Scott McDonald scott@dnshat.com 386-588-7745

Bio:

- Started career in the late 90s building and securing one of the world's first ISPs.
- Early roles at SecureWorks helped to secure bank networks followed by a successful startup (which led to an AWS case study and employment as one of the first ProServe consultants for Amazon).
- Left AWS to learn security on Google Cloud working for several years as a badged Google PSO consultant on major Google security engagements (with large Financial Services clients and the largest security vendor using the Google Cloud platform).
- Leader of deeply technical security delivery teams at 4 of Google Cloud's key partners.

February 2022 - Present – Senior Manager Security Consulting – Accenture, Remote

- Delivery focused role in a new GCP Security Practice with Google's largest Partner..
- Rescued struggling client engagement to deploy a Secure Cloud Foundation in GCP. Took over as team lead and guided resources to a successful implementation within the remaining timeline.
- Automated the deployment process for the Terraform code base supplied by Google to create a Secure Cloud Foundation. Reduced terraform code base deployment time from 6 months to 1 month, and reduced required resources from 10 to 2.
- High Availability and Disaster Recover SME consultant for major healthcare deploying an AI data lake for security sensitive patient data. Help plan and implement DR strategies for the major of GCP services and AI related 3rd party components including Databricks on GCP.
- Won Google's Vulnerability Reward Program in 2022 – received a monetary award from Google for finding a Vulnerability in Cloud Source.
- Google Cloud Certified Professional Cloud Architect - May 11 2023.

July 2021 - February 2022 – Head of Security – 66degrees|Cloudbakers|Qwinix, Remote

- Initiated and grew a security consulting practice focused on Google Cloud infrastructure.
- Helped to grow and lead a deeply technical security delivery team subcontracting for Google PSO.
- In addition to building the delivery practice, served as the Head of Security, responsible for all security within the company, as well as the security solutions delivered to Google Cloud clients.

August 2020 - July 2021 – Manager, Cloud Security – SADA, Remote

- Manager of Cloud Security for SADA, built a security practice focused on Google Cloud.
- Built SADA's initial Google Cloud Security Practice. Defined go to market strategy, sales training, packaged security offerings, then hired and trained security delivery team (all on the side, while being a full time billable consultant on security streams in critical engagements).
- Helped develop the sales pipeline for the security practice, and ensured my team was able to deliver high quality security outcomes in a repeatable way.
- Discovered a way to insert workable GCP Projects into other GCP Orgs. This Vulnerability could be used to insert malicious Projects into other GCP accounts. The Attacker's Projects show up in the Victim's GCP Org browsing and searching without indications the projects are hosted in another GCP account. Google VRP - Accepted Vulnerability: **https://bughunter.withgoogle.com/profile/2c30f0ff-a73c-49c9-b038-338ab3910c93**
- My security session presentation at Google Cloud Financial Services Summit 2021: **https://www.youtube.com/watch?v=HZuReRlvsDY**

June 2019 - August 2020 – Senior Security Consultant Google PSO – Scalable Security, Remote

- Shifted focus from Devops at AWS cloud to security at Google cloud (GCP). Badged as TVC for Google PSO for over a year now. Earned 3 GCP certifications in a month while working.
- One early AWS related client engagement to generate attack signatures for AWS log activity that could be alerted on in Splunk SIEM and responded to with Phantom automations.
    - Used Pacu too to simulate AWS attacker activity and generate fingerprinting patterns.
    - Wrote a public blog article on the Pacu pentesting utility and how attackers could use it in a scenario similar to a recent major financial breach that was in the news.
- Successful 9 month engagement for a very large financial industry client post data center breach to lay secure foundations for an all-in GCP migration. Created client specific technical design documentation for GCP platform for VM Security, Container Security, Secrets Management, Threat and Asset Management, and single handed POCs for several security related projects with results as deliverables. Helped with initial FedRAMP efforts. Found 2 existing data exfiltration vectors and worked with SVP to identify resolution paths.
- Worked with one of the largest GCP clients, a cyber security vendor, doing a security audit for their full Org and coming up with a new secure design for GCP to increase their security posture of over 35k projects. Surfaced insider threat activity.

June 2014 - May 2019 – Senior Consultant – ProServe — Amazon Web Services, Seattle, WA

- After being approached by Jeff Barr of AWS for a case study on my 2nd startup company (ran it on the side, scaled to 14 countries, first cloud based DNS provider. Did a pivot into cloud based DNS Failover services [then came Route53+Health Checks after a case study]. Shut-down dnshat.com to work for AWS in a consulting role.
- Helped build from zero a DevOps consulting practice for AWS Professional Services.
- Solved the windows enterprise datacenter migration puzzle – developed migration model and cross region sql server solution that are the keys to unlocking 70% of enterprise data centers which are running legacy windows stacks. Created a presentation for reinvent and ran the demo on stage – youtube: **https://www.youtube.com/watch?v=Hd5mOBZAPVQ**
- Presented for AWS at ChefConf 2015 in Santa Clara, CA. Taught the Chef audience how to do IaaC on AWS using CloudFormation. Video available on youtube here: https://www.youtube.com/watch?v=WXLDdGxfEsI
- Spent a month in London working with a Consortium of AWS, Google, and IBM to bid on business for the largest IT deal in history (competing against a consortium of Microsoft and Accenture). Received direct feedback from the client executive team that my demo of a hybrid cloud solution between AWS and IBM was the deciding factor as it avoided single cloud vendor lockin. AWS won the largest cloud IT deal in history as a result.
- Spotted a data leak in the EC2 hypervisor that could have been used to fingerprint where AWS had rolled out critical Zen patches, which regions had not been patched yet, and which regions had to be rolled back after patching failed. This was shortly before Spectre/Meltdown - and significantly increased the security posture of the entire AWS cloud which helped prevent exploitation of client environments.

