Curry Searle

currance@gmail.com ❖ (940) 597-1183 ❖ Denton, TX

Seasoned IT security professional with 30 years experience delivering technical solutions in the corporate, start-up and higher-ed fields. I bring a strong background and track-record for solving technical problems by reducing complexity, increasing automation and scalability with a focus on security, reliability and cost savings. My experience working in small teams and the large enterprise provides me confidence to evaluate a scenario and implement a reliable solution no matter the scale.

SKILLS / TOOLS / CERTIFICATION / TRAINING

Cloud: AWS, Azure, GCP, Linode **Tools:** Cribl (Edge, Stream, Search), Wiz, Bitsight, Cycode, Grafana, Palo Alto Cortex XSOAR (Demisto), Prisma Cloud (TwistLock / RedLock), Mimecast, CyberArk, Akamai, Rapid7, Microsoft Defender ATP, TripWire Enterprise, DataDog, Jenkins, Saltstack, Terraform, Okta, Docker, Git, Jira, Confluence, Bitbucket, ServiceNow, Zabbix, SCCM **Scripting:** Python, BASH, PowerShell, CMD **Operating Systems:** Debian, Ubuntu & RedHat Linux (RHEL, Centos, Rocky), FreeBSD, OpenBSD, Mac OS X, Microsoft Windows Server 2016, 2012

Certifications & Training:
Cribl Certified Observability Engineer - CCOE User - April 2023 / CCOE Admin - July 2023
Cloudbees Certified Jenkins Engineer - Sep. 2016
TripWire 8.x training - Nov. 2019

WORK EXPERIENCE

Cribl **March 2023 – Present**
Sr. SecOps Engineer *(Remote) San Francisco, CA*

- Immediately identified and remediated problems with DMARC, SPF & DKIM records related to customer signup messages being flagged as junk mail.
  - o This early catch and resolution unblocked multiple customer sign ups and reduced toil for sales leading to significant revenue opportunities for the company.
- Implemented FIM solution using native Linux tooling along with existing internal Cribl tooling to meet compliance standards.
  - o This low-cost solution unblocked Cribl's expansion to the EMEA market by securing the cloud product and customer data for millions in additional ARR. This solution subsequently became part of the troubleshooting stack used by SRE to maintain the Cribl.Cloud product further showcasing Cribl's flexibility as a platform.
- Evaluated traditional and cloud-native EDR solutions for Cribl Cloud including Wiz, CrowdStrike, OSSEC & others.
  - o The evaluation and comparison data told a compelling story for protecting the Cribl Cloud offering further fostering the Cribl / Wiz partnership.
- Led the rollout and remediation effort of all critical errors to earn a spot on the "Zero Criticals" list in one of the fastest times seen by Wiz for a deployment of our size.
  - o This accomplishment further fostered Cribl's relationship with Wiz and led to a case study highlighting the rapid ROI seen by quickly and efficiently implementing the Wiz Agent as an EDR solution.
- Reduced personnel and time costs related to monthly product releases by automating the ProdSec Release Sign-off process.
  - o Manual, hours-long process reduced to an automated process requiring only a one-time review of an artifact and ticketing bugs for security compliance and certification of the release.

Apollo Information Systems **February – March 2023**

Engineer III - Cloud Migration Project *(Remote) Round Rock, TX*

- Developed and executed plan in coordination with Security Onion Solutions Enterprise Support for migrating on-premise, Security Onion distributed deployment architecture to Microsoft Azure.
  - o The solution increased reliability and reduced on-premise hardware costs while supporting terrestrial as well as cloud endpoints for monitoring security posture of dozens of remote locations.

