alijohn ghassemlouei
INFORMATION SECURITY LEADER

202.600.0651
Washington, DC
alijohn@secureagc.com
portfolio.secureagc.com

SUMMARY

Responsible, honest, passionate, and hard working security leader with strong interests in technology and business; qualified and actively seeking employment.

PROFESSIONAL EXPERIENCE

2023 – Present **Senior Director - Sovereign Cloud Technology and Engineering - SAP, Reston, VA**

Responsible for internally developed product, Shared Management Services (SMS), and 13 individuals. Lead team of 7 to support regional security capabilities for engineering, remediation, and compliance. Advise on technical and programmatic security topics for new products, features, and capabilities. Facilitate requests and issues from regional security organizations to 12 product development teams. Manage vendor and product security backlogs.

Supported transfer of responsibility and ownership of four teams to other managers as part of a transfer, from subsidiary to parent with a 95% retention rate. Coordinated the deployment of internal monolithic solution with 22 services into two regions concurrently within four months. Improved understanding of complex technical topics through creation of enablement materials e.g., documents, presentations, and videos. Established security organization with 13 unique services within the Technology and Engineering organization, consolidating global functions, for a new line of business within six months. Reduced operational burden for infrastructure and application management for log ingestion, log correlation, vulnerability management, and web application scanning globally across four countries. Developed dynamically updating security roadmap to support new line of business responsible for 12 SAP solutions.

2017 – 2023 **Director - Research and Development - SAP National Security Services, Herndon, VA**

Lead team of 35+ individuals, organized into five teams, managing two internally redesigned products, SAP Integrated Business Planning (IBP) and S/4HANA Private Cloud Edition (PCE) and one internally developed product Shared Management Services (SMS). Planned and forecasted capabilities for product roadmap with internal stakeholders.

Recovered multi-year business critical project within three months and expanded capabilities within additional two. Organized and managed product development, hardening, automation, and provisioning to deploy into three public cloud providers within five months. Assisted in deployment, hardening, and assessment of two SAAS and one PAAS offerings which achieved FedRAMP Moderate accreditation. Grew team from 5 to 25 individuals through weekly coaching and mentorship. Established recruitment process, processed over 380 candidates, and transitioned process to recruitment team of five. Established and maintained strategic relationships with GitLab, Red Hat, AWS, SUSE, and Microsoft to drive collaboration and improve over 89 product gaps and features. Organized and maintained hardware purchases for 50 individuals across engineering teams. Established and transitioned image creation pipeline which grew to encompass AWS Commercial, AWS GovCloud, Azure Commercial, Azure Government, and GCP Assured Workloads. Saved over 4.8 million (USD) through pursuit of open source solutions, infrastructure automation, elimination of redundant capabilities, and ephemeral development infrastructure.

2015 – 2017 **Senior Information Security Consultant - Bishop Fox, New York, NY**

Communicated complex technical concepts to stakeholders of various backgrounds. Analyzed client issues and created practical solutions. Lead risk assessments, gap analyses, and vendor security assessments. Worked on long-term strategic projects with Fortune 50 companies. Analyzed requested evidence and interviewed stakeholders to identify gaps. Leveraged CIS 20, NIST 800-171, NIST 800-53, and PCI DSS 3.0, and HIPPA Security Rule frameworks. Drafted executive roadmaps, reports, and outbrief presentations. Optimized and formalized existing internal processes.

Lead a two-person, six month, vulnerability management engagement for a 6.2 million customer ISP. Conducted HIPPA Security Rule audit for leading health insurance agency. Managed three month vendor security assessment for a multinational technology company. Lead a team of five on a access control assessment using client's agile process and provided complete transparency on project progress. Oversaw a team of five on a complex multi-business unit assessment for a single client. Interfaced with potential clients to communicate security assessment processes during pre-sales meetings. Automated manual data analysis and manipulation process from five days to less than five minutes. Reviewed business contracts to identify potential legal risk due to known technical gaps. Created sales presentations, scoping templates, detailed delivery guides, dynamic reports, outbriefs, and templates for Vulnerability Management and CIS 20 engagements. Brought potential client to consultancy due to outstanding work on another engagement.

