Paul E. Williams

16835 Albers Pointe Ct.

Florissant, MO 63034

(314) 518-9074

[pwill\_66@yahoo.com](mailto:pwill_66@yahoo.com)

**PROFESSIONAL SUMMARY**

An IT professional with over 20 years of proven experience in a wide range of technologies. Experience includes Information Systems Security governance and compliance, networking, technical support, switch and router configuration, Active Directory management, DHCP, DNS, and WINS management, system migration, software management, packaging, and deployment. I have implemented and administered Windows 2000 Active Directory infrastructure with domain controllers running DNS and DHCP. I have monitored the firewall of Zone Alarm for servers, laptops, and desktop systems. I have also monitored our exchange e-mail servers using Barracuda to filter and detect unwanted e-mail traffic.

###### EDUCATION

**Bachelors of Science Dillard University** - New Orleans, LA

Major: Mathematics/Physics / Minor: Computer Science

**Professional Experience**

**Federal Reserve Bank (contractor) –** St. Louis, Mo **May 2016 – Present**

Information Security Analyst/ Engineer

* Manage Security, Test, and Evaluation (ST&E) on production and integration systems by performing remediation efforts, collecting enterprise information, tracking plan of action and milestones, and building residual risk reports, knowledge of published security standards (ISO, NIST)
* Performed risk assessments on software, web applications, and other tools used.
* Draft remediation guidance and implement information assurance best practices to restore affected systems.
* In the assessment process tested, and evaluated he items and tested against the security controls and gave the evaluations best on the performance on those controls.
* Identify security risks and exposure by participating in security reviews and risk assessments
* Tested for vulnerabilities and drafted documents for review and to address any and all issues.
* Presented documentation on the findings presented to potential owners and gave the evaluation and risk factors.
* Once the risk factors have been review and accepted any remediation where addressed and tested and continuous monitoring was done.
* Monitored and addressed vulnerabilities in the network.
* Applied SAFR policies to all systems that were assessed.
* Made recommendations from the data gathered on the Matrixes on the level of the risk for KPI.
* Perform risk analysis of applications and appliances being used in our environments using the standards of FISMA in conjunction with the compliance of NIST 800-53 that all security controls are addressed and recommendations of the risk levels are reported to the business owners.

**US Bank –** St. Louis, MO **August 2007 – November 2015**

Information Security Engineer / Information Security Compliance and Governance Specialist

* Manage Security, Test, and Evaluation (ST&E) on production and integration systems by performing remediation efforts, collecting enterprise information, tracking plan of action and milestones, and building residual risk reports, knowledge of published security standards (ISO, SOX, PCI and some NIST)
* Participate in external/third party vendor security audits and risk assessments and supported third party tools such as Quest and Password Vault.
* Ensure standards are being implemented to secure personal information and data is secure during the process of using PCI and making sure that we stay up[ to date with the processes and monitor any unusual activity and once notice take immediate action.
* Identify security risks and exposure by participating in security reviews and risk assessments
* Monitor a large farm of servers in multi-geographical locations.
* Review security logs and assessed any unusual and malicious activity.
* Make contact with vendors access to our network with access that may be considered a threat, an analysis has been written to document the vulnerability and suggestions on how to remediate it meeting the SOX standards.
* Identify and resolve configuration issues on all our servers.
* Manage projects and people in the remediation process and the deployment of the required access. Use numerous automation tools to deploy and remove permissions needed.
* Support the IP network infrastructure of the company.
* Troubleshoot any malfunctions of network hardware and software applications.
* Draft remediation guidance and implement information assurance best practices to restore affected systems.
* Conduct information assurance safety briefs to 250+ personnel during annual personnel training.
* Perform server design, installation, and maintenance for clients, ensuring all systems installed according to schedule and within scope of budget.
* Conduct dynamic analysis by collecting and analyzing threat intelligence to ensure secure data transmission between classified systems.
* Maintain scripts used to generate reports for access on servers and databases.
* Experience in scoping, designing, developing, and supporting enterprise scale business applications and business intelligence software for the company.
* Administer and maintain user's access to applications Active Directory.
* **Governance/ Compliance** – review application and database access look at the access models and entitlements and make recommendations to the application owners and database administrators on how to make their application compliant. Follow up with audit reviews to make sure compliance is still maintained.
* Place users in their appropriate Enterprise Role for the correct access upon validation of their credentials.
* Extensive use of Active Directory to manage user accounts, groups, and make sure the users are placed in the correct SAP group.
* Present Business partners with risk factors of any applications brought to the company’s network environment, and what effects could happen if brought into production.
* Develop and implement security solutions to help secure the enterprise as technology and applications are introduced into the web environment
* Create and update solution documentation, which may include procedure documentation, and US Bank technical documentation. This may include risks and proposed recommendations of actions needed to mitigate these risks. Once the solutions document is completed it is then sent to our Audit team for review.
* Work directly with vendors, developers, and Data Base Administrators to identify, report or resolve any security issues.
* Assist with planning, scheduling, and staffing for work efforts and resources.

