Ian Macdonald

Email jobs@imacdonald.com
Address: Herndon, VA 20170
Cell: 571 406 4266

Professional Summary

Accomplished IT and Cyber Security Leader with nearly 25 years of experience in managing and securing IT infrastructure, leading cyber security programs, and developing operational solutions for organizations of all sizes. Expertise spans Cyber Security, Governance, Risk & Compliance (GRC), IT Operations, and DevOps. Adept at advising executive teams, building teams, and ensuring compliance with global standards like PCI DSS, ISO 27001, SOC2, and HIPAA. With a hands-on approach to security, risk management, and driving organizational transformation.

Core Competencies & Skills

- **Cyber Security & Risk Management**: ISO 27001, PCI DSS, SOC2, HIPAA, FedRAMP, GDPR, CCPA, GRC tools
- **Security Operations**: Vulnerability assessments, Incident Response, Penetration Testing, Security Engineering
- **Compliance & Auditing**: SOC2, ISO 27001, PCI DSS, GDPR, HIPAA, LGDP, CCPA
- **Cloud Infrastructure**: AWS (IAM, Lambda, EC2, S3, RDS, GuardDuty, etc.), Terraform, Kubernetes, Docker
- **IT & DevOps**: Infrastructure as Code (IaC), Automation Pipelines, AWS, MDM, Malware Protection
- **Leadership & Team Building**: Mentoring, Career Development, Cross-functional Collaboration
- **Project Management**: Scrum, Agile, Budgeting, Network Design, High Availability Solutions

Technical Skills

- **Cloud & Infrastructure**: AWS, Terraform, Kubernetes, Docker, Elastic Search, Chef, Office 365
- **Networking & Security**: Splunk, Puppet, Bro/Zeek, Arista Packet Brokers, Moloch, Security Incident Management (SIEM)
- **Operating Systems**: Linux (CentOS, Rocky, Ubuntu), Windows, Mac OS
- **Security Tools**: Vulnerability scanners, Penetration Testing, Firewalls, IDS/IPS, Network Monitoring

Professional Experience

Banneker Partners (Private Equity) | **Cyber Security Practice Director**
Nov 2023 – Present

- Established and led the Cyber Security Practice for a private equity firm, advising 16 portfolio companies on strengthening their security postures.
- Initiated and managed Cyber Insurance programs, performed multiple cyber risk assessments, and guided security due diligence for mergers & acquisitions (M&A).
- Created best practices and frameworks for business continuity, risk assessments, cyber policies, and security tools selection, including SOC2, ISO27001, and PCI compliance support.
- Provided hands-on support to portfolio companies on tools like MDM, Malware Protection, and GRC platforms.

SuccessKPI (Experience Analytics) | **CISO, Head of Security, Operations, and IT**
May 2021 – Nov 2023

- Built and led a new security team, developing policies and controls to support the company's security compliance program.
- Oversaw annual PCI DSS renewal and achieved ISO27001, and SOC2+HIPAA Type 2 certifications.
- Conducted in-depth research and implemented robust security controls, policies, and procedures, leading to a successful external audit for compliance with GDPR, LGPD, and CCPA.
- Led an infrastructure improvement program, implementing Infrastructure as Code (IaC) and automation pipelines to enhance development, testing, and production environments.
- Directed IT operations, including Office 365 migration, global laptop deployment, IT helpdesk setup, and employee onboarding/offboarding processes for a remote workforce.

Salesforce (SaaS) | **Lead Security Engineer**
Dec 2020 – May 2021

- Deployed and managed network monitoring infrastructure across Salesforce's global physical data centers and acquisitions.
- Led proof-of-concept evaluations of new security technologies, including the deployment of full packet capture systems for enhanced security monitoring.

Salesforce (SaaS) | **Senior Manager, Information Security**
Feb 2018 – Dec 2020

- Managed a team of 7 engineers, supporting security detection and response functions across global data centers.
- Oversaw a security uplift project, upgrading network monitoring and log forwarding pipelines for core and acquired data centers.
- Worked with M&A teams to perform security audits for new acquisitions, ensuring the integration of acquired companies met Salesforce's security standards.

Salesforce (SaaS) | **Lead Security Operations Engineer**
Jan 2017 – Jan 2018

- Created and led the Security Systems Operations team responsible for supporting Detection and Response.
- Designed and implemented network monitoring and security log solutions, collaborating across teams worldwide to improve data security monitoring.

Clarabridge (Experience Analytics) | **Lead Systems Engineer**
May 2015 – Dec 2016

- Led a team of 3 engineers, managing relationships with hosting providers and overseeing a multi-million-dollar budget.
- Implemented network and routing security solutions, automated infrastructure with Chef, and deployed large-scale Elastic Search clusters.

Other Relevant Positions:

- **VBrick (Video Solutions)** | **DevOps Lead** (Aug 2013 – May 2015)
- **Angel.com / Genesys (Telephony)** | **Sr. Systems & Security Architect** (Nov 2008 – Aug 2013)
- **The World Bank (Finance) | Security Engineer** (Apr 2008 – Oct 2008)
- **AOL (Internet) | Technical Security Engineer** (May 2006 – Mar 2008)
- **Constellation Energy (Power Generation)** | **Security Engineer** (Mar 2002 – May 2006)
- **Strategy.com (Personalized Content) | Security Engineer** (Oct 2000 – Nov 2002)
- **MicroStrategy (Business Intelligence)** | **Software Engineer** (Oct 1997 – Oct 2000)

Education

Edinburgh University, Scotland,
BSc (Hons) Computer Science.

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 a Multiplier, and Leading with Emotional Intelligence.

George Washington University and ESI International
Managing IT Projects.

Security Conferences
Attended multiple BSidesNoVa, Shmoocon, Black Hat Briefing Las Vegas and Defcon, IANS DC forums conferences.

Institute for Applied Network Security, DC Forum 2007
Attended and Presented on the topic of Windows Mobile security vs Rim Blackberry Security

Cisco
Cisco Certified Network Associate, CCNA (lapsed).

Personal Projects

- **Home Lab**: Designed and managed a personal network with Linux, Android, and Apple machines, virtualized environments, self-hosted websites, email servers, and DNS services.
- **Automation**: Ongoing home automation using Z-Wave devices and IoT technologies.

Volunteering

- BSA Assistant Scout Master, BSA Merrit Badge Councilor, Elementary School Lego Club, High School Marching Band Photographer.