

BEN TOMHAVE, MS, CISSP

Herndon, VA • tomhave@secureconsulting.net • +1 703-282-8600 • linkedin.com/in/btomhave

SUMMARY

SENIOR CYBER/INFORMATION SECURITY ARCHITECT AND LEADER

I am a pragmatic, SME-level security architect, with 25 years of IT and information security experience. I hold a MS in Engineering Management from George Washington University, a BA in Computer Science from Luther College, a CISSP (#46697), and am a graduate of the BJ Fogg Behavior Design Boot Camp, which gives me a unique perspective on information security practices and challenges.

Specific recent experience includes providing security architecture technical leadership within a Fortune 500 hospitality leader; managing a team of security architects and engineers; cloud (AWS) and container security, data security, and bi-modal enterprise security; research, publication and advisory services on topics including risk assessment and management, application security and DevSecOps, and security strategy; security architecture for identity and access management and multi-factor authentication projects; and, product and application security, including application security testing strategy, developer outreach and education on secure coding, and advising product teams on security practices and requirements.

What drives me as a security architect is the challenge of clearly identifying a problem and then pursuing a solution in a structured, logical manner, including defining clear criteria for completion and success. The joy of this work is in the ever-changing challenge and diverse technical challenges. I have worked hands-on with dozens, perhaps hundreds, of different technologies over the course of my career.

CAREER HIGHLIGHTS

I have worked for a wide range of organizations, from small to large, serving in almost every information security role. My experience includes:

- Principal Security Architect @ Hilton
- Firewall Lab Analyst @ ICSA Labs
- BJ Fogg Behavior Design Boot Camp (2017)
- Sr. Technical Security Engineer @ AOL
- IT Auditor @ E&Y
- Public speaking @ dozens of events, including RSA, MISTI, ISSA, RMISC, RVASec, and Gartner events
- Research Director @ Gartner
- InfoSec Analyst (Firewalls) @ Wells Fargo
- Tripwire 2011 "Top 25 Influencers in Security" and CISO Platform 2018 "Top 100 IT Security Influencers"

CORE COMPETENCIES

Security architecture design and assessment (legacy and cloud), management, and strategy; application security program management and securing DevOps (DevSecOps); IAM strategy and architecture (including federation and MFA); governance, risk management, and compliance (GRC); security education, training, and awareness program development, management, and delivery, including a focus on behavioral information security; security product strategy and market analysis; analyst relations.

Keywords: AWS, cloud, container, DevOps/DevSecOps, application security, secure coding, IAM, GRC, behavioral infosec, architecture, strategy, program management, product security, program assessment and efficacy, enterprise security architecture, digital transformation, agile, waterfall, SDLC, CIS benchmarks, FAIR, risk management, pragmatic, functional

BEN TOMHAVE, MS, CISSP

RECENT WORK EXPERIENCE

Hobsons, Arlington, VA (remote)

June 2020 to present

Cloud Security Architect

Provided technical security leadership within the CloudOps team and across all of the Technology division. Day-to-day responsibilities included working with software development project teams to ensure proper cloud security measures were in place and maintained, leading tooling evaluations (e.g., log management, container and serverless security tools), and leading clean-up of AWS IAM configurations (including a transition to federated SSO). Worked in a matrixed relationship with the Security team to also provide input and propose direction on key capabilities such as security standards and operational security practices.

Hilton Worldwide, McLean, VA (remote)

March 2019 to June 2020

Principal Cyber Security Architect

As principal security architect, I was a technical leader within the Global Information Security team providing security architecture and strategy guidance to projects and teams on a variety of topics, including DevSecOps, application security testing, secure coding, secure application and system design, cloud and container security, and enterprise security. My day-to-day activities included reviewing or advising project designs, working within internal security resources on testing approaches, planning and developing security standards, and being a general advocate for information security across the organization.

Falcon's View Consulting, LLC, Herndon, VA

June 2015 to present

Principal

As a solo consulting practice, providing cybersecurity professional services to multiple industries. Project work includes content development, security architecture, security product strategy and development, high-level security assessment and advisory services, specialized security training, and DevOps/DevSecOps architecture. Engagements include technical security ghost writing, program assessment based on NIST CSF, security advisory services on topics including risk management and container security, and general enterprise security architecture.

Project highlights:

- Security assessment and architecture for an e-commerce platform software development firm.
- Security architecture services for a major entertainment company.
- Development and delivery of DevOps and DevSecOps courses.
- Technical editing for a pentesting firm.
- Technical project management for a major financial services company (application security monitoring).
- Custom content development for security vendors (e.g., blogs and articles).

Pearson, Centennial, CO (remote)

September 2017 to April 2018

Manager, Security Engineering and Architecture

Provided front-line management of a team of security engineers and architects responsible for identity and access management (IAM), multi-factor authentication (MFA), cloud security, container security, and data security (including encryption and certificate management). Provided technical leadership for the IAM and MFA initiative, including support for solution design and program communications.

BEN TOMHAVE, MS, CISSP

New Context, San Francisco, CA (remote)

June 2016 to July 2017

Principal Security Scientist

Served in a variable role performing research, product management of in-house development projects, and conducting business development. Efforts included creation of materials around the "Lean Security" methodology, development of presentations for conferences, and writing copy for sales collateral, blog posts, and byline articles. New Context has a focus on secure DevOps services and product development.

