

Objective: Security Architect, Senior Security Consultant or IT Security Manager

SUMMARY of Experience

Business

- 20+ years IT industry experience
- 11+ years Oil and Gas industry experience
- 10+ years consulting experience
- Owned or participated in 4 startup IT businesses
- Written or guided business plans for startups
- RFP preparation, management, responses as vendor and end user, vendor management
- Budget and project stewardship of \$4M/\$1.5M capex/opex, with teams of employees and contractors

Information Security

- Deep experience with information security control frameworks (NERC CIP v3, ISO/27002, PCI, NIST 800-53, FISMA, COBIT).
- Design of information security programs, including policy, standards, guidelines and procedures that implement risk reduction and compliance mandate assurance. Most recent focus on NERC CIP v3.
- Design of enterprise security controls based on regulatory and voluntary compliance requirements and evolving threat mitigation (SABSA, ISF, TOGAF frameworks).
- Design and implementation of preventative, detective and corrective technical and administrative controls to support information security program objectives, including network segmentation, content filtering, logging/SIEM, IDS/IPS, access controls, stewardship definition, authorization for access. Controls include security metrics.
- Design and execute Security Risk Assessments to develop security requirements within projects.
- Consult with project teams to ensure business requirements include adequate security controls to satisfy security policy. Conduct validation of system and network design support of security policy.
- Support ISO/27002 and NERC CIP audits and assessments, including financials and Areva (Alstom) EMS
- Design and implementation of computer security incident response team, including integration with CIP cyber sabotage reporting requirements.

Leadership

- 10+ years of IT team leadership experience
- Team building and management experience in both IT and sales roles
- Director for IT startup companies
- VP Sales for software company

Education, Certifications, Associations

- MSc, CISSP, CISA, ITIL, JNFW (exp), CCSA (exp)
- ACM, ISACA, ISC(2), SPIE, Council of Advisors

Infrastructure

- Design and assessment of IT systems, network security, backup/recovery, operations and DRP.
- Systems architecture for multi-tier UNIX based infrastructures supporting advanced technical and commercial environments (such as high volume web hosting, e-commerce, Oracle database, document management and geo-technical processing).
- Security, performance, and high reliability tuning and design of distributed computing infrastructures (such as web hosting/applications, Oracle database, e-commerce) and corporate IP networks (IPsec/SSL, VPN, firewall, remote access).
- Systems management consulting for lights out operations and trouble shooting large UNIX server networks.
- System design, implementation, audit of IP based networks including internetworking (routing, service provisioning), security (multilayer firewall, VPN, host authentication, IDS/IPS), web servers and other key Internet based services.

PROFESSIONAL Experience

ArcSight (HP)

Calgary, AB
Apr 2011 – Present

Senior Systems Engineer

- Leverage extensive knowledge of security controls (ISO/27002, NIST 800-53) used to implement regulatory compliance (NERC CIP, PCI, SOX, HIPAA) with ArcSight products.
- Architect solutions for prospects and existing customers from a pre-sales perspective, including technology, process, and personnel aspects.
- Provide expert assistance to customers in adapting and extending ArcSight

technology to cover advanced business cases in health care, utilities, energy and financial verticals.

- Proficient with ArcSight centralized log management (CLM), correlation and incident management (SIEM) and GRC automation/reporting tools.
- Proficient with HP Enterprise Security Products security lifecycle suite, including Fortify, TippingPoint and ArcSight.

Alberta Electric System Operator (AESO)

Calgary, AB
Jan 2010 – Mar 2011

Enterprise Security Architect

- Created IT security program to implement desired maturity levels in compliance (NERC CIP, ISO/27002) and best practice.
- Developed enterprise wide mandatory security assessment and requirements develop processes, integrated into the Project Management Office
- Consult with various project teams, providing expert IT security recommendations to enable risk reduction and regulatory mandate compliance
- Primary member of IT Security Committee advising IT leadership on risk
- Leader of Computer Security Incident Response Team

ICSynergy (AESO)

Calgary, AB
Feb 2008 – Dec 2009

IT Security Specialist

- Defined high level elements of the IT security roadmap with the goal of introducing industry best practices to build required IT security capability and maturity levels (including tactical use of ISO/27002 and NERC CIP).
- Developed IT and Cyber Security Supporting Policy to coordinate IT security initiatives.
- Implemented centralized system access logging to improve security posture visibility. Leveraged logging to enable verification of key IT security safeguards including access control roles and responsibilities.
- Implemented Administrator account restrictions to reduce risk of malware infection and unauthorized system modifications.
- Integrated Computer Security Incident Response Team with AESO incident management process.
- Performed Security Risk Assessments to convey recommended safeguards to reduce risk to levels acceptable to the business.
- Consulted with various project teams, providing expert IT security recommendations to enable risk reduction and regulatory mandate compliance.

