Dipl.Ing.Bernhard Bowitz © 2024

Nationality:	**German National - (also Singapore PR work permit)**
Usually located at:	**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)**

Security Clearances:	**German / European SÜ2 (until 2026) and Paragr. 7 LuftSIG, Air Security Clrearnce until 2025**
Education-Experience	**Diplom Ingenieur ,IT-Network Engineer, Software Developer, Project manager,... more details below in complete 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, RHEL Openshift, Erfahrung an Anforderungen durch Geheimhaltungsgrade der Bundesrepublik Deutschland (Verschlusssachenanweisung), sowie EU, NATO und MISSION...more in CV below...**
Languages:	**German (Mothertongue 1), English (Mother tongue 2) , Spanich (Basics) ,Chinese (Basic)**
Summary – short term CV	**More than 30 years working as a technical PM/IT Engineer, Analyst, Architect,... more details below in complete CV**
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,... more details below in complete CV**
Industry Experience:	**Governments, Military, Finanz, Banks, Automotive, Insurances, Internatonal Industries, Chemical, Health, Multi National Corporations Europe, Asia,.... more details below in complete CV**
Dataprotection Information:	**The information contained in this document falls under statutory data protection. Any reference, distribution or use, even partial, is only permitted with the WRITTEN permission of the author!**

Complete CV

Position Projects Career: 1988 - 2024 (ongoing).

TOPIC, the latest summarized:

I am specialized in digital security for more than 15 years now. I have been certified Ü2 and LSÜ2 (aviation security) for many years and have taken part in several BSI courses, in addition to my numerous other certifications
I managed and technically implemented several projects, particularly in the area of VS-NfD and NATO security.I am an expert in NATO directives compliance.
I proposed and developed “all in one” solutions from VSA-compliant data processing to SECRET, according to my customer’s requirements in an advisory role as well as a technical role, and also implemented them hands-on.
Advice on how classified information should be processed digitally throughout, under VS-NfD conditions.
I was and still am active in the development of secure hardware, at network layer 2: transmitting large amounts of data quickly and securely, mobile platforms for mobile devices - from smartphones to tablets. I have identified vulnerable system points and suggested, developed and implemented appropriate protective measures ..
I'm at home on all systems...
My customers are from the public, military and industrial sectors, my experience lies in the areas of network security, endpoint security, VS, state security, sovereign tasks, electronic identities, compliance, PKI, certificates, email and web security, as well as obvious border areas such as IAM, PAM etc.
In financial areas I work primarily based on suggestions of 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..

Strength and experience....

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

Basic consulting experience (also "hands-on") ...

- I am an educated and trained sales engineer with more than 20 years of experience in product development, product marketing and customer acquisition, especially in the areas of telecommunications, digital communication, network and cybersecurity ...
- Planning / conceptual design as well as consulting services in relation to the entire IT/Networks, from Conception to implementation, as well holding workshops and team training
- Pre-sales Coordinator, technical and commercial sales manager, sales team consultant
- Planning / conceptual design as well as consulting services in relation to information security guidelines
- Planning / conceptual design as well as consulting services in relation to IT security concepts
- Planning / conceptual design as well as consulting services in relation to IT service management (including service design and agreement of SLAs), negotiations with suppliers
- Planning / conceptual design as well as consulting services with regard to degrees of secrecy (security lock instructions etc.) in the area of authorities (national, EU, USA, embassies, as well as other regions and alliances)
- Since 2020 Development of Blockchain encryption on Quantum Computer Technology

I use my strengths and very broad experience for ...

- Help and support clients in finding the right business and technology solutions by working as a consultant and consultant on design trend-setting security architectures. Main goal is the sales of a product for the technical and commercial advantage of a client
- Assist my customer to build a sales team with the correct arguments to sell (my developed) product to third party clients, Subsidiaries and daughter corporations

• Lead projects to the desired success by working as a project manager
• Support of the company's research departments to find new market solutions in order to achieve sales growth and profit in the fields
• Process creation for the establishment of SOC, SIEM, ISMS, SOAR, IAM, PAM, PAS, CISO, Blockchain Security etc.
• Development of new products and services (software and hardware), IT and telecommunications
• Support of sales and marketing for the position of products and services in future markets
• Training and creation of high-performance service teams to have even the most demanding tasks in the industry under control
• Risk & Compliance Management

Industry experience – roles….

• Banking - Secure banking via the Internet - Smart Card access
• Automotive - GPS - internal electronics
• Transport and traffic, energy, GSM-R, aviation, automotive industry
• Test and certification, BSC, MSC, BSS, NSS
• (E) Government - eBanking - eCompanies
• Source code analysis, adaptations, extensions, corrections
• Risk management, risk / residual risk analysis
• IBM (Qradar), HPe ArcSight, McAfee ePO, MicroSoft Security, CyberArk, Fireeye, Sophos, EndpointSecurity
• IT / TK technology - for large industry and consumers
BeyondTrust, Sophos, Endpoint Security, TrendMicro
• 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

Technology – Hardware – Software Expertise....

