



## **Dr. Eric B. Cole Biography**

Dr. Cole is an industry expert with breadth and depth experience across integrated cyber security. He focuses on creating, enhancing and solving complex problems by bridging the gap between a business and technology mindset, with a focus on security and innovation.

Dr. Cole is a founder of Firmitas Secure and Secure Anchor Consulting, both leading providers of cyber security solutions and services. Dr. Cole is an invited speaker and subject matter expert on SCADA and critical infrastructure cyber security. He is a member of many key organizations including the Commission on Cyber Security for the 44th President (25 industry experts), the Purdue University Executive Advisory Board and a SME for the Nuclear Regulatory Commission.

Dr. Cole continuously executes on high-end consulting services to Fortune 500, Fortune 50, financial institutions, international organizations and the federal government. Engagements included creative ways to allow a major nuclear power plant to become compliant and put together a remediation plan to postpone fines for the organization. Dr. Cole continually stays abreast of cutting edge technology and industry regulations including NERC-CIP, CFATS and HSPD-7 and creates solutions that meet the business goals of an organization. Dr. Cole acts as an expert witness for several government and commercial companies in a variety of litigation (i.e. FTC vs. Microsoft and Nomadix vs. Second Rule).

At McAfee; Dr. Cole was a Senior Vice President and Chief Technology Officer of the Americas. As McAfee's visionary and evangelist Dr. Cole was responsible for strongly influencing the company's technical direction in alignment with our CEO, EVP, Product Operations and other key product executives and technologist across the world. Dr. Cole played an integral role in the company's strategic direction, development, and future growth as the global leader in digital security solutions. Dr. Cole was a key leader in the execution of technology strategy for technology platforms, partnerships, and external relationships. Dr. Cole worked closely with the CEO, EVP of Product Operations and other key stakeholders to establish a product vision and road map to achieve McAfee's goals and business strategies. Dr. Cole was engaged in identifying and capturing intellectual property and driving new innovation across the company.

Dr. Cole served at Lockheed Martin as IS&GS Chief Scientist and Lockheed Martin Senior Fellow. Lockheed Martin selected Dr. Cole into its prestigious fellowship program, an award it makes to less than 1% of its 130,000 employees. Moreover, Dr. Cole was the first Fellow within Lockheed Martin's Information Technology Division. As a Lockheed Martin Senior Fellow, he is a frequently invited speaker at a variety of conferences and security events focusing on security for SCADA systems. As Lockheed Martin Chief Scientist, Dr. Cole current role included performing research and development to advance the state-of-the-art in information systems security. Dr. Cole specialized in: secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems performing several security assessments for the energy sector. Over his 5+ years at Lockheed Martin, he played a lead technical advisory role in many high profile, security focused projects for Federal clients to include civil, Intel and department of defense, including the FBI Sentinel, DHS Eagle, JPL, Hanford and FBI IATI programs.

Dr Coles serves the SANS Institute as Dean of Faculty and a member of a 5 person team tasked with creating a degree granting institution and receiving certification from the state of Maryland. Currently offering two Master's degree program focused on technical people that need managerial skills and managers who need technical skills. The institute successfully passed first two phases of certification and should have official certification by the end of 2011. Designed and implemented curriculum and provide leadership to faculty to successfully deliver the degrees. Dr. Cole also served as Director of Research-Computer Network Attack-Enterprise Security Architecture and Director of the Cyber Defense Initiative. Dr. Cole was lead instructor and course developer for several security courses. Dr. Cole executed and contributed to the development of several of the GIAC certifications including GIAC Certified Security Essentials (GSEC), GIAC Certified Advanced Incident Handling Analysts (GCIH) and GIAC Certified Firewall Analysts (GCFW).

Dr. Cole has served as Chief Information Officer, Chief Security Officer, V.P. of Enterprise Security and Director of Security for several leading organizations including: Sytex Group, GraceIC, American Institutes for Research, Vista Information Technologies, and Teligent.

