Michael Fedorovsky

DevSecOps Engineer | Cloud Security Specialist | Cybersecurity & Data Protection Engineer

📍 Bat Yam, Israel • 📱 054-763-2418 • ✉ michaelovsky5@gmail.com • 🔗 LinkedIn • 💻 GitHub (100+ repos)

DevSecOps and Cybersecurity Engineer with 2 years of experience embedding security across the full software development lifecycle. Deep expertise in data security, cloud security posture management, vulnerability scanning, secrets management, network defense, and compliance automation. Proficient in threat detection, incident response, identity & access management, and building security-first CI/CD pipelines. Passionate about protecting infrastructure, data, and applications through automation, zero-trust architecture, and continuous monitoring.

🔐 SECURITY EXPERTISE

Data Security — **Encryption:** AES-256, TLS/SSL, at-rest & in-transit encryption • Data masking, tokenization, DLP policies • Database encryption (PostgreSQL, MySQL, MongoDB) • Backup encryption (Restic, AES) • GDPR/compliance awareness

Cloud Security — **AWS:** IAM least-privilege, SCPs, GuardDuty, Security Hub, CloudTrail, Config, Inspector • **Azure:** Defender for Cloud, Entra ID, Conditional Access, Key Vault • **GCP:** Cloud Security Command Center, IAP

SAST/DAST — SonarQube, Snyk, Semgrep, Bandit (Python), gosec (Go) • OWASP ZAP, Nikto, Burp Suite basics • Shift-left security in CI/CD pipelines, automated code scanning on every PR

Container Security — **Trivy, Snyk, Grype, Clair** • Docker image scanning, base image hardening, non-root containers • Kubernetes: OPA/Gatekeeper, Kyverno, Pod Security Standards, Falco runtime threat detection

Secrets Management — **HashiCorp Vault** (dynamic secrets, PKI, encryption-as-a-service) • **AWS Secrets Manager** • **Azure Key Vault** • Auto-rotation policies, zero hardcoded credentials enforcement, audit logging

Network Security — Firewall rules (iptables, UFW, nftables), VPN (WireGuard, OpenVPN), IDS/IPS (Snort, Suricata), fail2ban, nmap scanning, network segmentation, zero-trust networking, Cloudflare WAF/DDoS

Identity & Access — Keycloak (SSO, OAuth2, OIDC, SAML), LDAP, Active Directory, MFA enforcement, RBAC/ABAC, privileged access management, service account auditing, JWT security

Threat Detection — Falco (runtime), SIEM integration, ELK/Splunk log analysis, anomaly detection, AI-powered threat analysis (LangChain/Python), behavioral monitoring, incident triage & response

Vulnerability Mgmt — CVE tracking, patch management automation (Ansible), dependency scanning, CVSS scoring, remediation workflows, compliance reporting, CIS Benchmarks, NIST framework basics

Compliance & Audit — Policy-as-code (OPA, Rego), audit logging, GDPR data protection basics, SOC2 awareness, CIS Benchmarks for Linux/K8s, cloud compliance dashboards, access reviews

Penetration Testing — nmap, Nikto, Metasploit basics, OWASP Top 10 awareness, web app security testing, API security testing, network reconnaissance, port scanning, vulnerability assessment

Secure CI/CD — GitHub Actions secret scanning, signed commits (GPG), container image signing (Cosign/Notary), SBOM generation, dependency auditing, supply chain security (SLSA framework)

Endpoint Security — Malware removal & prevention, Windows Defender hardening, antivirus deployment, SSH hardening (key-only, no root), OS patching automation, secure boot, full disk encryption

Security Scripting — **Python:** Custom security tools, log parsers, automated scanners, API integrations • **Bash/PowerShell:** Security auditing scripts, system hardening automation, incident response playbooks

Monitoring & SIEM — ELK Stack (security events), Splunk, Prometheus/Grafana (security dashboards), PagerDuty (incident alerting), Datadog security monitoring, log correlation, threat hunting

AI in Security — LangChain + OpenAI/Claude for threat analysis, AI-powered log anomaly detection, automated incident triage, LLM-based vulnerability research, intelligent security automation

