コジュハロフ・カリン
KOZHUHAROV, Kalin

情報セキュリティ専門家　CISSP, GCIH

国籍: ブルガリア

生年月日: 1977 年 4 月 12 日 (45 才)

家族: 結婚、子供二人

ビザ: EU: Resident
日本: 永住者
USA: Visitor (B1/B2)

住所: Storchenbuehl 4, 72336 Balingen, GERMANY

TEL: +49 159 0557-5411

e-mail: Kalin@KOZHUHAROV.de

プロフィール: https://linkedin.com/in/kozhuharov
https://angel.co/kalin-kozhuharov
http://KOZHUHAROV.de/

概要

私は毎日のようにセキュリティを「呼吸」しています：ハードウェア・物理セキュリティ、ソフィとウェアセキュリティ、人・組織のセキュリティやリスク分析。膨大な分野であるため、何時も興味を持ち、常に研究し、発見しています。私は日常的にシステムやプロセスを監査し、問題点を特定し、改善を指摘する（リアルタイム）。10 年以上のセキュリティ経験と IT 分野で長い経験を元に、私は自信をもって、あらゆる問題に対する解決策を見つけることができます。いくつかの企業や仕事類を経験し、コンサルティングが一番得意であることを分かりました：小規模なチームまたはクライアントのスタッフと直接に緊急な課題を解決すること。どんなに小さくても、大きくても、貴社のセキュリティプロジェクトや IT 関連の問題について話をさせてください。2007 年以来、主に反応的なセキュリティ（インシデントレスポンスやデジタルフォレンジック）に焦点を絞り、一部の先進的なセキュリティサービス（コンサルティング、修復）も提供しています。そして、物理的なセキュリティを含め、評価/監査（PCI DSS、ペンテスト、新しいシステム設計）も実施しています。

現時点では、ドイツ国での自営業として「KOZHUHAROV – IT Security Services」を 24/7 (ベストエフォート)のサービスを提供しています。時間制またはプロジェクト毎での請求が行い、オンサイトまたはリモートでのサービスとなります。現在は、リモートでできるフルタイムのポジションも検討しています。

最近のポジション

Exabeam	**シニア プロジェクト マネージャー、IT サービス管理**
2021 年 12 月～2024 年 1 月 **[25 ヶ月、フルタイム]** **/ホームオフィス、ドイツ/**	サポート組織のトラブルシューティングの改善、製品管理組織の特定の機能の改善、CloudOps の SaaS プラットフォームのアップグレード/改善など、さまざまな社内プロジェクトを主導していました。サポートでのトラブルシューティングの実践を標準化するための社内 CLI ツールを個人的に開発しました。それにより、オンプレミスや SaaS システムの両方の統括トラブルシューティングが可能になりました。 本番インシデントの数少ない L3 インシデント コマンダーの一人として、多数の大規模・複雑な運用上の問題を短期間で確定し、解決してきました。
Exabeam	**テクニカル アカウント マネージャー、EMEA**
2019 年 12 月～2021 年 12 月 **[25 ヶ月、フルタイム]** **/ホームオフィス、ドイツ/**	顧客開拓の段階サポートとトレーニング、そして最終的なアップセルを通じた顧客へのセールストークの段階から関与しました。 Exabeam 内の顧客の代表として、私は販売、サポート、開発、製品管理の間のすべてのコミュニケーションを調整していました。 私は、顧客向けに Exabeam プラットフォームの特定の機能に関するトレーニング セミナーやスキルアップ セッションを企画し、特定の環境での使用方法についてコンサルティングを行いました。