Technology expertise (25 years ++)

• **Expert in the development of modern cloud infrastructures, private clouds, new types of cloud platforms with marketplace portals for selling cloud services**
• - Expert in privileged access security (PAM, PSM, EPV, CPM, PVWA), a critical layer of IT security for protecting data, infrastructure and resources throughout the company, in the cloud and in the entire DevOps pipeline
• Network segmentation, NGW, VLAN security concepts,
• Expert in **Secrecy levels** like the German VS-NfD on TC/IC Networks
• Expert in Privileged Access Security (PAM, PSM, EPV, CPM, PVWA), a critical IT security layer protecting data, infrastructure and resources across the enterprise, cloud and DevOps pipeline
• Knowledge of the German Secrecy Handbook (internal Government priviledged)
• UE2 certifying ongoing....2023.....
• A-960 military Information Security Concepts based oon BSI Basic Protection
• Vendor management, certified with many service providers and application providers
• Source code analysis, adjustments, extensions, corrections
• IAM, SAM, PAM, GRC, AMR4V, Frontdesk, CyberArk, BeyondTrust, Qradar, ...
• Qradar, TheHive, Cortex, NexPose, MISP, zAlert, SIEM, SOAR,….
RHEL Openshift
• Java, C ++, SQL .....
• BeyondTrust, Sophos, Endpoint Security, TrendMicro
• Beyondtrust – privileged Remote Access, Z-scaler
• Script development with PowerShell, VBS or Batch
• BCM – GRC HyScout suite
• PKI, SSL , MS NDES, SafeNet Networks HSM
• Cloud Azure, AWS, Strato, Telecom, SaaS, LaaS, XaaS, TrendMicro Deep Security Antivirus.....
• Risk management, risk / residual risk analysis, GRC
• HPe ArcSight, McAfee ePO. Kapersky 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 technology - for large industry and consumers
• Data center architecture
• Large networks, industry and public sector
• Penetration Testing Tools - Wireshark, MetaSploit, AcuNetix Scanner, w3af, Netsparker, Burp Suite, Aircrack
• Wireless and mobile (Android, Windows) networks
• Creation of documentation, support solutions
• Prototype design, manufacture management

• Project Management, Big Data, Scrum, Kanban, MS. PMO
• Creation of test environments and necessary tools

Hardware expertise (25 years ++)

• - 2015, developed the first portable passport scanner on Android core, with integrated multi fingerprint scanning for border patrols, the registration of asylum seekers, police, BKA, security forces, banks ... ..
• - Semiconductors, chipsets - design and embedded software Mobile hardware and software - especially the latest cyber security with a special chip-based algorithm, AES 256, Diffie-Hellmann PKI
• - Identification with biometrics (fingerprint, patented high security solution Nurugo) - Security based on new SIM card technology ...
• - Java, Json
• - Cloud Security - SaaS - Enterprise - Government - Public Services - Military - Endpoint Security -
• - Azure, AWS, Blockchain - cloud migrations, from concept to implementation
• - Internet traffic - access identification
• - Secure transactions - UAF access without passwords - Special military classified security
• - NFC smart card
• - Research and development, software developers, hardware developers
• - IP - VoIP networks, voice, messages, data, video
• - New technologies based on SIM and SD cards, identification without passwords
• - Analysis of network security, risk management, risk analysis, hunt for cyber criminals and hackers
• - Personal security - Biometrics - CCTV systems with biometric detection methods
• - New high security solutions for HR and other applications with mobile devices
• - Blockchain network security and applications
• - Development of a SIEM SOC, from design to implementation (including IBM Qradar and TheHype / Cortex) integration

Roles....

• Consultant, enterprise project manager / project manager / MS-Project / Clarity PMT / Sprint / Gitlab /
• Sales and Pre-sales Consultant/Manager/Team Leader – new customer acquisition
• Agile / Jira certified / Scrum Master
• Consultant, PMO / Administrator / Security Auditor (27001 / BSI), IT architect
• Technical PM with "Hands On"
• DVSGO consultant according to EU basic protection guidelines
• Software development / programming / hardware design / network architecture
• Advice / Consulting / Hands On / Technical PM
• Project management / leadership / organization / coordination /
• Team leadership of teams of up to 80 members,
• Global, on-site and remote penetration testers, test managers
• Engineering / IT-related engineering services
• Cloud architect
• Blockchain developer

Summary – Short Information- CV

Comprehensive advice for customers on the introduction of new software or IT solutions. In-depth needs analysis when determining the required software and hardware. Development, planning and implementation of IT concepts.

• Project manager consultant, project management office, technical project manager, from concept creation to application
• Creation of sales strategies for newly developed security and other IT products and projects
• Creation of SLA's, support of suppliers, creation of technical and project-related tender documents
• Data security officer - technical support / advice for companies in compliance with the regulations of the BSI IT-Grundschutz, BSI TR, BaFin (Bait, VAG, WpHG, WpPG, WpUEG, BoersG, VAIT, KAIT ....), compliance with the secret protection book of BRD, understanding of the Chinese data protection law of 2020, regulations of the US American data protection.
• 100% remote and 100% on-site, or mixed as needed
• CORONA information - during the CORONA restrictions, we work 100% remotely in all projects with the aid of VPN connections and ZOOM conference systems. The highest level of security guaranteed. For VPN and work

applications, we use our high security MERP blockchain platform.
• More than 20 years, working (multilingual, German, English, basic Chinese) operational and non-operational, analytical and administrative, development and process development, project management,
• Leadership of multinational teams of all sizes, many years of experience in areas such as data centers, networks, mainframe, Oracle, Unix, Linux, Windows (certified), ...
• Infrastructure management, ISMS / ISO27001 / 27005-2013, BSI100..XX, training courses, CISSP, AISP, ISO certified, IT consulting, IT / cyber / network security (encryption, PKI), BSI 100, BSI security tools,
• Basic protection, networks (mobile (LTE, 2G, 3G, 4G, ...), Ethernet, wireless), VoIP networks (e.g. Avaya, Cisco ...)
• Cloud security and administration, public networks, DOI, IVBB, IVBV, VPN, project management, endpoint security
• (Genoa, Sina, Checkpoint ...), SOC, Blockchain and eCoin, work with any platform (Windows, Mainframe, Unix, Linux, RHEL Openshift, Oracle etc.),
• CyberArk, SOAR, SIEM, SiemPlify (from concept to application and implementation), Qradar concept, extension, application, clouds ...
• Since 2004 I have successfully completed several ISMS / ISO 27001 / BSI 100 certifications. I am CISSP, CISA, MCP, AISP, BSI and others certified.
• I speak English as my second mother tongue, as well as Chinese Basic, Spanish as colloquial language.
• Expert in data center migrations, hardware and software, development of security based on BSI basic protection.
• Have successfully completed several ISMS/ISO 27001/BSI 100 certifications since 2004. Am CISSP, CISA, MCP , AISP, BSI and others certified.
• Speak English as a second mother tongue, as well as Chinese Basic, Spanish slang.
• Expert in data center migrations, hardware and software, development of security based on BSI basic protection. Cloud migrations….
• Work worldwide, experience in DACH, USA, Asia

