RONALD A. DILLEY

http://www.uberadmin.com ● Simi Valley, CA 93065 ● ron.dilley@uberadmin.com

Certifications & Training

CISSP, 2003
GCIH, 2004
GCFA, 2005

Key Skills

Organization & Staff Development

Network & System Security

Risk Management

Vulnerability Assessments

Network & Computer Forensics

System Monitoring

Policy & Regulatory Compliance

Programming

Malware Analysis

Incident Response

Education

California Lutheran University, CA

Computer Science

INFORMATION SECURITY ARCHITECT

Certified Expert in Enterprise Information Security

Information security practitioner whose qualifications include CISSP and advanced training and experience in incident handling and forensic analysis; and detailed knowledge of security tools, technologies and best practices. More than 20 years of experience in the creation and deployment of solutions protecting networks, systems and information assets for diverse companies and organizations.

Technology Summary

Security Technologies:	FoundScan; Qualys; Nessus; WebInspect; EnCase; TCT; Memoryze; IDS/IPS (ISS, SourceFire, Palo Alto, TippingPoint)
Systems:	Unix-Based Systems (Solaris, Linux, BSD); Windows (all)
Networking:	TCP/IP; LANs; WANs; VPNs; Routers; Firewalls (Cisco, Netscreen/Juniper, Palo Alto, Checkpoint)
Languages & Software:	Shell Scripts (sh, csh, ksh, bash); Perl; C; C++; x86 Assembler; Python; IDA Pro; Olly Debug; MS Office

IT Experience

WARNER BROS., Burbank, CA	**Exec. Dir. Information Security,** 2008-Present
AMGEN INC., Thousand Oaks, CA	**Director Information Security,** 1999-2008
APPLIED DIGITAL ACCESS, San Diego, CA	**Sr. UNIX Network Administrator,** 1997-1999
AIRTOUCH CELLULAR, San Diego, CA	**Sr. UNIX Administrator,** 1996-1997

Became an expert in information systems security over multiple years of dedicated study and application of skills protecting enterprise environments. *Notable Highlights:*

- **Architecture & Engineering:** Currently directing the information security portion of all system implementations. Devised enterprise security strategies safeguarding information assets and ensuring compliance with regulatory mandates.
- **Incident Response:** Built several security incident response programs and teams. Led all major incident response activities for several large corporations.
- **Policy and Awareness:** Modernized outdated information security policy and built enterprise class awareness programs for large corporations, and led companywide training on crucial new infosec policies, procedures and technologies.
- **Infrastructure:** Led comprehensive security infrastructure upgrades (e.g., firewall/VPN upgrades, intrusion detection, logging and vulnerability management) for large companies.
- **Risk Management:** Protected vulnerable networks following detailed risk assessments. Guided cross-functional teams in the design, validation, acceptance testing and implementation of secure systems and applications.