

Dan Davis

dandavis@dandavis.com

5328 Albright Drive, Virginia Beach, VA 23464

(757) 271-8193

Summary

Computer/Network/Security Engineer with over 8 years of experience working in demanding operations environments offering extensive web application and tool design experience with a strong foundation of networking and security expertise.

Work Experience

AT&T Chief Security Office

Managed Security Services Development

Security Engineer

June 2008 – Present

Responsible for design, development, documentation and training for AT&T Managed Security Services. Serve as Subject Matter Expert for Cisco Firewall Services Modules on the AT&T CSO MSS Development team. Provide tier 4 support and guidance to MSS Operations team.

AT&T Managed Security Services

MSS Security Operations Center

Security Manager (Tier 3) & Team Lead

Durham, NC

August 2004 – June 2008

As Security Manager: Provide tier 3 support to junior associates of the MSS Operations team. Provide mentoring and training to junior and senior associates to ensure optimum efficiency when dealing with diverse customer base.

- Serve as Subject Matter Expert on a number of technologies utilized within MSS operations including:
 - Lucent Brick firewalls
 - Cisco Firewall Service Modules
 - Cisco Network Analysis Modules
 - McAfee ePolicy Orchestrator
 - McAfee Secure Content Management/Secure Internet Gateway appliances
- Operate as lead Security Manager on a number of standard and custom offers supported by MSS including large government and private sector contracts
- Well versed on numerous technologies while in a supporting role as a member of the Security Manager team. Technologies include:
 - CheckPoint Firewall-1 operating on Nokia and Sun Solaris platforms both in stand alone and high-availability configurations
 - CheckPoint Provider-1 operating on Sun Solaris platforms
 - Cisco PIX/ASA firewall appliances
 - Cisco Routers/Switches of various models (25xx and 26xx series routers; 29xx, 35xx, 6509, and 7613 series switches)
 - Cisco 3000 series VPN concentrators
 - iPolicy Enforcer network-based firewalls
 - Juniper/Netscreen firewall products

As Team Lead: Provide leadership to systems administration team supporting MSS operations platform and

infrastructure devices. Develop web, command-line, and Windows-based applications and tools to support and empower MSS operations.

- Manage a number of critical server platforms (running Red Hat Enterprise Linux, Microsoft Windows Server 2003, and Sun Solaris) that support daily MSS operations.
 - MediaWiki server running on Linux with Apache, MySQL, and PHP
 - Created custom authentication plugin for MediaWiki software to interface with AT&T corporate single sign on infrastructure allowing for seamless integration with existing tools and services
 - Multiple Windows Server 2003 terminal servers that support virtual office and teleworker user base
 - Various internal and offer specific servers operating on RHEL and Sun Solaris
- Creation and ongoing maintenance of complex web-based applications used by MSS operations personnel to support daily operations. Technologies utilized:
 - Apache
 - PHP
 - MySQL
 - Smarty Template engine for PHP
- Creation and ongoing maintenance of numerous command-line tools and utilities to assist MSS operations personnel including auto-login scripts, custom wrappers for existing tools, etc

Misys Healthcare Systems

Application Developer

Raleigh, NC

December 2004 – June 2005

- Develop, deploy, and maintain a managed network and host monitoring solution. Development, testing, and installation of specialized tools, scripts, and software plug-ins required for proper monitoring and maintenance of client devices such as AIX and Windows 2000 servers. Technologies utilized:
 - Nagios
 - MRTG
 - Nessus
 - Red Hat Linux servers
- Develop and maintain a database driven client configuration database. Script development for exporting client configuration from the database and deploying the resulting configuration files to various network devices.

Durham County Government

Network Security Engineer

Durham, NC

February 2004 – August 2004

- Plan, design, implement and manage network and host monitoring system built upon the Nagios and MRTG network monitoring tools.
- Implement and secure wireless network segments in order to provide secure, high-speed connectivity to remote offices within the county using Cisco Aironet access points and Cisco PIX firewalls.
- Install and maintain CryptoCard authentication server to provide secure authentication services to routers, switches and servers via RADIUS.
- Create configurations to meet security parameters for operating systems and network devices including the development and installation of secure IOS templates for network infrastructure devices consisting of 2500, 2900, 3600, and 6500 class routers and switches.
- Implement and maintain a centralized syslog system to collect and consolidate logs from network

infrastructure devices and servers.

- Plan, design, implement and manage networking solutions for Microsoft, UNIX, and Linux systems on Nokia, Sun, and Intel platforms and Cisco internetworking.
- Design, implement and manage network security architecture including Check Point and PIX firewalls, multiple virtual private networking gateways, authentication servers, and network infrastructure components.
- Microsoft systems engineering including Exchange, IIS, SMS, SQL, and proxy server.
- Provide technical support and training to network technicians and server administrators.
- Provide information to and assist with full documentation development and updates to network security practices and procedures.
- Assess different Voice-over-IP technologies and providers for viability on the county's network. Work with Cisco engineers to define requirements and develop a implementation plan to transition the county's 1900+ phones to Cisco VoIP equipment.

Cable & Wireless USA

Network Security Engineer

Cary, NC

January 2000 – February 2004

- Install and maintain corporate and customer firewalls running Check Point FireWall-1 on both Sun Sparc and Nokia based systems.
- Install and administer Solaris-based servers in support of the Firewall and Security groups.
- Install and administer Apache web servers and MySQL database servers.
- Develop and maintain a customer information database using a MySQL database server and Perl scripts accessible via web.
- Install and administer a Nessus scan server.
- Develop and maintain a MySQL database to store Nessus scan information and results. Create Perl scripts to control Nessus scans and to parse the XML results and store them in the MySQL database.

Mobile and Portable Radio Research Group/Virginia Tech

Lead Systems Administrator

Blacksburg, VA

August 1998 – December 1999

Serve as the lead systems administrator for a research group made up of 20 faculty/staff and 50 Ph.D./M.S. students. The systems administration team is comprised entirely of 2 - 6 part-time student employees.

- Administer a heterogeneous network of PC and Sun workstations.
- Maintain a Windows NT server which serves as the group's primary domain controller, file server, web server running IIS.
- Maintain a large customer database in Access.
- Develop and maintain an Access database containing information of student papers. Develop a PHP-based web interface to allow searching by keywords, dates, and/or authors.

Additional Skills and Technologies

- Bluecat Meridius Spam filter
- DNS using Bind and DJBDNS
- F5 Networks FirePass SSL VPN
- General VPN Design and Implementation

- Network Security and Analysis Tools and Protocols [Ethereal/Wireshark, Nmap, Tcpdump]
- Nortel Contivity Extranet Switches
- Programming and Scripting Languages [Expect, JavaScript, PHP, Perl, Shell (bash, csh, ksh)]
- Qmail

Education

Strayer University

Virginia Beach, VA

Master of Science, Information Systems, Computer Security Management

Anticipated graduation Summer 2010

Current GPA 4.0

Virginia Polytechnic Institute and State University

Blacksburg, VA

Bachelor of Science, Computer Engineering

December 1999