

Dr. Bernard Robert Bowitz (Dipl. Ing., CISSP, AISP, MCP, ITIL, BSI100, GDPR, EGDPR, ISO27001, Splunk,..)



Curriculum Vitae 2019 in deutsch

Go to english CV version:
http://seurescrypt.com/team-pictures/CV_EN_BB.pdf

Derzeitige Anschrift

aktuell: 65185 Wiesbaden, Germany (German National)
und
remote: PR (Permanent Resident) 757487 Singapore

Kontakte

Deutschland : +49-1711638089 / +4961169667879
Email: bernardbowitz@gmail.com, robertbowitz@gmail.com ,
info@seurescrypt.com
Webseite: <http://seurescrypt.com>
Fuer Singapore: Phone +65-90090296

Website/References

Projekt Management – Cyber Sicherheit – Networks – Clouds

<http://seurescrypt.com> Head of : <http://software-consultants.net>

Blockchain/References

<http://ehalal.eu> , <http://sentosaxchange.com>

Projekt Manager-Berater, Projekt Management Office, Technischer Projekt Manager, von Konzept erstellung bis Anwendung

Fachliche Schwerpunkte

Zusammenfassung

Mehr als 20 Jahre, arbeite (Mehrsprachig, Deutsch, English, basic Chinese) Operative und nicht Operative, Analytisch und Administrativ, Development und Process Entwicklung, Projekt Leitung, Fuehrung von multinationalen Teams jeder Groesse, langjaehrige Erfahrung in unter anderen in Bereichen wie Rechenzentrum, Netzwerke, Mainframe, Oracle, Unix, Linux, Windows (Zertifiziert), Infrastructure Management, ISMS/ISO27001/27005-2013, BSI100..XX , Schulungen, CISSP, AISP, ISO certified, IT Consulting, IT / Cyber /Netzwerk Security (Encryption, PKI), BSI 100, BSI Security Tools, Grundschatz, Netzwerke (Mobil (LTE, 2G,3G,4G,...), Ethernet, Wireless), VoIP Netzwerke (z.B. Avaya, Cisco...) Cloud Sicherheit und Administration, oeffentliche Netzwerke, DOI, IVBB, IVBV, VPN, Project Management, Endpoint Security (Genua, Sina, Checkpoint...), SOC, Blockchain und eCoin, arbeite mit jeder Plattform (Windows, Mainframe, Unix, Linux, Oracle usw.), CyberArk (von Konzept bis Anwendung und Implementation), Qradar Konzept, Erweiterung, Anwendung, Clouds ...

Einzelheiten

Habe seit 2014 erfolgreich mehrere ISMS/ISO 27001/BSI 100 Zertifizierungen durchgefuehrt. Bin CISSP, CISA, MCP , AISP, BSI und andere zertifiziert. Spreche English als 2 Muttersprache, sowie Chinesich Basic, Spanisch Umgangssprache.

Experte in RZ Migrationen, Hardware und Software, Entwicklung von Sicherheit basierend auf BSI Grundschatz. Vergangene Projekte

Referenzen: DB Netz, BAMF, BA, Atos, VWFS, CGI, OCBC, DBS, IBM, Credit Suisse Forst Boston, BSI, BDR, Cisco, Deutsche Bank, Bundesbank, EZB, Telefonica, NTT, Juniper, BWI usw.

Fuehre Schulungen ueber den neusten Stand des Grundschatzes durch.
Prozess Erstellung fuer SOC und SIEM.

Ich bin ein leitender Netzwerksicherheit Fachmann (CISSP) mit einem breiten Verstaendnis der Technologie und der zugeordneten Applikationen . Meine Erfahrung erstreckt sich ueber beide Bereiche , Mobilfunknetze und traditionelle Netzwerke .

„State of the Art“ Security Architectures, BSI IT-Grundschatz, ISO 27001, ISO 80001, IT Sig, Relevant Security in Bundes Agenturen – SG – Bamf- EHR-BDR und andere, Enterprise Security.....

Meine Schwerpunkte sind alle Aspekte rund um die IT und TK (Telekommunikation) Sicherheit von Basistechnologie bis zur Anwendungsschicht. Das bedeutet, von der Hardware zur Software-Entwicklung und Consulting- und Beratungsdienstleistungen. Vor allem in den letzten Jahren arbeitete ich in der Infrastruktur und mobilen Sicherheitsumgebung von Big Data mit dem Ziel von Analytics-Technologien für neue Analysekonzepte und zur aktiven Suche nach Sicherheit Anomalien um Angriffe zu verhindern und zu reduzieren.

Die besondere Stärke liegt in dem mobilen Bereich, Android/iOS, Entwicklung von sicheren Applikationen im Zahlungsverkehr und e-commerce sowie komplexen Netzwerkstrukturen, Big Data, Cloud Sicherheit, SIEM, Endpoint Security und vortschrittlicher Sicherheit, im praktischen wie im administrativen Umfeld.

Zertifikationen

CISSP, AISP, CISA, CISM, MCP, ITIL, Prince2, ISO27001, BSI GRUNDSCHUTZ, EGDP, GDPR, CyberArk, Qradar, Cloud (AWS, Azure, private Clouds, Blockchain), PhD

Ich nutze meine Stärken und sehr breite Erfahrungen für...

- Hilfe und Support für Kunden die richtigen Geschäfts- und Technologielösungen zu finden, durch die Arbeit als Berater und Konsultant fuer Design trend-setting security architectures
- Leite Projekte zum gewünschten Erfolg durch die Arbeit als Projektmanager
- Unterstützung der Unternehmens Forschungsabteilungen um neue Marktlösungen zu finden, um Umsatzwachstum und Gewinn auf den Gebieten zu erzielen
- Prozess Erstellung fuer die Einrichtung von SOC, SIEM, ISMS, IAM, PAM, PAS, CISO, Blockchain Security usw.
- Entwicklung neuer Produkte und Dienstleistungen (Software und Hardware), IT und TK
- Unterstützung von Verkauf und Marketing zur position von Produkten und Dienstleistungen in zukuenftigen Maerkten
- Training und Erstellung von hochleistungs Dienstleistungs Teams um alle auch noch so anspruchsvolle Aufgaben der Industrie im Griff zu haben
- Risk & Compliance Management

