

Lev Kantorovich

Las Vegas, NV | lev.kantorovich@gmail.com | linkedin.com/in/levkantorovich

Senior Systems Engineer | Detection Engineering | Security Telemetry | Platform Reliability

PROFESSIONAL SUMMARY

Senior Systems Engineer with 20+ years of experience building, operating, and troubleshooting security-focused software systems. Extensive background in endpoint telemetry, observability, diagnostics, event processing, automation, and platform reliability. Experienced working across the full telemetry lifecycle—from endpoint collection and instrumentation through data processing, monitoring, operational response, and engineering automation. Strong hands-on expertise in Python, C++, Windows, Linux, cloud-based infrastructure, and large-scale security environments.

CORE SKILLS

Detection Engineering • Security Telemetry • Endpoint Visibility • Observability • Data Pipelines • Platform Engineering • Reliability Engineering • Python • AWS • Event Processing • Automation • Monitoring & Alerting • Diagnostics • Security Operations • AI-Assisted Engineering Workflows

PROFESSIONAL EXPERIENCE

Arctic Wolf Networks — Senior Kernel & Systems Engineer (2024–2026)

- Developed endpoint telemetry, diagnostics, and operational infrastructure supporting cloud-delivered security services.
- Built engineering automation, validation workflows, and telemetry-analysis tooling.
- Contributed to observability, event-processing, and operational monitoring workflows used in large-scale security environments.
- Performed troubleshooting, performance analysis, and reliability improvements across complex distributed systems.

Microsoft — Systems Engineering Consultant (2023–2024)

- Investigated production failures using ETW traces, telemetry, memory dumps, and networking diagnostics.
- Analyzed large-scale endpoint behavior and operational data to identify root causes and reliability issues.
- Developed repeatable troubleshooting and diagnostics approaches for enterprise-scale environments.

SentinelOne — Senior Kernel Developer (MTS) (2021–2023)

- Developed endpoint telemetry, inspection, and security capabilities for large enterprise deployments.
- Designed and optimized data collection and visibility components supporting endpoint security operations.
- Improved performance, reliability, and operational effectiveness of security infrastructure.

Forcepoint — Principal Software Engineer / Senior Software Engineer (2017–2021)

- Built enterprise security technologies including endpoint protection, DLP, telemetry collection, and network-security capabilities.
- Developed monitoring, diagnostics, and troubleshooting capabilities supporting operational security workflows.
- Worked on scalable, multi-threaded systems processing security and networking events.

AI-ASSISTED ENGINEERING & AUTOMATION PLATFORM (PERSONAL PROJECT)

- Designed and implemented an AI-assisted engineering control plane for managing complex software-development and data-processing initiatives.
- Built structured workflows including goal definition, task decomposition, implementation planning, validation gates, test gates, and human approval checkpoints.

- Developed orchestration concepts for coordinating multiple AI-assisted work streams while maintaining observability, traceability, auditability, and operational control.
- Implemented structured handoff workflows, quality validation processes, progress tracking, and roadmap execution mechanisms across concurrent engineering tasks.
- Applied systems-engineering principles to agentic workflows including context management, reproducibility, failure analysis, and controlled automation.

SECURITY TELEMETRY & PLATFORM INITIATIVES

- Worked across endpoint telemetry collection, diagnostics, event analysis, monitoring, and operational troubleshooting.
- Built and evolved tooling supporting telemetry quality, visibility, observability, and engineering productivity.
- Focused on monitoring, troubleshooting, performance optimization, and reliability of production systems and security platforms.

TECHNICAL SKILLS

Languages: Python, C++, C, JavaScript

Platforms: AWS, Linux, Windows, Docker

Systems: Endpoint Telemetry, ETW/WPR, Observability, Monitoring, Diagnostics, Event Processing, Performance Analysis

Security: Endpoint Security, Detection Infrastructure, Security Operations Support, Telemetry Pipelines

Automation: AI-Assisted Engineering, Control Plane Concepts, Agentic Workflows, Validation Automation

EDUCATION

Master of Science in Computer Engineering