Lawrence Loftley Jr

[lawrence.loftley@gmail.com](mailto:lawrence.loftley@gmail.com)

910-224-1196

**Sr. Cyber Security Engineer and Sr. Security Analyst**

Risk Management Framework (RMF) ♦ Vulnerability Scanning & Vulnerability Assessment ♦ Security Control Assessment ♦ Host Based Security Systems (HBSS) ♦ Electronic Enterprise Mission Assurance Support Service (eMASS). ♦ DISA Vulnerability Management System ♦ Internal Control Selection ♦ Static and Dynamic Code Scanning ♦ Security Analytics ♦ DISA STIG Implementation ♦ Security Test and Evaluation (ST&E) ♦ Assured Compliance Assessment Solution (ACAS)

Experience consist of working in a small to large enterprise organization troubleshooting and providing assistance with complex network issues as well as information assurance/ cyber security issues. Continued efforts to ensure the highest security posture by conducting security assessments, manage and maintain vulnerability lifecycle, manage enterprise architectural requirements, develop, implement, and manage certification and accreditation process, workflows, and security controls. Perform duties as an System Engineer managing and maintain the network infrastructure and equipment. Working with stakeholders and users gathering requirements and translate the information gathered into technical requirements to support development and analysis utilizing the SDLC model.  Developing artifacts in support of the development such as design and documentation using DODAF SE, Risk Management Framework, and DIACAP, familiar with DOORS methodology. Experience using McAfee and Splunk to monitor and investigate events. Familiar withArcSight, Fortinet, Symantec End Point Manager.Experience and familiar with Web Application Firewalls,Intrusion Protection Systems, SharePoint Gateways, and Proxy. Experience in preparing for DISA Cyber Security Readiness Inspection by performing Command Cyber Readiness Inspection (CCRI). Responsible for conducting compliance and vulnerability assessments by utilizing the following tools: ACAS, SCAP, & STIG scans; performing Patching and Remediation, creating Risk Assessment Reports (RARs), Plans of Action and Milestones (POA&Ms); Governance, Risk, and Compliance (GRC), and technical support in the areas of Vulnerability Management.  Strong experience in NIST 800-53 Rev 4 /NIST 800-53A Rev 4 security guidance and security control assessment (SCA) process, NIST SP 800-30, Internal Controls, and industry best practices. Can perform operational tasks for Threat Log and Analysis, Host Based Intrusion Systems, Vulnerability Scanners, Log Collectors and Analyzers, Policy Auditing, Firewall Settings, and Computer Network Defense from experience as a MacAfee HBSS Engineer (McAfee ePo Orchestrator).  In-depth operational experience on creating custom queries and dashboard for continuous monitoring; improving Enterprise Security procedures; drafting Security Assessment Reports and Risk-Based Decisions, tailoring controls, and analyzing vulnerability reports and trend analysis to reduce exploits for defined analytics.  Maintain compliance for security frameworks, standards, and best practices: DISA STIGS, FISCAM, FISMA, FIPS, NIST, OMB, DoD 8500, ISO 2700, and ITIL. Holds **Top-Secret Clearance** (DOD-Current/Active). Actively pursuing **Certified Information Security System Professional (CISSP)** certification.

**Skills**

**Security:**  Cyber Defense, Threat Management, Auditing, System Hardening, Risk Assessment, Disaster Recovery, Vulnerability Management, Malware Defense, Security Awareness, Compliance, Policy Enforcement, Incident Handling and Response, Security Event and incident Management / Monitoring (SEIM), Implementing Controls, Configuration Management

**Documentation:** Risk Assessments, Contingency Plans, Security Assessment Plans and Reports, Change Management Plans, Configuration Management, Interconnection Security Agreement(s), Privacy Impact Assessments, and Business Recovery Procedures, SOP's, and INFOSEC Policies  
**Software:** NIST and DoD SCAP, SIEM, HP WebInspect and Fortify; Nessus, Splunk, eEye REM/Retina, DISA Gold Disk , Symantec Antivirus, McAfee Antivirus and ePolicy Orchestrator (ePO), HBSS, WireShark, Microsoft : Server 2003/2008, Windows XP/VISTA/7, Active Directory  
**Policies** FISMA, NIST, DoD 8500, NIST 800 Series, NIST 800-53, FIPS 199, FIPS 200, HIPAA, ISO-27002

