Owen McCusker

East Lyme, CT, 06333 | 860-912-7166 | mccuskerowen@gmail.com | LinkedIn
https://scientia-fusione.org/ | https://owenmccusker.org/

Senior Principal Software Engineer

Accomplished leader with proven success spearheading transformative initiatives at the intersection of cybersecurity and data science. Over two decades of trailblazing expertise across diverse domains, driving breakthroughs in program development, product innovation, and technical leadership. Known for leading high-impact teams and envisioning/creating cutting-edge solutions that redefine industry standards.

Experienced Cyber-Security Researcher and Software Engineer with a track record of excellence in cloud and embedded systems architecture, software design, and installation. Distinguished for success in diverse industries, including cyber security and machine control. Experienced in pioneering groundbreaking contributions, such as the patented aggregate behavior analytics concept in 2009. Stellar record of overseeing seamless migration of the CTP platform from inception to a private cloud (VMware) and culminating in a transition to AWS. Instrumental in maintaining uninterrupted operations and processing billions of daily events on the CTP platform, now trillions with the new Taegis platform. Credible history of constructing effective solutions from the ground up, evidenced by the establishment of cutting-edge laboratories, including a basement security lab and a behavior lab at Sonalysts. Rich background in machine control and systems development.

- Accomplished cyber security researcher, data science researcher specializing in aggregate behavioral analytics; astute architect and software/systems developer with skills in distributed and embedded technologies; versatile project and technical lead; and dynamic Cloud DevOps architect; equipped with a background in LIMS systems management.
- Visionary thinker with solid understanding of assimilating diverse techniques from various domains, such as nature-inspired defense strategies, and adapting them ingeniously to fortify cyber security.
- Seasoned cyber security lecturer traveling and speaking at NATO/Estonia, UK, Wales, MIT, University of Memphis, and San Francisco.
- Dedicated to playing a pivotal role within an innovative and diversified team, fostering the evolution of next-generation reactive/agile data processing, machine control, and machine-learning platforms.

AREAS OF EXPERTISE

Project Management | Data Science | Cybersecurity | Machine Learning | Cybersecurity Strategy & Implementation | Cloud DevOps/AWS
Network Security | Technical Leadership | Behavioral-Based Cyber Fusion Technologies | Product Development & Innovation
Data Fusion & Mining | Program Development & Management | CICD Pipeline Enhancement | Threat Detection & Mitigation
Cyber Threat Analysis | Data Visualization | Agile Methodologies | Cloud Computing | Data Fusion Techniques | Incident Response

ACHIEVEMENTS RELATED TO MACHINE LEARNING, DATA SCIENCE, CLOUD COMPUTING. ARCHITECTURE & SOFTWARE DEVELOPMENT

- Led the establishment of a groundbreaking capability centered around aggregate behavioral analysis of network security data.
  - Formulated a proof-of-concept (POC) solution for extracting VPC flows from S3, followed by data transformation for storage in PostgreSQL.
  - Crafted a suite of Python-based tools reminiscent of USCERT's SILK platform for VPC flow with ongoing enhancement efforts, including porting to Golang for boosted performance.
  - Created an immersive collaborative VR prototype where analysts can interact with flow data using Unreal Engine v5.
- Spearheaded the development of an ontology-driven data fusion and data mining prowess, specifically tailored for DHS (refer to projects section) using C++, and Java.
- Documented and captured platform design and changes using Confluence, Miro, Lucid.
- Managed tasking with JIRA, created stories, subtask, and bugs, managing backlogs implementing features and fixes using Agile Sprints.
- Developed classification models leveraging the amalgamation of network security data from diverse sources (detailed in security tools and data science tools sections).
- Advocated for the adoption of a comprehensive data science development lifecycle employing Jupyter and Java technologies.
- Engineered inventive multi-modal user interface functionalities deploying Java and JavaScript, exemplified by dynamic tools like D3.js.
- Devised and implemented robust data acquisition mechanisms compatible with a wide range of network sensor technologies (explore security tools section).

