**Ali A. Aqel**

10424 Pentagon Drive | Orland Park, IL 60467 | aqel\_ali@hotmail.com | 708-381-9595

PRINCIPAL IT SECURITY CONSULTANT

(ENTERPRISE ARCHITECTURE- ENGINEERING- ON-PREMISE & CLOUD CYBERSECURITY- INFORMATION SECURITY- IT GOVERNANCE- MANAGEMENT- ADVISORY)

**Overview**

A Principal Enterprise IT Consultant heavily focused on Security Architecture, Engineering, Information Security, Cyber Security, IT Management and Advisory. I have more than 25+ years of global enterprise IT technical and management experience. I carry decades of consecutive Information and Cyber Security Expertise based on all functional and technical levels, for all IT Platforms.

Specialties include Enterprise Network and Systems Infrastructure, Cloud Security, On-premise security, Virtualization, Private and Public Cloud solutions, IT Security compliance & Governance, Security Assessments, remediation, prevention, troubleshooting, design, planning, deployment, implementation, and documentation.

I’m well versed and extremely knowledgeable with information systems security regulations, policy design, security controls, best practices, requirements, and processes inclusive of Identity Access and Management, Firewalls, CSPM, XDR, SIEM, CNAPP, CIEM, CWP, DSPM, Security metrics, WAF, Application Gateway, NAC, SDN, Proxy, PKI, SIEM, Dev-Ops, S-SDLC, Reporting, Azure, AWS, Information Security, Cloud Security, GRC, DLP, IPS/IDS, PCI/DSS, HIPAA, ITIL, ISO, SOC, CIS, GDPR, NCSC, and NIST.

**Proficiencies**

Datacenters, Virtualization, Azure, AWS, Windows Server OS and applications, Centos, Red Hat, Clustering, Identity, Active Directory, Azure AD, Ping, OKTA, Advanced Threat Protection, XDR, EDR, ADFS, SecurID, Microsoft Exchange 2003 to Exchange 2019\Azure, ISA/TMG/UAG, Windows, Linux, Unix, Network LAN and WAN, Express Route, Firewalls, SDN, WAFs, Access controls, SSL, VPN, Micro-Segmentation, Zero Trust, EDR, XDR, NDR, IPS/IDS devices, TCP/IP, DNS, SMTP, SNMP, Snort, Nmap, Wireshark, Bash, McAfee, Splunk, Azure Sentinel, MCAS, CrowdStrike Falcon Carbon Black (All Versions Firewalls, routing, Proxy, RSA, VPN, IPSEC, Direct Access and web caching) , SQL, SharePoint, IIS, Terminal Services, VDI, TS Gateway, Palo Alto Panorama, SCOM, SCCM, DPM, FIM, DNS, WINS, DHCP, Forefront Security Products an etc.

**EDUCATION AND CREDENTIALS**

Business Technical Management

**DEVRY UNIVERSITY** – Chicago, Illinois

**Certifications:** AZ-900, AZ-104, AZ-500, AZ-304 **In-Flight**: CISSP, CCSP, CISSP, ISSAP

**PROFESSIONAL EXPERIENCE**

***ADP , Inc. Remote (Roseland)* New Jersey** **01**/**2023 – Present**

***Title:*** *Principal**Cloud Security Architect* ***(Contract)***

**Job Description:**

As a Principal Cloud Security Architect, I oversaw and was responsible for ADP’s Global Azure Security Program. My primary focus was on building and developing ADP’s new Azure Security Program, including designing security requirements and standards, service designs, security controls, and policies. I worked closely with the Governance, Risk, and Compliance (GRC) team to develop assessment processes for all Azure services, workloads, features, and services.

I also collaborated with compliance teams to integrate the Azure Security Program with custom ADP processes. As one of the key stakeholders, I helped create a custom cloud security compliance and metrics platform called ARP (Assessment, Remediation, and Prevention). This platform was designed for real-time visibility and monitoring of cloud resources, providing status updates on threats and vulnerabilities, security controls, and compliance failures to gauge the security and compliance posture of all cloud resources (e.g., subscriptions, VMs, databases, storage accounts).

I developed custom Azure Preventative Policy Controls (PPC) security controls and policies for the Azure ecosystem. I worked closely with Security Engineering, Cloud Infrastructure, App Development, Identity and Access, Application Security, Compliance, and Risk teams. I conducted and assessed technical risk reviews for all production workloads as part of a weekly process. Additionally, I co-authored ADP’s custom security frameworks and other frameworks based on ADP personal standards and legal requirements, including CIS, NIST, PCI, ISO, and HI-TRUST/HIPAA,SOC\SOX standards. etc.



**Role Responsibilities: Duties include:**

* Gathering and development of functional and Security requirements for all Security Platforms and tooling, by guiding and advising stakeholders.
* Design of Azure Security architectures and operational documentation in conjunction with engineering, application development, compliance, and operational staff.
* Designed and developed security controls and policies in the overall Identity ecosystem.
* Created Azure MFA design with conditional Access requirements and Standards (Ping, EntraID, Okta) Each for different tenants.
* Advise, consult, lead, guide and mentor project teams, engineers, analysts, and support staff in the delivery of solutions.
* Developed the EDR\XDR Design for CrowdStrike Falcon for certain isolated workloads.
* Participated in all cloud security agile planning processes and delivery methodologies.
* Conducted threat modeling and security gap assessment exercises in concert with other teams.
* Developed Security Standards and Requirements for all Azure AI Services.
* Developed and created a CSPM+CWP POC & POV for (WIZ, PRISMA, Defender for Cloud)
* Created reusable patterns for reoccurring cyber challenges.
* Co-Contributor to the creation of policy, standards, Minimum Security Baselines (MSBs), procedures and guidelines.
* Development and implementation of WIZ CSPM +CWP (Onboarding, Integration, Service Now, IAM and Workloads and services, policy engine customization)
* Conducted quarterly Security Posture Assessment based on Security Risk and Score (Cloud Platforms). visibility to and escalated security risks, as well as, technical, execution, deployment, or other risks as applicable.
* Lead Proof of Concept/Value Architect providing Read outs by communicating results and recommendations to stakeholders.
* Conducted post-mortem reviews of projects / products to measure design versus implementation differentials.
* Contributed to the Client Cyber Architecture Practice by supporting Cyber Enterprise Architecture objectives.
* Created a process for security baseline checks for cloud-based applications and services. (Implementing security best practices, and mitigating risks across the Azure environment.)
* Heavily Experienced and versed (Subject Matter Expert) in entire MSFT cloud Security tools Stack (Cloud and On-premise). (Defender for Cloud & CWP, Defender XDR, Sentinel, DSPM, CNAPP, CIEM etc.)
* Managing and developing Security for one of the most complex security environments on the globe, while extending MSFT security capabilities in the cloud.
* Azure Conditional Access Policies Design and implementation (Audit & Enforcement)
* Extensive Architectural design, engineering and Endpoint Security using the Microsoft Defender XDR Stack (Defender for Cloud, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, EntraID identity Protection, App Governance)
* Developed and setup Azure Purview (Compliance Manager) for continuous Security control and Posture assessments. (All Azure Workloads and services)
* Developed Baseline and Custom AI Security standards and requirements & security Controls & policies.(Azure AI + AWS Bedrock)
* POC and Pilot of Defender for AI.(Azure)
* Microsoft Sentinel configuration and tuning Plus Policy and Azure Security Stack Integration
* Microsoft Intune Assessments, remediation, and Prevention Policies (MDM + MAM)
* Part of key Security Committee for collaboration with cross-functional teams, including IT, DevOps, and development teams, to design and enforce security policies, frameworks, and solutions.
* Design and implementation of secure cloud architectures for Microsoft Azure environments.
* Defined security standards, best practices, and policies to ensure cloud systems meet compliance and regulatory requirements (e.g., GDPR, HIPAA)
* Developed and maintained Azure security policies, governance frameworks, and technical security controls.
* Performed security assessments, identified Threats & Vulnerabilities, and led remediation efforts to address risks and threats within the Azure environment.
* Architected and implement identity and access management (IAM), encryption, and security monitoring solutions.
* Collaborate with DevOps and development teams to integrate security policies for Azure Policy, into the CI/CD pipeline.
* Conduct risk assessments, threat modeling, and security reviews for cloud-based solutions
* Conducted Lunch and learns for other teams on Azure security technologies and industry best practices and recommend improvements or new tools as necessary.
* Designed and architected security of Azure-based services such as Azure AD, Azure Key Vault, Azure Security Center, and Azure Sentinel, etc.
* Assisted in incident response activities and security investigations.
* Developed policy Lifecycle management process for EntraID/AD, Microsoft two factor, FMA, Defender, Purview and Azure Security overall.

