Kevin Law

https://kevinlaw.info | mail@kevinlaw.info
Github | Codewars

Site Reliability Engineer & Security Professional

- **Ten+** years working in application development with high availability and time-critical services.
- Twelve+ years experience in various facets of **information security**
- Experienced working successfully with **remote teams of all sizes** to bring projects to timely release.
- Continuously up to date with **emerging** infrastructure and development **trends**, **methodology**, and **tooling**.

Professional Experience

Dell SecureWorks | Taegis Detection Verification | **Jan 2024 - Present**
Technical Lead

- Python Framework to test Endpoint Agents completely End-to-End to determine detection gaps
- Automated customizable attack range labs in Azure and AWS to simulate client environments
- Simulated **MITRE Engenuity ATT&CK Scenarios** to prepare for Evaluations
- Extending Atomic Red Team framework to include custom Techniques and attacks not offered.

Dell SecureWorks | Taegis Threat Detection and Response | **June 2018 - Jan 2024**
Senior Principal DevOps Engineer

- Created Terraform modules to define our entire cloud **infrastructure as code**
- Automated deployment of scalable **Kafka cluster** on AWS. Worked with AWS on their own managed offering (MSK)
- Turned various applications into **automated cloud deployments** like Vault, Nexus Artifact Repository, and Matomo
- Implemented a pipeline for researchers to launch their own Jupyter Notebooks backed by Apache Spark using **AWS Sagemaker** and **AWS EMR**
- Complete CICD automation for team using Gitlab-CI and custom hooks
- Deployments to production **hundreds of times** per day
- Cookiecutter project templates for Engineering team to use, including importable modules for Gitlab-CI
- Developed **Push-Button Kubernetes Clusters** using Terraform, and GitOps
- Created Push-Button Environments to stand up the entire platform in new AWS accounts using **Terragrunt, Terraform, and GitOps**
- **Live Migration** of K8s workloads from Rancher to EKS.
- Wrote API in Golang for keeping metadata of all environments for CI consumption
- Wrote **Golang** application to generate Terraform from a yaml specification
- Wrote various Pulumi modules for Pulumi's Automation API for self-service infrastructure
- Developed an **Internal Developer Platform** using Spotify's Backstage
- Service Discovery and shared configuration using **Consul**
- Supported a rapidly growing team through **metrics driven automation**

Dell SecureWorks | Counter Threat Unit | **June 2015 - June 2018**
Information Security Research Advisor

- **Python** development for security-related tools to assist researchers
  - Application to ingest detonations from various **malware analysis** sandboxes using an extensible solution for processing, storing, discovering, classifying, and clustering **hundreds of millions** of malicious and non-malicious files
  - Network IDPS Signature Management with signature review and testing using a fleet of network sensors
  - **Vulnerability Database** that feeds into other applications and processes
  - Ruleset **REST API** for serving ruleset packages to clients
- Delivered deployment pipelines for AWS, vRealize, and Marathon using Packer, Ansible, and Terraform (https://bit.ly/2Rzy9XQ)
- Converted Proof of Concept projects to full-stack production grade applications
- Dynamic Configuration Management using **Vault**
- Implemented **ChatOps** and the ability the deploy from slack using Hubot with custom modules

Stackfocus | May 2014 - Present
Co-Founder, https://stackfocus.org

- Developed **full-stack web applications** designed to be packaged and deployed easily
- Postmaster, a web application to manage domains, users, and aliases on a **Linux mail server**
- **ChescoDispatch.com** - A website dedicated to showing Active Incidents in Chester County, PA

Education

Champlain College | May 2015
Bachelor of Science in Computer Networking and Information Security
Specialization in Cyber Security, Minor in Digital Forensics
Dean's list | Trustee's Scholar
Teacher's Assistant - Intro to Networking

Activities & Achievements

Certified Kubernetes Administrator (CKA) | Winter 2020

AWS Certified SysOps Administrator - Associate | Fall 2017
AccessData Certified Examiner (ACE) | Spring 2013
CompTIA Security+ Certified | Fall 2013
VMware Certified Associate - Data Center Virtualization | Fall 2013
Competed in the **2013, 2014, & 2015** North Eastern Collegiate Cyber Defense Competition
Won contest to attend Black Hat Security Conference 2014
Contributed to the Linux Kernel - bf5777bcdc540661f2f5d531a13e4e9c9fb7ee22
This resume has its own continuous delivery pipeline (https://bit.ly/2F42xEA)

Technical Buzzwords

Languages
Python, Golang, Terraform, Ansible, Perl, Bash, TCL
Frameworks/Libraries
Flask, SQLAlchemy, Django, Click, Buffalo, Gin, Rails, Sinatra
Databases/Queues
MySQL, PostgreSQL, Memcached/Redis, RabbitMQ, Kafka, ElasticSearch
Operating Systems/Virtualization
Kubernetes (EKS, Rancher, K3s, OpenShift/OKD), Mesosphere DC/OS, SmartOS, Docker, KVM, Proxmox, VSphere, VirtualBox
Clouds
AWS, Azure, GCP, Digital Ocean, Civo