Anthony Hudnall
Cell 448-777-2302
anthony.hudnall@gmail.com
usaf email Anthony.Hudnall.1.ctr@us.af.mil
GitHub profile https://github.com/Anthonyhudnall92

Objective: To obtain a position that will enable me to use my technical and organizational skills, educational background, and ability to work well with people

Qualifications:

- Identify and diagnose moderate to complex problems and implement solutions rapidly and effectively.
- Strong ability to quickly learn/retain information specific to hardware configurations and software applications.

Skills and Abilities:

- Submitting Remedy Tickets for COTS and GOTS
- Help Desk Trainer for FAA support 100+ Technicians.
- Computer System Repair/Computer Technician
- Complex Problem Solving
- Reporting and analysis eMASS
- Writing security impact analysis or Concept of operation for special test equipment
- Application Troubleshooting with GOTS software development team
- I have implemented Splunk, Nessus, SCAP Scanners and STIGS, CKL on multiple collateral and AP enclaves.
- Dameware NT Utilities
- RedHat 7, 8, 9 or Ubuntu 22.04 LTS (Jammy Jellyfish)
- SQL Server 2019 or 2022
- Microsoft OS: Windows 10 or 11
- Nessus vulnerability scanner, OpenVAS, or RedHat ACAS Kickstart, SCAP & STIG Viewer or Evaluate-STIG
- Host Base Security System (HBSS) , sentinelone , CrowdStrike SolarWinds NPM, Splunk
- Cisco, Fortinet, Pfsense , Ubiquiti,
- VMWare ESXI Version 7, VMWare Workstation Pro 17, Hyper-Visor, Docker, Kubernetes, LXD/LXC containers , Proxmox
- Powershell, Bash, Ansible, JuJu, Git, Terraform, YAML, Python

Operating Systems and Software Application Experience

- Microsoft Office 2016 or Office 365
- Windows Server 2019 or 2022

Certifications:

- CompTIA Security +
- Pursing CISSP

Clearance Level:

- Top Secret Security Clearance (Active) 2020

Education:

- Associate of Art – Northwest Florida State College 2016
- Bachelors of Science – Project Management in Technology Management – Northwest Florida State College 2019
- Pursuing Master's Degree -- Cyber Security – Western Governor University

Professional Experience:

Rackner DevSecOps Engineer Date:02/2023-02/2024

- On-site customer support working to resolve complex customer problems related to AWS and Ubuntu OpenStack technologies, Juju, MAAS, charms, as well as general Ubuntu Server.
- Research issues with databases, IaaS, PaaS, SaaS for customer.
- Experienced with IaC such as Terraform, Ansible-Playbooks, AgroCD, Kustomize, YAML, Git, GitHub Actions
- Support continuous integration / continuous development for customers using DevOps tools such as Gitlab, Kubernetes, Docker, LXD/LXC containers, and Vagrant.
- Coordinate meetings with software developers for applications that will need to be tested and deployed.
- Incorporate secure code best practices with the code.
- Experienced with generating CA and other credentials.
- Experienced with deploying large scale nodes, lxd, and containers.
- Proficient with PowerShell, , SQL, Python, Bash and Juju
- Proficient with stig automation and implementation and providing reports for CAT I, II, III
- Experienced with VLANS XVLANS and HA implementation for nodes and clusters.

Qualis Corporation Information Systems Security Officer III Date: 06/2022-02/2023