**Education**

Capella University – Minneapolis, MN - MS in Information Systems and Technology Management, Graduated 04/2016

St. Leo University - St. Leo, FL - MBA with a concentration in Information Security Management, Graduated 04/2009

St. Leo University - St. Leo, FL - BS - Computer Information Systems, Graduated 01/2007

**Certifications**

Certified Ethical Hacker version 9 (C|EH) Certification Number: ECC07098158315

SAP Certified Application Associate (Edition 2013) – SAP HANA - Certified

SAP Certified Technology Associate - System Administration (MS SQL DB) with NetWeaver 7.0 - Certified

Comptia Advanced Security Practitioner (CASP) - Certified-COMP001020686030

Comptia Security + Certified - COMP001020686030

Microsoft Certified Systems Engineer (MCSE) Certified - Microsoft ID: 1205525

Microsoft Certified Systems Administrator (MCSA) Certified - Microsoft ID: 1205525

Cisco Certified Networking Associate: (CCNA) Certified - CSCO10234384

Comptia A + Certified - COMP001020686030

Comptia Network + Certified - COMP001020686030

Microsoft Certified Professional (MCP) Certified - Microsoft ID: 1205525

Microsoft Certified Technology Specialists: SQL 2005 (MCTS) Certified - Microsoft ID: 1205525

VMware Certified Professional on vSphere 5 (VCP) VCP certification Number: 121770

VMware Certified Professional 5 on Data Center Virtualization (VCP5-DCV) VCP certification Number: 121770

ITIL Foundations Service Management (2011) Certified & ITIL Intermediate Service Operations (2011) Certified

**Experience**

**Cyber Threat Intelligence Analyst / Incident Response – M9 Solutions/USPS CSOC 8/10/16 – Present**

**Raleigh, NC**

Provide support for the customer's Cyber Threat Intelligence Program. Provide source monitoring activities, cyber threat analysis and mitigation course of action. Provide the actionable intelligence used in organizational IT Asset protection, strategic cyber threat trending and situational awareness of customer leadership. Compile cyber threat data gathered through independent research and analysis along with Security Operations Center activity, and look at emerging technology, techniques and adversarial capabilities and tactics on a near real-time basis. Analyze cyber threat Indications & Warning and fuse unclassified/open source cyber threat information correlating internal activity to external indicators across numerous boundaries. The correlation provides insight into every stage of a potential intruder's cyber kill chain as well as other activities in the wild. Investigate alerts, anomalies, errors, intrusions, malware, and identify treat agents. Assist in determine the nature and extent of problems being reported by tools, emails, and systems. Assists in analysis and investigation of problem reports or anomalies. Follow strict guidance on reporting requirements. Follow standards-based workflow. Engage with other internal and external parties to get and share. information to improve processes and security posture. Communicates with leadership. Produce relative design documentation. Leads analyzing/investigating reports or anomalies.

**Database Manager / Knowledge Manager –Crystal Clear Technologies June 2015 – August 2017**

**U.S. Army Fort Bragg, NC**

Provide specialized database and information management support across a range of operational and administrative disciplines in support of classified information, including serve as principal advisor on deployment of both existing legacy and newly deployed information technology infrastructure. Support the knowledge management applications of specialized services and support the Knowledge Management Center of the U.S. Army Combined Arms Center. Plan, track and apply IT support for each training evolution, and transfer critical data and knowledge between and among the Sponsor’s command elements and disparate and segregated components. Manage and maintain the implementation, deployment, and management of a controlled, limited access, and proprietary database in support of the Sponsor’s command structure along with instruction and applications. Provide security consultation as needed.

