



Craig Kirby
GCIH, GCED, GCWN, CISSP, MCSA, Security+, Network+
resume-craigkirby@snkmail.com

Craig Kirby

OBJECTIVE

To gain a position as a Senior System or Security Architect that lets me utilize my seventeen years of experience in security, programming and Windows and Linux platform knowledge.

CERTIFICATIONS

- **GIAC:** Incident Handling Analyst (GCIH Gold), Enterprise Defender (GCED), Windows Security Administrator (GCWN)
- **(ISC)2:** CISSP
- **Microsoft**: MCSA
- **CompTIA:** Security+, Network+, A+

PATENTS

- Dynamic Employee Security Risk Scoring (US Patent Application 20110167011) - Filed January 4, 2010
- Login Initiated Scanning Of Computing Devices (US Patent 8,590,046) - Issued November 19, 2013

SKILLS

- **Operating Systems:** Windows, DOS, Linux, iOS, Android
- **Microsoft Technologies:** Active Directory, SCCM, Exchange, SQL, WDS/MDT, Group Policies
- **Virtualization:** VMware ESX/Workstation, Hyper-V, P2V migrations
- **Security:** Splunk, Nessus, SEP, ePO, Snort, Foundstone, Wireshark, EnCase, Retina, Websense, Vericept, Nmap, ChangeAuditor, Tripwire
- **Programming:** Perl, VBScript, DOS Batch, PowerShell, Java, Objective-C, Python, VB, C++, Pascal, KiXtart
- **Web:** PHP, JavaScript, XML, CGI, DHTML, CSS, AJAX, HTML, Flash, ASP.Net
- **Software Packaging:** Wise, InstallShield, NSIS, Inno
- **Full Disk Encryption:** Credant, PGP, Bitlocker
- **Mobile Device Management:** MaaS360, AirWatch, MobileIron, Zenprise, Good
- **File Sharing:** WatchDox, Accellion, ShareFile
- **DLP:** Symantec, Websense, RSA

EXPERIENCE

Oaktree Capital Management — Los Angeles, CA — Jan 2010 - Present

- **Position: VP, IT Security Officer**

Primary responsibility is to govern and enforce the IT Security Controls. Secondary, mature the security posture.

- Established the Acceptable Use Policy and got sign off for every employee and contractor.
- Established the security patch rating system based on risk to the environment.
- Established the enterprise standard desktop, laptop and server images using MDT on WDS.
- Established the centralized logging server for security events in preparation for a SIEM. All network devices, domain controllers and security applications send their logs to this collection server.
- Pushed out security patches to all servers, workstations and laptops in the enterprise for a year before handing it back to the infrastructure team.
- Revamped the antivirus infrastructure, technical controls and established anti-malware policies.
- Created numerous programs to automate the installation of administrative tools and management agents throughout the enterprise.
- Created and implemented all essential technical security controls for endpoint and servers via GPOs.
- Created a new logon script to consolidate 42 scripts down to one; along with a 25x speed improvement.
- Fixed many long and outstanding problems in the Enterprise that were dismissed as unsolvable years ago.
- Managed the penetration testing and vulnerability assessment programs.

- Generated and reviewed SOX reports on a daily basis.
- Evaluated multiple Security Awareness videos and made selection for our Security Awareness Training program.
- PoC top Disk Encryption software (Credant, PGP, Bitlocker) and selection of a product.
- PoC top SIEM products (ArcSight, Splunk, Q1 Labs, Symantec, RSA EnVision) and selection of a product.
- PoC top DLP products (Symantec, RSA, WebSense) and selection of a product.
- PoC top MDM products (MaaS360, AirWatch, MobileIron, Zenprise, Good) and selection of a product.
- PoC top File Sharing products (WatchDox, Accellion, ShareFile, Credant) and selection of a product.

Bank of America/Countrywide Simi Valley, CA Aug 2005 - Jan 2010

- **Position: AVP, Senior Security Engineer**

Primary responsibility is to govern and enforce the IT Security Policy. Secondary, is to develop security tools that help security and IT engineers do their jobs faster and more efficiently by automating redundant tasks through scripting and automation. Tertiary, collect and trend data elements for security compliance purposes.

- Created a portal page in ASP.Net, AJAX and SRS for SOC to be the SOC engineers and users interface for SOC software. The portal includes a very extensive risk rating system. For this project I was awarded US Patent #20110167011.
- Created Countrywide's second version internal compliance scanning engine from scratch. Scans ranges of IP addresses and interrogates target machine for compliance information such as installed patches for the operating system and any installed application by way of file existence, file version, or registry values. Reports results back into a backend database. For this project I was awarded US Patent #20120030757.
- Created an executable Perl script that VPN users would run to interrogate their machines for compliance items such as desktop agents, patches, and unapproved software and have results automatically sent back in via SMTP. This saved our security engineers a lot of time as the old system required the user to take screenshots and phone calls into our SOC.
- Set up several VMWare servers for Development environments
- Wrote small programs and scripts as the "glue" between our departments and other departments main applications.
- Created universal parsing script in Perl that would parse out several vulnerability scanners output and stores them into a backend database.
- Wrote several smaller scripts to help other business units and Active Directory architects. These scripts fixed the following: corrupted SPNs, corrupted user objects properties in AD, migration of workstation objects from NT to AD, remote detection and installation of desktop agents (BigFix, Radia, McAfee, etc)
- Completed many application security reviews and vulnerability assessments

- **Position: AVP, Infrastructure Manager**

Primary responsibility is to manage a team of technicians and oversee the infrastructure, servers and workstations, for the Countrywide Capital Markets division.

