

Allen Pomeroy

Enterprise Security Architect

Cell: 403-990-5445
Email: apomeroy@networkforensics.ca
Web: www.networkforensics.ca

Objective: IT Security Director, IT Security Architect, or Senior Information Security Consultant

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

Infrastructure

- System design, implementation, audit of IP based network infrastructure including internetworking (routing, service provisioning), security (multilayer firewall, VPN, host authentication, IDS/IPS), web servers and other key Internet based services.
- 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 infrastructures).
- 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.

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

Certifications, Associations

- MSc, CISSP, CISA, ITIL, JNFW (exp), CCSA (exp)
- SPIE, ISACA, ACM

Information Security

- Design, Assessment and Review of IT systems and network security, backup/recovery, operations and DRP. Consulting to support InfoSec program, architecture, and audit preparation. (SABSA, TOGAF)
- Technical implementation of controls to support information security programs, via firewalls, logging, IDS/IPS, network compartmentalization, access controls, logging, UTM, SIEM. Familiar with information security control frameworks including ISO/27002, NERC CIP, PCI, NIST 800-53, FISMA, COBIT.
- Design of information security programs, including policy, standards, guidelines and procedures that implement risk reduction via threat and vulnerability identification and incident response.
- Vulnerability assessment, penetration testing, validation of system and network security design (internal and perimeter). Design and execution of Security Risk Assessments (RCMP TRA, OSSTMM, NSA IAM). Focus on web applications.

PROFESSIONAL Experience

Alberta Electric System Operator (AESO)

Calgary, AB
Jan 2010 – Present

Enterprise Security Architect

- Created IT security programme to implement desired maturity levels in compliance (NERC CIP, ISO/27002) and best practice.
- Developed enterprise wide mandatory security assessment and

Allen Pomeroy

Enterprise Security Architect

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
- 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
- Consult with various project teams, providing expert IT security recommendations to enable risk reduction and regulatory mandate compliance

Intellitactics

Calgary, AB / Reston, VA
Sept 2005 – Jan 2008

Senior Security Engineer (SIEM Software)

- Provide expert security specialist assistance to clients looking to improve their security operations and/or compliancy verification capabilities.
- Support multiple Account Executives covering the west coast and central region of North America.
- Perform 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.
- Present value proposition to multiple audiences, including executive level, internal audit, security operations, and network/infrastructure groups.
- Consult with customers, providing expert SIEM recommendations and assist clients with escalation of technical issues.
- 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
July 2005 – Sept 2005

Director, Compromise Prediction

- Develop Security Strategy and Information Security Policies for clients – evaluate business requirements and develop recommended Information Security Strategy to frame and prioritize security related projects. Recommendations usually included framework for development of Information Security Program.
- Provide 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.

Allen Pomeroy

Enterprise Security Architect

- Conduct 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
March 2005 – June 2005

Senior Security Architect

- Provide specialist consultation to internal clients to identify and help mitigate network connectivity risks
- Participate in all network related IT projects and provide InfoSec certification
 - Steward Perimeter Security Redesign project
 - Provide security assessments of client infrastructure, including perimeter network security, corporate inter-office, and DMZ Cisco, Juniper, Checkpoint, ISS solutions evaluated.
 - Develop Security Guidelines - provide guidelines for 'rules of engagement' for wired and wireless network and system design, in anticipation of revamped SOX compliant Information Security Policy.
 - Provide specialist guidance to corporate IT management team for creation of new Information Security policy
 - Manage Information Security team with 2 direct reports
 - Position dissolved with sale of Precision Drilling assets to Weatherford

Network Forensics Consulting

Calgary, AB
Oct 2004 – March 2005

Director, Compromise Prediction

Provide IT security specialist assistance to clients in order to reduce the risk of Internet and extranet connectivity, including:

Network Security Assessments – Oilfield Services Company

- Provide security assessments of client infrastructure, including external network security assessments, internal network security assessments, and 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

Repatriate External DNS – Multinational Oil and Gas Company

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

Develop Regionalized Centralized Log Repository Architecture – Multinational Oil and Gas Company

- Work with client to establish business requirements for Centralized Log Repository sufficient to support a global Security Event Management implementation
- Develop architecture framework including alternatives considered and recommended solution
- Develop staged implementation plan for recommended architecture, including operational impact assessment

Develop Enterprise DNS Architecture – Multinational Oil and Gas Company

- Work with client to establish business requirements for comprehensive Enterprise DNS Architecture, covering External, Internal, Extranet, and DRP functional silos
- Develop Architecture framework including alternatives considered and recommended solution
- Developed staged implementation plan for recommended architecture,

Allen Pomeroy

Enterprise Security Architect

- including operational impact assessment
- Solution supported UNIX and Windows (AD) environments, as well as eased DRP activation

