JUSTIN M. JOHNSON

Atlanta, GA
850.691.9708 ✧ e-mail: justin@initcyber.com
https://www.initcyber.com ✧ https://www.linkedin.com/in/imjustinjohnson/

LEAD INFORMATION SYSTEM SECURITY ENGINEER ✧ CYBER SECURITY ANALYST

Clearance ✧ Top-Secret ✧ Active (Tier 5 Investigation Complete 7/2019)

Cybersecurity and Information Technology Professional with a proven history of delivering high-quality results, swiftly addressing technical challenges, and resolving issues quickly. Adept in a broad range of system and security protocols, cutting-edge technologies, and defensive measures for safeguarding digital infrastructure. Offers extensive hands-on experience with Windows, Linux, Vulnerability Scanning/SIEM, and GRC Tools. Equipped with strong communication, presentation, teamwork, and analytical skills. Eager to contribute my knowledge and innovative spirit to stimulating and impactful initiatives. I bring a comprehensive understanding and skill set in Zero Trust architecture and DevSecOps methodologies, ensuring robust security integration in every phase of development.

CERTIFICATIONS

ISC(2):
- Certified Information System Security Professional (CISSP)

CompTIA
- A+
- Network+
- Security+

Microsoft:
- Certified: Azure Fundamentals
- 365 Certified: Fundamentals
- Certified: Security, Compliance and Identity Fundamentals

AWS:
- Solutions Architect Associate

PROFESSIONAL EXPERIENCE

SeKON ✧ Rosslyn, VA ✧ 2020 – Present ✧(Active Top-Secret Clearance)
Lead Information Systems Security Engineer / CONMON + Compliance Management

- Led a team of Information Systems Security Engineers who reported to Government Leadership on daily tasks and developed/improved team processes.
- Reviewed the guidance from CISA and DISA and offered recommendations to our current Cyber team members on how to effectively implement best practices based on that guidance.
- Analyzed Executive Orders (EO), Office of Management and Budget (OMB) policies, and other relevant guidelines to offer additional instructions and insights to team members. This included topics such as Zero Trust (NIST 800-207) and the changes introduced in NIST RMF Revision 5.
- Received Cyberspace Tasking Orders from JFHQ-DODIN and offered guidance to system engineers and administrators on addressing remediation tasks and meeting the specified deliverables."
- Received multiple recognitions from Government and Corporate Leadership for delivering outstanding results in a timely and efficient manner.
- Managed and developed policies, standard operating procedures, directives and deliverables for the Cybersecurity Team, as well as maintaining the accuracy of the documents.
- Provided support and response coordination with the government in completing annual reviews, risk assessments, and impact assessments for ATO efforts.
- Assisted with developing Contingency Plans with other teams (ISSO's) for RMF and ATO Requirements.
- Implemented automation of weekly vulnerability scanning from ACAS into eMASS, which included connecting Information Systems to DISA's Continuous Monitoring and Risk Scoring (CMRS) dashboard, and developing Splunk Dashboards to capture and monitor RMF 800-53 controls
- Reviewed Security Packages with the ISSO's and suggested appropriate STIG/SRG recommendations (and related Test Plans) for Annual Reviews and ATO events (Risk Assessments, Impact Assessments, etc.).
- Conducted SCAP scans and completed STIG Checklists for information systems.
- Configuration Management, Change Requests, POA&M management.
- Provided policy expertise and assisted in writing several technical proposals for bids on other government contracts.

Georgia Tech Research Institute ✦ Atlanta, GA ✦ 2018 – 2020 ✦(Top-Secret Clearance)
Information Systems Security Officer

- Risk Management Framework (RMF), NIST SP 800-37 (800-53 controls), Joint Special Access Programs Implementation Guide (JSIG) and National Industrial Security Program Operating Manual (NISPOM).
- Developed and wrote Security Documentation for Information Systems to include: Security Control Traceability Matrix (SCTM), System Security Plans (SSP)/Security Assessment Plans (SAP), Contingency plans, Risk Assessment Reports (RAR), Continuous Monitoring and Plans of Action and Milestones (POAM) for systems, as well as maintaining system design/architecture throughout the lifecycle of the information system.
- Conducted weekly vulnerability scanning utilizing vulnerability scanning and SIEM tools such as Nessus and Splunk. Monthly Patching of Nessus Scanners.
- Conduct weekly/annual cyber-security training to both technical and non-technical personnel.

Mount Vernon Towers ✦ Atlanta, GA ✦ 2018
IT Technician

- Redesigned company network to optimize data, efficiency, and cost by integrating multiple external services.
- Established testing and hardening practices for network and physical security.
- Assisted residents and employees with day-to-day IT issues and new technologies.
- Managed wireless and wired networking, VPN, and IP/POT Telephones.

Bay County Sheriff's Office ✦ Panama City, FL ✦ 2013 – 2018
Corporal, Field Services Division

- Supervise and lead multiple patrol deputies.

EDUCATION

Colorado State University-Global Campus, Greenwood Village, CO: 2018
Bachelor of Science- Information Technology, Specializing in Cyber Security

Florida State University, Tallahassee, FL: 2011
Bachelor of Science – Criminology

TOOLS AND SKILLS

CLOUD	AWS/Google/Azure/Oracle
GRC TOOLS	eMASS
IAC/AUTOMATION	Ansible, Terraform
Network/Network Design	Firewalls, Routers, Distributed Networks/VPNS, VLANS, etc.
OPERATING SYSTEMS	Windows (10/11, Server 2016/2019/2022), OSx and Linux/FreeBSD
PROGRAMMING AND SCRIPTING	Python, Powershell, Bash, Git
REGULATORY COMPLIANCE	NIST 800-37, 800-53, 800-171. Zero Trust (800-207), HIPAA
SIEM/VULNERABILITY MANAGEMENT	Splunk, ELK, Nessus (Tenable)/ACAS, OpenVAS
SERVER ADMINISTRATION	Windows and Linux
VIRTUALIZATION	VMware (ESXI/vSphere/vCenter), Microsoft Hyper-V, KVM/QEMU/libvert

PERSONAL PROJECTS

Homelab Environment ✦ GitHub - initcyber/homelab

Currently designing and implementing a hybrid cloud homelab as a testing environment for Proof of Concept (PoC) ideas, leveraging Terraform and Ansible playbooks to create a virtual machine environment. It currently utilizes several logging and monitoring solutions such as Splunk and Wazuh and CI/CD Pipelines using GitHub Actions and integrated security tools to streamline development and testing processes.

Detailed Professional References Available upon Request

✦ ✦ ✦