

Kevin Law

<https://kevinlaw.info> | mail@kevinlaw.info
[Github](#) | [Codewars](#)

Site Reliability Engineer & Security Professional

- **Five+** years working in application development with high availability and time-critical services.
- Eight+ 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 | RedCloak Threat Detection and Response | **June 2018 - Present**

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
- Created **Push-Button Kubernetes Clusters** using Terraform and Helmfile
- Wrote **Golang** application to generate Terraform from a yaml specification
- 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
 - OSINT Vulnerability list scraping using **Python Scrapy** and **Jira**
 - 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 to deploy from slack using Hubot with custom modules

Dell SecureWorks | Counter Threat Unit | **May 2014 - August 2014**

Security Researcher Intern

- Developed web application to provide coverage metrics for iSensor Appliance using **Python Flask** and **Extjs**
- Programmed Ixia Breaking Point appliance to run a large suite of **automated tests**

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**

Senator Patrick Leahy Center for Digital Investigation (LCDI) | April 2013 to May 2015

Network Administrator

- Managed lab computers using Lansweeper and pushing images using **WDS**
- Implemented a robust backup solution of case data using RAID arrays and **Domain Isolation**
- Used vSphere to virtualize services on the network, including Active Directory and **Enterprise Forensic tools**
- Designed and implemented a **HIPAA compliant** Digital Forensics Lab.

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

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, Buffalo, Gin, Rails, Sinatra

Databases/Queues

MySQL, PostgreSQL, Memcached/Redis, RabbitMQ, Kafka, ElasticSearch

Operating Systems/Virtualization

Kubernetes (EKS, Rancher, K3s), Mesosphere DC/OS, SmartOS, Docker, KVM, Proxmox, VSphere, VirtualBox

Clouds

AWS, GCP, Digital Ocean