References

• Carry out training on the latest state of the basic protection
• Process creation for SOC, SIEM (i.e.. Splunk, Qradar, LogRythm, Siemplify...),, SOAR, PAM, IAM, ...
• I am a Senior Network Security Professional (CISSP) with a broad understanding of the technology and associated applications. My experience spans both areas, cellular networks and traditional networks.
• State of the Art "Security Architectures, BSI IT-Grundschutz, ISO 27001, ISO 80001, IT Sig, Relevant Security in Federal Agencies - SG - Bamf- EHR-BDR and others, Enterprise Security .....
• My focus is on all aspects of IT and telecommunications (telecommunications) security from basic technology to the application layer. That means from hardware to software development and consulting and advisory services as well of sales of the developed products including finding new markets and customers
• Especially in the last few years I worked in the infrastructure and mobile security environment of Big Data with the aim of analytics technologies for new analysis concepts and for the active search for security anomalies in order to prevent and reduce attacks.
• The special strength lies in the mobile area, Android / IOS, development of secure applications in payment transactions and e-commerce
• as well as complex network structures, big data, cloud security,
• SIEM, endpoint security and advanced security, in both practical and administrative environments.

I have written documentations, Operational Manuals, and more then 1000 papers all around IT. All my write ups are in my personal Library, available on demand to my customers.

Positions-Projects-Career: …. – 2024:

7/2024 – 12/2024

Security for Large Networks Across Europe (VS-NFD Project)

Consulting, planning, verification, documentation
Strictly confidential

Technical Consulting in the Network Area
Migration planning, segmentation, IP harmonization
The focus is on supporting the regular operation of the network's security infrastructure
Identification, planning, and independent implementation of projects for updating or improving the underlying security infrastructure
Technical, active project management, leading internal teams
VS-NfD requirements

1/2023 – 5/2024

Consulting, planning and active project management for a closed, high security network.

- Technical advice in the network area
- The focus is on supporting the regular operation of the network's security infrastructure
- Identification, planning and independent implementation of projects to update or improve the underlying security infrastructure
-Technical, active project management, leading internal teams
- VS-NfD, BSI secret protection in closed networks
- GENU VPN architecture development and continuous update
- Architecture and development work in Windows and Linux areas
I am firm in OYTHON, Java and other languages, as well DevOps.
- network segmentation,
- Share Point Project Management
- RHEL Openshift update,
- Reporting to C Level and BoD
- Budget planning and suggestions for further development or new introduction of necessary security precautions.
- Management of the entire IT security department and all teams as well as vendors and service providers
- Customer name protected

9/2022 – 1/2023

Advice on the architecture of a hospital network.
Renewal of the network to the latest B3S security level
Advice on safety regulations in the health sector
Advice on the tender and implementation
Consulting, planning and active project management for a closed high security network

---

1/2022 – 8/2022

PM: Architecture-Conception-Implementation Complete rebuilding of a third-party connection platform and data lock with several thousand users (clients) High-security strategy up to Nato security level-on premises and cloud integration of Deep Security Enterprise solutions (i.e.Opswat-Infodas-SDot) Introduction of an IAM/PAM/LDAP in the

government network
Various connection solutions such as Thin Client, Sina, Terminal Services, ReCoBS.... in the VS-NfD environment

1/2022 – ongoing in the authority environment (highest level of secrecy UE2 clearance required)

- **Conducting a needs assessment for data gateways to other organizations connected to the network. The data is stored on high-security end devices.**
- **Developing the solution for a third-party connection platform to the network, connection of organizations.**
- **Evaluation and consolidation of requirements**
- **Identification and evaluation of possible solutions for the data lock with cost statement**
- **Developing the solution for a third-party connection platform to the network, connection of organizations.**
- **\using for BCM and GRC HyScout Suite integration**
- **Architecture in the authority environment VS-NfD**
- **RHEL updates Openshift**
- **Compliance with the requirements of the classification levels of the Federal Republic of Germany (classified information instructions), as well as the EU, NATO and MISSION**
- **Carrying out a market survey and creating a PoC/PoV to select the platform, data lock and connections**
- **Presentation of the finally developed solution**
- **Technical implementation for more than 2000 users**
- **Observance of BSI, NATO security regulations in closed networks and external connection of third-party organizations**
- **Creation of a complete audited project documentation**
- **Training workshops**

Architecture Conception Complete rebuilding of a SIEM (Splunk) with planning for the expansion of a SOAR/SOC/CDC - IAM PAM- Development of a Cyber Security Strategy-on premises and cloud
Integration of Deep Security Enterprise (Opswat-Infodas-SDot-Trend Micro)

11/2020 – (1-2022)

Voellige Neuentwicklung des Threat and Risk Managements ,
Neuaufbau von SPLUNK, Ziel Einrichtung eines automatisierten Threat Management (SOAR)

- Review existing security events
- Analyze available data sources, security tools,monitor threat trends
- Support configuration of security tools
- Manage SIEM Platform NetIQ, if necessary update and reconfigure
- Manage RHEL Openshift
- Identify logics to find attackers and develop Playbooks and use cases
- Plan future actions to secure the euopean 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 or Omada)
- Finish the Project with implementation and hand over to operations

Development and implementation of a cloud management platform

04/2020 – 31/10/20

Development of a cloud management platform with payment gateway For Sale of SaaS applications and services. Community project in Asia for a government agency. Joint project with the SecureScrypt team in Germany.

