

SUMMARY

- Wide-ranging experience in network and information security, including intrusion detection, digital forensics, incident response, vulnerability assessment, management policy review, and system hardening.
 - Private Investigation License from Texas Private Security Board.
 - Experienced with Guidance Encase Forensic Edition, Sleuthkit, Forensic Toolkit, Solaris, Linux, OpenBSD, and general TCP/IP networking. Also experienced with other network security tools such as nmap, Nessus, Nikto, Snort, tcpdump, Wireshark, WebInspect, AppScan, and many others.
 - Trained in EnCase, SilentRunner, Solaris, Autopsy/Sleuthkit, Checkpoint Firewall-1, and ISS SiteProtector.
 - Fluent in conversational and professional Spanish, both spoken and written.
 - Educated in statistics and applied mathematics.
 - Excellent analytical and troubleshooting skills.
-

EXPERIENCE

Digital Discovery Corporation

Dallas, TX (June 2008 - May 2009)

Senior Security Analyst

Respond to client security incidents and perform full lifecycle investigation, including initial quarantine, incident management, law enforcement coordination, forensic analysis, and recommendations / "lessons learned". Assess client networks & systems proactively and create detailed risk profiles for executive review. Research new forensic techniques for cutting-edge technical investigations. Collect and deliver data for e-discovery projects.

Enterprise Controls Consulting

Irving, TX (June 2007 - Feb 2008)

Senior Consultant

Performed management Sarbanes-Oxley (SOX) reviews of IT General Computer Controls, including security and systems management, regulatory compliance, and policies & procedures. Clients included Hallmark Financial Services and Regency Gas Services.

Crypto Security Systems

Fort Worth, TX (Mar 2007 - May 2008)

Chief Investigator

Investigated misconduct and network intrusions for clients in a confidential capacity. Assessed IT security posture of external organizations and provided documentation and recommendations in cooperation with their audit and IT departments.

Horn Murdock Cole

Dallas, TX (Nov 2005 - Feb 2007)

Senior IT Security Consultant

Assessed vulnerability and perform penetration tests for external and internal networks across multiple clients. Assessments included testing of databases, Windows and Unix servers, virtual private network devices, web servers and applications, and wireless networks. Performed management Sarbanes-Oxley (SOX) reviews of IT general controls, including security and systems management, regulatory compliance, and policies & procedures. Provided security consultation services regarding database security, encryption controls, investigation procedures, regulatory compliance, account management, and intrusion detection. Clients included financial institutions, retail companies, energy providers, and consulting and manufacturing firms.

Verizon

Irving, TX (Aug 1999 - Nov 2005)

Enterprise Security Architect (Jan 2002 - Nov 2005)

Designed and implement international intrusion detection and vulnerability assessment deployments for Global Security Operations Center using ISS RealSecure SiteProtector (Canada, Puerto Rico, Dominican Republic, Costa Rica, Mexico, Venezuela, Thailand, and United States). Tested security of international affiliate networks via regular vulnerability assessments and ad hoc penetration tests. Performed internal network and system forensics investigations for network intrusions and employee misconduct as required using Encase, Sleuthkit, and other relevant tools. As interim manager (8 months), managed team of 6-9 technical staff responsible for vulnerability assessment & management, incident response, threat intelligence, and infrastructure management at the Global

Security Operations Center. Wrote substantial portions of Verizon hardening guidelines for Solaris and Linux and evaluated overall information security policies and practices. Designed business processes and technical architecture for new managed firewall service. Oversaw internal web application development based on Linux, Apache, MySQL, and Perl, including case and vulnerability tracking.

Senior System Administrator (Sep 2000 – Jan 2002)

Part of system administration team responsible for administering over 60 production systems for SuperPages.com, one of the twenty most-trafficked websites in 2000 and 2001. Lead engineer for security and Sun Solaris migration. Deployed site security initiatives including firewalls, intrusion detection, centralized logging, regular vulnerability scanning, and system hardening. Redesigned Internet gateway architecture to enhance security and eliminate single points of failure. Performed capacity planning (including storage, bandwidth, and CPU/memory resources). Deployed Storage Area Network (SAN) involving over 7 TB of storage. Validated internationalization of SuperPages.com for Costa Rica, Dominican Republic, and Puerto Rico.

Advisory Systems Engineer (Aug 1999 – Aug 2000)

Part of four-person team responsible for administering over 80 firewalls enterprise-wide, primarily Checkpoint Firewall-1 on Solaris. Administered an additional 10 proxy servers, primarily Interlock on Solaris. Provided security expertise during enterprise network planning. Performed security audit and SLA negotiation with Mexico data center (reviewing both procedural and architectural problems related to network security). Provided technical assistance and analysis during security investigations.

CS Wireless/The Beam

Plano, TX (Oct 1997 – May 1999)

Coordinator, Residential Internet Services (June 1998 – June 1999)

Coordinated customer-site activity for a wireless broadband ISP. Supervised installation technicians. Maintained network diagrams for internal, DMZ, and customer-serving networks. Various Unix system administrator responsibilities, focusing on customer and user support. Member of incident response team for external intrusion investigations.

Telecommunications Engineering Analyst (Oct 1997 – June 1998)

Prepared FCC engineering applications for nationwide network of MMDS/ITFS microwave systems. Coordinated efforts to map signal levels across the Dallas/Ft. Worth metroplex. Managed local desktops, including antivirus, user support, and user security privilege management.

TSSI

Dallas, TX (Nov 1995 – Oct 1997)

Programmer/Analyst

Maintenance programming for Substitute Teacher Management System (IVR). Wrote and maintained code including DB management, reporting, administration. Ported software from C/C++ in a DOS environment using Btrieve to Windows NT using Delphi and C++Builder. Worked part-time to support self in college.

CERTIFICATIONS AND MEMBERSHIPS

- Licensed Private Investigator (TX License #A13523)
- Certified Information Systems Security Professional (CISSP #99385)
- Certified Information Systems Auditor (CISA documentation pending)
Passed December 2006 exam with score of 87
- Associate Member of ACFE (Association of Certified Fraud Examiners)

EDUCATION

University of Texas at Dallas - B.S. Mathematics (August 2004)

Coursework included Computer Architecture & Design, Mathematical Statistics, Stochastic Methods, Linear Algebra, Computer Organization (assembly language), Partial Differential Equations, and Data Analysis for Statisticians and Actuaries.