Andrey Pautov

Email · Tel Aviv, Israel
linkedin.com/in/andrey-pautov · github.com/anpa1200

May 2026

Dear Hiring Manager,

Most organizations treat threat intelligence as a reporting function — analysts produce reports, and somewhere downstream, detections may or may not get written. I built my career around closing that gap. As Threat Intelligence Research Engineer at XPLG, I translate adversary behavior into validated detection content for enterprise SIEM and XDR platforms — building end-to-end production cases from theoretical threat definition through lab validation to customer-ready Sigma rules and hunting hypotheses.

What sets my profile apart is the source of my offensive depth. Before moving into cybersecurity, I served 7 years as an operator and fighter-paramedic in a Special Reconnaissance and AntiTerror Unit under the Israel Ministry of Public Security. That experience — operational security, adversary behavior, high-stakes decision-making under pressure — informs how I approach threat actor profiling in ways that training alone cannot replicate. At the Israel Police Cyber Defence Unit, I led red-team operations against national law-enforcement infrastructure and converted offensive findings directly into SOC-ready defensive intelligence: detection hypotheses, coverage gap analysis, and incident response runbooks.

My technical work reflects the same rigor. I maintain a 177-article local archive on CTI tradecraft, detection engineering, malware analysis, and cloud security, and maintain 8 practitioner field guides including the CTI Analyst Field Manual — a structured reference covering attribution methodology, infrastructure pivoting, confidence tiering, and detection backlog management. My open-source tooling includes AIDebug (malware reverse engineering walker with Capstone, FLIRT, CFG, Frida, and INetSim) and stratus-ai (cloud attack simulation platform for AWS and GCP). This body of work is designed to enable analysts to operationalize intelligence faster, reduce detection gaps tied to real adversary TTPs, and build sustainable coverage rather than one-off alerts.

If your team needs someone who can bridge the gap between raw threat intelligence and production detection capability — and has done it under real operational pressure — I would welcome the opportunity to discuss how I can contribute.

Sincerely,

Andrey Pautov