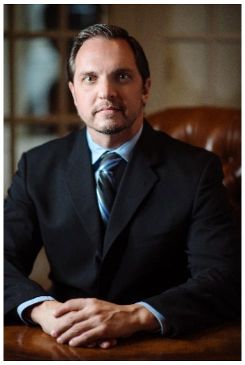
Dr. Eric B. Cole
Cyber Security Expert

43605 Edison Club Court
Ashburn, VA 20147
703-675-2055



A computer and cyber security expert with over 20 years of hands-on experience, Dr. Cole consults in information technology with a focus on information technology and cyber security. He is an invited speaker for and a member of many key organizations including the Commission on Cyber Security for the 44th President and the Purdue University Executive Advisory Board, and is a senior fellow with SANS. He is the author of several books and inducted into the InfoSec European Hall of Fame in 2014.

Professional Experience

Secure Anchor Consulting Services: 2005-Present
Consulting services to Fortune 500, Fortune 50, financial institutions, international organizations and the federal government. One assignment has included a major system design and assessment for an international financial institution in Hong Kong. Employs cutting edge technology and technical components (network security, network architecture, and incident response, NOC/SOC design) to provide security solutions. Serves as an expert witness for a variety of litigation involving government and commercial companies.

SANS (SysAdmin Audit Network Security): 1999-Present
Director of Research-Computer Network Attack-Enterprise Security Architecture
Director of the Cyber Defense Initiative
Lead instructor and course developer for several security courses, including the top selling courses. One of the highest rated instructors and one of the few instructors teaching a variety of courses. 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). Responsible for staying up on technology and developing new course material that teaches students the state of the art in networking, information technology, and security. Created and led several key efforts including the Levelone Notebook, top 10/20 vulnerability list and the Cyber defense initiative, including the author of the Critical Controls for Effective Cyber Defense. Developed business plans for and created new technological initiatives. Constantly researched, tested and evaluated new security products and research efforts.

STI (SANS Technology Institute): 1999-2015
Dean of Faculty
Member of a five-person team tasked with creating a degree granting institution and receiving certification from the state of Maryland. Offered two Master's degree programs focused on technical people needing managerial skills and managers needing technical skills. Designed and implemented curriculum and provided leadership to faculty to successful deliver the degrees. Successfully achieved accreditation.

McAfee: 2009-2010

SVP, CTO of the Americas

McAfee's visionary and evangelist responsible for strongly influencing the company's technical direction in alignment with the CEO, EVP, Product Operations and other key product executives and technologists across the world. Played an integral role in the company's strategic direction, development, and future growth as the global leader in digital security solutions. Key leader in the execution of technology strategy for technology platforms, partnerships, and external relationships. 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. Focused on identifying and capturing intellectual property and driving new innovation across the company.

Lockheed Martin: 2005-2009

IS&GS Chief Scientist

LM Senior Fellow

The Sytex Group, Inc. (TSGI) was acquired by Lockheed Martin with a key component being the intellectual property created under the CTO leadership. I was selected by Lockheed Martin into its prestigious fellowship program, an award it makes to less than 1% of its 130,000 employees. As a Lockheed Martin Senior Fellow (the first Fellow within Lockheed Martin's Information Technology Division), I was a frequently invited speaker at a variety of conferences and security events. As Lockheed Martin Chief Scientist, performed research and development to advance the state-of-the art in information systems security. Specialized in: secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. 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.

The Sytex Group, Inc. (TSGI): 2001-2005

Chief Technology Officer (CTO)

Positioned company to accomplish corporate growth and meet financial targets by utilizing and enhancing technology. Worked as an executive team member to determine and implement technical direction and focus of company. Extensive experience with running projects including managing development efforts to exceed client requirements. Successfully created an intellectual property base (to include patents, journals, books and white papers) – this effort resulted in an overall increase in market value. The efforts of the research team's intellectual property increased advertising, market share and customer satisfaction through conferences, proposal and magazine articles. Maintained full accountability for revenue of $55 million and indirectly involved in revenue of over $80 million. Provided continuous leadership to research team of over 20 people that created intellectual property that competed and surpassed teams 20 times their size. Yearly patents were in line with the top 1000 producing patent companies in the United States. Developed and executed on creative techniques for influxing technology into non-technical business units to drive revenue and profit. Interfaced with government officials, including the Pentagon, White House and Capitol Hill, and corporate executives to identify critical network security problems that needed to be addressed and researched.

GraceIC: 2000-2001

Chief Security Officer (CSO)

Designed and executed in establishing GraceIC as a leader in the network security arena. Developed the product line and executed on the expertise to build the services. Provided management and gave direction to successfully delivery on technical skills of security employees. Provided leadership and implemented the proper internal security infrastructure within Grace such as secure email, proper protection of data and security policies. Presented at several national and international conferences and wrote several articles. Performed and documented research into the area of future applications and solutions to the network security problem existing in the current market. Trained sales people, program managers and engineers on how to sell, manage and deliver security services. Maintained a pulse on technology in the market place to produce trending and markets plans.

American Institutes for Research: 1999-2000

Chief Information Officer (CIO)

Brought in to fix and revamp the entire IT infrastructure based on the organization having several security breaches, virus outbreaks and unreliable performance on the network. Within three months stabilized the entire IT infrastructure and within nine months rebuilt the entire infrastructure. Network designed to achieve a balance between functionality and security while minimizing the monetary impact to the organization. After one year, there were no severe security breaches and all attempted breaches were contained prior to causing any significant monetary loss. Virus problems were contained and controlled and network uptime was 99.999%. Security and performance were greatly increased while overall IT costs were reduced by 15%. In addition, provided technical support for DARPA sponsored research projects. Helped invent technology and innovation that lead to a spin off company, Pynapse, which created a state of the art intrusion detection system known as Checkmate that was later sold to SAIC.