Industrie Erfahrung

- Banking – Sicheres Banking via Internet – Smart Card Zugänge
- Automotive – GPS – interne Elektronik
- Transport und Verkehr, Energie, GSM-R
- Test und Zertifikation, BSC, MSC, BSS, NSS
- (E)Regierung – eBanking – eUnternehmen
- Source code analysis, adaptations, extensions, corrections
- Risk management, risk / residual risk analysis
- IBM (Qradar), HPe ArcSight, McAfee ePO, Kaspersky, MicroSoft Security, CyberArk, Sophos, EndpointSecurity
- IT / TK technology - for large industry and consumers
- Large networks, industry and the public sector
- Wireless and mobile (Android, Windows) networks
- Creation of documentation, support solutions
- Prototype design, manufacturing management
- PMO/PM, Project Management, Big Data, Scrum, Kanban, MS
- Creation of test environments and necessary tools

Technology Fachwissen

- - Experte für privilegierte Zugriffssicherheit (PAM, PSM, EPV, CPM, PVWA), eine kritische Schicht der IT-Sicherheit zum Schutz von Daten, Infrastruktur und Ressourcen im gesamten Unternehmen, in der Cloud und in der gesamten DevOps-Pipeline
- - Quellcode Analyse, Anpassungen, Erweiterungen, Korrekturen
- - IAM, SAM, PAM, GRC, AMR4V, Frontdesk, CyberArk, Qradar,...
- - Qradar, TheHive, Cortex, NexPose, MISP, zAlert....
- - Java, C++, SQL
- - PKI, SSL, MS NDES, SafeNet Networks HSM
- - Cloud Azure, AWS, Strato, Telecom, SaaS, LaaS, XaaS.....
- - Risk management, Risiko / Rest Risiko Analyse, GRC
- - HPe ArcSight, McAfee ePO, Kaspersky Sicherheit, HiScout GRC Suite, MSS,...
- - Mainframe, Windows, Linux, Unix, Oracle,
- - IT / TK Technologie – für Groß Industrie und Verbraucher
- - Große Netzwerke, Industrie und Öffentlicher Sektor
- - Drahtlose und Mobile (Android, Windows) Netzwerke
- - Erstellung von Dokumentationen, Support Lösungen
- - Prototype Entwurf, Herstellung Management
- - Project Management, Big Data, Scrum, Kanban, MS, PMO
- - Erstellung von Testumgebungen und notwendigen Tools

Hardware Fachwissen

- - 2015, entwickelt, den ersten tragbaren Passport –Scanner auf Android core, mit integriertem Multi Fingerabdruck -Scanning für Grenzpatrouillen , die Registrierung der Asyl Flüchtlinge , Polizei, BKA , Sicherheitskräfte , Banken
- - Semiconductors, Chip sets – design und embedded Software Mobile Hard – und Software – insbesondere neueste Cyber Security mit speziellem Chip basierten Algorithmus, AES 256 , Diffie-Hellmann PKI
- - Identifizierung mit Biometrie (Fingerabdruck ,patentierte Hoch Sicherheitslösung Nurugo)– Sicherheit basierend auf neuer SIM Karten Technologie ...
- - Java, Json
- - Cloud Sicherheit – SaaS - Unternehmen – Regierung – öffentliche Dienste – Militär - Endpoint Security
- - **Azure und AWS cloud migrationen, von Konzept zur Implementation**
- - Internet Verkehr – Zugangs Identifikation
- - Sicher Transaktionen – UAF Zugang ohne Passwörter – Spezielle Militär klassifizierte Sicherheit
- - NFC- Smartcard
- - Forschung und Entwicklung , Software-Entwickler , Hardware Entwickler
- - IP – VoIP Netzwerke, Sprache, Nachrichten, Daten, Video
- - Neue Technologien basierend auf SIM und SD Karten, Identifizierung ohne Passwörter
- - Analyse von Netzwerk Sicherheit,Riskmanagement, Risiko Analyse, Jagd auf Cyber Kriminelle und Hacker
- - Persönliche Sicherheit – Biometrie – CCTV Systeme mit Biometrie Erkennungs Methoden
- - Neuartige hoch Sicherheits Lösungen für HR und sonstige Anwendungen mit Mobil Geräten
- - Blockchain Netzerk Sicherheit und Applikationen
- - Entwicklung eines SIEM SOC, vom design zur implementierung (einschl. IBM Qradar und TheHype/Cprtex) integration

Rollen

Enterprise Projektleiter / Projektmanager / MS-Project PMO / Administrator / Sicherheits Auditor (27001 /BSI)
Technischer PM mit „Hands On „
DVSGO Berater nach EU Grundschutzlinien
Software-Entwicklung / Programmierung / Hardware design / Netzwerk Architektur
Beratung / Consulting / Hands On / Technischer PM
Projektmanagement / -leitung / Organisation / Koordination/ PMO
Teamleitung von Teams bis zu 80 Mitgliedern, Global, vor Ort und Remote
Engineering / IT-nahe Ingenieurdienstleistungen

Kommentar

Als Experte für IT Sicherheit in festen und mobilen Netzen, habe ich in den letzten Jahren Projekte unter BSI 100, ISO 27001 , zertifizierung von öffentlichen Netzen unter ISMS usw. durchgeführt. Mehr als 15 Jahre Erfahrung in IT Sicherheit , Projektleitung, Audit, Analyse usw. Speziell habe ich bei der Einrichtung mehrerer SOC/SIEM beraten und praktisch mitgearbeitet.

Detaillierte Kenntnisse in den Projekt Beschreibungen aktualisiert!

Ich habe tiefe Kenntnisse des Geheimschutz Buches(GB) des BMWI sowie DSGVO , EUGDPR und baue viele meiner Projekte auf die Vorgaben des GB auf.

White Papers (copyright 2019 Dr. Bernhard Bowitz, download and copy not allowed) samples only:

[IT Security planned, managed effectively](#) – [Build a SOC with Open source](#) - [Public Cloud Security](#) - [The art of IT error reporting](#) - [Process Modeling](#) - [ISMS Governance](#) - [DLP-Richtlinien](#) - [Cloud-IAM](#) - [An Overview of Cryptography](#) - [CyberSecurity vs. IT Security](#) - [Introduction of an ISMS under ISO 27001 \(German\)](#) - [ESA definition](#) - [Introduction of an ISMS under ISO 27001 \(English\)](#) - [MSS / Managed Security Services](#) – [CASB](#) - [Security Information and Event Management](#) - [SIEM](#) - [SIEM-SCRUM](#) - [Telephone knowledge](#)

Projekte – berufliche Laufbahn

04/2019 – laufend

Hauptprojekt Leiter – Cyber Security (Cyber Ark, PAM, IAM, SIEM , SOC , Datacenter, Applications , – Planung – Implementation

Verantwortlich fuer 3 Teilprojekte, CyberArk Zugriffsschutz, Windows, Mainframe, Oracle Datenbanken, Enterprise Firewalls

Verantwortlich fuer Budget Planung, Ueberwachung, Technologie, Applikationen

Von Planung bis Implementation, weltweit

Direkt verantwortlich gegenueber Geschaefsfuehrung fuer alle Phasen einschlieslich operational.

