***Dallas L. Stephens II***

**Dallas.Stephens2@gmail.com *● (480) 343-9077***

[***https://www.linkedin.com/in/dallasstephens***](https://www.linkedin.com/in/dallasstephens)

#### Global Enterprise IT Security Professional

Executive SummarY

IT Security Professional with 17 years of enterprise global experience ensuring integrity, confidentiality and availability of technology resources. Developed and demonstrated accelerated solutions to achieve IT risk reduction built on frameworks to improve performance with greater agility, confidence and clarity. Provided an enhanced security posture, resiliency and architectural strategy for all security domains and top twenty security controls to improve management controls. Developed and led innovative methods for best practice, SME guidance, knowledge transfers, and mentoring programs. Ensured regulatory compliance while delivering new processes to identify security gaps. Performed internal audits and assessments resulting in impact reduction to brand and reputation. Demonstrated ability to participate in multiple full project lifecycles simultaneously while assessing complex environments for infrastructure redesign. Provided heightened visibility to executive leadership while improving reporting functionality for SAS 65, SAS 70, SSAE 16, SOC 2 requirements. Planned, led and managed corporate compliance and operational effectiveness to ensure functionality of controls. Demonstrated ability to managing third party vendors, providers and partner relationships while reducing the introduction of third party risk.

Areas of Expertise

* Extensive knowledge and experience with: Windows, Unix, & Linux client/server enterprise architectures for multi-tiered domains including Cloud, IoT, AI & Deep Learning; Security Awareness Training; Executive Reporting; Policy Implementations; Tactical & Strategic objectives design, planning, metrics & automation; ROI Projections and Feasibility Studies; Security Auditing & Risk Management; Global Presence and Compliance Initiatives; Innovation in Disruptive Technologies
* End-to-End & Business-to-Business (E2E/B2B) Solution Provision; Identity & Access Management; VPN Remote Access Security Designing; NFS/SAN/NAS Management & Auditing; Disaster Recovery Planning; Mergers & Acquisitions; Real-Time Security Information Event Management; Network and Telephony system security; Penetration Testing; Secure Software Development Lifecycle (SSDLC); Network & Endpoint Protection Programs
* Management of Continuous Quality Improvement (CQI); Critical Success Factors (CSF); Key Performance Indicators (KPI); Critical Performance Factors (CPF); Standards, Policy & Procedure development; COBIT, ITIL & ISO Frameworks; Project Management and IT Governance
* Vulnerability Management programs including Scan Automation; Patch Management; Change Advisory Board (CAB) Management; Endpoint Hardening; Configuration Management & Maturation; Threat and Risk Assessments & Audits for compliance
* Intrusion Detection/Prevention Systems (IDS)/(IPS); Network Intrusion Detection (NIDS), Host Intrusion Prevention Systems (HIPS), Traffic Signature Development; Network Architecture Design; Virus outbreak response, DDoS Protection, Root Cause Analysis, Malware Forensics & Investigations; Incidence Response; Identification and Mitigation of new & existing attack vectors.
* Resource Planning & Management; Mentoring; Team Building; Business Security Design, Security Operations Center Design; Playbook/Run-book Design; Business-To-Technical liaison translating requirements into specifications; 3rd Party Vendor Management; Contractor & Provider management; Off-shore, Near-Shore and On-Shore resource management.

