Dipl.Ing.Bernhard Bowitz ,PhD © 2024

Nationality:	**German National - Singapore PR**
Gewoehnlicher Aufenthalt:	**Deutschland, Wiesbaden / Muenchen**
Office Address:	**Germany: 65185 Wiesbaden – Asian Office: Singapore**
Office Telephone:	**+49 611 3417 1215**
Mobile:	**+49 171 163 8089**
eMail direct:	**bernardbowitz@gmail.com**
eMail Office:	**info@securescrypt.com**
Internet:	**https://securescrypt.com A global Consulting and Technical Project Management Team (German security clearance UE2)**
Sicherheits Ueberpruefungen:	**gültige SÜ2 (bis 2026) und Ueberprueft Paragr. 7 LuftSIG, bis 2025**
Education-Experience	**Diplom Ingenieur ,IT-Network Engineer, Software Developer, Project manager mehr Details im kompletten CV**
Certifications:	**CISSP,AISP,CISA,CISM,MCP,ITILv3,Prince2,ISO27001(last update 2020),BSI GRUNDSCHUTZ,EGDPR, GDPR, CyberArk, Fireeye, Qradar, Cloud (AWS, Azure, private Clouds, Blockchain), Scrum Master, Sprint, Clarity, Jira, Diplom Ingenieur, PhD (Elektronik und Netzwerk Topology)VS-NfD, Erfahrung an Anforderungen durch Geheimhaltungsgrade der Bundesrepublik Deutschland (Verschlusssachenanweisung), sowie EU, NATO und MISSION…more in CV below…**
Languages:	**Deutsch (Muttersprache 1), English (Mother tongue 2) , Spanisch (Basics) ,Chinesich (Basic)**
Summary – short term CV	**More than 30 years working as a technical IT Engineer, PM, Sales Analyst, mehr im kompletten CV folgende Seiten**
Strength – Expertise:	**Help and support for clients in finding the right business and technology solutions by working as a consultant and consultant on design trend-setting security architectures**
Experience - Roles:	**Consultant, technical project manager, PM, administrator, auditor, analyst, document writer, developer, architect….**
Technology Hardware Experience:	**Unix, Linux, RHEL, Windows, Cloud, SaaS, VMWare,… Details im kompletten CV**
Industry Experience:	**Oeffentlicher Dienst, Militaer, Finanzen, Banken, Automotive, Versicherungen, Internatonal Industries, Multi National Corporations Europe, Asia,…. mehr im kompletten CV**
Datenschutz Hinweis	**Die in diesem Schriftstueck enthaltenen Informationen , fallen unter den gesetzlichen Datenschutz. Jegliche Referenz, Weitergabe oder Verwendung, auch teilweise, ist nur mit SCHRIFTLICHER Genehmigung des Authors gestattet!**

Komplettes CV

Ich habe Dokumentationen, Betriebshandbücher und mehr als 1000+ Artikel rund um die IT geschrieben. Alle meine Beiträge befinden sich in meiner persönlichen Bibliothek und stehen meinen Kunden auf Anfrage zur Verfügung.

Positions-Projects-Career: 1988 - 2024 (ongoing).

TOPIC, das Aktuelleste zusammengefasst:

Seit nun mehr als 15 Jahren habe ich mich auf digitale Sicherheit spezialisiert. Ich bin seit vielen Jahren Ü2 überprüft, sowie auch LSÜ2 (Luftsicherheit), habe an mehrern Kursen des BSI teilgenommen, neben meinen zahlreichen anderen Certifications
Besonders im Bereich VS-NfD, Nato Sicherheit, habe ich einige Projekte geleitet und technisch implementiert.
Habe **„All in One" Lösungen von VSA konforme Datenverarbeitung bis GEHEIM**, entsprechend den Anforderungen meines Kunden in berateneder Funktion wie auch technischer Funktion, vorgeschlagen, entwickelt.und auch hands-on implementiert.
Berate wie Verschlusssachen durchgehend digital zu bearbeiten sind, unter VS-NfD Bedingungen.
Ich war und bin immer noch in der Entwicklung sicherer Hardware tätig, auf Netzwerkschicht 2: Große Datenmengen schnell und sicher zu übertragen, mobile Platformen für mobile Endgeräte – vom Smartphone bis zum Tablet.und habe verwundbare Systemstellen feststgestellt und passende Schutzmaßnahmen vorgeschlagen, entwickelt und implementiert..
Ich bin auf allen Systemen zu Hause..
Meine Kunden sind vom öffentlichen, militärischen und Industrie Bereich, meine Erfahrung liegt in den BereichenNetwork Security,Endpoint Security, VS, Staatsschutz, Hoheitliche Aufgaben, Elektronnische Identitäten, Compliance, PKI, Certificates, email und web security, **sowie naheliegenden Grenzbereichen wie IAM, PAM usw.**

Im Finanzbereich arbeite ich vorwiegend mit DORA, Digital Operational Resilience Act, covering Risk Management and Governance, Incident Reporting, Third-party Oversight, Cybersecurity Standards, Testing and Scenario Planning, strengthen the cybersecurity and operational resilience of the European financial sector in the face of evolving digital threats and challenges.

IAM / PAM Loesungen
ABAC-RBAC in Verbindung mit IAM Loesungen kopiere den link in einen Browser: https://securescrypt.com/docs/ABAC - RBAC - IAM.pdf

Note: This document partly contains highly confidential information, which falls under the Data protection Laws. Further usages must be first agreed with the author!

Strength and experience....
Staerken und Erfahrungen

Grundsaetzliche Beratungserfahrung (auch „hands-on")(UE2 und LUEV2 zertifiziert)...

- Ich bin graduierter Ingenieur, hands-on PM, mit mehr als 20 Jahren Erfahrung in Produkt Entwickung, Produkt Marketing und Kunden Acquisition, speziell auf den Bereichen Telelkommunikation, digitale Kommunikation, Netzwerk und Cybersicherheit... ich habe ein sehr breites Wissen und Erfahrung in Netzwerk Architekturen, local Networks, Cloud Networks,, auch GiT gestuetzte Codeverwaltung, scripten usw.