- Responsible for the architecture of a non-public cloud that is not connected to cloud services such as AWS or Azure
- Head of the development of a new platform for the provision of cloud Services
- Development of the new payment gateway SentosaXchange, for marketplace transactions in the cloud environment
- Use of an ERP and SCM platform that allows cloud services to be offered
- SEPA Gateway ready for digital payment transactions
- The entire development must already be prepared for blockchain services in the future also to offer.
- Services such as IAM and PAM (SaaS) must be integrated on the platform
- Requirements: Good knowledge of NIST, Docker, Linux, Red Hat, ISO17789 IAM, PAM,SaaS, cloud systems, cloud management, special regional catalogs of requirements
- Knowledge of cloud security in large enterprise networks
- Training of staff in administration of the developed cloud services
- Creation of documentation

ERP/SCM System Singapore Pte

07/2020 – 30/09/20

Preparation of a new blockchain based security platform (PAM / IAM / SIEM / SOAR) as a complete package for sale to internal and external members / subsidiaries of the group in Singapore / South East Asia

• Responsible sales team leader, technical training and sales arguments
• Acquisition of possible new customers for the product outside the company
• Support, commercial and technical for the new product
• Head of the technical pre-sales team,
• Responsible for the architecture and adapted concept of the new customer
• Creation of the complete offer adapted to the infrastructure of the respective customer
• Support in selling the concept
• Technical support for the customer during the introduction and commissioning as well lifetime of the product
• "Subject Matter Expert" sales / pre-sales, technical support
• Creation of complete documentation and handover to internal sales

Technologies employed:

- IAM-IDM-PAM new development on Blockchain platform

IT - Finance Industry - Bank

02/2020 – 07/2020

Public service - PM - integrator of a complete CyberArk -IAM-PAM-PSM-Vault system with integration / on-boarding of around 64 AWS (banking environment), consultant / technical consultant

• Responsible for migration,
• New installation and integration and partial administration,
• CyberArk access protection, Windows, mainframe, Oracle databases, enterprise firewalls,
• Integration of the OMADA (OIS) IAM / PAM Identity suite (conception, architecture and implementation)
• Introduction of RHEL Openshift
• Responsible for planning, monitoring, technology, applications
• Directly responsible to management for all phases including operational.
• Project tasks with direct technical responsibility and hands on
• Preparation of the pre / sales team, technically and commercially, for the sale of the new security product to the subsidiaries

Technologies employed:

• CyberArk, Antivirus Solutions, PMS, Wallet, Vaults….
• Pentests in the Enterprise WLan network

• MS Windows Server 2012/2016, Windows 7 + 10 clients, mainframe, Linux, Oracle, SAP
• Check point VPN, end2end, Citrix RDP
• Microsoft Active Directory + ADFS, LDAP, ...
• TCP / IP, DNS, LAN / WAN, client / server, monitoring
• Script languages and programming (e.g. Powershell, Perl, Python)
• RedHat Enterprise Linux, Oracle, SAP
• Omada Identity Suite in the Windows environment (technical advice)
• Azure / AWS Stack
• Competence (e.g. ITIL, ISO9001, IS rules, DevOps concept, Agile, Scrum, MS Office, Jira)
• Migration of the existing test, developer and production environment / server from CyberArk 10.X to CyberArk 11.X
• Special situation: the current production operation must not be disrupted, no new hardware can be used, the existing test network is first migrated and then moved to production. Developers don't really have a separate network, they are attached to the test network and have to deal with it.
• The network is fully redundant, based on CyberArk architecture
• 64 attached business units with applications and use cases must either be migrated or newly added (onboarded).
• Technical hands on work, checking of developers and interfaces, help with scripts is necessary and must be carried out
• Documentation must be created

IT- Logistic-Transport

10/2019 – 03/2020

(external) sub-project consultant - SOAR Enterprise - technical advice - planning - implementation of Siemplify and CyberArc environments (aviation and logistics environment) - preparation of the pre / sales team for sales to the subsidiary company

Certified/checked Paragr. 7 LuftSIG, until 2025

• Architecture consulting
• Pre/Sales conceptio
•Technical support
• Project management introduction to SOAR
• Definition of the processes

Technologies employed:

• Creating the Governance of the existing security concepts at the main group and subsidiaries (customers)
• Direct or indirect contact with work packages
• Setting the necessary penetration tests also in the cloud environment
• Establishing the coordination
• Management of the construction
• Cloud architecture - structure in Azure
• external IT providers (IBM, Telekom, Siemplify, Incman, Demisto)
• Selection of the SOAR vendor Siemplify
• Working with Splunk, MicroFocus, Sentinel, Omada, CyberArk, HPServiceDesk, on Linux, Unix, Windows Platform in Azure Cloud
• SDLan, VPN Horizon

• RFI, RFP, PoC
• Powershell scripting
• Structure in the cloud (Azure)
• PoC, pilot, sandbox, operation
• Planning the on boarding of various BU
• Creation of all documentation
• Agile, Scrum, MS-Project, Jira, Clarity, Sprint, Gitlab
• Active hands-on daily technical work with all internal departments
• Daily status meetings - C-level reports

Security –Public Services Sector

04/2019 – 10/2019 **Main Project Leader / Consultant - Cyber Security (Cyber Ark, PAM, IAM, SIEM, SOC, Datacenter, Applications, - Planning - Implementation (Public Environment, Security)**