TechnicaL QUALIFICATIONS

* ***Operating Systems:*** NT - Server 2012; Unix *FreeBSD* 3.5 - Current, *AIX* 4.3 - 5L 5.3, *HP-UX* 9x-11x, *Solaris* 9.0 - 10; Linux *RedHat* 3.2 – 5E, *CentOS, Kali, BackTrack*, Ubuntu, Citrix, *VMWare*
* ***Protocols:*** Include but not limited to, SSH, FTP, Telnet, SMTP/POP, DNS, HTTP/HTTPS, ICMP, TCP/UDP, EIGRP, SOCKS, BGP, AH, OSPF, ARP, PPP, SNMP, IPv4, IPv6, etc.
* ***Networking:*** Exposure to multiple Cisco products including firewalls, routers and switches, configurations 1600, 1700, 2600, 3600, 5500/56050 series devices; Cisco Guards 5650; Cisco ISE for Network Access Controls; Juniper; F5 Load-Balancers; etc.
* ***IDS/IPS/NIPS, Endpoint &DDoS Protective Systems***: - Arbor’s Peakflow-SP, Peakflow-X & Peakflow TMS; Cisco Guards; SourceFire; FireEye; McAfee Product Suite ePO/HIPS/etc., Symantec Suite, Multiple DNS Solutions; Solarwinds; Snort/Barnyard/Suricata; HP TippingPoints; TrendMicro; ArcSight; RSA; Splunk; Nagios; OSSIM; CA Spectrum; Tanium; Bromium; Encase; BlueCoat; WebSense.
* ***PenTesting Applications:*** Multiple Pen-Testing tools on Kali/Backtrack (e.g. Yersinia, NMAP, hping, THC-Hydra, Metasploit & Meterpreter consoles, Nessus, Armitage, Burp Suite, etc.) Additional notable tools BinDiff; IDA; Olly; GDB; WinDbg; Immunity with plugins (e.g. Mona); Canvas; Core Impact; Borland Suite; Microsoft Visual Studios; AppScan; nCircle’s IP360; Qualys; WebSense; Systernals; EnCase; Multiple Fuzzers; Wireshark; Tripwire; VirusTotal; Fiddler; eEye Retina; Saint
* ***Operations Experience:*** Security Operations Center; Network Operations Center; Abuse; Fraud Prevention and Investigations; Incidence response handling; On-call rotations; Internal & External Investigations; Malware Analysis; Full lifecycle penetration testing and evaluations with associated report generation; Forensics; Root Cause Analysis; Azure Platform, Remediation of attack vectors; Risk and threat assessments; 0-day development (PoC) and mitigation; Updating or generation of new standards, Amazon Cloud; identification of network, appliance and application deficiencies, Compliance Planning & Testing; SharePoint Site Administration; Server New Build On-Boarding
* ***Telephony Experience:*** Avaya; Nortel; Cisco Call Manger; DFIR; DDoS protection & Scale Planning; Pen-Testing; Configuration & Policy Implementation
* ***Ticket Management:*** Remedy; Track-It; ESM; PAC2000; Peregrine; Service Now; Service Desk
* ***Programming and Scripting:*** Experience with SDLC processes & procedures; Sprints; Prototyping MS Visual Studios; Borland; Bloodshed C; Python; Ruby; HTML, JavaScript, CSS, and PHP; Shell Scripting

PROFESSIONAL EXPERIENCE

*CEMSol OCT 2016 - Current – CHIEF INFORMATION SECURITY OFFICER (CISO)*

* Ensure organization meets, exceeds & maintains GSA (Government Services Administration) requirements to obtain GSA award; Ensure additional Federal mandates are achieved
* Oversee & participate in review, assessment & analysis of Federal solicitations for Cyber Security Services; Assemble RFQ, RFI or RFP (Proposals) to reflect organizational capabilities; Ensure delivery of Cyber Security Services for all Federal contracts
* Ensure human capital and resources are delivered to maintain project timelines, milestones & goals; Provide organizational assurance of project viability; Ensure data privacy; Oversee & manage organizational and project documentation needs
* Ensure critical controls are established and maintained to achieve compliance while overseeing Identity & Access Management; Maintain strong endpoint and network security standards.
* Oversee project security architecture; Ensure oversight of electronic discovery and digital forensics is maintained while maintaining a CIRT (Critical Incident Response Team); Consult with peer and executive stakeholders to ensure Business Continuity Plan is maintained;

*SAIFE Inc OCT 2015- OCT 2016 – CHIEF INFORMATION SECURITY OFFICER (CISO)*

* Designed, defined, implemented and executed a company-wide security philosophy with associated supporting principals, policies, standards, procedures and guidelines; Ensure critical controls are established to achieve compliance with all applicable federal regulations.
* Oversee regulatory compliance efforts (e.g. SOX, GLBA, HIPAA, FISMA, CISP or PCI-DSS, etc.) while achieving ISO/IEC 27001, SOC 2 Type 2 and HiTrust certifications implementing best practices (e.g. NIST, ISO, etc.)
* Establish relationships with 3rd party consulting agencies while negotiating contractual agreements (e.g. KPMG, E&Y, Deloitte, PwC, etc.) to leverage services professional services for assurance.
* Ensure all IT Security strategic plans are developed and designed to mature security CMMI levels; Supervise all IT Security management personnel and provide leadership, direction and mentoring.
* Meet with various stakeholders to ensure IT Security department is aligned to business direction to further streamline cost and maximize risk buy-down
* Join internal sales force teams to meet with consumers, which promote broader security for both organizations while improving pipeline flow and maturing relationship with Law Enforcement channels.
* Produce 5 year financial forecast for CapEx / OpEx to account for program’s full cost, budget management and justification, potential TCO and ROI, ALE, while scaling for DR, BCP, Inventory as it relates to implementation and maturation
* Provided oversight, direction and approvals for Business Impact Analysis, Change Management, Architectural Changes, Firewalls, WAN/LAN, Endpoints, IDS/IPS, IR/SOC teams