2013 – 2015 **Senior Penetration Tester - World Wide Studios - Sony PlayStation, San Diego, CA**

Assessed all first party published titles with online functionality across America, Europe, and Japan. Conducts security assessments on titles, internal and mobile applications, and backend infrastructure. Coordinated all assessment related activities including meetings, dates, data collection, escalation and outbriefs. Maintained good working relationships with studio producers, developers, and respective system administrators. Kept up to date with latest PlayStation hacking tools and methodologies. Conducted vulnerability assessments, penetration tests, and architecture reviews. Managed vulnerability discovery for 9,000+ hosts. Coordinated vulnerability mitigation, remediation, and acceptance efforts through tickets within JIRA and WebRT trackers along with formal documents.

Created internal web presence through Sharepoint site, JIRA tracker, Confluence wiki, and DevTrack project. Centralized and pruned all existing information into filers, website, wiki, and project. Identified and maintained target list for internal and external assets. Deployed Tenable Security Center with assistance from Systems and Network engineering teams. Designed department brand and identity and created tailored instructional Security Center videos in conjunction with internal L&D team. Established thorough and well documented assessment methodology. Communicated processes through formal documents, presentations, websites, and wiki's. Identified systemic issues, formalized remediation actions, and raised issues to management regularly.

2013 – 2013 **Senior Penetration Tester - SRA International, Rosslyn, VA**

Lead team of 2-5 to perform penetration, vulnerability, and red team assessments, attacking a diverse range of international classified and unclassified hosts and operating systems. Emulation of current adversarial threats through commonly available tools and methodologies. Identification of vulnerabilities, weak security controls, and potential mitigations for the federal client. Evaluated configuration of target Linux, Unix, and Windows systems. Contributed in technical post-review report generation for federal, contractor staff, and management by contributing raw technical data summaries of specific items and providing in-depth analysis of all information gathered. Provided direction for future assessments.

Organized, restructured, and implemented more efficient team processes and methodologies. Defined terms within team and refocused efforts for better results. Created scoping metrics for site assessment selection.

2010 – 2013 **Cyber Security Specialist - Unwin Company, Germantown, MD**

Administered networks and Linux/Unix systems of penetration testing lab. Performed penetration testing in teams of 3-6, attacked a diverse range of classified and unclassified hosts and operating systems using such tools as Nessus, SAINT, Netsparker, Metasploit, and Nmap. Evaluated configuration of target Linux, Unix, and Windows systems. Assisted in technical post-review report generation for federal and contractor staff and management by contributing raw technical data summaries of specific items and providing in-depth analysis of all information gathered. Created and managed virtual attack platforms as a part of laptop image management. Directed software and hardware purchases for penetration testing team ($250,000+).

Presented technical demonstrations and briefings to U.S. congressmen, top-level DOE officials, and DOE security conference attendees. Completely reimplemented an existing BSD firewall and bridge with a streamlined ruleset syntax designed for maximal efficiency. Excised unnecessary equipment, consolidated hardware, and rewired the network and power for the entire internal lab. Redesigned RSA SecurID appliances system to bolster security. Consolidated hardware via hardware clustering and virtualized 90% of the lab by implementing VMWare ESXi.

EDUCATION

2007 – 2009 **University of Advancing Technology - Tempe, AZ**
Bachelor of Science in Software Engineering, Network Security
Undergraduate Thesis - Proactive Malware Prevention Software

RELATED PROFESSIONAL DEVELOPMENT

Co Authored “The Hacker’s Guide to OS X - Exploiting OS X from the Root up” Syngress		2012
Certified Information Systems Security Professional [CISSP]		2012
NSA Certified Junior Blue Team Analyst		2011
Certified Ethical Hacker [CEH]		2010
DEF CON 25	Vendor Department Lead	2017 - 2018
DEF CON 22	Speaker	2014
Black Hat USA	Senior Technical Associate Lead	2008 - Present
DEF CON 16 & 17	Mystery Box Challenge Winner	2008 - 2009