

CURRICULUM VITAE

Technical Skills:

- **OS:** RedHat/CentOS, Ubuntu
- **Cloud services:** AWS
- **Code version control and management:** Github
- **IaC:** Ansible, Terraform, Kubernetes
- **Analysis and monitoring:** Prometheus, Grafana, ELK, Zabbix, Splunk
- **Programming:** python, perl, php, shell-scripting (awk, sed, bash etc), html/xml, javascript
- **Databases:** MySQL/MariaDB, PostgreSQL, Redis
- **Networking:** routing and switching on CCNA+CCDA level
- **Security (Firewalls, LoadBalancer, Proxy):** F5, Fortinet, CheckPoint, PaloAlto, pf/ipfw/iptables, Squid, Bluecoat, OpenVPN, Wireguard

Work experience

Nov. 2018 till now *Senior System Engineer*, Managed Security Service (MSSi) at Swisscom AG (Zürich, Switzerland)

Developing, maintaining and administering tools which automate operational activities and improve engineering productivity. Automating infrastructure management using configuration management and provisioning tools. Designing, implementing, supporting and improving tools the team depends on (monitoring, process automation). Providing continuity and stability to the production environment.

Specialties: RedHat/CentOS, Ansible, Docker/docker-compose, Terraform, Git, python, shell-scripting, Zabbix, Apache, Nginx, ELK, Grafana, F5, Fortigate, Bluecoat, Zscaler

Dec. 2017 to Oct. 2018 *Senior System Engineer*, IFA/WES at CreditSuisse (Zürich, Switzerland)

Responsible for administration and maintenance proxy/reverse proxy environment for internet facing applications (as Mobile banking). Automating infrastructure management, improving tools and monitoring.

Specialties: RedHat/CentOS, Web-related technology (web application security, proxy/reverse proxy, WAF, Apache/Nginx, OpenSSL), perl, python, shell-scripting, svn.

Apr. 2016 to Nov. 2017 *Technical Security Officer / Security Analyst (SOC)*, Security Operation Center at RBS Services – RBS Group (Zürich, Switzerland)

Responsible for analyzing and responding to security events from FWs, IDS/IPS, DLP, AV, sandbox and other security data sources. Log management and integrations. Creating and maintaining Splunk dashboards, reports and alerts for security event detection. Managing System Compliance, Vulnerabilities and Network Security. Performing vulnerability identification, assessment and remediation tracking.

Specialties: Splunk / syslog-ng, FireEye, Qualys, McAfee MVM (Foudstone), Forcepoint DLP, Skybox.

Nov. 2011 to Mar. 2016 *Security Engineer*, Swisscom AG (Zürich, Switzerland) - designated to CreditSuisse

Implementing the IT security concept, maintaining and operating the security infrastructure, performing network troubleshooting. Providing 3rd level support for the IT responsible community (NOC / SOC).

Specialties: RedHat/CentOS, CheckPoint (Nokia IPSO, SPLAT), Juniper (Netscreen/ScreenOS, SSG, ISG, IDP, NSM), PaloAlto Next-Generation Firewall, McAfee Sidewinder, Bluecoat, shell-scripting.

Nov. 2010 to Oct. 2011 *Security Engineer / Security Analyst (MSS)*, Managed Security Services at Trustwave Holdings, Inc. (Warsaw, Poland)

Performing network troubleshooting to isolate and diagnose common network problems, configuring, managing, and monitoring FW, NAC, IDS/IPS, SELM and IVS platforms. Analyzing and responding to security events from FWs, IDS/IPS, AV and other security data sources. Responding to needs and questions of customers concerning their access to network resources through their managed device.

Specialties: RedHat/CentOS, CheckPoint, Juniper (Netscreen/ScreenOS, SSG, IDP, NSM), Fortinet (Fortigate), iptables, Snort, Nessus, Squid, shell-scripting.

Jan. 2007 – Oct. 2010 *IT Security Engineer*, Solidex S.A. (Warsaw, Poland)

Primary duties included support, troubleshooting and resolving highly complex problems related to hardware failure, systems design and misconfiguration for multi-vendor security solutions such as CheckPoint, Juniper, Crossbeam. Designing and implementing the IT security concept based on firewall, VPN, IDS/IPS, proxy. Performing installation and system migration between different platforms such as CheckPoint, Juniper, ASA, Fortinet, iptables/pf/ipfw. Additional duties included sales team support, technical consultations, pre-sales and post-sales consultants in technical matters, workshop training for clients.

