# Justin Johnson

Atlanta, GA justin@clouddefenselabs.com (850) 691-9708 www.clouddefenselabs.com
imjustinjohnson clouddefenselabs

## Information Systems Auditor SME

Highly accomplished Information Systems Auditor SME with 10+ years of experience in cybersecurity and IT management. Proven track record of delivering exceptional results, leading teams, and implementing best practices in compliance and risk management. Skilled in Zero Trust architecture, NIST RMF, and regulatory compliance. Proficient in cloud security, vulnerability scanning, and governance frameworks.

## Education

**MBA** **Western Governors University**, MBA - IT Management — Aug 2024 – May 2025
- Masters of Business Administration - In Progress

**B.Sc** **Colorado State University-Global Campus**, Cyber Security — Aug 2016 – May 2018
- 4.0 GPA
- Magna Cum Laude

**B.Sc** **Florida State University**, Criminology — Aug 2007 – May 2011
- 3.7 GPA

## Experience

**SeKON**, Information Systems Auditor SME — Atlanta, GA (Remote) Aug 2020 – present
- As an Information Systems Analyst SME/Systems Security Steward Lead, I support the CDC's mission to protect public health through innovative IT solutions and robust cybersecurity measures. Working with SeKON Enterprise, Inc., I contribute to the security, integrity, and compliance of the CDC's information systems while supporting the agency's digital transformation efforts.
- Leading a team of Information Systems Analysts/Systems Security Stewards in supporting the CDC's mission to protect public health through innovative IT solutions and robust cybersecurity measures
- Execute Authorization & Accreditation (A&A) processes within the NIST SP 800-37 Risk Management Framework (RMF).
- Evaluate information systems' security control compliance with federal requirements and CDC's monitoring strategy.
- Ensure system operations align with approved security authorization packages.
- Vulnerability Management
- Conduct annual assessments to ensure compliance with CDC standards.
- Participate in Configuration Control Board (CCB) activities to manage cybersecurity-relevant configurations.
- Provide expert guidance on cybersecurity best practices and CDC's monitoring strategy.
- Communicate effectively with stakeholders to track and report on information system monitoring efforts.

**SeKON**, Information Systems Engineer Lead — Atlanta, GA (Remote) Oct 2022 – Oct 2024
- 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.
- Implemented Cybersecurity Dashboards integration with several Programs/Systems of Record
- Developed Splunk Dashboards to be used as a SIEM tool to monitor system logs and events, metrics, and NIST 800-53 Control Families
- Implemented Automated Vulnerability Scanning capabilities which were directly/automatically fed into eMASS.
- Reviewed Quarterly STIGs and SCAPs for each Information System to Ensure Compliance was met.

**SeKON**, Information Systems Engineer — Atlanta, GA (Remote)
Aug 2020 – Oct 2022

- Cybersecurity leader with a proven track record in elevating government systems to full ATO certification. Successfully spearheaded the transition of multiple Systems of Record from ATO-C to ATO status, showcasing expertise in security compliance and stakeholder management. Adept at devising efficient strategies to meet stringent government regulations while fostering seamless collaboration between technical teams and government stakeholders.
- Implemented DISA's Continuous Monitoring and Risk Scoring (CMRS) system's API to eMASS for various Information Systems, utilizing ACAS Security Center for integration with eMASS.
- Conducted weekly ACAS scans, providing ASR/ARF pair files to ISSOs and verifying CMRS results for accuracy. Offered feedback on false positives, vulnerabilities, and IAVMs.
- Audited Information System Security Packages to ensure sponsor/customer compliance.
- Supported ISSOs during Quarterly and Annual Security Reviews, selecting appropriate STIGs/SRGs and reviewing STIG checklists.
- Actively participated in Configuration Management, Change Requests, and POA&Ms throughout the RMF Lifecycle, focusing on steps 2-4 and 7.
- Authored Standard Operating Procedures (SOPs) for Cyber Security and Information Systems Security Engineering teams.
- Validated POAM and TSAR documentation from joint entities for completeness and accuracy.
- Ensured system security requirements, tools, and architecture compliance for various systems.

**Georgia Tech Research Institute**, Information Systems Security Officer — Atlanta, GA
Nov 2018 – Aug 2020

- Implemented the Risk Management Framework (RMF), NIST SP 800-37, JSIG, and other relevant compliance documents.
- Developed Security Documentation for Information Systems, including SCTM, SSP/SAP, Contingency Plans, RAR, Continuous Monitoring, and POAM, while maintaining system design throughout the lifecycle.
- Conducted weekly vulnerability scans using Nessus and Splunk, with monthly patching of Nessus scanners.
- Delivered weekly and annual cyber-security training for technical and non-technical personnel.

**Mount Vernon Towers**, IT Technician — Atlanta, GA

- Redesigned company network to enhance data efficiency and reduce costs by integrating external services.
- Established testing and hardening practices for network and physical security.
- Assisted residents and employees with daily IT issues and new technologies.
- Managed wireless and wired networks, VPN, and IP/POT telephones.

July 2018 – Nov 2018

**Bay County Sheriff's Office**, Corporal, Field Services Division

Panama City, FL
July 2013 – July 2018

- Supervised and led multiple patrol deputies.

## Current Certifications

**CISSP**, ISC(2)

**AWS Solutions Architect Associate**, Amazon Web Services

**Azure Fundamentals**, Microsoft

**Office 365 Fundamentals**, Microsoft

**Security Compliance and Identity Fundamentals**, Microsoft

**Security+**, CompTIA

**Network+**, CompTIA

**A+**, CompTIA

## Projects

**Hybrid Cloud Homelab**

github.com/clouddefenselabs/homelab

- Currently designing and implementing a hybrid cloud homelab as a testing environment for Proof of Concept (PoC) ideas.
- Utilizes several logging and monitoring solutions such as Splunk and Wazuh.
- CI/CD Pipelines for automation with Github Actions.
- Integrated security tools for streamline development and testing processes.

## Technologies

**Languages:** Python, Powershell, Bash, Git

**Technologies:** Cloud (AWS, Azure, GCP, Oracle) VMware, KVM, Hyper-V

**Tools:** Ansible, Terraform, Splunk, Wazuh, Nessus, VMware, AWS, Azure, Docker, Splunk, ELK, Nessus,

**Regulatory Compliance:** NIST 800-37/800-53/800-171, Zero Trust (800-207), HIPAA, JSIG, NIST Cybersecurity Framework