- Planung / Konzeptionierung sowie Beratungsleistungen in Bezug auf die gesamte IT/Netzwerkstruktur, Administration, Planung, Implemantation, Schulungen usw...sowie Insbesondere...

- Vorbereitung von Verkaufskonzepten – technische und kommerzielle Leitung von Pre- und Sales teams

- Planung / Konzeptionierung sowie Beratungsleistungen in Bezug auf Informationssicherheitsrichtlinien

- Planung, Architektur, Integration von Encryption im Finanziellen und Kommerzialen Umfeld.

- Planung / Konzeptionierung sowie Beratungsleistungen in Bezug auf IT-Sicherheitskonzepte

- Planung / Konzeptionierung sowie Beratungsleistungen in Bezug auf IT-Service-Management (inkl. Service-Design und Vereinbarung von SLAs) , Verhandlungen mit Lieferanten

- Erfahrung mit Automatisierungs werkzeugen wie VMware vRealizeAutomation, Ansible,

- Planung und Konzeption von Cloud Management Platformen, Implementierungs Konzepte, Virtualisierungslösungen VMware Cloud Foundation etc.

- Security mit Sicherheitsgateways, Entropiequelle bzw. HSM, DDI, Sicherer Schlüsselspeicher (KMS), IAM und PKI

- Planung / Konzeptionierung sowie Beratungsleistungen in Bezug auf Geheimhaltungsgrade (Verschlussachen Anweisungen etc.) im Behördenumfeld (National, EU, USA, Botschaften, sowie anderer Regionen und Buendnisse)
- Seit 2020 Entwicklung von Blockchain encryption mit Quantum Komputern
- ISO 2001,2002
- Langjaehrige Erfahrung in Assessment der IT Security Architekturen und Audits vorhandenener Konzepte und Prozesse ,Umgang mit Atlassian Jira und Confluence ,Umgang mit Atlassian Jira und Confluence , Methoden (, SAFe, Kanban
- BSI Sicherheitsberater – ISMS – BCM – GRC – HyScout Suite

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, mein Hauptaugenmerk ist auf profitable Weitergabe (Verkauf) eines Sicherheitsproduktes gerichtet.
- Helfe dabei meinem Kunden die richtigen Verkaufs Argumente zu bilden, um das entwickelte Sicherheitsprodukt auch an dritt Kunden oder Tochterfirmen zu verkaufen
- 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, SOAR, IAM, PAM, PAS, CISO, Blockchain Security. Encryption echnologien usw.
- Entwicklung neuer Produckte und Dienstleistungen (Software und Hardware), IT und TK
- Unterstuetzung von Verkauf und Marketing zur position von Produkten und Dienstleitungen 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
- Bank und Versicherungs Experte, VAIT, BAIT, BSI
- Automotive – GPS – interne Elektronik
- Transport und Verkehr , Energie, GSM-R, Aviation, Automobil Industrie
- 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),Fireeye Endpoint Security, Sophos
- IBM (Qradar), HPe ArcSight, McAfee ePO, MicroSoft Security, CyberArk, Fireeye, Sophos, EndpointSecurity
- BeyondTrust, Sophos, Endpoint Security, TrendMicro
- Beyondtrust – privileged Remote Access, Z-scaler
- IT / TK technology - for large industry and consumers
- Large networks, industry and the public sector
- Wireless and mobile (Android, Windows, iPhone) 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

Technologie – Hardware – Software Fachwissen

Technology Fachwissen (25 Jahre++)

- Experte in Entwicklung von modernen Cloud Infrastrukturen, Private Clouds, neuartige Cloud Plattformen mit Marketplace Portalen zum Verkauf von Cloud-Services
- 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
- Netzwerk Segmentierung, NGW, VLAN Sicherheitskonzepte, SAN, NAS
- Experte in **Geheimhaltungs** Vorgaben wie VS-NfD (Deutschland) / TC/IC
- Ü2 zerifiziert laufend....2024.....
- Notfall Management nach BSI100.4, erstellen der Dokumentation zum Umsetzungsrahmenwerk (confidential**)
- Kenner des Geheimhaltungs Buches der BRD (vertraulich)
- VS-NfD, Nato Secret, Nato Restricted, Nato unclassified,.....
- Vendor Mangement, zertifiziert mit vielen Dienstleistern und Aplikations Anbietern
- Quellcode Analyse, Anpassungen, Erweiterungen, Korrekturen
- IAM, SAM, PAM, GRC , AMR4V, Frontdesk, CyberArk,empowerID managed access, BeyondTrust. Qradar,Saviynt intelligente Identity Loesung
- Qradar, TheHive, Cortex, NexPose, MISP, zAlert, SIEM, SOAR,….
- Java, C++,SQL, DOT Net, Microsoft Softwareentwicklungsinfrastructur, (V ,Net 8.0)
- Script Entwicklung mit PowerShell, VBS oder Batch
- PKI, SSL , MS NDES, SafeNet Networks HSM
- Cloud Azure, AWS, Strato, Telecom, SaaS, LaaS, XaaS, TrendMicro Deep Security Virenschutz.....
- Risk management , Risiko / Rest Risiko Analyse, GRC
- HPe ArcSight, McAfee ePO. Kapersky Sicherheit, Fireeye Endpoint Security, HiScout GRC Suite, MSS,...
- TripleDES, Blowfish,,AES,Twofish,IDEA,RSA Security.MD5, Blockchain, Quantum
- Mainframe, Windows, Microsoft Windows Server 2003, 2008, 2012, 2016,2020… Linux, Unix, Oracle, ...
- IT / TK Technologie – für Groß Industrie und Verbraucher
- Daten Center Architektur, Infrastruktur
- Infrastruktur Dienste DNS, DHCP, RDP....
- Große Netzwerke, Industrie und Öffentlicher Sektor
- Penetration Testing Tools – Wireshark, MetaSploit, AcuNetix Scanner, w3af, Netsparker, Burp Suite, Aircrack
- 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 (25 Jahre++)