***NIKE INC. JAN 2015 – OCT 2015 – EXPERT IT SECURITY ARCHITECT***

* Provide effective oversight and direction to Nike’s security capabilities requirements while being technology agnostic; Meet with various stakeholders, including executive, to ensure goals are achieved by baselining current environment and forecasting/directing engagement efforts to align security demands with business direction ultimately providing levels of acceptable risk
* Partner with internal teams to develop solutions and operation models through management of internal and external resources while analyzing, developing and supporting the implementation/maintenance of security strategies
* Establish and maintain enterprise IT Security standards through policy, architecture and training processes while ensuring comprehensive brand protection.
* Collaborate with IT Staff, Nike business leaders and external partners to ensure efforts are effective while ensuring the efforts are efficient, measureable and produce value added metrics.
* Ensure countermeasures are implemented in accordance to industry best practice, company standards and regulatory compliance requirements; Provide guidance to engineering and support teams on security risk while understanding effectiveness of security policies and technologies.

*Visa JAN 2013- DEC 2014 – GIS Controls Management*

* Conduct reviews of Ethical Hacks in relation to internally and externally hosted environments & applications; Manage consultants & professional services for multiple enhancement projects; Review new product offerings & identify security strengths and weaknesses.
* Design processes, documents and standards for organizational improvements; Improve analysis and reporting with cross team education; Training and Awareness program development assistance; Function/methodology and strategy advancement.
* Plan and direct significant project, product, service and functional requirements by management resources within functional areas; improve existing work processes to achieve business goals, define business security requirements for Global Information Systems;
* Support and consult multiple adjacent projects such as DDoS protection design/improvements, SSDLC, optimization, determine and perform testing and reporting through expert techniques of any given subject in fast-paced and highly technical environment,
* Troubleshooting of network appliances & disruptions; Automation of environment’s operations, Daily report generation; HIPS rules development; Document and Procedure development, Operational improvement engagements.
* Virus infection response; Cross-Team support for AD and VPN account management; new build security auditing for pre-deployment. Environment software & hardware implementation, hardening and upgrading, administration & support.

*RSA/EMC JUL 2012 – DEC 2012 - Director of IT Security – SOC ManAGER*

* Design RSA’s new MSS Security Operations Center in Scottsdale, AZ to facilitate the handling of all global Enterprise and Commercial accounts and USA (commercial only) security monitoring. Including selection of materials, colors, sound dampening surfaces, low-shine flooring, imagery for controlled environment, lowering EMI, bulletproof glass, and improved lighting effects for enhanced staff alertness (Physical Security).
* Provide coverage, leadership and mentorship to direct reports for all 10 domains and 20 critical controls. Train direct reports for improved production in relation to Envision, NetWitness, DLP, and Archer. Provide leadership to improve employee skillset of event and incident handling, log monitoring, vulnerability scanning, compliance monitoring, while improving customer service, experience and communications.
* Improve SOC’s analytical skillset while improving security architecture design concepts. Improve change management programs; increase incident management workflows while reducing bottlenecks. Create internal focus groups to improve general knowledge of industry regulations. Improve handling of customer compliance concerns (e.g. PCI, SOX, and HIPPA).
* Manage multi-faceted integration projects, Metrics generation, analysis and risk management, define and generate next-gen run-books, leverage existing frameworks while integrating new technologies or concepts, manage virtual teams while improving standards, processes and policies, develop next-gen architecture built to custom specifications
* Conduct quarterly reviews. Schedule monthly team meetings \* weekly meetings with leads. Ensure 24x7 \* 365 coverage for MSSP customers.

