Engineering of an Attack: Evidence, Limits, and Priority Actions for Public Institutions

CFP 2025 — English Version

Speaker: Thomas Schaal – Cybersecurity Expert, OCI Informatique et Digital

Classification and dissemination

TLP: **GREEN**.

Presentation language: **French**. Recording and redistribution: **Allowed**.

Title

Reverse Engineering of an Attack: Evidence, Limits, and Priority Actions for Public Institutions

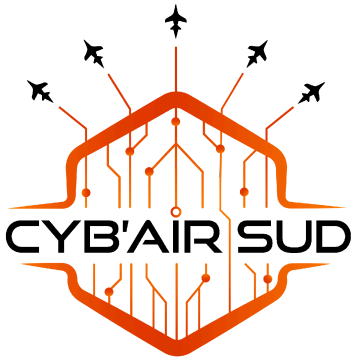
Short Description

Without properly collected and preserved evidence, reverse engineering becomes an illusion. This talk focuses on concrete levers — forensic readiness, judicial procedures, and inter-service cooperation — to obtain valid and usable analyses.

Abstract

This session provides a deep dive into the reverse engineering of an attack experienced by a public institution. Beyond technical aspects, it explores the crucial question of digital evidence: how to collect it, protect it, and make it legally exploitable.

Through concrete cases, essential levers for forensic readiness, best practices for inter-service cooperation, and priority actions will be presented, showing how to transform an attack into a source of learning and resilience.



Reverse engineering d'une attaque : preuves, limites et actions prioritaires pour les institutions publiques

CFP 2025 — Version Française

Intervenant : Thomas Schaal – Expert Cybersécurité, OCI Informatique et Digital

Classification et diffusion

TLP : **VERTE**.
Langue de présentation : **Français**.
Enregistrement et rediffusion : **Autorisés**.

Titre de la conférence

Reverse engineering d'une attaque : preuves, limites et actions prioritaires pour les institutions publiques

Description courte

Sans preuves collectées et protégées, le reverse engineering devient une illusion. Focus sur les leviers concrets — forensic readiness, procédures judiciaires et coopération inter-services — pour obtenir des analyses valides et utilisables.

Résumé

Cette intervention propose une plongée au cœur du reverse engineering d'une attaque vécue par une institution publique. Au-delà de la technique, elle explore la question cruciale des preuves numériques : comment les collecter, les protéger et les rendre exploitables juridiquement ?

À travers des cas concrets, seront présentés les leviers essentiels de la forensic readiness, les bonnes pratiques de coopération inter-services et les actions prioritaires à mettre en œuvre pour transformer une attaque en source d'apprentissage et de résilience.