HILASSOUN A. ROLAND SANOU

Cybersecurity R&D Engineer — Endpoint Detection & Response | Threat Analysis | ML-based Security
Mersin, Turkey · +90 536 992 12 17 · rolandS01@outlook.fr
linkedin.com/in/hilassoun-a-roland-sanou · github.com/rolandsanou

PROFESSIONAL SUMMARY

Cybersecurity R&D Engineer with 3+ years of experience at C-Prot, Turkey's leading endpoint security company serving 5M+ users worldwide. Expert in developing ML-powered and heuristic-based threat detection and remediation systems for EDR and mobile security platforms. Currently building Windows EDR solutions with 99% detection accuracy for banking, energy, and defense sector clients. Pursuing an M.Sc. in Artificial Intelligence to deepen expertise in adversarial ML and next-generation threat intelligence.

PROFESSIONAL EXPERIENCE

R&D Engineer — EDR & Windows Endpoint Security

C-Prot Siber Guvenlik Teknolojileri A.S. · Mersin, Turkey · *January 2025 — Present*

- Design and develop Endpoint Detection and Response (EDR) solutions for Windows platforms, integrating ML-based and heuristic detection engines to identify advanced persistent threats (APTs), ransomware, and zero-day exploits.
- Architect real-time threat detection pipelines achieving 99% detection accuracy across malware families, significantly reducing false positive rates for enterprise clients in banking and energy sectors.
- Build automated remediation workflows that quarantine, rollback, and neutralize threats with minimal user disruption, reducing incident response time.
- Collaborate within a 10-engineer R&D team to deliver security solutions deployed to 5M+ users globally (enterprise and individual).
- Conduct threat intelligence research on emerging Windows attack vectors including fileless malware, living-off-the-land binaries (LOLBins), and process injection techniques.
- Develop YARA rules and behavioral signatures for proactive threat hunting and static/dynamic analysis pipelines.

R&D Engineer — Android Security & Threat Research

C-Prot Siber Guvenlik Teknolojileri A.S. · Mersin, Turkey · *September 2024 — January 2025*

- Researched and classified diverse attack types targeting Android devices, including phishing, malware injection, permission abuse, and overlay attacks.
- Designed and trained ML models (classification, anomaly detection) to detect phishing URLs and malicious APKs with high precision, integrated into C-Prot's mobile security product.
- Developed heuristic detection methods combining behavioral analysis and static code inspection to identify previously unseen threats.
- Built proof-of-concept exploits for Android attack surfaces to validate detection capabilities and improve coverage.
- Authored technical documentation on threat research findings and model performance benchmarks for the R&D team.

Intern Engineer — Android Development

C-Prot Siber Guvenlik Teknolojileri A.S. · Mersin, Turkey · *February 2023 — August 2024*

- Contributed to the development and maintenance of C-Prot's Android antivirus and mobile security application.
- Implemented security features including real-time scanning, threat alerts, and malware quarantine functionalities.
- Participated in code reviews, sprint planning, and agile development processes within the mobile team.
- Optimized application performance and battery consumption while maintaining comprehensive threat coverage.

TECHNICAL SKILLS

Area	Technologies
Security Tools	Wireshark, Metasploit, Burp Suite, YARA, IDA Pro, Ghidra, Frida, SIEM (Splunk, ELK), Nmap, OWASP ZAP
EDR / Endpoint	Threat detection engines, behavioral analysis, static and dynamic analysis, sandboxing, incident response, threat hunting
ML for Security	scikit-learn, TensorFlow, PyTorch, anomaly detection, malware classification, NLP for phishing detection
Programming Languages	Python, C/C++, Java, Kotlin, C#, Bash, SQL, Go, JavaScript
Platforms	Windows (kernel-level debugging, PE analysis), Linux, Android (AOSP, APK reverse engineering)
Cloud / DevOps	AWS, GCP, Azure, Docker, Kubernetes, CI/CD (Jenkins, GitHub Actions), Git
Reverse Engineering	PE file analysis, disassembly (IDA Pro, Ghidra), dynamic instrumentation (Frida), Android APK decompilation
Networking	TCP/IP, DNS, HTTP/TLS analysis, packet capture, firewall rules, VPN, network forensics

EDUCATION

M.Sc. Computer Science — Artificial Intelligence

Mersin University, Mersin, Turkey · *2025 — 2027 (in progress)*

Research: adversarial machine learning, AI-driven threat detection, LLM applications in cybersecurity.

B.Eng. Computer Engineering

Mersin University, Mersin, Turkey · *2020 — 2024*

CERTIFICATIONS

- Penetration Testing — Coursera (Certified)
- Machine Learning Specialization — Coursera (Certified)

NOTABLE PROJECTS

ML-Powered Phishing and Malware Detection Engine — C-Prot R&D

Designed classification models to detect phishing URLs and malicious Android APKs, achieving 99% accuracy. Integrated into a production mobile security product serving millions of users.

Windows EDR Threat Detection and Remediation Pipeline — C-Prot R&D

Built a real-time detection engine combining ML models and heuristic rules for ransomware, fileless malware, and APTs on Windows endpoints. Deployed to enterprise clients in banking and energy sectors.

Emotion Detection Mobile App

Developed a deep learning model for facial emotion recognition deployed on Android using a CNN architecture with TensorFlow Lite for on-device inference.

Solar Panel Cleaning Robot Controller

Built an Android application for real-time remote control of an industrial solar panel cleaning robot via Bluetooth/WiFi, including a telemetry dashboard and automated cleaning schedules.

LANGUAGES

French: Native · **Dioula**: Native · **English**: C1 (Advanced) · **Turkish**: Fluent

INTERESTS

CTF competitions, threat intelligence research, open-source security tools, AI/ML applied to cybersecurity, IoT security.