Juashua Villarejos

Cybersecurity Engineer - USCIS SOC - Department of Homeland Security

Cybersecurity engineer with experience in SOC operations, incident response, Identity and Access Management and vulnerability management supporting a large federal enterprise environment. Proven track record in triaging complex security events, managing KEVs and ISVMs, automating Splunk workflows to reduce analyst workload and managing user accounts and access requests in accordance with least privilege standards to reduce organizational risk. Passionate about protecting privacy and mission critical assets while continuously improving processes, documentation, and team readiness.

Experience

Cybersecurity Engineer (SOC SADOM)
USCIS SOC / Aretec *Stennis Space Center, MS* | March 2025 - Current

Information Security Vulnerability Management (ISVMs)

- Review and process Known Exploitable Vulnerabilities (KEVs) to strengthen the agency's security posture and prioritize remediation.
- Analyze DHS/USCIS bulletins and technical advisories, translating them into actionable remediation tasks for stakeholders.
- Manage change records to support vulnerability remediation activities, ensuring policy compliance and operational stability.
- Build and maintain Splunk searches to track ISVM status and remediation, improving visibility and reporting accuracy for leadership.
- Assume ownership of the Cisco data call report, delivering weekly updates on vulnerability status and trends to DHS stakeholders.
- Participate in weekly coordination meetings to drive awareness of open vulnerabilities and improve response coordination.

Accounts and Access Management

- Complete onboarding, offboarding, and team-change requests, ensuring secure and timely account transitions across the environment.
- Process and validate access requests, enforcing least-privilege and standard approval workflows.
- Resolve ServiceNow tickets related to account provisioning and removal, reducing queue backlog and mis-provisioned access.
- Update and maintain GitHub documentation and runbooks, improving accuracy and reducing ramp up time for new team members.
- Develop SOPs for core workflows to ensure continuity during team absences and role transitions.
- Troubleshoot access/account issues for end users, improving first contact resolution and user experience.

Additional Contributions

- Help automate the Daily CTI report using Splunk, significantly reducing manual analyst effort and report generation time.
- Support operational response tasks including IP/domain blocks, trace and purge of malicious emails, and USB exception requests.

Greater New Orleans Region
juashua.com@proton.me
LinkedIn | Blog | GitHub

Security Tools & Platforms

FireEye | CrowdStrike | Splunk | Swimlane/Turbine/Tines | FlareVM Suite | Azure | O365 | AWS | Gurucul | Exabeam | Active Directory (UC, AC) | VMRay | Tenable

Projects

juashua.com

Transformed this resume in to a website built with AWS

Designed and deployed a secure AWS resume website using S3, CloudFront, Route 53, and ACM, with hardened access controls, logging, and least-privilege IAM. Added a serverless visitor counter backed by DynamoDB, Lambda, and API Gateway, and automated provisioning and delivery with Terraform and GitHub CI/CD.

Certifications

GRTP (GIAC Red Team Professional)
GCIH (GIAC Certified Incident Handler)
eCTHPv2 (Certified Threat Hunting Professional)
CompTIA CySA+
CompTIA PenTest+

Awards

Solutions by Design – SOC Team of the Year Winner 2023
Evolver Federal 2025 Cybersecurity Team of the Year
Evolver Federal SOC 2025 Team of the Year

- Process and review quarterly phishing exercise results in Splunk and maintain dashboards used for awareness and training.

SOC CSIRT Analyst
USCIS SOC / *CSS Evolver Federal, Stennis Space Center, MS | June 2022* – March 2025

- Monitor network activity, evaluate/escalate security alerts, and coordinate response, containment, eradication, and recovery.
- Perform network and host-based analysis using SIEM tools.
- Review and triage DLP alerts, coordinate user training to prevent further incidents.
- Analyze malware and suspicious files using EDR tools and Out-of-Band devices.
- Handle spam/phishing reports and raise enterprise-wide awareness.
- Consume and act upon daily Cyber Threat Intelligence (CTI) reports.
- Conduct incident response based on standard operating procedures.
- Investigate network violations and coordinate user remediation and training.
- Lead log analysis for both host and network systems.
- Train new team members on tool usage and IR procedures.
- Collaborate with multiple teams to process and remediate classified spills.

Education

SANS Technology Institute
Purple Team Operations Graduate Certificate
In progress - expected completion April 2027

Louisiana State University, Baton Rouge, LA
Bachelor of Arts, Political Science
Aug 2010 – Aug 2014