Senior Information Security Analyst Senior Information Security Analyst Senior Information Security Analyst Philadelphia, PA Proactive, focused, accomplished, Windows information security analyst and systems administrator with demonstrated success within high-pressure and high profile engagements for private sector, government and defense employers. VMware, vCenter and Horizon View virtual machine administration; Nessus, Security Center, Retina and SCAP vulnerability scanner administration. Windows Server Update Service (WSUS), Big Fix and SolarWinds patch management; PowerShell and Windows command line scripting automation. Windows Server 2008-2012 R2 and Windows 7-10 troubleshooting; Microsoft Office. US citizen. Authorized to work in the US for any employer Work Experience Senior Information Security Analyst Akima LLC, Cloud Lake Technology LLC, MVM, Inc - Chantilly, VA August 2016 to October 2018 Relocated by MVM) Department of Justice (DoJ) Drug Enforcement Administration (DEA) Contractor. Led cybersecurity and information assurance for federal law enforcement agency, including IT security policy development and deployment. Key technical engineer facilitating Authorization To Operate (ATO) processes; granted October 2017. Administered Tenable Nessus - Security Center vulnerability scanning and Security Content Automation Protocol (SCAP) assessment tools. Configured enterprise virtual and physical production devices according to DISA Security Technical Implementation Guides (STIG). Facilitated agency's GRC (Governance, Risk and Compliance) requirements (CSAM) with SME knowledge of federal security, industry and market trends, security audits, including Certification and Accreditation (C&A) processes (FISMA). Orchestrated monthly Patch Tuesday enterprise patch management and vulnerability remediation with Windows Server Update Service (WSUS) and Big Fix, implementing security policy enforcement via Active Directory Group Policy Objects (GPO). Reduced IT staff involvement with security practices by 75%, utilizing hands-on experience with Windows command line and PowerShell scripting automation. Oversaw security processes and standards to stabilize Windows Server 2008-2012 R2 and Windows 7-10 workstation troubleshooting, administration of VMware virtual workstations and servers. Developed and validated test lab strategies for supporting enterprise operations and published daily network security posture metrics with Excel for

government and contractor IT leadership. Security Support Engineer- Systems Engineer Parata Systems LLC - Durham, NC June 2013 to July 2014 Relocated by Parata) Department of Defense (DoD) Contractor. Committed Microsoft operating system controls and configurations in compliance with Department of Defense (DoD) security standards to include Department of Defense Information Assurance Certification and Accreditation Process (DIACAP, C&A, A&A) for area's leading federal government and commercial pharmacy robotics manufacturer. Directed and analyzed vulnerability scans (SCAP, Retina, and Nessus) within simulated DoD VMware lab environment, to include manual STIG assessments, compliance and cybersecurity policies evaluation (POA&M). (CSAM), (NIST), (US-CERT), (HIPAA), (FISMA). Executed Tier 4 troubleshooting of Windows 2008 R2 application server software issues, Windows 7 workstations and associated systems; VMware vSphere ESX, remote production, corporate applications, onsite research and development environments. Regulated testing, auditing and legal evaluation of core applications against inventory of system patches and upgrades to ensure compatibility with software development life cycles (SDLC), DoD and commercial cybersecurity operations. Orchestrated WSUS (Windows Server Update Service) and SolarWinds Patch Manager deployment of Microsoft Patch Tuesday updates; including application packaging, system performance smoke testing and patch management. Leveraged Windows command line scripting for cybersecurity compliance automation and advanced Excel engineering to render analytical metrics on health of production robotic fleet. Achieved ATO (Authorization to Operate) status by contributing technical and tactical expertise on DIACAP audits. Information Assurance Security Specialist II Jacobs Tybrin - Fort Lee, VA February 2012 to May 2012 Department of Defense (DoD) Contractor. Held accountability for compliance with DoD and Army cybersecurity protocols by conducting vulnerability testing of Logistical Standard Army Management Information Systems (STAMIS) for Tactical Logistics Systems at Software Engineering Center/Tactical Logistics Directorate. Appraised SCAP, Retina and Nessus vulnerability results for Windows 7 and Windows Server 2008 lab simulations. Identified issues and expedited resolution for government, military and COTS applications. Created Hyper-V virtual hosts with STIG GPO implementations. Configured and deployed Ghost images for

Windows 7 desktops and Windows Server 2008 R2 application servers. Leveraged high-level understanding of STAMIS and associated applications, as well as DoD Information Assurance Certification and Accreditation Process (DIACAP) to ensure compliance with regulations. (NIST), (US-CERT), (FISMA), (ACAS), (POA&M). Senior Systems Administrator - SAMS-E - Kuwait McLane Advanced Technologies - Temple, TX June 2009 to November 2010 Relocated by McLane) Department of Defense (DoD) Contractor. Certified system hardness and cybersecurity requirements through deployment of Army-approved Information Assurance Vulnerability Assessment (IAVA) releases, STIG and anti-virus updates, Retina vulnerability scans and Risk Management Framework (RMF) analysis. (NIST), (US-CERT), (FISMA). Framed and implemented Standard Operating Procedures (SOPs), operating manuals, PowerPoint presentations and technical documentation to ensure strict adherence to security system performance and regulatory standards. Spearheaded scripting automation of major SAMS-E software upgrades. Expedited Windows systems administration, application server administration and CSSAMO lead expertise during Kuwait deployment to ensure optimal availability of SAMS-E within STAMIS 24/7 environment. Excelled with subject matter expert (SME) requirements with vision and innovation to swiftly and accurately resolve data integrity, user assessments and software or hardware failures. Regulated maintenance of all desktops and laptops, HP network printers, Oracle 11g application servers, Dell managed switches, and fiber optics. Education Diploma of Distinction in Computer Programming And Operations Computer Learning Center - Fairfax, VA Skills ACTIVE DIRECTORY, DNS, ENCRYPTION, NETWORKING, SOLARWINDS, TCP/IP, NESSUS, NIST, SECURITY, VISIO, DHCP, TCP, VMWARE, APPLICATION PACKAGING, R2, AUTHENTICATION, GHOST, MULTI-FACTOR AUTHENTICATION, MFA, RSA, testing, training Military Service Branch: United States Army Rank: Civilian Contractor Additional Information Skills Platforms: Windows 7, Windows 10, Windows Server 2008-2012 R2, VMware. Security: DISA, Army Gold Master, SCAP, BeyondTrust Retina, Tenable Nessus, NIST, MalwareBytes, US-CERT, Windows Server Update Service (WSUS), SolarWinds Patch Manager, Symantec Encryption Desktop, Windows Group Policy (GPO), POA&M, Identity IQ, Windows Registry, Multi-Factor Authentication, (MFA), RSA,

Symantec Endpoint, McAfee, Norton, Global Protect, Dell Change Auditor, CSAM. Networking: TCP/IP, Active Directory, DNS, DHCP, wireless. Tools: Microsoft Office Suite (365, Word, Outlook, PowerPoint, Excel, Communicator, Project, Lync, Skype for Business), Adobe Acrobat, Symantec Ghost Solutions, Visio, PowerShell, Service Now. Additional: Application packaging, attention to detail, auditing, automation, leadership, presentations, policy development, reporting, technical documentation, troubleshooting, upgrades.

Name: John Rhodes

Email: tknapp@example.net

Phone: +1-405-389-2474x0572