***Clario, Inc. Remote (Philadelphia)* Pennsylvania** **06**/**2022 – 12/2022**

***Title:*** *Principal IT Security Architect* ***(Contract)***

**Job Description:**

As a Principal IT Security Architect, I was responsible for designing and architecting Clario’s workload migration from on-premise to Azure Cloud. I designed and implemented the Azure Security Stack (M365 Defender, Sentinel, MDC + CWP+ DSPM + CIEM + CNAPP+CSPM) for on-premise and cloud security across IaaS, SaaS, and PaaS workloads. I also architected and managed the Clario Defender EDR + XDR platform for both corporate and manufacturing environments.

In my role as the designated Info-Sec Architecture and Engineering lead, I created security controls, policies, requirements, and standards for Clario’s cloud platforms (Azure and AWS). I served as the technical leader for the Zero Trust, EDR, and XDR initiatives, overseeing security for all devices and IoT endpoint platforms. I designed initiatives for Zero Trust pillars and built proof-of-concept (POC) and pilot environments based on Clario’s approved service designs for cloud workloads.

The scope of my work encompassed all Azure and AWS platforms and the workloads hosted within. I performed comprehensive security posture assessments, validating the security controls and policies for all workloads and services. Additionally, I led the design and architecture of Data Loss Prevention (DLP) workflows for policy audit and enforcement, as well as platform-hardened configuration and policy structure.

* Built and led Proof of Concept (PoC) and Pilots for Production deployments using these Azure XDR Defender M365, Defender for Cloud and Azure Sentinel technologies.
* Assisting clients with transitions to the M365 cloud services such as tenant setup and service configuration with a focus on cloud cyber risk mitigation.
* Built and Designed a POC environment for the Azure AI services Platform.
* Created AI Based Security Requirements and Standards for AI Services Structure.
* Created an AI Service Exploratory team of Security Architects.
* Created a Generative AI and CHATGPT Risk Review
* Development, design, and implementation of PingFederate, Ping Access, Ping One, Ping ID, and LDAP directories. (Applied on Different Workload Models for IAM controls)
* PingFederate, Ping Access, Ping One, Ping ID, SiteMinder and LDAP directories.
* Experience in working on Ping federate 8.x, 9.x, SAML 2.0, Oauth 2.0, OpenID/Connect (OIDC). Demonstrated POCs for API security like integration with Open AM, Site Minder, OAuth 2.0, JWT token and certificate authentication.
* Integrated the Federation service between Site Minder federated web services to Ping federate for classic migration of applications that are SAML and WS applications. Experienced with multiple Ping Federate adapter’s HTML form, x509, Kerberos, open token, referenceID, ping ID and composite adapters.
* Built Polices and Hardened configurations for the Azure XDR platform tools.
* Designed and Deployed AAD P2 Features, with Conditional Access, Intune, Azure Defender for Cloud, and Azure Sentinel.
* Performing technical Security health checks for these Cloud platforms/environments prior to broader deployments.
* Functioned as technical point of contact for product development teams as they related to cyber security and privacy.
* Conducted Identity & Access (AD platform) Performance Benchmarking with Defender for Identity to detect Identity traffic Performance thresholds and increases.
* Identity & Access Platform Design for On-premise to Cloud Migration.
* Created all Identity and Access Standards for the Clario Enterprise and Manufacturing Platforms.
* Architected Legacy Endpoint Strategy for all Servers and Clients.
* Performed Intune (MEM) & MDM Assessments for Endpoint Security
* Conducted complete lifecycle security architecture framework and technical assessments for Legacy Endpoints (Client\Server Endpoints + IOT)
* Conducted complete lifecycle security architecture framework and technical assessments as required.
* Conducted GRC and Security based Assessment threats, risks, and vulnerabilities from emerging security issues to advise pertinent stakeholders on Application Security Threats & Vulnerabilities and Security Posture of the Clario Common Endpoint Platform.
* Recommended constant changes to engineering standards based on new regulations and business requirements to conform to new security measures.
* Led the enterprise wide "Release and Review" quarterly waves in full. I conducted and assessed technical risk reviews for all production workloads.
* Conducting cloud security analysis, evaluating configurations, and providing recommendations of prospective clients' O365, EMS, and W10\11 platforms and environments based on Clario’s Cloud Cyber Risk Framework.

***Alcon, Inc. Remote (Fort Worth)* Texas** **06**/**2021 – 06/2022**

***Title:*** *Principal Endpoint & Identity Security Architect* ***(Contract)***

**Job Description:**

As a Principal Endpoint & Identity Security Architect, I was responsible for Alcon’s migration from McAfee EPO EDR to Microsoft’s Defender EDR and XDR. I designed and managed the Alcon Defender EDR + XDR platform for both corporate and MTO (Device Manufacturing) environments.

In my role as the Info-Sec Architecture and Engineering lead, I developed security controls, policies, and standards for Alcon’s Zero Trust and Endpoint Security Platform Initiatives. I also constructed Proof-of-Concept (POC) and pilot environments based on Alcon's Zero Trust design to validate and test internal workloads against company security requirements and standards. Moreover, I led Identity & Access Security Assessments, focusing on threats and vulnerabilities within Alcon’s On-Premise Active Directory (AD) and Azure AD environments.

I architected the Modern Identity Principles Frameworks and facilitated the migration of On-Premise workloads to Azure Cloud using the Azure Adoption Framework. This was done to prepare and remediate the On-Premise and Cloud IAM environments for Zero Trust controls enablement.

