

Joshua Beye, Sr. Security Architect Engineer Analyst

JoshLBeye@gmail.com 201-306-8828

Summary

Proven information security leader with success in guiding implementation of leading-edge technology solutions while balancing security initiatives to risks, business operations and innovations. Specialties include server engineering, security design, systems architecture, configuration management, and systems administration with extensive experience healthcare, financial, cloud computing, and software development industries.

Experience Highlights

Assessment and Risk Management

- Penetration Testing
- Vulnerability Assessment
- Risk / Compliance Assessment
- Change Control Board Director
- Cyber Security Analyst

Security Frameworks

- ISO 27001 • COBIT • ITIL • FedRamp
- NIST 800-171 800-53 • DFARS

Compliance Experience

- PCI-DSS • HIPAA • HITECH • SOX
- Six Sigma • Agile • ITIL • PMI • GRC

Certifications

- CISSP • MCSE • PMP
- VMWare VCP • Network+

Operating Platforms

- Windows • Linux • Unix • OSX
- Azure/Entra • AWS • Office365

Industry Verticals

- Healthcare • Financial Services • Technology Consulting and Support • Professional Services
- Government • Software as a Service (SaaS) • Datacenter/Hosting Provider/Cloud/On-Prem

Education

Berkeley College • Bachelors of Arts • Business Management: Information Technology

Employment History

JBeyeIT Security Consultant • Boca Raton, FL

2023 - Current

Sr. Security Architect Consulting

My primary responsibility is developing Expert IT solutions for mid to large size companies in the Healthcare, Financial, Government, and Manufacturing industries. These services help executive management understand IT requirements and establish a baseline for infrastructure, security, and expansion for all IT requirements.

- Architect and support for Information Security Management Systems for DHS services.
- Strong communication skills and ability to work collaboratively with different stakeholders
- Work with sales team on pre-sales and post-sales customer security evaluations
- Developed and implement security architecture solutions that align with business goals and objectives
- Developed and enforce cybersecurity policies and procedures in alignment with healthcare regulatory standards.
- Developed and Implemented Information Security Solutions with Vendors Azure/Entra DevSecOPS SDLC AKS.
- Developed and Implemented Information Security Reporting using Nessus combined with risk controls and gap analysis
- Reviewed and tested emerging security technologies and their potential impact on the enterprise.
- Integrated security into SDLC process by enabling security testing in Continuous Integration and continuous delivery/deployment processes by using application security principles and best practices, including secure software development methodologies and security testing.
- Deployed Security risk management methodologies, including gap analysis, risk assessments, threat modeling, and vulnerability management.
- Production Support administering, monitoring, troubleshooting, configuring, enhancing and providing advanced customer support for the existing multi-level security infrastructure
- Deployment / Implementation planning and executing the implementation of new network designs or configurations or enhancements to the existing multi-level security infrastructure
- Design researching, recommending and designing new technologies, new configurations and enhancements to existing networks; providing consulting advice to customers on the capabilities of the multi-level security infrastructure environment

Gainwell Technologies LLC • Hamilton, NJ

2021 - 2023

Sr. Security Architect

- Consult, advise, and oversee the secure design of key IT system and infrastructure projects to ensure alignment with enterprise security architecture.
- Assist in planning, designing, and developing IAM technical solutions and alternatives with client teams to meet business requirements in adherence with client's and NIST standards, processes, and best practices to meet compliance and regulatory requirements.
- Provided technical guidance and support to project teams to ensure security requirements are integrated into project plans and solutions.
- Architected DHS web site solutions with FedRamp Moderate compliance. DevSecOps and Agile governance.
- Maintain and improve quality results by following standards, recommending improved policies and procedures.

Joshua Beye, Sr. Security Architect Engineer Analyst

JoshLBeye@gmail.com 201-306-8828

- Provided IAM SME experience for day-to-day system development, engineering, decision making, directions and maintenance activities of the team.
- Provided guidance, Leadership, and support to the IT Security department on security architecture matters
- Provided Strong analytical and problem-solving skills to identify and resolve complex security issues.
- Change Management Security review and approvals Approval POC for infrastructure changes
- Facilitated Cybersecurity security audit and systems architecture using NIST and ISO127001 regulations.
- Implementation project: Windows security hardening with Powershell scripting (Servers and Workstations)
- Implementation project: proof of concept security access web interface user authentication with IGA and MFA for DHS
- Security applications experience: SQL, PowerBI, Service Now, LDAP, Azure SSO, SAML, ADFS, Cyberark PAM, McAfee EPO, SCCM, IAM Sailpoint, Digicert, Server encryption, Nessus and Radar server monitoring, IT and Security Risk Management, Symantec VIP, Active Directory GPO, JSON API(AWS), and security auditing policies.

