Andrey Pautov

CTI-to-detection practitioner. Threat Intelligence Research Engineer. AI security tooling builder.

Tel Aviv, Israel · Email · 1200km.com · linkedin.com/in/andrey-pautov · github.com/anpa1200 · medium.com/@1200km

PROFESSIONAL SUMMARY

CTI-to-detection analyst across government cyber defence (Israel Police Cyber Defence Unit) and commercial security engineering (XPLG). Profiles adversary infrastructure, reconstructs kill chains, maps TTPs to ATT&CK-aligned detection candidates, and builds AI-assisted tooling for IOC investigation, OpenCTI/MISP/STIX workflows, log/PCAP triage, and analyst-ready reporting.

Strong offensive security background grounded in real operational environments — 7 years in a special reconnaissance unit (Israel Ministry of Public Security, 2016–2023) and 2 years leading red-team operations against national law-enforcement infrastructure. Offensive experience directly informs detection engineering depth: adversary behavior understood from the inside out.

Maintains a 172-post exported Medium archive, 8 Docusaurus field guides, and a public AdversaryGraph (v6.0.0) documentation ecosystem covering CTI tradecraft, detection engineering, malware analysis, AI-assisted IOC investigation, OpenCTI integration, and cloud security — all collected at 1200km.com. External validation: 8 upstream contributions accepted across open-source security projects, 31 more under maintainer review; three analyst tools assigned to the Kali Linux 2026.2 milestone by the Kali maintainer.

PROFESSIONAL EXPERIENCE

Threat Intelligence Research Engineer

May 2025 – Present

XPLG — Enterprise Security Data Platform · Tel Aviv, Israel

- Maps adversary TTPs (Iran-nexus campaigns, hacktivist clusters, cloud-native threats) to XPLG platform telemetry fields; produces log-based detection use cases covering endpoint, network, cloud audit log, and IOC-enrichment sources.
- Translates CTI assessments into Sigma/YARA-compatible detection content, hunting hypotheses, ATT&CK coverage logic, and analyst-ready investigation guides scoped to enterprise SIEM and XDR deployment contexts.
- Builds and documents CTI enrichment workflows covering parser field mapping, anomaly detection logic, and structured threat reporting pipelines for security operations teams.

Head of Red Team — Cyber Defence Unit

Jul 2023 – May 2025

Israel Police — יחידת הגנת הסייבר · Jerusalem, On-site

- Directed red-team assessments against national law-enforcement infrastructure: reconnaissance, vulnerability chaining, privilege escalation, lateral movement, and attack-path validation in sensitive operational environments.
- Converted offensive findings into structured defensive intelligence: detection hypotheses mapped to observed attacker behavior, telemetry coverage gap analysis, hardening recommendations, and incident response runbooks.
- Produced adversary behavior research and hands-on lab environments used by blue team and SOC personnel for detection development and threat hunting training.

Operator — Special Reconnaissance and AntiTerror Unit

2016 – 2023

Israel Ministry of Public Security · Israel

- Served 7 years as operator and fighter-paramedic in a special reconnaissance unit conducting field operations in high-threat environments.
- Developed deep understanding of adversary tactics, operational security, and mission planning under real-world conditions — experience that directly shapes current threat actor profiling and red-team methodology.

Independent Cybersecurity Researcher & Technical Author

Oct 2024 – Present

Self-employed · Israel, Remote

- Maintains a 172-post exported Medium archive covering CTI tradecraft, detection engineering, malware analysis, cloud security, AI-assisted workflows, and security tooling. This is a local export count, not a live Medium publication metric.
- Shipped open-source analyst tooling including AdversaryGraph v6.0.0, AIDebug, AuditAI, and String-Analyzer — with documentation, release notes, Docker deployment flows, and reproducible investigation use cases. Three tools assigned to Kali Linux 2026.2 milestone; 8 upstream contributions accepted and 31 open submissions under review.
- Maintains the 1200km research ecosystem: AdversaryGraph docs and use cases, CTI Analyst Field Manual, Israel Gov Threat Actors CTI, Customer-Driven AI CTI Project, OpenCTI Intelligent Shield, and CVSS v4.0 Field Guide.

