CTO/Head of Security CTO/Head of Security Security Consultant Denver, CO Andy is a seasoned "hands on" Sr. Technology Manger whom has over 20 years in IT whom held multiple positions from the bottom up. Andy is a visionary that is proficient in leading technical programs and departments. He has provided leading ship to STAR and established the company's technical vision and leads all aspects of the company's technological development. Andy has designed leveraged merging technologies with Cloud and Hybrid services to give companies like Thyssen Krupp the managed security solution to stay ahead threats, reduce risks and stay competitive. He specializes in creating Security Programs using best practices from NIST 800. As the "Face of Security" as he held a position on the Security Council. At GDIT was a key leader in the security the OMNI Cloud program (Federal and Non Federal Cloud Provider) obtain FedRAMP certification by developing processes and checklists for security controls. Andy has a special ability to use multiple languages to create High Level Views that are important to Stake holders and possesses the detail hands-on skills to configure the tools necessary for a mature Security Network Enterprise Architecture. Andy brings over eleven years of management experience working with inter agency teams to design, develop and implement FISMA compliant solutions that meet current and future business requirements and enhance and optimize the existing security architecture. Work Experience CTO/Head of Security STAR, LLC - Littleton, CO January 2019 to Present Responsible for providing leadership to department heads in a fashion that supports the company's culture, mission and values. Directs the company's strategic direction, development and future growth. Works collaboratively with corporate compliance, internal auditing, corporate risk management, corporate security, regulatory bodies and authorities and various technical teams in the design and implementation of audit, security/compliance assessment, and regulatory security/compliance practices of IT. Advises IT and business executives on the status of IT Security and Compliance issues based on assessment results and information from various monitoring and control systems. Oversees the monitoring of network, systems, and logs to ensure availability and security of all systems and facilitates internal security assessments of all new and existing technology, processes, systems, and projects. Lead and build multiple teams of STAR security services that are focused on asset identification, vulnerability management, red team, penetration testing and security product & engineering. Establish the company's technical vision and leads all aspects of the company's technological development. Works in a consultative fashion with other department heads, such as marketing, production and operations as an advisor of technologies that may improve their efficiency and effectiveness. Provides leadership to department heads in a fashion that supports the company's culture, mission and values. Conducts research and case studies on leading edge technologies and makes determinations on the probability of implementation. Determines security requirements by evaluating business strategies and requirements; information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates. Develop, maintain, review and improve strategic company-wide security programs to keep the company from cyber-threats and to protect digital assets. Constantly update the cyber security strategy to leverage new technology and threat information. Ensures ~~~~~~~~~ compliance with laws and applicable regulations. Brief management on status and risks, including taking the role for the overall strategy and necessary budget. Continuously communicate best practices and risks to all parts of the business, outside IT. Approves SOW for Technical related projects Sr. Global Security Consultant NCUA - Denver, CO September 2018 to December 2018 Architect, test and certify full-stack private and public cloud infrastructure including AWS and FlexPod (Cisco Cloud) application solutions to meet diverse and complex business opportunities. Provide advanced technical leadership in research, design, analysis, testing and problem-solving efforts to the SDN/NFV products and services. Architect customers' requirements for End-to-End Orchestration, Service Assurance, Virtual Infrastructure, and Cloud Responsible for design, development, and hands-on implementation of Amazon Web Services cloud solutions Served as an AWS technical resource in team's efforts to determine the needs of our clients. Participated in planning, implementation, and growth of customer's AWS foundational footprint Designed business solutions using Palo Alto Networks VMSeries (VMware Cloud) virtualized next generation firewalls within the Amazon Web Services (AWS) public cloud Supported a VMware cloud on AWS Responded to customers' requests regarding Governance and compliance (FISMA security requirements) Determine security requirements by evaluating business strategies and requirements; information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates. Audited and managed Palo Alto's, QRadar, Nexpose, tenable security center, trend endpoint and more Created Run Books for Major Security Changes including replacing DC HA pair Palo Altos in a PAN environment. Sr. Cyber Security Architect Thyssen Krupp - Denver, CO October 2016 to April 2018 Represent the Security Department as the "Face of Security" on the Security Council. Design, implement and support Security solutions as company transitions from legacy platform. Primary focus is to drive adoption of T-Systems security services through direct customer engagement in partnership with customer.Manage security