Oskar Ibatullin

Santa Cruz, CA | Remote/Hybrid (SF Bay Area)
LinkedIn: https://www.linkedin.com/in/oskaribatullin
Website: https://obormot.github.io/

Staff Product Security Engineer / Architect

Summary

Product and application security technical leader with 24 years across threat research, security architecture, and practical security engineering for enterprise security products and platforms. Hands-on contributor partnering with developers, PMs, and platform teams to design, review, and harden systems across the product lifecycle. Focused on reducing business risk by combining strategic direction with adversarial security fundamentals and AI-accelerated AppSec workflows.

Skills

- Security Engineering: security architecture, threat modeling, secure SDLC, secure design review, secure code review, vulnerability management, SBOM, SCA/SAST/DAST, CVE triage, risk-based prioritization, bug bounty, penetration testing, incident response
- Platform & Infra: Linux hardening, containers, Docker, supply chain, remote provisioning, AWS cloud security, TPM, measured boot
- Cryptography & Auth: TLS, SSH, OAuth2, OIDC, PKI, key/secret lifecycle
- Tools & Languages: Python, Bash, Trivy, Syft, Grype, Tenable, DefectDojo, Jira, Git, Jenkins
- Compliance: Common Criteria, FedRAMP, FIPS, DISA STIG, NIST SP 800-53, OWASP.

Professional Experience

Vectra AI, Inc. — Staff Product Security Architect

San Jose, CA | Feb 2016 – Mar 2026

Scope covered three parallel tracks: security architecture and platform hardening, program governance and compliance, and hands-on security engineering and operations.

Security Architecture and Platform Hardening

- Led security architecture reviews and produced threat models and risk assessments for high-impact product changes, serving as the sole security authority and final sign-off for assigned product domains across multiple engineering teams.
- Drove Linux OS/platform hardening initiatives (kernel and services hardening, containers, supply chain, cryptography, FIPS mode) aligned with NIST and DISA STIG guidance.
- Led deep technical security reviews of update/package distribution architecture and cryptographic controls; identified design/implementation risks and partnered with engineering teams on risk acceptance and remediation strategy.

- Designed and applied authentication and authorization protocols for distributed systems across 4 deployment models: on-prem, cloud, hybrid and SaaS.
- Designed trusted execution, encrypted storage and measured-boot integrity for virtual appliances across 4 platforms (VMware, AWS, GCP, Azure) – using TPM-sealed keys, remote attestation, and integrity-gated unlock flows to resist snapshot cloning and offline tampering.

Governance, Compliance, and Cross-Functional Security Leadership

- Built and scaled Vectra's Product Security program over 10+ years as one of 2-3 senior security ICs – from early startup to a ~600-person engineering org – embedding threat modeling, secure review gates, and vulnerability operations into the full SDLC.
- Acted as primary security SME across engineering and customer-facing teams, advising on architecture decisions, vulnerability impact, and hardening posture.
- Designed and scaled vulnerability operations by integrating security and SBOM scanning into centralized vulnerability management and issue tracking workflows, including triage states, version tracking, and engineering handoff.
- Developed governance documentation including security exception processes, vulnerability management workflow, cryptographic guidelines, enterprise-readiness and compliance requirements mapped to Common Criteria/NIST/OWASP.
- Delivered security controls documentation and evidence packages for Common Criteria and FIPS-140-2 compliance, supporting enterprise and US Federal customer procurement cycles.
- Reviewed and approved security exceptions, designed compensating controls, and guided risk-acceptance decisions with tracked mitigation plans.
- Published customer-facing security advisories and technical response guidance for high-impact vulnerabilities.

Hands-On Engineering and Security Operations

- Built automated tooling for CI/CD integrated SBOM and vulnerability scanning, ticket enrichment, CVE search, SLA metrics, reporting, and dashboarding to improve visibility into vulnerability posture.
- Developed and productized an internal risk rating methodology and an LLM-augmented automated threat model to re-score public CVE findings based on reachability, blast radius, and system risk to prioritize remediation.
- Triaged and risk-rated hundreds of vulnerability findings annually across scanner, customer-reported, and incident channels; authored corrective control recommendations and risk-acceptance criteria that reduced engineering remediation time.
- Conducted internal security audits and discovered exploitable vulnerabilities in product components and protocols; authored exploit PoCs, design proposals for remediation.
- Managed bug bounty and external penetration testing programs – defined scope, validated findings, and drove remediation prioritization across a leading disclosure platform and third-party assessors.
- Implemented IP protection for sensitive Python components through a custom obfuscation and native compilation pipeline with binary stripping in release builds.
- Applied agentic AI workflows to accelerate threat modeling and risk assessment, and to broaden security design and code review coverage with human-in-the-loop validation.

Vectra AI, Inc. — Senior Security Researcher

San Jose, CA | Jun 2013 – Feb 2016

- Researched modern network attack behaviors (reconnaissance, lateral movement, C2, exfiltration) and developed detection logic partnering with data science teams for production NDR use cases.
- Built Python-based internal tooling and production services for threat research, customer deployments, automation, telemetry, and threat intelligence REST APIs.

Juniper Networks, Inc. — Security Research and Engineering Leadership Roles

Sunnyvale, CA / Moscow, Russia | May 2005 – Jun 2013

- Progressed from Security Analyst to Manager and Senior Security Researcher across IDS and integrated anti-malware product lines.
- Led/managed 5-10 headcount research and engineering teams focused on threat research, detection content, testing, and release operations.
- Conducted malware analysis, reverse engineering, and protocol/vulnerability research to develop detection content and improve product efficacy.

Yukos — Software Engineer

Ufa, Russia | Mar 2002 – Jun 2005

- C development and reverse engineering work spanning a university R&D lab and regional corporate division.

Education

- **BS, Computer Networks and Systems** | Ufa State Aviation Technical University | Russia | 2003
- **MS, Management of Organizations** | Bashkir Academy of Public Administration and Management | Russia | 2006

Patents

- **Attack Detection and Prevention Using Global Device Fingerprinting** | US 9106693 | 2015 (co-inventor)
- **System and method for detecting network intrusions using layered host scoring** | US 20150264061 | 2015 (co-inventor)