- - 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 Algorythmus, 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 –
- - Script Entwicklung mit PowerShell, VBS oder Batch
- - **Azure, AWS, Blockchain - cloud migrationen, von Konzept zur Implementation**
- **- Microsoft Windows alle Plattformen**
- **-** Microsoft Client Betriebssystemen Windows NT .. bis Windows 11 mit Sonderformaten
- **-** Windows-Fileservices und NAS-Systemen
- - 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 Apllikationen, Netzwerke allgemein, Komputer, Daten Center, Quantum Computing
- CISCO Asyync, Palo Alto,Checkpoint,....
- - Entwicklung eines SIEM- SOC, vom design zur implementierung (einschl. IBM Qradar und TheHype/Cortex) integration

Rollen

- Berater, Enterprise Projektleiter / Projektmanager / MS-Project/ Clarity PMT/ Sprint / Gitlab/
- Verkaufsleiter/Berater – Markt Erforschung fuer neue Sicherheitskonzepte, Kunden Acquisitation
- Agile /Jira-zertifiziert/ Scrum Master
- Konsultant, PMO / Administrator / Sicherheits Auditor (27001 /BSI), IT Architekt,
- Technischer PM mit „Hands On „
- DVSGO Berater nach EU Grundschutzlinien
- BSI Sicherheitsberater
- Software-Entwicklung / Programmierung / Hardware design / Netzwerk Architektur
- Beratung / Consulting / Hands On / Technischer PM
- Projektmanagement / -leitung / Organisation / Koordination/
- Teamleitung von Teams bis zu 80 Mitgliedern,
- Global, vor Ort und Remote Penetration Tester, Test Manager
- Engineering / IT-nahe Ingenieurdienstleistunge
- Cloud Architekt, Sicherheits Architekt
- Blockchain Entwickler, eigene Platform Encryption Architektur entwickelt

Zusammenfassung – Kurz Information- CV

- Projekt Manager-Berater, Projekt Management Office, Technischer Projekt Manager, von Konzept Erstellung bis Anwendung. Projektnetreuung von Entwurfsplanung bis Fertigstellung.
- Erstellung von Verkaufs Strategien fuer neu entwickelte Sicherheits und sonstige IT Produkte und Projekte
- Erstellung von SLA's, Betreuung von Lieferantenm Erstellung technischer und Projektgebundener Ausschreibungsunterlagen
- Datensicherheitsbeauftragter – technische Betreuung / Beratung von Unternehmen unter beachtung von Vorschriften des BSI IT-Grundschutz, BSI TR, BaFin (Bait, VAG, WpHG, WpPG, WpUEG, BoersG, VAIT, KAIT....), Einhaltung des Geheimschutz Buches der BRD, Verstaendnis des Chinesischen Datenschutz Gesetzes von 2020, Vorschriften des US amerikanischen Datenschutzes.
- Interims IT Security Experte, IT Bereiche analysieren, Erstellung einer Roadmap, Einfuehrung eines neuen ISMS, Unterstuetzung der internen Fachbereiche. Eigenstaendige, einschlaegige Erfahrung zur Aufnahme und Pruefung von Prozessen, Schutz der IT Systeme, Test und Produktions Betrieb, Erstellung der entsprechenden Dokumentationen,
- 100% Remote und 100% vor Ort, oder gemischt, je nach Bedarf
- CORONA Information – waehrend den CORONA Beschraenkungen arbeiten wir in allen Projekten 100% remote unter Zuhilfenahme von VPN Verbindungen und ZOOM Konferenze systemen. Hoechste Sicherheit gewaehrleistet. Fuer VPN und arbeits Applikationen, benutzen wir unsere Hochsicherheits MERP Blockchain Plattform.
- Mehr als 20 Jahre, arbeite (Mehrsprachig, Deutsch, English, basic Chinese) Operative und nicht Operative, Analytisch und Administativ, Development und Process Entwicklung, Projekt Leitung,
- Fuehrung von mulltinationalen Teams jeder Groesse, langjaehrige Erfahrung 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, Cyber Security Architekt
- Grundschutz, 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, SSL Secure Shell,SSH (FTP) – PKI based Encryption

- (Genua, Sina, Checkpoint…), SOC, Blockchain und eCoin, arbeite mit jeder Platform (Windows, Mainframe, Unix, Linux, Oracle usw.), SAN.NAS
- CyberArk, BeyondTrust, SOAR, SIEM, SiemPlify (von Konzept bis Anwendung und Implementation), Qradar Konzept, Erweiterung, Anwendung, Clouds ...
- Habe seit 2004 erfolgreich mehrere ISMS/ISO 27001/BSI 100 Zertifizierungen durchgefuert. 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 Grundschutz. Vergangene Projekte
- Arbeite weltweit, Erfahrung in DACH, USA, Asien
- **Referenzen**
- Fuehre Schulungen ueber den neusten Stand des Grundschutzes durch
- Prozess Erstellung,Architectur und Integration für SOC, SIEM (z.B. Splunk, Qradar, LogRythm, Siemplify...), SOAR, PAM, IAM,...
- Ich bin ein leitender Netzwerksicherheit Fachmann (CISSP) mit einem breiten Verständnis der Technologie und der zugeordneten Applikationen . Meine Erfahrung erstreckt sich über beide Bereiche , Mobilfunknetze und traditionelle Netzwerke .
- Aufbau eines VS-NfD konformen Umfelds, um BSI konform damit umgehen zu können
- State of the Art“ Security Architectures, BSI IT-Grundschutz, 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 und Verkauf der entwickelten Produkte, finden von neuen Kunden und Absatzmaerkten.
- 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. Insbesonder mit modernen tools iike empowerID im Cloud Bereich on premises.
- Die besondere Staerke liegt in dem mobilen Bereich, Android/IOS , Entwicklung von sicheren Applikationen im Zahlungsverkehr und e-commerce
- sowie komplexen Netzwerk Strukturen, Big Data, Cloud Sicherheit,
- SIEM, Endpoint Security und vortschrittlicher Sicherheit, im praktischen wie im administrativen Umfeld.

