Alvaro A. Sanchez Almanzar

Email: alvaro1688@gmail.com
Cell: 301-820-5977
Active: Public Trust (Department of The Treasury "IRS")
Digital Resume: Online Resume

EXPERIENCE SUMMARY

Results driven Cybersecurity and Risk Management Analyst with 7+ years of experience securing enterprise systems and ensuring compliance with federal standards, including FISMA, FedRAMP, and NIST 800-53. Proven expertise in vulnerability management using tools such as Tenable Security Center, Qualys, and Nessus, and applying DISA STIGs and CIS Benchmarks for security hardening. Skilled in system security planning, POA&M management, and cross-functional remediation coordination. Experienced with cloud security, compliance documentation, and risk assessments across diverse environments.

Entry-level Python and .NET developer with foundational skills in scripting, automation, and secure coding practices. Complemented by 2 years of hands-on experience as a Power BI Data Analyst, building dynamic dashboards, performing data modeling, and delivering actionable insights through data visualization. Strong communicator, detail-oriented, and committed to continuous learning and process improvement

CERTIFICATIONS.

- ✓ ISC2 CC.
- ✓ CompTIA Security+
- ✓ CompTIA CASP+
- ✓ Azure AZ-900

EDUCATION

A.A.S Cyber Security, Montgomery College, 2018

SUMMARY OF SKILLS, TOOLS, AND TECHNOLOGIES

Coding Languages: Python, C#, HTML & CSS, JavaScript (Learning), Terraform (Training Completed)

CyberSecurity Tools: **Nessus** (Tenable Security Center), **Qualys**, **ServiceNow**, Jira, Rcats, CSAM

Operating Systems: Linux (5 yrs), Windows (15yrs), Mac OS (15yrs)

Data Analysis: PowerBI Data visualization & Dashboard creation (2yrs)

EXPERIENCE DETAILS

<u>Booz Allen Hamilton (NIH Project) & (IRS Project-IRS)</u>

October 2022 – Present
Senior Cybersecurity Vulnerability Engineer

- Led full-cycle implementation of the Risk Management Framework (RMF) to support Authorization to Operate (ATO) in compliance with NIST SP 800-53 Rev. 5, working closely with ISSMs, System Owners, and Authorizing Officials to deliver core security documentation (SSPs, FIPS-199, BIA).
- Supported cloud security initiatives by collaborating with the Cloud Assessment Security Office (CASO) on the development and revision of security documentation for Microsoft Azure Government (MAG) environments.
- Executed organization-wide vulnerability management programs, identifying, prioritizing, and remediating risks using tools like Qualys VMDR, BigFix, and ServiceNow, leading to a measurable reduction in risk posture.
- Performed advanced Qualys Policy Compliance tuning, aligning policies to CIS Benchmarks and NIST controls, reducing false positives and enhancing scan accuracy through control customization (e.g., password complexity, timeout thresholds).
- Integrated Qualys VMDR with BigFix for streamlined patch management, accelerating remediation timelines and improving operational efficiency.
- Conducted regular vulnerability scans and coordinated with cross-functional teams to remediate high-risk findings, particularly in hybrid and cloud infrastructures.
- Mentored junior staff and led security awareness sessions to build internal cybersecurity competencies and a culture of continuous improvement.
- Delivered detailed risk and compliance reports to executive leadership, offering actionable insights and strategic recommendations to enhance the security program.
- Maintained expert-level awareness of emerging cybersecurity threats, compliance trends, and best practices to proactively safeguard systems.

Power BI Data Analyst Responsibilities (Concurrent)

- Built and maintained interactive dashboards and business intelligence reports using Power BI, enabling real-time insights and data-driven decisions.
- Conducted data modeling using DAX to optimize performance and reporting accuracy across large datasets from databases, cloud services, and Excel.
- Validated and troubleshot dashboards for performance, ensuring accurate, up-to-date reporting and stakeholder confidence.
- Provided training to end-users and executives on dashboard navigation and data interpretation.
- Developed Excel reports using PivotTables, VLOOKUP, and advanced formulas to analyze trends, support compliance reporting, and optimize data integrity.

WhiteHat Auditors

December 2021 to October 2022
Senior Cybersecurity Engineer and Information Assurance Specialist
(Summarized)

- This role involved leading the vulnerability management program, overseeing the full lifecycle from identification to remediation. Responsibilities included preparing documentation based on customer information using accepted guidelines like the Risk Management Framework (RMF) and working with Information System Security Officers (ISSOs) and the Authorizing Official (AO) to support FISMA systems through the Security Assessment & Authorization (SA&A) lifecycle.
- The position also involved preparing Security Test and Evaluation Plans, providing certification and accreditation support, and conducting risk and vulnerability assessments. Duties included analyzing policies against federal regulations, developing and updating system security and contingency plans, recommending security improvements, scanning systems for compliance, and performing vulnerability assessments.
- The role also required communication with auditors, creation and management of Plans of Action and Milestones (POA&Ms) and conducting configuration compliance checks against standards like DISA STIGs and CIS Benchmarks.

