**GALEKWAN SANGO**

Rochester, NY

(347) 824-1576

[galekwansango@gmail.com](mailto:galekwansango@gmail.com) |<https://www.linkedin.com/in/galekwansango/> | <https://github.com/Gs5570>

Software Engineer with Cyber Security background my experience stem from a combination of building full-stack web application, requirement engineering, design, project planning, version control and testing. Skilled in developing, implementing, testing, and deploying web applications according to software development life cycle. **Available to work** now

Portfolio:[**https://galekwan-portfolio.netlify.app**](https://galekwan-portfolio.netlify.app/)

**Education**

**Rochester Institute of Technology**, Rochester NY| Master of Science Software Engineering **Expected May 2024**

**Per Scholas Software Engineering Bootcamp** on Full stack development **Completed**

**St John’s University**, Queens, NY| Bachelor of S Cyber Security Systems| **Minor:** Digital Forensic **May 2019**

**Certifications:** CompTIA Security +, CompTIA Linux+

**Skills /Languages/Technology/Framework**

**Languages & library:** React JS, JavaScript, Java, CSS/HTML

**Frameworks:** Express JS, Agile(scrum)

**Version Control:** Git,

**Skills:** Web Design, Scrum, Threat Detection, Threat Analysis, Access Control, Data Recovery, Incidence Response, Network Security, Vulnerability Assessment, Linux, Disaster Recovery Planning, French

**Related Experience**

**RIT Capstone Project “SrcML Web application”** [**https://github.com/Gs5570/srcML\_web-application.git**](https://github.com/Gs5570/srcML_web-application.git)

* Built client/server web application to offer a user-friendly interface of the research tool SrcML.
* Implemented user authentication schema to track user registration.
* Leveraged REST API calls to run SrcML processes in the back-end based on user input and return output in the front end.
* Implemented MongoDB to store files converted by ScrML.

**RIT course SWEN-610** **“E-store”** <https://angular-estore.netlify.app>

* Worked in a development team of four students to build a front-end web page for an online retailer.
* Created a design document to architect the web page according to the project needs.
* Utilized Trello to organize the software engineering process and assign tasks to team members.
* Implemented Agile framework in Software Development Life Cycle to incrementally work on each phase.
* Managed the project through Scrum to define our backlogs and sprints promptly.
* Implemented REST API calls to perform CRUD operations for the online retailer.
* Implemented Static code analysis with SonarQube to measure the quality of our code.

**Per Scholas Boot Camp April – August 2022**

**Software Engineer Trainee**

* Trained weekly in the design, development, and deployment of restful APIs using the MERN stack to create full-stack applications.
* Collaborated with other developers to improve and maintain code through testing and code refactoring.
* Implementation of Object-Oriented Programming (OOP) principles and Model View Controller (MVC) design patterns in code.
* Trained Weekly in building website layout/user interface using responsive HTML/CSS practices.
* Trained in the utilization of version control such as GIT to leverage pull requests during teamwork.

**Cognizant Technology Solution, Denver, CO Jan 2019 – Jan 2022**

**Lead Security Engineer Jun 2020 – Jan 2022**

* Conduct open-source intelligence (OSINT) collection manually using anomaly for threat intelligence to create reports for team awareness and rule creation.
* Acted as the subject matter Expert bridge between clients and Cognizant.
* Provided knowledge transfer presentation session to new L1 Analyst.
* Reviewed offenses worked on by New L1 Analysts and ensured they followed the Security Operation Procedures enacted.

**Information Security Analyst Jan 2019 – June 2020**

* Perform daily incidents Management, which includes incident detection and recording, Incident ownership, monitoring, tracking and communication, and resolving incidents within established service times for an average of 10 security incidents.
* Utilize threat intelligence tools such as Anomali and Cisco umbrella to gather IOC for security incident analysis and correlation.
* Suggest Vulnerability mitigation as the first line of defense against Cyber threats through network monitoring and analysis of security incidents for rule tuning.
* Provide daily monitoring recommended improvements based on events or incidents of apparent security breaches in areas including networks, applications, databases, systems, and endpoints.
* Recommend tuning suggestions for SIEM to reduce the rate of false positives and improve use cases.
* Experience with Security Information and Event Management (SIEM) such as Q-radar and Splunk.
* Utilize SNOW as a ticketing tool to escalate security incidents.