projects and team members, vendors and systems. Work with the Thyssen Krupp IT teams to ensure that security standards are created and adopted into the Enterprise Architecture frameworks. Created programs including processing and procedures to identify security gaps, develop controls, determine functional and non-functional security requirements and design solutions that meet business objectives while complying with security standards. Created proposals and recommend, develop, implement and maintain systems and processes that protect business and client information. . Provide oversight of the enterprise's security solutions and operations through management of internal and external resources. Held a seat as the Face of Security on the Security Council Responsible for analyzing current processes and procedures. Sales / Pre-sales Engineering ? Focused on driving expansions in existing enterprise for the Thyssen Krupp account. ? Sold and implemented new Enterprise wide Vulnerability Management program tailored to the customer that meets governance regulations requirements. Review existing architecture, identify design gaps, and recommend security enhancements by designing network maps for Palo Alto Networks Firewalls. ? Creating AS-IS Security models ? Creating To-Be Security models ? Create Transitional security models ? Manage Transitional changes ? Implement Transitional changes Audit all Palo Alto current state and created Risk Matrix and mitigation plans. SPLUNK Administrator responsible for design configurations. Provide artifacts to "Prove" Network traffic is in fact traveling thou and being inspected as designed. Upgrade legacy Palo Alto's Palo Alto Panorama 500-5000 series project (4.x code to 8.x code) Participate in Architecture Review and Security Council Review boards to define and explain the strategic Information Security direction and work with cross-organizational IT areas Serve as information security subject matter expert, trusted advisor; provide advisory and consulting services as needed NIST 800-37 ? Responsible for evaluating current MOD (Mod of Operation) of Risk Management and Threat Protection for Thyssen Krupp Materials ? Responsible for creating a holistic risk management process for all mission critical systems. ? Created a "Road Map" by Categorizing, Selecting, Implementing, Accessing, Authorizing and Monitoring ? Gap Analysis to Support the Implementation of the Thyssen Krupp Materials Threat and Vulnerability Management Policy ? Created Risk Matrix and supported my findings and suggestions to the Security Council. Meet with project teams and other system architects to develop system designs and project plans that include the appropriate security controls and meet security standards Conducts ongoing vulnerability testing (SAINT)of the information system to verify security features and operating controls are functional, effective and meet government standards Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle Lead as a Senior of Security Operations on Incident response in creating a Virtual War room inviting all key players. Sr. Cyber Security Architect BALL Corp - Broomfield, CO February 2016 to May 2016 Design Security Stacks based on the transactions identified which may require viewing traffic flows to alter and confirm application firewall rules. Tests in development and QA to ensure rules are working as intended. Copies the configuration settings into QA and then into production. Completes post-deployment testing and monitoring in production to ensure rules are working as intended. Troubleshoots in the event of web application failures.; Evaluates, designs, documents, installs, implements, tests, and performs problem isolation and resolution on all security controls (RSA Secure ID, Checkpoint R80 4000, 13000,15000 series and Palo Alto Panorama 500-5000 series, Cisco ASA 5540 Nexpose Rapid 7 Forensics - FireEye PX, NX (NTAP and SIEM - Central syslog and SPLUNK) Responsible for day to day security operations of information systems Develops and implements security measures in accordance with applicable government regulations and local facility procedures Develop and maintain information systems security plan Conducts ongoing vulnerability testing of the information system to verify security features and operating controls are functional, effective and meet government standards Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle Support major corporate infrastructure expanding and contracting. Support Global DNS - Create Honey Pots and or sinkholes Install Security Stack for new WAN Data Center Assist R80 evaluation Beta Version for Check Point and help Check Point develop R80 General Release. l Network Security Architect General Dynamics I.T - Broomfield, CO January 2015 to January 2016 Assist the OMNI Cloud program (Federal and Non Federal Cloud Provider) to obtain FedRAMP certification by developing processes and checklists for security controls, also by designing and implementing boundaries to separate Federal and NON-Federal environments. Develop processes and procedures using ITIL and CISSP best practices to technically manager engineers, using hands-on vulnerability assessments on networks and systems. Responsible for making recommendations for improving network security, and implement those recommendations. Plan and manage Data Center Network Virtualization Design DLP Scanning for (PCI-DSS) personally Identifiable Information and remediation. Created Privacy Impact Statements keep a repository before allowing access to systems Engineering risk mitigations with a CCNP and higher level. Design advanced networks using TCP/IP, dynamic routing protocols, VPN, and failover best practices Design firewall and VPN's - Cisco ASA firewalls (VPN concentrators as well