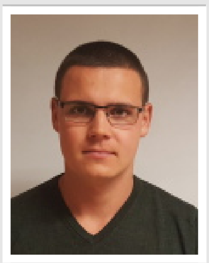

Mgr. Severin Simko

+421 902 196 845, severinsimko@gmail.com

Personal details

Address:	Tolsteho 19, 04001 Kosice, Slovakia
Date of birth:	28 September 1992

Education

Providence University, Taichung, Taiwan
Exchange Program / 2017 - 2018

Masaryk University, Faculty of Informatics , Brno, Czech Republic
Master's Degree in Service Science, Management, and Engineering / 2016 - 2018

Technische Universität Dresden, Germany
Erasmus Exchange Program / 2016 - 2016

Johannes Kepler Universität Linz, Austria
Erasmus Exchange Program / 2013 - 2014

Masaryk University, Faculty of Informatics, Brno, Czech Republic
Bachelor's degree in Applied Informatics / 2012 - 2016

Courses and training

IBM
IBM Security QRadar Technical Sales Foundations - Level 100 / 03/2018 - 03/2020

TOEFL
TOEFL iBT - 100 / 02/2017 - 02/2020

Flowmon Networks
INVEA-TECH FlowMon Consultant / 01/2016 - 01/2018

Employment history

Software Development Team Lead
10/2019 - yet, Siemplify, Tel Aviv, Israel

Lead Generation & Optimization Specialist
12/2017 - 10/2019, LightFoot Media, U.S.A.
Experience:
- Lead tracking platforms - Leadspedia, HasOffers
- Data management and processing - MongoDB, Python (pandas, database access packages), PowerBI
- Mean Stack Development - Node JS, MongoDB, Express & PHP
- Front End & Network Optimization
- DNS Networking - Amazon Route53, dnsimple, Cloudflare
- System & Network Administration

IT Security Engineer
10/2015 - 10/2019, AXENTA a.s.
Responsibilities:
- Design, implementation, and monitoring of security measures for the protection of computer systems, networks, and information
- Identification and definition of system security requirements
- Design of computer security architecture and development of detailed cyber security designs
- Linux server & network administration
- Development of technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks

Experience:
- Log Management - syslog-ng, syslog-ng Store Box, Graylog
- NetFlow Monitoring - Flowmon
- SNMP Infrastructure Monitoring - Centreon/Nagios
- Scripting in PYTHON/SHELL/BASH
- VMware Virtualization Technology
- Ticket tracking system implementation and configuration - Request Tracker
- Host-based Intrusion Detection System configuration - OSSEC
- Open Source Log Management System - Graylog
- Automation/Configuration Management Tools - Ansible/AWX

Projects:
A, O2 Security Expert Center (SOC)
- infrastructure monitoring - Centreon
- log management - syslog-ng, syslog-ng Store Box
- Request Tracker implementation and configuration

B, Axenta lab
- infrastructure monitoring - Centreon
- log management - syslog-ng, syslog-ng Store Box

C, Krajské operační centrum - Jihomoravský kraj (SOC)
- infrastructure monitoring - Centreon
- log management - syslog-ng, syslog-ng Store Box
- network administration

- Request Tracker implementation and configuration

D, Axenta Security Operations Center - CyberSOC (SOC)
- Security Operations Center implementation and administration
- Log Management design and implementation
- Infrastructure Monitoring design and implementation
- Request Tracker implementation and configuration

E, Teplárny Brno
- Log Management design and implementation

F, Veřejný ochránce práv, Brno
- Log Management design and implementation

DevOps Engineer
12/2017 - 05/2018, NXLog Ltd
Development and Testing of NxLog Log Management Tool and Technical Writing

Experience:
- Log Management
- NxLog Comunity Edition. NxLog Enterprise Edition
- NxLog Integration with SIEM
- GDPR, PCI-DSS
- Technical Writing

Full Stack Python Developer
09/2016 - 11/2017, Computer Security Incident Response Team at Masaryk University
Development of framework for IP flow analysis by using technologies for real-time data processing, network traffic monitoring, and visualization - Stream4Flow

Experience:
- Apache Spark
- Bash/Python scripting
- Python programming
- Splunk REST-API
- Web2py and Bootstrap Frameworks
- HTML/ CSS/ JAVASCRIPT

Additional information on employment history
Projects:

03/2020 - SIRANGA - Platform for automatic setup and management of private cloud servers
- Goldinger IT GmbH, Switzerland

The platform is a Django application from which customers can automatically set up and manage their own private cloud, the application is integrated with a payment gateway (Stripe) and Ansible AWX which is used as a core system for automation.

Technologies:
- Automation: Ansible AWX
- Development: Python, Django, Stripe
- Others: Proxmox, Samba, Kopano, OPNSense, HAProxy

Learn More: siranga.com

01/2019 - SimkoLab

Complex CyberSecurity platform in which potential clients can try the services and different open-source technologies which I'm offering as a freelancer. SimkoLab is the CyberSecurity portfolio consisting of multiple open-source technologies focusing on different CyberSecurity fields.

Technologies:
- Infrastructure Monitoring - Centreon, Zabbix, Icinga2
- Log Management - ELK Stack, Graylog, Splunk
- Log Daemons - syslog-ng, rsyslog, filebeats
- Intrusion Prevention Systems - Suricata
- Intrusion Detection and Host-Intrusion Detection Sytems - OSSEC/Wazzuh, Proxy: HAProxy, Squid
- Configuration Management/Automation - Ansible/AWX
- Firewalling - pfSense

Learn More: simkolab.com

Jul 2019 – Oct 2020 - Long Term Support for Log Management and Infrastructure Monitoring - Cinoware, Austria

Long term support of Graylog and Zabbix and technical training for the internal team.

Technologies: Graylog, Zabbix

Jul 2020 - Implementation of Centralized Infrastructure Monitoring System - Vivanet, Switzerland

Design and implementation of an SNMP-based centralized infrastructure monitoring system using Centreon.

Technologies: Centreon

05/2018 - Log Management & Intrusion Detection using Graylog and OSSEC - Value-Ad, Australia

Implementation of best-practice Intrusion Detection rules and Centralized Log Management installation and configuration using Graylog, OSSEC, and syslog-ng as the log shipper. Ansible used for the deployment automation.

11/2017 - Customized Configuration of Graylog - Dial-Once, France

Log Analysis Optimization for easier and more efficient analysis, creation, and deployment of custom decorators and plugins to increase the readability and custom alerting.

09/2017 - Real-Time Data Streaming Platform Evaluation - Wallaroo Labs, U.S.A.

Deployment and Testing of the Real-Time Data Streaming Platform and the Design & Implementation of the Real-Time Network Security Monitoring Use-Cases.

08/2017 - Graylog - OSSEC Integration Project - Paisaease, India

Intrusion Detection installation and configuration using OSSEC and integration with Graylog. Implementation of best-practice detection methods and alerting.

07/2017 - Infrastructure Monitoring Integration REST-API - Goldinger IT GmbH, Switzerland

Implementation and testing of the API capable of fetching and processing the data from the Zabbix monitoring system.

02/2015 - 09/2015 Performance Testing of Apache Storm Framework (JAVA SE)

Language skills

Slovak	Proficiency (C2)
English	Proficiency (C2)
German	Intermediate (B1)

Driving licence

B category