Maksim Melnik

IT Security Professional
Software Developer

Born: 1993
Languages: English, German, Russian

Email	maksim@mmelnik.com
Website	mmelnik.de
GitHub	github.com/KeksTheAllmighty
StackOverflow	stackoverflow.com/users/5173658/maksim-melnik
LinkedIn	linkedin.com/in/maksim-melnik

Areas of Expertise and Skills

IT-Security

SOC, Incident Responce, Penetration Testing, Kali Linux, ArcSight, Splunk, Elasticsearch, Opensearch, Hive.

Software Development

Machine Learning, Data Engineering, Deep Learning, Process Automation, Time-Series Analysis, Financial Markets, Risk Management, Social-Media Automation, Web-Development.

Technologies and Libraries

Google Cloud, Docker, Ansible, Packer, Terraform, Git, Jenkins, Django, Flask, Numpy, Pandas, PyTorch, Tensorflow, Selenium,Keycloak IDM, Apache Kafka, Wordpress.

Programming Languages

Python, Java, Powershell, Bash, C, C#, C++, PHP, Javascript, Flutter/Dart, Solidity, Gradle.

Education

B. Sc. Computer Science
2012-2016
- Cryptography
- Thesis: Private Set Intersection based on Elliptic Curve Cryptography.

M. Sc. IT-Security
2016-2020
- IT Security
- Network Security
- Embedded System Security
- Public Key Infrastructures
- Cryptocurrencies
- Post-Quantum Cryptography
- Security of Critical Infrastructures
- Data Mining and Machine Learning
- Thesis: Social-Media based detection of crisis events

Certificates

Google Cybersecurity
Splunk Fundamentals 1
Lpic-1
Comptia Security+
Comptia Pentest+
Comptia CySA+
eJPT
eCPPTv2
OSCP

Work Experience

SOC-Analyst @ ACG - Automation Consulting Group
November 2020 - Present

- SOC-Analyst at KfW Bank: incident detection and response using ArcSight, Splunk, Hive.
- Conducted a penetration test on the internal web-application and external services.
- Configured an internal Opensearch SIEM instance.
- Developed internal sigma rules.
- Set up a CTF-Challenge in scope of ITCS-event.
- Deployed Instagram automation.
- Development of numerous Python/Bash scripts for the internal purposes.
- Created an internal Cybersecurity Awareness training program.

Student Developer @ Ericsson
May 2016 - November 2020

- Developed Gradle scripts for test and deployment of Ericsson BSCS product.
- Configured Jenkins jobs for deployment and test of the Ericsson BSCS product.
- Developed internal PHP web-applications.
- Integrated SSO using Keycloak IDM into the internal Spring product.
- Implemented high performance messaging system using Apache Kafka.
- Performed Java resource consumption analysis of the internal Java application using JNI/JVMTI.
- Developed Python Robot Tests using Selenium for the internal web application.
- Developed a Flutter-application for finding general goods in supermarkets.

Student Research Assistant @ TU Darmstadt
November 2017 - June 2018
January 2019 - July 2019

- Developed Wordpress PHP plugin for submission of cyber crime reports.
- Designed a PoC of a Hyperledger Smart-Contract.
- Implemented a Python LSTM model to forecast Linux machine's vulnerability.
- Django backend was implement to interact with the application.

Projects

Financial Markets Data Science & DevOps

- Configured Freqtrade trading bots.
- Implemented trading strategies and backtest process using TA-Lib, backtrader.
- Studied performance of trading strategies.
- Created a Python Flask website to showcase machine learning approach for stock price forecasting.
- Configured GitHub Workflows to build and deploy Google Cloud instances with Ansible and Packer.

Sewing Patterns Online Shop

- Wordpress website for selling sewing pattern PDF files.
- Configured infrastracture for file sharing as well as python interface for easy cropping and rendering of the sewing pattern PDF files.
- Configured Facebook Ads, Google Ads, Etsy.
- Link

Social Media Automation

- Developed Python application to analyze trending topics using Google Trends.
- Developed another Python application to automate video cutting process using moviepy.
- Automated Instagram, Youtube and Pinterest content upload.

Other

- Participated in Computer Chaos Group meetups @ Darmstadt.
- Participated in numerous CTF events.
- Achieved 1st Place @ Merck Hackathon where a Speech-to-Text and Text-to-Speech chat-bot was deployed in Azure infrastructure.
- Discovered and reported kernel vulnerability @ TU-Darmstadt.
- Co-Authored a paper.