**State Farm Insurance (PDS) -** Bloomington, IL **April 2007 - August 2007**

Network Security Analyst / Administrator

* Administer and maintain user's access to applications Active Directory.
* Create Domain Logical Groups and Global groups for the appropriate SQL .net and non-.net databases and gave proper permissions to the member and authorizers of the Databases.
* Create and maintained VB Scripts for the appropriate procedures for the SQL server database to initiate.
* Edit VB scripts and FTP scripts to comply for the needs of the process they are used for.
* Create accounts and make sure they go to the appropriate OU’s with the company.
* Nest the DLG (Domain Local Groups) to the appropriate Global Groups.
* Extensive use of Active Directory to manage user accounts, groups, and computers and make sure the users is placed in the correct OU group policy.
* Monitor Intrusion Detection with the State Farm Network.
* Present Business partners with risk factors of any applications brought to the company’s network environment, and what effects could happen if brought into production.
* Assist in identifying security exposures, risks, issues, requirements, or impacts for web applications.
* Recommend, select, and implement proper information security controls. Develop, recommend, and author security policies and procedures.
* Develop and implement security solutions to help secure the enterprise as technology and applications are introduced into the web environment.
* Create or update solution documentation that may include procedure documentation, and State Farm technical documentation. This may include risks and proposed recommendations of actions needed to mitigate these risks.
* Work with business partners to perform security risk analysis, compose documentation of security risks, and proposed recommendations of actions needed to mitigate these risks.
* Work with project team to thoroughly understand the business needs being addressed and create security solutions that align with State Farm Technical Architecture.
* Navigate and apply Systems' and Security's structure and processes.
* Assist and/or advise business partners on critical design decisions and production implementations within each Enterprise Initiative.
* Review and/or create appropriate team deliverables. (training plan, walkthroughs, topics of discussion, etc)
* Assist business partners and auditing with consulting and reports as needed for the web environments.
* Create, update and utilize specialty security tools.
* Monitor and resolve HP Service desk production calls and issues.
* Work directly with vendors to identify report or resolve any security issues.
* Assist with planning, scheduling, and staffing for work efforts and resources.
* Present documentation in the meetings on my findings and recommendations to make our processes more efficient.

**Citi Group (TEK Systems)** - St. Louis, MO **September 2006 – March 2007**

Network Systems Security Administrator

* Administer and maintain user's access to applications both on Novell and Active Directory.
* Give rights to the user of the appropriate groups requested.
* Create Novell and Active Directory accounts if needed, create user's e-mail account and grant access to Citrix applications.
* Assist in moving some of the application from the Novell environment to Windows environment.
* Implement security policies on the users for a more secured environment.
* Extensive use of Active Directory for managing the Domain Controllers, PC’s and users accounts under the different Domains for their environment.
* Implement policies on workstations for a more secure network environment.
* Administer Microsoft Windows Security and Event logs with the use of Microsoft monitoring tools. (Active Directory).
* Implementation of application software groups to user profiles using a tool called Quick Complete.
* Monitor intrusion detection from outside our environment and making note of it and documenting it, governing, and maintaining the Internet policies placed in environment and make sure they are enforced.

.

