Cybersecurity Consultant

Summary

Seasoned Cybersecurity consultant with passion for aligning security architecture plans and processes with security standards and business goals. Versed in robust network defense strategies such as high availability, elasticity, fault tolerance, troubleshooting, security-in-depth, and ongoing maintenance

Work Experience/Employment History

Cybersecurity Senior Consultant /Solutions Architect – Credit Suisse, Wroclaw, Poland (Jan 2021-Present)

- Architected, developed, and deployed of two custom designed exact data matching DLP python scanning solutions (EMEA and APAC region) with scanning capability of 2.3TB daily to assist end users with finding precise Client Identifying data sets across an inventory of over 100k Network Drive, Sharepoint and O365 data at rest repositories
- Prepare enterprise ISO-27017/ ISO/IEC-27017 cloud security audit of program/architecture compliance
- Prepared configuration hardening documentation for both AWS and Azure environment stakeholders as pertaining to network and endpoint security, current threat and attack trends mitigation,
- Architected and developed python monitoring tools for monitoring of security events in a complex application with over 60 interfaces.
- Built and maintained Azure/AWS infrastructure using Terraform and AWS CloudFormation
- Implemented DevOps practices such as infrastructure as a code, continuous integration/automated deployment
- Deploy Azure IaC through third party platforms like Terraform, Ansible and Chef
- Knowledge of Vulnerability management and common Vulnerabilities affecting Cloud environments
- Architect and design AAD B2B external entity client onboarding/offboarding configurations (Security Hub) for functionalities like domain white listing, access packages, and cross tenancy rules to provision conditional access to specific SPOL directories
- Responsible for complex integration of multiple DLP technologies and Password Management (PAM) tool to classify, move and delete data; specific focus on system performance with loose coupling utilizing APIs and services.
- Solutions architecture of a Secure Data Exchange alternative solution to replace USB usage through Azure Active Directory, Share Point Online, PowerApps, and O365 data leakage prevention technology
- Provided system documentation, reporting, and security review of architecture, data flows, and access controls associated with fully automated system that can access and modify files in repositories across EMEA/AMER/APAC
- Strong experience working in an international environment with global teams

Cybersecurity Manager - M3 Network, LLC (Freelance/Remote UK) (Oct 2020-Jan 2022)

- Administered IT-monitoring Azure Security Center toolset to collect and track metrics, collect and monitor log files, and set alarms that notify security team of users with console access and no two-factor authentication enforced
- EDR management of over 1000 endpoints/interfaces using combination of Webtitan, Perchy, Azure Defender, NinjaOne, Knowbe4, Vipre, ESET, DarkwebID to provide systematic management of cloud infrastructures to include GCP, AWS, Sage, SFDC in multitenant architectures
- Setup GCP firewall rules to allow/deny traffic on VM instanced based on specified configuration used GCP cloud CDN to deliver content from GCP cache locations drastically improving user experience and

latency

- Hands-on experience in security architecture solutions leveraging AWS Services such as AWS CloudWatch, CloudTrail, GuardDuty, Trusted Advisor, AWS COnfig
- Push custom Powershell scripts to update/configure client cloud infrastructure and mobile devices to ensure NCSC CyberEssentials compliance levels met
- Evaluated, deployed, and supported application security technologies, processes and workflows on multiple platforms (Server, Client, Mobile, Tablets)
- Advise SMB (10M+ GBP Revenue) in identifying IT boundaries and architecture, as well as how to define and protect assets.
- Create workflows and requirements for Powershell scripts to enable OTP for unfederated clients as part of external party onboarding into enterprise Azure federation

Digital Commercial Banking Expert | Solution Architect – Alior Bank, Warsaw, Poland
(April 2016- December 2020)

- Designed and deployed over 30 cybersecurity integrations associated with a customer facing commercial banking application with over 150k active clients involving steering or traffic redirection methods
- Good exposure to Agile software development and DevOps practices such as IaC, Continous integration and deployments leveraging Terraform, Git, Jenkins, Code Pipeline, Code Deploy
- Ran, maintained, and utilized security tools as part of enterprise Appsec program, e.g., static and dynamic test tools for defense in depth
- Good understanding of the principles and best practices of software configuration management (SCM) in agile, scrum, Kanban, "Scran-ban" methodologies
- Prepare enterprise ISO-27017/ ISO/IEC-27017 cloud security audit of program/architecture compliance
- Prepare Ansible Playbooks using YAML functions and utilizing setup and automate the CI/CD pipeline and deploy microservices, provision load balancer, auto-scaling group using Ansible
- Project lead for the development and integration a portable network security interface device to encrypt and secure online transactions
- Develop and design a masked password replacement for authenticating clients into application
- Perform detailed vulnerability analysis and security upgrades related to TPM, vector side attacks of hardware from application, while offering functional business use of device for various usecases

US Army Officer | Information Security Officer - United States Army – Various Global Locations
(October 2000 – February 2016)

- Solution Architect of a Theater Security Cooperation Management system synchronizing operational applications with logistics management systems to gather, analyze and communicate competitive and market intelligence
- Enforce enterprise information security/cloud security best practices for ISO-27017, NIST, and FIPS frameworks
- Drive International/multinational private and public Sector engagements with executive level stakeholders in multibillion dollar/multiyear projects
- Project Manager of multiple multiyear and multibillion dollar foreign military sales program in EMEA region
- Drive senior stakeholder discussion on deriving tech requirements from business requirements and high-level architecture for over 50 program level projects

Education

- **MS.I.T., Cybersecurity -** University of Maryland (2016 -2018)
- **Bachelor of Arts, International Relations -** George Washington University (2000 - 2002)
- **Associate of Arts, General Education -** St. Petersburg College (2018 - 2020)

Experienced in Regulations/ International Standards
NIST Cybersecurity Framework
ISO 27017/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services
NCGC CyberEssentials
CISA CyberEssentials

Languages
English: native, Russian: fluent, Polish: native