**SAP HANA Technology Consultant for Hewlett Packard – Insight Global Jan 2015 – June 2015**

**Remote Work from Home, Raeford, NC**

HP SAP HANA Consultant (Work from home, remote position), providing support for the SAP HANA Deployment Accelerator service. Plan and review documentation relative to the SAP Implementation. Performing 70%-80% Travel. Incorporate the HP AppSystem for SAP HANA into the Customer's local network. Perform validation on the SAP HANA environment (hardware setup, network connectivity, and bandwidth). SAP HANA software patching, if required. Install SAP HANA Studio on one PC or workstation. Implementation of SAP HANA Test Import some sample test data into SAP HANA and run sample reports using Excel plug-in. Provide knowledge transfer on the use and operation of the SAP HANA system: Hardware, Configuration, Networking, HANA Studio, System Administration, Roles and Users, and Backup and Recovery. Provide services as an HP Consultant by traveling to assigned customer sites to deploy and configure the Converged System 300 for Microsoft Analytics Platform (formerly Parallel Data Warehouse (PDW)) and the data loading or backup server, connect them to the customer’s network, configuring the 5120 Ethernet switches according to the customer’s specifications, and test the system using TPC-H test data, which HP will generate. Also configure the HP Insight Remote Support (IRS) server or VM, and connect and configure the Converged System 300 for Microsoft Analytics Platform to the IRS server. Support Microsoft SQL server 2012 for Data Warehouse. Provide knowledge transfer of the appliance and conduct a hand off to the customer.

**Senior Information Security Analyst – STG, Inc. Oct 2014 – Jan 2015**

**U.S. Army Forces Command (FORSCOM) - Fort Bragg, NC**

Managing a Team of highly knowledgeable and experienced team of Information Security Analyst and Engineers which ensure the highest level of security compliance are adhered to in accordance with the Department of Defense (DoD), Department of the Army (DA), and the federal government by providing technical knowledge and analysis of information assurance, to include applications, operating systems, physical security, networks, risk assessment, critical infrastructure continuity and contingency planning, emergency preparedness and security awareness and training. Developed artifacts in support of the development such as design and documentation using DODAF SE. Familiarity with the DOORS methodology. Conducting security analysis on existing system's vulnerabilities to possible intrusions, resource manipulation, and resource denial of service and destruction of resources. Performing research on the DoD Information Assurance Certification and Accreditation Process (DIACAP) to Risk Management Framework (RMF) Transition to support the Army-wide Certification and Accreditation efforts. Develop, manage, maintain, conduct assessment, and review current DIACAP packages for updates and changes. Review current processes within FORSCOM for improvement and development. Develop, manage and maintain the required accreditation and certification for mission service applications and the development/test network IAW DoD Information Assurance Certification and Accreditation Process (DIACAP and the Army's Certificate of Networkthiness (CoN) process.

Provides technical support and analysis to document organization information protection framework, and support policy and procedures preparation and implementation.

Manages the Information Assurance Vulnerability Management (IAVM) program currently in place in support of FORSCOM and Army Enterprise Network. Provide technical analysis and support to document and implement the SIPRnet Public Key Infrastructure (PKI) for SIPRnet users. Maintain and manage ACAS/NESSUS Scanning tool, Symantec Endpoint Protection, McAfee Antivirus endpoint solution, eEye Retina, Host Based Security System (HBSS), System Center Configuration Manager (SCCM), and Windows Server Update Services (WSUS).

Provide weekly and monthly status reports of mission service applications to ensure IAVA compliance based on NEC-provided IAVA scan reports and reviewing logs.

Possess strong knowledge and familiarity DoD and NIST IA policies, SCADA related processes, and risk assessment methodology.

Perform analysis on programs, policies, procedures, and processes to evaluate compliance in accordance with Department of Defense and National Institute of Standards and Technology (NIST) Information Assurance policies, SCADA related processes, and risk assessment methodology. Where necessary, recommended improvements, closed gaps, and removed extraneous information.

Conduct incident investigations by using forensic tools and procedures in efforts to gather evidence when an incident has occurred, consisting of identifying, collecting, and preparing submissions in response to evidence requests.

Assisted in audit preparation activities, including writing responses for the Reliability Standard Audit Worksheets (QRSAWs) and identifying, collecting, and preparing submissions in response to evidence requests. Provided validation during regional audits and internal mock audits. Provided compliance support to internal business partners, such as System Protection, Field Operations, Telecom, Management and Process Control Systems, and others.

Developed mitigation / remediation plans and implemented measures to mitigate risk. Communicated status updates to senior-level stakeholders.

Ability to communicate technical terms effectively in front of an audience and interpret regulatory guidance. Experience in writing and executing test cases, POA & M's and policies. Experience in reviewing/editing/writing technical documents. Capable in conducting high level briefings, presentations and perform public speaking task when needed.

Familiar with technical knowledge of network devices and interconnections (i.e., routers, switches, IDS/IPS, firewalls and DNS) and configuring or testing computer systems according to DISA Security Technical Implementation Guides (STIGs) or similar configuration guidance.

