

Sean T. Malone

6810 168th St SW
Lynnwood, WA 98037

Mobile: 206-707-5025 Email: sean@seantmalone.com

Personal Website: www.seantmalone.com

LinkedIn: www.linkedin.com/in/seantmalone

C|CISO, CISSP, CISM, CISA

Summary

Assists organizations in achieving real risk reduction by ensuring that they have the people, technologies, and processes in place to enable business operations while preventing, detecting, and responding to attacks by sophisticated cyber adversaries. Deeply skilled in **Security Vision & Leadership, C-Suite Collaboration, Penetration Testing, Information Risk Management** and more. Open to challenging leadership opportunities that consist of moving quickly to create a direct, positive impact.

My Top 5 Strengths

Strategic – Futuristic – Competition – Activator – Ideation

Education

MS in Information Security & Assurance

Western Governors University, Salt Lake City, UT, March 2013

BS in Mathematics with Computer Science Concentration

University of Dallas, Irving, TX, May 2010

Key Certifications

Certified Chief Information Security Officer (**C|CISO**), ID# ECC21404275320, 2016

Certified Information Systems Security Professional (**CISSP**), ID# 409298, 2011

Certified Information Security Manager (**CISM**), ID# 1527229, 2015

Certified Information Systems Auditor (**CISA**), ID# 12100224, 2012

Professional Experience

FusionX

October 2012 to Present

FusionX helps customers manage cyber risk through a variety of services geared towards minimizing exposure and maximizing ROI. FusionX has a unique approach to providing holistic security solutions in complex environments to counter the most advanced and persistent cybersecurity threats. FusionX was acquired by Accenture in August 2015.

Chief Strategy Officer

April 2015 to Present

Business Development & Solution Engineering: Designed solutions to meet client needs for adversary simulation and strategic advisory services, with a reputation for closing deals through demonstration of technical excellence and understanding of the client's security program. Consistently achieved 50% year-over-year revenue growth.

Security Vision & Strategy: Consulted on baseline assessments, strategic vision, and gap analyses for complex enterprise information security programs. Produced executive roadmaps for continual improvement in teams, technology and processes. Implementation of these security strategies resulted in increased ability to withstand cyber attacks, as measured by annual sophisticated attack simulations.

C-Suite Collaboration: Worked directly with members of the executive team and board, including the CIO, CTO, CISO, and legal counsel of multiple organizations. Translated complex technical security issues into the language of business risk and provided guidance on security assessments, governance and incident response. Trusted member of informal security steering committees.

Cybersecurity Delivery Operations Manager

September 2014 to March 2015

Service Delivery Management: Managed service delivery for FusionX accounts with a total annual contract value over two million dollars. Responsible for project scoping, burn rates, scheduling, resource assignment, execution, report delivery and executive debriefing on key accounts. Achieved 100% renewal rate for these accounts and grew them year-over-year by expanding existing services and adding new services.

IT Operations Management: Responsible for delivery capabilities including internal IT infrastructure, exploit and tool development and build versus buy decisions. Designed dedicated assessment environments to meet client security requirements, resulting in account growth and renewal.

Principal Security Consultant

October 2012 to August 2014

Advisory Services Practice Lead: Lead the advisory services practice within FusionX and defined the service offering in this area. Assisted in the sale of advisory services to new clients and as an add-on to existing clients.

Sophisticated Attack Simulations: Executed advanced scenario-based red team assessments designed to evaluate the organization's ability to prevent, detect, and respond to sophisticated adversaries. Consistently identified critical technical and procedural issues with the potential to expose millions of payment cards and customer PII records, with possibly catastrophic impact to the client's bottom line.

Created Engagement Management Application: Designed, architected, prototyped, and managed the development of an internal web application for engagement management. Increased delivery team efficiency by using this application to facilitate collaboration and communication across local and distributed teams.

Coalfire Systems

July 2011 to September 2012

Coalfire is an IT Governance, Risk and Compliance (IT GRC) firm, serving as a trusted advisor and IT GRC tools-provider to security-conscious leaders in Retail, Financial Services, Healthcare, Hospitality, Higher Education, Government and Utilities.