References available upon request

- Executed documentation including Security Control Traceability Matrices (SCTM), Systems Security Plans (SSP), Information Assurance Standard Operating Procedures (IA SOP), SIEM Continuous Monitoring Plans, Risk Appetite, Risk Assessments, Plan of Action & Milestones (POA&M), equipment specifications, practices and procedures.
- Executed SIEM Continuous Monitoring with Crown Bowl, Splunk, SolarWinds, SentinelOne for Collateral and AP enclaves. activities as required by frequency.
- Performed Security Impact Analysis (SIA) with MKRun, ACAS and Tenable Nessus to capture and create a CVE score.
- Implement NIST 800-53 ver 4 and 5 control families, and Joint Special Access Program JSIG, SAP Cybersecurity controls.
- Verifying Configuration Management (CM) of all associated hardware, software, and security relevant functions is maintained and documented. In addition, collecting letter of volatility (LOV) from vendors if possible or creating LOV for logic bearing component.
- Experienced with applying system requirements and techniques for planning current and future system architecture.
- Experienced with commonly applied principles, concepts, and methodologies, operating characteristics and capabilities of systems, media, equipment, and related software systems, processes and procedures and assisting Change Control Board CCB.
- Experienced with requirements and procedures for monitoring systems security and responding to network security incidents on network enclaves.
- Performed compliance audits and system configuration on multiple networks and standalone machines weekly for unclassified and classified enclaves. Ensuring HBSS Anti-virus engine / agents are compliant.
- Coordinated, 692nd Networks level III and IV VTCs with Navy VTCs AF7 VTCs SIPRNet VTCs NIPRNet VTCs
- Understand network ports and protocols such as DNS, DHCP, TCP, UDP,SIP, Layer 2 and Layer 3
- Experienced with conducting TEMPEST assessment and inspection for unclassified/classified network infrastructure.
- Performed daily duties to ensure integrity and confidentiality of sensitive data.
- Knowledgeable of Wireshark practices and procedure for software & security vulnerabilities.
- Performed sanitization procedures and release of hardware in accordance with IA security policies or Authorizing Official (AO) guidance.
- Performed information systems reviews to ensure compliance with the security authorization package.
- Communicate any changes or modifications to hardware, software, or firmware of a system with the 96TW ISSM and AO/DAO prior to the change
- Verified network enclaves information systems are operated, maintained, and disposed of in accordance with the Risk Management Framework (RMF) documented security policies and procedures including but not limited to Certification & Authorization (C&A).

Colsa Corporation IT Analyst level III Date: 03/2021-06/2022

- Provided customer support to 2000+ users between Eglin AFB, Robins AFB, China Lake AFB, on several secure networks.
- Created SOPs, SSP, HMF, SCTM, SIA for system administrators, ISSO, ISSM, GSSO, PSO
- Implemented SIEM with Splunk, Corner Bowl and SIEM PowerShell command-let on Windows and Linux environments
- Experienced with windows and Linux audits and CM assessments on collateral and special program networks
- Held privilege to general user access with NIPRNet, SIPRNet, 692nd Networks, JWICs, FENCES, DARPA and offline networks
- Conducted vulnerability scans of windows and Linux utilizing , HBSS, SentinelOne, ACAS, and SCAP, Nessus, Vulnerator for compliance/configuration audits
- Implements, enforces, communicates, and develops security policies or plans for, software applications, hardware, telecommunications, and information systems security education/awareness programs for customers on JSIG/ Collateral networks
- Executed RMF policies and procedures for AMRAAM and how to assess/ address the organization risk-appetite
- Performed daily duties to ensure availability, integrity and confidentiality of sensitive data.
- Oversaw TEMPEST assessment and inspection for unclassified/classified network infrastructure.
- Planned VIPer/STE update to keep 200+ users in compliance policies and procedures
- Coordinated level III and IV VTCs with Navy VTCs AF7 VTCs SIPRNet VTCs NIPRNet VTCs
- Understand network ports and protocols such as DNS, DHCP, TCP, UDP,SIP, Layer 2 and Layer 3
- Upgraded 200+ Thin clients to Red Hat virtual environment
- Oversaw VMWare 6.0 upgrade to 7.0 and utilized window
- Developed standalone systems accreditation ATO packages and POA&M system accreditation procedures for collateral/classified networks.

- Experienced with eMass and RMF packages, and CCI bridging the gap between high-level policy expressions and low-level technical implementations

Qualis Corporation Systems Administrator (USAF DoD Ctr) Date:08/2020-03/2021

- Provide client support to 500+ users on a number of secure networks.

