Owen McCusker

Senior Principal Software Engineer

👤 Profile

Experienced Cyber-Security Researcher and Software Engineer adept in bringing forth cloud and embedded expertise in the architecture, design, installation of software systems. In 1989-1991, an experienced analytical chemist, focused on method development, analysis, and data acquistion. My roots are in machine control, distributed computing, and later in my career I introduced a patented concept for the cyber security industry called **aggregate behavior analytics** in 2009. At Secureworks, as part of a team, we migrated our CTP platform initially to a private cloud, VMware, and then to AWS, all while staying live and processing **trillions of events** a day.

💼 Employment History

Senior Principal Software Enginner at Secureworks, remote
January 2014 — Present

- Lead a 5 person Development Team, for CTP (Zulu), based on Kanban Agile, held daily scrums, managed KPIs, and monthly goals.
- Developed a file extractor/analysis capability pipeline in golang, integrated into an AWS environment e.g. S3, SNS, SQS.
- Created gitlab-ci pipelines using multiple stages including terraform, monitor, helm. Established moving platform to multiple production environments to providing scalability
- Containerized multiple applications using docker, providing a consistent development and deployment process
- Prototyped a Python application that ingests vpcflows from S3, and transforms the data to store into postgresql.
- Prototyped a normal detection models using network flow data transformed within Sagemaker using Spark and Jupyter
- Prototyped an XR concept using UE5, and projecting data has objects within the game environment, for analyst to interact with
- Developed and researched UXs using d3.js and javascript dynamically visualizing transformed network and host data based on time series
- Matured the root cause analysis (RCA) process reducing major incidences for the company

Principal Analysts at Sonalsyts, Waterford, CT
January 1999 — November 2014

- Lead a team of 15 people, consisting of multiple organizations creating a behavioral-based ontology driven cyber fusion technology under a contract by DHS S&T.
- Developed a streaming framework to parse and process network flow data

Details

15 Spring Rock Road
East Lyme, CT, 06333
United States
860-912-7166
mccuskerowen@gmail.com

Links

owenmccusker.org
scientia-fusione.org
Devops SRE Blog
Data Science Blog

Skills

Project Management

Proposal Writing

Patent Writing

Agile Methodologies

AWS EC2, S3, SQS, IAM

Terraform/AWS

Data Science

Jupyter, Spark

Kali Linux , SiLK, honeypots, IPtables, Packet Filter Firewall (PF), SNORT, Nessus, Nmap

gitlab-ci, Jenkins

Graphql, Rest API Dev

Java

Golang

C++

C

Python

SQL, Postgres, Mysql

Mongo

- Personally wrote a patent on the concept, which was awarded in 2011, reviewed by a patent attorney.
- Invited to attend a number of workshops in cyber-security from NITRD, DARPA, and ODNI.
- Lectured NATO in Estonia at their CCDCOE on behavior analytics
- Acted as technical lead for the Finance Sector in the largest "to-date" cyber security exercise put together by DHS called "Livewire" that involved the financial, energy and government sectors. Worked with various financial institutions to create meaningful network typologies and "attack trees" to simulate a nation-state attacking our information infrastructure
- Developed a next generation distributed weather analysis ingesting GB of data per day, using C/C++ OOAD running on Redhat, persisting in a tuned postgresql db, where I developed DDL to manage the instance.

☙ Education

MS in computer science, Rensselaer Polytechnic institute, Hartford, CT

September 1994 — December 1999

My studies were focused on Object Oriented Analysis and Design, and Distributed Agent technologies. My Master's project report received a 1st runner up in the annual student conference in 1998 which was focused on a prototype web spider I built using a custom distributed agent framework written in Java. The goal was to fuse data from heterogeneous data sources. The project was called DHAS.

BS in chemistry, and minor/studies in computer science, University of Connecticut, Storrs, CT

September 1984 — December 1988

My studies were focused in on environment chemistry, analytical chemistry and computer science. My main goal was to combine computers and chemistry for data acquisition.

★ Patents

Patent - System and method for privacy-enhanced cyber data fusion using temporal-behavioral aggregation and analysis, Waterford, CT

June 2013

 https://patents.google.com/patent/US20120072983

◄ References

References available upon request

★ Clearances

TS/Secret - At Sonalysts, Waterford, CT

January 2003 — January 2014