Dr. Cole began his career at the Central Intelligence Agency rising to Program Manager / Technical Director for the Internet Program Team with Office of Technical Services. Dr. Cole was a Senior Officer of the agency and implemented the Internet Program Team that specializes in rapid development and in exploiting the latest Internet technologies. Dr. Cole designed and developed several secure communication systems and was responsible for providing technical direction, technical design, security assessment, and programming modules. Dr. Cole secured internal servers, continually performed intrusion detection, and reviewed audit logs. Dr. Cole performed independent security reviews and penetration testing of (World Wide Web) servers for other offices. Identified several weaknesses and ways to fix those problems and secure the system. Dr. Cole received letter of appreciation from the DCI (Director of Central Intelligence) and several Exceptional Performance Awards for this project.

Dr. Cole is an Adjunct Professor at Georgetown University and New York Institute of Technology.

Dr Cole received a Doctorate degree in Network Security from Pace University, a Master of Science Degree in Computer Science from New York Institute of Technology where he was recognized as the sole recipient of the Harry Schure Graduate Memorial Award. Dr Cole received his Bachelor of Science degree from New York Institute of Technology in Computer Science with the following honors: Graduated Magna Cum Laude, Dorothy Schure Memorial Award, Jules Singer Award, Grace Hopper Award from Computer Associates, Presidential Academic Award (4.0 semesters), Presidential Service Award, Dean's List, Member of Who's Who Among Students in American Universities, and Member of Nu Epsilon Tau Honor Society.

### **Certifications / Organizations**

CISSP (Certified Information Systems Security Professional), MCSE (Microsoft Certified Systems Engineer), CCNA (Cisco Certified Network Associate) and ISS Internet Scanner and Real Secure Certification. Created several of the GIAC certification programs and exams. Member of ACM, IEEE, International Who's Who in Information Technology, CSI Computer Security Institute), ISSA (Information Systems Security Association), and ICSA (International Computer Security Association). Member of the editorial board for CVE (Common vulnerability and exposures) and member of the HoneyNet project. Both are invitation only memberships. Author and speaker for SANS Institute

### **Security Clearances:**

Top Secret clearances and Sensitive Compartmented access (TS/SCI/ISSA).

### **Publications and Journals**

Sample list of publications

Eric Cole and Sandy Ring, *Insider Threat*, Syngress Publishing, 2005

Eric Cole, Ron Krutz., and Jim Conley J.W., *The Network Security Bible*, John Wiley & Sons, New York, New York, 2005

Eric Cole, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*, John Wiley & Sons, 2003

Eric Cole, *Hackers Beware, The Ultimate Guide to Network Security*, New Riders, August, 2001

Eric Cole, Sandy Ring Taking a Lesson from Stealthy Rootkits, *IEEE Security and Privacy*, Vol 2 (4), pp. 38-45, Aug 2004

Eric Cole, Sandy Ring Volatile Memory Computer Forensics to Detect Kernel Level Compromise, *Lecture Notes in Computer Science, Information and Communications Security*, Springer Press, Vol 3269, ICICS Sep 2004, Malaga, Spain

Eric Cole, David Esler, and Sandy Ring Self-healing Mechanisms for Kernel System Compromises, *Proceedings of ACM Workshop on Self-managed Systems (WOSS) 04*, Oct 2004, Newport Beach, CA, USA

Eric Cole, Vignesh Kumar and Sandy Ring, Ant colony based optimization based model for network zero-configuration, *Proceedings of SPCOM 04*, Dec 2004, Bangalore India

Eric Cole, Vignesh Kumar, Sandy Ring, Transform Domain Steganography Detection using Fuzzy Inference Systems", *IEEE International Symposium on Multimedia Software Engineering*, 2004