Possess experience working in a Network Enterprise Center, a Network Operations or Security Center. Dynamic and results-oriented Information Assurance Engineering professional supporting customer requests, managing, monitoring and investigating all incident response activities. Training and mentoring analysts. Participate in an on call after hours to allow for reporting of incidents by customers or supporting analysts with investigations.

**Senior Information Assurance Engineer – Verizon Business Solution / Ampcus, Inc. Feb 2014 – Oct 2014**

**USARC G-6 Information Assurance Department – Incident Response**

**United States Army Reserve Command- Fort Bragg, NC**

Dynamic and results-oriented Information Assurance Engineering professional supporting customer requests, managing, monitoring and investigating all incident response activities. Training and mentoring analysts. Participate in an on call after hours to allow for reporting of incidents by customers or supporting analysts with investigations. Solid and diverse experience in a variety of fields managing overall operations and optimizing organizational processes. Highly reliable and analytical computer security analyst, efficient in meeting goals and ensuring utilization of manpower and resources, problem analysis, consulting, deploying vulnerability management strategies, DOD and army approved information assurance tools and problem-solving skills adept at engaging requirements while designing solutions based on strong technical expertise and experience. Enthusiastic individual and an excellent communicator recognized ability to establish and maintain effective working relationships across cross-functional teams and diverse individuals at any levels. Conduct a maturity assessment of IT operations using a template to assess the overall level of IT maturity. Coordinate, plan, and perform effective provisioning, installation/configuration, Information Assurance, operation, and maintenance of systems hardware and software. Server Administration duties are: install servers and operating systems, patches and program releases for specified servers. Administer and manage VMware and physical environments. Ensure all servers are IAVA and STIG compliant.

Install/update all O/S patches as required. Perform security vulnerability scans on current servers and environment using Gold Disk and eRetina scanning tools. Familiar with managing vulnerability and threats using tools such as Nessus, Maintain and manage ACAS/NESSUS Scanning tool, Symantec Endpoint Protection, McAfee Antivirus endpoint solution, eEye Retina, Host Based Security System (HBSS), System Center Configuration Manager (SCCM), Windows Server Update Services (WSUS), QRadar and Imperva and providing end to end protection using SIEM for DLP. Ensure all servers have current anti-virus software IAW customer specifications. Perform periodic backups within the physical and virtual environment. Conduct incident investigations by using forensic tools and procedures in efforts to gather evidence in the event that an incident has occurred, consisting of identifying, collecting, and preparing submissions in response to evidence requests. Maintain and manage the SharePoint 2007/2010 environment as the Site Collections system administrator and Content Manager for C4IM services. Provide guidance to the technical staff on the functional procedures/processes/policies reflecting detailed knowledge of the following functional areas: software engineering, communications, and system integration. Interfaces with Government management personnel and functional proponents. Performed all security scans, remediated vulnerabilities, Developed DIACAP Artifacts and POA&Ms. Assisted with the completion of security requirements in support of the Service Level Management Project. Familiarity with managing critical assets based on IA controls. Work with the process team to develop ITIL-based processes, include process diagramming and description to re-engineer processes based on ITIL best practices. Developed artifacts in support of the development such as design and documentation using DODAF SE. Familiarity with the DOORS methodology

Manage United States Army Reserve Command (USARC) Information Security Posture by maintaining the maintaining the compliance of the USARC network environment in accordance with DODs, Army standards and regulations AR 25-2, DODi 8500.1, DODi 8500.2, Federal Information Security Management Act (FISMA) and the National Institute of Standards and Technology (NIST) documentation. Possess strong knowledge and familiarity DoD and NIST IA policies, NERC / CIP compliance, SCADA related processes, and risk assessment methodology. Perform analysis on programs, policies, procedures, and processes to evaluate compliance in accordance with Department of Defense and National Institute of Standards and Technology (NIST) Information Assurance policies, North American Electric Reliability Corporation (NERC) / Critical Infrastructure Protection (CIP) compliance, SCADA related processes, and risk assessment methodology. Where necessary, recommended improvements, closed gaps, and removed extraneous information. Assisted in audit preparation activities, including writing responses for the Reliability Standard Audit Worksheets (QRSAWs) and identifying, collecting, and preparing submissions in response to evidence requests. Provided validation during regional audits and internal mock audits. Provided compliance support to internal business partners, such as System Protection, Field Operations, Telecom, Management and Process Control Systems, and others.

