John Stewart

608.729.4572
MadisonComputerGeek@gmail.com

Skills Summary

I am the wizard behind the curtain. With an ability to quickly understand a complex issue and manage a multidisciplinary team, I can expertly manage a crisis. With over twenty years of experience in all areas of information technology, I am able to prevent a crisis from happening at all. I have a GSEC certification and a security focus but have a very broad background and am an IT generalist at heart. My experience in understanding the larger picture and my ability to effectively communicate with people at all levels of technical expertise make me an indispensable asset in a complex environment.

Core Technical Competencies

Security / GIAC Security Essentials (GSEC) Certified, Cisco ASA and IDS/IPS, VPN: Cisco AnyConnect, Cisco S2S, OpenVPN, Cisco Access Control Server, Rapid7 Nexpose and Metasploit, PKI, SSL, Windows Certificate Authority, Kaspersky, Symantec, SAML, ADFS, KnowBe4, Compliance: WISP, PCI, GDPR

OS / Windows: NT4, 2000, 2003, 2008, 2012, 2016, Linux: RedHat, CentOS, Ubuntu, FreeBSD, Solaris 2.5.1–10, VMware ESXi, Cisco: CatOS, IOS, ASA, Mac OS X, iOS

Network / Cisco, EIGRP, LAN, WAN, free space optical, LAN wireless, switching, routing (static/dynamic/policy based), VPN, MPLS, GRE, QoS, Nexus, Splunk, WhatsUp Gold, SNMP, WMI

Microsoft / Windows (NT4, 2000, 2003, 2008, 2012, 2016, XP, 7, 10), Active Directory, Group Policy, DNS, SMS/SCCM, Lync/Skype for Business, Sharepoint, Office 365

Cloud / AWS, EC2, Route53, S3, Glacier, VPC, Azure, O365, Rackspace

Collaboration / WebEx, Zoom, GoToMeeting, LifeSize, MOVEit DMZ/Transfer

DNS / ISC BIND, Windows Active Directory, split horizon, MarkMonitor, Route 53

Firewall / Cisco ASA, Check Point, Palo Alto, Juniper, VMware NSX, AWS VPC

Helpdesk / Service Now, ITIL, Change Management

Languages / Perl, bash/sh/csh/ksh scripting, PowerShell, expect, PHP, Objective-C

Mail / Exchange, Sendmail, Postfix, IMail, SpamAssassin, Postini, Google Apps/G Suite, Office 365, SPF, DKIM, DMARC

Phone / Cisco CallManager, Cisco Unity, unified messaging, ThinkingPhones/Fuze

SIEM / Splunk, NetWitness, QRadar, InsightIDR

Storage / NetApp, Equallogic, Nimble, Sun, Samba, DLT, LTO, iSCSI, FC, S3, Glacier

Virtualization / VMware VCP, ESX, ESXi, vCenter, Veeam, vRA, Xen, EC2

Web / Apache, IIS, Tomcat, PHP, Perl, mySQL, Wordpress, Service Now, AWS, Hugo

Wireless / Cisco LWAPP Controllers and WAPs, WPA2, 802.1x

Employment

Senior Security Operations Engineer
Madison Gas and Electric – Madison / April 2018 – present

- Provide technical expertise and protection of assets by reviewing, analyzing, and implementing security controls, functions, tool sets, and processes to allow for a secure, robust, and reliable environment.
- Administer firewalls, SIEM systems, and endpoint protection.
- Perform security assessments for new technologies and applications.
- Analyze and migrate audit reports, triggers, and rules from IBM QRadar to RSA NetWitness.
- As member of the blue team during Dark Sky security exercise in May 2018, collaborated with MG&E security operations colleagues, other IT team members, and military personnel. Performed threat hunting utilizing RSA NetWitness suite. As Palo Alto SME, performed all firewall operations for the network team.

Software Architect
Madison Computer Geek – Madison / October 2017 – April 2018

- Build a multi-platform iOS application utilizing Xcode and native Apple APIs including SpriteKit, Core Data persistent storage backed with SQL Lite database, iCloud integration, and Game Center online multiplayer capability.

Director of Infrastructure and Security
Ipswitch - Madison, WI / December 2014 – October 2017

- Led a multi-site cross-functional team supporting IT Infrastructure, including helpdesk operations, network, security, Active Directory, and central applications.
- Monitored security news. Processed alerts from vendors, CERT, SANS, MITRE, and other security organizations. Determined risk to Ipswitch systems and remediated high risk threats.
- Led incident response for breaches and outages; performed root cause analysis.
- Managed domain names, registrars, SSL certificates, and nameservers.
- Responded to vendor security assessments about IT processes and security posture.
- Built extranet connections to partners via S2S VPN; limited and managed allowed access.
- Built a vulnerability scanning and remediation program based on Rapid7's Nexpose scanning suite, with weekly scans and ongoing remediations. Reported monthly to security council and management. Proposed and implemented changes to improve security posture.
- Deployed company-wide security training with ongoing testing to determine user susceptibility, resulting in 75% reduction in responses to phishing over 3 months.
- Designed and built an offline root certification authority infrastructure, with automatic deployment of user identity certificates via group policy.
- Designed, built, and deployed a certificate-based two-factor authentication (2FA) system utilizing existing Cisco ASA firewalls and Windows AD/group policy infrastructure.
- Built a centralized syslog server, gathering critical logs from all network devices.
- Incorporated AWS based download infrastructure into IT patching and remediation regime.

IT Manager
Ipswitch - Madison, WI / January 2012 - December 2014

- Senior technologist, analyzing business requirements and evaluating technologies.
- Mentored, educated, and developed junior staff.
- Deployed VM-level backups across all production VMware clusters.

Senior Network Administrator
Ipswitch - Madison, WI / March 2010 - January 2012

- Supported all local IT needs for Madison Ipswitch office.
- Acted as technical lead for network, security, and VMware for all Ipswitch sites.
- In 2010, integrated acquired company's existing infrastructure into Ipswitch.
- Led technical team to move headquarters to new site with minimal downtime for servers and systems upon which all users globally depend.

Network Engineer
Eragen Biosciences - Madison, WI / October 2009 - March 2010

- Managed all IT infrastructure for privately held biotech firm.
- Ensured proper access control to meet applicable FDA standards.
- Managed and assisted helpdesk staff in providing end user support.

Senior Technical Specialist
Emerson Network Power - Madison, WI / May 1995 - September 2009

- Developed, implemented, and maintained infrastructure for growing telecommunications engineering and manufacturing firm, including network, servers, security, and AD.
- After company acquisition, led project to integrate legacy Active Directory domain and Exchange infrastructure into larger corporate forest.
- Designed and implemented secure wireless infrastructure in three sites and two countries based on Cisco LWAPP technology, integrating into Active Directory using Cisco ACS.

System Administrator/Programmer
Computer Systems Lab, University of Wisconsin–Madison, Madison, WI / Nov 1993 - Aug 1995

Education & Training

B.S. in Computer Science, University of Wisconsin–Madison, May 1995

GIAC Security Essentials, June 2017

Nexpose Certified Administrator, July 2016

VMware Certified Professional, August 2007

System and Network Security Conferences (SANS) 1997, 1998