



**SENIOR CYBERSECURITY ENGINEER  
AVAILABLE FOR SUBCONTRACTING  
CONTACT: L.KINKEAD@PETRACYBERTECH.COM**

---

## **PROFESSIONAL SUMMARY**

Cybersecurity expert with over 20 years of experience in both the federal government and private sector organizations. Possesses extensive knowledge of state-of-the-art security tools and procedures which has ensured the safety of computer systems utilized by tens of thousands of users.

## **GOVERNMENT EXPERIENCE**

**Agencies:** Federal Aviation Administration and the United States Department of Transportation

**Military:** Air Force Village West Primary Medical Campus, March Air Reserve Base, Camp Pendleton

## **SECURITY CLEARANCE – Secret, Confidential**

## **TECHNOLOGY EXPERIENCE**

Invicti/Netsparker Dynamic/Interactive Application Security Testing (DAST / IAST) tool, Qualys, JASK/Sumo Logic, Nessus, Netskope, Snort, Fortinet, Palo Alto - Cortex, Symantec DLP/WSS, Code42, AdTran, Check Point Technologies, BlueSocket, Dell EqualLogic, VMWare, Barracuda Web and SPAM Filters, IDS/IPS NGFW (Palo and Fortinet), SonicWall, NetApp, BlueCat DHCP Appliances, EMC, NMAP, Wireshark, Ethical Hacking (Penetration Testing), SIEM, Vulnerability Management, CISCO, VOIP (Cisco, Mitel, AdTran), MicroWest iFams, American Healthtech LTC, Walt Disney DU Training / Mentor, Answers On Demand (AOD), CompTIA Security+, Sage ERP, Microsoft Exchange, Active Directory, Novell, HIPAA / NIST Standards and Practices, MS Windows, Linux, MSSQL, MySQL, PostgreSQL

## **PROFESSIONAL EXPERIENCE**

**Petra Cyber Technologies**

**05/2020 – 04/2022**

**Senior Cybersecurity Engineer/Subject Matter Expert  
Columbus, OH**

**Senior cybersecurity engineer providing Dynamic/Interactive Application Security Testing (DAST / IAST) services for the Federal Aviation Administration and the United States Department of Transportation**

- Coordinated and managed the deployment of Invicti Netsparker DAST solution with the USDOT and FAA infrastructure teams.
- Served as the primary application administrator and Subject Matter Expert for DAST and IAST solution.
- Managed daily DAST scanning processes and provided remediation guidance to development teams for discovered vulnerabilities.
- Acted as a USDOT liaison to Invicti engineering and support teams.
- Created and maintained documentation standards, policies, and procedures.
- Provided technical and professional training and mentoring to FAA/USDOT engineering colleagues.

**Member of the security team responsible for providing a full range of MSSP / security services for globally-based clientele. Our services included security planning and development. Policy and standards framework development. Physical implementation of internally developed security solutions.**

- Prepared overall security plans and managed security operations.
- Oversaw the management of project lifecycles through successfully facilitating working relationships between clients, partners and project teams.
- Created and maintained documentation standards, policies, and procedures.
- Created and maintained Security Operations playbooks.
- Reviewed, analyzed, and approved exceptions to security policies or controls.
- Collaborated with Security Architecture and Security teams to perform product evaluations, identify security gaps, design security controls, and perform architecture reviews.
- Acted as an escalation point for Incident Response activities.
- Provided implementation and architectural advice on infrastructure and development projects.
- Provided technical and professional mentoring to engineering colleagues.
- Developed automated firewall configuration management system for CISCO/PALO/Check Point Appliances.

**Member of a small security team responsible for providing a full range of security services for a global manufacturing enterprise. Our services included security monitoring, digital forensics, security incident response, and architecture reviews. Provided advisory services for systems and network configuration hardening, incidence response and compliance initiatives.**