Positionen – Projekte – Karriere ....-2023:

1/2023 – current (end April 2024)

Beratung, Planung und aktives Projekt Management fuer ein geschlossenes On Premises) Hoch Sicherheits Netzwerk (BSI,VS-NfD,VSA)

- Technische Beratung im Netzwerkbereich
- Der Schwerpunkt liegt bei der Unterstützung im regulären Betrieb Security Infrastruktur des Netzwerkes
- Identifikation, Planung und **selbständige** Umsetzung von Projekten zur Aktualisierung oder Verbesserung der zu Grunde liegenden Security Infrastruktur
- Technisches, aktives Projekt Management, Leitung interner teams
- VS-NfD, BSI Geheimschutz in geschlossenen Netzwerken
- GENU VPN architectur Entwicklung und fortlaufendes Update
- Architektur und Entwicklungs arbeiten im Windows und Linux Bereich
- Netzwerk Segmentierung,
- Verbesserung der email Sicherheit (DLP)
- Einfuehrung von ProofPoint als zusaetzliche email Sicherheit
- Share Point Proejct Management

- Reporting an C Level und BoD
- Budget Planung und Vorschlaege Weiterentwicklung oder Neueinfuehrung von notwendigen Sicherheits Vorkehrungen.
- Fuehrung der gesamten IT Sicherheits Abteilung und allen Teams sowie Vendoren und Service Providern
- Name des Kunden geschüzt (Airbus/Eurofiter Munic)

9/2022 – 1/2023 Beratung zur Architektur eines on premises Krankenhaus Netzwerkes.
Erneuerung des Netzwekes auf den letzten Sicherheitsstand B3S
Infrastruktur Dienste DNS, DHCP, RDP ....
Beratung der Sicherheitsverschriften im Gesundheitsbereich
Beratung bei der Ausschreibung und Umsetzung
Beratung, Planung und aktives Projekt Management fuer ein Geschlossenes Hoch Sicherheits Netzwerk

---

1/2022 – 8/2022

PM: On premises Netzwerk - Architektur-Conception-Implementation voelliger Neuaufbau einer Dritt Anbindungs Platform und Datenschleuse mit mehreren Tausend Nutzern (Clients)VS-NfD, Hochsicherheits Strategy bis Nato Sicherheits Stufe-on premises und cloud Integration von Deep Security Enterprise Loesungen (i.e.Opswat-Infodas-SDot) Einfuehrung eines IAM/PAM/LDAP im Behoerden Netz Verschiedene Anbindungs Loesungen wie Thin Client, Sina, Terminal Services, ReCoBS....im VS-NfD Umfeld (confidential) im Behoerdenumfeld (hoechste Geheimhaltungsstufe Ü2 clearance erforderlich)**

- Durchfuehrung einer Bedarfserhebung fuer Datenschleuse zu anderen Organisationen die an das Netzwerk angebunden sind. Die Daten werden auf hochsicherheits Endgeraeten hinterlegt.
- Script Entwicklung mit PowerShell, VBS, Batch ....
- Erarbeiten der Loesung fuer eine Dritt-anbinder Platform an das Netzwerk, Anbindung von Organisationen.
- Architektur im Behördenumfeld VS-NfD
- BCM-GRC HyScout Suite Management
- Einhalten der Anforderungen durch Geheimhaltungsgrade der Bundesrepublik Deutschland (Verschlusssachenanweisung), sowie EU, NATO und MISSION
- Auswertung und Konsolidierung der Anforderungen
- Aufzeigen und Bewertung moeglicher Loesungen fur die Datenschleuse mit Kostenaufstellung
- Durchfuehrung einer Marktsichtung und Erstellungeines PoC/PoV zur Auswahl der Plattform Datenschleuse und Anbindungen
- Vorstellung der endgueltig erarbeiteten Loesung
- Technische Implementation bei mehr als 2000 Nutzern
- Beachtung von BSI, Nato Sicherheits Vorschriften in geschlossenen Netzwerken und aussen Anbidung von Dritt-Organisationen VS-NfD ...
- Erstellen einer kompletten audited Projekt Dokumentation
- Trainings-Workshops
- Name des Kunden geschuetzt, oeffentlicher Kunde Finanz bereich

- Kunde Luftfahrt

Netzwerk Architektur – On Premises - Conception voelliger Neuaufbau eines SIEM (Splunk) mit Planung auf Erweiterung eines SOAR/SOC/CDC – IAM PAM- Entwicklung einer Cyber Security Strategy-on premises und cloud Integration von Deep Security Enterprise (Opswat-Infodas-SDot-Trend Micro) (confidential)**

11/2020 – laufend (1-2022)

Voellige Neuentwicklung des Threat and Risk Managements , Neuaufbau von SPLUNK, Ziel Einrichtung eines automatisierten Threat Management (SOAR)-Ueberarbeitung eines neuer neuen Cyber Security Strategy. Hoechste Geheimhaltungsstufe- UE2 zertifiziert

- Project unter hoechster Geheimhaltungsstufe (UE2)
- Entwicklung eines neuen Konzeptes welches dem Europaeischen Standard entspricht
- Projekt Umgebung in allen europaeischen Sprachen definieren, Projekt Sprache english
- Review existing security events
- Analyze available data sources, security tools, monitor threat trends
- Replace tools install new roles
- Support configuration of security tools
- Manage SIEM Platform NetIQ, if necessary update and reconfigure
- Identify logics to find attackers and develop Playbooks and use cases
- Plan future actions to secure the European wide networks
- Roadmaps, vulnerability assessments,penetrating measurements
- Perform planning of incident response, identifying and prioritizing potential threats, support the IT Sec support Groupand ISM
- Point to technical awareness relation about new threats or new attack trends through the planning and architecture of a new SOC or CDC in cooperation with a new CERT
- Also introduction the design of an IAM PAM Tool (CyberArk, Omada und Saviynt intelligente Identity Loesung), empowerID dynamic access management….
- Stormshield und Cisco Firewalls, getrennte private Netzwerke, hoechste Sicherheitsstufe
- Analyse von Security events
- Ausrollen von TrendMicro Deep Security Server und Agenten
- Erstellen von Patch scripten
- Installation und Konfiguration von Trendmicro Deep Security
- Schnittstellen einrichtung zu Splunk und DLP
- eMail Sicherheit, Attachement scanning
- Finish the Project with implementation and hand over to operations

