Alvaro A. Sanchez Almanzar

**Email:** [alvaro1688@gmail.com](mailto:alvaro1688@gmail.com)

**Cell:** 301-820-5977

**Active: Public Trust (Department of The Treasury “IRS”)**

# EXPERIENCE SUMMARY

Dedicated Risk Management and Cyber Security Analyst with over 7 years of hands-on experience in ensuring robust security postures for complex systems within corporate environments. Proficient in leveraging Tenable Security Center, **Qualys**, Nessus Professional, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and Center for Internet Security (CIS) Benchmarks for vulnerability assessments and compliance scans.

Demonstrated expertise in navigating the Federal Information Security Modernization Act (FISMA) lifecycle, National Institute of Standards and Technology (NIST) 800-53 controls, and the Federal Risk and Authorization Management Program (**FedRAMP**) security packages. Adept at liaising with cross-functional teams to ensure timely remediation of security vulnerabilities and seamless cloud transitions. Proven leader in developing and maintaining comprehensive system security plans and POA&M strategies. Python and .Net entry level developer.

Detail-oriented and results-driven PowerBI Data Analyst with 2 years of experience in collecting, transforming, and visualizing data to create dynamic dashboards and reports. Expertise in developing interactive PowerBI reports, performing data modeling, and collaborating with stakeholders to deliver data-driven insights. Skilled in optimizing data models, enhancing reporting performance, and translating complex datasets into user-friendly business intelligence solutions.

## **CERTIFICATIONS. EDUCATION**

✔️ ISC2 CC. A.A.S Cyber Security, Montgomery College, 2018  
✔️CompTIA Security+

✔️CompTIA CASP+

✔️Azure AZ-900

## **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

## **Booz Allen Hamilton (NIH Project) & (IRS Project-IRS)**

*October 2022 – Present*

Senior Cybersecurity Vulnerability Engineer

* Led the implementation of the Risk Management Framework (RMF) process to support the system's journey to Authorization to Operate (ATO), ensuring compliance with NIST SP 800-53 rev.5 and other federal cybersecurity requirements. Collaborated with system owners, Information System Security Managers (ISSMs), and Authorizing Officials (AOs) to develop and review security documentation, including System Security Plans (SSPs), FIPs-199 Security Categorization, Business Impact Analysis (BIA), and other core documents.
* Provided subject matter expertise on RMF processes to internal teams, ensuring a clear understanding of requirements and supporting compliance efforts. Contributed to the creation of security documentation for ATO submission, including security categorization, risk assessments, and compliance evidence. Collaborated with cross-functional teams to prioritize ATO deliverables. Worked with the CASO team on updating and creating Cloud security documents and following up their step-by-step process.
* Led vulnerability assessment programs, by identifying, and analyzing security vulnerabilities across the organization's infrastructure. Developed and implemented comprehensive vulnerability management strategies, ensuring timely detection and remediation of security risks.
* Performed in-depth **Qualys Policy Compliance** (PC) tuning to improve accuracy and reduce false positives in security compliance reporting. This involved reviewing out-of-the-box policies, identifying misaligned or redundant controls, and customizing them based on internal security baselines and regulatory requirements (e.g., CIS, NIST). Collaborated with system owners to validate results, adjusted scan parameters and target scopes, and integrated feedback loops to ensure ongoing policy effectiveness.  
  for example: Edit control values (e.g., password length, timeout thresholds).
* Collaborated with cross-functional teams to prioritize and mitigate critical vulnerabilities found on **Microsoft Azure Government (MAG)** environments, reducing the organization's overall security risk posture by conducting regular vulnerability assessments to proactively identify weaknesses and recommend security enhancements.
* Implemented and managed security tools and technologies to automate vulnerability scanning and helped the patching team connect Qualys (**VMDR**) to **BigFix** to for the remediation/patching processes, resulting in increased efficiency and reduced time to resolution.
* Mentored and trained junior team members, fostering a culture of continuous learning and skill development.
* Prepared and presented reports to executive leadership, providing insights into the organization's security posture, and recommending proactive measures.
* Stayed abreast of the latest cybersecurity trends, emerging threats, and vulnerability management best practices to keep the organization's security posture ahead of potential risks.
* Performed comprehensive vulnerability management for a hybrid cloud infrastructure by leveraging Qualys for detection and **ServiceNow** for tracking vulnerability life cycle and workflow automation.
* Data Collection & Preparation: Gather data from various sources (e.g., databases, spreadsheets, cloud services) and preprocess it to ensure accuracy and consistency for reporting. Data Modeling: Build and optimize data models in PowerBI, creating efficient relationships between datasets and implementing calculated columns and measures using DAX to enhance reporting capabilities.
* Dashboard & Report Creation: Design and develop interactive PowerBI dashboards and reports that provide actionable insights to stakeholders, incorporating a variety of charts, tables, and visuals. Worked closely with business users, including executives and managers, to understand reporting requirements, ensuring dashboards meet their needs and provide meaningful data.
* Quality Assurance: Validate the accuracy and consistency of data in dashboards, ensuring real-time or up-to-date information. Troubleshoot and resolve any issues related to data sources or report functionality.
* Performance Optimization: Monitor dashboard performance and optimize data models for faster load times and report generation.
* Training & Support: Provide training to end-users on dashboard navigation and data interpretation, ensuring effective use of reports for decision-making.
* Reporting & Insights Delivery: Regularly update and distribute business intelligence reports, making sure stakeholders receive the necessary information to support their strategic decisions.
* Excel Functions: Proficient in using VLOOKUP to cross-reference and extract data from large datasets, improving data accuracy and workflow efficiency.
* Data Analysis: Skilled in organizing, summarizing, and interpreting complex data using Pivot Tables to create detailed reports and uncover trends.
* Data Management: Expertise in managing large datasets, cleaning data, and ensuring integrity while performing advanced analysis using Excel tools.
* Reporting & Visualization: Ability to design custom Excel reports and dashboards to present key metrics, trends, and insights to stakeholders.