Petro-Canada

Calgary, AB
Nov 2001 – Sept 2004

Team Leader, Unix/Storage

- Responsible for a team of technical specialists supporting the UNIX and Storage infrastructure for the Upstream and Corporate divisions. Supported environment includes over 27TB of EMC storage (SAN and NAS), 63 Sun, HP, and Linux servers, as well as 120 geo-technical desktops (Sun Solaris).
Highlights:
 - Steward \$3.5M capital, \$1M G&A budget - four budget cycles;
 - In-source and manage team of 3 UNIX system administrators, establish operating procedures for architecture, procurement, build, maintenance, and group management;
 - Liaison with Database, Networking, Security, Intel groups, as well as with application support groups (Upstream engineering and geological/geophysical applications, Corporate financial and commercial applications);
 - Manage annual organic disk growth rate of +60% (EMC), establishment of regular organic expansion, planned business driven expansion in a planned and controlled manner;
 - Architect and implement DRP infrastructure to support defined application RTO objectives (Sun, HP, Linux), with frugal DRP budget (selective sync of data over 10Mbps short haul link);
 - Establish host and network IDS operating environment (Enterasys Dragon on Solaris, Linux), provide standards for secure server build and maintenance procedures;
 - Establish UNIX access and privilege auditing, control, and reporting system for Sarbanes-Oxley (SOX) compliance (with TFS UnixControl, formerly RSA Keon);
 - Establish central syslog environment for Sarbanes-Oxley (SOX) compliance;
 - Architect and implement Oracle database consolidation project - 6 Sun servers to 2 Sun V880 with Veritas Cluster Server 3.5;
 - Establish 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;
 - Establish regular nmap system scanning to identify new ports listening on the corporate network.

Sun Microsystems, Professional Services: US (Shaw Cablesystems)

Calgary, AB
April 2001 – July 2001

Senior Systems Consultant

- Provide best industry practices experience to support the operations of Residential ISP
- Provide 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 (allows 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.

Allen Pomeroy

Enterprise Security Architect

- Configuration and troubleshooting host based firewall software and policies (IPfilter 3)

Burntsand Solutions

Calgary, AB
August 2000 – April 2001

e-Solutions Integration Specialist

- Provide senior e-commerce technical consulting to Burntsand clients
- Provide technical consulting services including:
- Audit and re-design of client perimeter networks, including security posture and assessment of vulnerabilities - usually due to M&A activity
- Checkpoint Firewall-1 3.0, 4.0, 4.1 / Cisco PIX 525 product installation, configuration, and operation, including remote office VPN construction and remote firewall management, audit and re-design of firewall management including firewall rule set design and change control.
- Advanced Solaris performance tuning
- Design of e-commerce enabling infrastructures, including consulting on multi-tier security and web application architectures
- Advanced troubleshooting of high availability 3 tier database Documentum system (AT&T Wireless, NJ)
- Design, configuration of sites with iPlanet Enterprise Server
- Teach firewall design section of Internet Security course at SAIT

CommGeneral

Calgary, AB
January 1998 – August 2000
Petro-Canada/Amerada-Hess
Nov 1995 – August 2000

Co-founder, Senior Systems Consultant

- Launch highly specialized, premier quality UNIX and network systems consulting company, lead the first year of growth
- Work 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 short comings 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
 - DataFellows ssh (Secure Shell) DMZ secure FTP server implementation for Petro-Canada
 - Security hardening, auditing, and intrusion testing of Solaris and Linux machines attached directly to the Internet (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 discovered and gap closure plan
 - Project manage and implement large scale system migrations (HP/UX)

Client list included 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
January 1995 – October 1995

VP, Sales and Marketing

- Created marketing group – including Marketing Communications
- Direct sales of consulting resources, fixed bid, over \$1M
- Manage sales and marketing team of 4

Nova Gas

Transmission Ltd
Calgary, AB
January 1994 – Dec 1994

Senior Systems Administrator

- Design and implementation of IBM RS/6000-590 Oracle server pair
- Implementation of ESCON channel to MVS server for backup/recovery
- Conduct security review of server environment, recommend and implement changes (40+ IBM RS/6000 nodes)
- Design and implementation of HP9000 T500, G50, G60 Oracle servers

Amerada-Hess

Calgary, AB
Sept 1991 – January 1994

Senior Systems Administrator

- Hired to guide first decentralized accounting applications in Canada for Amerada-Hess
- Established UNIX/Oracle infrastructure for integrated oil and gas application PW*Sequel
- Implemented service availability management processes - including alerting
- Implemented DRP processes
- Designed and implemented secure source code control layer over RCS

RELATED Organizations and Projects

- Member of Information Systems Audit and Control Assoc (ISACA) 2005
- Member of Council of Advisers (Technology Council) 2004
- Member of Security Professionals Information Exchange (SPIE) Calgary 2004

- Design and implementation of web hosting system for small clients (Calgary Ultimate League, Crystal Waters, Demetre, ReservoirEngineer, NetworkForensics.ca, suncluster.org, objectivemetrics.com) - delivered via SSL based web services. Focus on Content Management Systems and Webmail.
 - Hot-standby firewall using OpenBSD and CARP (several second failover, with connection state synchronization, open source VRRP implementation)
 - Layer 4 load balancing through use of Linux Virtual Server (LVS)
 - Clustered Apache, SMTP, IMAP, PHP, MySQL platform provides service delivery
 - NIDS and HIDS through snort, BASE (ACID)

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
- Veritas Cluster Server 3.5, Calgary, 2003
- Sun Network Conference Sessions, San Francisco, 2002
- Sun Microsystems, T300 Storage Administration, Calgary, 2001
- 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

July 2010