Eric Cole, Vignesh Kumar and Sandy Ring, Least Significant Bit-Spatial Domain Steganography Detection using Least Significant Bit Plane Smoothness, *The 6th IASTED International Conference on SIGNAL AND IMAGE PROCESSING*, 2004

Eric Cole, Sandy Ring, Detecting Kernel Rootkits, *Sys Admin Magazine*, Vol. 12 (9), pp. 28-33, Sept 2003

Eric Cole, Ron Krutz The Computer Forensics CMM, *Proceedings of the SPIE Defense & Security Symposium*, 28 March-1 April, 2005

Eric Cole and Angela Orebaugh, Intrusion Prevention and Active Response: Implementing an Open Source Defense, *SysAdmin Magazine*, 2005

## **Patents**

### **Sample patents/patent pending**

Eric Cole, Scott Treadwell, CRYPTOGRAPHIC METHOD, SYSTEM AND ENGINE FOR ENCIIPHERED MESSAGE TRANSMISSION, Patent Pending, 1/20/04

Eric Cole, Sandra Ring, METHODOLOGY, SYSTEM, AND COMPUTER READABLE MEDIUM FOR DETECTING OPERATING SYSTEM EXPLOITATIONS, Patent Pending, 2/02/04

Eric Cole, Sandra Ring, METHODOLOGY, SYSTEM, COMPUTER READABLE MEDIUM, AND PRODUCT PROVIDING A SECURITY SOFTWARE SUITE FOR HANDLING OPERATING SYSTEM EXPLOITATIONS, Patent Pending, 2/26/04

Eric Cole, Sandra Ring, METHODOLOGY, SYSTEM, AND COMPUTER-READABLE MEDIUM FOR COLLECTING DATA FROM A COMPUTER, Patent Pending, 3/18/04

Eric Cole, Scott Treadwell, METHODOLOGY, SYSTEM AND COMPUTER READABLE MEDIUM FOR STREAMS-BASED PACKET FILTERING, Patent Pending, 4/22/04

Eric Cole, Sandra Ring, METHOD, SYSTEM, AND COMPUTER-READABLE MEDIUM FOR RECOVERING FROM AN OPERATING SYSTEM EXPLOIT, Patent Pending, 6/17/04

Eric Cole, James Conley, DETECTOR AND COMPUTERIZED METHOD FOR DETERMINING AN OCCURRENCE OF TUNNELING ACTIVITY, Patent Pending, 8/09/04

Eric Cole, James Conley, METHODOLOGY FOR CONFIGURING NETWORK FIREWALL, Patent Pending, 8/17/04

Eric Cole, James Conley, METHODOLOGY, SYSTEM AND COMPUTER READABLE MEDIUM FOR ANALYZING TARGET WEB-BASED APPLICATIONS, Patent Pending,

9/29/04

Eric Cole, METHODOLOGY, SYSTEM AND COMPUTER READABLE MEDIUM FOR DETECTING FILE ENCRYPTION, Patent Pending, 4/01/03

Eric Cole, METHODOLOGY, SYSTEM AND COMPUTER READABLE MEDIUM FOR RATING COMPUTER SYSTEM VULNERABILITIES, Patent Pending, 4/29/03

Eric Cole, METHODOLOGIES, SYSTEMS AND COMPUTER READABLE MEDIA FOR IDENTIFYING CANDIDATE RELAY NODES ON A NETWORK ARCHITECTURE, Patent Pending, 5/23/03

Eric Cole, METHODOLOGY, SYSTEM AND COMPUTER READABLE MEDIUM FOR DETECTING AN EXISTENCE OF HIDDEN DATA IN BITMAPPED IMAGE FILES, Patent Pending, 8/19/03

Eric Cole, METHODOLOGY, SYSTEM AND COMPUTER READABLE MEDIUM FOR DETECTING AN EXISTENCE OF HIDDEN DATA IN BMP FORMAT COLOR IMAGE FILES, Patent Pending, 11/03/03