Richard Bejtlich

CURRENT POSITIONS

Nonresident Senior Fellow, The Brookings Institution. January 2014-present.
Founder, TaoSecurity LLC. June 2005-present.
Advisor, Threat Stack Inc. October 2013-present.
Advisor, Sqrrl. June 2014-present.

PAST POSITIONS

Chief Security Strategist, FireEye. January 2014-March 2017.
Advisor, Critical Stack. August 2014-July 2016.
Board Member, The Open Information Security Foundation. March 2011-April 2015.
Chief Security Officer, Mandiant. April 2011-January 2014.
Director, Incident Response, General Electric. July 2007-April 2011.
President and CEO, TaoSecurity LLC. Jun 2005-June 2007.
Technical Director, ManTech International Corp. February 2004-June 2005.
Principal Consultant, Foundstone. April 2002-January 2004.
Senior Security Engineer, Ball Aerospace & Technologies Corp. February 2001-April 2002.
Chief, Real Time Intrusion Detection, Air Force CERT. September 1998-February 2001.
Intelligence Officer, Air Intelligence Agency. February 1997-September 1998.

EDUCATION

Air Force Intelligence Officers Training Course. 14N1, Military intelligence, 1997.
Harvard University, John F. Kennedy School of Government. Master of Public Policy, 1996.
United States Air Force Academy. Bachelors of Science, History and Political Science, 1994.

RESEARCH AND TEACHING INTERESTS

Cybersecurity. Military operational art. Strategic thought.

PUBLICATIONS

Books

Practical Network Security Monitoring: Understanding Incident Detection and Response, 2013. No Starch Press.
Extrusion Detection: Security Monitoring for Internal Intrusions, 2005. Addison-Wesley Press.
Real Digital Forensics, 2005. Co-author with Keith Jones and Curtis Rose. Addison-Wesley Press.
The Tao of Network Security Monitoring: Beyond Intrusion Detection, 2004. Addison-Wesley Press.

Book Chapters

Cyber War in Perspective: Russian Aggression against Ukraine, 2015. Chapter 18. Editor: Kenneth Geers. NATO CCD COE.

Practical Malware Analysis, 2012. Foreword. Authors: Michael Sikorski and Andrew Honig. No Starch Press.

Linux Firewalls, 2007. Foreword. Author: Michael Rash. No Starch Press.

Incident Response: Computer Forensics, 2nd Ed, 2003. Contributor to chapters 8 and 14. Authors: Kevin Mandia, Chris Prosise, and Matt Pepe. McGraw-Hill/Osborne.

Hacking Exposed, 4th Ed, 2003. Case Study: Network Security Monitoring. Authors: Stuart McClure, Joel Scambray, and George Kurtz. McGraw-Hill/Osborne.

Articles

No scholarly journal publications.

Technical community contributions listed at http://www.taosecurity.com/research.html and https://brookings.academia.edu/RichardBejtlich.

AWARDS, GRANTS, FELLOWSHIPS.

Scholarship to attend Harvard University, John F. Kennedy School of Government MPP program.

AFFILIATIONS AND SERVICE TO THE PROFESSION.

None.