

OPSEC Guide

Operational Security for Civilians and Red Teams

CORE PRINCIPLES

01 Introduction

Defining OPSEC and its importance in modern security operations

02 Communication Security

Securing messaging, email, and metadata to prevent leaks

03 Device Security

Hardening mobile, desktop, and virtual machines against compromise

04 Online Identity & Personas

Managing operational identities and separating personal footprints

PRACTICE & APPLICATION

05 Case Studies

Successes and failures in real-world OPSEC operations

06 Practical Exercises

Hands-on challenges for civilians and red team operators

07 Red Team OPSEC Guide

Step-by-step methodology for professional offensive security teams

08 OSINT & Counter-OSINT

Using open-source intelligence for defense and adversary simulation

RESOURCES

09 Additional Resources

Checklists, templates, case studies, and tools for OPSEC practice

10 Conclusion

Key takeaways and the evolving nature of OPSEC