*GoDaddy, LLC SEP 2010 – JUL 2012 – SOC Analyst*

* Security Domains: All 10 domains are covered as a security analyst.
* Global Security Operations Center for cloud provider. Processing & reviewing over 100,000 security events per second in 24x7 environment including: Monitor, Analyze and Resolve Security Incidence, DDoS & Flood mitigation; Review for Indicators of Compromise, Investigations of compromised servers; Malware analysis.
* Troubleshooting of network appliances & disruptions; Automation of environment’s operations, Daily report generation; Identify and resolve IDS, IPS, HIPS problems and rules; AV and Digital Signature improvement, Document and Procedure development, Operational improvement engagements.
* Virus response; Special APT investigation and defense, Cross-Team support for AD and VPN account management; New build security development, auditing and deployment, Environmental Hardening, Bastion maintenance and upgrading, administration & support.

*American Express – MAR 2009 – SEP 2010 - Internet Security Analyst*

* Global security operations center lead for enterprise antivirus solutions; Security Infrastructure re-engineering; Development of real-time reporting sites; SharePoint site administration; Process and documentation development (white papers); Incidence response in 24x7 on-call support environment; Policy design; Automation of auditing processes, Network device configuration & patch audits.
* Vulnerability Management Program (VMP) establishing on-boarding processes of new builds; Full internal vulnerability risk assessment & review; Analysis & scoring of each business unit’s security awareness/posture/adherence to standards; Development of PCI-DSS compliance standards which are used internationally; External penetration testing analysis; Manual security assessments.
* False-Positive, patch supersedence, and adherence for Windows, Linux & UNIX environments; Configuration assessments for all OS environments, Cross-team mentoring and training.
* Re-engineering of vulnerability management programs to generate increase work flow, Identify and remove duplication of efforts, streamline auditing operations; automate remediation; improve internal communications with partner channels to lower overall risk scores & improve visibility to leadership.
* Review & establish new IT security standards to further promote security rating pertaining to PII and Section 404 of SOX;

*Wells Fargo OCT 2008-MAR 2009 - Systems Analyst/Integration Developer*

* Security Domains include: Application and Security Development, Access Control, Security Architecture, Network Security, Computer Operations Security, Physical Security, Cryptography, BCP and DRP.
* Support and monitor Corporate Investment infrastructure; Provide monitoring and security for International Business Sales in existing Machine-to-Machine (M2M) transactions & File Upload Services (FUS); Monitor and respond to financial transactional systems alerts on Unix/Windows environments; Develop in webMethods Integration environment; Monitor real-time transactions for Fraud, Hacks, Viruses or other malicious activity; Automate multi-layered application systems scanning process; Detect brute-force incidence & facilitate response teams; Root cause analysis.
* Document & define platform parameters; Establish & streamline processes for recovering lost transaction data; QA testing to ensure compliance to SOX; Coordinate F5 & DNS team efforts for planned outages & updates; Analysis & monitoring report generation.
* Incidence response to internal & external threats while generating trending reports that operate on an advanced model for forecasting server & network failure of 24x7 environment; Centralized log management; Custom inventory tracking development; Internal process and associated white papers design; In-house software tracking through the CVS.
* Monitoring & tracking of partner certificates; Improve security posture through role enhancements; Improve functionality of internal WIKI & SharePoint site.

*AVNET JAN 2006 – OCT 2008 - security Analyst-Integration developer-Desktop Support*

* Remediation of nodes identified to be outside security thresholds; Security Incidence response including attacks and system failures of integration systems; Penetration of rogue systems; Network Management and disabling of newly discovered rogue devices; Enterprise antivirus solutions and virus incidence response.
* Remediation of global clients endpoints; Local & Global policy design assistance, Compliance validation; Feasibility studies; 3rd party product analysis; Development of security automation tools; Incidence response to Cisco PIX & Nokia firewalls alerts; Trending analysis; Virus & Spyware deobfuscation; Desktop support for Blue Team/Red Team assignments.
* Custom patch development for internal software containing buffer overflows, out-of-bound-arrays & dated systems compatibility issues; Improved existing systems through KPIs & CPFs (Key Performance Indicators & Critical Performance Factors); Software true-ups for vendor licensing agreements.
* Support, assist and mentor enterprise users on software applications; Assist in storage solutions & disaster recovery efforts; Implementation of enterprise automation; SOX compliance testing; Digital certificate management; Backup & purge routine process definition; Internal Wiki development; Data repository standards definitions & development
* Support Windows, Unix & Linux for webMethods installation, configurations, administration, troubleshooting & security for integration processing of $6B annually in global transaction, SharePoint site administration, DNS/Bind administration; IP scoping and assignment, Clustering
* Defining server parameters; Shell scripting; Account administration; User right assignments & access controls; HP OpenView integration; Operations statistics and analysis; Change advisory board (CAB) reviews; Production deployment of services, patches, hot fixes & in-house code enhancement.
* Software rollout planning & implementation; Leap & EAP-FAST wireless implementation assistance; Corporate integration of Sprint telecommunications solutions; Splunk; Technical liaison for Avnet Executive Care