Provided input and prepared self-reports of compliance violations; technical feasibility exceptions (TFE); internal exceptions to cyber security policy; and periodic reports to regional entities, such as self-certifications, Part B reviews of accepted TFEs, and quarterly and annual TFE filings. Developed mitigation / remediation plans and implemented measures to mitigate risk. Communicated status updates to senior-level stakeholders.

Performed all security scans, remediated vulnerabilities, Developed DoD Information Assurance Certification and Accreditation Process (DIACAP), Risk Management Framework (RMF) Artifacts and POA&Ms. Assisted with the completion of security requirements.

Conducted periodic scans and remediation using DISA Gold Disk, Army Gold Master, DISA STIGs, SCAP, VMS, NESUS, and Eye-Retina. Provided reports indicating current security posture and remediation strategies. Developed SOPs, POA&Ms, Risk assessments, Certification and Accreditations package to manage the relative IA controls. Performed all security scans, remediated vulnerabilities, Developed DoD Information Assurance Certification and Accreditation Process (DIACAP), Risk Management Framework (RMF) Artifacts and POA&Ms. Assisted with the completion of security requirements. Familiarity with managing critical assets based on IA controls in accordance with NIST, FIPS 140/199/200, FISMA, and NIFS/ NEI 08-09 guidance, NERC / CIP compliance, SCADA related processes, and risk assessment methodology.

**IT SLM Capability Manager / Deputy Program Manager –RLM Communications Dec 2012 – Feb 2014**

**IT Service Level Management Project**

**United States Army Reserve Command- Fort Bragg, NC**

As an IT Service Level Management resource, responsible for the development and implementation of ITIL processes and best practices at the USARC G-2/6 using ITSM integrated tools. Conduct requirements analysis and information gathering by meeting with representatives within the USARC, RSCs and installations. Analyze data related to current processes. Identify gaps within IT operations current practices and provide solutions in which to resolve those gaps using ITIL best practices.

Develop and improve processes using ITIL best practices. Develop and execute a plan which will utilize the IT resources and provide the organization the best benefit. Provide effective solutions in accordance with ITIL best practices. Develop and coordinate the execution of ITIL Disciplines across services provided as an end-to-end IT services management solution between the organization, suppliers, and the vendors. Conduct a maturity assessment of IT operations using a template to assess the overall level of IT maturity.

Coordinate, plan, and perform effective provisioning, installation/configuration, Information Assurance, operation, and maintenance of systems hardware and software. Server Administration duties are: install servers and operating systems, patches and program releases for specified servers. Administer and manage VMware and physical environments. Ensure all servers are IAVA and STIG compliant.

Install/update all O/S patches as required. Perform security vulnerability scans on current servers and environment using Gold Disk and eRetina scanning tools. Remediated and mitigated vulnerability and threats using tools such as Nesus, QRadar and Imperva and providing end to end protection using SIEM for DLP. Ensure all servers have current anti-virus software IAW customer specifications. Perform periodic backups within the physical and virtual environment.

Maintain and manage the SharePoint 2007/2010 environment as the Site Collections system administrator and Content Manager for C4IM services. Provide guidance to the technical staff on the functional procedures/processes/policies reflecting detailed knowledge of the following functional areas: software engineering, communications, and system integration. Interfaces with Government management personnel and functional proponents. Performed all security scans, remediated vulnerabilities, Developed DIACAP Artifacts and POA&Ms. Assisted with the completion of security requirements in support of the Service Level Management Project. Familiarity with managing critical assets based on IA controls.

Work with the process team to develop ITIL-based processes, include process diagramming and description to re-engineer processes based on ITIL best practices. Interact with all levels of client staff, including senior-level decision makers and executives and conduct qualitative and quantitative analyses in support of solution development. Assists with the development of metrics and measures assess compliance and process success. Participate in disperse, collaborative team environment and maintain a key role in conducting the initial analysis and developing the process solution. Develop and implement lifecycle management plan relating to the adding, deleting, decommissioning of USARC C4IM Services.