💼 PROFESSIONAL EXPERIENCE

DevSecOps Engineer @ TovTech — 2 Years

- Implemented shift-left security across all CI/CD pipelines: SAST (SonarQube/Snyk), container scanning (Trivy), secret detection on every commit
- Deployed HashiCorp Vault for dynamic secrets, PKI management, and encryption-as-a-service — eliminated all hardcoded credentials
- Configured Falco runtime threat detection on Kubernetes clusters with custom rules, PagerDuty alerting, and automated incident response
- Enforced zero-trust network architecture: Cloudflare WAF, DDoS protection, mTLS between services, network policy segmentation in K8s
- Built automated vulnerability management pipeline: CVE tracking, patch prioritization, Ansible-based remediation achieving 100% patch compliance
- Implemented data encryption at-rest and in-transit across PostgreSQL, MongoDB, and S3 — full audit logging for compliance
- Designed IAM policies with least-privilege principles across AWS/Azure environments; conducted quarterly access reviews and cleanup

🛡️ SECURITY PROJECTS & TOOLS

Container Security Scanner
Trivy • Snyk • Grype • Docker
Automated vulnerability pipeline: image scanning in CI, severity gating, SBOM generation, remediation reports, base image hardening

Secrets Management Platform
Vault • AWS Secrets Manager • Key Vault
Enterprise secrets lifecycle: dynamic secrets, auto-rotation, PKI automation, K8s integration, zero hardcoded credentials policy enforcement

Runtime Threat Detection
Falco • Prometheus • PagerDuty
K8s runtime security: custom Falco rules, behavioral anomaly detection, real-time alerting, automated incident response playbooks

Data Encryption Framework
Vault • AES-256 • TLS • PostgreSQL
End-to-end data protection: database encryption, backup encryption (Restic), TLS everywhere, key rotation automation, audit trails

Cloud Security Posture Mgmt
AWS Security Hub • Defender • OPA
Multi-cloud CSPM: misconfig detection, compliance scoring (CIS/NIST), policy-as-code enforcement, automated remediation workflows

Secure CI/CD Pipeline
GitHub Actions • Cosign • Semgrep • Snyk
Supply chain security: signed images, SBOM generation, SAST/dependency scanning, secret detection, SLSA compliance enforcement

Identity & Access Platform
Keycloak • OAuth2 • OIDC • LDAP
SSO platform with MFA, role-based access, SAML federation, service account management, privileged access controls, audit logging

Network Defense Stack
Cloudflare WAF • Fail2ban • WireGuard
Multi-layer network security: WAF rules, DDoS mitigation, IDS/IPS, VPN access control, network segmentation, traffic monitoring

AI Threat Analysis Engine
Python • LangChain • ELK • OpenAI
LLM-powered security: anomaly detection in logs, automated threat triage, CVE research assistant, incident summary generation

Vulnerability Mgmt System
Ansible • Trivy • Snyk • Python
End-to-end vuln lifecycle: automated discovery, CVSS-based prioritization, Ansible patching, compliance dashboards, audit reports

Malware Removal Toolkit
PowerShell • Defender • Security Tools
Automated endpoint security: malware detection/removal, rootkit scanning, browser cleanup, registry repair, security hardening scripts

Windows System Hardening
PowerShell • DISM • CIS Benchmarks
OS security automation: CIS benchmark enforcement, patch automation, audit policy configuration, secure boot, BitLocker, event log monitoring

SIEM & Log Correlation
ELK Stack • Splunk • Grafana
Security event aggregation: log parsing, correlation rules, threat hunting dashboards, automated alerting on suspicious patterns

Network Recon & Scanner
nmap • Python • Wireshark
Internal security assessment: automated network scanning, open port detection, service fingerprinting, vulnerability surface mapping

Backup Security & DR
Restic • AES-256 • AWS S3
Encrypted disaster recovery: AES-256 backup encryption, immutable cloud storage, automated restore testing, retention policy enforcement

K8s Policy Enforcement
OPA • Gatekeeper • Kyverno
Policy-as-code: admission controllers blocking non-compliant workloads, Pod Security Standards, image registry restrictions, resource limits

AndroidMonitor Security
C# • ADB • Device Security
Mobile device security monitoring: USB-connected device health checks, unauthorized app detection, storage encryption verification

Compliance Automation
Python • Ansible • OPA • Reporting
Automated compliance checks: CIS Benchmark scans, GDPR data inventory, access review automation, compliance reporting dashboards

🎓 EDUCATION & CERTIFICATIONS

Data Analysis & Security Engineering Program
TovTech (1 Year) • Data protection, threat analysis, security automation, infrastructure security

Engineering Preparatory Year
Ariel University • Physics, Mathematics, Technical English

Security Certifications (In Progress)
CompTIA Security+ preparation • AWS Security Specialty • Certified Ethical Hacker (CEH) preparation • CISSP foundations