Intellitactics

Calgary, AB
Sep 2005 – Jan 2008

Senior Security Engineer (SIEM Software)

- Provided expert security specialist assistance to clients looking to improve their security operations and/or compliancy verification capabilities.
- Supported multiple Account Executives covering the west coast and central region of North America.
- Performed proof-of-concept engagements on client sites: Integrate into customer environments, illustrate how product speeds regulatory compliance proof and provides real-time information security risk management.
- Presented value proposition to multiple audiences, including executive level, internal audit, security operations, and network/infrastructure groups.
- Product suite includes Security Event Management, Security Information Management, Alert Assessment, Incident Response, Advanced Forensics, and communications dashboard software tools.

Network Forensics Consulting

Calgary, AB
Jul 2005 – Sep 2005

Director, Security Services

- Developed security strategy and information security policies for clients – evaluate business requirements and develop recommended information

- security strategy to frame and prioritize security related projects (ISO/27002).
- Provided subject matter expert advice for security redesign – develop product and configuration recommendations for improvement of perimeter and core security, including network and host IDS, centralized syslog hosting and alerting, firewall rule set tuning.
- Conducted vulnerability and security risk assessments – including penetration testing and exposure impact assessments. Deliver recommended gap closure plans for implementation by internal staff.

Precision Drilling Corporation

Calgary, AB
Mar 2005 – Jun 2005

Senior Security Architect

Managed InfoSec group and consulted with internal clients to identify and mitigate network connectivity risks and provide InfoSec certification of project designs.

Highlights:

- Stewarded Perimeter Security Redesign project, including technical, budget and project management oversight.
- Provided security assessments of network infrastructure, including perimeter network security, corporate inter-office, and DMZ (Cisco, Juniper, Checkpoint, ISS solutions evaluated).
- Developed Security Guidelines (rules of engagement) for wired and wireless network and system design, in anticipation of revamped SOX compliant Information Security Policy.
- Provided specialist guidance to IT management team for creation of new Information Security policy.
- Managed Information Security team with two direct reports.
- Position dissolved with sale of Precision Drilling assets to Weatherford.

Network Forensics Consulting

Calgary, AB
Oct 2004 – Mar 2005

Director, Security Services

Provided IT security specialist assistance to clients including:

Network Security Assessments – Oilfield Services Company

- Provided security assessments of client infrastructure, including external and internal network security assessments, gap identification and closure assistance. Vulnerability assessment as well as targeted penetration testing.
- Fundamental tools used: Nessus+plugins, Whisker, nikto, nmap, MBSA, Titan, JASS, Metasploit.

External DNS – Petro-Canada

- Performed solution research and presented alternative architectures with recommended implementation plan.
- Delivered technical solution, including move of 63 domains with zero downtime.

Regionalized Centralized Log Repository Architecture – Petro-Canada

- Established business requirements for Centralized Log Repository sufficient to support a global Security Information and Event Management implementation.
- Developed architecture framework including alternatives considered and recommended solution.
- Developed staged implementation plan for recommended architecture, including operational impact assessment.

Enterprise DNS Architecture – Petro-Canada

- Established business requirements for comprehensive Enterprise DNS Architecture, covering External, Internal, Extranet, and DRP functional silos.
- Developed architecture framework including alternatives considered and recommended solution.
- Developed staged implementation plan for recommended architecture,

- including operational impact assessment.
- Solution supported UNIX and Windows (AD) environments, and sped DRP activation.

Petro-Canada

Calgary, AB
Nov 2001 – Sep 2004

Team Leader, Unix/Storage

- Lead UNIX and Storage infrastructure teams for Upstream and Corporate divisions.
- Supported environment included over 27TB of EMC storage, 63 Sun, HP, and Linux servers, as well as 120 geo-technical desktops (Sun Solaris).
Highlights:
 - Stewarded \$3.5M capital, \$1M G&A budget.
 - In-sourced and managed team of three UNIX system administrators, established operating procedures for architecture, procurement, build, maintenance, and group management.
 - Communicated with Database, Networking, Security, Intel, Engineering, Geological/geophysical, Financial and Commercial application groups.
 - Managed annual organic disk growth rate of +60% (EMC) through planned organic expansion.
 - Designed and implemented DRP infrastructure to support defined application RTO objectives (Sun, HP, Linux), with frugal DRP budget (selective sync of data over 10Mbps short haul link).
 - Established host and network IDS operating environment (Enterasys Dragon on Solaris, Linux), provided standards for secure server build and maintenance procedures.
 - Established UNIX access and privilege auditing, control, and reporting system for Sarbanes-Oxley (SOX) compliance (with TFS UnixControl/Keon).
 - Established central syslog environment for Sarbanes-Oxley (SOX) compliance.
 - Designed and implemented Oracle database consolidation project - 6 Sun servers to 2 Sun V880 with Veritas Cluster Server 3.5.
 - Established customer care web site (Apache/MySQL/PHP/Mambo) with On-call, Vacation, Help Desk, system event calendar, as well as central portal for backup/recovery status, system statistics, group task documentation.
 - Established regular nmap system scanning to identify new hosts and ports on the corporate network.