Performed all security scans, remediated vulnerabilities, Developed DIACAP Artifacts and POA&Ms. Assisted with the completion of security requirements in support of the Service Level Management Project. Familiarity with managing critical assets based on IA controls in accordance with NIST, FIPS 140/199/200, FISMA, and NIFS.

**Systems Administrator / Subject Matter Expert – SAIC Aug 2011 – Dec 2012**

**Advanced IT Systems (AITS) program / Reserve Component Automated System (RCAS)**

**United States Army Reserve Command- Fort Bragg, NC**

Serves as the subject matter technical expert on to the Advanced IT Systems (AITS) program project.

Coordinate, plan, and perform effective provisioning, installation/configuration, Information Assurance, operation, and maintenance of systems hardware and software.

Server Administration duties are: install servers and operating systems, patches and program releases for specified servers. Administer and manage VMware and physical environments. Ensure all servers are IAVA and STIG compliant.

Install/update all O/S patches as required. Perform security vulnerability scans on current servers and environment using Gold Disk and eRetina scanning tools. Conducted scans, managed, remediated and mitigated vulnerability and threats using tools such as Nessus, Maintain and manage ACAS/NESSUS Scanning tool, Symantec Endpoint Protection, McAfee Antivirus endpoint solution, eEye Retina, Host Based Security System (HBSS), System Center Configuration Manager (SCCM), Windows Server Update Services (WSUS), QRadar and Imperva and providing end to end protection using SIEM for DLP. Ensure all servers have current anti-virus software IAW customer specifications. Ensure all servers have current anti-virus software IAW customer specifications. Perform periodic backups within the physical and virtual environment. Provide guidance to the technical staff on the functional procedures/processes/policies reflecting detailed knowledge of the following functional areas: software engineering, communications, and system integration. Interfaces with Government management personnel and functional proponents. Developed artifacts in support of the development such as design and documentation using DODAF SE. Familiarity with the DOORS methodology. Performed all security scans, remediated vulnerabilities, Developed DIACAP Artifacts and POA&Ms. Assisted with the completion of security requirements in support of the Service Level Management Project. Familiarity with managing critical assets based on IA controls in accordance with NIST, FIPS 140/199/200, FISMA, and NIFS.

Possess strong knowledge and familiarity DoD and NIST IA policies, SCADA related processes, and risk assessment methodology.

Perform analysis on programs, policies, procedures, and processes to evaluate compliance in accordance with Department of Defense and National Institute of Standards and Technology (NIST) Information Assurance policies, SCADA related processes, and risk assessment methodology. Where necessary, recommended improvements, closed gaps, and removed extraneous information.

Assisted in audit preparation activities, including writing responses for the Reliability Standard Audit Worksheets (QRSAWs) and identifying, collecting, and preparing submissions in response to evidence requests. Provided validation during regional audits and internal mock audits. Provided compliance support to internal business partners, such as System Protection, Field Operations, Telecom, Management and Process Control Systems, and others.

Maintain Inventory in support of lifecycle replacement of Hardware and Software products relating to the Reserve Component Automated System (RCAS)

Reports in writing and orally to Contractor management and Government representatives, including the Government CO and COR.

**Encryption Engineer / Security Analyst III- Chickasaw Nation Industries March 2010 – Aug 2011**

**Center for Disease Control and Prevention- OCISO- Atlanta, GA**

Project Manager for the McAfee Biometric Encrypted USB drive Enterprise project providing centrally managed encrypted mobile devices in an enterprise environment. Provide consultation and technical support for Installing, maintaining, updating and deploying security products (hardware and software). Perform research, analysis, development, evaluation and testing of current or new security products. Implemented life cycle management process within the deployment and implementation of the McAfee Biometric Encrypted USB drive Enterprise project.

Collect, record, analyze, synthesize and report data and information related to computer security events and incidents in accordance with the IR Plan and related policies, procedures and directions. Recommend and/or implement mitigation actions in response to incidents in accordance with the IR Plan. Participate in ongoing operation, maintenance and user support of cyber security tools including, but not limited to, firewalls, scanning tools and systems, traffic analyzers, sniffers, asset management and vulnerability management tools, forensics tools, etc. Administer Windows 2003, Windows 2008 server, SQL 2008 Server. Administer and maintain Linux platforms, create users, provide rights and permissions, install applications, update patches, security updates, and troubleshoot issues. Perform provisioning, installation/configuration, operation, and maintenance of systems hardware and software and related infrastructure for Windows 2000 / XP Pro, Windows 2000 / 2003 Server, 2008 Server, Linux, Solaris, and VMware environment. Manage OS and Security Patches. Implement updates, patches, service packs for Solaris, red hat, windows servers.