株)ブロードバンドセキュリティ	**チームリーダ、デジタルフォレンジックチーム**
2011 年 3 月～2016 年 12 月 **[70 ヶ月、約 150 時間/月]** **/東京, 日本/**	顧問として、デジタルデータサービス部の設立・拡張し、セキュリティ緊急対応サービス、デジタルフォレンジック調査、(一部のケース)情報セキュリティコンサルティング(改善支援など)を提供しました。「Splunk 運用・分析サービス」を先導し、大手企業での大規模なシステムを導入しました(コンセプト、購入、セットアップ～ユーザートレーニングなど)。様々な業種(ブライダル、報道、マーケティングリサーチ、オンラインゲーム、製造、電力網、銀行、地方自治体、防衛、など)と幅広い企業サイズ(SOHO～国際大手企業や政府機関)での顧客ベースでした。さらに、私は PCI DSS に関連したコンサルティングや評価に積極的に関わっていました。
デロイト・トーマツ FAS	**SVP, Analytic and Forensic Technology**
2009 年 3 月～2011 年 1 月 **[23 ヶ月、フルタイム]** **/東京, 日本/**	私の雇用の目的は、日本での「Analytic and Forensic Technology」サービスを設置することでした。私は割り当てられたコンサルタントを順調に訓練し、デジタルフォレンジックラボを設立し、新しいビジネスプラクティスを精巧しました。大規模な e ディスカバリープロジェクトを支援し、フォレンジック会計やさまざまな調査(内部調査、特許侵害、保険紛争など)の技術サポートを提供しました。そして、大手サービス提供者の PCI DSS アセスメントにも関わっていました。
Hill and Associates Japan Co., Ltd.	**情報セキュリティコンサルタント**
2007 年 10 月～2009 年 2 月 **[17 ヶ月、フルタイム]** **/東京, 日本/**	* 情報セキュリティコンサル:内部統制(SOX/j-SOX、ISO27001)デザイン、最適化、実施;有線・無線ネットワークのペンテストや脆弱性診断;ソース・コード・レビュー;市 S 手無デザイン;システムデザインのセキュリティ監査;物理的セキュリティコンサル * カード決済業界:VISA CVP 外部監査;PCI DSS コンサルや審査(QSA);PABP/PA-DSS コンサル * デジタルフォレンジック:デジタル証拠の見付だし、保全、インデクス化、検索と提供;データ復旧

教育

北海道大学 **1999 ～ 2005** **[6 年間、学部生・大学院]** **/札幌、日本/**	**工学研究科　電子情報工学専攻　修士課程** **工学部　情報工学科　学士(工学)** 修士論文:SSOS-WSA: ″Development of a Self-configuring Stochastic Optimization System based on a Web Service Architecture″ 部活:北大山学部、札幌クライミングクラブ

言語能力

母国語	ブルガリア語:	流暢(毎日利用)
外国語	英語:	流暢(30 年以上の業務・生活用)
	日本語:	流暢(25 年以上の業務・生活用)
	ロシア語:	流暢(折々業務用、1990 年以降での利用)
	ドイツ語:	中(毎日利用、2017 年以降)

証明書

CISSP	2013 年 9 月～2019 年 9 月 :ライセンス番号 436315
GCIH	2015 年 9 月～2027 年 9 月 :ライセンス番号 26198
PCI DSS QSA (exp.)	2008 年～2009 年、2011 年～2013 年、2014 年～2015 年:ライセンス番号 039-008

IT 専門スキルやツール

フォレンジック	Intella, Volatility, Sleuthkit, Splunk, F-Response, FTK, EnCase
SIEM 関連	Exabeam, Splunk, Splunk ES, ELK/Grafana, Bro, Moloch
Cloud	GCP, AWS
OS	Linux (L+++$), Android (ユーザ/管理者); Windows 2-7(ユーザ/管理者), 10-11
プログラミング言語	流暢な Perl(P+++$)と Bash、中 Python; 上級 C、 中級 Java 初級 VisualBasic、Pascal と x86 assembly; 中級 JavaScript 上級 MySQL、初級 PL/pgSQL
データベース	MySQL, MongoDB, cdb
Web 開発	HTML, XML, XSLT, JavaScript; Linux/Apache/Perl/MySQL
デザイン	Inkscape, GIMP, gnuplot, ffmpeg
CAD / CAM	FreeCAD, OpenSCAD, KiCAD
オフィス系	LibreOffice, MS Office / O365, gvim
SaaS ツール	SalesForce/SFDC, JIRA, Confluence, DataDog
リモートツール	Zoom, MS Teams, TeamViewer, Webex, Slack, GoTo Meeting
(Linux) デーモン	djbdns, qmail, apache, ntpd, fcron, sshd, vsftpd, cupsd, samba
ハードウェア	x86, amd64, mips, arm7, avr; 自作電子回路やセンサなど
その他	wireshark, nmap, strace, gdb, wireguard, git, awscli, vim, rsync, ansible