As the Global Endpoint Lead, I concentrated on the Endpoint and Identity Access pillars of Zero Trust. I conducted and assessed technical risk reviews for all production workloads as part of a weekly process and co-authored Alcon’s Global Information Security framework and custom Zero Trust frameworks based on CIS, NIST, ISO, and HI-TRUST/HIPAA standards.

The scope of my work extended across all Azure and AWS platforms, as well as the workloads hosted within. I performed comprehensive security posture assessments, validating the security controls and policies in place for all workloads and services. Additionally, I led the design and architecture of Data Loss Prevention (DLP) workflows for policy audit and enforcement, as well as platform-hardened configuration and policy structure.

* Built and led Proof of Concept (PoC) and Pilots for Production deployments using these Azure XDR Defender M365, Defender for Cloud and Azure Sentinel technologies.
* Assisting clients with transitions to the M365 cloud services such as tenant setup and service configuration with a focus on cloud cyber risk mitigation.
* Built Polices and Hardened configurations for the Azure XDR platform tools.
* Designed and Deployed AAD P2 Features, with Conditional Access, Intune, Azure Defender for Cloud, and Azure Sentinel.
* Configuring Ping ID MFA in Ping Federate
* Integrating Ping with identity stores like LDAP, relational databases, and application servers
* Creating adapters, service provider and identity provider connections
* Installing and configuring Ping Access servers, gateways, and agents
* Working with CA to resolve issues.
* Developing scripts for checking the performance in directory server
* Performing technical Security health checks for these Cloud platforms/environments prior to broader deployments.
* Functioned as technical point of contact for product development teams as they related to cyber security and privacy.
* Conducted Identity & Access (AD platform) Performance Benchmarking with Defender for Identity to detect Identity traffic Performance thresholds and increases.
* Identity & Access Platform Design for On-premise to Cloud Migration.
* Created all Identity and Access Standards for the Alcon Enterprise and Manufacturing Platforms.
* Architected Legacy Endpoint Strategy for all Servers and Clients.
* Performed Intune (MEM) & MDM Assessments for Endpoint Security
* Conducted complete lifecycle security architecture framework and technical assessments for Legacy Endpoints (Client\Server Endpoints + IOT)
* Conducted complete lifecycle security architecture framework and technical assessments as required.
* Assessed threats, risks, and vulnerabilities from emerging security issues to advise pertinent stakeholders on Application Security Threats & Vulnerabilities and Security Posture of the Alcon Common Endpoint Platform.
* Recommended constant changes to engineering standards based on new regulations and business requirements to conform to new security measures.
* Led the enterprise wide "Release and Review" quarterly waves in full. I conducted and assessed technical risk reviews for all production workloads.
* Conducting cloud security analysis, evaluating configurations, and providing recommendations of prospective clients' O365, EMS, and W10\11 platforms and environments based on Alcon’s Cloud Cyber Risk Framework.

***Ernst & Young Chicago (Global)*, Illinois** **04**/**2020 – 06/2021**

***Title:*** *Principal Information Security Consultant* ***(Contract)***

**Job Description:**

As an Information Security Consultant for EY's largest global service portfolio, I serviced the Global Tax Platform (GTP) as well as other EY portfolios. As one of the designated Info-Sec leads for the Global Tax Platform, I led the enterprise-wide "Release and Review" quarterly waves in full. I conducted and assessed technical risk reviews for all production workloads and co-authored and contributed to the EY “SASP” Information Security framework for EY and its global service portfolios.

I constantly engaged with all Product Owners, App Development, Architecture, Infrastructure, Info-Sec, DevOps, and other client teams from each portfolio to validate security controls and policies. My role was to ensure security standards and requirements were fully met prior to any production workload release. As one of the Info-Sec Consultants, I gave the "Approve/Deny" for 18 global EY teams across 8 global service portfolios.

I conducted in-depth Application Security Assessments for GTP and other portfolios, performing granular technical security reviews to certify API endpoints used in all applications across cloud and on-premise platforms. I also led the Info-Sec engineering teams in the "Release and Review" waves, creating test plans for the Info-Sec engineering teams to test and validate against all workloads for security control and policy failures.

The scope of my work encompassed all Azure and AWS platforms, as well as the workloads hosted within. I performed comprehensive security posture assessments from an end-to-end standpoint, validating the security controls and policies in place for all workloads and services.

* Functioned as technical point of contact for product development teams as they related to cyber security and privacy.
* Conducted complete lifecycle security architecture framework and technical assessments as required.
* Conducted complete lifecycle security architecture framework and technical assessments as required.
* Assessed threats, risks and vulnerabilities from emerging security issues to advise pertinent stakeholders on Application Security Threats & Vulnerabilities and Security Posture of the GTP Platform.
* Designed, implemented, and configured Policies for Microsoft's Azure XDR platform for cloud Security such as Microsoft 365 Defender (Microsoft defender for Cloud Apps (MCAS), Defender for Endpoint, Defender for Identity, Defender for 365, Microsoft Information Protection (MIP), Conditional Access, Intune, Azure Defender for Cloud, and Azure Sentinel.
* Built and led Proof of Concept (PoC) and Pilots for Production deployments using these Azure XDR Defender M365, Defender for Cloud and Azure Sentinel technologies.
* Assisting clients with transitions to the M365 cloud services such as tenant setup and service configuration with a focus on cloud cyber risk mitigation.
* Built Polices and Hardened configurations for the Azure XDR platform tools.
* Performing technical Security health checks for these Cloud platforms/environments prior to broader deployments.
* Recommended constant changes to engineering standards based on new regulations and business requirements to conform to new security measures.
* Led the enterprise wide "Release and Review" quarterly waves in full. I conducted and assessed technical risk reviews for all production workloads.
* Co-authored and contributed to the EY “SASP” Information Security framework, for EY and its global service portfolios.
* Conducting cloud security analysis, evaluating configurations, and providing recommendations of prospective clients' O365, EMS, and W10\11 platforms and environments based on EY’s Cloud Cyber Risk Framework.
* Collaborate and work with key executives and technology leadership teams to assess and communicate security impacts during business case development.
* Reviewed customer-specific security process requirements and facilitated action in engineering teams to meet requirements.
* Designed tests and tools to break into security-protected applications and networks to probe for vulnerabilities.
* Conducted IT Security assessments with advanced Security tooling for systems or applications to recommend solutions to mitigate risks.

**Below outlines the in-depth Security tooling I used to administer the entire Information Security function in full for EY.**

**Application Security Tooling:** (Threat, Vulnerability & Security Posture Assessments)

|  |  |  |  |
| --- | --- | --- | --- |
| **API Management Platforms:** | **API Validation Tools:** | **Azure Security Stack:** | **Application Security Threat & Vulnerability:** |
| APIM | Swagger | Defender for Cloud (all Modules) | WhiteSource |
| Apigee | Postman | M365 Defender (XDR) | Checkmarx\Veracode |
|  | OpenAPI3 | Azure Sentinel SEIM & XDR | Qualys WAS |
|  |  | Azure Policy | Webinspect |
|  |  | Azure WAF | Container Security (AquaSec + Defender for AKS) |
|  |  | Azure Firewall + Manager |  |
|  |  | Azure App Gateway |  |
|  |  | Defender for AKS |  |

***Honda Corporation Chicago*, Illinois** **04**/**2019 – 04/2020**

***Title:*** *Domain Security Architect* ***(Contract)***

**Job Description:**

As a Domain Security Architect, I worked on Honda’s Global Merger and Acquisition technology transformation into Azure, encompassing 50 subsidiaries worldwide. I was responsible for the Security Design, Security Standards, and Policies for the Azure Transformation Initiative. My work focused on Enterprise Cyber Security, Identity & Access, and Security Controls and Policies for all services and workloads within Azure.