Entwicklung und Implementierung Blockchain Encryption

2020 – laufend

Entwicklung einer Blockchain Sicherheits Struktur, Encryption mit der Hilfe von QKD (Quantum KeyDistribution) over Fiber Optics zwischen 2 Daten Zentrums. Hoch Sicherheits Entwicklung fuer finanzielle Anwendung in

Asien. Das Projekt ist ein Firmen Projekt (SecureScrypt Pte. Ltd.) mit Firmen Team Member. Das Projekt unterliegt hoher geheimhaltung

Entwicklung und Implementierung einer Cloud Management Plattform

---

04/2020 – 31/10/20 **Entwicklung einer Cloud Mangement Plattform mit Payment Gateway fuer Verkauf von SaaS Anwendungen und Services. Gemeninschaft Projekt in Asien fuer eine Regierungsstelle. Gemeinsames Projekt mit dem SecureScrypt Team in Deutschland.**

- Verantwortlich fuer die Architektur einer nicht oeffentlichen Cloud, welche keine Verbindung zu cloud Dienste wie AWS oder Azure hat.
- Verantwortlicher Leiter der Entwicklung einer neuen Plattform fuer die Bereitstellung von Cloud Services
- Entwicklung des neuen Payment Gateways SentosaXchange, fuer Marketplace Transaktionen im Cloud Umfeld
- Verwendung einer ERP und SCM Plattform, welche es erlaubt Cloud Dienste anzubieten
- SEPA Gateway faehig fuer digitale Payment Transaktionen
- Die gesamte Entwicklung muss bereits darauf vorbereitet werden Blockchain Dienste in Zukunft ebenfall anzubieten.
- Beachtung von Magnet, NUIX, Griffeye und XWAYS Applikationenals Teil der Entwicklung
- Dienste wie IAM und PAM (SaaS) muessen auf der Plattform integriert sein
- Vorraussetzungen: Gute Kenntnisse von NIST, Docker, Linux, Red Hat, ISO17789 IAM, PAM, SaaS, Cloud systeme, Cloud Mangement, spezielle regionale Anforderungskataloge
- Kenntnisse ueber Cloud Sicherheit in grossen Enterprise Netzwerken
- Training von Personal in administration der entwickelten cloud Dienste
- Erstellung von Dokumentationen

ERP/ SCM System Singapore Pte

07/2020 – 30/09/20 **Vorbereitung einer neuen Blockchain basierten Sicherheits Plattform (PAM/IAM/SIEM/SOAR) als komplett Paket zum Verkauf an interne und externe Mitglieder / Tochtergesellschaften der Firmengruppe in Singapore/South East Asia**

- Verantwortlicher Leiter des Verkaufs-teams, technisches Training und Verkaufsargumente
- Zusammenstellung moeglicher neuer Kunde fuer das Produkt ausserhalb der Firma
- Unterstuetzung , Kommerziell und technisch fuer das neue Produkt
- Verantwortlicher Leiter des technischen pre-sales teams,
- Verantwortlich fuer die Architectur und angepasstes Konzept des neuen Kunden
- Erstellung des Kompletten Angebotes angepasst an die Infrastructur des jeweiligen Kunden
- Unterstuetzung beim Verkauf des Konzeptes
- Technische Unterstuetzung des Kunden bei der Einfuehrung und Inbetriebnahme sowie „Lifetime“ des produktes
- „Subject Matter Expert“ Sales/Pre-sales, technische Betreuung
- Erstellung einer kompletten Dokumentation und Uebergabe an den internen Vertrieb

Technologies employed:

- IAM-IDM-PAM neue Entwicklung auf Blockchain Technology

Bundes –Oeffentlicher Dienst (confidential**)

02/2020 – 07/2020 **Oeffentlicher Dienst - PM – On premises netzwerk - Integrator eines completten CyberArk -IAM-PAM-PSM-Vault systems mit Integration / Onboarding von etwa 64 AWS (Militaer Umfeld), Berater/technischer Konsultant**

Vertraulich: Aufbau eines voellig neuen Systms mit Sicherhheitsgateways Mit sicheren Schluesselspeichern HSM,DDI,IAM, PKI, implementierung von BSI und BMWI Vorgaben, NATO level.

- Audit aller Systeme und Services
- Verantwortlich fuer Migration, Architektur und Implementation von BeyondTrust zu CyberArk
- Neu Installation und Integration und teilweise Administration,
- CyberArk Zugriffsschutz, Windows, Mainframe,Oracle Datenbanken, Enterprise Firewalls,
- Integration der OMADA (OIS) IAM/PAM Identity suite (Konzeption,Architektur und Implementation)
- Verantwortlich fuer Planung, Ueberwachung, Technologie, Applikationen
- Direkt verantwortlich gegenueber Geschaeftsfuehrung fuer alle Phasen einschlieslich operational.
- Projekt Aufgaben mit direkter technischer Verantwortung und hands on
- Script Entwicklung mit PowerShell, VBS und Batch
- Vorbereitung des Pre/Sales Teams, technisch und kommerziell zum Verkauf des neuen Sicherheits Produktes an die Tochterunternehmen

Technologies employed:

- CyberArk, Antivirus Solutions, PMS, Wallet, Vaults ….
- Pentests im Enterprise WLan netzwerk
- MS Windows Server 2012 R2,/2016/2020, Windows 7+10 Clients, Mainframe, Linux, Oracle, SAP
- Microsoft Client Betriebssystemen Windows
- Check point VPN , end2end, Citrix RDP
- Microsoft Active Directory + ADFS, LDAP,…
- TCP/IP, DNS, LAN/WAN, Client/Server, Monitoring
- Scriptsprachen und Programmierung (z.B. Powershell, Perl, Python)
- RedHat Enterprise Linux, Oracle, SAP
- Omada Identity Suite im Windows Umfeld (technische Beratung)
- Azure / AWS Stack
- Kompetenz (z.B. ITIL, ISO9001, IS rules, DevOps concept, Agile, Scrum, MS Office, Jira)

- Migration der vorhandenen Test, Entwickler und Produktions Umgebung / Server von CyberArk 10.X nach CyberArk 11.X

- Besondere Situation: Der laufende Produktionsbetrieb darf nicht gestoert werden, keine neue Hardware kan eingesetzt werden, Das vorhandene Testnetz wird zunaechst migrated und dann in die Produktion verschoben. Entwickler haben kein wirkliches separates Netz, sie haengen am Test Netz und muessen damit auskpmmen.

