

Cailen McQuattie

Software Craftsman. Data and ML Ops. Cybersecurity Expert.

Toronto, Canada

EXPERIENCE

N-Dimension - VP, Engineering (Toronto Area)

2018 - PRESENT

Protected NA critical infrastructure from cyber threats using machine-augmented intelligence. Built and owned the full product portfolio, through full product lifecycle.

60/40 split of Engineering / Engineering Management.

Designed, architected, and built:

- Assets and tools to ingest, contextualize, and predict on **25k events / second**, and billions of events at once
- Research tools, predictive scoring, and prioritization algorithms for cybersecurity professionals
- **CI/CD, containerization, orchestration, secrets management, health telemetry reporting and alerting** tooling for network of IoT devices, private x AWS hybrid cloud
- IDS, IPS, continuous vulnerability scanning
- **High durability and high availability** strategies for mission-critical data ingest and query platform
- Transform individual analyst investigations in to highly-automated threat intelligence for entire customer base
- Sourced, interviewed, and hired engineers and data scientists, conducted personnel reviews, set career growth targets with team
- Coached, unblocked, reviewed code, lead scrum and retro
- Developed product requirements, designs, and architecture by interviewing key customers and stakeholders
- Set product roadmap with executive and board, estimated capitalization requirements and deadlines

Tools I use daily or weekly:

Python, Go, Bash, Postgres, PostgREST, TimescaleDB, JavaScript, React, AWS, Django, Pandas, Jupyter Notebooks, Redis, Celery, RabbitMQ, Docker, Ansible, AWX (Ansible Tower), Bamboo, TravisCI, Prometheus, Grafana, AlertManager, Syslog, Syslog-ng, Snort, Suricata, OpenVAS, OpenVPN, Fail2Ban, UFW, iptables, Logwatch, sed, monit, crontab

N-Dimension - Senior Full Stack Engineer (Toronto Area)

2017 - 2018

- Moved product from a 45-minute PDF generation process to cloud-native real-time analytical research, reporting, and alerting tools with sub 4-second API query response times
- Built **advanced IDS detection capabilities**, including **multi-step**

SKILLS

Software Engineering

Software Architecture

Engineering Management

Data Engineering

Data Science

Log Management

Network Intrusion
Detection

Web Application Security

Applied Cryptography

Network Security
Assessment

Orchestration

CI/CD

AWS

Infrastructure as Code

Database Design and
Admin

Data Mining

Networking, Routing, DNS

Firewall Management

TOOLS I'M EXPERT WITH

Python, Django, Pandas,
Flask

Postgres, TimescaleDB,
PostgREST

Docker, Docker Swarm

Bash

AWS just about everything

Prometheus, Grafana

attack classification, anomaly detection, and recommenders

Pattison Outdoor Senior Full Stack Web Developer (Toronto)

2012 - 2017

- Designed, built, launched, supported products worth > \$3M ARR in 2017
- Devops, orchestration, CI
- Microservices, web apps, microcontroller / human-interface integrations
- Security incident response
- Human-machine interface design and build, especially mobile
- Web application security
- Log management

Tools I used:

Python, Django, Flask, Pandas, Celery, RabbitMQ, Redis, Postgres, MongoDB, MySQL, Node.js, WebSockets, Docker, AWS, JavaScript, Angular

EDUCATION

University of Toronto, Trinity College

B.A. Specialist Economics

2007 - 2011

Minor in Comp. Sci. Coached intramural rugby for 3 years. Ran / Chair Frosh Week 2009. Student Life Don 2008.

PROJECTS

Canadian Dep't National Defence — *Understanding Cyber Intent*

2019

Machine intelligence augmented cyber-adversary detection, classification, and prediction. NLP, density estimation, principal component analysis, neural networks.

EthSF Winner — *BlocuSign*

2018

A SIMPLE decentralized merkle-proven, identity-attested, non-fungible, immutable, cryptographically-signed, interplanetarily-archived, digital-notarization-and-document-signature-as-a-service protocol on the blockchain!

EthDenver Winner — *DecentPost*

2018

dApp with state channel, curved bounty-slashing, decentralized exchange, and more.

JavaScript, ES6

Ansible, AWX

Bamboo, TravisCI

Snort, Suricata

OpenVAS

OpenVPN

TOOLS I'M ADEPT WITH

React

Redis

Celery, RabbitMQ

MongoDB

Node.js

Angular

MetaSploit

TOOLS I USE REGULARLY

ElasticSearch

LogStash

Elastic Beat

Cryptography 1 by Dan Boneh — *Stanford*

2017

Crypto-primitives and history through public key encryption.

Machine Learning 1 by Andrew Ng— *Stanford*

2016

Regression, SVMs, neural networks, anomaly detection, recommenders, dimensionality reduction.