I also built and configured the technical platforms for the Proof-of-Concept (POC) and Pilot environments. My primary focus areas included the Azure foundation, Azure AOVPN, M365 Defender, Defender for Cloud, Defender for Endpoint, Defender for Identity, Defender for AKS, MCAS (Security Center), Intune, Endpoint Manager, Windows Defender, Defender Firewall, and BitLocker. Additionally, I served as the Lead Architect working on the Azure Cloud Security Stack, as well as Privileged Access Management (PAM) for on-premise environments and Privileged Identity Management (PIM) for hybrid identity control in Azure.

* Lead Architect on Azure Security and the MS Cloud Security Stack toolset.
* Lead on design, Standards and polices for POC\Pilot of Azure foundation.
* Designed and created Standards & Polices for Azure AOVPN, Azure XDR Stack, Defender for Endpoint, Defender for Identity, Defender for AKS, MCAS, Azure Defender (Security Center) Intune, Endpoint Manager, Windows Defender, Defender Firewall and Bit Locker.
* Configuration, integration, and troubleshooting of all Cloud Security Tool Stack components and services.
* Technical Lead on Design, Implementation and deployment of Windows Defender, Windows Firewall and Bit locker to 76 thousand endpoints globally.
* Created Windows Defender, Windows Firewall and Bit locker Standard configurations and policies.
* Designed AKS Security Requirements & Application Security Requirements for EKS & AKS.
* Implemented Container Security Design and Standards using Prisma & Defender for AKS.
* Architected and engineered the Azure Foundation for all Red Data workload migrations.
* Designed secured container snapshots, Secured Images, and managed Docker volumes.
* Designed Policy Standards and Design for Intune, Azure Sentinel and MCAS.

***Eli Lilly\Elanco Chicago*, Illinois** **04**/**2018 – 04/2019**

***Title:*** *Principal Information Security Architect* ***(Contract)***

**Job Description:**

A Principal IT Security Consultant working on the Transformation to Azure Migration initiative. Focused heavily on Enterprise Cyber Security, Identity & Access, Security Controls and Policies, Kubernetes & other Cloud workload Migrations, Enterprise Security Architecture, Engineering, Compliance and Governance. Lead Architect working on the Office 365 migration, PAM (On-premise), PIM (Azure), Snowflake Data warehouse and Datahub migration Projects. Deploying the Azure Foundational Security Standards and Assessments.

* Lead Architect for Global IT roadmap focused on Security & Identity Access. (Interim +Long term)
* Lead Azure Cloud Security Architect (Security Controls, Policies, Standards and GRC)
* Lead on Unified GRC assessments for Enterprise On-Premise and Cloud Platforms.
* Provided full Advisory on Best Practice, Standards, Policy, and Industry Analysis & RD (Gartner)
* Assisted in the Design, Architecture and Engineering Microsoft PAM Red Forest model for Enterprise evaluation VS CyberArk the Holistic On-Premise environment.
* AD OU Structure Project (Tiering Model for Containment and segregation)
* Lead Architect on IAM/PAM/PIM tools with deployment, configuration, integration and troubleshooting CyberArk Privileged Account Security product suite - Enterprise Azure Key Vault, Password Vault Web Access, Central Policy Manager, Privileged Session Manager, Application Identity Manager, and Privileged Threat Analytics
* Designed and Implemented Container Code VRM Scanning (Sonar Cube, AKS Defender, Twistlock)
* Designed AKS Security Requirements & Application Security Requirements for OCP & AKS
* Implemented Container Endpoint Security Design and Standards.
* Architected and engineered the Azure Foundation for all Red Data workload migrations.
* Lead on Security Reviews for Cloud based Workload (AKS, GKS, Datahub, Data Factories)
* Designed secured container snapshots, Secured Images, and managed Docker volumes.
* Designed Policy Standards and Design for CrowdStrike Endpoint and MDM security Platform.
* Designed and implemented NGAV Falcon Prevent for Endpoint Malware Protection.
* Designed and implemented Crowd strike Insight- EDR for Detect and Alert for select subsidiaries.
* Designed and implemented Falcon for mobile- Endpoint Protection for MDM.
* Designed and implemented CrowdStrike HFW- Host Firewall management for SSC
* Experience as a security professional in installing, managing, and monitoring of CyberArk Privileged account security tool modules.

Privileged Access Management (PAM) Remediation and Engineering team whose role is to secure Web Based applications on user access and authorization.

* Designed SEIM Integration Standard and Cloud Storage account Security Standards.
* Incident Response, Application Security, Threat Defense, Vulnerability Management, Threat Intelligence Process Validation, and design.
* Created logical and Physical Infrastructure Diagrams for all security Platforms including Application-Level Security plans, Dataflows.
* Created the Cloud On-Boarding Standard & Policy for Gold Standard Application Onboarding into Azure and On-premise.
* Assisted in Defining Azure Subscriptions, RG’s, VM’s and all other resource’s structure.
* Defined and assisted in the creation of an S-SDLC process for remediation of security Vulnerabilities.
* Defined Azure Network & Systems Architecture using Azure VNETS, VPN and express route to establish connectivity between on premise and cloud.
* Architected the Azure Security foundation with (NSG’s, ASG’s, MCAS, ATP, AIP, MTP, INTUNE, PKI, security Controls and Policies.
* Performed CIS Hardening and overall Security Assessments for Azure Foundation, Palo Alto Panorama, Azure AD and On-Premises Active Directory Infrastructures.
* Defined and assisted Application and Infrastructure owners in architectural reference designs and artifacts.
* Created and Defined On-prem and Cloud Network and Systems Infrastructure Security Plans.
* Defined Azure Identity architecture using Azure AAD, MFA, Conditional Access, SSO, Application proxy, B2B, B2C, PIM, SSPR and Azure Sentinel SIEM integration. (Documented)
* Architected the CF Azure Function and APP Service Plan design and implementation plans for PAAS services.

***CNA Insurance Chicago*, Illinois** **04**/**2017 – 04/2018**

***Title:*** *Senior Information Security Architect* ***(Contract)***

**Job Description:**

A Senior Consultant working on the company’s global IT initiative for Cloud Design and migration, Zero Trust, EDR, NDR, Information and Cyber Security. Focused heavily on Enterprise Cyber Security, identity management, Identity Access, Security Controls and Policies, Cloud workload Migrations, Enterprise Security Architecture, Engineering, Compliance and Governance.

