

Rotem Dror

Cloud Security Leader · Applied Security Research · AI & Platform Security

Tel Aviv, Israel · rotemdrorcv@gmail.com · [linkedin.com/in/rotem-drorcs](https://www.linkedin.com/in/rotem-drorcs)

SUMMARY

Cloud security leader and applied security researcher. I investigate emerging attack surfaces, analyze cloud and AI threat vectors, and build working defensive proofs of concept — securing identity boundaries, hardening SDLC pipelines, and embedding guardrails into enterprise cloud and LLM architectures.

CORE SECURITY COMPETENCIES

Security Research & Threat Analysis: Attack path analysis, vulnerability research, threat modeling, trust boundary evaluation, zero-to-one defensive prototyping

Cloud & Identity Security: Multi-tenant isolation, cloud IAM & AuthO architecture, privilege escalation mitigation, CSPM, container & Kubernetes security

AI & LLM Security: AI agent guardrails, automated secure code review (LLMs), Azure AI Foundry security, GenAI workflow governance (Claude, ChatGPT)

AppSec & DevSecOps: Secure SDLC ownership, SAST/DAST & supply chain integrity, runtime security telemetry (Datadog APM), C#/.NET code hardening

Cloud Infrastructure: Azure, AWS, GCP, Kubernetes (GKE), Docker, infrastructure as code security (Terraform, Ansible)

EXPERIENCE

Cloud Security & Platform Lead (CTO Office)

Jul 2026 – Present

Mize · Tel Aviv

Previously: Cloud Solution & Security Architect | Lead Engineer (Nov 2024 – Jul 2026)

- Partner with the CTO to lead applied security research — investigating ambiguous security challenges, evaluating emerging attack vectors and building defensive POCs from scratch.
- Researched and engineered an AI-powered PR security reviewer that uses LLMs to detect logic flaws, insecure patterns and vulnerabilities before merge.
- Lead cloud and application security architecture: threat modeling and refactoring legacy services to enforce strict multi-tenant isolation and secure-by-design principles.
- Architected and coded end-to-end authentication and authorization on AuthO, mitigating identity attack paths and securing complex token and session flows.
- Ran security feasibility research and built working POCs for enterprise AI integrations (Azure AI Foundry) and multi-tenant embedded analytics (MS Fabric, Power BI).
- Own the Secure SDLC and DevSecOps platform: CI/CD build integrity, automated SAST and dependency scanning, and the secure migration from TFVC to Git.
- Engineered runtime telemetry and security audit logging in C#/.NET with Datadog APM to detect anomalous behavior and accelerate incident investigation.

Senior Cloud Cyber & Security Architect

Jan 2024 – Nov 2024

KPMG Israel · Tel Aviv

- Led offensive-informed architecture reviews, threat assessments and complex security escalations as a primary technical authority for enterprise clients.

- Investigated cloud attack paths, IAM misconfigurations and lateral-movement risks across hybrid environments, designing defensive frameworks to eliminate systemic vulnerabilities.
- Assessed software supply chain security, artifact provenance and dependency risk, guiding R&D teams through remediation of architectural gaps.

Cloud & Cyber Security Lecturer / Speaker

May 2025 – Present

CyberproAI & Technion – Israel Institute of Technology · Global / Tel Aviv

- Research and present emerging cloud attack vectors, Kubernetes and container hardening, and Azure security strategy to engineering and security audiences, including ISACA.
- Turn vulnerability research and defensive patterns into practical workshops that train engineers to build exploit-resistant cloud systems.

Cloud Security & Infrastructure Engineer

Nov 2022 – Jan 2024

OnCloud · Tel Aviv

- Engineered secure infrastructure across AWS, Azure and GCP, hardening cloud IAM permissions, cryptographic key management and certificate lifecycles.
- Implemented network segmentation, multi-tenant isolation controls and container security policies for distributed Kubernetes environments.

CERTIFICATIONS

- | | |
|--|--|
| ✓ Microsoft Certified: Azure Solutions Architect Expert | ✓ Microsoft Certified: Azure Security Engineer Associate |
| ✓ Microsoft Certified: Identity and Access Administrator Associate | ✓ Certified SAFe® DevOps Engineer |
| ✓ Innovation in Education Award | |

EDUCATION

DevOps Engineer · DevOps Experts

Cyber Security Specialist · ITQ Ltd

2021 – 2022

Diploma, Computer Science & Physics · Ironi Tet High School