SKILLS

CTI Tradecraft

ATT&CK Navigator · passive DNS · OSINT pivoting · IOC relationship graphs · Tier 1/2/3 pivots · confidence tiering · PIR/SIR frameworks · kill chain reconstruction · attribution methodology · Shodan · Censys · urlscan · GreyNoise · crt.sh · MITRE D3FEND

Detection Engineering

Sigma · YARA · YARA-L · hunting hypothesis development · telemetry field mapping · ATT&CK coverage analysis · detection backlog construction · log/PCAP use case design · SIEM / XDR rule logic

Malware Analysis

Capstone · FLIRT · Frida · INetSim · LIEF · static PE/ELF analysis · APK analysis · CFG extraction · behavioral pattern detection · import table triage

Cloud Security

AWS CloudTrail · GCP Audit Log · Kubernetes threat modeling · ECS Fargate · Cloud Run · Terraform · attack simulation · container attack paths

Offensive Security

Deep knowledge — red-team operations · reconnaissance · vulnerability chaining · privilege escalation · lateral movement · adversary simulation · attack-path validation

CTI Platforms & Tooling

OpenCTI · STIX 2.1 · TAXII · MISP · connector engineering · VirusTotal · OTX · ThreatFox · Malpedia · urlscan · GreyNoise · AbuseIPDB · Shodan · Censys · NVD API · CISA KEV · EPSS · Python · Bash · C/C++ · PowerShell · Linux · Docker

OPEN-SOURCE TOOLING & VALIDATION

AdversaryGraph v6.0.0 — self-hosted CTI-to-detection workbench covering IOC investigation, AI report/log/PCAP analysis, ATT&CK/ATLAS mapping, Tier 1/Tier 2/Tier 3 relationship expansion, actor/campaign TTP overlap, OpenCTI symmetric sync, MISP/STIX/TAXII import/export, VirusTotal/OTX/ThreatFox/Malpedia/urlscan/GreyNoise/AbuseIPDB/Shodan/Censys enrichment, MalwareGraph-backed malware analysis, Attack Simulation with real lab telemetry and AI kill-chain drills, SIEM forwarding for detection rule validation, enterprise RBAC, MFA workflow support, session management, authentication audit history, CVE Library with NVD/CISA KEV correlation, and analyst-ready investigation reports. GitHub · Docs · Use-case article

AIDebug, AuditAI, String-Analyzer — analyst tooling for malware static triage, function-level disassembly explanation, code auditing, and string extraction. All three tools assigned to the Kali Linux 2026.2 milestone by the Kali maintainer (g0tmi1k). Public packages on PyPI; release documentation and credibility evidence at 1200km.com. 8 upstream contributions accepted across open-source security projects (MISP Galaxy, security resource collections, Kali packaging); 31 open submissions remain under maintainer review.

RESEARCH & PUBLICATIONS

- From Log to Report: Using AdversaryGraph to Turn Firewall and EDR Noise Into a CTI Investigation — AI log analysis, IOC extraction, Tier 1/2/3 investigation, relationship graph review, and report generation. Jun 2026
- Historical AdversaryGraph v4 Capability Map — Version-specific archive covering the earlier platform rename, ATT&CK workflows, IOC Library, OpenCTI/MISP/STIX/TAXII, YARA/Sigma, and feed management. Jun 2026
- MuddyWater / Seedworm / Mango Sandstorm — ATT&CK-mapped kill chain, infrastructure pivot, detection candidates. Mar 2026
- Infrastructure Pivoting: IOC to Actor Network — Passive DNS, reverse IP, ASN reuse, TLS cert, WHOIS field manual. Mar 2026
- CTI Research: Kubernetes & Cloud-Native Threat Landscape — Kill chain analysis and detection architecture for container-native threats. Apr 2026
- ATT&CK as a Working Tool — Gap analysis, Sigma mapping, adversary emulation beyond compliance. Mar 2026
- Manual CTI vs. AI-Assisted CTI — Timing comparison: where AI compresses analyst work and where it fails. May 2026
- CTI Research: Handala Hack Group — Persona and cluster analysis, evidence labeling, IOC handling, defensive guidance. Mar 2026

EDUCATION, EARLIER CAREER & LANGUAGES

- 120+ professional certifications across cybersecurity domains: threat intelligence, detection engineering, malware analysis, cloud security, and offensive security.
- ICU Paramedic — Magen David Adom (2011–2016).
- **Languages:** Russian — native · Hebrew — bilingual · English — professional working proficiency.