تجربه در زمینه تحلیل بدافزار، بدافزارنویسی و جرم‌یابی دیجیتال

دارای تجربه تخصصی در **تحلیل بدافزار (Malware Analysis)**، **توسعه نمونه‌های آزمایشگاهی بدافزار (Malware Development)** و **جرم‌یابی دیجیتال (Digital Forensics)** با هدف شناسایی تهدیدات، ارزیابی امنیت سامانه‌ها و افزایش سطح دفاع سایبری.

در حوزه تحلیل بدافزار، توانایی بررسی رفتار فایل‌های مخرب به روش‌های استاتیک و داینامیک، مهندسی معکوس، استخراج شاخص‌های نفوذ (IOC)، تحلیل ترافیک شبکه و شناسایی تکنیک‌های فرار از شناسایی را دارم. همچنین در محیط‌های آزمایشگاهی کنترل‌شده، نمونه‌های تحقیقاتی و Proof of Concept (PoC) را برای شبیه‌سازی تهدیدات و ارزیابی اثربخشی راهکارهای امنیتی توسعه می‌دهم.

در زمینه جرم‌یابی دیجیتال، تجربه تحلیل حافظه (Memory Forensics)، بررسی هارددیسک و سیستم فایل، بازیابی و تحلیل شواهد دیجیتال، تحلیل لاگ‌ها، بررسی رخدادهای امنیتی و تهیه گزارش‌های فنی و مستند مطابق اصول تحقیقات دیجیتال را دارم.

تسلط به ابزارهایی مانند **IDA Pro**، **Ghidra**، **x64dbg**، **Wireshark**، **YARA**، **Volatility**، **Autopsy**، **Procmon**، **Process Explorer**، **dnSpy** و همچنین برنامه‌نویسی با **C**، **C/C++**، **Python**، **C#** و **Windows API** از توانمندی‌های فنی من است.

تمرکز اصلی فعالیت‌های من بر **تحقیق و توسعه امنیت سایبری، تحلیل بدافزار، جرم‌یابی دیجیتال، تست نفوذ، شبیه‌سازی حملات و توسعه ابزارهای دفاعی** با هدف افزایش امنیت سازمان‌ها و کاهش ریسک‌های سایبری است.