- Formulated a groundbreaking solution for handling substantial volumes of network security data, implementing statistical aggregation as outlined in the associated patent.
- Established a pioneering layered machine learning architecture that fosters fusion and facilitates knowledge discovery (consult publications and MIT lecture link: https://vimeo.com/105563432).
- Delivered lectures on the subject of Behavioral Aggregation at distinguished symposiums, workshops, and institutions like MIT.
- Oversaw the development of an immersive VR proof-of-concept (POC) utilizing Unreal Engine v5 for the in-depth analysis of flow data.
- Created an advanced file analysis capability using Golang within the AWS environment to enhance system functionality/security.
- Developed an efficient Mitre labeling pipeline utilizing Java to streamline the process for enhanced threat detection and analysis.
- Developed Docker-based applications designed for deployment within Kubernetes (K8s).
- Founded multiple cyber security labs leveraging tools like: Snort, Suricata, Pfsense, Openbsd, Endace DAG, USCERT Silk tools, Metasploit, directional antennas for wardriving, Kali, nmap.
- Instituted comprehensive guidelines and standards inspired by 12-factor applications and reactive platforms. Standards include principles like statelessness and agility.
- Integrated Metrics and Observability capabilities into intricate cloud-based solutions, effectively managing the processing of billions of events daily. These initiatives significantly enhanced system monitoring and performance analysis.
- Designed and implemented end-to-end Continuous Integration and Continuous Deployment (CICD) solutions, orchestrating the cloud deployment of multiple components. Utilized tools, such as Jenkins, Openshift, and Docker for seamless deployment.
- Spearheaded research and architecture efforts aimed at expanding capacity through innovative scaling methods.
- Directed the establishment of Root Cause Analysis studies, resulting in notable improvements in system resilience and stability. This contributed to minimizing downtime and enhancing overall system robustness.
- Avid open source developer and blogger at owenmccusker.org.

PROFESSIONAL EXPERIENCE

SECUREWORKS – REMOTE

SENIOR PRINCIPAL SOFTWARE ENGINEER| 2016 TO PRESENT

Architect, Software/Systems Engineering, Data Science and Machine Learning:

- Led technical initiatives as a part of the Counter-Threat Platform and Taegis teams, while serving as Technical Lead and AWS Developer.
- Employed Terraform and Golang to orchestrate the creation of EC2 instances along with associated resources like S3, SQS, and SNS, pivotal in establishing a novel file analysis pipeline for the platform.
- Utilized Java within the Counter-Threat Platform (CTP) to enhance and mature Mitre Attack Coverage research through event data. Employed data visualization techniques, such as interactive bubble charts and heatmaps for improved insights.
- Successfully Led, designed and implemented the transition of our platform from on-prem hardware, to a private cloud (VMware) and finally to a public cloud (AWS). This involved the containerization of our applications using docker and the use of kubernetes. The system had no downtime affecting SLAs for clients.
- Designed and executed a proof-of-concept (POC) that effectively ingests VPC flows from S3, transforming the data and storing it in PostgreSQL. Crafted a suite of Python-based tools resembling USCERT's SILK platform tailored for VPC flow.
- Spearheaded the creation of a collaborative Data Science platform, leveraging Zeppelin, and seamlessly integrating diverse tools for streamlined development and scaling, transitioning Machine Learning (ML) projects from development to production.
- Demonstrated proficiency in data visualization by developing Proof of Concepts (POCs) utilizing technologies like D3, Bootstrap, and Apache Tiles. Visualized transformed graph flow data in the immersive environment of Unreal Engine.
- Constructed a central Zeppelin/Spark capability in VMware, and introduced an EMR-based Jupyter Lab capability in AWS for efficient handling of network sensor data.

