Ian Macdonald

Email web@jobs.imacdonald.co.uk

Introduction

My name is Ian Macdonald. I graduated from University of Edinburgh with a Bsc (honours) in Computer Science. I have worked in the IT field for most of my career, specializing in computer security for the first 10 years. I have refined my IT Security skills in over the years, managing a team of Security Engineers at Constellation Energy, performing incident response and forensics for Time Warner AOL, deploying complex security Systems that covered multiple counties at multiple companies. Most recently I have been a Systems Architect building complex Linux and Windows based systems for a SaaS deployment. As part of my work I created an information security program, successfully obtained PCI DSS level 1 certification and built out multiple highly available data centers, utilizing NAS, SAN, Fibre Channel, VMware, Dell/HP Blade Centers, F5 and Netscaler Load Balancers.

New areas of interest for me include Platform as a Service, Mobile Security and the growing DevOPS movement and how to securely deploy tools like Puppet and Chef.

I am always looking for the next challenge or opportunity to take my career or skills to the next level.

Skills & Tools

- Managing IT Projects, DSS PCI Level 1 Compliances, Strong trouble shooting skills, Designing highly available data centers.
- Dell Servers and Blade enclosures, F5 Load Balancers, Netscaler Load Balancers, Netapp, Cisco Firewalls, Cisco Switches, Cisco Routers, Dell Switch, Juniper Switches
- Microsoft Server 2012, 2003, Red Hat, Centos, Ubuntu, Apple OS X.
- Capistrano, Chef, Jenkins, Splunk, Kickstart. PXE Boot, Nagios
- Security Engineering and deployment, Penetration testing, Virus discovery and remediation, Vulnerability Assessments, Data modelling and Data Integration, Incident Response.
- Snort, Nmap, Nessus, Tcpdump, ModSecurity, Tenable, Wikid, OpenVPN
- Cyrus, Postfix, Bind, Apache, Active Directory, VMWare, KVM, MS SQL Server tuning and administration, and Mysql tuning and administration, Jira.
- TCP/IP, SMTP, HTTP, DNS, and other protocols analysis.
- C, C++, Perl, Unix shell scripting, ML, Ruby, Java.

Experience

- 14 years of computer and network security experience.
- 16 years experience administrating Linux and other flavours of Unix.
- 16 years experience administrating Windows Servers.
- Over 5 years of database/data modelling and data analysis experience.

Current Employeer ***DevOPS Lead*** ***Aug 2013 to present***

- Automated Windows and Linux based build processes using Jenkins
- Manage and release builds to Development and Quality Assurance.
- Building out Lab test environments for support services like Active Directory and Open LDAP.
- Migrated multiple projects from PVCS to Git.
- Built out Lab environment using Amazon VPC EC2 instances with a combination of Windows Servers 2012, Ubuntu LTS, Riak and Riak CS and Chef.

Angel.com/Genesys ***Sr. Systems and Security Architect*** ***Nov 2008 to Aug 2013***

- Architected and deployed a new customer solution at Angel.com using technology from a company Genesys had recently acquired. The solution performed speech analytics on 8-14,000

call recordings a day using windows 2012, clustered MS SQL, and combination of SAN and NAS storage.
- Architected new network layout to aid in future rapid deployment and automation.
- Responsible coordinating the deployment of 6 new Blade Enclosures and upgrading the firmware and the other 12 blade closures.
- Responsible for migrating and retiring old legacy servers in the datacentres.
- Responsible for coordinating purchase and deployment of new VMware infrastructure for Test and Production and upgrading existing infrastructure.
- Responsible for creation of new DMZ VMware infrastructure.
- Responsible for Production IT Security, including obtaining PCI Level 1 certification.
- Joint responsibility for 24x7 uptime
- Architected switch from Jboss on Windows to Jboss on Linux, including creating rpm packages for application deployment.
- Implemented single sign on for Windows, Linux, and Apache web services.
- Deployed updated IDS and Antivirus to the Production Environment.
- Deployed application firewall for protecting against cross site scripting and sql injection attacks.
- Deployed internal certificate authority.
- Researched and selected outsourced vendors to conduct network and application security penetration testing.
- Architected and deployed new log management and monitoring system using Splunk.
- Maintained and expanded Nagios monitoring solution.
- Architected and deployed Linux and Windows patch management solution.
- Standardized production platform on Centos/Redhat Enterprise linux.
- Tested and Deployed VMware for QE and Production environment.
- Created Linux system configuration and deployment system using Capistrano.
- Created taught Security Awareness and PCI compliance classes.
- Tested and deployed Vulnerability Management System.
- Tested and deployed Two Factor Authentication system for critical systems.
- Tested and deployed new VPN solution for Production and developement data centers.
- Planned and deployed a remote data center which included blade enclosures, firewalls, switches, NAS storage, SAN storage and VOIP telecom equipment.

