Michael Metcalf

Email   LinkedIn   Github   **PDF Format**

Security Engineer with 9+ years experience in corporate identity and access management programs.
Primarily interested in designing, implementing and operating IAM tooling and services.

Currently at Citadel, building identity infrastructure for quantitative researchers and engineering teams alike.

Work Experience

2022 - Present   Citadel LLC   ⌐

Senior Security Engineer

- Drove continued adoption of Hashicorp Vault for static and dynamic secrets management across the firm's broad compute footprint.
- Designed and implemented Configuration and Policy as Code for Hashicorp Vault.
- Contributed to Github Enterprise Configuration as Code Terraform project.
- Designed and implemented short-lived privileged access management to Linux hosts
- Designed and implemented an on-prem to Google Cloud Identity bridge backed by Vault OIDC.
- Vendor Security Reviews & Line of business application/cloud security oversight.
- Contributed to an identity provider migration

2017 - 2022   Riot Games   ⌐

2020 - 2022   Security Engineer – Information Security

- Tech lead the org-wide identity provider migration. Resulted in 700+ services migrated within a year.
- Wrote large-scale terraform projects (providers & modules) to support various IAM operations
- Contributed to refactoring AWS tooling used across the engineering org
- Implemented serverless event-based logging pipelines for all systems in the IAM stack
- Vendor/internal security reviews
- Continued discovery in BeyondCorp Access Proxies for employee use

2018 - 2020   Systems Administrator - Information Security

- Published internal RFC for identity federation criteria, lead the vendor evaluation and presented findings to security leadership
- Designed and implemented a RESTful API for LDAP user and group management in Go
- Integrated corporate AuthZ into player-facing AuthZ to grant access to R&D assets for internal Rioters and contractors
- Implemented a BeyondCorp Access Proxy proof of concept for intranet sites via Duo Network Gateway
- Wrote ETLs for various IAM functions/authorization automations
- Designed and implemented geo/org based authorization pipeline as a compensating GDPR control for all production facing servers to consume.
- Organized team's codebase and documentation structure
- Contributed in disaster recovery, incident response, and internal threat scenarios

2017 - 2018   Systems Administrator - Information Technology

- Defined standards, administrate and document the corporate Identity Provider - Onelogin
- Assisted internal teams in defining their AuthN/Z tech stack and authorization models against given business requirements
- Managed vendor relationships for SSO, user lifecycle management, and overall security auditing
- Core contributor to the Rioter/Vendor onboarding pipeline

2015 - 2017   Broadcom   ⌐

Desktop Support Services Engineer - Information Technology

- Managed/Resolved high volumes of emergent operational tickets while maintaining stringent team SLA
- Supported company-wide AD Domain migration and Email migration from Exchange to Google Apps
- Wrote knowledge base articles for DSS L1-L3 teams (Pertaining to SAP, PGP, and Cisco/telecom)
- Wrote macOS software deployment packages and scripts for JAMF
- Managed enterprise apps

2014 - 2015   AIT Management

Systems Administrator & Trainer

- Rebuilt and maintained corporate LDAP Directory Services and Identity Provider
- Administrated enterprise apps and MDM Program
- Built employee onboarding and IT utility automations
- Wrote and maintained technical/operational documentation
- Maintained network infrastructure across 45+ office sites
- Taught new hire training and onboarding

Education

2016-2017, 2020 Irvine Valley College

My academic history reflects the seasons in life where I have wanted to learn more, even if occupationally it was less relevant. My end goal is to earn a BS in Computer Science.

Skills

```
Last login: Tue Jun 13 01:42:56 on ttys006
metmac resume.md [metmac/resume/2021]
tree -L 2 ./skills
./skills
├── auth-standards
│   ├── kerberos
│   ├── ldap
│   ├── OAuth-2.0
│   ├── open-id-connect
│   ├── x509/pki/mTLS
│   ├── radius
│   ├── saml-2.0
│   └── u2f/FIDO2/webAuthN
├── gcp
│   ├── google-cloud-identity
│   ├── iam
│   ├── gcs
│   ├── anthos
│   ├── secrets-mgr
│   ├── artifacts-registry
│   └── workforce/workload-identity-federation
├── aws
│   ├── aws-sso
│   ├── cloud-watch
│   ├── ec2
│   ├── eks
│   ├── event-bridge
│   ├── iam
│   ├── lambda
│   ├── secrets-mgr
│   ├── sts
│   ├── vpc
│   └── workspaces
├── concepts
│   ├── etl-pipelines (airflow)
│   ├── containers/k8s
│   ├── event-driven-architecture
│   ├── microservices-architecture
│   ├── serverless-architecture
│   ├── infrastructure-as-code
│   └── sop/xss/cors/csrf
├── enterprise-systems
│   ├── active-directory
│   ├── azure-ad
│   ├── carbon-black
│   ├── data-dog
│   ├── duo-security
│   ├── intune
│   ├── jamf
│   ├── mobile-iron
│   ├── new-relic
│   ├── okta
│   ├── onelogin
│   ├── ping-federate
│   ├── pulse-secure
│   ├── splunk
│   └── slack-enterprise-grid
├── frameworks-and-libraries
│   ├── aws-sdk-for-go
│   ├── hvac
│   ├── boto3
│   ├── go-ldap
│   ├── labstack-echo
│   ├── passport-js
│   ├── py-ldap3
│   ├── serverless-framework
│   └── tailwindcss
├── languages
│   ├── go
│   ├── python
│   ├── powershell
│   └── bash shell-scripting
├── markup
│   ├── ascii-doc
│   ├── css
│   ├── html
│   ├── json
│   ├── markdown
│   └── yaml
└── open-source-software
    ├── airflow
    ├── atlantis-ci
    ├── consul
    ├── dir389
    ├── docker
    ├── elk-stack
    ├── function-beats
    ├── git
    ├── jupyter-notebooks
    ├── jenkins
    ├── locust.io
    ├── open-ldap
    ├── terraform
    ├── terragrunt
    ├── vault
    └── datadog-vector

9 directories, 83 files
```