Verhandlungssicher mit Lieferanten und Dienstleistern

Projekt Aufgaben mit direkter technischer Verantwortung und hands on:

- CyberArk, Antivirus Solutions, PMS, Wallet, Vaults
- MS Windows Server 2008 R2 and höher, Mainframe, Unix, Oracle, SAP
- Microsoft Active Directory + ADFS, LDAP,...
- TCP/IP, DNS, LAN/WAN, Client/Server, Monitoring
- Scriptsprachen und Programmierung (z.B. Powershell, Perl, Python)
- Arista, Netscaler
- RedHat Enterprise Linux, QRadar, SAP
- Azure / AWS Stack
- Hyper-V inkl. Storage Spaces direct, Microsoft SCOM, Oracle, SQL
- Hardware X86/X64-basierend (RAID, LAN, etc.) e.g. HPE Apollo Hardware
- Kompetenz (z.B. ITIL, ISO9001, IS rules, DevOps concept, Agile, Scrum, MS Office, MS Project)

9/2018- 03/2019

Projektleiter, PMO, Technischer PM (Financial Industrie)

Entwurf, Entwicklung Implementation eines Europa weiten Security System fuer die EZB im 4CB Netzwerk (Zentral Banken Italien, Spanien, Franreich, Deutsche Bundesbank) mit zentraler SIEM SOC Anbindung fuer die EZB und die 4CB Networks der Deutschen Bundesbank, Central Banks of Italy, Spain, France.

Integration und Anpassung an BAIT (Bankfachliche Anpassung an IT), beachtung der MaRisk Fassung von 2017 , laut Bafin definierte system relevanten Institute.

Betrieb in der Cloud

QRadar Konsole, zAlert, SIEM Interfaces UBA, NexPose, TheHive, DFIR, SIEM Console, SIEM Event Processor, Flow processor, CTI, SecLog, SecMon, beachtung von IDW audits, verschiedene Malware Scanner.

Vulnerability Scanner, APT, IDS/IPS, Network Security Monitoring, AV, VM, MISp, VAMP ,NetWork Insights.

Trendmicro Software implementation, BlueCoat (Symantec) CAS - Mainframe and Windows Infrastructure, Linux.

Hilfsmittel Micro Focus, Splunk, Fireeye- ArcSight, NetIQ. Verschiedene Audit Tools, Script und Software Python, JS, Perl, Powershell, Java.

Komplette Erstellung in MS-Project. MS-Planning, WBS-Entwuerfe unter Verwendung von Word, Excel, Visio, SharePoint, unter zuhilfe von ITIL V3, PulseSecure, Tanium, Prince 2 und Sparx.

Entwicklun eines SIEM Handbuch und Security Operation Manual

Hilfsmittel und Projekt Vendoren: AgileSI, BlueLiv, CheckPoint, CyberArc, Exabeam, Cylance, ForeScout, F5, Resilient (IBM), LasLine, LogRhythm, PaloAlto, Nozomi Networks, ProofPoint, SIEMPLIFY, SecureMatters, Sophos, SkyHigh, Synack, Tenable, Vectra.

Schulungs Konzepte

Operativ und Administrativ

Aufbau des kompletten Testsystems mit Sandbox (Cuckoo)

Aufbau des 4 Region Europaeischen Central Bank Netzwerkes mit Anbindung an die Europaeische Zentral Bank.

System Zertifizierung nach BSI, 27001, 27002

Anschluss Projekt (Project Plan in MS Project):

Segmentierung der Infrastrycture Architektur fuer Cloud Migration

Vorbereitung zur Migration nach Azure und AWS cloud.

Proof of Concepts - Unterstuetzung und Beratung

Cloud Governance

Cloud-Readiness-Assessment

Cloud Vision und Strategie

Cloud Onboarding

Technische Implementierung

Abschluss Dokumentation

11/2017-10/2018

MNC , Global Project Manager und PMO (Telco Industrie fortsetzung)

Architecture, planning, integrating of a complete global new DLP, ATP, EDR, AntiDDoS system, over networks, clouds enterprise wide.

Implementing ISMS, SIEM with SOC. **Vorbereitung einer cloud migration.**

Using agile approach

Splunk

For all Platforms

- Durchfuehrung von Soll und IST Status im Bereich IT Sicherheit – besonders O 365 –Cloud DLP, EDR, AntiDDoS
- Anti Malware APT email, Data, Security Protection
- Drafting eines neuen Sicherheits Konzeptes nach den neusten DSGVO und EUGDPR Richtlinien, ISO 27001, 27002
- HLD Governance
- Erstellen eines neuen Riskmanagement Framework
- Pflege der vorhandenen Tools, Einfuehrung eines neue Tools (Symantec, Check Point)
- Beratung , Umsetzung, Implementation der neuen Tools
- Erstellung von Reports
- Komplettes Projekt Management
- Training der internen Ressourcen
- Vendor und Systems Integrator Management

PM fuer Projekt 2

Implemetierung und Konfiguration einer Priviledged Access Management Loesung und **Cloud Migration**

Skills:

- Priviledged Access Management (PAM)
- Identity and Access Managemet (IAM)
- Netzwerk und Infrastruktur Architekt
- CyberArk und/oder Beyond Trust
- ISO und BSI Sicherheits Grundlagen/Zertifizierung
- Prozessmodellierung
- Erstellung von Dokumentationen
- MS Project, Office
- Retina Vulnerability Management oder anderer Tools
- Discover network, web, mobile, cloud, virtual, Docker images and IoT Infrastructure
- Profile asset configuration and risk management
- Pinpoint vulnerabilities, malware and attacks
- Manage SOC
- Analyze threat potential and return on remediation
- Remediate Vulnerabilities via integrated patch management
- Report on vulnerabilities, compliance, benchmarks
- Protect endpoints against client-side attacks
- Make logical and analytical informed privileged decisions