Ajilon/The World Bank ***Technical Security Analyst*** ***March 2008 to October 2008***

- Responsible for developing and deploying an Internet security filtering solution to protect all computers at The World Bank.
- Reviewed and performed performance tuning of the Bank's McAfee EPO and VirusScan Enterprise implementation.
- Deployed a Nagios monitoring solution for Security Servers.
- Created a logging server based on Sawmill.

AOL LLC ***Technical Security Engineer*** ***April 2006 to March 2008***

- Updated Perl based IDS reporting tool.
- Helped develop information security training courses.
- Performed a complete rebuild of the IDS monitoring solution covering multiple countries.
- Performed security design reviews and host assessments for multiple projects
- Member of the Computer Emergency Response Program, responsible for handling and coordinating computer incidents across all of Time Warner.
- Performed malware analysis and mitigation.
- Responsible for presenting a biweekly training course to new hires on computer security awareness.
- Integrated IDS reporting into Enterprise Security Management (ESM) system

Constellation Energy Group IT Security Engineering Team Lead November 2004 to April 2006

- Managed the IT Security Engineering Group. Responsible for weekly team meetings, weekly status reports to upper management, Project Scheduling, task prioritization and workload management within the group.
- Consulted on IT Security related issues in IT projects.
- Technical lead and coordinator of incident response for virus and other security incidents.
- Presented "BindView Control's place in a Security Organization" at the 2005 BindView Insight User Conference in Houston Texas to over a 100 people.
- Responsible for maintenance and upgrading the IDS infrastructure that monitors 15,000+ workstations and servers.
- Created IDS signatures for tracking Viruses and other Security events.
- Created team SharePoint site for tracking group tasks and engineering procedures.
- Created a web front end for displaying information generated by BindView Control.
- Coordinated testing and deployment of virus software upgrade to 12,000 machines.
- Responsible for coordinating and supporting internal IT Security systems, projects and associated budget.
- Conducted a bake off between 4 enterprise vulnerability assessment tools. Looked at quality of scan, the quality of reporting, costs and how it would fit into existing procedures and processes.

Constellation Energy Group IT Security Analyst March 2002 to November 2004

- Designed, built, and monitored a multi sensor Intrusion Detection System that covering multiple security zones and multiple subsidiaries.
- Deployed an IDS web front end that was written by myself and extended it to include virus data from our centralized virus protection solution.
- Performed network security audits.
- Performed forensic analysis of machines that were suspected of being compromised.
- Created an automated system for emailing out security alerts and reports.
- Developed an 802.11 secure wireless solution.
- Implemented a web content monitoring and blocking solution.
- Maintained and performed analysis of syslog data supplied by firewalls and other devices.
- Deployed a centralized virus protection solution to 12,000 desktops and servers.

Education

Cisco
Cisco Certified Network Associate, CCNA (lapsed).

Managing IT Projects
Week long course developed by George Washington University and ESI International.

Shmoocon, Washington DC 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014
Attended three day conference on Computer Security

Institute for Applied Network Security, DC Forum 2007
Attended two-day forum and presented on the topic of Windows Mobile security vs Rim Blackberry Security.

Black Hat Briefing, Las Vegas 2000, 2003, 2012
Attended the security conference plus the Defcon convention that followed.

Microstrategy Technical Training
Technical boot camp,
Microstrategy Broadcaster,
Quality Engineering and testing.

Teradata
NCR Unix System Administration.

Edinburgh University, Scotland,
4 Year BSc (Hons) Computer Science, 1993-97

Other Activities and Interests

Personal Projects
My home network consists of machines running Linux, Windows XP and OSX. I have about 2 terabytes of storage on the home file server running in Raid 10 mode with extra disks for backup and redundancy. My person virtualization environment is KVM running on top of Centos. I run a number of websites that are either hosted on my home network or on virtual private servers. I manage my own email and dns servers. I have also been experimenting with Arduino boards and I am investigating home automation using Z-Wave devices.