- Das Netz ist voll redundant aufgestzt, nach CyberArk vorgegebener Architektur

- 64 angehanegte Geschaefts Einheiten mit Applikationen und Use cases muesen entweder migrated werden oder neu aufgenommen (onboarded) werden.

- Technische Hands on Arbeit, Ueberpruefung von Entwicklern und Schittstellen, Hilfe bei Scripten ist notwendig und muss durchgefuehrt werden
- Dokumentation sind zu erstellen

IT- Logistic-Transport (confidential**)

10/2019 – 03/2020 **(externer) Teilprojekt Berater – SOAR Enterprise – technische Beratung - Planung – Implementation von Siemplify und CyberArc Umgebungen (Luftfahrt und Logistik Umfeld) – vorbereitung des Pre/Sales Teams zum Verkauf an die Tochter Unternehmen**

Ueberprueft Paragr. 7 LuftSIG, bis 2025

- Architektur - Beratung
- Pre/Sales konzeption
- Technische Unterstuetzung
- Projekt Management Einfuehrung SOAR
- Auswaehlen der Vendoren
- Verhandlungen mit Vendoren und SLA
- Verhandlung mit neuen Kunden
- Erklaeren der Vorteile des Produktes
- Definition der Prozesse

Technologies employed:

- Governance erstellen der vorhanden Sicherheitskonzepte bei Hauptkonzern und Tochtergesellschaften (Kunden)
- Direkt oder indirekter K t mit Arbeitspaketen
- Setzen der notwendigne Penetration Tests auch im Cloud Umfeld
- Festlegung der Koordination
- Management des Aufbaus
- Cloud Architektur – Aufbau in Azure
- Planung einer Cloud Architektur, SaaS
- externe IT Provider (IBM,Telekom, Siemplify, Incman,Demisto)
- Auswahl des SOAR Vendors Siemplify
- Auswahl der ersten Kunden zur Einfuehrung

- Strategische Vorbereitung des Verkaufs Teams
- Aktive Mitarbeit beim Verkauf
- Arbeiten mit Splunk, MicroFocus,Sentinel,Omada,CyberArk,HPServiceDesk, auf Linux,Unix,Windows Platform in Azure Cloud
- SDLan, VPN Horizon
- RFI, RFP, PoC
- Aufbau in der Cloud (Azure)
- Erstellen von scripts mit Powershell
- PoC, Pilot, Sandbox, Betrieb
- Planung des on boarding verschiedener BU
- Erstellung der gesamten Dokumentation
- Agile, Scrum, MS-Project, Jira, Clarity,Sprint, Gitlab, Scrum,Kanban
- Aktive handson tägliche technische Arbeiten mit allen internen Abteilungen
- Taegliche Status Meetings – C-level Reports

Sicherheit – Automotive Sektor
(confidential**)

04/2019 – 10/2019 **Hauptprojekt Leiter / Berater – Cyber Security in embedded automotive platforms (Cyber Ark, PAM, IAM, SIEM , SOC , Datacenter, Applications , – Planung – Implementation (VWFS Braunschweig Umfeld.Sicherheit)**

- Verantwortlich fuer 3 Teilprojekte,
- Sicherheit in embedded systems in der Automotive industry
- CyberArk Zugriffsschutz, Pentest
- Windows, Mainframe,Oracle Datenbanken, Entwicklung
- Enterprise Firewalls, Integration der OMADA (OIS) IAM/PAM Identity suite (Konzeption,Architektur und Implementation)
- Verantwortlich fuer Budget Planung, Ueberwachung, Technologie, Applikationen
- Angebotserstellung an externe Nutzer (Kunden)
- Von Planung bis Implementation, weltweit
- Direkt verantwortlich gegenueber Geschaeftsfuehrung fuer alle Phasen einschlieslich operational.
- Verhandlungssicher mit Lieferanten und Dienstleistern
- Projekt Aufgaben mit direkter technischer Verantwortung und hands on:

Technologies employed:

- CyberArk, Antivirus Solutions, PMS, Wallet, Vaults ….
- Pentests mit Wireshark und Aircrack im Enterprise WLan netzwerk
- 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
- Omada Identity Suite im Windows Umfeld (technische Beratung)
- Einfuehrung des IAM/PAM NetIQ (von MicroFocus)
- 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)
- Erarbeitung einer SOAR Loesung fuer Cloud Betrieb

IT – Enterprises - Finance

09/2018 – 03/2019 **Projektleiter, Technischer PM (Financial Industrie) – Planung und Implementation eines SOAR**

- 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
- Integration HiScout GRC Governance Risk Compliance im Rahmen BSI Grundschutz – Informations Sicherheit
- Komplette technische und kommerzielle Dokumentation, zur Weiterverwendung innerhalb der Gruppe

Technologies employed:

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. (Integration in das SOAR)

- 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 (from Concept,Testphase to Implementation) 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.
- Planung der Penetration Tests fuer des Pentest team (Burp Suite, MetaSploit)
- Entwicklun eines SIEM Handbuch und Security Operation Manual
- Hilfsmittel und Projekt Vendoren: AgileSI, BlueLiv, CheckPoint, CyberArc, Exabeam, Cylance, SAFe ForeScout, F5, Resilient (IBM), LasLine, LogRythm, 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 Zertifizierng nach BSI, 27001, 27002
- Anschluss Projekt (Project Plan in MS Project):
- Segmentierung der Infrastrcture Architektur fuer Cloud Migration

Vorbereitung zur Migration nach Azure und AWS cloud.