* Spearheaded CNA’s Highest-level IT Security Projects as an Architectural & Engineering lead.
* Assisted in the Design, Architecture and Engineering of the Holistic Azure Foundation
* Responsible CNA’s Zero Trust program Architecture related to (Network, Endpoints, Application & Data Micro-Segmentation, SDN, EDR and NDR)
* AWS Cloud platform and its features which includes EC2, VPC, EBS, AMI, SNS, RDS, EBS, Cloud Watch, Cloud Trail, Cloud Formation AWS Config, Autos calling, Cloud Front, IAM, S3, R53.
* Incident Response, Application Security, Threat Defense, Vulnerability Management, Threat Intelligence Process Validation, and design.
* Implemented Container Security VRM Platforms (Microsoft Defender, Twistlock, Prisma)
* Implemented Container Code VRM Scanning (Sonar Cube, AKS Defender, Twistlock)
* Designed AKS Security Requirements & Application Security Requirements for GKS & AKS
* Implemented Container Endpoint Security Design and Standards
* Architected, engineered and deployed the Azure Foundation for all Red Data workload migrations.
* Lead on Security Reviews for Cloud based Workload (AKS, GKS, Datahub, Data Factories)
* Designed secured container snapshots, Secured Images, and managed Docker volumes.
* Designed Docker Scan of images and Containers function using Kubernetes by creating master and node and Container security Platforms and functions.
* Assisted in Defining Azure Subscriptions, RG’s, VM’s and all other resources structure.
* Created Security Design and Standards for Container and Pod Micro-segmentation.
* Assisted in Development of ARM templates to automate the provisioning and resource deployment process.
* Defined and assisted in the creation of an S-SDLC process for remediation of security Vulnerabilities.
* Defined Azure Network & Systems Architecture using Azure VNETS, VPN and express route to establish connectivity between on premise and cloud.
* Architected the Azure Security foundation with (NSG’s, ASG’s, MCAS, Defender for Identity ATP, Defender ATP, AIP, MTP, Intune, PKI, Policies, and other security Controls.
* Performed CIS Hardening and overall Security Assessments for Azure Foundation, Palo Alto Panorama, Azure AD and On-Premise Active Directory Infrastructures.
* Implemented Cisco ISE Endpoint access control and visibility, globally for all CNA and its subsidiaries in the UK and Europe.
* Migrated from Carbon Black for EDR to CrowdStrike EDR for North\South traffic restriction, containment, and control. NGAV Endpoint Threat prevention\Insight for EDR Protection\Falcon for device and Identity MDM and HFW- Host based Firewall management.
* Defined and assisted Application and Infrastructure owners design Application-Level Security plans
* Created and Defined On-prem and Cloud Network and Systems Infrastructure Security Plans.
* Defined Azure Identity architecture using Azure AAD, MFA, Conditional Access, SSO, Application proxy, B2B, B2C, PIM, SSPR and Azure Sentinel SIEM integration.
* Provided technical guidance on building solutions using Azure SAAS, PaaS and other services.
* Architected methodology used for enterprise-wide data flow mappings of End Points, Applications and Data for all East\West lateral Traffic and North\South traffic.
* Worked with 3 MSP’s to build, evaluate and Pilot,Palo Alto Panorama, Guardicore, Illumio, Pulse Secure & Cisco Tetration for Micro-segmentation solution.
* Experience in handling various modules of CyberArk, mainly Enterprise Password vault (EPV), Application Identity management (AIM), Central Policy Manager (CPM), Privileged Session management (PSM), Event Notification Engine (ENE).

***Microsoft Chicago*, Illinois** **04**/**2016 – 04/2017**

***Title:*** *Senior IT Security Consultant* **(Contract)**

**Job Description:**

Part of the **Microsoft Secured Infrastructure Services** division. Focused heavily on Enterprise Cyber Security, identity management, Identity Solutions, Cloud Migrations, Technology Divestitures, Enterprise Security Architecture, Engineering, Compliance and Governance. My duties were dedicated to Working on two separate and extremely complex Divestitures for Ecolab, Gap-Old Navy. Heavily focused on Identity segregation and migration, migration of Application Workloads to Azure, also was dedicated to Houston Metro for Compliance, Risk assessment, and Vulnerability Posture.

* Lead of Identity Architecture & Engineering for Enterprise grade Cybersecurity engagements,

focused on Azure AD Identity design, Integration, migration, and implementation.

* Provide subject matter expertise and project management experience on Azure Infrastructure migration for Identity focused on Azure IAAS, PAAS, and SAAS solutions.
* Senior Identity Consultant lead for **GAP\OLD NAVY** Divestiture
* Incident Response, Application Security, Threat Defense, Vulnerability Management, Threat Intelligence Process Validation, and design.
* Designed and Built the Security controls and Policies for the AKS containerization environment.
* Created Secured Docker orchestration and Docker containerization using Kubernetes.
* Secured Kubernetes for the deployment, scaling and management of Docker Containers.
* Developed Security Requirements and Standards for Azure Cloud Services, AKS, Azure Audit, Logging, Azure Storage, SQL Azure and in different PaaS Solutions with Web, and worker Roles and Azure Web Apps.
* Implemented Cloud Micro services architecture and workload Migration from On-Premises to Azure. (AKS, and all IAAS based workloads within Cloud)
* Performed various Migrations from OCP, GKS to AKS for centralized container platforms Hosting.
* Created Security requirements for Docker/Kubernetes container technologies in Azure.
* Involved in migrating physical Linux/Windows servers to Cloud (Azure) and testing.
* Created RBAC Security Design and Standards with Azure AD and AKS integration.
* Formation).
* Designed Docker image security model using a Docker file structure. (ACR functions).
* Implemented Azure Policy security control policies for Ansible and Ansible Tower automated playbooks.
* Worked in JIRA for ticketing and as well as defect tracking system and configure various workflows, customizations and plug-ins for JIRA bug/issue tracker, integrated Jenkins with JIRA, GitHub, Maven.
* Implemented phases of Software development life cycle (SDLC) with focus on the build and release of quality software and good Confidential Waterfall model, Agile Methodology (Scrum).
* Senior Identity Consultant lead for **ECOLAB\SPINCO** Divestiture
* Heavily engaged in designing, Integrating, and deploying Cloud, On-Prem Identity solutions. IDM (AD, Azure AD, IBM LDAP, SUN LDAP, OKTA, RSA, PING), DLP, IPS, IDS, MFA, Conditional access, Authentication, Web Security, Email Security, Vulnerability Security Assessments, SIEM, Encryption, Network Security and Disaster recovery for Cloud and On-Prem platforms.
* Senior Identity Consultant for **Houston DC Metro** Risk and Remediation RAP, for compliance

and Governance requirements and measures.

* Engaged in as Identity lead for Program management design for Sentinel SIEM
* Heavily engaged in designing the workload processes and deployment plans using SCCM for all Application tiers 1, 2, and 3.

***Grant Thornton LLP Chicago*, Illinois** **04**/**2015 – 04/2016**

**Title:** Senior IT Security Architect **(Contract)**

**Job Description:**

Enterprise IT Architect focused on Cybersecurity Protect/Detect/Respond lifecycle for the firm’s IT environments and for Critical Infrastructure Protection in the forms of Cyber Governance, Policy, and Strategy Services. Heavily focused on Azure and O365 Cloud security deployments and migrations.