GameStop, HQ **October 2018 – January 2023**

Sr. Security Engineer - Security Automation *(Remote) Grapevine, TX*

- Experience developing in Palo Alto's XSOAR tool (formerly Demisto) creating Automations & Playbooks to automate handling of incidents reported to the CIRT.
  - o Work included various 3rd-party plugins as well as custom automations (Python).
- Technical lead for on-boarding to Mimecast platform managing DMARC (SPF & DKIM) for all GameStop domestic and International properties.
- Principal CIRT engineer including after hours and on-call support requiring the ability to act as a stand-alone responder.
  - o On-call CIRT rotation to monitor and respond to security incidents, reviewing incoming alerts, analyzing data across multiple platforms to correlate behaviors, identifying suspicious or malicious activities and taking action to contain threats.
- Configure and manage Platforms & Safes in CyberArk including on-premise Active Directory, cloud and federated systems running Windows and Linux.
- SIEM migration from IBM QRadar to Rapid7 InsightIDR. Configured Log Sources (syslog, S3 bucket, WMI, tail file, etc.) for ingestion by the SIEM including custom scripting solutions for non-traditional log source ingestion.
- Configured RedLock & TwistLock monitoring and scanning of on-premise, cloud and container workloads. Migration from hosted solutions to Palo Alto's Prisma Cloud and associated reconfiguration of scanning and alert policies.
- Upgrade TripWire from 8.1 to 8.7.. Monitor and alert coverage for all systems in PCI scope.
- Technical lead for ThinkGeek infrastructure and services migration from Fairfax to Grapevine. Migration of on-premise services to AWS cloud. Troubleshooting custom warehouse and order management system written in Perl with MySQL back-end. Migrate VirtualBox Enterprise virtualization systems to AWS EC2 and RDS instances. Export and integrate OpenLDAP and SAMBA services to GameStop's enterprise Active Directory forest.

Bloomreach **November 2017 – April 2018**

Head of Internal IT Operations *(Remote) Round Rock, TX*

- Upgrade and consolidate multiple Atlassian Confluence instances to one providing a unified intranet for internal collaboration and documentation.
  - o Impact was global across all nine geographies of the company saving over ten-thousand dollars annually across all instances.
- Consolidate across all geographies our mixed environment of Google Hangouts and WebEx to the Zoom platform.
  - o Consolidation saved several thousand dollars annually as well as provided a uniform experience for all locations.

Bloomreach **(Continued)**

- Experience with Terraform and SaltCloud for AWS automated deployments of Linux EC2 instances and other AWS technologies including EBS, RDS & ELB in Classic and VPC instances
    - Implementing IAC reduced configuration errors and reproducibility as well as acting as a built-in disaster recovery measure with configurations stored in git repository in a separate Amazon AZ.
- Data migrations from local MySQL & PostgreSQL to Amazon RDS
    - Annual cost savings with increased reliability and redundancy from eliminating hardware, power and cooling of on-prem hardware.
- Manage secure web applications (Java, Python, Go) in Amazon ELB reverse-proxy configurations (Nginx, Apache)
- Administrator of multiple Single Sign On and authentication & authorization platforms (Okta, Auth0, LDAP, Active Directory)
- Work with staff counsel on GDPR compliance documentation for internal IT systems and processes.
    - Inventory and documentation of third-party services uncovered duplicate and orphaned services which resulted in annual cost savings as well as eliminating risk of potential legal exposure.

University of North Texas - System / Denton Campus **October 1993 – November 2017**

System Administrator / ITSM / Postmaster / Team Lead *Denton, TX*

- Various departments, roles & responsibilities including large-scale server & desktop deployment/management in both cloud (Azure) and on-premise virtual and physical infrastructure (Linux, Windows, Mac OS X)

MEDIA

Jenkins World 2016 - *Jenkins for Smarter Operations* - Presenter: https://youtu.be/QAxfoyxBuZM

EDUCATION

University of North Texas **September 1993 - August 2023**

Major in Applied Technology Training and Computer Education *Denton, TX*

- Alpha Phi Omega - National Service Fraternity
- UNT Billiards Club - President / Staff Sponsor