The Department of Energy

12/2019 – 12/2021
Federal Employee
Germantown Md
Information System Security Officer (ISSO)
(Summarized)

- The role involves reviewing business system missions and objectives, collaborating with system owners and the Information System Security Manager (ISSM) to ensure compliance with NIST, the Office of the Chief Information Officer policies, and the risk-based cybersecurity program for CFO-managed applications. Responsibilities include assisting with drafting system security plans (SSP), system categorization, business impact analysis, contingency plans, and obtaining ISSM approval.
- The position also entails developing and maintaining security authorization package documentation, including security plans, disaster recovery plans, privacy impact assessments, and Plans of Actions and Milestones (POAMs), and ensuring timely updates to system security plans. The individual will coordinate annual assessments and accreditations, track Authorization to Operate (ATO) dates, review risk logs, and provide recommendations for resolution.
- Other duties include supporting privileged and service account reviews, analyzing vulnerability scans, offering mitigation strategies, tracking vulnerabilities, and staying informed on emerging threats, offering solutions, and conducting reconnaissance activities for FISMA systems.

Oasis Systems

***(**08/2018 – 12/2019)*
Federal Contractor
Rockville, MD
Information Assurance & Vulnerability Specialist
(Summarized)

- The role involves preparing documentation based on customer information using guidelines like the Risk Management Framework (RMF), collaborating with Information System Security Officers (ISSOs) and Authorizing Officials (AOs) to support FISMA systems through the Security Assessment & Authorization (SA&A) lifecycle.
- Responsibilities include creating Security Test and Evaluation Plans, assisting with certification and accreditation, developing security and contingency plans, conducting risk and vulnerability assessments, and analyzing policies for compliance with federal regulations.
- The position also involves recommending system enhancements to address security deficiencies, scanning for compliance, and performing vulnerability assessments, configuration compliance checks, and risk mitigation strategies using standards such as DISA STIGs and CIS Benchmarks.

PowerBI Projects

Cybersecurity Vulnerability Dashboards

As a PowerBI Data Analyst, I have successfully integrated Tenable Security Center data with PowerBI to provide the Cybersecurity Department with actionable insights and visualizations on network vulnerabilities and security risks. By leveraging the combination of PowerBI's interactive reporting capabilities and Tenable's vulnerability scanning tools, I streamlined the process of monitoring, analyzing, and presenting cybersecurity risk data.

Key Responsibilities and Achievements:

- Integrated Tenable Security Center with Power BI to automate ingestion and transformation of vulnerability scan data, including CVSS scores, compliance flags, and asset risk metrics, improving data visibility and reporting efficiency.
- Developed structured Power Query scripts and custom data transformation pipelines to convert raw vulnerability data into actionable insights, enabling real-time dashboard updates.
- Designed and deployed custom Power BI dashboards for tracking key security KPIs: severity levels, asset exposure, remediation timelines, and compliance adherence.
- Created trend analysis and forecasting reports using DAX to identify recurring vulnerabilities and project remediation performance, including metrics like average time to patch and system compliance trends.
- Built automated alerting systems within Power BI to notify the cybersecurity team of high-priority vulnerabilities and compliance violations, significantly reducing response times.
- Delivered intuitive, interactive dashboards to stakeholders including security engineers, risk teams, and executives, allowing for deep dives into vulnerability data and strategic risk assessments.
- Partnered with system administrators to validate scan results and ensure metrics remained aligned with the evolving threat landscape and organizational priorities.

- Created compliance-oriented reports aligned with NIST, CIS, and PCI DSS frameworks to support audit readiness and regulatory reporting.
- Produced detailed visualizations and data exports for external auditors, providing clear evidence of the organization’s vulnerability management program and its ongoing effectiveness.
- Significantly enhanced the organization’s cyber risk posture by combining advanced Power BI analytics with comprehensive vulnerability insights from Tenable.

Booz Allen Hamilton Open Req Report Dashboard

- Designed and developed an interactive PowerBI dashboard that enables employees to easily discover and explore other ongoing projects across the organization.
- Collaborated with cross-functional teams to gather requirements and understand the types of projects employees would be interested in.
- Integrated data from various company sources, such as project management tools and internal databases, ensuring real-time updates and data accuracy.
- Implemented advanced PowerBI features including filters, drill-through functionality, and custom visualizations to enhance user experience and usability.
- Provided training and support to employees, enabling them to efficiently navigate the dashboard and identify potential collaboration opportunities.
- Regularly updated and maintained the dashboard to ensure that it reflects the most current project information, project statuses, and team members.