- Actively monitored events in near-real time through the ArcSight and Symantec MSS SIEM console.
- Designed and implemented global IDS/IPS deployment for Honda North America utilizing Fortinet, Palo Alto and Check Point Technologies IDS/IPS/NGFW.
- Scanned and monitored infrastructure and endpoint modifications for potential vulnerabilities via Qualys and Fortinet.
- Created and maintained Security Operations playbooks.
- Created and implemented SOC procedures for daily operations.
- Reviewed, analyzed, and approved exceptions to security policies or controls.
- Developed automated firewall configurations for Cisco ASA / Fortinet devices.
- Utilized McAfee A/V and DLP solution for Honda Global.
- Actively monitored events through Splunk, QRadar, Fortinet, Palo and Check Point.
- Tracked and remediated potential/verified malware, viral infections and malicious intent compromises throughout global network.
- Provided Security Analysis and best practice suggestions based on company need and budget.
- Managed projects and initiatives from concept to implementation for a ground-up security infrastructure.
- Documented and presented security data analysis findings and proposed preventative measures and any necessary remediation steps.

**Senior Security Engineer for a private military medical organization. Responsible for safeguarding corporate / military information assets across several key locations. Locations include March Air Reserve Base, Camp Pendleton, and Air Force Village West Medical Center. Also served as the Senior Engineer providing professional mentoring, design review, incident response, and advisory services for both military security team members and medical staff. Developed a forensic / testing lab for secure data encryption, transfer, handoff and process development.**

- Developed a strategic I.T. roadmap and enterprise technical architecture to prepare the organization for expansion.
- Utilized Brocade / Cisco network equipment for Air Force Village West's enterprise environment, creating and modifying VLAN's, Access Control List, CPAN, Monitor sessions and individual interface configurations.
- Designed, configured, implemented and maintained ESXi 4+ / VMWare HA / DR environment consisting of 15 physical and 20 VM servers for a 250-acre 400+ user network.
- Designed, configured, implemented and maintained SonicWall / Cisco ASA firewall with virtual contexts and IPS 4260/70 systems, including working site-to-site connections and load-balancing solutions.
- Conducted firmware and software upgrades to maintain Brocade/ Cisco ASA and IPS systems.
- Administered Cisco VOIP, Call Manager 4.0, 6.0 and 8.0, Unity 8.0 and 7900 series IP Phones.
- Provisioned and administered remote office wireless back-up solutions involving a combination of Cisco and LinkSys broadband routers and SonicWall VPN Tunnel appliances.
- Proficient with Cisco TelePresence MCU, C20, C60, MXP all-in-one, EX90 codecs and Polycom HDX 8000 and LifeSize Room video conferencing solutions.
- Designed, configured, implemented and maintained several long-term care software applications and databases for growing on-site medical facility.
- Proficient with equipment such as Cisco Catalyst 1900-3700 series, Catalyst 4006 and 6509(SUP II and III) Switches with IOS/CatOS and Cisco Aironet 802.x Wireless Access Points. VLAN configuration and management, Identifying and troubleshooting layer 1-3 connectivity issues.
- Utilized Barracuda and SonicWall web and SPAM filters to scan and trend traffic analysis to prevent transmission and infection of malware and viruses within the company LAN.
- Developed a process for secure data transfer and handoff with auditable checks and balances to verify data integrity and to secure end-to-end transfer traversing both digital and physical gateways.
- Provided end-to-end encryption validation for Exchange mail and secured file transfers and sensitive data handoff.
- Performed scheduled penetration tests to assure implemented security methodologies and practices are valid and up to date.
- Provided SIEM (Security information Event Management) analysis and reports to senior management and compliance personnel.
- Provided Intrusion Prevention Analysis and proactive management of network infrastructure and servers to prevent potential security issues before they become an issue.
- Performed Network Security and access list modifications, Pix ACL modifications, Pix syslog and monitoring, DMZ configuration.
- Conceptualized, designed and implemented DLP framework including appliances and procedures to prevent potential data loss or breaches.
- Performed continual data and web traffic analysis to predict and prevent security breaches and maintain performance standards based on user traffic and WAN to LAN data.
- Oversaw the management of project lifecycles through successfully facilitating working relationships between clients, partners and project teams.
- Provided remote assistance and local client help desk support as necessary.
- Provided quarterly training to management teams and the user community on new security standards and best practices.

## EDUCATION

**ITT Technical Institute** – Anaheim, CA

**Bachelor of Science:** Computer Science / Electronic Engineering

June 2004

**CAL ARTS** – Valencia, CA

**Associate of Arts:** Animation / Design

June 1998

**Cypress College** – Cypress, CA

**Associate of Science:** Computer Science

June 1994