Brooks Imperial
Cloud Engineer, Cybersecurity Analyst, Developer
contact@brooksimperial.com (720) 519-3359

EXPERIENCE SUMMARY

Brooks Imperial is a versatile results-driven technology professional who really enjoys getting the machines to work. His areas of emphasis are Google Cloud Platform (GCP) and Amazon Web Services (AWS) cloud management, cybersecurity, business assessment/consulting, and software development. He has hands-on experience in large publicly held and small private firms – Oil and Gas, Stock Transfer systems, Transportation (Steamship and Trucking), Medical Device sourcing – as well as Independent Business ownership. He enjoys working in dynamic teams, learning from and mentoring with others. Brooks is flexible, and is comfortable working in-office and remotely. He can travel as required in U.S. or overseas, and is eligible for security clearance.

_____

Cloud/CyberSec Certifications

GCP – Associate Cloud Engineer
CISSP – Associate of (ISC)^2
CCSK – Cloud Security Knowledge
GPEN - GIAC Penetration Tester

Education

BA – Economics, Philosophy, Business Administration
Hillsdale College

Ruby on Rails Development

Intensive Ruby on Rails development bootcamp taught by industry veterans.
Areas of focus: Agile, GIT, RSPEC, TDD, Guard, Heroku, MVC
DaVinci Coders

Legal Studies

California First Year Law School Exam – FYLSE (Passed on 1st take)
Concord University

Certificate in International Trade

World Trade Center - Denver

Business Skills Endorsements

Change Management
Process Improvement
Contract Management
Budgets & Accounting
Business & Strategic Analysis
Business Intelligence

Location

Denver Metro Area

CONSULTING BUSINESS

ImTekSec (Principal Consultant/Owner)   Oct 2018 - present

Contract penetration testing, vulnerability scanning, and remediation services on Windows & Linux platforms. Kali Tools applied for recon, vulnerability scans, fuzzing, payload delivery, exploit pivots, machine compromise and data ex-filtration. Penetration testing utilized scanning tools (Nessus and Burp). Endpoints investigated locally and remotely through secure connections. Developed a remote cloud-based penetration testing platform in AWS using Docker Containers and Kubernetes.

ACTIVE CLOUD AND CYBERSECURITY CERTIFICATIONS

GCC-ACE (Google Cloud Certified Associate Cloud Engineer)   ID #vfCFCq   April 2020

"An Associate Cloud Engineer deploys applications, monitors operations, and manages enterprise solutions." The Google Cloud Console and the command-line interface are used to perform platform-based tasks to maintain one or more deployed solutions that leverage Google-managed or self-managed services on Google Cloud. GCP services covered include:

- setting up a cloud solution environment (project setup, incl. IAM, Stackdriver, billing, and SDK)
- planning and configuring a cloud solution (pricing, machine and network resources, data storage)
- deploying and implementing a cloud solution (Compute, Kubernetes, App Engine, data, network)
- managing successful operation of cloud solution (resources, storage, database, network, logging)
- configuring access and security (IAM, service accounts, audit logs)

CISSP Certified - Associate of (ISC)^2 ID #648411   Dec 2017

The vendor-neutral CISSP credential confirms technical knowledge & experience to design, engineer, implement, & manage the overall security posture of an organization.

CCSK (Certificate of Cloud Security Knowledge V4) Code: EWP8kyypnEwWmki15KTCBsY   April 2019

Certification exam encompasses the key concepts of Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing V4, the CSA Cloud Controls Matrix, & European Network & Information Security Agency (ENISA) Cloud Computing: Benefits, Risks & Recommendations for Information Security.

GIAC Penetration Tester (GPEN) Certified   Analyst #12781   May 2018

Certification requires demonstration of ability to execute penetration testing methodologies & properly conduct a penetration test, as well as best practice techniques specific to conduct a penetration test. "Professionals holding the GPEN are qualified for job duties involving assessing target networks & systems to find security vulnerabilities."

CLOUD AND CYBERSECURITY EDUCATION

Online Learning

- Live remote preparation for Association Cloud Engineer GCP Certification
- DevOps tools for CI/CD pipeline AWS dev (Git, Jenkins, Ansible, Maven, Rancher, Docker, Kubernetes)

SecureSet Academy CORE Technical Program   Graduated: 22 Dec 2017

- *UX & MS config & admin, Python & Bash scripting
- Virtual Machines – Local (VirtualBox, Citrix, VMWare) and Cloud (GCP, AWS, Azure)
- Docker container life cycle
- Virtual router config with VLANS to host web apps
- Model web apps using HTML, CSS, PHP & GitHub repositories to explore security exploits & payloads
- Pen testing intros w/ Nmap, Arpspoof, Metasploit, Burp, Zap, Sqlmap, Beef, Armitage, Recon-ng, Peach3, Nessus, Kali Linux
- Configured SSL certs, SSH connections, SCP code movement
- Regulatory & compliance standards - GRC, PCI, HIPAA, GDPR - legal context
- LogRhythm SIEM mgmt console w/Linux syslog, auditctl & Windows Sysmon, Splunk, Phantom in VMWare
- Blockchain experimentations: Bitcoin node, Ethereum & Hyperledger
- Spun up app/OS/network, local and cloud, scenarios as required for testing & analysis

PAST WORK EXPERIENCE

Medical Product Sourcing – developed China & Southeast Asia disposables sourcing partners
Independent Business Owner – Pioneer Home Medical Supply (built business from scratch)
Programmer/Developer in Database Applications (Model 204, Pick/Unibasic/Visual Basic)
Employers/Clients: Paradigm Technologies, Gemisys Corp., LCS Corp., American President Lines, Roadway Express