Cicada Cyber Intel Division – White Paper

Specialized Division of Cicada 3301 Corporations

By Dr. Sibusiso Kanny Siboza (aka Mercurius Ozeus)
Red Team Operative | OSCP-Certified | Bug Bounty Analyst | Cyber Defense Strategist

---

Mission

To develop and deploy defensive AI-driven cybersecurity solutions that protect individuals, organizations, and governments using ethical hacking, OSCP standards, and intelligent protocol engineering.

Core Focus Areas

Hybrid Cryptography Research

- Development of advanced cryptographic systems
- Reverse engineering of cipher systems
- Blockchain and zero-knowledge proof integrations

Deep Penetration Intelligence

- Legal penetration testing for government and private networks
- Reverse shell scripting and intrusion response
- Offensive testing with OSCP standards

Malware & Data Analysis

- Analysis and neutralization of real-world malware
- Behavioral analysis of ransomware, spyware, and worms
- Recovery from APT (Advanced Persistent Threats)

Defensive AI Security Systems

- IDS/IPS integrated with AI learning
- Scripting defenses in Python, Ruby, and C++
- Kernel and OS hardening for Kali, Parrot, and Red Hat Linux

OSCP-Level Training & Tools

- Field-tested tools from real penetration tests

- Support for Red Team, Blue Team, and hybrid tactics
- Community cybersecurity training and certification path

Development Philosophy

All technology is coded in-house and informed by public reference for educational research only. Inspiration sources include:

- Getting Started Becoming a Master Hacker.pdf
- Every Protocol Explained – Privacy Matters.mp4
- Mastering Metasploit & Hping3 – Shadow Pentest Series

> “We no longer just trace the attack – we pre-design its failure.”
> – Dr. Sibusiso Kanny Siboza

Contact

- GitHub: Cicada-3301-Corporations
- Email: cicada3301corp@proton.me