as contexts) Stand up new Data Center as a Cloud serveries using Cisco Nexus series (7000, 5000, 2000, 1000v switches), ACS and UCS resources Create processes for advance FedRAMP Cloud Services offerings. Create process of Auditing and address vulnerabilities to meet FedRAMP unique elements of cloud computing Manage network projects across functional teams and customers Continuous service improvement of networks and network services Design new management networks for the U.S. Department of Labor to separated internal and external management networks. Architect infrastructures as well as troubleshoot and restore technical service and equipment issues by analyzing, identifying, and diagnosing faults and symptoms. Stand up new Services for customers Including Network / server installation / Virtual configuration / routers, switches, and firewalls. Sr. Security Audit Engineer Avaya - Denver, CO February 2014 to December 2015 Responsible for designs and plans of network communications systems. Provides specifications and detailed schematics for network architecture. Provides specific detailed information for hardware and software selection, implementation techniques and tools for the most efficient solution to meet business needs, including present and future capacity requirements. Evaluates and reports on new communications technologies to enhance capabilities of the network Assess current Security program and make recommendations for security hardening using NIST 800-37 standards. Design Network infrastructure and supporting protocols for future business needs. Designing and leading audits to validate that controls are adequate and functioning effectively. Documenting IT processes, controls, and exposures Communicating progress of audits to IT Audit Manager and audit clients in a timely manner Configuring 9000 services cisco with F5 ASM (LTM) to mitigate core redesigning to use security firewall and load balancing at network speeds to a virtual environment. Made changes to over 600 rules effecting over 50 policies on 5 Management systems, effectively hardening 200 Juniper devices, 100 Palo Alto's and 50 ASA's firewalls per NIST 800-37. Writing audit reports communicating audit observations and recommendations to both technical and non-technical audiences Participate on new systems development / implementation projects to ensure appropriate controls are incorporated Consult with IT and user personnel on system control methodologies and techniques. Principal Consultant STAR, LLC - Littleton, CO April 2013 to February 2014 Sales consultant focused on closing new business and driving expansions in existing enterprise for new and existing accounts. Project Manager ultimately responsible to ensure the client's satisfaction and realization of business requirements in technology solutions. Customer: Zoll Data ? Assess current security program to meet HIPAA security compliances. ? Project managed Lead Systems Architect for VOIP, Data and Server design to create a confidante, integrity, and available VOIP system to meet HIPPA compliances. ? Installed Tufin SecureTrack to ensure all firewalls, IPS's/IDS's, switches and routers to provide top down approach for security control view for all ? Created Change Control Processes and documentation for all security related changes. TravelPort, Saber and World Span ? Designed and implantation IDS/IPS systems for Saber and World Span in 3 Global Data centers. ? Follow-up IT Audit Findings and contribution to IT Dept. for closing those findings aligned with CobiT Regulations ? Discovered and designed the plan for Travel Port Corporate network over to World Span's 20,000 node network, this consisted of Cisco ASA version -15, Check Point R65-R70, and Juniper 240 and 650 Gateway routers and M series Juniper routers SRX, and ISG1000 Security applications. ? Installed trouble shoot Cisco, router 2800-7200, Juniper routers M series , along with Cisco Nexus 5550 , and Cisco IOS 2900-65000 switches Manager of Information Security SERVICE SOURCE INTERNATIONAL - Denver, CO February 2013 to April 2013 Responsible for safeguarding the company's information/data assets, intellectual property and computer systems through creating and implementing security operations "runbooks" across organization's infrastructure and applications teams. Solved big data security invisibility problem by Designing Infrastructure wide solution with HP ArcSight to provide a unified view of security through collection, storage, and analysis for IT security, compliance, ops, and analytics. Provide guidance and support for governance of the global infrastructure using CISSP best practices. Created weekly executive reports for monitoring and maintain the operational awareness of the global infrastructure. This report included stats for malicious code, intrusions, failed logins by users, etc. also including snap shots of live charts for easy digestion of the information. Implemented incident response standards, plans and protocols to ensure that security incidents and policy violations are promptly addressed. Assessed various vendor security solutions for end point security of mobile device for host based IPS/IDS software. Project managed full life cycle of Palo Alto IPS (in-line) controls. Configured network requirements of routes, DNS, SNMP and Zones, policies for the successful deployment of the Palo Alto Network Unified gateway devices. Developed Security Office "runbook", which is collection of procedures and operations that IT Security can use to effectively manage, execute and troubleshoot. Manager of SOC (Security Operations Center) consisting of 7 fulltime Security Analyst and 4 Security vendors resources that composed the incident response team,   Managed day to day activities of all security related changes, maintenance and counter measures.   