Specialties: Linux, CheckPoint (Provider-1, firewall/VPN, Integrity/EndpointSecurity, Edge), Juniper (Netscreen/ScreenOS, SSG, IDP, NSM), Nokia IP (IPSO, Voyager), Crossbeam, TrendMicro (IWSS, IMSS, OfficeScan), shell-scripting.

Jun. 2004 – Oct. 2006 *System Administrator*, Network department at Auchan Polska Sp. z o.o. (Warsaw, Poland)

Responsible for administration and maintenance of firewalls (CheckPoint and Juniper), proxy-, antivirus- and mail- servers all based on FOSS (free open-source software). Maintaining a monitoring system based on Cacti, Nagios and NetFlow.

Specialties: Linux (RedHat / Gentoo), CheckPoint, Juniper (Netscreen/ScreenOS, SSG, NSM), Nokia IP (IPSO, Voyager), TrendMicro (IWSS, IMSS), Squid, DansGuardian, sendmail/qmail, openldap, nagios/mrtg/cacti, shell-scripting.

Sep. 2001 – Aug. 2003 *System Administrator*, IT Department at Maxcom AG (Luzern, Switzerland)

Jun. 2000 – Aug. 2001 *System Administrator*, IT Department at Maxcom Polska Sp. z o.o. (Warsaw, Poland)

Responsible for maintaining and administering network infrastructure (switches, routers, firewalls, monitoring system etc.). Administrating of databases and web servers as well as developing web applications.

Specialties: Linux, Open/FreeBSD, Windows 98/2000/NT, Sophos, SonicWall, iptables/pf/ipf, Apache, bind, nagios, dBase/MySQL/PostgreSQL, perl/php/Delphi.

Jan. 1999 – Apr. 2000 *Senior IT Specialist*, Savings Bank of Ukraine (Zalishchyky, Ukraine)

Sep. 1996 – Dec. 1998 *IT Specialist*, IT Department at bank "Ukraina" (Zalishchyky, Ukraine)

Responsible for maintaining and administering database and file servers. Maintaining electronic payment system and mail system. Software development for internal usage.

Specialties: MS DOS/Windows 3.11/95/98, OS/2, Novell NetWare 3.12, Borland Pascal/Delphi

Education – Professional Training

- **1993 – 1999** - Chernivci National Yuriy Fedkovych University (mathematic)
- **2008 – 2009** - Postgraduate Studies "Effective IT Management and IT Governance", Warsaw School of Economics
- **2004 – 2022**
 - Various courses on "A Cloud Guru" and Pluralsight
 - CheckPoint Security Administration I / II NG (CCSA/CCSE), Provider-1 NGX
 - Crossbeam XOS Specialist (CBS-TRNG-XOS-L1), XOS Expert (CBS-TRNG-XOS-EXP)
 - Configuring Juniper Networks Firewall/IPSec VPN Products
 - Advanced Juniper Networks IPSec VPN Implementations
 - Interconnecting Cisco Network Devices (ICND Part 2)
 - Securing Networks with ASA Foundation (CCSP SNAF)
 - PaloAlto Bootcamp (PAN-EDU: Extended FW Management / Advanced FW Troubleshooting)
 - WireShark (TCP/IP Netzwerk Analyse)
 - BlueCoat Bootcamp (BCCPA, BCCPP, Director & Reporter)
 - F5: Bootcamp
 - Splunk – Splunk PowerUser level

Certificates

- AWS Certified Solutions Architect - Associate (SAA-C03)
- CompTIA Security+
- Certified Ethical Hacker (CEH)
- CheckPoint (ACE, CCSA, CCSE, CPSC)
- Crossbeam Systems Certified Expert (CSCE)
- Cisco (CCNA, CCDA)
- F5 (F5-CA)
- Fortinet: NSE4, NSE5
- Juniper Networks (JNCIA-JUNOS, JNCIS-SEC, JNCIS-FWV)
- Palo Alto Certified Network Security Engineer (PCNSE6)
- Tufin Certified Security Expert (TCSE)
- Skybox (STSP, SCSE)
- Zscaler: Private Access (ZCCA-PA), Internet Access (ZCCA-IA)

Other skills

Social:

- Attitude to live in common with other people
- Attitude to work and travel in international environment
- Ability of fast adaptation and learning
- Ability to work under pressure

Language:

- Ukrainian – native
- Polish – fluent as native
- English – advanced (C1)
- German – intermediate (A2)