

Scott Palmer, CISSP, PCIP, GPEN

Colorado Springs, CO 80951 • (719) 362-5581 • scott.palmer@serenitytek.com

SUMMARY OF QUALIFICATIONS#

- CISSP with over 22+ years of experience in the systems administration and engineering fields; effective at multitasking and working under pressure to accomplish overall objectives
- Committed to collaboration and team unity
- A quick study; adapts easily to new environments
- Organize, motivate, and develop others to accomplish goals

CLEARANCES : Top Secret/SSBI (SCI last active 02/08)

PROFESSIONAL EXPERIENCE

Oct 2019 – Current – Professional Services Engineer (Cyber) – Skybox Security

- Provide professional services for Skybox Security customers, including Fortune 500 and Government organizations, in modeling their environment and identify risks
- Worked with a multitude of products from network and security vendors to assist the customer in compliance and best practice efforts to reduce risk
- Debugged issues with Skybox software and customer networks, worked with development to identify bugs and provide paths forward

July 2018 – Oct 2019 – Solutions and Integrations Engineer GPS (contract work) – ASRC

- Provide solutions and integration for the Global Positioning System (GPS) Control Segment. Work with RMF requirements for technical solutions and mitigation efforts as required.
- Provide SME guidance on technical and security requirements, encryption of data at rest and transit, host and network segmentation and access control and application security best practices
- Architected improvements to the VMWare/VCenter environment to improve performance in the development and test environments, provided segmentation controls to manage data flow
- Mentor team members and taskings management
- Returned to support a significant upgrade effort

January 2018 – July 2018 – Security Solutions Consultant – Lumeta (company sold)

- Provide Fortune 500 clients professional services as a Network Security/Cyber Security architect in base-lining and defining risk across global network environments using Lumeta's Spectre product
- Provided DoD customer base guidance for meeting RMF requirements
- Extensive travel, 70%+, to client sites to provide architectural support and training

March 2016 – December 2017 – JTAGS Product Office – Cyber Security Engineer VII, Sigmatech

April 2013 – February 2016 – JTAGS Product Office – Cyber Security Consultant (part-time), IES

- Provide Cyber Security and system engineering support on JTAGS mission platform consisting of Redhat Server and Workstation, Windows Server, Cisco, and NetAPP devices
- Provide assessments and guidance using NIST 800-37 and 800-53 (RMF)
- Perform penetration and assessment activities on classified government systems to validate against Information Security requirements on an annual or semi-annual basis at CONUS and OCONUS locations
- Design and validation on classified network and security design
- Provide direction on Incident Response scenarios and plans
- Deploy and manage Security Center (ACAS) environment for the enterprise vulnerability management
- Provide SME support for Linux, Cisco/Networking, and cyber security matters
- Consultant role converted to full time role, March 2016

September 2012 – January 2016 – Security Engineer III - Cabela's

- Performed penetration and assessment activities to determine risk areas and assign a risk rating, manage projects to remediate findings and prioritize based on the assigned risk rating
- Managed vulnerabilities using industry standard assessment tools, such as Security Center, Kali Linux (penetration testing), and HP Fortify

- Managed PCI compliance and perform assessments for US and Canada operations using PCI DSS
- Managed Security Analysts, assigned tasking's, provided guidance, and perform employee assessments
- Provide SME input for security on Windows, Linux, and Network systems based on best practices to company and department leadership
- Provide data security architecture for all projects involving PII, Credit Card data (PCI) and company sensitive information, such as which data sets must be encrypted and controlled

January 2011 – September 2012 – IASO / Security Engineer – Northrop Grumman / Ciber, Inc

- JTAGS JSF Information Security Officer, Information Management Officer (IASO/IAO)
- Perform information security audits to check system security integrity using DISA STIG's, Retina, DISA Gold Disk, and SRR on all JTAGS Assets (IRIX, Solaris, Linux, Netapp, Cisco, and Windows)
- Perform evaluations of engineering designs, code reviews, and proposals to insure security compliance
- Develop, troubleshoot, and configure Cisco switches and ASA 5510 firewall appliance configurations
- Design and implement security controls for Linux, IRIX, and Network platforms

February 2008 – January 2011 – Security/Network Architect, IAM – Port Graham Development Corp

- Provided all Information Assurance (IA) direction, reports, scans, and requirements
- Lead engineer working with rapid deployment communications systems which utilized satellite connectivity and VoIP to provide the first responder with land, cell, and data services in a disaster
- Introduced key design changes and implemented the Emergency Alerts System (EAS) disaster recovery system for FEMA as directed by Presidential Executive Order. This project reached all targets of success ahead of schedule, and utilized inter-agency interoperability
- Provided SME support for all Solaris, Linux (CentOS and Redhat), and Cisco platforms

August 2001 – February 2008 – Senior Unix Administrator (SBIRS/MDA/GPS) – Lockheed Martin

- Senior Systems Administrator and team lead for Space Based Infrared Program (SBIRS), Missile Defense Agency (MDA) HPCC environment, and Global Positioning System (GPS)
- Managing an install base of over 100 UNIX systems, comprised of SGI 3000 series servers, Tezzro workstations, Sun E6900, T1000/2000 "CoolThreads" servers, and V480/V490 servers and workstations
- Engineering and review of the Disaster Recovery and Continuity of Operations (DR COOP)
- Responsible for installing, configuring, and maintaining Unix workstations and servers in support of business processing requirements.

September 2000 – August 2001 – Unix Administrator – Quris, Inc

- Worked as a Unix and network administrator on Sun and Linux servers; Cisco and NetApp

October 1999 – September 2000 – Unix Administrator – Sun Microsystems, Inc

- Worked with Sun's internal users to identify, diagnose and correct problems relating to all aspects of Sun's internal infrastructure

November 1997 - October 1999 – Unix Administrator / Technical Sales Advisor – PCI Systems

October 1996 - November 1997 – IT Consultant – Mountain Enterprises

October 1992 - October 1996 – US Army

EDUCATION AND TRAINING#

CISSP (384723)– April 2011

GIAC Penetration Tester – GPEN – October 2014

Payment Card Industry Professional (PCIP) – PCI Security Standards - 2013

Bachelors of Science in IT, Information Assurance and Security – Capella University

VOLUNTEER ACTIVITIES#

Mentor – CyberPatriot – Vista Ridge HS, Colorado Springs, CO

Red Team – Rocky Mountain Collegiate Cyber Defense Competition

SKILLS SUMMARY#

Apache/SSL, Postfix, Squid/Proxy, Samba/NFS, Shell/Perl Scripting, Solaris Zones, VMware ESX/GSX, XEN/KVM, Linux HA Cluster, Sun Cluster, Cisco IOS, Asterisk, VoIP, IPFilters (Solaris/BSD), IPTables (Linux), TCP Wrappers, Nessus, NMAP, Sidewinder Firewall, Cisco IOS ACL's, ASA, PGP/GunPG, SNORT, John the Ripper, IDS', OpenVPN, FireEye, Bluecoat, Solera DeepSee, Security Center (ACAS), Splunk