• Responsible for 3 sub-projects,
• CyberArk access protection,
• Windows, mainframe, Oracle databases,
• Enterprise firewalls, integration of the OMADA (OIS) IAM / PAM Identity suite (conception, architecture and implementation)
• Responsible for budget planning, monitoring, technology, applications
• From planning to implementation, worldwide
• Directly responsible to management for all phases including operational.
• Confident in negotiations with suppliers and service providers
• Project tasks with direct technical responsibility and hands on:

Technologies employed:

• CyberArk, Antivirus Solutions, PMS, Wallet, Vaults….
• Pentests with Wireshark and Aircrack in the Enterprise WLan network
• MS Windows Server 2008 R2 and higher, Mainframe, Unix, Oracle, SAP
• Microsoft Active Directory + ADFS, LDAP, ...
• TCP / IP, DNS, LAN / WAN, client / server, monitoring
• Script languages and programming (e.g. Powershell, Perl, Python)
• Arista, netscaler
• RedHat Enterprise Linux, QRadar, SAP
• Omada Identity Suite in the Windows environment (technical advice)
• Introduction of the IAM / PAM NetIQ (from MicroFocus)
• Azure / AWS Stack
• Hyper-V including Storage Spaces direct, Microsoft SCOM, Oracle, SQL
• Hardware X86 / X64-based (RAID, LAN, etc.) e.g. HPE Apollo Hardware
• Competence (e.g. ITIL, ISO9001, IS rules, DevOps concept, Agile, Scrum, MS Office, MS Project)
• Development of a SOAR solution for cloud operation

IT – Enterprises - Finance

09/2018 – 03/2019 **Project manager/Consultant, technical PM (financial industry) - planning and implementation of a SOAR**

• Design, development, implementation of a Europe-wide security system for the ECB in the 4CB network (central banks in Italy, Spain, France, Deutsche Bundesbank)
• with central SIEM SOC connection for the ECB and the 4CB networks of the Deutsche Bundesbank, Central Banks of Italy, Spain, France.
• Integration and adaptation to BAIT (bank-related adaptation to IT), observing the MaRisk version from 2017, system-relevant institutions defined according to Bafin.

Technologies employed:

Service in the cloud (SaaS)

• QRadar console, zAlert, SIEM interfaces UBA, NexPose, TheHive, DFIR, SIEM console, SIEM event processor, flow processor, CTI, SecLog, SecMon, observance of IDW audits, various malware scanners. (Integration into the 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.
• Tools Micro Focus, Splunk, Fireeye-ArcSight, NetIQ. Various audit tools, script and software Python, JS, Perl, Powershell, Java.
• Complete creation in MS Project. MS planning, WBS drafts using Word, Excel, Visio, SharePoint, with the help of ITIL V3, PulseSecure, Tanium, Prince 2 and Sparx.
• Planning of penetration tests for the pentest team (Burp Suite, MetaSploit)
• Development of a SIEM manual and security operation manual
• Tools and project vendors: AgileSI, BlueLiv, CheckPoint, CyberArc, Exabeam, Cylance, ForeScout, F5, Resilient (IBM), LasLine, LogRythm, PaloAlto, Nozomi Networks, ProofPoint, SIEMPLIFY, SecureMatters, Sophos, SkyHigh, Synack, Tenable, Vectra.
• Training concepts
• Operational and administrative
• Construction of the complete test system with sandbox (Cuckoo)
• Development of the 4 region European Central Bank network with connection to the European Central Bank.
• System certification according to BSI, 27001, 27002
• Project connection (Project Plan in MS Project):
• Segmentation of the infrastructure architecture for cloud migration

Preparation for migration to Azure and AWS cloud.

• Proof of Concepts - support and advice
• Cloud governance
• Cloud readiness assessment
• Cloud vision and strategy
• Cloud onboarding
• Technical implementation
• Completion of documentation

Telco Industry

11/2017 – 10/2018 **MNC, Global Project Manager for 3 sub-projects in Telco Industry**

- Architecture, planning, integrating of a complete global new DLP, ATP, EDR, AntiDDos system, over networks, clouds enterprise wide.
- Implementing ISMS, SIEM with SOC. Preparation of a cloud migration.
- Agile approach, Splunk for all sub-projects and platforms

Technologies employed:

- Implementation of target and actual status in the area of IT security - especially O365 - Cloud DLP, EDR, AntiDDoS
- Anti Malware APT email, data, security protection
- Drafting of a new security concept according to the latest GDPR and EUGDPR guidelines, ISO 27001, 27002
- Introduction of the OMADA IAM platform for cloud
- Pentests in an enterprise environment
- HLD governance
- Creation of a new risk management framework
- Maintenance of the existing tools, introduction of a new tool (Symantec, Check Point)
- Advice, implementation, implementation of the new tools
- Creation of reports
- Complete project management
- Training of internal resources
- Vendor and Systems Integrator Management

Establishing a new 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
Creation and implementation of the latest security guidelines of the "Secret Protection Manual" of the Ministry of Economics and Technology and the latest requirements of the GDPR and EUGDPR

(Start of PM2)

Creation of a cloud architecture, Paas, IaaS, SaaS, preparation for Azure migration in project 2

Creating a blockchain security infrastructure

- Conception of the ISMS
- Introduction of a (BC) Information Service Management System
- Development of a BC Network Security Application
- Development of the first financial / investment banking application management service security concept for the establishment and commissioning of a new data center. Adapted security concept, audit of the existing infrastructure, draft of the new high level design and architecture. Final assessment and preparation for necessary certifications.
- Specification of all security measures
- Cooperation with internal teams
- Development of the latest security components

Subproject 2

Implementation and configuration of a Priviledged Access Management solution and cloud migration - technical PM
Skills:

- Priviledged Access Management (PAM)