Vorbereitung zur Azure Migration

- Entwicklung und Migration zur Azure-Cloud
- Konzeption, Planung, Beratung sowie Technischen Umsetzung und RollOut
- Erstellen von Strukturen
- Cloud Anbindung an Office 365, Mail Exchange
- Decentralized identity ,DevOps, E-commerce, Sharepoint,
- Openshift, Red Hat Container Application Platform
- Kubernetes open-source system for automating deployment, scaling, and management of containerized applications
- Workshop and Training of internal resources
- Documentation

2018-- Gruendungsmittglied und Board Member DEFENSOR, Die erste SaaS Blockchain Netzwerk Sicherheit NaaS / PaaS / Ddos Tools

Project Manager (Telco Industry)

Einrichten eines neuen ISMS, Information Security Management System - part of the overall management system, based on business risk approach to establish, implement, operate, monitor, review, maintain and improve information security

Erstellen und Einfuehrung der neusten Sicherheits Richtlinien des "Geheimhaltungshandbuch" des Ministeriums fuer Wirtschaft und Technology und der neusten Vorgaben des DSGVO und EUGDPR

(Beginn PM2)

Erstellen einer Cloud Architecture, Paas, IaaS, SaaS, Vorbereitung zur Azure Migration in Projekt 2

Erstellen einer Blockchain Sicherheits Infrastruktur

- Konzipierung des ISMS
- Einführung eines (BC) Information Service Management Systems
- Development of a BC Network Security Application
- Development of the first Financial / Investment Banking Application Management Service
- Sicherheits Konzept fuer die Einrichtung und Inbetriebnahme eines neuen Daten Zentrums. Angepasstes Sicherheits Konzept, Audit der vorhandenen Infrastruktur, Entwurf des neuen high Level Designs und Architektur. Abschliessende Beurteilung und Vorbereitung fuer notwendige Zertifizierungen.
- Spezifikation aller Sicherheits Massnahmen
- Zusammenarbewit mit internen Teams
- Entwicklung von neuesten Sicherheits Komponenten

05/2017 – (15 April 2018) 11 Monate (Finanz Industrie)

Project Manager Security Compliance in Big Data (Bank / Government) Network

Erstellen eines Konzeptes fuer das ISMS unter Beachtung von DSGVO

Mainframe, Windows, Oracle, Solaris, Linux, DB-Unity, DB-Symphony, Remedy, CMBD, IBM-Maximo, Customer – Vendor Relations, confirmation of IBM Security products, Entwicklung eines SIEM

Security Compliance Management, IAM, SAM , AMR4V Process / Cloud Migration

Projektleiter für ein globales Netzwerk von ca. 25.000 Server und Datenbank

Einführung eines ISMS unter Beachtung der neusten DSGVO und EUGDPR Verordnungen

- Koordinierung und Entwicklung von Informationssicherheitsrichtlinien und -verfahren und Verbreitung der Nutzer Richtlinien
- Entwicklung und Anwendung eines ICS basierten patch und update Prozesses, im WIN 10, Mainframe, Unix und Linux Environment
- Implementation von Monitoring Tools zur Kontrolle der Stabilitaet und anderer Prozesse
- Endpoint Security (BM BigFix, Tanium, Checkpoint, GFI, HPE, Sophos, Kaspersky...)
- Sicherstellen, dass das Inventar des Informationssystems laufend aktualisiert wird, regelmaessige Scans und Pentests
- Sicherstellen, dass die Ergebnisse auf die Geschäftsauswirkungen regelmäßig durchgeführt und überprüft werden
- Arbeit mit System- und Anwendungseigentümern, um die Einhaltung von Informationssicherheitsbestimmungen zu beurteilen und Maßnahmen zur Risikominimierung zu planen, zu dokumentieren und umzusetzen
- Erstellen und Verwalten einer Risikotabelle, die alle Risiken für Informationssysteme identifiziert
- Sicherheitsbewertungen für neu entwickelte oder neu erworbene Unternehmen, Geschäftsprozesse, Systeme und Anwendungen durchführen
- Koordinierung und Entwicklung eines Bildungs- und Ausbildungsprogramms zur Informationssicherheit fuer interne und externe Mitarbeiter
- Entwickeln des Prozesses der Sicherheitsereignisverwaltung und dem zugehörigen SIEM-System
- Entwicklung und Verbesserung des Prozesses der Sicherheitsvorfälle, Remediation
- Audit externe Dienstleister, um die Einhaltung der Bestimmungen der Informationssicherheit zu gewährleisten
- Governance, Plan, Implementierung von Multi-Passwort-Zugriffssystemen mit hoher Verfügbarkeit (neu entwickelter Prozess neueste Technologie)
- SIEM, Erstellen eines SIEM Konzeptes basierend auf HP Arcsight
- Arbeiten mit mehreren Anbietern, entwickeln maßgeschneiderte Sicherheit für Großrechner.
- Reorganisieren von Admin-Rechten (AMR4V)
- Budgets verwalten
- Hauptverantwortlich fuer RfP, RfS, SOW, RfI, Vendor Management
- Schaffung eines neuen SOC für globale Operationen
- Erstellung von Testspezifikationen (Szenarien und Cases)
- Evaluierung von Testdaten und -fällen
- Integrations- und Abnahmetests
- Test-Dokumentation

- Ansprechpartner für Nutzer des Systems, Koordination mit SW Hersteller
- Führen eines Teams von ca. 19 Sicherheits- und Netzwerkexperten auf allen Ebenen

09/2016 - 04/2017 8 Monate

Projektleiter -Senior Enterprise Security Architect (ESA) bei einem Internationalen Telekommunikations Unternehmen (IT security)

Projektinhalte

Dokumentation und Durchführung von Sicherheits Vorgaben nach BSI 100 Grundsatz und ISO 27XXX – Beratung des Konzerns bezüglich Cloud Migration

