

Resume

Andrew J Krug

1075 Washburn Lane

Medford, OR 97501

Mobile: 541 708 1002 Email: andrewkrug@gmail.com

Skills

Specialty: AWS Cloud, Google Cloud Organization, Identity and Access Management, risk analysis, serverless, DynamoDb, AWS Lambda, Cloud Security, Response Automation, and Forensics.

Education

Bachelor of Science Computer Science Southern Oregon University. Computer Security Information Assurance provides a unique security focused degree program. It has a strong emphasis in Systems Administration with emphasis in IDS, Algorithms, and industrial computer forensics.

RHCSA v7 - Recertified 2014

Computer Experience

Formerly Staff Engineer and Architect on Mozilla Identity and Access Platform serving 100,000+ contributors using AWS Lambda, Kinesis and DynamoDb. Also have a diverse background in leadership, technical evangelism, courseware authoring, teaching, and security research.

Product Management

Prior product management of Mozilla Google Cloud Organization, Mozilla Change Integration Service, Mozilla SSO Dashboard, and Mozilla Kubernetes Reference Architecture.

Conferences

- 2016 BlackHat USA - Automating IR and Hardening AWS Environments
- 2016 DerbyCon - Automating IR and Hardening AWS Environments
- 2016 BSides PDX - Automating IR and Hardening AWS Environments
- 2017 BlackHat USA - Hacking Serverless Runtimes
- 2017 BSides PDX - Hacking Serverless Runtimes
- 2017 Code Monsters - Hacking Serverless Runtimes
- 2018 BSides PDX - Container Cloak
- 2018 ReInvent - 5 Open Source Security Automations
- 2019 ReInforce - An Open Source Adventure in the Cloud
- 2020 ReInvent - DIY Guide to runbooks, playbooks, and incidents

Hobbies

At Southern Oregon University I pursued a classical education finding ways to integrate and fuse the arts into my education. I am an avid classical saxophonist and play in a number of large and small saxophone ensembles. I also enjoy the outdoors, currently having two horses that I use for trail riding and timed events.

Cloud Security Vacasa.com

Jan 2020 - Present

Direct all efforts around Security in the AWS Cloud Environment. Create roadmaps for security engineering, perform threat models, risk assessments, and create tooling to enhance posture and remediate key findings. On-call for incident response. Advise in architecture reviews and create governance standards.

Lead an interim engineering team of DevSecOps to perform Security, Devops, and IAM. In response to the COVID-19 virus. Organize, facilitate, and measure success of different cost cutting initiatives.

Design, Develop, Document Services Developed In House:

- Blockabot - Universal Blocklist Pipeline
- Continuous Auditing Capability

Staff Security Engineer - Mozilla

Mozilla - August 2018 - Jan 2020

*Lead the effort around **Mozilla Open Source Security Software Brand**.*

- Product Management of Mozilla Enterprise Defense Platform.
- Security architecture for Mozilla multi-cloud strategy (specifically GCP).
- Design, develop, and market internally tooling in python, rust, etc to make Mozilla more secure.
- Present at conferences as an evangelist for security and open source.

Collaborate as needed with other product managers, program managers, and product managers to facilitate desired outcomes raised by engineering.

Report to Senior Leaders and board on progress for KPIs.

Product innovation:

- Mozilla Defense Platform
- GuardDuty Multi Account Manager
- PyKMSSig
- AWS Cross Account Output Service
- Mozilla AWS Federated Access CLI
- GSuite Community Drive Driver

Participate in:

- Mozilla Culture of Experimentation
- DevOps Cohort
- RedTeam Exercises
- Incident Response Remediation
- Phishing Investigations

Senior Security Engineer - Mozilla

Mozilla - February 2017 - August 2018

Senior Engineer working on Identity and Access Management Stack. Design, develop, support APIs for information around Identity as it relates to security. Additionally, perform DFIR for AWS Cloud, design controls, carry pager. Participate in ideation, user journeys, design for cohesive IAM system design.

Senior Software Engineer - Symantec

Symantec - August 2015 to January 2017

Note : BlackFin Security was acquired by Symantec

As a Senior Software engineer design and develop capture the flag challenges to meet learning outcomes. Serve as technical architect for emerging prototype platforms to facilitate gamified security education. Contribute design, code, patches.

Product Innovation:

- Cyber Skills Platform
- ThreatForge

Senior Content Developer - BlackFin Security

BlackFin Security - May 2014 to August 2015

The Senior Content Developer designs capture the flag challenges at varying degrees of difficulty in a variety of languages. Creating content and contributing features to RoR Stack platform ThreatForge. Heavy emphasis on DevOps automation and custom tooling.

Technical Training RHCSA - InfoSec Institute

Technical Training RHCSA InfoSec Institute - February 2013 to Present

Responsible for the development of curriculum for RedHat courses and instruction. Teach candidates from a diverse background in bootcamp style training.

IT Operations Manager - Oregon Shakespeare Festival

IT Operations Manager Oregon Shakespeare Festival - November 2012 to May 2014

The IT Operations Manager's role is to ensure the stable, reliable and uninterrupted service of IT infrastructure for the Oregon Shakespeare Festival by constantly monitoring & evaluating current systems for improvements in efficiency, security and cost reduction. This person will take a key role in ensuring organizational PCI compliance, participate in departmental strategic & budget planning, and manage the day-to-day activities of the operations team.

--- More History and References Available on Request ---