Simon Biles. FBCS CITP, CISSP, OPSA
Senior Digital Forensic Analyst
specialising in computers, networks and information security

Forensic Scientist since: 2002

Summary

Simon Biles is a highly experienced digital forensic analyst and information security specialist with over 20 years' experience in working with Microsoft, UNIX and assorted LAN, WAN and mobile networking products.

During the course of his career, Simon has obtained significant exposure to infrastructure and network architecture and holds technical skills and architectural expertise across a wide variety of technologies, including Cloud (IaaS, PaaS, SaaS), Virtualisation, E-commerce and Social Media.

Simon also has extensive experience of creating policy and procedure to support Information Management, including Disaster Recovery (DR), Business Continuity (BC), Security, Incident Response (IR) and Data Protection. He is also certified as a Lead Auditor on ISO 17799, the predecessor to ISO27001, with experience of implementing both standards.

Simon's experience and expertise have been utilised across both private and public institutions, including: Banking and finance, software and hardware development, national and international charities, criminal defence, central government and the NHS.

Experience

- Leading computer and digital forensic examiner.
- Leading forensic analyst in audit and fraud assessment and in loss prevention.
- Leading defence expert, having successfully analysed and reported on some of the most serious, high profile and complex multi-layered cases. These have included charges of possessing indecent images, fraud and terrorism.
- Simon's work includes: finding and retrieving material, copyright and intellectual property theft, breaches of acceptable use policies, data recovery (including the retrieval of deleted data such as email correspondence, address book contacts, calendar entries, internet history and dates and times of key events), user identification, hard drive and server imaging and the securing of volatile data.
- Vastly experienced across multiple Operating Systems (Windows, Linux, UNIX and MacOS), Virtualisation (VMWare) and Software (SQL, Oracle, Office, Encryption, Anti-Virus, etc.)
- Infrastructure architecture, security architecture and secure system design specialist, with technical expertise across a wide variety of technologies including Cloud (IaaS, PaaS, SaaS), Virtualisation, E-commerce and Social Media.
- Holds an in-depth knowledge of numerous information management and security standards and best practice guides, including HMG Information Security Standards (IAS1, IS2, JSP440, NHS, CESG Memos, etc.) and Risk Management Accreditation Document Sets (RMADS), ISO 27001, ISO/BS 17799, COBIT and Sarbanes-Oxley Standards.
- Highly experienced and respected e-mail, mobile (Blackberry, SmartPhones), satellite and telecommunications analyst and digital examiner.
- All Investigations are undertaken in strict compliance with the Association of Chief Police Officers

Areas of expertise

Digital forensics
Computer forensics
Information security
Infrastructure and network architecture
Mobile phone forensics and networking

(ACPO) guidelines for managing and evaluating digital evidence.
- Heavily involved in the research and development of new forensic tools and techniques.
- Highly accomplished risk, vulnerability and threat assessor.
- CISSP Certified (since 2004).
- Encryption expert – public key, certificates and secret/shared key, full disk encryption (FDE).
- Payment Card Industry (PCI) Data Security Standard (DSS) – audit and compliance expert.
- Highly respected policy and procedure development consultant for global organisations.
- Teacher and mentor at a postgraduate level: Visiting Lecturer at De Montfort University Cyber Security Centre in Network Forensics and Alternative Operating Systems.
- Experienced and qualified trainer in all aspects of digital forensics and information security including: forensic awareness, security awareness, first responder and incident response, security assurance and linux security.

Committee memberships

- Certified as a Lead Auditor for ISO 17799.

Notable work

- Author of a number of key publications including:
- Building Security and Directory Solutions for UNIX Using the Windows Server 2003.
- Active Directory Kerberos and LDAP Services - Microsoft, January 2004.
- UNIX and Microsoft Single Sign-on. - SysAdmin Magazine, September 2004.
- Migrating UNIX Daemons to .Net Services using Visual C++ - Microsoft, March 2004.
- Several Lessons in the "Hacker High School" Series from ISECOM.
- Snort Cookbook - O'Reilly UK, 2005. ISBN: 0596007914.
- Hacking Exposed - Linux 3rd Edition, Osborne/McGraw-Hill, U.S., ISBN: 0072262575
- Technical Reviewer for Computer Security Basics, 2nd Edition, O'Reilly.
- Internet Forensics, Robert Jones, O'Reilly.
- Regular columnist on Information Security for Forensic Focus.

Recommendations

"Simon's advice, guidance and knowledge proved invaluable in a complex computer/cyber fraud case. Due to Simon's expert report, we were able to break the bat of the prosecution's case and as a result, avoided the risk of trial. Simon broke down the technical jargon into plain English which was of great assistance to us, our client and indeed the Judge.

Forensic Equity are always available to assist at short notice and always provide a prompt response to queries. Their professional, knowledgeable and courteous staff are efficient, effective and reliable and we have no hesitation in recommending both Simon and Forensic Equity to others."
Solicitor, Stuart Miller Solicitors

"Can I pass our thanks to you for your incredibly helpful and efficient work over the past few months. It has made an appreciable difference to the evidence as it stands at the end of the case."
Barrister, Matrix Chambers