Sahil Dharamsi

sdharamsi1@gmail.com - 571-330-7304 - Bristow, Virginia

Profile

Security Engineer who is a highly motivated, versatile, and dynamic team player - able to adapt quickly and excel in fast paced environments to complete tasks independently and in collaboration with proven track records of leading large scale business problems from design to production. Experienced in Cloud Security, Vulnerability Management, DevSecOps, Application Development, Platform Engineering + Automation.

Education

- **Georgia Institute of Technology** — Atlanta, Georgia
  Master of Science - Cybersecurity — *January 2025 - December 2026*
- **George Mason University** — Fairfax, Virginia
  Bachelor of Science - Cybersecurity Engineering - GPA: 3.8 — *August 2019 - May 2023*

Skills

- **Programming**: Python, Terraform, Ansible, Bash, Appian SAIL, SQL
- **Technologies**: Appian, Crowdstrike CSPM, Prowler, AppOmni, Git, Gitlab, Jira, Okta, Vault, Tenable, Splunk SOAR, Nessus, Bitsight, Security Scorecard, Semperis Purple Knight, Qualys, Keylight, Symantec, Chef
- **Platforms**: Linux, Windows, Amazon Web Services, Google Cloud Platform
- **Certifications**: ISC2 Certified in Cybersecurity, AWS Certified Cloud Practitioner, Appian Certified Associate Developer

Experience

- **Appian Corporation** — McLean, Virginia
  Information Security Engineer — *August 2023 - Present*
  - **Cloud Security Posture Management**: Deployed Crowdstrike & Prowler to identify security misconfigurations in order to harden our corporate and customer cloud environments against CIS 3.0 AWS Foundations Benchmark.
  - **AMI Building, Scanning, & Distribution**: Enhanced a comprehensive CI/CD pipeline enabling engineering teams to seamlessly perform OS scanning and compliance auditing on AMI builds in order to distribute images. Built custom ansible playbooks for installing security tools on golden images used in our commercial + fedramp environments.
  - **Application Development**: Utilized Appian's low code platform to design and develop multifaceted applications for dashboarding, process automation, and trend analysis for numerous stakeholders to improve visibility. Highlights included applications for centralized vulnerability/cloud security dashboarding, capturing metrics, and scan coverage analysis.
  - **Vulnerability Management**: Built, maintained, and hardened infrastructure-as-code, third party tools, and custom internal services - all used for scanning multiple environments to ensure compliance and improve our security posture.
  - **Detection & Monitoring**: Developed in house detection and monitoring tools by building Terraform modules, CloudFormation Stacksets, Lambda Functions, API development, and deploying secure infrastructure. Highlights include asset inventory, AMI metrics, and custom alerting for critical workflows.
  - **Highlights**: Played a key role in helping Appian pass FedRAMP and AWS Foundational Technical Review Audits, which led to a 2024 Impact Award, recognized by the Chief Information Office Department.
- **Amtrak** — Washington, D.C.
  Cybersecurity Intern — *September 2022 - May 2023*
  - **Engineering**: Supported security engineers on the deployment, configuration, and patching of Microsoft Defender & Symantec Endpoint Protection for mobile devices, cloud applications, and Amtrak Station devices.
  - **Defense & Assessment**: Worked with the security operations center to revise multiple incident response playbooks. Assisted the cyber assessment team during penetration tests and vulnerability scanning.
  - **Risk & Compliance**: Managed foreign travel security requests and identified awareness/training modules to create a tailored organization wide security training for all Amtrak employees for 2023.
- **Cvent** — McLean, Virginia
  Information Security Intern — *June 2022 - August 2022*
  - **Vendor Risk Assessments**: Conducted comprehensive security risk reviews on new and existing third party vendors to ensure alignment with compliance frameworks such as SOC2, PCI, and ISO 27001.
  - **Security Assessment Automation**: Leveraged Chef Inspec & Ruby to create compliance checks for AWS security to align with Trusted Advisor recommendations. Automated access reviews for non-sso apps via API development.

Projects

- **Automated Vulnerability Remediation with Security Orchestration, Automation, & Response (SOAR)**: Utilized Splunk SOAR to create automation playbooks targeting low tier vulnerability detection, remediation, and notification for small sized firms like our capstone sponsor Avint. Implemented a open source threat management capability utilizing the MITRE ATT&CK framework. Presented a business proposal to the sponsor highlighting impact, cost/time savings, and productivity increase.