- Projektierung eines neuen / erweiterten SOC /ISMS
- Prozess Erstellung fuer ein SIEM
- Neugestaltung des WIN 10 Update und Patch Prozesses
- Process Management Konzepte Hpe ArcSight, McAfee ePO
- Erstellung einer Governance im Enterprise Umfeld-
- Erstellung eines ISMS und Beratung zur Zertifizierung-
- Vorbereitung zur ISMS / ISO 27001 Zertifizierung-
- Beratung und Presentation – Risk Analyse
- ESA end-to-end , Netzwerk Segregations, etc.
- Encryption Vorschläge für das gesamte Projekt, Cloud, Data Center, Mobile, Laptop, Desktop
- Bedrohungsanalysen und Erstellung eines Sicherheits Katalogs
- Empfehlungen fuer ein modernes Enterprise RAS Konzept
- Dokumentation im SCRUM Umfeld
- Abbildung und Entwicklung von Prozessen
- Modellierung verschiedener Konzepte
- Dokumentation von Embedded Software unter Linux/Android
- Dokumentation von Sicherheits Prozessen und Funktionen im Mobilen und festen Netzwerk Bereich
- Erstellung von Manuals / Handbüchern
- Dokumentation vorhandener Software fuer den Systembetrieb
- Erstellung von Trainings Konzepten im Betriebs Umfeld
- Erstellung Kryptographischer Lösungen im Mobilen Umfeld
- Dokumentation / Entwicklung von Test und Umgebungen-Configuration auf verschiedenen Plattformen, Windows, Android, IOS unter Common Criteria Evaluation
- Übergabe in den Regelbetrieb am Projekt Ende

07/2016 - 08/2016

Projektmanager -Entwicklung von Schulungskonzepten und Prozessen zur IT Sicherheit basierend auf BSI Grundsatz und ISO 27001

Workshops zum SOC und SIEM

Projektinhalte

- Einführung in die Schulung von Teams
- Konzeption und Betrieb von Technologien zur Erkennung von gezielten Angriffen auf Unternehmensnetzwerke
- Wie erstelle ich ein ISMS
- Projektierung der NOC und SOC
- Entwickeln von innovativen Detektions- und Verteidigungsmaßnahmen
- Kontrollen und Prozesse zur Sicherheit im laufenden Betrieb
- Eigenverantwortliches Analysieren von Angriffen und Erstellen von Handlungsempfehlungen
- Durchführung von Penetrationstests und Sicherheitsanalysen inklusive Ausarbeitung von Angriffsszenarien und Dokumentation von Arbeitsergebnissen
- Erstellung von Leitlinien fuer IT Sicherheit
- Erstellen von Sicherheits Notfallkonzepten

- Erfahrung in der Administration und Absicherung von Firewalls (z.B. Juniper, Checkpoint, Cisco), Content Security Systemen, SSL-VPN Gateways, IPS/IDS, Sina, Genua, Doi ... etc.
- Kenntnisse der wichtigsten Standards der IT-Sicherheit (ISO 27000 ff, PCI, Common Criteria)
- IT Infrastrukturen (Netzwerke, Client-Server Systeme, Virtualisierung, Zugriffskontrolle etc.)
- Konzeption eines darauf basierenden SOC
- Die neusten Kenntnisse in Windows 10 und Windows mobile
- Sicherheit von SAN und NAS, SANE (storage area network encryption)
- Abschliessende Beurteilung eines gesamt Sicherheitskonzeptes mit praktischer Implementierung

02/2016 - 07/2016 6 Monate

Projektleiter/Manager - Projekt bei einer der grossten Transport und Beförderungsunternehmen (Deutsche Bahn)

Projekthinhalte

- Einführung eines ISMS unter den betrieblichen Bedingungen im GSM-R Netzwerk und BSI Grundschutz unter ITSig
- Vorarbeiten zum erweitern des vorhandenen NOC in ein SOC
- Erstellung eines Netzwerkstruktur Plans
- Planung und Implementation * eines SOC (Security Operation Center) , zusammengefasst fuer die Verschiedenen Abteilungen (System, TK, LST usw..)**
- Fokus und Planung, Ressourcen, Risiko und Change Management.
- Workshops mit Teams aus verschiedenen Fachbereichen und Stakeholders
- Erstellung der Governance
- Erstellung des Asset Managements
- Bedrohungs Analyse nach ISO 27001 und BNA 109
- Riskmanagement, Risiko Analyse
- Gefährdungs Analyse mit Restrisiko Abschätzung
- Planung der Sicherheits Zertifizierung
- BSI Grundschutz, ISF, Cobit, BNA, ITU 1501
- Analyse des GSM-R Networks und Schnittstellen zu System ,LST...
- Verständnis von neuen Planungen, IP Networks und Re-investment Projekts, LTE updates
- Praktische implementation aller Ergebnisse und Process in ein SOC
- Übergabe in den Regelbetrieb

* Planung und layout des vorgesehenen Real Estate, Planung notwendiger Hardware, Erstellung von Rahmenverträgen fuer Lieferanten, People Management, Relevante Prozess neu strukturieren

** Monitor/Analyze Network Traffic, IDS Alarm, Network Intrusion detection, Incident declaration, threat management (Aufbau des SIEM), Monitor all relevant Network appliances and analyze logs fuer malicious activities. Entwicklung von Prozessen aller art zur Optimierung von Incident Response Zeiten. Automatisiertes Melde System an die BNA und das BSI unter Vorschrift des ITSig. Dokumenten und Berichts Prozesse aller Vorfälle. Prozesse zur Incident automatisierung.....

09/2015 - 02/2016 6 Monate

Projektleiter - Deutschland Projekt im oeffentlichen Dienst (BAMF Nürnberg)

Projekthinhalte

- Komplette System Analyse
- Erstellung eines ISMS Konzeptes
- Umstrukturierung des vorhanden SOC und Erweiterung des SIEM
- Moderation von Kunden/Internen/ Externen Workshops
- Übergabe in den Regelbetrieb
- Reparatur und Vorbereitung der derzeitigen (Windows/Unix) Umgebung zur Migration in ein neues RZ
- Migration and definition of MS CA, POC
- SSL – SHA1 nach SHA-2 migration
- ADS patching
- Umgang mit HSM, Hardware Security Modules (SINA, SafeNet), documentation des Key lifecycle
- MS NDES, Installation, implementation von PKI componenten
- Decommissioning nach updates und patches installation
- Dokumentation des gesamten Prozesses
- Uebergabe in die Produktion und local Team training
- BIG Data Projekt Manager, (Kanban, Scrum), MS,...
- Berechnung von Daten Speicherung (SAN) in einem neuen RZ

