

Dillon Watts

Application Security Engineer

San Antonio, TX

dmgwatts@gmail.com

Application Security Engineer (DevSecOps)

Working knowledge languages: Go, Bash, Python,

Primary Devops Skills: Terraform, Vault, Docker/Swarm, Kubernetes

Code review languages: C,C#, Ruby, Swift

Current Skills Development: Rust, Scala

Authorized to work in the US for any employer

Work Experience

Security Engineer

HEB - San Antonio, TX

October 2019 to Present

-

- Integrate Vault and consul devices with liver eyes using Istio as a proxy service mesh.
- Implement automated mobile SAST Scanning via Mobs F within gitlab secure pipelines.
- Create Secure Amazon Machine Images (CentOS7) using Vagrant alongside Ansible-OS-Hardening roles.
- Deploy and manage Vault using AWS EKS for a elastic, scalable deployment.
- Lead the deployment and integration of Hashicorp Vault to AWS cloud providers with current on-prem solution using IAC tools such as Terraform, Gitlab, Jira & Confluence.
- Deploy various services leveraging Kubernetes (Vault, Datadog, Consul)
- Act as an SRE/SME for Hashicorp Vault.
- Automate monitoring and alerting solutions with Terraform providers including "Datadog, Prometheus & Pagerduty"
- Extended Vault patterns to organization PKI requirements.
- Implement logging solutions with Cloudwatch, Prometheus & Datadog & New Relic
- Implement custom CICD pipelines using Jenkins & Gitlab CI within our version control processes
- Work alongside a squad of Developers focused on development, deployment and maintenance of security focused tools such as Hashicorp Vault, Veracode, checkmarx, Veracode and more.
- Develop / Test web api's using Golang, Insomnia & Burpsuite Pro.
- Create local "Vaults" using Hashicorp Vagrant + VMware Fusion providers for local development and testing.

DevOps Engineer

TrueAbility - San Antonio, TX

Present

- Current tasks include being responsible for creating docker images using docker-compose.

- Creating, monitoring and maintaining BASH scripts to ensure that provisioning for end-user will complete as expected.
- Testing various scripts in a test environment before pushing to production.
- Ensuring that AWS and GCP network traffic is being logged and tagged for parsing.
- Assisting build scalable, resilient AWS EC2 infrastructure by leveraging AWS auto-scaling.
- Understanding various Linux distros such as Ubuntu, CentOS, Redhat & OpenSUSE.
- Utilizing Jira, Trello and GitHub for change management and version control.

Systems Administrator

Diligent Consulting - San Antonio, TX

June 2018 to July 2019

Implemented a security monitoring system for over 200 hosts

Managed Windows 2008, 2012, 2016 and Linux based servers (total +- 50)

Use various tools including Nessus & Opencast security testing

Utilizing power-shell scripts to manage Office 365/ Active Directory sync with Azure.

Managed IAM roles within AWS Cloud environment

Manage docker based images

Created/Manage test vagrant images.

Working experience securing servers based on STIG's

Familiar with frameworks such as PCI-DSS and NIST

- Manage vulnerability program to assess various servers, services and web applications
- utilized OWASP and WAP for web application vulnerability assessments
- Implemented a BYOD (Bring Your Own Device) security policy
- Managed patches via a identical test environment
- Presented risk reports based on industry findings
- Maintain various snapshots for virtual environments including vSphere/VMware
- Managed the procurement and deployment of various endpoints.

Junior Systems Administrator (SOC Environment)

Daemon Systems - San Antonio, TX

November 2015 to August 2018

Renegotiated a new contract with SIEM provider to save 66% total cost per month (Over 45k per year savings)

Interacted with wire-shark, Nap and OpenVAS for vulnerability testing

- Acted as the POC for all customers in regards to network upgrades, contract dealing and SLA requirements. (roughly 50 customers)
- Maintained Domain Controller servers for over 50 customers.
- Maintained Fileserver environments
- Implemented remote security access systems (RAS) using cisco VPN routers
- Engaged, tested and quantified user awareness by conducting email phishing campaigns
- Utilized both auto-task and Salesforce CRM as a platform to track and quantify ticket metrics
- Desktop Analyst I (SOC Environment)
- Manage all level I and II helpdesk tickets (50-75 tickets per day)
- Managing the add and removal of users from active directory

Education

BAAS in Information Security & Assurance

Texas A&M San Antonio

April 2020

AAS in Information Security & Assurance

San Antonio College

September 2017

Skills

- PCI-DSS (2 years)
- Python (4 years)
- Bash (4 years)
- Powershell (3 years)
- Networking (5 years)
- Vulnerability Scanning (3 years)
- Git (3 years)
- Ubuntu (2 years)
- Fedora (2 years)
- Active Directory (3 years)
- Azure
- AWS
- Jenkins
- Docker
- VMWare
- TCP/IP
- bash (4 years)
- Python (3 years)
- Go (1 year)
- MySQL
- APIs
- Operating Systems
- Scripting
- Linux
- Agile
- Ansible
- CI/CD
- DevOps
- Jira

- Cloud Computing
- S3
- Istio (1 year)
- Kubernetes (1 year)
- AWS (5 years)
- Packer (2 years)
- Terraform (2 years)

Links

<https://about.gitlab.com/releases/2020/10/22/gitlab-13-5-released/>

Certifications and Licenses

Security+

Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

CySA+

Present

CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA). Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

CSAP (Certified Security Analytics Professional)

Present

Groups

Board Representative Alamo ISSA

Present

- Assisting with the recruitment of teachers for CyberPatriot for high school students
- Responsible for vendor relations of Alamo ISSA

Infragard Member

Present

- A partnership between multiple big businesses and the FBI.
- We get private national security concerns that can be translated to warn organizations before public knowledge.

Publications

Gitlab Mobile SAST using MobSF

My team at HEB developed a mobile SAST analyzer for the Gitlab secure product line. Publication is currently under legal review.