*AVNET Memec DEC 2004 - DEC 2005 - GIS SUPPORT SPECIALIST & Security Analyst*

* Resolve a broad-spectrum of issues with an emphasis on WAN/LAN administration & security technologies; Configuration, Administration and Security of multiple Cisco devices, Sun Blades like Sun Fire V210 Servers, Compaq Proliant 6500 series servers, End-User PC & Laptops; Migration Project Management from Memec to Avnet; Bridge technological gaps between internal systems requirements & external business needs; Developing process improvements to increase work flow.
* Develop & improve network security across all segments; Support DHCP, DNS, Email, Active Directory servers; Provide analytical reporting of performance while introducing models for securing overall architecture; Windows & Unix shell scripting; Co-develop triggered event handling & response.
* Develop company programs in advanced engineering’s proprietary 16 & 32-bit applications with proprietary high-level languages. Security monitoring & system event response handling.
* Develop advanced hardware controls bridged through existing USB & Bluetooth technologies; Translate existing technical documentation combined with manufacture’s specifications for standard ISO 9001 formatting; Infrastructure security logging & response with HP OpenView.

*IBM Jan 2003-NOV 2004 - BAND 3 Systems Specialist*

* Virus&Trojan Response; Custom patch development; Protocol auditing; Develop and implement systems and infrastructure configuration; Full lifecycle pen-testing; Remediation of compromised nodes; root cause analyze & diagnose of device failures; Develop new & update existing Hardware**/**Software of embedded systems.
* R &D (Research & Development) of advanced technology Washington Mutual proprietary applications; Unix Shell Scripting; C/C++ programming, Windows batch & VB scripting.
* Desktop and Server support for IBM contract to Honeywell Aerospace; Support and direction of documents on contractual agreements; Patches; Remediate custom login scripts; Deployment of new Workstations on IBM, Dell and Compaq hardware; Implementation for asset tracking and control solutions for IBM and Honeywell partnership.
* Maintain IBM repair and remediation processes documents; Provide data recovery solutions as needed; Break-Fix operations for end-users; Shell scripting and development of USB technology for deployment; Rollout updates and patches for end-users.

*Wells Fargo Private Client SERVICES Jan 2001- DeC 2002 - LEAD Analyst*

* Support Lead for internal break/fix operations of desktop support & migration; Maintain excellent verbal & written communication skills by reporting to leadership; Troubleshoot existing Exchange, DNS & Proxy servers as needed for network clients.
* Lead team of eight for migration project of Wells Fargo Private Client Services assets to new NOVO platform; Charter validation efforts to verify all software & hardware migration; ensure properly functionality of new systems.
* Learn & Support a blend of banking software used such as: Baseline, Proprietary Databases, ILX-BETALINK, Customer Stratification, Market Link to support Norwest Integrated Structured Asset Corporation (NASCOR), instruct and lead users on security methodology and best practices.

**EDUCATION**

|  |  |
| --- | --- |
| ***Institution*** | ***Course*** |
| **UEI** | Computer Science Networking Technology |
| **United States Army** | Military Police Officer - Fort McClellan, AL |

**EXAMPLE OF PROFESSIONAL TRAINING & EXPERIENCE**

|  |  |
| --- | --- |
| ***Organization*** | ***Course*** |
| **SANS** | 660 GXPN – Advanced Exploit Research & Development |
| **SANS** | 560 GPEN – Network Penetration Testing & Ethical Hacking – Placed 1st in Washington D.C. hacking competition. Achieved 560 Coin |
| **Veris Group** | Adaptive Red Team Tactics (Penetration Testing) |
| **ISC2** | CISSP #423514 |
| **EC-Council** | CEH |

**INTEREST**

|  |  |
| --- | --- |
| **Interest** | Baseball, Football, Rock Climbing, Cross-Fit, Scuba Diving, MMA |
| **Security Interest** | Offensive Security & SANS Training, DefCon, Toorcon. BlackHat |

**REFERENCES**

|  |  |
| --- | --- |
| **References** | Available upon request |



Dallas L. Stephens, CISSP

480-343-9077

[***https://www.linkedin.com/in/dallasstephens***](https://www.linkedin.com/in/dallasstephens)