I also provide the firms Cyber Regulations, Privacy, Compliance measures and Services for the Data Protection Services council. I work heavy on Architecture and Design Services across the spectrum. I was also involved with Modern Authentication enablement across the organizational platforms focused on On-Prem and Off-Prem (Cloud) Infrastructure solutions.

* Coordinate large-scale cybersecurity engagements focused on Azure & O365 Security
* Provide subject matter expertise and project management experience on Azure Infrastructure migration for IAAS, PAAS, and SAAS elements to serve as the "point person" for Cloud engagement teams.
* Implemented cloud services IAAS, PAAS, and SaaS which include Openstack , Kubernetes, Docker and Openshift .
* Heavily engaged in designing and deploying Cloud Security realms Such as IDM, DLP, IPS, IDS, Web Security, Email Security, Security Assessments, SIEM, Encryption, Network Security and Disaster recovery for Cloud and On-Prem platforms.
* Involved in Incident Response, Application Security, Threat Defense, Vulnerability Management, Threat Intelligence Process design and Validation.
* Engaged in design and deployment of various NAC’s such as Cisco ISE and Trend Net.
* Design of RSA infrastructure and Identity management platform. Authentication Manager, SecurID
* RSA VPN integration, Terminal Services SecureID deployment, Integration with AD.
* Heavily engaged in designing the roadmap and migrating Tier 1, 2, and 3 enterprise business applications to Azure Private and Hybrid cloud IAAS platforms.
* Develop and review reports and presentations for both technical and executive audiences.
* Assist staff by providing mentorship and coaching to grow their technical and consulting skills.
* Heavily focused on Azure Network Infrastructure connectivity model focused on Express route architecture, design, and deployment.
* Heavily engaged with over 8 MSP’s in the design and deployment of a complex Azure and Cloud ISP environment.
* Planning and budgeting to motivational and promotional activities expounding the value of cybersecurity.
* Auditing and remediation of cybersecurity frameworks / standards like RMF, ISO/IEC 27001:2013, NIST CSF, NIST 800-53, etc.
* Participate in preparation and implementation of necessary cybersecurity policies, standards, procedures, and guidelines, in conjunction with the Security Committee.
* Participate in the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies etc. and applicable laws and regulations.
* Participate in cybersecurity risk assessments and controls selection activities.

***RPAI (Retail Properties of America) Oakbrook*, Illinois** **06**/**2014 – 04/2015**

**Title:** Senior IT Security Architect **(Contract)**

**Job Description:**

Enterprise IT Architect Responsible Active Directory, Proxy, Azure, Exchange Hybrid, DNS and Office 365 migration and enhancement. My core role was to optimize and enhance the Entirety of AD, O365 & Proxy. Responsible for AD, O365, Proxy Security Standards and Principles for business and technology, Enterprise Wide.

* Architected, Engineered, and deployed new AD Security, AD Domain consolidation, AD Cleanup projects in full.
* Analysis and implementation of Active Directory Enterprise Services & hardened Authentication methods across the Enterprise Infrastructure Platform.
* RSA SecurID and Authentication Manager device Deployment for IDM integration.
* RSA deployment with VMware integration.
* Implemented Service Now and AD Audit & Management Plus integration and SSO authentication core for application Tier security.
* Active Directory, MS Exchange, Identity Management, SIEM, Firewalls, Proxy, Reporting, Azure, AWS, IPS/IDS, PCI/DSS, HIPAA, SOC, FISMA, ITIL and NIST
* Encryption (Two Factor/SSO/Kerberos/LDAP/SSL/ADFS/LDAPS/SAML)
* Conducted an Active Directory, Exchange and Office 365 Security Risk Assessments and prepared recommendations for Countermeasures.
* Provisioned input for the determination and analysis of AD, Proxy Security Policies, Risk Analysis, accreditation package analysis, Engineering change proposal analysis, and developing process and procedures such as implementation guides.
* Implementing and standardizing Directory Service, Identity Management, and AD structures.  
  Providing operational engineering and support for AD infrastructure design in the establishment of the AD Enterprise system.
* Developed and implemented a consolidated and standardized Group Policy Object (GPO) and Internet Protocol Security (IPsec) model designs in support of the multiple AD environments across the enterprise.
* Reviewed and advised The IT steering committee on the alignment of project requirements with related AD applications, and enterprise designs and plans.
* Providing advanced Engineering integration support to mitigate unforeseen high Level and complex technical issues.

***United Airlines Chicago*, Illinois** **02**/**2013 – 06/2014**

**Title:** Principal IT Security Architect **(Contract)**

**Job Description:**

A Senior IT Enterprise Architect strongly focused on holistic Cyber Security for United Airlines. My role at United is **Architecture, Engineering, Management and Deployment oversight** of highly secured enterprise-wide Web Proxy solutions, focused on Forward, Reverse, Applications Security and Source IP.

I was brought on with the role of analyzing the United Airlines web proxy landscape globally. The goal was to perform an assessment of the current health state and security vulnerabilities that may exist for United’s Web proxy environment.

* Designed, implemented, and deployed new highly secured Enterprise Proxy Infrastructure solutions for Forward, Reverse and Source IP Infrastructure design.
* Analysis of current issues, risks, and vulnerabilities within the current Enterprise Proxy layout Enterprise-wide.
* Design and Deployment of O365 with Azure and AWS platforms integrated with AD.
* Designed Active Directory integration and Access & Authentication model for O365 deployment.
* Designed Proxy PAC’s security Files for Proxy implementations with Blue Coat and Zscaler
* Created scripts with code focused on ensuring data security and protection.
* Design of enterprise-wide Active Directory Kerberos\LDAPS\MFA authentication integration with Web proxy with O365.
* Design and implementation of Private, Public, and Hybrid cloud Security solutions for Azure, AWS and proprietary cloud-based systems.
* Global Proxy Infrastructure oversight and management control. (F5, TMG, Zscaler & Blue Coat Proxy)
* Designed new Proxy architecture to replace TMG Proxy with F5 APM and SWG within the united Proxy enterprise platform and virtual infrastructure.
* Design and Deployment of Zscaler Web proxy Firewall globally over 795 Global sites.
* Designed Hybrid Zscaler Cloud Firewall solutions and deployment for Edge firewalls.
* Design of Security Policies and access controls for web access and usage.

***Continuum IT, Inc. Chicago*, Illinois** **04**/**2010 –02/2013**

**Title:** Senior IT Consultant **(Contract)**

**Job Description:**

Lead IT Consultant Responsible for overseeing a company's **cloud computing** technical and functional strategy. This includes **cloud** adoption plans, **cloud** applications design, and **cloud** management and monitoring.

Senior Technical Oversight of Network and Systems Infrastructure solutions, Virtualization, security compliance and solutions. Lead security Architect responsible for design, Deployment and support of Microsoft and Non-Microsoft End to End Infrastructure Technologies.

Lead IT Consultant responsible for Enterprise and middle market Cloud Migrations and transitions. Global BPO Security Solutions using advanced security and compliance protocol for enterprise Applications Solutions, integrated with heavy MPLS and Public Tunneling infrastructure, using Exchange, Lync/SIP TMG\UAG\Cisco ASA\ security Platforms. PCI & HIPPA Systems Security compliance lead for 3 major BPO’s in the US, Philippines, and China.

