Kalin KOZHUHAROV

Berater für Informationssicherheit
CISSP, GCIH

Staatsangehörigkeit:	Bulgarisch	Adresse:	Storchenbühl 4, 72336 Balingen, DEUTSCHLAND
Geburtsdatum:	1977-04-12 (45)	TEL:	+49 159 0557-5411
Familienstand:	Verheiratet, mit 2 Kinder	e-mail:	Kalin@KOZHUHAROV.de
Visa:	EU: Bewohner Japan: Aufenthaltserlaubnis USA: Visitor (B1/B2)	Profile:	https://linkedin.com/in/kozhuharov https://angel.co/kalin-kozhuharov http://KOZHUHAROV.de/

ÜBERBLICK

Ich "atme" Sicherheit täglich: von physischer / Hardware über Software bis hin zu Personen / Organisationen und Risikoanalysen. Das interessiert mich angesichts der riesigen IT-Landschaft immer wieder, ich recherchiere und entdecke immer neue Probleme und deren Lösungen. Ich überprüfe regelmäßig Systeme und Prozesse, entdecke Probleme und schlage Abhilfemaßnahmen vor. Mit über 10 Jahren Sicherheitserfahrung (und mehr in der IT Bereich) bin ich zuversichtlich, für jedes Problem eine Lösung zu finden. Ich musste mehrere Unternehmen und Jobs wechseln, um herauszufinden und zu bestätigen, dass Beratung ist, was ich am besten, in kleinen Teams oder in direkter Zusammenarbeit mit Kundenmitarbeitern, kann. Ich freue mich, jedes Sicherheitsprojekt oder IT-Problem von Ihnen zu besprechen - egal wie klein oder groß. Seit 2007 konzentriere ich mich hauptsächlich auf reaktive Sicherheit (Inzident Response und Digitale Forensik), gefolgt von proaktiver Sicherheit (Beratung, Fehlerbehebung). Ich habe eine Reihe von Bewertungen / Audits durchgeführt (PCI DSS, Pentesting, neues Systemdesign), einschließlich physischer Sicherheit.
Ich bin als "KOZHUHAROV - IT Security Services" (selbständig in Deutschland) registriert und rund um die Uhr erreichbar (nach bestmöglichem Bemühen). Ich berechne stündlich oder pro Projekt und arbeite vor Ort oder als Fernarbeit. Ich erwäge auch manchmal spezifische Vollzeitstellen (nur Fernarbeit).

LETZTE / BESONDERE POSITIONEN UND KUNDEN

Exabeam — **Senior Project Manager, IT-Servicemanagement**

2021-01 .. 2024-01
[24 Monate, Vollzeit]
/Home-office, DEUTSCHLAND/

Ich habe verschiedene interne Projekte geleitet, wie z. B. die Verbesserung der Fehlerbehebung für die Support-Organisation, die Verbesserung spezifischer Funktionen für die Produktmanagement-Organisation, die Aktualisierung/Verbesserung der SaaS Plattform für CloudOps usw. Ich habe persönlich ein internes CLI-Tool entwickelt, um Fehlerbehebungspraktiken im Support zu standardisieren Engineering, sowohl für On-Premise- als auch für SaaS-Systeme.
Ich war einer der wenigen L3-Vorfallkommandeure für Produktionsvorfälle. Als solcher habe ich innerhalb kurzer Zeit zahlreiche große und komplexe Produktionsprobleme behoben.

Exabeam — **Technical Account Manager, EMEA**

2019-12 .. 2021-12
[24 Monate, Vollzeit]
/Home-office, DEUTSCHLAND/

Ich war für über 40 Kunden in EMEA verantwortlich. Ich war von der Phase des Verkaufsgesprächs mit dem Kunden über den Support und die Schulung bis hin zum eventuellen Upselling beteiligt. Als Vertreter des Kunden bei Exabeam koordinierte ich die gesamte Kommunikation zwischen Vertrieb, Support, Entwicklung und Produktmanagement. Ich habe Schulungsseminare und Fortbildungsveranstaltungen für Kunden zu spezifischen Funktionen der Exabeam-Plattform organisiert und sie darüber beraten, wie sie diese in ihrer spezifischen Umgebung nutzen können.

