Ian Macdonald

Email web@jobs.imacdonald.co.uk

Introduction

My name is Ian Macdonald. I am a graduate of University of Edinburgh with a Bsc (honours) in Computer Science. I have worked in the IT field almost all of my career, specializing in computer security, production operations and systems deployments. I have refined my hands on and management skills over the years, managing Security Engineers at Constellation Energy & Salesforce and Operations Engineers at Clarabridge. Over my career I have created multiple engineering programs, including PCI Level 1 software as a service, building out disaster recovery data centers, migrating jboss on windows to a linux based system, adopting Devops practices and tooling, deploying custom network monitoring solutions globally. Most recently I have returned in an individual contributor role to concentrate on expanding my technical skill after building out a Security Operations team supporting Detection and Response at Salesforce.

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

Skills & Tools

- Manage and build teams focusing on Mentoring, Team career development
- Scrum and Agile, Managing IT Projects, DSS PCI Level 1 Compliances, Strong trouble shooting skills, designing highly available datacenters.
- Dell/HP Servers and Blade enclosures, F5 Load Balancers, Netscaler Load Balancers, Netapp, Cisco Firewalls, Cisco Switches, Cisco Routers, Dell Switch, Juniper Switches, Arista Switches, Cisco Sourcefire
- Centos, Redhat, Ubuntu, Apple OS X, Microsoft Server 2012.
- Puppet, Capistrano, Chef, Jenkins, Splunk, Kickstart. PXE Boot, Nagios, Zabbix
- Security Engineering and deployment, Penetration testing, Virus discovery and remediation, Vulnerability Assessments, Data modelling and Data Integration, Incident Response.
- Bro/Zeek, Suricata, Snort, Nmap, Nessus, Tcpdump, ModSecurity, Tenable, Wikid, OpenVPN
- Cyrus, Postfix, Bind, Apache, Active Directory, VMWare, KVM, Mysql tuning and administration, Jira.
- TCP/IP, SMTP, HTTP, DNS, and other protocols analysis.
- C, C++, Perl, Unix shell scripting, ML, Ruby, Java.

Experience

- 6 years either leading or managing teams.
- 20 years of computer and network security experience.
- 22 years experience administrating Linux and other flavours of Unix.
- 22 years experience administrating Windows Servers.
- Over 5 years of database/data modelling and data analysis experience.

Salesforce ***Lead Security Engineer Dec 2019 – Present***

- Deploying networking monitoring to all of Salesforce's global physical datacenters, IT Hub sites and new merges and acquisitions. This included design, working with vendors on hardware specs and selection, creating bill of materials, purchase requests, and working with business partners to drive the projects to completion.
- Perform proof of concept evaluations on new security technologies.
- Design and deploy next generation full packet capture capabilities.

Salesforce ***Senior Manager Information Security Feb 2018 – Dec 2020***

- Manage the Security Systems team supporting Detection and Response.

- Manage a team of 7 direct reports spread across 3 different locations.
- Responsible for managing, triaging, and prioritizing work for the team using agile methods.
- Work with the M&A team to perform security uplift projects for new acquisitions.
- Completed a security uplift project that upgraded the network monitoring and log forwarding pipelines in all datacenters. The project involved designing solutions that used existing tap, packet brokers where possible or ordering and installing new taps, packet brokers, and monitoring servers where needed. The team covered core datacenters, datacenter locations from companies we have acquired, and all IT ISP hub sites. The work utilized staff members from different teams both inside and outside security who were spread around the world.
- Responsible for the team that maintains and secures close to 2,000 servers spread around the world which support the Detection and Response function at Salesforce.
- Worked with the team to develop run books and procedures which were used by our Tier 1 team to monitor and performs initial triage on any access management or server related issues.
- Responsible for on going development of the network monitoring solution using open source and off the shelf tools.

Salesforce Lead Security Operations Engineer Jan 2017 – Jan 2018

- Created a new Security Systems Operations team supporting Detection and Response
- Helped design and build procedures to deploy a new security and log monitoring solution as part of a security uplift program
- Managed a team of engineers in Europe and the US responsible for the care and feeding of all Detection and Response servers
- Created repeatable run books for common team functions like patching and troubleshooting. Captured tribal knowledge in 'How To' articles
- Supported network monitoring, including taps, and packet brokers company wide
- Supported network forensics tools
- Worked with Puppet, Elastic Search, Hadoop, Splunk, Centos, Windows, Arista Packet Brokers, Network Taps, Moloch, Bro/Zeek,

Clarabridge Lead Systems Engineering May 2015 to Dec 2016

- Leading a team of 3 Systems Engineers.
- Responsible for the relationship with our hosting provider, including managing the multi-million dollar budget, ordering, upgrading and replacing all servers across multiple datacenters spread round the world.
- Responsible for network, load balancing, hardware, high availability and the operating systems for all machines in our datacenters.
- Responsible for our production and development environments, which are made up of approximately 400 machines, including Linux, Windows, virtual and baremetal.
- Introduced chef, creating quick start guides, how-tos, and deploying the framework and initial cookbooks, we are now using chef to deploying new Database, Elastic Search, and Micro Service instances, as well as common basic post bootstrap needs
- Responsible for keeping servers patched.
- Introduced new routing and network segmentation solutions to enhance security.
- Deployed multiple large Elastic Search clusters.
- Created many wiki articles that documents our datacenters, including architectural documents, how-tos, runbooks, etc.

VBrick DevOPS Lead Aug 2013 to May 2015

- 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.
- 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 for migrating and retiring old legacy servers in the datacentres.
- 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 application firewall for protecting against cross site scripting and sql injection attacks.
- Researched and selected outsourced vendors to conduct network and application security penetration testing.
- Architected and deployed Linux and Windows patch management solution.
- Standardized production platform on Centos/Redhat Enterprise linux.
- Created Linux system configuration and deployment system using Capistrano.
- Created taught Security Awareness and PCI compliance classes.
- Tested and deployed log management and monitoring system using Splunk , Blade Enclosures, new DMZ VMware infrastructure, IDS and Antivirus, internal certificate authority, Nagios, VMware, Vulnerability Management System, Two Factor Authentication system, and Two Factor Authentication system.
- Planned and deployed a remote data center which included blade enclosures, firewalls, switches, NAS storage, SAN storage and VOIP telecom equipment.

Education

Cisco

Cisco Certified Network Associate, CCNA (lapsed).

Salesforce Training

Emotional Intelligence, 7 Habits of Highly Effective People, Coaching for Success, Driving Performance Improvements, Emotional Intelligence, Engaging & Retaining Employees, Advanced Architecting on AWS, Agile – Product Owner, Agile – ScrumMaster, Architecting on AWS, Kubernetes Fundamentals, Puppet Fundamentals, Manager Bootcamp: Becoming an Multiplier, and Leading with Emotional Intelligence.

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.

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, Android, and Apple. I have about 2 terabytes of storage on the home file server running in Raid 10 mode with extra disks for backup and redundancy. I run my own email servers. My personal 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 am slowly automating my home using Z-Wave devices and other automation technologies. I have most recently been exploring Docker and Kubernetes