Aug, 2013 – June 2014 – Director, DevOps – Altisource Labs, Atlanta, GA

- Secured AWS environment. Implemented Continuous Patching principles and built early security tools for AWS.
- Built a DevOps team. Managed a large AWS cloud (VPC) powered by Chef. Atlassian tools

integration (Stash, Crowd, Jira, Confluence, Bamboo, Fisheye).

- Initially hired, managed and mentored a small team of DevOps engineers while staying hands-on with the technologies.
- Built out and supported a complex CI environment based on the Atlassian suite.
- Supported 550+ engineers (working in a VPC connected via openvpn) located across several geographies while maintaining CI availability and performance across the full build pipeline.

Feb, 2012 – Sept, 2013 – Managing Director of Technical Operations – AAA, Atlanta, GA

- In charge of all Security, Operations, Hosting, and Support for a start-up company TST funded by AAA club owners. Originally a contract – salary conversion took place after 6 months. In less than 1 year recruited and hired a strong DevOps team of Sr. Linux Engineers. Led the effort to replace millions in recurring leased data center costs with thousands in Cloud Deployments.
- First week terminated entrenched admin that had backdoored all systems. When he was terminated, he used a stolen ssh key from Jenkins to take out the central logging server in AWS. Made an image copy of it after losing visibility into his lateral movements. Next used photo image recovery tools to recover log files on the virtual machine image that had been nuked with an "rm -rf *". The recovered ssh logs showed a source IP address that exactly matched the IP address in email headers from the terminated attacker. HR and Legal used the information the next day to threaten legal action to halt the attacks. This gave enough time to rebuild the entire production infrastructure from scratch to replace rootkits and rotate all ssh keys to restore production security of the inherited AWS environment.
- Created a transparent release process with multiple hot sites hosted by multiple vendors in different geographic regions – full HA redundancy with complete on demand traffic failover capabilities. Setup MySQL replication farm at the heart of the hybrid cloud deployment. Deployed enterprise wide Zabbix monitoring solution.

July, 2010-Feb, 2012 – Director of Cloud Engineering – What's Up Interactive, Atlanta, GA

- Primarily focused on architecting, hosting, scaling and supporting the largest visitor traffic site in Georgia: galottery.com
- MySQL DBA managed 4 master MySQL servers in circular replication across multiple hosting providers where both web farms could be hot for live traffic at the same time.
- Built a hybrid cloud to cut expenses and be able to handle very large post jackpot traffic spikes. Private cloud was based on a VMWare ESXi and 100Mb Cogent fiber connection in a traditional office space telco closet. Public cloud was Amazon EC2 with automated backups into S3.

July, 2008-July, 2010 – Sr. Cloud Engineer – Premiere Global Services, Atlanta, GA

- Managed Hot/Hot failover sites with approx 200 Linux servers per site.
- Maintained all security including design, IR, and operating system patches.
- Designed, set up, and administered a very complex, hot-hot, fully replicated MySQL environment across cloud platforms. Full failover capability for zero downtime releases.
- Responded to production outages and incidents.
- Planned and executed scheduled system maintenance.

- Debugged, analyzed, and resolved production issues with tomcat and jboss applications.
- Developed / deployed scripts to automate monitoring and management.

June, 2006 - July, 2008 – Unix Administrator, TechOps – Secureworks.com, Atlanta, GA

- Employee of the month: August 2007 & September 2007
- Employee of the month twice, two months in a row, for saving the day for clients.
- Deep security industry experience helping to build one of the first security focused vendors.
- HOK helped secure thousands of bank networks under extreme threat conditions.
- Plan and execute scheduled system maintenance.
- Automate regular system management activities via scripts and scheduled tasks.
- Demonstrated competence in administering and developing the following:Debian, RedHat (RHEL 4 and RHEL 5), SUSE (v9 and v10), FreeBSD,OpenBSD, Apache, MySQL, PHP, SSH, sendmail, qmail, pop/imap, DNS, NIS, LDAP

April, 2005 – May 2006 – Network and Systems Team - Unique Solutions, Anderson, SC

- Shared roles included: ORACLE DBA, VMware ESX, Windows Domain admin, Exchange server admin, Active Directory, Inkra router management, 3PAR SAN storage administration, and Unix Systems Administration.
- Worked daily with Linux, RedHat, Debian, Mandrake 10.1, Windows 2k, 2k3, and Oracle 9i
- Developed an online system for scheduling vendor employees for retailer maintenance in PHP/MySQL.
- Developed Microsoft Access based forms for Customer Service employees to modify information in Oracle, SQLServer, Advantage, and MySQL databases - coding in Visual Basic.
- Developed SOPs and emergency contact procedures.

March, 1997 – December, 2004 – Systems Administrator – MyLink, Inc., Macon, GA

- Handled all security for an Internet Service Provider with thousands of customers and hosting sites for over 7 years. Deep experience with forensics, attack vectors, buffer overflows, packet inspection, intrusion detection, intrusion response, red teaming, and blue teaming before those were phrases. Handled over a dozen high profile post-breach incidents working with federal authorities. Helped build and secure one of the world's first home internet providers.
- Unix Administration of multiple servers. Distributions changed over the years from Solaris, to Linux (RedHat, Debian), to an OpenBSD environment totaling 7 Years of daily Unix Systems Administration across the enterprise.
- Setup, Administer, and Scale: RADIUS, FTP, HTTP (Apache), SMTP (Sendmail, Postfix,Qmail), POP3, DNS (Bind 4.x,8.x,9.x), LDAP.