- Analyse von vorhandenen schwach Stellen (Sicherheit)
- Riskmanagement und Restrisiko Analyse
- Analysieren von verdächtigem Verhalten
- Analysieren und Empfehlung zur hoch Verfügbarkeit des neuen Netzwerkes
- Planung der Migration des vorhandenen NOC/ SOC in ein neues SOC gemäss ITSig und BSI 100/ISO 27001 Vorgaben
- Implementation eines komplett neuen bb (bahn betrieblich) SOC
- IT und TK Anpassung an das mobile (Android, IOS) Netzwerk, Entwicklung von speziellen Android Applikationen
- Empfehlung von Hardware Lieferanten
- Vendor Management, Budget Erstellung, Rahmenvetraege
- Migration mit minimalen Betriebsunterbrechnungen
- Ziel, reduzieren möglicher Angriffe von 50%-60%
- Integration von encrypted VoIP und Fax Verkehr
- Analyse von Redundanz und Latenz, operationelle Verbesserung
- Erstellung kompletter Dokumentation
- Schulung des Fachpersonals
- Präsentationen für die oberste Geschäftsleitung
- Übergabe an interne Administratoren, Schulung

02/2009 - 09/2015 6 Jahre 8 Monate (Banken und Telekommunikations Umfeld – einschliesslich Herstellungs Management)

Director Projekt Management - SecureScript Neoi Pte. Ltd. (IT)

Job / Projektinhalte

- Direktor (Mobile IT - Cyber Security – Unterstützung, Management, Konsultant) Professionelle Konsulting Gruppe, SecureScript erworben von PIC -Technologie im Jahr 2009
- Verantwortlicher Direktor fuer Firmen Leitung unter lokalen Vorschriften, Vertrags Position
- People Management (120 Konsultants), Vendor Management, Rahmenvetraege
- Konsultant und Projekt Manager, IT HR **
- Manager Team Cyber Security
- Entwicklung moderner Verschl"sselungen im mil./Regierungsbereich
- 2014 fuer die Fussball WM, Entwicklung einer Fernseh applikation die es erlaubt Online Streams von verschiedenen Laendern in einer eLauncher – eNtertain applikation zusammen zufassen. Die Entwicklung wurde fuer Amazon gemacht (sehen Sie unter Amazon „elauncher“)
- Android Entwicklungen im Enterprise Umfeld, Commerce und Zahlungs Applikationen
- Riskmanagement, Risiko Analyse, Riskassessments
- Spezielle Software Kenntnisse : Eclipse IDE mit ADT, Scrum, Java, Agile , Kanban, Android Platform Tools, C, C++, Java Script,
- Android SDK, NDK, Titan Mobile SDK, Hyper,API, Adobe Air, HyperNext Android Creator (HAC), jQtouch, HTML5, CSS3, LungoJS
- Entwicklung Android Applikationen, IOS, Windows
- Cyber / IT Informations System Architektur / Sicherheit
- Mitarbeiter Management und Schulung
- IT-Sicherheit -Software Entwurf und Entwicklung
- Management der internationalen Entwickler Gruppe von 100+
- Umsetzung einer neuen Netzwerk und Internet Sicherheits Plattform mit SINA und AVDA sowie eigener Entwicklung von Algorithmen
- Übergang / Umwandlung von traditionellen Enterprise- Telefonanlagen auf IP / VoIP , IP - Videokonferenzen , VoIP / IP- Verschlüsselung
- Entwurf und Entwicklung von IT / Cyber Security / IP / VoIP-Lösungen in mobilen Systemen , für alle Plattformen (Windows, iOS, Android , Blackberry etc.)
- Sicherung von Clouds mit neuer PKI- basierten Sicherheit und spezielle verschlüsselten Festplattenlaufwerken
- Verschlüsselung kritischer Daten mit kundenspezifischem UAF Authentifizierung's und Identifizierung's Faktor , dediziertem Zugriff auf bestimmte ausgewählte Einzelpersonen und Gruppen
- Aktualisierung der bestehenden Systeme auf die neueste Sicherheitstechnik
- Ausbildung und öffentliche Vorträge über Risikomanagement und Cyber Sicherheit
- Verwalte und Manage das Marketing des Unternehmens
- Beratung , Projekte, Analyse der Kundenanforderungen mit Vorschlägen für Änderungen und Lösungen , so dass Vertrieb das Marketing unterstützen kann und neue Kunden gewinnen

** Planung von neuen Threat Monitor Prozessen, NOC und SOC ueberpruefungen und updates. Implementierung von IT Security Prozessen

01/2005 - 01/2009 4 Jahre 1 Monat (Telekommunikation und IT Netzwerke)

CEO-CTO (Kombinierte Position), Soft-Hardware Entwicklung von Mobil Geräten (Mobil Technology, IT Security, Encryption)

Job / Aufgaben / Positionen

Projekt Manager - PIC Intl. Ltd. Hong Kong

Projekthinhalte

- Leitung von 200 technischen Mitarbeitern in Hong Kong, China, South America
- Mitarbeiter Schulung und Anleitung
- Leitung der Niederlassungen und Vertragspartner vor Ort
- Entwurf neuer IT Sicherheits und Netzwerk Lösungen
- Design und Implementierung anspruchsvoller IP / VoIP-Systeme für Service Provider und Unternehmen
- Häufige Reisen
- IT-Risikomanagement , Analyse , Vorträge, Schulungen
- Spezielle Ausbildung für Investitionsbank IT- Personal Schulung ueber Risikomanagement

08/2004 - 12/2004

5 Monate

Interims CTO - Elektronische , Entwicklung, Herstellung

Job Aufgaben

Projektleiter - Lintux Hong Kong Ltd.

