ING.ONDREJSEVCIK

CSOC Engineer
Splunk, Cribl and Sentinel Specialist

✉ o.sevcik91@gmail.com

🌐 sevcik.dev

ABOUT ME

I've always been passionate about computers and new technologies.

In 2016, I purchased my first course on creating iOS applications, which marked the beginning of my software engineering journey.

Since then, I've been driven to learn new skills and tackle complex problems.

TECHNOLOGIES

...that I have in depth experience with:

- Splunk
- Cribl
- Sentinel
- React / Next.js
- Node.js
- Typescript
- SQL
- Python
- Bash

...some other that I've been using:

- JIRA
- Confluence
- Azure DevOps
- ServiceNow
- GitHub / GitLab / BitBucket
- CI/CD
- Agile / Scrum
- Vercel's DevOps
- Jenkins
- JEST
- Playwright
- Selenium
- Java
- Kotlin
- Swift

WORK EXPERIENCE

Novartis (Migration)   2023 – 2025
LEAD CSOC MIGRATION ENGINEER
CRIBL, SPLUNK & SENTINEL

- I've been the lead migration engineer for two major security log migrations spanning across ~500 indexes.
  - Integrating Cribl Stream as middleware (Splunk's UF/HF -> Cribl Stream -> Splunk)
  - Replacing Splunk with Sentinel (Splunk's UF/HF -> Cribl -> Sentinel)
- During both migrations, I was responsible for creating proof of concept, preparing initial guidelines for the migration process, and reviewing Cribl Stream packs created by other engineers to ensure event breakers, time extraction, and data processing were done correctly
- I was also able to save Novartis a vast amount on Splunk license costs by optimizing the size of Palo Alto and Checkpoint logs in Cribl Stream, saving over 55% of license costs
  - Led Cribl Stream pack development code reviews for 12 other engineers across several hundred indexes
  - Created guidelines and proof of concept for migration processes, including Universal Forwarder, Heavy Forwarder, Syslog, HEC, API, and other integrations, including custom ones
  - Directly responsible for the data quality of migrated data — focused on correct field/time parsing, data loss prevention, and coding standards
  - Worked closely with the CSOC Platform team on initial Splunk integrations
  - Besides code reviews, my main focus was the integration of XML Windows and Security event logs, and firewall logs

Novartis (Onboarding)   2020 – 2023
SPLUNK CSOC ONBOARDING ENGINEER
SPLUNK

- Managing the process of onboarding security logs from internal applications running multiple different technologies to the Splunk
- Experience with onboarding security logs of MS WIN, RHEL, AIX, Solaris, MSSQL, Oracle DB, PostgreSQL, Azure, AWS, MS IIS, Cisco, SalesForce, IBM SVC, and custom vendor appliances
- Having full responsibility over the complete onboarding process of an application onboarding from gathering configuration items scope to onboarding process itself and proper documentation of the full process
- Working in a strictly confidential and process driven environment of big pharma
- Working with Splunk's configuration files, creating custom indexes/sourcetypes, modifying parsing and transformation rules

WORK EXPERIENCE

CODE MARKETER S.R.O. – FREELANCING

REACT/NEXT.JS FULL STACK DEVELOPER

2025 – Trainer Helper – Personal project – in development
- Next.js/PostgreSQL web app that helps trainers with workout creation and planning, trainers can define own database of movements and leverage AI for ideas of new workouts

2025 – sbernakrmelin.cz
- Next.js/MongoDB web app for metal collection company
- Sberna has 2 other locations (Havirov and Centrum) all of them are reusing same component library
- All locations have Admin system that allows owner to control content of website including materials definition with pricing, information blocks, promo banners, etc.