• Identity and Access Management (
• NetIQ installation
• Network and Infrastructure Architect
• CyberArk and / or Beyond Trust
• ISO and BSI security basics / certification
• Process modeling
• Creation of documentation
• MS Project, Office
• Retina Vulnerability Management or other 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
Preparation for Azure Migration
• Development and migration to the Azure cloud
• Conception, planning, advice and technical implementation and RollOut
• Creating structures
• Cloud connection to 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

05/2017 – 04/2018 **Project Team Security Compliance in Big Data (Bank / Government) Network**

Creation of a concept for the ISMS taking into account the GDPR

Mainframe, Windows, Oracle, Solaris, Linux, DB-Unity, DB-Symphony, Remedy, CMBD, IBM-Maximo

Vendor Relations, confirmation of IBM Security products, development of a SIEM

- Security Compliance Management, IAM, SAM, AMR4V Process / Cloud Migration
- Team member for the development of a global network of approx. 25,000 servers and databases
- Introduction of an ISMS in compliance with the latest GDPR and EUGDPR regulations

Technologies employed:

• Coordination and development of information security policies and procedures and dissemination of user guidelines
• Development and application of an ICS based patch and update process, in WIN 10, mainframe, Unix and Linux environment
• Implementation of monitoring tools to control the stability and other processes

• Endpoint Security (BM BigFix, Tanium, Checkpoint, GFI, HPE, Sophos, Kaspersky ...)
• Penetration tests in wifi and cloud networks (Aircrack, Wireshark, w3af)
• Ensure that the inventory of the information system is continuously updated, regular scans and pentests
• Ensure business impact results are conducted and reviewed regularly
• Working with system and application owners to assess compliance with information security regulations and to plan, document and implement risk minimization measures
• Create and maintain a risk table that identifies all risks to information systems
• Perform security assessments for newly developed or newly acquired companies, business processes, systems and applications
• Coordination and development of an education and training program on information security for internal and external employees
• Develop the security event management process and associated SIEM system
• Development and improvement of the process of security incidents, remediation
• Audit of external service providers to ensure compliance with information security regulations
• Governance, plan, implementation of multi-password access systems with high availability (newly developed process, latest technology)
• SIEM, creation of a SIEM concept based on HP Arcsight
• Working with multiple vendors, developing bespoke security for mainframe computers.
• Reorganization of admin rights (AMR4V)
• Manage budgets
• Mainly responsible for RfP, RfS, SOW, RfI, Vendor Management
• Creation of a new SOC for global operations
• Creation of test specifications (scenarios and cases)
• Evaluation of test data and cases
• Integration and acceptance tests
• Test documentation
• Contact person for users of the system, coordination with software manufacturers
• Instruct and help a team of around 19 security and network experts at all levels

Enterprise IT - Telco

09/2016 – 04/2017 **Senior Enterprise Security Architect (ESA) at an international telecommunications company (IT security)**

• Documentation and implementation of security requirements according to BSI 100 basic protection and ISO 27XXX
• Advising the group on cloud migration
• Risk Analyst
• Level 3 support

Technologie yed:

• Project planning of a new / extended SOC / ISMS
• Process creation for a SIEM
• Redesign of the WIN 10 update and patch process
• Process Management Concepts Hpe ArcSioght, McAfee ePO

• Creation of a governance in the enterprise environment
• Creation of an ISMS and advice on certification
• Creation of a penetration test concept
• Preparation for ISMS / ISO 27001 certification-
• Advice and presentation - risk analysis
• ESA end-to-end, network segregations, etc.
• Encryption suggestions for the entire project, cloud, data center, mobile, laptop, desktop
• Threat analyzes and creation of a security catalog
• Recommendations for a modern enterprise RAS concept
• Documentation in the SCRUM environment
• Mapping and developing processes
• Modeling various concepts
• Documentation of embedded software under Linux / Android
• Documentation of security processes and functions in the mobile and fixed network area
• Creation of manuals / handbooks
• Documentation of existing software for system operation
• Creation of training concepts in the company environment
• Creation of cryptographic solutions in the mobile environment
• Documentation / development of test and development environments configuration on different platforms, Windows, Android, IOS under Common Criteria Evaluation
• Handover to normal operation at the end of the project

IT – Energy und Chemie/ Pharma

07/2016 – 08-2016 **Development of training concepts and processes for IT security based on BSI basic protection and ISO 27001**

Workshops on the SOC and SIEM

• Project documentation creation
Technologies employed:
Schulungs Inhalte

• Introduction to team training
• Conception and operation of technologies for the detection of targeted attacks on company networks
• How do I create an ISMS
• Project planning of the NOC and SOC
• Development of innovative detection and defense measures
• Controls and processes for security during operation
• Independent analysis of attacks and preparation of recommendations for action
• Implementation of penetration tests and security analyzes including the development of attack scenarios and documentation of work results
• Creation of guidelines for IT security
• Use of Wireshark penetration software
• Creation of security emergency plans
• Experience in the administration and protection of firewalls (e.g. Juniper, Checkpoint, Cisco), content security systems, SSL-VPN gateways, IPS / IDS, Sina, Genua, Doi ... etc.
• Knowledge of the most important standards of IT security (ISO 27000 ff, PCI, Common Criteria)
• IT infrastructures (networks, client-server systems, virtualization, access control, etc.)
• Conception of a SOC based on it

• The latest knowledge in Windows 10 and Windows mobile
• Security of SAN and NAS, SANE (storage area network encryption)
• Final assessment of an overall security concept with practical implementation

Logistic and Transport

02/2016 – 07/2016

Team member / consultant - Project at one of the largest transport and haulage companies in Europe (Germany) - Extension and protection of the existing GSM-A network - Planning of handover to a new LTE network

