Kalin KOZHUHAROV

Information Security Professional
CISSP, GCIH

Nationality:	Bulgarian	Address:	Storchenbuehl 4, 72336 Balingen, GERMANY
Date of birth:	1977-04-12 (45 y.o.)	TEL:	+49 159 0557-5411
Family status:	Married, with 2 kids	e-mail:	Kalin@KOZHUHAROV.de
Visas:	EU: Resident Japan: Permanent resident USA: Visitor (B1/B2)	profiles:	https://linkedin.com/in/kozhuharov https://angel.co/kalin-kozhuharov https://KOZHUHAROV.de/

SUMMARY

I "breathe" security daily: from physical/hardware, via software to people/organizations and risk-analysis. Given the vast landscape, this always keeps me interested, constantly researching and discovering. I routinely audit systems and processes, spot issues and suggest remediation (all in real-time). With over 10 years security experience and more in IT, I am confident finding a solution to any problem. I had to change several companies and jobs to discover and reconfirm that consulting is what I do best, in small teams or directly working with client staff. I am happy to discuss any security project or IT issue of yours - no matter how small or big. Since 2007 I have been focusing mostly on reactive security (incident response and digital forensics), followed by proactive security (consulting, remediation); I have performed a number of assessments/audits (PCI DSS, pentesting, new system design), including physical security.
I am registered as "KOZHUHAROV - IT Security Services" (self-employed in Germany) and am available 24/7 (best-effort). I bill hourly or per project and work on-site or remotely. I am also considering mostly remote/online full-time or near-full-time positions.

RECENT / NOTABLE POSITIONS AND CLIENTS

Exabeam
2021-12 .. 2024-01
[25 months, Full-time]
/Home-office, GERMANY/

Senior Project Manager, IT-Servicemanagement

I was leading various internal projects such as improving troubleshooting for the Support organization, improving specific features for the Product management organization, upgrading/improving the SaaS platform for CloudOps, etc. I have personally developed an internal CLI tool to standardize troubleshooting practices in Support and Engineering, for both on-premise and SaaS systems.
I was one of the few L3 Incident Commanders for production incidents. As such I have troubleshooted and resolved numerous large and complex production issues within short time.

Exabeam
2019-12 .. 2021-12
[25 months, Full-time]
/Home-office, GERMANY/

Technical Account Manager, EMEA

I was involved from the stage Sales talk to the customer through support and training and eventual up-sell. As a representative of the customer within Exabeam, I was coordinating all communications between Sales, Support, Development and Product Management. I organized training seminars and up-skill sessions for customers for specific features of the Exabeam platform as well as consulting them how to use it in their specific environment.

BroadBand Security, Inc. **2011-03 .. 2016-12** **[70 months, ~150 h/month]** **/Tokyo, JAPAN/**	**`Team Leader, Digital Forensics Team`** Although a contractor, I was leading the Digital Data Services, mainly focusing on Emergency Incident Response (firefighting), followed by Digital Forensics Investigations (deep investigations of cause and scope) and often Information Security Consulting (remediation). I spearheaded the "Splunk as Managed Security Service" for our MSS/SOC with a large and complex installation (from concept, purchase, setup to user training). We covered the all types of clients and industries from SOHO to big multinationals in bridal, mass-media, marketing research, gaming, manufacturing, power grid, banking, municipal, defense, etc. industries. Additionally, I was actively involved in PCI DSS related consulting and assessments across several continents and few data recovery assignments.
Deloitte Tohmatsu FAS Co., Ltd. **2009-03 .. 2011-01** **[23 months, full time]** **/Tokyo, JAPAN/**	**`SVP, Analytic and Forensic Technology`** I was hired to launch the Analytic and Forensic Technology service line in Japan for Deloitte, focusing on digital forensics. I successfully trained the assigned consultants and put together a digital forensics laboratory and established the new business practices. We assisted large-scale e-Discovery matters, provided technical support for forensic accounting and various other investigations (internal investigations, patent infringement, insurance disputes, etc.). On the side I assisted in large service provender's PCI DSS assessment.
Hill and Associates Japan Co., Ltd. **2007-10 .. 2009-02** **[17 months, full time]** **/Tokyo, JAPAN/**	**`Information Security Consultant`** 1. Information Security Consulting: internal controls (SOX/j-SOX, ISO27001) design, optimization and implementation consulting; wired/wireless network penetration testing and vulnerability assessment; application source code review; system design security assessment; physical security consulting 2. Payment Card Industry: VISA CVP external auditing; PCI DSS consulting and validation (QSA); PABP/PA-DSS consulting 3. Digital Forensics: locating, acquiring, indexing, searching and presenting digital evidence; data recovery

HIGHER EDUCATION

Hokkaido University **1999 - 2005** **[6 years, regular student]** **/Sapporo, Japan/**	**`M.E., Electronics and Information Engineering`** **`B.E., Information Engineering`** Master thesis: SSOS-WSA: "Development of a Self-configuring Stochastic Optimization System based on a Web Service Architecture" Activities and Societies: Academic Alpine Club of Hokkaido University, Sapporo Climbing Club

LANGUAGES

Mother tongue	`Bulgarian:`	`Fluent (daily used)`
Foreign languages	`English:`	`Fluent (30+ years of daily and professional use)`
	`Japanese:`	`Fluent (25+ years daily and professional use)`
	`Russian:`	`Fluent (often used professionally, since 1990)`
	`German:`	`Intermediate (improving, daily use since 2017)`

CERTIFICATIONS

CISSP	Sep 2013 – Sep 2019: License 436315
GCIH	Sep 2015 – Sep 2027: License 26198
PCI DSS QSA (exp.)	2008-2009, 2011–2013, 2014–2015: License 039-008

IT PROFESSIONAL SKILLS / TOOLS

Forensics	Intella, Volatility, Sleuthkit, Autopsy, F-Response, FTK, EnCase
SIEM	Exabeam, Splunk, Splunk ES, ELK/Grafana, Zeek, Moloch
Cloud	GCP, AWS
Operating systems	Linux(L+++$), Android (user/admin); Windows 2-7(user/admin),10-11
Programming	Fluent Perl (P+++$) and Bash, some Python; good C, some Java some VisualBasic, Pascal and x86 assembly; some JavaScript good MySQL, some PL/pgSQL; some R
Databases	MySQL, MongoDB, cdb
Web development	HTML, XML, XSLT, JavaScript; Linux/Apache/Perl/MySQL
Design / Graphics	Inkscape, GIMP, gnuplot, ffmpeg
CAD/CAM	FreeCAD, OpenSCAD, KiCAD
Office	LibreOffice, MS Office/ O365, gvim
SaaS tools	SalesForce/SFDC, JIRA, Confluence, DataDog
Remote tools	Zoom, MS Teams, TeamViewer, Webex, Slack, GoTo Meeting
(Linux) daemons	djbdns, qmail, apache, ntpd, fcron, sshd, vsftpd, cupsd, samba
hardware	x86, amd64, mips, arm7, avr; DIY electronics & sensors
misc. tools	wireshark, nmap, strace, gdb, wireguard, git, awscli, vim, rsync, make, parallel, ansible