BroadBand Security, Inc.
2011-03 .. 2016-12
[70 Monate, ~150 Stunde/Monat]
/Tokio, JAPAN/

Team Leader, Digital Forensics Team

Obwohl ich ein Auftragnehmer war, leitete ich die Digitalen Datendienste, wobei ich mich hauptsächlich auf "Brandbekämpfung" konzentrierte, gefolgt von Digitale Forensik Untersuchungen (eingehende Untersuchungen zu Ursache und Umfang) und häufig Informationssicherheitsberatung (Sanierung). Ich leitete den "Splunk as Managed Security Service" für unseren MSS / SOC mit einer großen und komplexen Installation (von der Konzeption, dem Kauf, dem Setup bis zur Anwenderschulung). Wir haben alle Arten von Kunden und Branchen abgedeckt, von Selbständige bis zu großen multinationalen Unternehmen in den Branchen Braut, Massenmedien, Marktforschung, Spiele, Produktion, Stromnetz, Bankwesen, Kommunalwesen, Verteidigung usw. Darüber hinaus war ich aktiv an der Beratung und Bewertung im Zusammenhang mit PCI DSS auf mehreren Kontinenten sowie an einigen Datenwiederherstellungsaufgaben beteiligt.

Deloitte Tohmatsu FAS Co., Ltd.
2009-03 .. 2011-01
[23 Monate, Vollzeit]
/Tokio, JAPAN/

SVP, Analytic and Forensic Technology

Ich wurde beauftragt, für Deloitte die Servicelinie für Analytik und Forensik in Japan mit dem Schwerpunkt auf digitaler Forensik zu gründen. Ich habe die beauftragten Berater erfolgreich ausgebildet, ein Digitaleforensiklabor aufgebaut und die neuen Geschäftspraktiken etabliert. Wir unterstützten umfangreiche E-Discovery-Angelegenheiten, leisteten technischen Support für die forensische Buchhaltung und verschiedene andere Untersuchungen (interne Untersuchungen, Patentverletzungen, Versicherungsstreitigkeiten usw.). Nebenbei habe ich bei der PCI-DSS-Bewertung eines großen Dienstleisters mitgewirkt.

Hill and Associates Japan Co., Ltd.
2007-10 .. 2009-02
[17 Monate, Vollzeit]
/Tokio, JAPAN/

Information Security Consultant

1. Informationssicherheit Beratung: Interne Kontrollen (SOX / j-SOX, ISO27001) Design, Optimierung und Implementierung Beratung; Penetrationstests für verdrahtete / drahtlose Netzwerke und Schwachstellenanalysen; Überprüfung des Quellcodes der Anwendung; Sicherheitsbewertung des Systemdesigns; physische Sicherheitsberatung
2. Zahlungskartenindustrie: Externe VISA CVP-Prüfung; PCI DSS Beratung und Validierung (QSA); PABP / PA-DSS-Beratung
3. Digitale Forensik: Auffinden, Erfassen, Indizieren, Suchen und Präsentieren digitaler Beweise; Datenwiederherstellung

SCHULBILDUNG

Hokkaido University
1999 - 2005
[6 Jahre, regulärer Schüler]
/Sapporo, Japan/

M.E., Electronics and Information Engineering
B.E., Information Engineering

Magisterarbeit: SSOS-WSA: "Development of a Self-configuring Stochastic Optimization System based on a Web Service Architecture"

Aktivitäten und Gesellschaften: Academic Alpine Club of Hokkaido University, Sapporo Climbing Club

SPRACHEN

Muttersprache Bulgarisch: fließend (täglicher gebraucht)

Fremdsprachen

Englisch: fließend (30+ Jahre täglicher/professionelle Gebrauch)
Japanisch: fließend (25+ Jahre täglicher/professionelle Gebrauch)
Russisch: fließend (oft beruflich eingesetzt, seit 1990)
Deutsch: B2 (wird verbessert, täglicher gebraucht seit 2017)

ZERTIFIZIERUNGEN

CISSP	Sept 2013 – Sept 2019: Lizenznummer 436315
GCIH	Sept 2015 – Sept 2027: Lizenznummer 26198
PCI DSS QSA (abgelaufen)	2008-2009, 2011–2013, 2014–2015: Lizenznummer 039-008

IT FÄHIGKEITEN

Forensik	Intella, Volatility, Sleuthkit, Autopsy, F-Response, FTK, EnCase
SIEM	Exabeam, Splunk, Splunk ES, ELK/Grafana, Zeek, Moloch
Cloud	GCP, AWS
Betriebssysteme	Linux(L+++$), Android (user/admin); Windows 2-7(user/admin),10-11
Programmierung	fließend Perl (P+++$) und Bash, bisschen Python; gute C; bisschen Java, VisualBasic, Pascal und x86 Assembler; bisschen JavaScript gute MySQL, bisschen PL/pgSQL; bisschen R
Datenbanke	MySQL, MongoDB, cdb
Webentwicklung	HTML, XML, XSLT, JavaScript; Linux/Apache/Perl/MySQL
Design / Graphik	Inkscape, GIMP, gnuplot, ffmpeg
CAD/CAM	FreeCAD, OpenSCAD
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
verschiedene	wireshark, nmap, strace, gdb, wireguard, git, awscli, vim, rsync, make, parallel, ansible