Richard Bejtlich

Chief Security Strategist at FireEye, Inc.

[redacted]

Summary

Richard Bejtlich is Chief Security Strategist at FireEye, and was Mandiant's Chief Security Officer when FireEye acquired Mandiant in 2013. He is a nonresident senior fellow at the Brookings Institution, a board member at the Open Information Security Foundation, and an advisor to Threat Stack, Sqrrl, and Critical Stack. He is also a Master/Doctor of Philosophy in War Studies Researcher at King's College London. He was previously Director of Incident Response for General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Richard began his digital security career as a military intelligence officer in 1997 at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. His fourth book is "The Practice of Network Security Monitoring" (nostarch.com/nsm). He also writes for his blog (taosecurity.blogspot.com) and Twitter (@taosecurity).

Experience

Master/Doctor Of Philosophy In War Studies Researcher at King's College London

August 2014 - Present (7 months)

Researching application of strategic thought, especially operational art, to counter-intrusion campaigns. The research will identify elements of a successful computer network defense campaign, inspired by both classical and modern thinkers.

Advisor at Critical Stack

August 2014 - Present (7 months)

Advises Critical Stack on business strategy, product opportunities, communications, and other commercial organizational issues.

Advisor at Sqrrl

June 2014 - Present (9 months)

Advises Sqrrl on business strategy, product opportunities, communications, and other commercial organizational issues.

Chief Security Strategist at FireEye, Inc.

January 2014 - Present (1 year 2 months)

Empowers policy makers, international leaders, global customers, and concerned citizens to understand and mitigate digital risk through strategic security programs.

Nonresident Senior Fellow at The Brookings Institution
January 2014 - Present (1 year 2 months)
Researches integrating strategic thought into private sector cyber defense. Investigates the extent to which detection and response scales beyond the enterprise.

Advisor at Threat Stack, Inc
October 2013 - Present (1 year 5 months)
Advises Threat Stack on business strategy, product opportunities, communications, and other commercial organizational issues.

Board Member at The Open Information Security Foundation
March 2011 - Present (4 years)
Advises OISF on business strategy, product development, communications, and other non-profit organizational issues. Advocates use of OISF open source software like Suricata to complement computer security programs worldwide.

Chief Security Officer at Mandiant
April 2011 - January 2014 (2 years 10 months)
Managed Mandiant's digital risks, advocated defenses against advanced threats, and helped customers detect and respond to intrusions using the company's methods, products, and services. Transitioned to FireEye after acquisition of Mandiant in December 2013.

Director, Incident Response at General Electric
July 2007 - April 2011 (3 years 10 months)
Built and led GE Computer Incident Response Team (GE-CIRT, ge.com/cirt) from 0 to 40 analysts, defending 300,000 employees and 500,000 nodes in over 100 countries.

President & CEO at TaoSecurity LLC
June 2005 - June 2007 (2 years 1 month)
Provided independent digital security consulting and services for military, government, and commercial clients worldwide.
1 recommendation available upon request

Technical Director at ManTech International Corp.
February 2004 - June 2005 (1 year 5 months)
Performed computer forensics and intrusion analysis for government clients, and network security monitoring for corporate customers.

Principal Consultant at Foundstone
April 2002 - January 2004 (1 year 10 months)
Led incident response engagements for Fortune 100, tier one ISPs, and other organized crime and corporate espionage victims.

1 recommendation available upon request

Senior Security Engineer at Ball Aerospace & Technologies Corp.
February 2001 - April 2002 (1 year 3 months)
Designed, hired, trained, and led a twelve-person, 24x7 team to detect intrusions on commercial networks.

Chief, Real Time Intrusion Detection at AFCERT
September 1998 - February 2001 (2 years 6 months)
Led Air Force CERT's security monitoring mission, supervising 60 civilian and military staff; conducted hands-on technical analysis.
2 recommendations available upon request

Intelligence Officer at Air Intelligence Agency
February 1997 - September 1998 (1 year 8 months)
Created and coordinated information warfare plans and policies, and executed operations during Bosnia conflict.

Skills & Expertise

Computer Forensics
Intrusion Detection
Corporate Security
Security Operations
Security Services
Managed Security Services
Cyber Security
Security Management
Information Security Management
Internet Security
CISSP
Computer Security
Network Security
Security Research
Network Forensics
Security
IDS

Patents

Network intrusion detection visualization
United States Patent Application 20110067106
Inventors: Richard Bejtlich, Scott Evans, Et al

Network attack visualization and response through intelligent icons
United States Patent Application 20110066409

Inventors: Richard Bejtlich, Scott Evans, Et al

Publications

The Practice of Network Security Monitoring

No Starch July 22, 2013

Authors: Richard Bejtlich

In The Practice of Network Security Monitoring, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks — no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools.

Extrusion Detection

Addison-Wesley November 8, 2005

Authors: Richard Bejtlich

Real Digital Forensics

Addison-Wesley September 23, 2004

Authors: Richard Bejtlich, Keith Jones, Curtis Rose

The Tao of Network Security Monitoring

Addison-Wesley July 12, 2004

Authors: Richard Bejtlich

Education

Air Force Intelligence Officers Training Course

14N1, Military intelligence, 1996 - 1997

Harvard University, John F. Kennedy School of Government

Master of Public Policy (MPP), National Security, 1994 - 1996

United States Air Force Academy

Bachelor of Science (BS), History, Political Science, 1990 - 1994

Grade: 3rd of 1024

Activities and Societies: French and German minors