**Ameren Energy Trading /Ameren UE** - St. Louis, MO **May 2000- June 2006**

Network Administrator / System Specialist/ Exchange Administrator

* Install Exchange Server 2003, 2000 and 5.5 on multiple servers and implemented ghost images of Windows NT workstation.
* Manage Active Directory to insure the policies within our company to guarantee usage of our e-mail system and that the firewalls properly blocked SPAM mail.
* Implement policies to give notification of attachments coming in from outside e-mail address. Advise members on my team the implementation of the policies for of e-mail accounts using the Active Directory tool with the exchange server. Instill in my team to perform maintenance and ensure backups are done and scheduled nightly.
* Install Security policies on users to limit their access to their C drive and allow access to a home network drive we assigned for them.
* Create polices in which no user is allowed to run any software (exe) that has not been tested and approved by our department.
* Make sure the users adhere to the policies and structure of the company.
* Watch for intrusions alerts coming through our firewalls
* Create User accounts in Active Directory and when user’s change positions or titles place them in the OU in which their position calls for.
* Lock down servers to insure security in our environment from viruses and hackers as much as possible.
* Use Active Directory Windows 2003 setup OU’s for the users according to the department and the policies in which they needed to be set up for.
* Software testing and packaged software in Wise format and pushed the software to our user PC anonymously. Also, package software in the same Wise format for implementation to be pushed through RADIA (novadigm). Write documentation for error messages on how to remedy the problems that may occur.
* Assist in and manage the upgrade from Windows NT 4.0 to Windows XP upgrade for the users at our head quarters and our other locations.
* Manage the Cluster Server to enable resources to be shared by other branches within the organization. Implement Routing messages between routing groups.
* Manage and maintained DHCP with the scope of IP addresses using DCHP instead of the static IP address to eliminate the possibility of duplication of an IP address to our users.
* Maintain and managed over 700 Windows 2000 and 2003 servers. Responsible for server builds, service patches and service packs and Norton Antivirus definition updates. Perform troubleshooting with any issues that arise.
* Implement policies on workstations for a more secure network environment.
* Upgrade our Remedy application for better tracking of our services.
* Perform performance monitoring and tuning utilizing Zone Alarm monitoring tool to monitor incoming from the outside network and Web sense to govern the Internet sites utilized by the users. Utilize Legato to backup servers on a nightly basis on tape.
* Build Ghost images with my team for the PC’s at Ameren for more effectiveness in performance; time, and money savings to ensure down time will be very minimal for our users.
* DHCP implementation on our network to insure effectiveness and less IP address duplication for the PC’s being used by our users.
* Troubleshoot network and computer problems for our users and bring them back online in a timely fashion.
* Manage network and e-mail accounts to ensure security on our network.
* Manage Windows 2000 servers.
* Manage Active Directory use in Exchange 2000.
* Implement my team and performed disaster recovery task to optimize the usage and continuation of productivity.
* Assist in managing and setup of Blackberry accounts and the Blackberry’s for our users. Supported e-mail and messaging for the users of the Blackberry’s and their company e-mail accounts.

**United States Army** - Fort Hood, TX **March 1994 - April 2000**

Network Administrator (was required to hold a secret security clearance)

* Install on NT 4.0 and Exchange 5.5 Enterprise Server.
* Implement Routing messages between routing groups.
* Conduct dynamic analysis by collecting and analyzing threat intelligence to ensure secure data transmission between classified systems.
* Create disaster recovery continuity plans and oversee annual security assessment project testing system vulnerabilities.
* Manage team of five network security engineers monitoring 25-35 government and defense sector computer system networks.
* Oversaw team of 20+ personnel monitoring intrusion detection and security information management for Army information systems and networks.
* Conduct analysis of computer security advisories, current network penetration techniques, and military intelligence threat reports.
* Plan and organize testing against networks and information systems to uncover potential security deficiencies.
* Design and integrate custom rules and reports into military security tools and data collection architectures.
* Set-up and maintain Windows NT LAN/WAN that supports over 900 clients.
* Set-up, manage, upgrade, and maintain over 200 Windows NT servers. Apply any patches that were needed to make our network environment run more efficiently.
* Convert from static IP addresses to a scope of IP address using DCHP.
* Manage network and e-mail accounts to ensure the highest level of system security.
* Install and set-up Microsoft Mail Server and Client applications to enable data/file sharing.
* Integrate TCP/IP, NETBEUI, NETBIOS, DHCP protocols to support WANs.
* Configure CISCO routers and switches for LANs/WANs.
* Manage Windows NT 4.0 servers in both office and tactical field exercise environments.
* Understand and perform fault tolerance, disaster recovery, and optimizing/tuning/troubleshooting tasks for Windows NT networks.
* Install and configure network cards.

Software Analyst

* Write, modify, debug, and update programs in ADA.
* Write programs using other languages such as COBOL, JCL, and C++.
* Install Novell, Windows NT/95/98, and LAN network systems.
* Configure PC's to the specified needs of the user.
* Support and maintain internet website and e-mail administration.
* Provide technical support to clients, and talk users through recovery procedures from application errors they encounter.
* Maintain and troubleshoot databases.