Deshler “Del” Armstrong

1850 Folsom St., Apt 602
Boulder, Colorado 80302

resume-web@thearmstrongfamily.org
http://del.thearmstrongfamily.org

Summary

- Experienced and passionate Computer Security Analyst and Manager with strong background in UNIX, TCP/IP and incident response.
- Excellent consulting and teaching skills; very good written and verbal skills.
- OSCP, CSSLP, GCUX, CISM, CISA, CISSP, GCIA (GCIA is expired - can recertify)
- Active Department of Defense Top Secret Clearance.
- M.S., Computer Science, Rochester Institute of Technology.

Skills

- QRadar, Tenable Security Center, Trend AV, Metaploit, Retina, WebInspect, ISS, Dragon, Snort, Nessus, Qualys Security Scanner, tcpdump, Nmap, Ethereal (Wireshark), EnCase.
- Kali, REMnux, AIX, Solaris, Linux, OpenBSD, Windows, SunOS, Ultrix, IRIX, HP/UX, VMS.
- Ruby, Python, PERL, C, FORTRAN, Forth, Pascal, Basic, Z-80 & VAX Assembler.
- PHP, HTML
- Cisco, Juniper, PF, IPchains.
- TCP/IP, NFS, NIS, AppleTalk.

Experience

Red Canary *(December 2018 – Present)*

Detection Engineer

IBM *(October 2013 – December 2018)*

GBS/FIMS – A MSS Supporting Federal Cloud Customers

Sr. Security Analyst *(January 2015* – Present)
In addition to the duties of Security Analyst, also:

- Tier 3 support for SOC.
- Mentor junior staff.
- Develop and document new processes and procedures.
- Develop software to automate SOC functions.
- Maintain and enhance locally developed SOC portal.
- Provide technical direction and support for incident response.
- Conduct forensics analysis.
- Maintain situational awareness and monitor threat intelligence sources.
- Work 12 hour day/night shifts as necessary.

Security Analyst *(October* 2013 – January 2015)

- Work 12 hour day/night shifts at 24x7 SOC supporting 1000+ device infrastructure.

- Monitor security systems.
- Investigate and document potential security incidents
- Assist in security incident response.
- Conduct security scans. Document results and interpret for customers.

Planned Systems International, Inc. *(September 2007 – October 2013)*

Supporting MHS/DHSS, Department of Defense

Team Lead, Security Team *(*January 2013 – October 2013)
In addition to the duties of Security Analyst, also:

- Team Lead for small team of security analysts.
- Helped plan major data sanitization effort.

Security Analyst (November 2012 – January 2013)

- Assisted in planning migration of 16 applications to a virtualized cloud provider.
- Documented architecture for multiple applications.
- Documented application migration requirements.

Supporting MHS/TMA, Department of Defense

Manager of Security (January 2009 – November 2012)

- Managed security team
- Served as IAO for integrated system of applications deployed across 100+ servers.
- Responsible for compliance with DoD CCIs, SRGs, STIGS, SRR/Checklists and CTOs.
- Managed C&A scanning activity and maintain required C&A documentation.
- Assisted in compliance with DOD security standards.
- Contributed to security in all phases of SDLC.
- Wrote security standards and procedures.
- Conducted security assessments.
- Developed software in support of assessment and C&A activities.

Manager of Security and Infrastructure (March 2008 – January 2009)
In addition to the duties as Manager of Security, also:

- Managed small infrastructure team (grew to 5 person team.)
- Responsible for administration of 50+ server infrastructure.
- Assist in migration to offsite cloud provider.

Manager of Security (September 2007 – March 2008)

- Responsible for security of mission critical applications.
- Managed small security team.
- Managed C&A scanning activity and maintain required C&A documentation.
- Assisted in compliance with DOD security standards.
- Contributed to security in all phases of SDLC.
- Wrote security standards and procedures.
- Conducted security assessments.
- Developed software in support of assessment and C&A activities.

Intellidyne, LLC *(June 2005 – September 2007)*

Deshler “Del” Armstrong

Supporting MHS/TMA, Department of Defense

Security Engineer (June 2005 – September 2007)

- Security liaison between two separate organizations.
- Managed C&A scanning activity and maintain required C&A documentation.
- Assisted in compliance with DOD security standards.
- Contributed to security in all phases of SDLC.
- Wrote security standards and procedures.
- Conducted security assessments.
- Developed software in support of assessment and C&A activities.

Consultant - Coalfire Systems, Inc. *(October 2004 – June 2005)*

- Conducted forensic investigations.
- Implemented IDS installation, configuration and training.
- Wrote security standards and procedures.
- Assist with SOX, HIPAA, Federal/NIST compliance

Global Crossing Inc. *(1997 – October 2004)*

Information Security Analyst (February 2004 – October 2004)

- Responsible for assuring compliance with corporate computing standards.
- Conducted security assessments.
- Produced detailed weekly report documenting security “health”.
- Member of 24x7 on-call security response team.

Security Auditor (2003 – February 2004)

- Founding member of two person IT security audit team.
- Developed and conducted security assessment procedures.
- Member of 24x7 on-call security response team.

Handled numerous internal and customer facing security incidents: including compromised/infected computers, DDOS attacks, extortion threats and spam.

Internet Security Analyst III (1997 – 2003)

- Responsible for security of Internet facing computers.

Helped manage security, respond to incidents, create policy and procedures and train staff for a 60,000 customer dial-up ISP.

- Responsible for designing/implementing proactive security scans and IDS.
- Assisted with network security, ACL maintenance.

University of Rochester *(1980 – 1997)*

School of Engineering and Applied Science

Senior System Manager and Manager of User Consulting (1992 – 1997)

- Co-managed network of more than 110 UNIX-based computers.
- Responsible for security of all UNIX machines.
- Managed user consulting services and administered series of UNIX tutorials.

Deshler “Del” Armstrong

Production Automation Project and Dept. of Electrical Engineering

Systems Programmer and System Manager (1980 – 1992)

- Co-managed large network of UNIX and VMS systems.
- Programmed in FORTRAN, Z-80 & VAX assembler, DCL and C.
- Wrote documentation. Taught seminars.