Vista Information Technologies: 1998-1999

VP of Enterprise Security Services

Developed and executed the Enterprise Security Services Group and responsible for all internal and external security issues. Tracked and managed separate profit and loss center for security. Grew the team from one person to over 12 people and executed on several million in annual revenue in less than a year. Set up the security and other monitoring services for the NOC/SOC. Created all of the security services offerings and generated all necessary marketing and sales material. Followed and assured compliance with business plan and financial tracking of security group. Performed security assessments and consulted on all areas of security. Designed, implemented and monitored security solutions including firewall design, intrusion detection, vulnerability assessment and penetration testing. Performed evaluation and analysis of security tools and provided technical recommendations and product improvements for VC funded startups. Key presenter at Cisco sponsored security seminars around the country and performed partnership activities with Fortune 500 organizations.

Teligent: 1996-1998

Director of Security

Created and in charge of IT Corporate Security Department. Central point of contact for all security concerns. Evaluated strategic plans and operational activities by performing risk assessment and determining how it might impact corporate security.   Designed security solutions to meet operational needs. Integrated security and help create NOC to provide for proper monitoring of network. Developed the company's security policy and all required security guidelines across the company. Set up security lab to properly test and enhance the security features of the network. Performed and executed on several computer investigations. Assisted and advised the legal department on researching laws, regulations, and policies relating to computer and information security.   Evaluated several secure email solutions and installed PGP company-wide. Established and set up web traffic monitoring and password tracking systems.

Central Intelligence Agency: 1991-1996

Received Six Exceptional Performance Awards.

Program Manager / Technical Director for the Internet Program Team with Office of Technical Services

A Senior Officer of the agency that implemented the Internet Program Team that specializes in rapid development and in exploiting the latest Internet technologies that meet customer's requirements. The team designs, develops, tests, and deploys products in three to six month intervals. Designed and developed several secure communication systems. Responsible for providing technical direction, technical design, security assessment, and programming modules. Secured internal servers, continually perform intrusion detection, and reviewed audit logs. Performed independent security reviews and penetration testing of (World Wide Web) servers for other offices. Identified several weaknesses and devised ways to fix those problems and secure the system. Received letter of appreciation from the DCI (Director of Central Intelligence) and several Exceptional Performance Awards for this project.

Computer Engineer with Office of Security
Member of the information security assessment team. Evaluated and performed security assessment of network operating systems. Identified potential vulnerabilities and ways to secure the holes. Designed a large scale auditing system with automated review capability. Worked on several virus investigations.

Education

Doctorate degree (now PhD) in Network Security, Pace University - 2003

M.S., New York Institute of Technology - 1993
Major: Computer Science
GPA: 4.0/4.0
Honors: Harry Schure Graduate Memorial Award (awarded to one graduating senior)

B.S., New York Institute of Technology - 1992
Major: Computer Science
Minor: Business
GPA: 3.7/4.0
Honors: Graduated Magna Cum Laude, Dorothy Schure Memorial Award, Jules Singer Award, Grace Hopper Award from Computer Associates, Presidential Academic Award (4.0 all semesters), Presidential Service Award, Dean’s List, Member of Who’s Who Among Students in American Universities, and Member of Nu Ypsilon Tau Honor Society.

Certifications

CISSP (Certified Information Systems Security Professional)
Created several of the GIAC (Global Information Assurance Certification) programs and exams

Organizations / Memberships

ACM (Association for Computing Machinery)
IEEE (Institute of Electrical and Electronics Engineers)
CSI (Computer Security Institute)
ISSA (Information Systems Security Association)
ICSA (International Computer Security Association)
International Who’s Who in Information Technology
CVE (Common Vulnerability and Exposures) - member of the editorial board (by invitation only)
HoneyNet Project - member (by invitation only)
for SANS Institute - author and speaker

Publications

Books

Eric Cole. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization.* Syngress, 2012.

Eric Cole. *Network Security Bible.2nd Edition*, Wiley, 2009.

Eric Cole, Ronald L. Krutz, James Conley, Brian Reisman, Mitch Ruebush, Dieter Gollman, and Rachelle Reese. *Wiley Pathways Network Security Fundamentals Project Manual*. Wiley, 2007.

Eric Cole and Sandra Ring. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft.* Syngress, 2006.

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

Eric Cole. *Hackers Beware: The Ultimate Guide to Network Security*, New Riders/Sams Publishing, 2001.

Monthly Column on TechTarget - http://www.techtarget.com/contributor/Eric-Cole

- Supply chain security: Controlling third-party risks
- Cyberhunting: Why enterprises need to hunt for signs of compromise
- Six ways to improve endpoint device security
- Why security operations centers are the key to the future
- Offensive countermeasures: How they can slow down adversaries
- Accidental insider threats and four ways to prevent them

Selected White Papers - https://www.sans.org/reading-room/analysts-program

- Decision Criteria and Analysis for Hardware-Based Encryption
- Threat Hunting: Open Season on the Adversary
- Automating the Hunt for Hidden Threats

Selected Journal Publications

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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.