• Planning and layout of the planned real estate,
• Planning of necessary hardware, creation of framework contracts for suppliers,
• People management, restructuring relevant processes
• Monitor / Analyze Network Traffic, IDS Alarm,
• Network intrusion detection, incident declaration, threat management (structure of the SIEM),
• Monitor all relevant network appliances and analyze logs for malicious activities. Development of all kinds of processes to optimize incident response times.
• Automated reporting system to the BNA and the BSI under the regulations of the ITSig. Documentation and reporting processes of all incidents. Incident automation processes

Technologies employed:

• Introduction of an ISMS under the operational conditions in the GSM-R network and BSI basic protection under ITSig
• Preparatory work to expand the existing NOC into a SOC
• Creation of a network structure plan (GSM-A standard)
• Planning and implementation * of a SOC (Security Operation Center), summarized for the various departments (Systel, TK, LST etc.) **
• Focus and planning, resources, risk and change management.
• Workshops with teams from different departments and stakeholders
• Establishing the governance
• Creation of the asset management
• Threat analysis according to ISO 27001 and BNA 109
• Pentest implementation with Pentest team (external)
• Risk management, risk analysis
• Hazard analysis with residual risk assessment
• Planning the safety certification
• BSI basic protection, ISF, Cobit, BNA, ITU 1501
• Analysis of the GSM-R network and interfaces to Systel, LST ...
• Understanding of new plans, IP networks and re-investment projects, LTE updates ... ..
• Practical implementation of all results and processes in a SOC
• Planning the handover to normal operation

IT – Public Services - Security

09/2015 – 02/2016 **Subproject - Team Member - Data Center Migration and Extension - Reconstruction of the data center - Reconstruction of external clients (police - Customs - BAMF) Connection to Black Fiber**

- Planning
- Implementation
- Handover to normal operation

Technologies employed:

- Complete system analysis
- Creation of an ISMS concept
- Restructuring of the existing SOC and expansion of the SIEM
- Moderation of customers / internal / external workshops
- Handover to normal operation
- Repair and preparation of the current (Windows / Unix) environment for migration to a new data center
- Migration and definition of MS CA, POC
- SSL - SHA1 to SHA-2 migration
- ADS patching
- Handling HSM, hardware security modules (SINA, SafeNet), documentation of the key lifecycle
- MS NDES, installation, implementation of PKI components
- Decommisioning after updates and patches installation
- Documentation of the entire process
- Handover to production and local team training
- BIG Data Project Manager, (Kanban, Scrum), MS, ...
- Calculation of data storage (SAN) in a new data center
- Analysis of existing weak points (security)
- Risk management and residual risk analysis
- Analyze suspicious behavior
- Analyze and recommend the high availability of the new network
- Planning the migration of the existing NOC / SOC to a new SOC according to ITSig and BSI 100 / ISO 27001 specifications
- Implementation of a completely new bb (railway operational) SOC
- IT and TC adaptation to the mobile (Android, IOS) network, development of special Android applications
- Recommendation of hardware suppliers
- Vendor management, budget preparation, framework agreement
- Migration with minimal business disruption
- Aim, reduce possible attacks by 50% -60%
- Integration of encrypted VoIP and fax traffic
- Analysis of redundancy and latency, operational improvement
- Creation of complete documentation
- Training of specialist staff
- Presentations for top management
- Handover to internal administrators, training

IT – Industry – Design-Development – Manufacturing- Software - Hardware

02/2009 – 09 /2015 - 6 Jahre 8 Monate Auslands Aufenthalt (Asien / Singapore PR)
Telecommunications - MNC- Intl. Banks - Factories - China Manufacturing Management of Telecommunication and Smartphones – Sales-Director Neoi Pte. Ltd.

- Software development
- Hardware development
- PCB layout
- Development of security concepts and processes in the Windows and Unix environment
- SLA drafts, manufacturing planning and supervision
- Control of Ipr's
- Planning of new threat monitor processes

Technologies and responsibilities:

- Director (Mobile IT - Cyber Security - Support, Management, Consultant) Professional Consulting Group, Securescrypt acquired by PIC -Technology in 2009
- Director responsible for company management under local regulations, contract position
- People management (120 consultants), vendor management, framework contracts
- Consultant and project manager, IT HR **
- Cyber Security Manager Team
- Development of modern locks in the military / government sector
- 2014 for the Football World Cup, development of a TV application that allows online streams from different countries to be combined in one eLauncher - eNtertain application. The development was done for Amazon (see under Amazon "elauncher")
- Android developments in the enterprise environment, commerce and payment applications
- Risk management, risk analysis, risk assessments
- Special software skills: Eclipse IDE with 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
- Development of Android applications, IOS, Windows
- Cyber / IT information system architecture / security
- Employee management and training
- IT security software design and development
- Management of the international developer group of 100+
- Implementation of a new network and Internet security platform with SINA and AVDA as well as our own development of algorithms
- Transition / conversion from traditional enterprise telephone systems to IP / VoIP, IP video conferencing, VoIP / IP encryption
- Design and development of IT / Cyber Security / IP / VoIP solutions in mobile systems, for all platforms (Windows, iOS, Android, Blackberry etc.)
- Securing of clouds with new PKI-based security and special encrypted hard disk drives
- Encryption of critical data with customer-specific UAF authentication’s and identification’s factor, dedicated access to certain selected individuals and groups
- Update of the existing systems to the latest security technology
- Education and public lectures on risk management and cyber security
- Manage and manage the company's marketing
- Consulting, projects, analysis of customer requirements with suggestions for changes and solutions so that sales can support marketing and win new customers

MNC Electronic – Telco-Engineering

01/2005 – 01/2009 **Telecommunications and IT Networks - Support and Services - PIC Pte. Ltd. Hong Kong**

• Employee training

• Risk Management

• Network architecture

Technologies / Responsibilities:

• Management of 200 technical employees in Hong Kong, China, South America
• Employee training and guidance
• Management of the branches and contract partners on site
• Design of new IT security and network solutions
• Design and implementation of sophisticated IP / VoIP systems for service providers and companies
• Frequent travel
• IT risk management, analysis, lectures, training
• Special training for investment bank IT staff Training on risk management