References available upon request

- Experience with sustaining Windows Domains as well as creating and managing Group Policies on unclassified/classified systems.
- Interfaces directly with supported 500+ end-users to provide hardware, software, network and applications problem resolution.
- Experienced with use of vulnerability scanning software STIG, ACAS, and SCAP, Nessus, Vulnerator for compliance/configuration audits.
- Performed compliance audits and system configuration on Microsoft Windows and Redhawk, Red Hat Linux systems and standalone machines weekly for unclassified and classified enclaves.
- Experienced with Windows PowerShell and understanding of DNS, DHCP, TCP, UDP, Layer 2 and Layer 3
- Proficiently applies required security patch updates to Microsoft Windows and Red Hat Linux systems on unclassified/classified networks.
- Build and load new OS software to meet current USAF standards and compliance on Microsoft and Red Hat Linux systems.
- Experienced with information assurance & technology principles, concepts, practices, systems software, database software, and immediate access storage technology required to carry out activities.
- Ability to assess and advise on a variety of sources and procedures and methods for systems and applications.
- Experienced with applying system requirements and techniques for planning current and future system architecture.
- Experienced with commonly applied principles, concepts, and methodologies, operating characteristics and capabilities of systems, media, equipment, and related software systems, processes and procedures.
- Experienced with requirements and procedures for monitoring systems security and responding to network security incidents.
- Experienced with troubleshooting hardware and software network problems, examining systems and processes for potential security violations; determined if breeches occurred and applied appropriate steps to mitigate any adverse impacts.
- Experienced with conducting TEMPEST assessment and inspection for unclassified/classified network infrastructure.
- Performed daily duties to ensure integrity and confidentiality of sensitive data.
- Knowledgeable of Wireshark practices and procedure for software & security vulnerabilities.

Odyssey Systems Network Admin (USAF DoD Ctr) **Date: 11/2017 – 08/2020**

- Provide client support to 300+ users on a number of secure networks.
- Interfaces directly with supported end-users to provide hardware, software, network and applications problem resolution.
- Resolves partial system failures (software or hardware-related) by providing for revised applications of system operating capabilities
- Experienced with use of vulnerability scanning software STIG, ACAS, and SCAP for compliance/configuration audits.
- Performed compliance audits and system configuration on multiple networks and standalone machines weekly for unclassified and classified enclaves.
- Ability to execute large data transfers on multiple networks on a weekly basis to prevent data loss.
- Proficiently applies required security patch updates to unclassified and secure networks.
- Build and load new OS software to meet current USAF standards.
- Experienced with information assurance & technology principles, concepts, practices, systems software, database software, and immediate access storage technology required to carry out activities.
- Ability to assess and advise on a variety of sources and procedures and methods for systems and applications.
- Experienced with applying system requirements and techniques for planning current and future system architecture.
- Experienced with commonly applied principles, concepts, and methodologies, operating characteristics and capabilities of systems, media, equipment, and related software systems, processes and procedures.
- Experienced with requirements and procedures for monitoring systems security and responding to network security incidents.
- Experienced with troubleshooting hardware and software network problems, examined systems and processes for potential security violations; determined if breeches occurred and took appropriate steps to mitigate any adverse impacts.
- Experienced with conducting TEMPEST assessment and inspection for unsecure and secure network infrastructure.
- Performed daily duties to ensure integrity and confidentiality of sensitive data.
- Experienced with ENDR, DRA, Security Groups and GPOs for NIPRNet and SIPRNet
- Experienced with DARPA network infrastructure.
- Experienced with standalone system ATO packages and POA&M system accreditation procedures.
- Experienced with setting up SVTC, VTC for NIPRNet and SIPRNet.

CACI Help Desk Technician (FAA Ctr) **Date: 05/2017 – 10/2017**

- Experienced administrator of Windows Active Directory for password resets, group policies, and procedures
- Knowledgeable of clerical procedures for word processing, managing files, records and other procedures for Remedy 8.1
- Knowledgeable of procedures for Dameware mini tool use for updating software and other applications

Internships:

SLE98 TECHNOLOGIES LLC -Cyber Security Consultant Date 2020 - Present

References available upon request

- Spearheaded large-scale projects for customers involving revamping their network controls and implementing ConMon solutions. Creating real time incident response dashboards with SIEM solution.
- Investigate and assess the threat posture of the customers network and provide a detailed write-up incident report, including the root cause, identification and remediation recommendations that aligns with the customers' current budget.
- Resolve website filtering security concerns implementing Fortinet and Cisco solutions.
- Mitigated potential data leaks holding sensitive information. In addition, providing customer cyber security awareness training.
- Provide continued maintenance and development for network infrastructure applying patches and remediating bugs for existing web applications.

Okaloosa County School District; **Computer Support** **Date: 05/2013 – 08/2013**

- Completed UWF computer IT summer program
- Deployed both Microsoft and Apple hardware devices throughout school district for classroom technology update.

Volunteer Experience:

Praise, Power, and Compassion Ministry Date: 09/2008 – Present

- Provide daily technical support for e-mail, network, connectivity, peripheral equipment, and system maintenance
- Set up computers and install software. Maintains wireless network infrastructure supporting 200+ user

References available upon request