* Design and implementation of Private, Public, Hybrid cloud solutions for Azure, AWS, and proprietary cloud-based systems.
* Design, build, maintain and support a Security Event Monitoring Platform (SIEM) using IBM Qradar.
* Integrated applications with Python designing database architecture and server scripting, studying & establishing.
* Building/Maintaining Docker container clusters managed by Kubernetes Linux, Bash, GIT, Docker, on GCP.
* Streamlined installation of OpenShift on partner cloud infrastructure such as AWS and Azure.
* Utilized Kubernetes for the runtime environment of the CI/CD system to build, test deploy.
* Implemented Qrader SIEM as an enterprise central event and security logging platform.
* Upper Tier levels Application integration with IBM Qradar.
* Senior technical lead and ambassador for Cloud Technologies within the organization
* Development and execution of strategies which increased cloud knowledge throughout enterprise and middle market companies.
* Develop standards and Standard Operating Procedures regarding Cloud operations.
* Technical Design/Architecture for Exchange and Lync Server and Lync Voice Deployment
* Technical Design/Architecture for Exchange Server and Unified Messaging Deployment
* Technical Design/Consulting for Voice Gateway Deployment and Integration,
* Microsoft Lync and Microsoft Exchange Deployment, Migration and Support Services
* Technical Design/Architecture for Integrated UC Platform
* Technology Solutions Consulting and Support Services
* Server Deployment, Administration and Support Services
* Training and Technical Guidance for Engineers, Administrators and End Users
* Extremely Proficient in Microsoft Infrastructure technologies (ISA/TMG/UAG/ADFS and /IIS/SQL/Exchange/SharePoint/Lync/SCOM/TS Gateway/Terminal Services/ERP)
* WAN (Public & Private Design, Deployment & Support) MPLS & Tunneling Solutions.
* Redundancy and Load Performance expert using Various Load Balancing Solutions integrated with TMG/UAG for Application Redundancy and performance.
* Tunneling (Public Design of Public Point to Point Network topologies) IPSEC/SSL
* Highly Secured Predictive Dialer Platform, Architect.
* Troubleshooting of complex Server OS based issues along with a wide variety of Systems and Systems infrastructure related issues.
* Cloud Migration Expert (Off-Premise Migration specialist, All Platforms)
* Proficient in Protocol and Packet Analyzers (Wireshark, Microsoft Analyzers)
* TMG/UAG Expert Network and Systems Architect and Solutions Engineer.
* Development and implementation of security, traffic shaping, and custom policies on server, domain, switching and routing environments.
* TMG/UAG/ADFS Infrastructure Lead Implementer for Global PCI project.
* TMG/ADFS/UAG Reverse Proxy and Edge Gateway Solutions Architect & Infrastructure Engineer.
* Reverse Proxy and Edge Firewall designs.
* TMG/UAG firewall design expert (MS Back Office & Cross Platform Infrastructure Base)
* TMG/UAG Encryption expert (Two Factor/SSO/Kerberos/LDAP/SSL/ADFS/LDAPS/SAML)
* TMG/UAG Firewall Policy design expert (Exchange/IIS/SharePoint/SQL/VPN/Direct Access/
* TS Gateway/Custom Protocols, AD Authentication, IPSEC Tunnels/PPTP L2PT and etc.)
* Firewall and security modeling Lead. (Focused on TMG/UAG/Cisco/Juniper solutions)
* Reverse proxy Architect using TMG\UAG\ADFS for Security Platforms.
* Lead on BPO Call center IT Operations for Systems & Network Infrastructure.
* Lead on PCI Compliance Security Architecture, Deployment, and support.
* Lead on VOIP Infrastructure design and implementation of SIP infrastructure and IPPBX
* Group policy, Power shell scripting, trust relationships, and multi-domain/multi-forest designs, Microsoft Active Directory, Microsoft Exchange Server 2003, Exchange 2007, Exchange 2010, TMG/UAG expert and migration specialist.
* Deployment, configuration and administration of Network infrastructure Platforms (ISA, TMG & UAG Gateway, Cisco, Juniper, F5, A10, Barracuda, RSA, SSL, SSO and etc.)
* Lead enterprise cluster consultant Windows Cluster 2003, 2008 &

***Allstate Insurance Company, Inc. HQ Northbrook*, Illinois** **02**/**2009 – 04/2010**

**Title:** Senior Systems Architect **(Contract)**

**Job Description:** Lead Systems Infrastructure Engineer responsible for Active Directory, ADFS, Exchange, PCI Architecture for AD systems Infrastructure. Major role involved AD Re-Architecture for Domain consolidation of AD Corp wide. In addition to lead Architecture of PCI compliance Infrastructure for Allstate corporation holistically. Sat on Allstate PCI compliance Board.

* Active Directory Infrastructure Lead, Corp wide. National and Global.
* ADFS Infrastructure Lead Implementer for Global PCI project.
* ADFS Reverse Proxy and Edge Gateway Solutions Architect & Infrastructure Engineer.
* Firewall Policy design for Reverse Proxy and Edge Firewall designs.
* Encryption (Two Factor/SSO/Kerberos/LDAP/SSL/ADFS/LDAPS/SAML)
* Proxy and Policy (Exchange/IIS/SharePoint/SQL/VPN/Direct Access Applications
* TS Gateway/Custom Protocols, AD Authentication, IPSEC Tunnels/PPTP, L2PT and etc.)
* AD Forest & Domain Consolidation Project Lead.
* Design of the new Allstate PCI infrastructure for PCI compliance firm wide.
* Lead on AD integration with Hadoop Data warehousing and data scrubbing solutions.
* Design and implementation of AD & Systems PCI complaint Infrastructure, Enterprise Wide.
* Design and implementation of AD sites and Services model for AD replication standards and in conjunction with Exchange 2003/2007/2010 Routing Model.
* Lead member representing AD & Security Architecture on Weekly meetings with Allstate ATO heads. CIO/VP/Director/Senior managers.
* Design of Active Directory domain consolidated infrastructure model, also implementer.
* Design of Active Directory Load balancing model for Cross Platform Designs. Windows and Non-Windows Platforms. LDAP & Kerberos Authentication basis integrated with f5 Load Balancers.
* Design of Security & Authentication models for Active Directory Infrastructure.
* Main Author of Enterprise Schematic designs and Policy & Procedure Documentation for Systems.
* Design of internal Active Directory coexistence versioning Models, also implementer.
* Design and lead of **Active Directory Redundancy and High Availability Model globally.**
* **Collaboration** with over 600 teams globally on anything which Involved Active Directory
* Infrastructure and PCI compliance.

***Insurance Auto Auctions, Inc. (A Division of KAR Holdings) Westchester*, Illinois** **01**/**2008 – 01/2009**

**Title:** Senior Systems Engineer **(Contract)**

**Job Description:** Lead Systems Infrastructure Engineer responsible for Active Directory, Exchange, ISA/TMG/EDGE/UAG/Forefront Identity Manager and VMware Systems Infrastructure.

