

Brad Geesaman

✉ bradgeesaman@gmail.com 🌐 bgeesaman 👤 in/bradgeesaman 🐦 @bradgeesaman 📍 Fairfax, VA

Summary

Motivated cloud-native Information Security Professional with expertise in a wide range of cloud platform and Kubernetes security technologies and a track record of producing extraordinary results. Looking for opportunities to make the secure path the easier path for your clients and the community.

Experience

- | | |
|---|--------------|
| Director of Cloud Security , Aqua Security | 2021-present |
| <ul style="list-style-type: none">• Technical lead working to design, prototype, and build new and improved product and SaaS service capabilities within the cloud and container security space across AWS, Azure, and Google Cloud. | |
| Co-founder, Chief Architect , Darkbit.io | 2019-2021 |
| <ul style="list-style-type: none">• Provided expert technical and strategic guidance to cloud-native organizations by assessing the security posture of their AWS, Google Cloud, and Kubernetes environments via point-in-time and continuous security configuration assessments.• Co-developed and open-sourced <u>OpenCSPM</u>, a graph-database engine for efficiently assessing the security posture of AWS, Google Cloud, and Kubernetes resources.• Developed and tested exam challenges for the Certified Kubernetes Security (CKS) certification. | |
| Professional Services Consultant (Contractor/TVC) , Google Cloud | 2018-2019 |
| <ul style="list-style-type: none">• Engaged with multiple clients migrating to Google Cloud and Google Kubernetes Engine (GKE). Performed security configuration reviews with strategic security guidance to client management.• Delivered multiple internal GKE Security educational assets and training sessions used by the greater partner ecosystem.• One of the first 20 to qualify for the Google Cloud Certified Fellow Program. | |
| Independent Security Consultant , Bradley Geesaman Consulting | 2018-2019 |
| <ul style="list-style-type: none">• Delivered practical security guidance, expertise, implementation assistance, and security training to several clients deploying mission-critical workloads inside Kubernetes on Baremetal, AWS, and GKE.• Designed, developed, and automated the cluster and deployment pipelines of a multi-team AWS/Kubernetes-based platform performing security analytics at 60K logs/sec into ElasticSearch. | |
| Senior Manager , Symantec Corporation | 2015-2017 |
| <ul style="list-style-type: none">• Led the team that successfully hosted a one-week, 1500 person, company-wide Capture-the-Flag event inside 10 AWS regions on top of multiple, hardened Kubernetes clusters.• Architected and built a fully automated Kubernetes cluster deployment tool on AWS to support the containerized targets on the Symantec Cyberskills platform.• Built and managed the federated logging and performance system used to monitor cluster and container health using EFK and Prometheus/Grafana. | |
| CTO , Blackfin Security Group - Acquired by Symantec Corporation | 2014-2015 |
| <ul style="list-style-type: none">• Led the technical operations team focused on delivering cutting-edge, realistic, and immersive training solutions to improve security awareness for large organizations and "hands-on" experience to expert security personnel charged with defending their data.• Managed the Customer Support, Operations, and Internal IT teams.• Administered The Hacker Academy, an ethical hacking subscription learning platform on top of AWS via Infrastructure as Code and Configuration Management. | |
| Chief Architect , MAD Security | 2012-2014 |
| <ul style="list-style-type: none">• Led and managed the team that designed, built, and delivered capture-the-flag (CTF) style ethical hacking/cyber wargames challenges designed for security professionals. The challenges have been played by over 9000 professionals world-wide in over 200 events lasting 2 hours to 30 days (24/7).• Delivered several one-day bootcamp instructional training sessions covering security penetration-testing basic concepts complete with custom CTF scenarios for hands-on skills reinforcement. | |
| Security/Sales Engineer , Check Point Software Technologies | 2008-2012 |
| <ul style="list-style-type: none">• Responsible for technical pre-sales support for the design, migration/implementation, and operation of security gateway solutions for Federal Civilian Agencies. | |

- “2009 North American Security Engineer of the Year” Award for outstanding team performance and customer satisfaction.

Manager, Assessment Services, Securicon

2006–2008

- Managed numerous security assessments from kick-off to final delivery. Assessments included electronic and physical penetration testing, vulnerability assessments, and solutions review.
- Formalized and streamlined the client engagement assessment data collection process to reduce final deliverable draft and completion time by up to 50%.

Principal Security Engineer, Symantec Corporation

2004–2006

- Provided Tier3 support to worldwide SOC Engineering teams in support of Fortune 500 customers.
- Designed, developed, and implemented the improved fault and performance monitoring system internally recognized for reducing 5% of all daily engineering workload.

Security Engineer/Senior Security Engineer, Symantec Corporation

2003–2004

- Responsible for supporting Symantec’s Managed Security Services (MSS) customer base from a 24x7x365 Security Operations Center as a senior member of the Security Engineering Team.
- Provided outstanding engineering maintenance, configuration, and support of all leading firewalls and IDS systems.

Systems Engineer, PEC Solutions

2002–2003

- Responsible for the secure transmission of electronic fingerprints and personnel photos to support Federal hiring processes at remote sites across the US.
- Received multiple internal performance-based awards.

Speaking

Keynote Panel: Hacking and Hardening in the Cloud Native Garden

KubeCon NA 2020

Kubernetes Attacks: What Your Cluster Is Trying To Tell You

CSA Boston Oct 2020

Advanced Persistence Threats: The Future of Kubernetes Attacks

RSA 2020/KubeCon EU 2020

Attacking and Defending Kubernetes Clusters: A Guided Tour

KubeCon NA 2019

Detecting Malicious Cloud Account Behavior

BlackHat USA 2018

Hacking and Hardening Kubernetes Clusters By Example

KubeCon NA 2017

Blog Posts

Google Cloud IAM Custom Role and Permissions Debugging Tricks

2021

Why You Should Enable GKE Shielded Nodes Today

2020

Vuln Research

CVE-2020-15157 “ContainerDrip” Write-up and Google 2020 VRP Prize Winner

2020

Falco Default Rule Bypass

Container Registry Search Order/Registry Name Squatting

CVE-2019-11253 Kubernetes DoS Writeup

2019

Certifications

Google Cloud Certified Fellow

2020–present

Certified Kubernetes Security Specialist Exam Developer

2020

Google Cloud Certified Professional Cloud Architect

2019–present

Certified Information System Security Professional (CISSP), ISC2

2007–2016

RedHat Enterprise Linux Certified Engineer (RHCE), RHEL 3.0

2004–2006

Education

BBA, Computer Information Systems, James Madison University, VA, USA.

1998–2002

Interests

Hockey, Formula 1™, Cloud/Kubernetes Vulnerability Hunting, Mexican food, and collecting e-books