CICD Development:

- Enhanced the Continuous Integration and Continuous Deployment (CICD) pipeline, combining Jenkins and Ansible frameworks for improved efficiency and reliability.
- Integrated Docker into the pipeline to facilitate the creation of images and smooth deployment processes to production environments. Future plans include integrating Kubernetes/OpenShift for enhanced container orchestration.
- Streamlined build processes by integrating Gitlab-CI, Terraform, Helm, Jenkins, Ansible, Maven, and Docker, which facilitated the deployment of images to both provisioned VMware systems and future EC2-based VMs in AWS.

Product Development and Architecture:

- Took charge as a Technical Lead (in 2019) with special emphasis on devising an ontology-driven data architecture instrumental in the application of Mitre Attack tactics and techniques to detectors.

Cloud DevOps:

- Demonstrated Cloud DevOps skills by implementing a cloud-agnostic CICD strategy, observability using Datadog and Grafana, Integrating Monitors to Pager Duty..

PRINCIPAL ENGINEER | 2014 to 2016

DevOps Technical Leadership:

- Steered a technical team from 2014 to 2016 focused on advancing an event pipeline handling billions of daily events.
- Leveraged a unique blend of systems-level expertise and computer forensic experience, applying time series analysis to address complex cross-platform challenges.
- Established critical system health metrics and real-time health dashboards, proactively addressing potential service disruptions.
- Transformed the pipeline's operational resilience, replacing challenges with structured processes like formal root cause analysis and policies like comprehensive online documentation.
- Founded the Zulu team, later evolving into SecureWorks' inaugural Site Reliability Engineering team, SRE-Trion.
- Orchestrated the maturation of the pipeline platform, unlocking avenues for innovative pursuits by enhancing operational efficiency.

Research and Development, Analytics, Machine Learning, GUI Development:

- Drove initiatives in Kill Chain Analysis, Graph Analysis, and Data Collection, capitalizing on the potential of R and RStudio.
- Initiated a pioneering Data Science Development Process, emphasizing comprehensive modeling from initial data understanding through normalization and transformation to advanced model development and training.

Product Development:

- Demonstrated proficiency in development, actively utilizing tools, such as Daemon Tools, ActiveMQ, and Protobuf for Java development.
- Oversaw the deployment of the initial vulnerability management feature, advocating for the adoption of the Mitre CPE standard, eventually evolving into a scalable Asset Management platform.
- Achieved a remarkable 30% performance boost in pipeline processing through strategic optimization efforts.

Technical Leadership:

- Pioneered one of the earliest DevOps teams as a technical leader, bridging the gap between development and operations. The team's evolution culminated in the establishment of SecureWorks' inaugural SRE team.
- Introduced the Kanban process (a flexible agile methodology) to enhance operational agility, enabling rapid adaptation to changing project dynamics.

CICD Development:

- Collaborated with the team to streamline the build process, transitioning from ANT to Maven for Java applications.
- Automated builds, initially using Electric Commander, and incorporated configuration templating to replace manual configurations, improving efficiency and reliability.

SONALSYTS INC. – WATERFORD, CT
PRINCIPAL ANALYST: GUARDIAN SERVICES | 1999 TO 2014

Program Leadership:

- Led a multifaceted team comprising 15 members across various organizations, collaboratively developing a cutting-edge behavioral-based cyber fusion technology for DHS S&T contract.
- Developed an advanced analytics platform focused on detecting cyber threat agents via behavior aggregation that bolstered cyber defense capabilities.
- Gained recognition by attending prominent workshops in the field of cybersecurity, hosted by organizations like NITRD, DARPA, and ODNI.
- Managed the deployment of a scaled-down cyber range employing virtualization, enabling comprehensive training and facilitating behavioral analysis development.

- Crafted and managed a sophisticated 9-node HBase (Hadoop, Zookeeper) system, proficiently handling substantial behavioral data volumes for machine learning research and development.