**Responsibilities:**

* Exchange 2003 Analysis and Stabilization Architect & lead implementer of project.
* Design and implementation of TMG\UAG Solutions for reverse proxy and Edge designs focused on (IIS, SharePoint, Exchange, SQL, Lync)
* Design and implementation of Exchange 2003/2010 Coexistence model.
* Design and implementation of Exchange 2010 Routing Model, and implementer.
* Design of Exchange 2003/2010 Internal and external Security model, in coexistence as well.
* Design of Exchange 2010 Network and Systems infrastructure model, also implementer
* Design of Exchange 2003/2010 Load balancing model.
* Design of internal Exchange 2003/2010 coexistence Routing Model, also implementer.
* Design of Exchange 2010 Redundancy and High Availability Model.
* Extremely Proficient with IIS 5/6/7/7.5 solutions and management.
* Cloud migration architect for 3 year Plan towards off-Premise development
* VMware Virtual Center specialist (Virtualized/Physical Exchange 2010/SQL/WEB environment)
* Design of off-premise VMware 4.1 ESXi DR environment of 175 servers used for DR scenarios.
* Design of Exchange 2010 DAG design model housed on (EMC V-MAX and VNX SAN Infrastructure)
* Design of DAG resiliency and failover integration model. (Load balancing and failover model)
* Exchange 2010 DAG Replication model and implementer (dedicated MPLS, OC3 pipes for MAPI Exchange network and MAPI services)
* Design of Exchange 2003/2010 Services and functions design model and implementer. (GAL, OAB, Public Folders, ECP.OWA, EWS, Outlook Anywhere, Active Sync and Windows Mobile)
* SharePoint Integration and mail data migration
* Successful Migration into 2010 and successfully migration of 6,000 users from 2003 to 2010.
* Exchange 2010 Archiving Design model and implementer.
* Active Directory Risk and health assessment lead and implementer.
* Active Directory Assessment changes implementer.
* TMG ISA 2006/2010 Expert (Firewall Design, Policy creation, routing, Protocol and etc.)
* Full Microsoft back-office specialist (Windows Server OS, Exchange, IIS, SQL, TMG, SCOM,

***Advanced Datacom Solutions, Inc. ADSI*** Oak Brook, Illinois 2003 – 2008

**Title:** Senior Information Technology Consultant

**Job Description:** Head IT specialist focused on Network and Systems Infrastructure projects all over the North America. Responsible for Microsoft Back-office projects such as, Active Directory, Exchange, SQL, SharePoint, DPM, SAN Infrastructure, Applications, ISA/TMG//UAG and Infrastructure as whole.

**Responsibilities:**

* Extremely proficient in Microsoft Server technologies such as, Microsoft Active Directory, Microsoft Exchange 2003 to Exchange 2010, ISA/TMG/UAG , SQL, SharePoint, IIS, Terminal Services, TS Gateway, SCOM, DPM, FIM, DNS, WINS, DHCP, Forefront Security Products an etc.
* Lead on VMware 4.1 ESXi Migration project of nearly 1000 servers from Hardware to Virtual. Ground up design, development and deployment of VMware infrastructure.
* Expert migration specialist from Existing to New Scenarios.
* Lead enterprise cluster consultant on various client networks. (Windows Cluster 2003, 2008)
* Reverse Proxy and Edge Gateway Solutions Architect & Infrastructure Engineer.
* TS Gateway/Custom Protocols, AD Authentication, IPSEC Tunnels/PPTP, L2PT and etc.)
* Lead enterprise level project consultant on Server 2003 to server 2008 infrastructure migration projects (large scale for various clients with thousands of users).
* Lead infrastructure engineer on various projects. (Security, SAN/NAS, WAN, LAN, WEB Application Development, VPN, VOIP, CRM and Stat integration).
* Implemented internal and external systems monitoring solutions.
* Microsoft Server OS, MS ISA Firewall, MS IIS, MS Exchange expert. (All versions)
* Highly Proficient of VPN, IPSEC, PPTP DNS, DHCP, WINS and etc...
* Development and implementation of security, traffic shaping, and custom policies on server, domain, switching and routing environments.
* Troubleshooting of a wide variety of infrastructure issues.
* Effectively respond quickly, reliably, and effectively to the requests for support from users of the systems.
* Storage (SAN and NAS EMC/DELL) configuration and deployment.
* Database implementation and Clustering (SQL environment).
* Document and communicate status, procedures, and plans.

***Sidley LLP,*** Chicago HQ 2000 – 2003

**Title:** Technology Integration Specialist

**Responsibilities:**

* Instrumental in developing and implementing business continuity and disaster recovery (BCP & DRP) Plans for firm sites throughout the global realm.
* Managed my immediate network team (eight member staff) (one of 23 teams) in the pre and post 9/11 attacks in moving our entire 900 staff from ground zero to temp 3rd Ave office space.
* Spearheaded creation of four new information-security departments, including risk assessment, vulnerability, penetration testing, and security infrastructure services.
* Hand selected employees from information technology department to build risk assessment team charged with analyzing all critical systems, developing reports to document systems vulnerabilities, and recommending appropriate solutions.
* Created company policies and procedures governing corporate security, email and Internet usage, access control, and helpdesk incident response.
* Designed and standardized the Westlaw & Lexisinfrastructure as well as the client design with billing validation tools. Migrated legal our research environment from local to web based.
* Developed policy and procedures for the new IS lab.
* Also assisted on designing ISA standards for specific internet traffic.
* Directed standard and non-standard methodologies for application distribution.
* Defined all base standards for firm wide (national & global) desktop & Server OS imaging environments.

***AON CORPORATION***, (TEK SYSTEMS) Chicago, IL 1999 – 2000

**Title:** Senior Network Engineer

**Responsibilities:**

* Managed and expanded high-volume load-balanced datacenter network environment serving millions of transactions a day.
* Manage all network infrastructure including Cisco firewalls, routers, switches etc.
* Made recommendations to enhance uptime, performance, and reliability.
* Ensure all network equipment is kept up to date with security patches and feature upgrades.
* Apply routine changes in support of technology projects and optimal day-to-day operations.
* Triage and resolve issues by working collaboratively with team members and service providers.

***PEOPLES ENERGY CORPORATION,*** Chicago, Illinois 1997 – 1999

**Title:** ITS Network Engineer

Provisioned comprehensive remote and onsite support for domestic and international customers including tier-III support for LAN/WAN Issues Company wide.

**Job Description:**

* maintained the availability of company computer resources including servers, workstations, laptops, printers, and multimedia equipment.
* Administered multi-server Windows NT LAN, 10,000+ workstations and 7000+ end-users.
* Recommended, evaluated, and purchased IT assets.
* maintained inventory of IT assets & IS LAB.
* purchased software licensing and tracked licensing compliance.
* Designed and implemented multi-node network expansion.
* Administered and maintained Microsoft Exchange Server and user accounts.
* Maintained system tape backups and implemented disaster recovery plan.
* Maintained all servers, PC’s, workstations, and printers.
* Help Desk / End-user support for hardware, software, and Windows operating systems.
* Designed and maintained corporate Intranet and Internet sites.
* Produced system/network documentation, IT policies.
* Maintained network security policy, addressed server security issues and applied appropriate security patches and upgrades.