08/2004 – 12/2004 **Interims CTO electronic developments – Lintux Hong Kong Ltd.**

- Sales & Acquisition of new customers
- Order coordination with Chinese factories
- Training of technical staff
- Exoertise and transfer of experience
- Development of IP systems (the company was later acquired by Lintux Hong Kong)

Technologies employed: Wireless Communications, mobile communications, public services

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

• Head of the Singapore Development Group - Main Coordinator with the Hong Kong Development Team - Design of the MXI Platform (combined mobile and VoIP services)
• Installation of the first VoIP network in Malaysia
• Special platform for portfolio management software

Technologies employed: GSM Technology – European Standards

12/2000 – 10/2003 **Developer – Hardware - Software Taitoma Group – Taipei – Taiwan –**

Industrial IT Networks and communication devices

• Responsible for the development and construction of software and hardware as external services of Asian manufacturers
• Responsible for the development and project management methods implementation of processes, procedures, reporting, strategic management
• Development of solutions for IT security and risk minimization
• Quality control used for major projects within the Asia-Pacific & Greater China regions, or / and industry vertical chart strategies to ensure the design and development service of the team and company in the region for the Titoma Group

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

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

• Responsible for the development and construction of software and hardware as third-party services of Asian manufacturers
• Stationed for a longer period of time for project implementation in Iraq, Lebanon, Syria, Saudi Arabia and some other countries (installation of complete radio communication networks)
• Complete systems installation and implementation
• Developed the first encrypted satellite telephone for a German group, which was then used by public services and ships.
• **In addition, remote studies at Princeton University USA, for Phd. Dr. Telecommunication encryption methods**

Technologies employed: VHF-UHF Technologies – Voice and Data encryption

IT – Banks – Investment Industries

02/1998 – 11/2000 **Credit Suisse First Boston (Hong Kong) - VP / IT - Head of Asia Pacific Group**

• Hong Kong Global Engineering and Infrastructure Support Team
• Responsible for communication between the technical and help desk groups worldwide
• Analysis of the existing networks and the search for security risks; Development of new risk solutions
• Development of solutions for existing networks - migration of existing systems to Windows

Technologies employed: MicroSoft Windows

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

• Network migrations
• Setting up the IP network
• Development of investment applications to monitor the stock market

Technologies employed:

• Complete systems installation and implementation
• Network migration from Novell to Windows and Transaction Server
• Service, training of local engineers, system analysis, telecommunications connectivity, routers (3Com, Transcend, Cisco)
• TCP / IP, DHCP, WINS, Ethernet, trust relationships with networks in the USA and Europe.
• Integration of NT 4 with BLITZ (an SQL / Excel-based price model and trend manager for portfolio trading).
• Developed new applications such as charge calculators, IROS and page pool for stocks, bonds and portfolio trading
• Wrote the pricing for numerous Excel macros models with live feeds from Reuters, Bloomberg, stock exchange and customer-specific applications from Merrill Lynch in New York and London (pioneer of IP-based TV)
• Installed applications for buying and selling products, messaging and notifications for individual stocks, bonds, portfolios. With: RAM Excel, RAM -Add-Ins, Newport, Loan -Manager, Anleihemanager, IORS, K-Tek, PDD, DDE.
• The implementation of the first security regulations for banks in the investment business

ENGINEERING - Mobile Communications - Networks

01/1988

Senior Systems Ingenieur
• Design and Developments
• Realizations
• Installations

Technologies employed:

• Customers including BOA, Deutsche Bank, BSI Machinery Germany, Indonesian Government, Thai Farmers Bank, Hoechst Chemicals Taiwan and Thailand, Anderson Singapore, SAP Germany.
• Mostly network planning and implementation. Experience in the financial world as well as the chemical industry and other industries
• There were also a lot of telecommunication tasks, including planning cellular networks, billing systems for Inmarsat, up-down-link interfaces to LANs.
• Planning and installation of a terminal server network for a leading Swiss banking group in order to overcome slow network connections and reduce costs by upgrading older PCs and notebooks for connection to NT / W 2000 / XP networks
• Experience in Packet Protocol, a protocol that was later used as the basis for GSM mobile phone systems installation and implementation
• Special projects, sale and installation of nationwide UHF communication networks, as a forerunner of today's mobile communication. Customers in the Middle East and Asia.
• Development and manufacture of UHF components, including development of the first "mobile phone" ETACS, AMPS.
• Experience with A-Netz car phones, development of the first satellite phone in an attache case, encryption of mobile devices

01-1987

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

- Development of CB and UHF radio systems
- Supervision of manufacturing in USA and Japan
- Worldwide customer support

Technologies employed:

- RF development engineer for the Pathcom Group in the USA, based in Germany.
- Developed the first free CB radio system, got the first ever approval from the FTZ in Darmstadt, set standards for the CB radio
- Technology Development of new data communication products in the USA and Yokohama Japan. Production control and training
- Developed the first Asian-made radio synthesizer, VHF and UHF transceiver and bundle cell phone, system development and manufacturing of Pathcom communication products

School – Education - Studies

Professional internship after graduation

- Electrical service
- Office administration
- Employee leadership

Studies - University

- TU Darmstadt Electrics, Electronics, Mthematics, Physics
- Graduate engineer - Philipp Reitz Polytechnic - Frankurt
- Employee leadership, Sales and marketing

Masters Degree in electrical engineering

- apprentice
- Journeyman
- Masters degree examination - Wiesbaden

Abitur- Graduation Humanistic Gymnasium Wiesbaden , average score 1.1

- Mathematik
- English

Remote studies and graduation - Princeton USA – Phd. Dr. Telecommunication

Back to top