- Created from scratch a new CCM's image build and rollout infrastructure. Cutting down the time it took from 4 hours to 1 hour. Also allowed CCM to standardize on one image build for workstations.
- Managed eight techs that worked with end-users on application installs, workstation issues, and new-hires.
- Wrote software installation packages and coordinated application rollouts to workstations.
- Managed CCM's OU in Countrywide's Active Directory implementation.
- Helped build out servers with my two server technicians.

Trust Company of the West Los Angeles, CA Dec 2003 - Jul 2005

- **Position: Windows Engineer**

Primary responsibility is complete 24/7 break/fix server coverage including server commissioning and decommissioning. Secondary, is to write automation scripts and security reviews of architecture and security suggestions.

- Wrote a Perl script to screen scrape all health information from managed APC UPS devices and store them into a SQL database.
- Created a software distribution Perl script for remote users to get Microsoft Security patches efficiently.
- Active Directory (2k & 2k3) administrator
- SMS (2.0 & 2k3) administrator
- Reviewed current security architecture and suggested many improvements and suggestions.
- Wrote many Perl and VBScripts to automate backend processes and monitoring of servers.
- Maintained and built several Citrix farms
- Maintained and built several Windows 2k & 2k3 clusters

Farmers Insurance Group Los Angeles, CA Jan 2000 - Sept 2003

- **Position: Security Engineer**

Primary responsibility was to respond to any incident, handle investigations and send out virus/vulnerability alerts to administrators and managers. Also assisted in security reviews and risk assessments of ongoing business projects.

- While at Farmer Insurance I single-handedly stopped the spread of CodeRed, Nimda, Blaster, Nachi/Welchia worms on their enterprise network.
- Wrote my own software distribution tool to distribute security patches since Tivoli was only deployed to 15% of the environment.
- Worked on many investigations into internal employees, hackers and incidents. In just one year, over 45 investigations completed with 100% successful completion rate. In several cases damages were collected.
- Established Farmers' first Security Operations Center (SOC).
- Established first centralized logging server where firewalls, VPN servers and Windows NT/2000 server would send their logs for review. Instant pages would be sent out when a trigger was tripped such as brute-force password attempts or employees I was investigation via VPN.
- Wrote IIS Security hardening document used on all DMZ and Intranet IIS servers.
- Wrote Windows 2000 Security hardening document used in all the corporate Ghost images.
- Wrote Farmers' Incident Handling procedural document and helped in writing and streamlining security procedures.

- **Position: Software Distribution Engineer**

My main responsibility was to distribute new versions of the CRN's Siebel and FileNet client to all of the Farmers' Claim Agents.

- Established and stabilized a standard to distribute software at Farmers Insurance. Wrote procedures for the two co-workers based on best practices to build and package software.
- Migrated from NetInstall to Tivoli and to use Wise Installation System to installation packages. This included evaluating SMS, Rumba, Novadigm's Radia, InstallShield for distribution and packaging methods.
- Pushed CRN's client application to over 2000 users, a first for Farmers Insurance.
- Pushed Norton Antivirus clients to 16,000+ users, a first for Farmers Insurance, during the Nimda outbreak because many clients did not have NAV installed or working.

- **Position: Windows Engineer**

Installed, built and maintained all Windows NT/2000 servers in Oklahoma City. Also co-maintained Los Angeles based servers with the LA teams.

- Maintained 600+ Windows NT/2000/2003 servers. 25 of which were NT/2000 Clusters. This includes over 30 DMZ servers which hosted several Internet only services like corporate webpages.
- Setup and maintained Norton Antivirus Corporate Edition v7.0 thru v8.0 in the whole environment.
- Installed and maintained 20+ Citrix MetaFrame servers.
- Wrote the CRN Disaster Recovery scripts to automatically fail over CRN NT servers to LA.
- Wrote and maintained KiXtart logon scripts for corporate wide use. Before my one KiXtart logon script there were hundreds of individual logon scripts that caused headaches to manage.
- Created standard Ghost Image used on every computer throughout Farmers.
- Maintained eight Domino v5.0 servers in OKC and a user base of 16,000 users throughout the enterprise.
- Wrote a Notes Client Automatic Configuration database used corporate wide to configure all Lotus Notes clients.

Entex/Phillips Petroleum Bartlesville, OK Jul 1997 - Dec 1999

- **Position: Desktop Administrator**

EDUCATION/PROTORING

- Bachelor's Degree in Business Information Technology: Software Development and Multimedia
  Rogers State University, Claremore, Oklahoma
  Distinguished Graduate Award
- GIAC Advisory Board member
- Proctor classes for the SANS Institute with *GCIH Track 4: Hacker Techniques, Exploits and Incident Handling*