Senior IT Security Consultant, Team Lead

Security Assessments and Consulting: Conducted network & application penetration testing, web application security reviews, mobile application reviews, and source code security analysis for Fortune-500 clients across all verticals. Consistently excellent performance led to a high rate of repeat business and being requested by name.

Team Leadership: Led the Seattle division of Coalfire Labs, responsible for project execution and team performance. Resolved schedule, project, and personnel conflicts resulting in on-time service delivery and satisfied clients.

Business Development: Served as the public face of Coalfire Labs in the Northwest region through research, trainings, and presentations designed both to educate and to attract potential clients and team members to Coalfire Systems. Received consistently positive feedback and strong leads as a result of this activity.

Pre-Sales Support: Supported the sales team in the northwest region and across the country by providing a deep level of pre-sales technical expertise to give the buyer a familiarity and comfort level with services and capabilities. Developed a reputation as the go-to guy when technical expertise was needed to close a sale.

Sears Holdings Corporation

June 2010 to June 2011

Sears Holdings Corporation is a leading integrated retailer focused on connecting the digital and physical shopping experiences. The company operates through its subsidiaries, including Sears, Roebuck and Co. and Kmart Corporation.

Technical Specialist, Enterprise Security Attack & Penetration Team

Penetration Testing / Web Application Security: Conducted network and application penetration testing, web application security reviews, and source code security analysis for internal clients. Identified vulnerabilities posing a high risk to the business and communicated them to the appropriate stakeholders for remediation, resulting in improved security posture and increased attack resiliency.

Secure Code Training: Provided secure code training for developers and instructed developers and system administrators on remediation of identified vulnerabilities. Repeated testing demonstrated improved defenses and lower likelihood of successful attacks.

Security Controls and Architecture: Reviewed security architecture specifications and modeled real-world threats against the architecture. Recommended improvements and additional security controls to protect critical data, applications, and systems.

IOActive (Internship)

May 2009 to April 2010

IOActive offers comprehensive computer security services with specializations in smart grid technologies, software assurance, and compliance.

Intern Computer Security Consultant

Web Security Assessments: Conducted manual security assessments web applications, perimeter networks, and internal networks. Identified critical vulnerabilities and developed proof-of-concept exploits that allowed the business to understand the risk, resulting in speedy remediation.

Selected Presentations

- Cyber Security (Panel) – Seattle Biz-Tech Summit, 2015
- Cybersecurity Risk Oversight – National Association of Corporate Directors, Texas TriCities Chapter, 2015
- How to Respond and Recover from a Cyber Event – Emerald Down IV: 2015 Cyber Security Workshop
- Cyber Forensics, Legal Requirements, and Business Continuity (Panel) – Emerald Down III: 2014 Cyber Security Workshop
- HiveMind – Distributed File Storage Using JavaScript Botnets – Toorcon Seattle, BSides Las Vegas, and DEF CON 21, 2013
- Hacking the Industry – BSides Seattle, 2012
- Securing the Application Layer – Institute of Internal Auditors, Puget Sound Chapter, 2012
- Solving Graph Theory Problems with Artificial Intelligence – University of Dallas, 2009

Publications

- Mark Torgerson, Richard Schroepel, Tim Draelos, Nathan Dautenhahn, Sean Malone, Andrea Walker, Michael Collins, and Hilarie Orman. "The SANDstorm Hash." Submission to NIST SHA-3 competition, 2008

Additional Training / Certification

- Cisco Certified Network Associate (CCNA), ID# CSC011928215, 2011
- GIAC Certified ISO-27000 Specialist (G2700), ID# 1034, 2012
- Computer Hacking Forensic Investigator (CHFI), ID# ECC956501, 2012
- Certified Ethical Hacker (CEH), ID# ECC956501, 2011
- Microsoft Certified Professional (MCP), ID# 6672707, 2009
- Red Team Training with Adversary Modeling, Sandia National Laboratories Information Design Assurance Red Team, 2008
- FCC Technician Class Amateur Radio License, 2002