Product Development:

- Served as Principal Investigator from 2006 to 2009 for DHS Botnet Detection and Mitigation Phase I and Phase II SBIRs.
- Integrated technologies and concepts to create DMnet, an innovative detection and mitigation system, later commercialized as Occulex.
- Conceptualized a unique data fusion system based on Mica Endsley's principles, implemented in C++ with more than 250K lines of code, facilitating data normalization for correlation.
- Architected a robust data model employing Postgresql, providing a strong foundation for cyber data fusion.
- Optimized the underlying data architecture, supporting data ingestion at 20 times real-time for medium-sized organizations.
- Deployed a collaborative configuration management system, combining Codebeamer and Subversion for streamlined development.
- Pioneered data mining methodologies applied to computer security using R and Weka, harnessing support vector machines, self-organizing maps, and decision trees, all empowered by data collected through the cyber data fusion system.

Externally Funded Projects:

- Acted as the Principal Investigator for Air Force's Wright-Patterson AFB, leading the development of cyber threat technologies centered around virtual behaviors.
- Took the lead as Principal Investigator for Phase I and II SBIRs under DHS Cyber S&T, driving the advancement of cybersecurity solutions.

ADDITIONAL EXPERIENCE

Principal Analyst, The Guardian Services Group & The Weather Group and Senior Analyst, The Weather Group at Sonalysts, Inc.

Senior Software Engineer, Lead Architect at Probot, Inc. **|** Senior Software Engineer, Lead Architect at Smartweb, Inc.

Senior Software Engineer, Lead Architect at Dictaphone, Inc.

Internet Engineer & Software Developer. Jamaica Trading Project at Fidelity Investments, Inc.

Senior Software Engineer at Gerber Garment Technology, Inc. **|** Open Source Development & Security Lab Development at Home Basement

Software Developer & Architect at Scancode, Inc. **|** Analytical Chemist, LIMS Manager at Environmental Research Institute, Inc.

EDUCATION

MS in Computer Science | Rensselaer Polytechnic Institute, Troy, NY

BS in Chemistry (Minor in Computer Science) | University of Connecticut, Storrs, CT

TECHNICAL SKILLS

Project Management: OKR, Scrum, Agile Development, CMMI Level 3, Requirements Management, Budget Management (> $1M)

Cloud DevOps: Private Cloud - VMware VRA (Provisioning Machines in Cloud), Public Cloud - AWS CLI, AWS Console, OpenShift/K8s, Helm, Datadog/Wavefront, Docker, Prometheus, Amazon Web services EC2, VPCs, and IGW (Simple Setups & Deployments), EMR setup for Data Science work using Jupyter

Containerization and Orchestration: Docker, Terraform, Kubernetes, and Helm

Visualization, HCI, HFE: D3js, OpenGL (Java-based), Unreal Engine v5

CICD/Configuration: GitLab-ci, GitHub workflows, Terraform/AWS, Jenkins, Groovy, Helm charts, Ansible, Docker, Codebeamer, Subversion, and Maven

Observation, Monitoring Tools: Datadog, Prometheus, Wavefront, jmon, Kabana, Filebeat

Data Science, AI, Machine Learning: Jupyter Lab, R, scikit_learn, Zeppelin, Weka, JESS, Cougar, Zeus, Agent Tool, BDIM Toolkit, KQML, KIF

Big Data: Hadoop, Spark

Database Systems, NoSQL: MongoDB, Cassandra, PostgreSQL, MySQL, Oracle

Security Experience: VPC Flow data, Kali Linux, NetflowTM, SiLK, Ourmon, honeypots (Nepenthes), ntop, IPtables, Packet Filter Firewall (PF), SNORT, ACID, OpenCA, Nessus, Nmap, SSLeay, PKI, Password Cracking, netcat, Ethereal, PGP, Security Modeling, Security Policy Creation, Backtrack, Auditor Security Collection, The Sleuth Kit, SANS SiFT, Metasploit

Languages: Java, Golang, C/C++, Python, Scala, HTML, XML, JavaScript, WSDL, IDL GoLang