Projekthinhalte

- Neukunden Gewinnung
- Auftrags Koordinierung mit Chinesischen Fabriken
- Schulung der technischen Mitarbeiter
- Exoertise und transfer von Erfahrung
- Entwicklung von IP Systemen (Das Unternehmen wurde später von Lintux Hongkong erworben)

11/2003 - 07/2004 9 Monate

Interims SVP – Die Entwicklung einer neuen Smart Mobile Platform MXI

Job Aufgaben

Goldtron Singapore

Projekthinhalte

- Leiter der Singapur –Entwicklergruppe - Hauptkoordinator mit dem Entwicklungsteam Hongkong - Entwurf der MXI Platform (kombinierte Mobil- und VoIP-Dienste)
- Installation desr ersten VoIP-Netzes in Malaysia
- Speziall Platform fuer Portfolio Management Software

12/2000 - 10/2003 2 Jahre 11 Monate (Industrie Netzwerke)

Taitoma Group – Taiwan (HTC Gruppe) - in Taipet-Taiwan Interims CTO

Projekthinhalte

- Verantwortlich für die Entwicklung und Konstruktion von Software und Hardware als Fremdleistungen asiatischer Hersteller
- Verantwortlich für die Entwicklung und Projektmanagementmethoden Umsetzung von Prozesse, Verfahren , Berichterstattung , strategische Leitung
- Entwicklung von Lösungen für IT-Sicherheit und Risikominimierung
- Qualitätskontrolle welche fuer Großprojektn verwendet werden, innerhalb der Asien-Pazifik & Greater China Regionen, oder / und Industrie vertikale Schaubild Strategien , um die Konstruktion und Entwicklungs Dienst des Teams und dem Unternehmen in der Region für die Titoma Gruppe zu gewaehrleisten

10/1999 - 11/2000 1 Jahr 2 Monate

Job / Projektinhalte

- Verantwortlich für die Entwicklung und Konstruktion von Software und Hardware als Fremdleistungen asiatischer Hersteller
- Stationiert für längere Zeit für Projektumsetzungen im Irak , Libanon, Syrien , Saudi-Arabien und einigen anderen Ländern (Installation von kompetten Radio Kommunikations Netzwerken)
- Komplettsysteme Installation und Implementierung
- Entwickelte das erste verschlüsselte Satelliten Telefon fuer eine deutsche Gruppe, welches dann vom oeffentlichen Diensten und Schiffen verwendet wurde. Nebenbei Fernstudium Princeton University USA , Abschluss Phd. Dr.

02/1998 - 09/1999 1 Jahr 8 Monate

CREDIT SUISSE FIRST BOSTON, (UK based)

Job / Projektinhalte

Vertrags Vize Praesident IT – Leiter der Asia Paizifik Gruppe

- Hong Kong Global Engineering and Infrastructure Support Team
- Verantwortlich fuer die Kommunikation zwischen den technischen und Helpdesk Gruppen weltweit
- Analyse der bestehenden Netzwerke und die Suche nach Sicherheitsrisiken ; Entwicklung neuer Risk Loesungen
- Entwicklung von Lösungen für existierende Netzwerke- Migration von bestehenden Systemen nach Windows

01/1997 - 01/1998 1 Jahr 1 Monat

MERRILL LYNCH INTERNATIONAL INC., Hong Kong Senior Konsultant

Job / Projektinhalte

- Komplettsysteme Installation und Implementierung
- Netzwerk- Migration von Novell auf Windows und Transaction Server
- Service, Schulung lokaler Ingenieure , Systemanalyse , Telekommunikation Konnektivität, Router (3Com, Transcend , Cisco)
- TCP / IP , DHCP , WINS, Ethernet, Vertrauensbeziehungen mit Netzwerken in den USA und Europa .
- Integration von NT 4 mit BLITZ (eines SQL / Excel-basierten Preismodell und Trendmanager für Portfoliohandel) .
- Entwickelt neuer Anwendungen wie Ladungsrechner, IROS und Pagepool für Aktien , Schuldverschreibungen und Portfolio-Trading
- Schrieb für zahlreiche Excel-Makros Modelle mit Live-Feeds von Reuters, Bloomberg , Börsenkanal und kundenspezifische Anwendungen von Merrill Lynch in New York und London die Preisgestaltung (Vorreiter von IP basiertem TV)
- Installierte Anwendungen für den Kauf und Verkauf der Produkte , Messaging- und Benachrichtigungs für einzelne Aktien, Anleihen, Portfolios. Mit : RAM Excel , RAM -Add-Ins , Newport, Loan -Manager , Anleihemanager , IORS , K- Tek , PDD , DDE .
- Die Umsetzung der ersten Sicherheitsbestimmungen für Banken im Investment Business

01/1988 - 12/1996 9 Jahre

KONSULTANT / SENIOR SYSTEMS Ingenieur

Job Aufgaben / Positionen

- Kunden unter anderem BOA, Deutsche Bank, BSI Machinery Germany, Indonesian Government, Thai Farmers Bank, Hoechst Chemicals Taiwan und Thailand, Anderson Singapore, SAP Germany.
- Meistens Netzwerkplanung und Umsetzung. Erfahrungen in der Finanzwelt sowie die chemische Industrie und andere Branchen
- Es gab auch eine Menge Telekommunikation Aufgaben , einschließlich der Planung von Mobilfunknetzen , Abrechnungssysteme für Inmarsat , Up-Down- Link -Schnittstellen zu LANs .
- Planung und Installation von Terminal-Server- Netzwerk für eine führende Schweizer Bankengruppe , um langsame Netzwerkverbindungen zu überwinden und die Kosten zu senken , indem ältere PCs und Notebooks für den Anschluss an NT / W 2000 / XP –Netzwerke aufgebessert wurden
- Erfahrung in Packet Protocol , ein Protokoll, das später die Basis für das GSM- Mobiltelefon -Systeme Installation und Implementierung angewendet wurde
- Spezial Projekte, Verkauf und Installation von landesweiten UHF Kommunikations Netzen, als Vorlaeufer der heutigen Mobile Kommunikation. Kunden im nahen Osten und Asien.
- Entwicklung und Herstellung der UHF Komponenten, unter anderem Entwicklung des ersten „Handies“ ETACS, AMPS.