Ellucian, Fairfax, VA

October 2015 to June 2016

Manager, Information Security Architecture

Evaluated current security processes, tools, and practices as a member of the information security team reporting directly to the CISO. Charged with evaluating the effectiveness of current solutions and identifying gaps in security protection. Developed a comprehensive security architecture framework to evaluate and manage security architecture strategy for both traditional on-premises and cloud environments. Worked with vendors and cross-organizationally to identify, evaluate, and test (pilot) solutions. Technologies evaluated included data loss prevention (DLP), endpoint detection and response (EDR), traditional endpoint security, email security solutions (on-premises and Office 365), enterprise mobility management (EMM), network security tools and capabilities, identity and access management tools and capabilities, application security practices, cloud security tools (such as for AWS) and container (Docker) security tools.

K12, Inc., Herndon, VA

March 2015 to October 2015

Security Architect

As a member of the enterprise architecture team, charged with broad responsibilities to inject security practices into the overall application stack. Reviewed overall environment and developed an incremental roadmap for addressing critical gaps and charting a progressive course to more effective enterprise security over time.

Gartner, Inc., Arlington, VA (remote)

June 2013 to March 2015

Research Director

As a member of the Security & Risk Management Strategies team within Gartner for Technical Professionals, I conducted research into topics including risk management, security programs, security planning and management, application security, DLP, and SharePoint security. Additionally, I contributed content as a speaker at several Gartner and non-Gartner events and webinars, as well as delivering advisory services to clients and providing direct support to the sales team, both virtually and in-person, in multiple regions.

LockPath, Inc., Overland Park, KS (remote)

August 2011 to May 2013

Principal Consultant

Although originally hired to build a professional services team (put on hold due to a change in sales strategy), redeployed as needed to provide a number of value-add services, including customer training (development and delivery of comprehensive product onboarding curriculum); writing (blog posts, articles, and white papers); sales support and public speaking (including talks delivered at RSA USA, Secure360, Rocky Mountain InfoSec Conference, ISC² Security Congress, and the ISSA International Conference); partner enablement; and, a variety of other one-off projects (e.g., market analysis, security policy development).

Gemini Security Solutions, Chantilly, VA

May 2010 to August 2011

Sr. Security Analyst, Business Development Management

Experienced consultant hired to develop business relationships and grow client-base. Contributed to billable projects, development of proposals and statements of work, and promotion of the company. Increased company profile through writing and speaking engagements. Provided subject matter expertise in core competencies for use on client projects, internal consulting, and contributing to industry groups and initiatives.

BEN TOMHAVE, MS, CISSP

Independent - Various, Fairfax, VA

December 2009 to May 2010

Consultant / Author / Speaker

Worked through a variety of sources to provide security professional services to clients. Engagements included security and risk assessment, policy development, security program development and management, encryption key management, and secure application development. Client organizations ranged in size from small to large.

Foreground Security, Fairfax, VA

October 2009 to December 2009

Senior Security Engineer

Implementation and project management of a complete security infrastructure upgrade for a large civilian government agency. Helped manage deployment of SIEM, NIDS, HIDS, FISMA tool, and network monitoring tool.

Highwinds, Phoenix, AZ

January – September 2009

Technical Director of Information Security & Compliance

Served as the first full-time security resource for the organization with a primary focus on achieving compliance with the Payment Card Industry Data Security Standard (PCI DSS). Activities included addressing policy development, data cleanup, vulnerability scanning and remediation, incident response management, network security, logging and monitoring, identity and access management, and application security.

BT Professional Services, Reston, Virginia

September 2007 – January 2009

Senior Security Consultant

Led and participated in information security consulting engagements covering the full spectrum of information security, information security management, and information risk management. Developed and delivered training programs that enhanced internal capabilities to support and promote the security portfolio. Provided pre-sales support for security-related opportunities.

AOL, LLC, Dulles, Virginia

December 2003 – September 2007

Senior Technical Security Engineer

Initially, individual contributor for incident response management and security assurance team. Then, team lead for information security management, security assurance/architecture, and security ET&A. The success of the program resulted in a measurable decrease in security incidents and an overall improvement in risk resiliency.

Additional Experience:

- WAN/Security Engineer, I_TECH Corporation, a subsidiary of First Interstate Bancsystem (August – October 2003)
- Senior Systems Engineer, Sofast Communications (October 2001 – April 2002, January – August 2003)
- Network Security Lab Analyst, ICSA Labs (July – December 2002)
- Information Security Analyst 4, Wells Fargo Services Corporation (December 2000 – August 2001)
- Senior Security Consultant, BORN Information Services (January – October 2000)
- Senior Security Consultant, Ernst & Young LLP (1999–2000)
- Associate Network Systems Engineer, International Network Services (1998–1999)

BEN TOMHAVE, MS, CISSP

EDUCATION

Master of Science, Engineering Management (*Concentration: Information Security Management*)

THE GEORGE WASHINGTON UNIVERSITY – Washington, District of Columbia

Bachelor of Arts, Computer Science

LUTHER COLLEGE – Decorah, Iowa

Professional Certifications

CISSP – Certified Information Systems Security Professional #46697

DevOps Institute DevOps Foundation

DevOps Institute DevSecOps Engineering

PROFESSIONAL TRAINING AND CONFERENCES

Recently Completed Training

DevOps Institute DevOps Foundation

Splunk Fundamentals 1

AWS: Cloud Practitioner Essentials, Security Fundamentals Online, Well-Architected Training

BJ Fogg Behavior Design Boot Camp

Speaking Experience

RSA USA; Rocky Mountain InfoSec Conference (RMISC); ISSA International; MISTI InfoSec World Cloud Security World, and Cybersecurity World; Secure 360; ISC² Security Congress; SIRAcon, OWASP AppSec USA, AppSec DC, and Summit; Security B-Sides Austin and Ottawa, EnergySec Summit, NESCO Town Hall

PROFESSIONAL AFFILIATIONS

Senior Member – Information Systems Security Association (ISSA)