- Proof of Concepts - Unterstützung und Beratung
- Cloud Governance
- Cloud-Readiness-Assessment
- Cloud Vision und Strategie
- Cloud Onboarding
- Technische Implementierung
- Abschluss Dokumentation

Telco Industry

11/2017 – 10/2018

MNC, Global Projekt Manager fuer 3 Teilprojekte in Telco Industry

- Audit aller Systeme und Services
- 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.
- Agiler Ansatz, Splunk fuer alle Teilprojekte und Platformen

Technologies employed:

- 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
- Einfuehrung der OMADA IAM Plattform fuer Cloud
- Pentests im enterprise Umfeld
- 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

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 "Geheimschutzhandbuch" 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 Infrastrktur

- 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 ServiceSicherheits Konzept fuer die Einrichtung und Inbetriebnahme eines neuen Daten Zentrums. Angepasstes Sicherheits Konzept, Audit der vorhandenen Infrastruktur, Entwurf des neuen high Level Designs und Architectur. Abschliessende Beurteilung und Vorbereitung fuer notwendige Zertifizierungen.
- Spezifikation aller Sicherheits Massnahmen
- Zusammenarbewit mit internen Teams
- Entwicklung von neuesten Sicherheits Komponenten

Teilprojekt 2

Netzwerk Architektur abbilden, Implemetierung und Konfiguration einer Priviledged Access Management Loesung und Cloud Migration – Technischer PM
Skills:

- Priviledged Access Management (PAM)
- Identity and Access Managmenet (
- NetIQ installation
- Netzwerk und Infrastructur Architekt
- GIT Codeverwaltung
- Planung und integration von Lancom VPN/Lancom 9100 GW
- 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

IT - Bank (Deutsche Bank)

05/2017 – 04/2018 **Project Team 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

Vendor Relations, confirmation of IBM Security products,

Entwicklung eines SIEM

- Security Compliance Management, IAM, SAM , AMR4V Process / Cloud Migration
- Team member für die Entwicklung eines globalen Netzwerk von ca. 25.000 Server und Datenbanken
- Einführung eines ISMS unter Beachtung der neusten DSGVO und EUGDPR Verordnungen

Technologies employed:

- 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
- Codeverwaltung GIT
- Implementation von Monitoring Tools zur Kontrolle der Stabilitaet und anderer Prozesse
- Endpoint Security (BM BigFix, Tanium, Checkpoint, GFI, HPE, Sophos, Kaspersky…)

- Penetration Tests im Wlan und cloud Netzwerk (Aircrack, Wireshark, w3af)
- 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 Informationsysteme 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 , Testsystem einrichten, endgueltige Uebergabe zum operativen Betrieb
- 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
- Unterweisen und helfen eines Team‘s von ca. 19 Sicherheits- und Netzwerkexperten auf allen Ebenen

Enterprise IT - Telco

09/2016 – 04/2017 **Senior Enterprise Security Architect (ESA) bei einem Internationalen Telekommunikations Unternehmen (IT security)**

- Dokumentation und Durchfuehrung von Sicherheits Vorgaben nach BSI 100 Grundschutz und ISO 27XXX
- Beratung des Konzerns bezuegich Cloud Migration

- Risk Analyst
- Level 3 Suppor

Technologies employed:

- Projektierung eines neuen / erweiterten SOC /ISMS
- Erarbeiten eines Vnware conceptes, SaaS fuer die naechste Generation server and services
- Anwendung von Automatisierungs werkzeug Ansible und Terraform
- Prozess Erstellung fuer ein SIEM
- Neugestaltung des WIN 10 Update und Patch Prozesses
- Process Management Konzepte Hpe ArcSioght, McAfee ePO
- Erstellung einer Governance im Enterprise Umfeld-
- Erstellung eines ISMS und Beratung zur zertifizierung-
- Erstellung eines Penetration Test Konzepts
- Vorbereitung zur ISMS / ISO 27001 zertifizierung-
- Beratung und Presentation – Risk Analyse
- ESA end-to-end , Netzwerk Segregations, etc.
- Encryption Vorschlaege für das gesamt 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
- Dokumentaion von Embedded Software unter Linux/Android
- Dokumentation von Sicherheits Prozessen und Funktionen im Mobilen und festen Netzwerk Bereich
- Erstellung von Manuals / Handbuechern
- Dokumentation vorhandener Software fuer den Systembetrieb
- Erstellung von Trainings Konzepten im Betriebs Umfeld
- Erstellung Kryptographischer Loesungen im Mobilen Umfeld
- Dokumentation / Entwicklung von Test und Entwicklungs Umgebungen-Configuration auf verschiedenen Platformen, Winodws, Android, IOS unter Common Criteria Evaluation
- Übergabe in den Regelbetrieb am Projekt Ende

IT – Energy und Chemie/ Pharma

07/2016 – 08-2016 **Entwicklung von Schulungskonzepten und Prozessen zur IT Sicherheit basierend auf BSI Grundschutz und ISO 27001**

Workshops zum SOC und SIEM

- Projekt Dokumentation Erstellung

Technologies employed:
Schulungs Inhalte

- Einfuehrung 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 Handlungs¬empfehlungen
- Durchführung von Penetrationstests und Sicherheitsanalysen inklusive Aus¬arbeitung von Angriffsszenarien und Dokumentation von Arbeitsergebnissen
- Erstellung von Leitlinien fuer IT Sicherheit
- Verwendung von Wireshark Penetration Software
- 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 Kentnisse in Windows 10 und Windows mobile
- Sicherheit von SAN und NAS, SANE (storage area network encryption)
- Abschliessende Beurteilung eines gesamt Sicherheitskonzeptes mit praktischer Implementierung

Logistic und Transport

02/2016 – 07/2016

Team member / Berater - Projekt bei einem des groessten Transport und Beforederungsunternehmen in Europa (Deutschland) – Erweiterung und Absicherung des vorhandene GSM-A Netzwerkes – Planung von Uebergabe an ein neues LTE Netzwerk

- Audit aller Systeme und Services
- Planung und layout des vorgesehenen Real Estate,
- Planung notwendiger Hardware, Erstellung von Rahmenvertraegen fuer Lieferanten,
- People Management, Relevante Prozess neu strukturieren
- Monitor/Analyze Network Traffic, IDS Alarm,
  etwork 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. Documenten und Berichts Prozesse aller Vorfaelle. Prozesse zur Incident automatisierung

Technologies employed:

- Audit aller Systeme und Services
- 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 (GSM-A Standard)
- Planung und Implementation * eines SOC (Security Operation Center) , zusammengefasst fuer die Verschiedenen Abteilungen (Systel, 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
- Pentest durchfuehrung mit Pentest team (extern)
- Riskmanagement, Risiko Analyse
- Gefärdungs Analyse mit Restrisiko Abschätzung
- Planung der Sicherheits Zertifizierung
- BSI Grundschutz, ISF, Cobit, BNA, ITU 1501
- Analyse des GSM-R Networks und Schnittstellen zu Systel ,LST…
- Verständnis von neuen Planungen, IP Networks und Re-investment Projekts, LTE updates …..
- Praktische implementation aller Ergebnisse und Process in ein SOC
- Planung der Übergabe in den Regelbetrieb

IT – Oeffentlicher Dienst

09/2015 – 02/2016 **Teilproject – Team Member – Data Center Migration und Erweiterung – Neuaufbau des Rechenzentrums – Neu aufbau der externen Klienten (Polizei – Zoll- BAMF) Anschluss an Black Fibre**

- Planung
- Implementation
- Uebergabe in den Regelbetrieb

Technologies employed:

- 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
- Decommisioning 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 gemaess 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, Rahmenvertraege
- 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

IT – Industry – Entwicklung Herstellung

02/2009 – 09 /2015 - 6 Jahre 8 Monate Auslands Aufenthalt (Asien / Singapore PR)

Telecommunications – MNC- Intl. Banken – Fabriken – China Herstellungs Management von Telecommunication und Smartphones – Verkaufs Director Neoi Pte. Ltd.

- Software Entwicklung
- Hardware Entwicklung
- PCB layout
- Entwicklung von Sicherheits Konzepten und Processen im Windows und Unix Umfeld
- SLA Entwuerfe, Fabrikations Planung und Ueberwachung
- Kontrolle von Ipr’s
- Planung von neuen Threat Monitor Prozessen

Technologies and responsibilities:

- Direktor (Mobile IT - Cyber Security – Unterstützung, Management, Konsultant) Professionelle Konsulting Gruppe, Securescrypt erworben von PIC -Technologie im Jahr 2009
- Verantwortlicher Direktor fuer Firmen Leitung unter lokalen Vorschriften, Vertrags Position
- People Management (120 Konsultants), Vendor Management, Rahmenvertraege
- Konsultant und Projekt Manager, IT HR **
- Manager Team Cyber Security
- Entwicklung moderner Verschluesselungen im mil./Regierungsbereich
- 2014 fuer die Fussball WM, Entwicklung einer Ferseh 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, Riskasessments
- Spezielle Software Kentnisse : 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 Algorythmen
- 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

01/2005 – 01/2009 **Telekommunikation und IT Netzwerke – Support und Services - PIC Pte. Ltd. Hong Kong**

- Mitarbeiter Schulung
- Risk Mangement
- Netzwerk Architektur
- Netzwerk Sicherheit

Technologies / Responsibilities:

- Leitung vonn 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 **Interims CTO Elektronische Entwicklungen – Lintux Hong Kong Ltd.**

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

Technologies employed: Drahtlose Kommunikation

11/2003 – 7/2004 **SVP Goldtron Group Singapore Pte. Ltd.**

- 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

Technologies employed: GSM Technology – Europa Standard

12/2000 – 10/2003 **Entwickler Taitoma Group – Taipei – Taiwan – Industrie Netzwerke**

- 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

Technologies employed: **J**ava, SQL, Python, Cobol, C++,....

10/1999 – 11/2000 **Vertrags Ingenieur PIC Intl. Hong Kong**

- 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 verschluesselte Satelliten Telefon fuer eine deutsche Gruppe, welches dann vom oeffentlichen Diensten und Schiffen verwendet wurde.
- **Nebenbei Fernstudium Princeton University USA , Abschluss Phd. Dr.**

Technologies employed: VHF-UHF Technologien – Verschluesselung von Telecommunication

IT – Banken – Investment Industrie

02/1998 – 11/2000 **Credit Suisse First Boston (Hong Kong) – VP / IT – Leiter der Asien Pacific 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
-

Technologies employed: MicroSoft Windows

01/1997 – 01/1998 **Senior Konsultant MERRILL LYNCH Internatioal Inc. Hong Kong**

- Netzwerk Migrationen
- Einrichtung des IP Netwerkes
- Entwicklung von Investment Applikationen zum monitoring des Akyien Marktes

Technologies employed:

- 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

ENGINEERING - Mobilfunk - Netzwerke

01/1988

Senior Systems Ingenieur

- Entwicklungen
- Umsetzungen
- Installationen

Technologies employed:

- 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 angwendet 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, Verschluesselung von Mobile Geraeten

1987

PATHCOM Inc. Las Vegas USA – Minthorne Intl. Inc. New York . Pathcom Ltd. Tokyo, Japan

- Entwicklung von CB und UHF Funkanlagen
- Ueberwachung der Herstellung in USA und Japan
- Weltweite Kunden Betreuung

Technologies employed:

- 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 JapanHerstellungs Kontrolle und Unterweisung
- Entwickelte den ersten asiatisch hergestellten Radio Synthesizer , VHF- und UHF- Transceiver und Bündel Handy,System Entwicklung und Fertigen der Pathcom Kommunikationsprodukte

Schule-Ausbildung-Studium **(vertraulich, Veroeffentlichung aus Datenschutz untersagt)**

Berufs Praktikum nach Studienabschluss

- Elektrischer Kundendienst
- Buero Verwaltung
- Mitarbeiter Fuehrung

Studium

- TU Darmstadt Elektrik,Elektronik, Mthematik, Physik
- Diplom Ingenieur – Philipp Reitz Polytechnikum - Frankurt
- Mitarbeiter Fuehrung, Wirtschaftswissenschaften, Marketing

Abschluss Meister Elektrik

- Lehrling
- Geselle
- Meister Pruefung - Wiesbaden

Abitur Humanistic Gymnasium Wiesbaden , Durchschnitt 1.1

- Mathematik
- Englich

Fernstudium USA – Phd. Telecommunication