2022–2024 – DHL – Global Call Planning Tool
- Application used for planning of global calls with ~200k visits / month
- Next.js application using DHL's UI (Material) library
- I was a sole developer with responsibility of developing new features and maintaining old code base

2021–2022 – DHL – Mango Core
- Angular development as part of 12 member team (3x FE)
- Application has been leveraging AG Grid to display generated offers

2016–2020 – WOD Time Calculator – Personal project
- Latest major release is Vue.js/MongoDB application used to calculate good time/score of any CrossFit workout
- +10k visitors/month
- Everything including back end, design and marketing done by myself

Other projects
- Dozens of other project including my cooking blog 7dietmeals.com, online shops lovelydreams.cz and mbkl.cz and some other business websites like studiobg.cz

ROBOTRON

SENIOR FRONT END REACT DEVELOPER
- Alternative position offered by Robotron for a short time after Covid-19 paralysed the economy and automotive sector
- I've been working as Front End Lead of two React applications developed for Linde, the goal was to match UI/UX between the projects and have it standardized through all dashboards

SPLUNK DEVELOPER
- For 1.5 years worked in a small team with excellent mentor who was Splunk Enterprise Certified Architect and learned everything from SPL to onboarding data, configuration files and deployment
- Working on multiple custom build Splunk dashboards by leveraging and extending SplunkJS functionality
- Creating several Splunk applications and custom search commands in a Python3

WORK EXPERIENCE

PROFIQ
2018 – 2019

JUNIOR SOFTWARE DEVELOPER
- I've been working on the development of server-side Node.js application, integrated Docker and CI/CD for that application and I've been part of the team that worked on the creation of unit tests for Avast.

LIONBRIDGE
2012 – 2019

INTERNET ASSESOR
- Long term part-time project to evaluate quality and utility of websites.

LIONBRIDGE
2018 – 2019

CZECH RATERS QA MANAGER
- Managing Czech raters on Transcription project and ensuring delivered quality.

WEBGEARS GERMANY GMBH
2015 – 2018

VOUCHER COORDINATOR
- Coordinating offer of valid vouchers on voucher aggregator website.

INPARK FITNESS S.R.O.
2015 – 2021

CROSSFIT LEVEL 1 TRAINER

COLLIERY CROSSFIT
2014 – 2015

CROSSFIT LEVEL 1 TRAINER
- Leading CrossFit classes of 10-20 people, several times per week.

EDUCATION

MASTERS DEGREE IN MARKETING & MANAGEMENT
2015 – 2017

SILESIAN UNIVERSITY OF OPAVA
- Winner of the best Masters Thesis that was about Online Marketing of Fitness Internet Blog that I've owned. Education has been focused on advanced marketing, management, economics, trade, and accounting.

BACHELORS DEGREE IN MARKETING & MANAGEMENT
2011 – 2015

TECHNICAL UNIVERSITY OF OSTRAVA
- Thesis about Client Satisfaction Measurement of the Sports Center. Education has been focused on marketing, management, economics, trade, and accounting.

SOFTWARE DEVELOPMENT
2010 – 2011

BRNO UNIVERSITY OF TECHNOLOGY
- University focused on computer science. I didn't finish it, my passion for programming has been fired up a few years later.

ELECTRONICS AND COMPUTER TECHNOLOGY
2010 – 2011

INDUSTRIAL HIGH SCHOOL OF ELECTRONICS, FRENŠTÁT POD RADHOŠTĚM
- The study focused on IT and electronics that for example included Computer Science, PLC Programming, Assembly Programming, Boolean Algebra, Electrical Engineering, and university-level Mathematics.

OTHER EDUCATION
2016 – present

PAID COURSES, ONLINE WORKSHOPS & LEARNING NEW TECHNOLOGIES
- In 2016, I began my self-learning journey with an iOS applications course on Udemy. Since then, I have completed hundreds of paid courses and online workshops on topics ranging from Harvard's CS50 and web development with React, Vue, and Angular, to building mobile apps with React Native, Java, and Swift, as well as Blockchain development, containerization with Docker, DevOps with Azure, CI/CD setup, Agile Project Management, and specialized training in Splunk, Cribl, and Sentinel. I've even explored Unity to create games. My passion for learning drives me to constantly discover new technologies.

ING.ONDREJSEVCIK