- Erfahrungen mit A-Netz Autotelefonen, Entwicklung des ersten Satelliten Telefon im Attache Koffer, Verschlüsselung von Mobile Geräeten

01/1985 - 12/1986 2 Jahre

PATHCOM Inc., USA / Tokyo – Radio Kommunikations Produkte

Job / Aufgaben

- RF Entwicklungs Ingenieur fuer die Pathcom Gruppe in USA, mit Sitz in Deutschland.
- Entwickelte das erste frei CB Funk System, bekam die erste jemals ausgegebene Genehmigung des FTZ in Darmstadt, setzte Standards fuer den CB Funk
- Technologie Entwicklung neuer Datenkommunikations Produkte in den USA und Yokohama Japan
- Herstellungs Kontrolle und Unterweisung
- Entwickelte den ersten asiatisch hergestellten Radio Synthesizer , VHF- und UHF- Transceiver und Bündel Handy, System Entwicklung und Fertigen der Pathcom Kommunikationsprodukte

01/1984 - 12/1985 2 Jahre

Kundendienst fuer elektrische, elektronische Geräete

Unternehmen

SYNTHEX
Einsatzort
Deutschland

Branchen

Bundes Behoerden, Regierungen, Banken, DB Netz, Deutsche Bahn, BAMF, Enterprises, mittlerer Unternehmen aller Branchen, Android Experte, Telekom Provider, Chemische Konzerne, Energie Firmen, Gross Unternehmen (ISMS Zertifizierung)

Fremdsprachen

English
Deutsch
Chinesisch
Spanisch

Produkte / Standards / Erfahrungen

Kompetenzen

- IT Konsultant - Projekt Manager – Produkt Marketing
- Cyber Sicherheit Experte durch Ausbildung und Erfahrung
- Netzwerk Sicherheit (mit Spezialisierung fuer Mobile Netzwerke)
- Cryptographische Entwicklungen, Software und Hardware
- Entwicklung neuer IT Sicherheits Methoden und Richtlinien
- Vermarktung neuer Produkte und Einführung neuer Ideen und Lösungen mit Blick auf neueste Cybersicherheitsvorfälle
- Software-Entwickler - Hardware -Design und Entwicklung
- IP Dienste – VoIP – Transitions – Entwicklungen -Loesungen – Globale / Unternehmens Netzwerke
- PKI/AES256, verschluesselte VoIP Netzwerke
- Spezifische Kenntnisse und Erfahrungen in der IT- Sicherheitsarchitektur
- Analysieren des Kunden Netzwerksicherheit , zu entwickeln und eine effiziente Lösung für Aktualisierungen und Änderungen vorschlagen
- Schulung und Betreuung von globalen und lokalen Teams
- Profi- HF-Techniker , analoge und digitale - 0-900 MHz , 900 MHz -6 Ghz , 2G, 3G, 4G, LTE und höher usw. Mobile Geräte und komplette Netzwerke
- Entwurf und Entwicklung Hard- und Softwarelösungen , Produktionsleitung

IT Kenntnisse

- OS System Erfahrung: DOS, Windows 7.8.10 , Windows NT 4.0, Exchange, Unix, Sun Solaris, Linux, Android, IOS,
- RDBMS: MS SQL Server, Sybase, Oracle Server
- Netzwerke: TCP/IP, NetBIOS and NetBEUI, SNA, UNIX, X25, MS SNA Server, Ethernet, Token Ring, Mail server SMTP, POP, Imap, CCMail, Exchange, VoIP

- ADVA Optical Multiplexer Networking , SINA Secure Inter-Network Architecture fuer Fibre Optik, Cryptographic, Genua
- Banyan Mail, Chat Server, News Server, Transaction Server, Exceed Platform, Novell, RAS, Windows.
- Telekommunikation: Drahtlose Systeme, Mobile Telefon Netzwerke, GSM, UTMS, CDMA, HSPDA, PCS,AMPS, 3G,4G,LTE ...
- Frame Relay, ATM, Fibre Optics, ISDN. RF Propagation. Router (Cisco, 3Comm, Bay Networks, Livingston, RAS, Access Server, etc.
- Mobil OS: Android, IOS, Windows, Blackberry, Linux

Hardware Kenntnisse

- RF-Chip entwicklung – komplette Geraete Entwicklung
- SD Sicherheits- Chip und Halbleiter -Design - Embedded Software
- NFC hardware und Software
- RF und Mobile Entwicklung- CPU Entwicklung – Audio Chip Entwicklung – Video Chip Entwicklung
- Streaming Media chip und embedded Software - PCB Entwicklung – Layout - Maskierung - Fertigung
- Mobil Geraete, tragbare Fingeabdruck und Pass / Ausweis Scanner

Software Sprachen / Kenntnisse

- Praktische Wissen von C/C++,Perl, Mosaic OA, AB2,Pascal,Fortran, SQL, VB, Intel, GSM, AMPS,HTML, Java, Oracle, dBase, MS alle Anwendungen, Linux, Android, IOS etc.
- Spezialisiert in verschluesselung, AES 256, PKI, FID, Biometrie
- Verschlüsselung von Mobilfunk und Wireless Daten Systemem , Cyber Sicherheit -Experte seit 1995 entwickelt den ersten verschlüsselten Satellitentelefon Terminal (P2P -Technologie)
- Entwickelt neuesten Internet -Banking-Sicherheit für mobile Systeme (FIDO basierend)
- UAF Passwort freie, menschliche Faktor Identifikation, Biometrisch basierende FIDO und Nurugo Funktionen, usw

Ausbildung – Weiterbildung

Zertifizierung

CISSP,AISP,CISA,CISM,MCP,ITIL,Prince2,ISO27001,BSI GRUNDSCHUTZ,EGDPR, GDPR, Blockchain, Cloud

Princeton USA

PhD in Telekommunikation

Spezial Gebiet Verschlüsselung von Satelliten Telefonen

Okt 1980 – Sep 1982

Studium TU Darmstadt Elektrik und Elektronik, Mathematik, Physik

Diplom Ingenieur at Philip Reitz Polytechnikum Frankfurt/Main

Jan 1999 – Dez 2000

Fernstudium Princeton University USA, fuer Phd. Dr.

Okt 1975 – Aug 1980

Praktikum , Lehrstelle , Geselle , elektrischer Meister BEI Elektro, Wiesbaden

Jul 1975

Abitur Griebing Humanistic Gymnasium Wiesbaden

Result: 1,1; Mathematiks und English

White Papers (copyright 2019 Dr. Bernhard Bowitz, download and copy not allowed)

[IT Security planned, managed effectively](#) – [Build a SOC with Open source](#) - [Public Cloud Security](#) - [The art of IT error reporting](#) - [Process Modeling](#) - [ISMS Governance](#) - [DLP-Richtlinien](#) - [Cloud-IAM](#) - [An Overview of Cryptography](#) - [CyberSecurity vs. IT Security](#) - [Introduction of an ISMS under ISO 27001 \(German\)](#) - [ESA definition](#) - [Introduction of an ISMS under ISO 27001 \(English\)](#) - [MSS / Managed Security Services](#) – [CASB](#) - [Security Information and Event Management](#) - [SIEM](#) - [SIEM-SCRUM](#) - [Telephone knowledge](#)
