



Pavel Yushkevich

Senior Security Platform Engineer

SIEM • SOAR • Detection & Response
Automation

- EMAIL
career@pavelyushkevich.com
- PHONE
+48 571 457 057
- LINKEDIN
linkedin.com/in/nicedeagbro
- WEBSITE
pavelyushkevich.com
- LOCATION
Warsaw, Poland • Remote

Profile

Security platform engineer who designs and owns **detection & response platforms end to end**: log collection and enrichment, SIEM, detection-as-code, and SOAR with AI-assisted triage. 4 years in security operations: 2+ years in 24/7 SOC and incident response, and since 2025 the owner of the security monitoring and automation platform at a globally regulated fintech (1,500+ employees). The platform serves a ~30-person security team.

I own the architecture, roadmap and stakeholder alignment with SOC, IT, engineering, compliance and business owners. I know what to log, how long to keep it and how to prove it to a regulator. When a project needs it, I personally ship the connector, detection or playbook.

≈1 TB / day

security telemetry through the pipeline I designed (OpenSearch SIEM)

50+ sources

IdP, EDR, CASB, WAF, cloud, PAM, finance & SaaS integrated into the platform

~95% ATT&CK

coverage of techniques relevant to company infrastructure, validated with Atomic Red Team simulations

2-5 min vs 15-40

time to first enriched triage after AI-assisted SOAR rollout; 50-75% auto-closure in automated alert classes

Core Expertise

Security Platform Architecture

End-to-end SIEM/SOAR design, build-vs-buy, design docs, roadmap. Reliability by design: buffering, DLQ, replay.

Log Engineering & Enrichment

Collection from any source: APIs, webhooks, syslog, streams, files. Normalization to a common schema, plus business and identity context enrichment at terabyte scale.

Detection Engineering

Sigma, detection-as-code with tests and CI/CD, behavioral analytics with personal and cohort baselines, MITRE ATT&CK.

SOAR & Automation

Custom SOAR core (Python/FastAPI, SQS, Kafka, Celery/Redis), n8n, playbooks-as-code, approvals, Jira and Slack.

AI for Security Operations

LLM triage agents with tool access, guardrailed auto-closure, feedback loops, MCP servers for engineers.

Compliance-driven Logging

DORA, ISO 27001, GDPR, FCA, CySEC, SCB, MAS: logging scope, retention, audit trail and evidence for auditors.

Experience

Security Engineer • SIEM / SOAR Platform Owner

Jan 2025 – Present

Capital.com • global multi-regulated fintech, 1,500+ employees

Platform architecture & ownership

- Designed and own the detection & response platform end to end: **collection** → **normalization** → **SIEM** → **detections** → **SOAR** → **case management**. Authored the design docs and drove them through approval.
- Built a custom SOAR core instead of buying one. The business had standardized on its ticketing system and a low-code orchestrator, so I designed an enterprise-grade core around them: an API layer with **Celery/Redis** workers, **SQS-buffered** event ingestion, **playbooks-as-code** and configurable approval rules. Orchestrator outages lose no events, and a new playbook is one file in Git.
- Structured automation logic in three tiers (detection rule, Python tool, AI agent), so each problem is solved at the cheapest tier that works.

Data collection, SIEM & enrichment

- Built an in-house **Python connector framework** and scaled the platform to **50+ integrated sources** (identity, endpoint, network, cloud, SaaS, finance systems, databases and streams), building, rewriting or maintaining their connectors.
- Run an **OpenSearch SIEM ingesting up to 1 TB/day**: per-source routing, normalization to a common schema, retention aligned with regulation, raw-event backup and DLQ for replay, log-loss monitoring.
- Designed the **enrichment layer**: identity and HR context, geo and IP reputation, infrastructure metadata, all cached to stay cheap at terabyte scale.

Detection engineering

- Introduced **detection-as-code**, the pipeline behind a library of **~200 custom detections**, each backed by a SOAR playbook: Sigma rules in Git, review, automated tests and CI/CD deployment. Every new rule automatically gets a ticket, dedup, severity and AI triage. Behavioral scorers with baselines cover logic that rules can't express.
- Reached **~95% MITRE ATT&CK coverage** of techniques relevant to company infrastructure, validated in annual Atomic Red Team simulations.
- Rolled out host telemetry and vulnerability detection across the fleet with Ansible. Evaluated Linux and Kubernetes telemetry down to the syscall level and defined CIS-aligned hardening requirements.

SOAR & AI-assisted response

- Built **LLM triage agents** with tool access to SIEM and case data. The first enriched verdict now arrives in **2–5 min instead of 15–40**, and analyst time per alert is down an estimated 30–50%.
- Designed **guardrailed auto-closure**: an alert closes only on an independent fact (access approval, privileged-access session record, verified content). Each class runs in shadow mode first, and every action is visible in the ticket. Result: **50–75% auto-closure** in covered classes, including 73% of DLP secret-exposure alerts on day one.
- Built a **self-improving triage loop**: analyst decisions become feedback, the system proposes prompt changes, and humans approve them through review.

Business, compliance & team

- Architected **monitoring of employee access to client PII**: static rules plus a behavioral model with personal and peer-group baselines, analyst verdicts fed back into the platform, and a weekly report for management. Also built leaver watch driven by HR offboarding data.
- Translated **DORA, ISO 27001, GDPR and FCA / CySEC / SCB / MAS** requirements into logging scope, retention and audit-trail design.
- Mentored SOC analysts and onboarded new engineers. Built MCP servers and AI skills for the team: Sigma generation and testing, tuning review, connector scaffolding.

SOC Analyst

Nov 2023 – Jan 2025

Capital.com

- Led investigations from endpoint detections to multi-stage attacks, covering containment, remediation, vulnerability patching and reporting.
- Worked across SIEM tuning, network monitoring (Zeek, Suricata, Arkime), honeypots and DLP controls.
- Improved SOC workflows, mentored analysts and started the automation work that grew into the platform role.

SOC Analyst

Oct 2022 – Nov 2023

Wargaming

- Worked in a large, mature 24/7 SOC: alert triage, threat hunting and detection-logic refinement to cut false positives.
- Handled incidents from simple tests to multi-stage attacks across multiple infrastructure layers.
- Wrote forensic artifact collection scripts for Windows, macOS and Linux.

Technical Skills

SIEM & Data	OpenSearch / Elastic Stack, Logstash, Kafka, Wazuh, Sigma
SOAR & Automation	Python, Bash, FastAPI, Celery, Redis, AWS SQS, n8n
Cloud & DevOps	AWS, Docker, Kubernetes, Terraform, Ansible, GitLab CI/CD, HashiCorp Vault
Security Domains	EDR, Identity & Access, CASB & DLP, WAF, Cloud Security, PAM & IGA, Vulnerability Management, Network Monitoring
AI Engineering	LLM agents, MCP servers, Claude Code, Codex, Cursor
Frameworks & Regulation	MITRE ATT&CK, Atomic Red Team, CIS Benchmarks, DORA, ISO 27001, GDPR, FCA • CySEC • SCB • MAS

Education

Bachelor's, Information Systems and Cybersecurity

Vilnius University, Institute of Applied Informatics • 2020 – 2024

Information Systems Management

School of Business of BSU, Minsk • 2019 – 2020

Languages

Russian — native

English — C1, professional working proficiency

Polish — basic (A2)

Architect by default, hands-on when it matters.

I design the platform, align it with the business and regulators, and personally ship the connector, detection or playbook that gets it live. The result is a working system.