Sun Microsystems, Professional Services: US (Shaw Cablesystems)

Calgary, AB
Apr 2001 – Jul 2001

Senior Systems Consultant

- Provided best industry practice experience to build the operations of Residential ISP
- Provided technical and ongoing operations support for ISP services including:
 - Primary support for Usenet News services (over 9.5TB of article store) bCandid Cyclone and Twister servers (XML and HTML presentation of Usenet articles)
 - Sun JumpStart / Quark (rapid system recovery and deployment tools)
 - Troubleshooting and fine-tuning of automatic monitoring via Netcool, SunMC, and HP OpenView
 - Providing consulting services for security hardening of hosts and network devices, auditing, and intrusion testing / vulnerability inventory and remediation.
 - Configuration and troubleshooting host based firewall software and policies (IPfilter 3)

Burntsand Solutions

Calgary, AB
Aug 2000 – Apr 2001

e-Solutions Integration Specialist

- Provided senior e-commerce technical consulting to Burntsand clients including:
 - Assessed and redesigned client perimeter networks, usually due to M&A activity
 - Designed and implemented Checkpoint Firewall-1 3.0, 4.0, 4.1 / Cisco PIX 525 architectures, including solution run books, remote office VPN construction, remote

firewall management, audit and re-design of firewall management including change and configuration control.

- Performed advanced Solaris performance tuning
- Designed e-commerce enabling infrastructures, including consulting on multi-tier security and web application architectures
- Performed advanced troubleshooting of high availability Documentum system (AT&T Wireless, NJ)
- Designed and implemented site infrastructure with iPlanet Enterprise Server
- Taught firewall design section of Internet Security course at SAIT

CommGeneral

Calgary, AB
Nov 1995 – Aug 2000

Co-founder, Senior Systems Consultant

- Launched highly specialized UNIX and network systems consulting company
- Worked with CommGeneral clients providing technical services including:
 - Checkpoint Firewall-1 (3.0, 4.0) product configuration and operation
 - Review and presentation of critical security improvements required to address shortcomings in client internal and perimeter networks
 - iPlanet Enterprise Server (3.6) installation and configuration
 - Apache Web Server (1.3.19) and OpenSSL installation and configuration
 - Security hardening, auditing, and intrusion testing of Solaris and Linux machines Internet accessible (mail, DNS, web applications, proprietary external access)
 - Setup and monitoring of Snort based IDS
 - Review of client internal network (CalFed Bank), preparation of security posture report including vulnerabilities and gap closure plan
 - Project manage and implement large scale system migrations (HP/UX)

Clients included Amerada-Hess, Crestar, Northstar, Norsk-Hydro, Spectrum Seismic, Kelman Technologies, Iron Mountain, Pan Alberta Gas, Enerlogix, Petro-Canada, Telus Mobility (ISM/BC), Beau Canada, Polaris Technologies, CalFed Bank (US), Fleet Mortgage (US)

ObjectWorks

Calgary, AB
Jan 1995 – Oct 1995

VP, Sales and Marketing

- Created marketing group; Directed sales of consulting resources; Managed sales and marketing team of four

Nova Gas Transmission

Calgary, AB
Jan 1994 – Dec 1994

Senior Systems Administrator

- Designed and implemented IBM RS/6000-590 Oracle server pair
- Conducted security review of server environment, recommended and implemented changes (40+ IBM RS/6000 nodes)

Amerada-Hess

Calgary, AB
Sep 1991 – Jan 1994

Senior Systems Administrator

- Lead first decentralized accounting applications in Canada for Amerada-Hess
- Established UNIX/Oracle infrastructure for integrated oil and gas application
- Implemented service availability management processes - including alerting

EDUCATION

- Master of Science, Information Systems, Athabasca University, Thesis Topic: Effective SQL Injection Attack Reconstruction using Network Recording, 2010
- ISACA, Certified Information Systems Auditor CISA #977990, October 2009
- ITIL Foundation Course, April 2005
- ISC(2) Certified Information System Security Professional CISSP #70777, April 2005
- ICCP, Certified Computing Professional CCP #25002, February 2005
- Juniper Networks, FW/VPN track, JNFW-CIA certificate, 2004; Checkpoint CCSA, Calgary, 2001
- HP/UX Virtual Vault 4.0, Mountain View, March 2000
- Sun Certified Administrator for Solaris; Oracle Database Administration; Programming in C
- Southern Alberta Institute of Technology, Industrial Electronics Technology, Sept 82-May 84

Sept 2011