

## Jonathan Glass

jonathan.glass@gmail.com 404.290.0261

A Cloud Security professional focused on security, compliance, automation, and DevSecOps seeking opportunities to help businesses improve outcomes, IT efficiency and Information Security by understanding business needs, technical solutions, and security and compliance requirements.

### EDUCATION

MSIS (Security), Kennesaw State University

### CERTIFICATIONS

CISSP #459838

AWS Certified Security - Specialty

Google GCP - Professional Cloud Architect

AWS Solutions Architect - Professional

ITIL v3 Foundations

AWS Solutions Architect - Associate

### EXPERIENCE

Candid Partners

Atlanta, Georgia

*Cloud Security Consultant, Architecture, Automation, & Compliance*

*April 2018 – Present*

Client: SunTrust Bank

- Contract Cloud Security Architect from April 2018 - January 2019
- Prepared the Cloud Security Strategy in partnership with the GVP, Head of Cloud Security
- Collaborated cross-functionally to ensure consistency in understanding of cloud solutions, security, and compliance requirements across appdev, infra, and security teams
- Worked with Cloud Business Office (CBO) on corporate policy review for cloud readiness
- Introduced NIST 800-53 standards to all cloud initiatives
- Assessed cloud solutions against NIST 800-53 and corporate security policies
- Reviewed solutions for security concerns, offering suggestions for improvement
- Automated AWS WAF using Terraform, using both open source and custom code

Client: REPAY

- Contract Cloud Security architect from February 2019 - March 2019
- Automated AWS WAF using Terraform, using both open source and custom code
- Reviewed Solutions for Security concerns, offering suggestions for improvement

VerSprite

Atlanta, Georgia

*Managing Consultant, Cloud Security & Security Operations*

*May 2017 – April 2018*

- Created a continuous cloud security monitoring service, using client feedback to drive features, based on AWS LAMBDA, Postgresql and AWS API calls
- Performed security assessments and architecture reviews for clients
- Improved the efficiency of Cloud Security Assessments from 6 weeks to 1 hour

- Managed a team responsible for Security Operations, Threat and Vulnerability Management, Application Development, and Security Training

Turner Broadcasting, Global Technology Office, Information Security

Atlanta, Georgia

*Cloud Security Architect*

*March 2016 – May 2017*

- Perform security assessments and architecture reviews for all Cloud Projects and Initiatives, including moving the Turner Data Cloud (data lake) to AWS, porting Cartoon Network to a Cloud based streaming service called BOOM
- Design the solution and rollout plan for the SkyHigh Cloud Access Security Broker (CASB) solution for recognizing and controlling Shadow IT across the enterprise
- Manage the rollout of Alert Logic across all Turner AWS accounts, working through business unit IT teams to achieve success
- Write a Cloud Auditor application to collect inventory data on all of Turner's AWS accounts, including users, permissions, policies, etc, from a variety of data sources, including CloudHealthTech, AlertLogic, and AWS APIs. This provided a single pane of glass for incident response teams to identify systems.
- Created, promulgated, and received executive approval for Turner-wide Cloud Security Policies
- In my first 90 days, I closed the majority of their outstanding audit findings; the largest number of audit findings ever closed in a quarter at Turner

Dell SecureWorks

Atlanta, Georgia

*Cloud Security Technical Product Manager*

*May 2015 – March 2016*

- Communicate with external clients to understand their current needs and upcoming plans for anything Cloud Security related.
- Create and maintain an 18-month forward looking roadmap for Cloud Security Services
- Present and discuss Cloud Security Roadmap with clients and prospects during Executive Briefings and in support of sales calls.
- Create, prioritize, and promote Engineering work efforts (Jiras, Enhancements) that define the features the Cloud Security Service products need to have to be successful
- Create and coordinate beta programs related to Cloud service launches.

*IT Solutions Architect, Cloud Architecture*

*October 2011 – May 2015*

- Introduced Cloud solutions to the IT team for a variety of issues, to the point that the VP of IT promoted me to Cloud Architect.
- Worked with Information Security Researchers, CISO, Internal Audit, and Product Management to bring an AWS-hosted endpoint monitoring security service called Red Cloak to market.
- Worked with Product Management on the Cloud Security project, defining services Dell SecureWorks could bring to market

- Proposed, built and lead an 8 person DevOps “Cloud Operations” team to support workloads on AWS, starting with Red Cloak
- Introduced the concepts of Pets vs Cattle, DevOps, Automation, CI/CD to IT teams, including distributing the book “The Pheonix Project” to IT Leadership, who then made it mandatory reading for their teams

*Engineering Lab Manager / Architect*

*August 2007 – October 2011*

- Progressively grew the position from a single systems administrator running a small development lab, to a manager leading a team of three systems administrators supporting 3000 machines across three states, responsible for budgeting, project management and IT Architecture for Engineering.
- Developed a budget and project process for Engineering IT to track all CapEx and projects, and managed the CapEx budget to within 1% every year

Georgia Institute of Technology

Atlanta, Georgia

*Information Security Engineer III, OIT Information Security*

*November 2004 – August 2007*

- Responsible for incident response, vulnerability assessment, forensics and assisting law enforcement with investigations into crimes involving campus computers.
- Developed a Sensitive Server database and web app that tracked vulnerabilities on servers containing sensitive data, or that the schools marked as critical. The CIO read the vulnerability report every Tuesday morning, and would escalate within business units whenever needed.
- Designed and built a forensics lab capable of handling dozens of drives and terabytes of data and multiple investigations. Procured write blockers, servers, safes and storage to handle incidents. Wrote scripts and tools to automate forensics processes, including one that analyzed all the files on a suspect system against known good sources, like Solaris’s list of known good hashes, and known bad, like NIST’s known hashes.
- Redesigned and deployed the Information Security department’s IT infrastructure using industry standard racks, power, networking, etc, and heavy automation using CFEngine and Kickstart, including providing high availability for all services using tools like LinuxHA. The infrastructure maintained 100% uptime for a year after both systems engineers left. This automation also freed up time for handling more investigations.
- Deployed a Netflow collection service that collected all Netflow off campus core routers, and made anonymized copies of the data available to the Research Network Operations Center for use by faculty and students.
- Developed a LAMP firewall management application that is still in use today. This application provided business units with the ability to manage their local firewall rules, while allowing the OIT Network Team to manage the centralized firewall rules. It ran vulnerability scans against hosts, created and managed the workflow within Remedy.

*System Support Specialist II, Inst. for Bioengineering & Bioscience*

*June 2002 – November 2004*

- Improved IBB's security standing so much that the CISO invited me to transfer to campus-wide OIT Information Security to help secure the campus.