Guardian Technology Consulting Services, LLC • Princeton, NJ

2011 - 2021

Sr. Manager Security Architect (Acting Information Security Officer)

Developed Information Security Management System (ISMS) based on ISO27001-2 framework for cloud-based Active Directory and EHR solution.

- Support independent assessments of security controls as documented in the System Security Plan (SSP)
- Conducted threat risk assessments based on findings of security controls assessments.
- Developed development of Security Assessment Report (SAR), documenting Plans of Action and Milestones (POA&Ms), and developing Executive Summaries (ES)
- Developed and Implemented Information Security Policies and Procedures
- Developed and Implemented Information Security Business Impact Plan
- Implemented Change Management system with change verification
- Implemented Threat intelligence and security monitoring, including security information and event management (SIEM) and threat intelligence platforms.
- Support Identity and access management, including authentication, authorization, and directory services.
- Cloud security principles and best practices, including cloud security models and control.
- Architect network and infrastructure security, including firewalls, intrusion detection and prevention systems.
- Mobile security principles and best practices, including mobile device management and mobile application security.
- Coordinated and validate periodic 3rd party vulnerability and penetration testing- Leidos and RSA
- Promote Agile Architecture with the appropriate level of governance and verification as part of the delivery process to minimize overhead, ensure continuous flow of value, and balance intentional design with emergent design.
- Establish and maintain contacts with departments associated with your assigned architecture domain (Systems/Applications, Security, Information, Technology) to understand activities, drivers, requirements, and alternatives being considered and/or implemented. Managing relationships with those key leads to staying connected, and influence alignment with future state architecture.
- Analyze and track technology industry and market trends and determine their potential impact on the enterprise.
- Conduct proof-of-concept solutions and make recommendations. Participate in vendor and product evaluations.
- Lead assigned governance activities following established processes for meeting logs, highlights, etc...

Joshua Beye, Sr. Security Architect Engineer Analyst

JoshLBeye@gmail.com 201-306-8828

- Reduced non-staff IT costs by 25% while maintaining key metrics through VMware virtualization, application rationalization, legacy system retirement, and SAN storage consolidation.
- Implemented periodic review of access controls NIST 800-171, 800-53 and DFARS compliance regulations
- Work with sales team on pre-sales and post-sales customer security evaluations
- Facilitated Cybersecurity security audit and systems architecture using NIST and DFARS regulations.
- Perform control mapping from NIST, COBIT, and ISO27001-2
- Perform company-wide risk assessment with Leidos and RSA
- Developed Security Auditing and Policy controls for Clients with 100 to 15,000 users
- Developed Server, Workstation, Appliance, Network Syslog control system SQL/HTML/ASPX
- Implemented a secure operating system deployment scheme for all new windows workstations using PXE boot and Slipstream which reduced time to deploy workstations by 20%
- Security tools experience Centrify MFA, MS ADFS, SCCM, SolarWinds Orion, RSA Netwitness, RSA Archer IT and Security Risk Management, McAfee EPO, AirWatch

L3/ Maryland Department of Transportation • Baltimore, MD

2009 - 2011

Security and VMWare Engineer

Developed VMware VSphere High-Availability system for multi datacenter, redundant environments for systems supporting EZPass and toll management.

- Architected, support and implement web application for Transportation Security Authority .Net and Java with Oracle and SQL database.

Merrill Lynch • Pennington, NJ

2007 - 2009

Systems and Security Analyst

Analyze infrastructure and system performance and failures for Client and server trading platform in use by Merrill Lynch Brokers (SWAT Team Senior Specialist Consultant)

- Perform forensic investigation and analysis using Custom trace tools NetIQ, Wireshark and Team Quest
- Architected and maintained Microsoft server systems. IIS, Exchange, SQL, VMWare

Kaiser Permanente • Pasadena, CA/ Silver Spring, MD

2005 - 2007

Production IT Manager

Manager/ Lead for team of 18 systems admins providing response and investigations into systems failures, security events and incidents in a large healthcare organization.

- Manager/Supervisor for thirty FTE's and Contractors
- SME in Server Systems and Information Security.
- Manage, document, and report escalation incidents to Executives and Business Partners

Merrill Lynch • New York, NY

2000 - 2005

Systems Engineer

Maintain infrastructure and servers for trading platforms used by Merrill Lynch Brokers