Escalation point and manager for multi-team security issues from start to finish.   Created processes for who can access data, how that access would be secured, and what and how data for each vendor would store information. Sr. Security Engineer, SOC Lead INNOVAR GROUP - Denver, CO October 2012 to February 2013 Responsible Security Hardening project which was a III Phase project. Phase I managing a team of engineers to audit and report on current security vulnerabilities of GeoEye's perimeter. Phase II write code and configuration and suggested hardware controls for procurement to mitigate for threat. Phase III Configure all firewalls, switches and router ACL's (Cisco, Checkpoint, Juniper) of the corporate infrastructure of the rules determined not valid and to reduce the foot print of access into the zones protected by the firewall.   Assess current Security program and make recommendations for security hardening.   Design, develop, test and implement security solutions, such as measurement matrix based on quantitative and qualitative methods to validate and classify data assets using NIST 800-37.   Responsible projects involving physical security, risk mitigation, security policies which often involved hands on configurations of new network and security hardware including Cisco, Juniper, Palo Alto 500 - 5000, ArcSight , Check Point SourceFire systems and IAM Systems (Blue Coat).   Responsible for perceiving the big picture and the ability to effectively influence others internally and externally.   Write new security policies for customer base via ticket request.   Saved Army 4 million dollar contract by addressing 2000 risky firewall policies holes by the implementation of intrusion prevention and network traffic segmentation.   Responsible for evaluating VPN technology to determine the best solution for replacement of Cisco VPN to Palo Alto VPN. Principal Consultant STAR, LLC - Littleton, CO September 2007 to July 2012 Sales consultant focused on closing new business and driving expansions in existing enterprise for new and existing accounts. Project Manager ultimately responsible to ensure the client's satisfaction and realization of business requirements in technology solutions   Customer: AVIS ? Project Managed AVIS to Black Stones network, this consisted of 296 Access sites with over 300 Cisco 3600's running OSPF over IBGP and BGP networks. ? Define and manage all aspects of the AVIS to Black Stones network project including scope, schedule, staffing, issues and budget ? Planned and implemented changes of Pix and ASA firewalls for Black Stone networks. ? Install and trouble shoot Big IP F5, versions 9-10and Foundry Load Balancers for server farms use of, DNS, VIP, SSL accelerators. Customer: Lucero Group ? Provide Lucero Group with an external IT department. ? Audited Lucero Group's three companies to segment data and implemented security measures. ? Implement Active Directory and migrated MS 2003 to 2008 servers. ? Managed and acted on all IT related requests ? Created test environment for load balancing of Web applications for Lucero Group. IT Operations Manager, NOC Manager MEETING ONE - Denver, CO July 2011 to June 2012 Ensures the stability and consistency of the IT infrastructure and IT services by maintaining the organization's day-to-day activities and processes. Hands on Manager that provides prompt diagnosis and resolution for any IT operations failures that occur. Designed and deployed redundant data center for load balancing and fail over. Worked with multiple vendors to ensure new data center services were delivered as expected. Created and executed test plan of load balancing, failover and DR of new data center. Created and implanted security controls and monitoring for new data center. Direct management of Operations Engineering and Operations in Denver, CO and Europe locations. Created and maintained project plans in accordance with CHI standards and requirements. Developed and manage departmental budgets (staffing, hardware, services, etc.) Responded to 24/7 outages, technically trouble shot and fix problem. Plan and implement maintenance (upgrades, patching, etc.) and system changes. BPG redesign to support global load balancing with BIG IP F5 load balancers. Implemented all Firewall Changes on Cisco ASA's. Installed firewalls, load balancers, switches and networks to insure no single points of failure exist system. Enterprise Network Architect I.B.M - Englewood, CO May 2007 to September 2007 Responsible for managing the design and execution of the migration for the Navigant networks to the Carlson Wagonlit networks. Responsible for developing architectural and Network engineering strategies for future implantations and troubleshooting of the Navigate Network in efforts to have a seamless migration to the Carlson Network. Project Manager/ Sr. Network Engineer CENDANT Corp - Englewood, CO May 2006 to May 2007 Responsible for developing organizational technology strategies by consulting with users, project Stake Holders and IT staff. Design and implement advanced new remote networked systems to core MPLS technologies. Sr. Network Engineer AMERIQUEST MORTGAGE - Centennial, CO June 2005 to May 2006 Network Engineer Groople, Inc - Centennial, CO December 2004 to April 2005 ANALYST INTERNATIONAL Contract Johns Manville - Denver, CO October 2002 to December 2004 NOC Engineer/ Sr. Systems Analyst Senior Information Technology Network Support Technician JANUS MUTUAL FUNDS - Denver, CO June 1998 to January 2001 Education Bachelor of Science in Computer Information Systems Metropolitan State College - Denver, CO PMP in Tufin Security Management Metropolitan State College - Denver, CO

Name: Jason Wright

Email: nlee@example.org

Phone: 728.646.8256x347