## **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:**

Data Integration:

Utilized Tenable Security Center's API to extract vulnerability scan data, such as security risks, compliance issues, and threat assessments, and imported the data into PowerBI for analysis and reporting.

Ensured smooth integration by transforming raw Tenable data into a structured format using Power Query and custom scripts, enabling real-time data updates.

Custom Vulnerability Dashboards:

Designed and developed custom PowerBI dashboards to track key security metrics such as vulnerability severity (CVSS score), affected assets, exposure times, and remediation progress.

Presented critical insights on top security risks, prioritized vulnerabilities based on their impact on the organization’s systems, and helped highlight high-risk areas needing immediate attention.

Trend Analysis and Forecasting:

Used Power BI's analytical tools to identify trends in vulnerability occurrences over time, providing the cybersecurity team with predictive insights on potential future risks.

Leveraged Power BI’s DAX formulas to create metrics such as average time to remediate vulnerabilities and trends in system compliance across the enterprise.

Real-Time Reporting and Alerts:

Created real-time, automated reporting systems in PowerBI to send regular updates and alerts to the cybersecurity team, ensuring they are informed about high-priority vulnerabilities and compliance issues.

Enabled the creation of alerts and notifications in PowerBI when new critical vulnerabilities were detected by Tenable scans, facilitating quicker response times.

Enhanced Collaboration:

Delivered interactive and user-friendly dashboards to key stakeholders, including security analysts, risk management teams, and executives, allowing them to drill down into vulnerability data and make data-driven decisions.

Collaborated with cybersecurity engineers and system administrators to ensure the accuracy of vulnerability data and adjust report metrics according to the evolving threat landscape.

Reporting for Compliance and Auditing:

Developed compliance-focused reports based on industry standards such as NIST, CIS, and PCI DSS, helping the organization meet audit and regulatory requirements.

Produced detailed vulnerability reports and visualizations for external audits, ensuring transparency and supporting evidence of ongoing security efforts.

By combining PowerBI’s powerful visualization and Tenable Security Center’s comprehensive vulnerability data, I was able to enhance the Cybersecurity Department's ability to quickly identify, prioritize, and remediate security risks, ultimately improving the organization's overall security posture.

## **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.