Administer and maintain VMware development and production environments. Create new VMs for different platforms. Familiar with VM ware technology such as Solaris containers, xen, and kvm. Manage and maintain active directory organizational units, create users, provide rights permissions, group policies when applicable. Experience in implementing, mitigating vulnerabilities reported using NESUS/ACAS eRetina/ AppScan. Evaluate results from NESUS/ eRetina/ AppScan and perform validation during the Certification & Accreditation System Testing and Evaluation process.

Conduct incident investigations by using forensic tools and procedures in efforts to gather evidence in the event that an incident has occurred, consisting of identifying, collecting, and preparing submissions in response to evidence requests.

Conducted scans, managed, remediated and mitigated vulnerability and threats using tools such as Nessus, Maintain and manage ACAS/NESSUS Scanning tool, Symantec Endpoint Protection, McAfee Antivirus endpoint solution, eEye Retina, Host Based Security System (HBSS), System Center Configuration Manager (SCCM), Windows Server Update Services (WSUS), QRadar and Imperva and providing end to end protection using SIEM for DLP. Ensure all servers have current anti-virus software IAW customer specifications.

Conduct POA&M Validation, RMW Validations, and False Positive Validations. Maintain SAN storage environments. Performed proof of concept for research and development of new architectural concepts and design. Perform tape backups on Windows 2003, Solaris 10 and Red Hat Linux servers. Provide project management and consultation for the backup solution. Conduct meetings with stakeholders to ensure critical data is being captured securely and proficiently. Design, configure, implement and test new backup solution with encryption. Create, develop and manage the Backup and Disaster Recovery Plan / Solution. Performed all security scans, remediated vulnerabilities, Developed DIACAP Artifacts and POA&Ms. Assisted with the completion of security requirements in support of the Service Level Management Project. Familiarity with managing critical assets based on IA controls in accordance with NIST, FIPS 140/199/200, FISMA, and NIFS., SCADA related processes, and risk assessment methodology.

Possess strong knowledge and familiarity DoD and NIST IA policies, SCADA related processes, and risk assessment methodology.

Performed audit preparation activities, including writing responses for the Reliability Standard Audit Worksheets (QRSAWs) and identifying, collecting, and preparing submissions in response to evidence requests. Provided validation during regional audits and internal mock audits. Provided compliance support to internal business partners, such as System Protection, Field Operations, Telecom, Management and Process Control Systems, and others.

Providing guidance, support, documentation, configuration, and processes of the encrypted hardware devices and Software in a centralized manner

**EXPERIENCE CONTINUED**

2009-2010 US Army - School of Information Technology Information Assurance Technical Trainer

2009-2009 Center for Disease Control and Prevention Senior Systems Engineer – BioSense

2006-2009 Center for Disease Control and Prevention Application Integrated Systems Engineer – PHINMS

2007-2007 US Army - Womack Army Medical Center Information Technology Specialist (Customer Support) GS-09

2006-2007 Center for Disease Control and Prevention Application Integrated Systems Engineer – PHINMS

2004-2006 Center for Disease Control and Prevention Helpdesk Support Specialist-PHIN

2003-2004 US Army Active Duty ("Enduring Freedom") Information System Security Officer (ISSO)

2003-2004 US Army Active Duty ("Enduring Freedom") Information Management Officer (IMO)

2000-2004 United States Army Reserve Command Remedy Administrator- RCAS

2000-2004 United States Army Reserve Command Telecommunications Network Systems Analyst III - RCAS

1998–2000 SunTrust Bank Client Technology Support Spec III

1999-1999 DHR / Key Resources Office Technical Support

1997-1999 New Horizons PC / Network Tech

1997-1998 NCR Technical Helpdesk analysts

1996-1997 GE Capital NEC Helpdesk Support Technicians

1993-1996 US Army, 267th Finance BN 44C Accounting Specialist

1992-1993 World Span Corporation / Olsten Computer Refurbishing Technician

1988-1992 US Navy, USS Cowpens (CG-63) Vertical Launching System Technician