Middleware, SOA, Web 2.0: Kafka, GraphQL, XML, JSON, Protobuf, Apache ActiveMQ, Kafka, ProtoBuf, JSON, SOAP, CORBA, DCOM, Java Message Service, MQSeries, Vitria, Servlet API, JRun, CGI, OpenMPI, (Socket programming), AJAX, SpringSource, GWT, MVP, Dojo, ZK Toolkit, GWT, JSON, XML, JPA, JDBC

Development IDEs: Idea, Visual Studio Code, Eclipse, Netbeans, GCC, AutoTools, MS VC++, Borland C++, Borland C++ Builder, Builder Accessory, Little Giant, Blue Cat 3.0, MS Device Driver Toolkit for NT, Orbix CORBA, JBuilder, Forte, Java SDK, JSEE, BSD Sockets, Winsock 2.0

Computer Systems: X86, Zilog Microprocessor, Hierarchical Storage Systems (HSM), MachZ, Arduino, Raspberry Pi (research only).

Operating Systems: CentOS, Mac OS X, Suse, Red Hat Linux, Slackware Linux, FreeBSD, OpenBSD, Windows NT 4.0, Windows XP, Solaris 2.5, HP-UX, HTTP Server Architecture

PUBLICATIONS

https://www.ccdcoe.org/uploads/2018/10/15_d2r2s2_mccusker.pdf

McCusker, O., Gittens, B., Glanfield, J., Brunza, S., Brooks, S., "The Need to Establish Both Object Identity and Behavior in Establishing the Trustworthiness of Network Devices within a Smart Grid," CSIIRW 2010

McCusker, O., Brunza, S., Gates, C., Glanfield., J., Patterson, D., McHugh, J., "Combining Trust and Behavioral Analysis to Detect Security Threats," Information Assurance and Cyber Defense, NATO April, 2010

McCusker, O., Brunza, S., Gates, C., Glanfield., J., Patterson, D., "DMnet: A Behavioral Analysis System Supporting Trust Measurements," Extended Abstract, Flocon January 2010, Visualization Track

McCusker, O., Kiayias, A., Newman, J., Walluck, D., "A Combined Fusion and Data Mining Framework for the Detection of Botnets," IEEE, CATCH 2009

McCusker, O., "Distributed Hybrid Agent Systems," in Proceedings of the 14th Annual Rensselaer at Hartford Computer Science Seminar, 1999. (1st Runner up in conference for best paper)

McCusker, O., "Tessera: An Agent-based Monitoring Framework that uses Agent Contexts to Facilitate Adaptability," Project/Thesis at RPI, 1999

PROJECTS **Details available on request*

Dept. of Homeland Security Phase I, Phase II, and Follow On Projects SBIR Project: Botnet Detection & Mitigation, (Jan 2006, Jun 2006) | (Jan 2007, Dec 2009, extending to 2013)

LECTURES

2012, Backus Hospital, Patient Safety Day. "Critical Decision Making and Cyber Security"

2011, Computational Cyber-security in Compromised Environments, C3E, "Threat Agents, Threat Behaviors, Cyber Analytics and Emergent Aggregate Behaviors"

2011, Cyber Security Expo, (CSE), "Promoting Mission Assurance and Risk Assessment Through Cyber Security"

2011, MIT/University of Wales Global Supply Chain Summit, "Aggregate Behavioral Analysis and Behavioral Trust"

2010, Cyber Security and Information Intelligence Research Workshop (CSIIRW), "The Need to Establish Both Object Identity and Behavior in Establishing the Trustworthiness of Network Devices within a Smart Grid"

2010, Information Assurance and Cyber Defense, NATO, "Combining Trust and Behavioral Analysis to Detect Security Threats"

2009, Cyber-security Applications and Technology Conference for Homeland Security, 2009, "A Combined Fusion and Data Mining Framework for the Detection of Botnets," McCusker et al