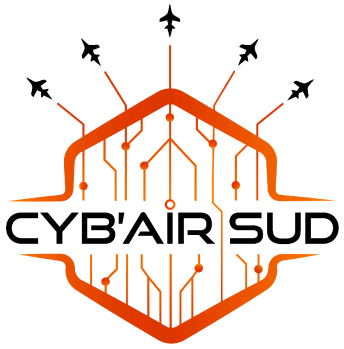


From SOC to CERT: What Malware Reverse Engineering Really Brings

CFP 2025 Summary

Speaker: Hugo RIFFLET

Short description

From SOC to CERT, malware reverse engineering is a key lever to qualify, understand, and respond to threats. This talk shares field feedback, statistics, and best practices to know when and how to apply it effectively.

Detailed abstract

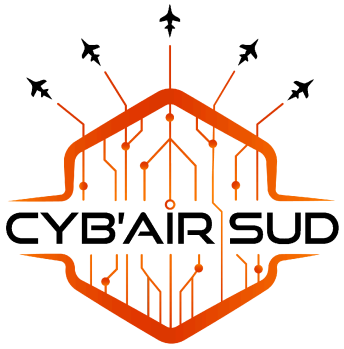
Not every detection becomes a confirmed intrusion, but some require deeper analysis to properly qualify the threat. Malware reverse engineering is then an essential tool for SOC and CERT teams to understand malicious behavior, measure impact, and guide response.

In this presentation, we will share the experience of Orange Cyberdefense's CERT: statistics from dozens of cases handled each year, concrete investigation examples, and best practices to know when to go deeper, how to train and equip teams, and when to outsource.

The goal: to help participants build a pragmatic and realistic approach to malware analysis, adapted to operational needs.

Additional information

— Presentation language: French
— TLP classification: GREEN
— Recording and broadcast agreement: Yes



Du SOC au CERT : ce que le reverse engineering de malwares apporte vraiment

Résumé pour CFP 2025

Intervenant : Hugo RIFFLET

Description concise

Du SOC au CERT, le reverse engineering de malwares est un levier clé pour qualifier, comprendre et répondre aux menaces. Ce talk partage retours de terrain, statistiques et bonnes pratiques pour savoir quand et comment l'appliquer efficacement.

Résumé détaillé

Chaque détection ne se transforme pas en intrusion confirmée, mais certaines nécessitent d'aller plus loin dans l'analyse pour qualifier la menace. Le reverse engineering de malwares est alors un outil essentiel pour les équipes SOC et CERT afin de comprendre le comportement malveillant, mesurer l'impact et guider la réponse.

Dans cette présentation, nous partagerons l'expérience du CERT d'Orange Cyberdefense : statistiques issues de dizaines de cas traités chaque année, exemples concrets d'investigation, et bonnes pratiques pour savoir quand approfondir l'analyse, comment former et outiller ses équipes, et quand externaliser.

L'objectif : aider les participants à bâtir une approche pragmatique et réaliste de l'analyse de malwares, adaptée aux besoins opérationnels.

Informations complémentaires

— Langue de présentation souhaitée : français
— Classification TLP : GREEN
— Accord concernant l'enregistrement et la rediffusion : oui