

Information Security Engineer Information Security Engineer Information Security Engineer - Synovus Bank Atlanta, GA Certified, results-driven, Information Security Engineer who has a range of experience from Security monitoring and investigation, vulnerability management, cloud security and understanding of various security compliance policies. Profound ability to effectively communicate, both orally and in writing, to various departments, agencies, and stakeholders. Identity and Access Management experience with detailed understanding of Active Directory and implementation of SSO, MFA etc with multiple frameworks. Implemented security controls while performing ongoing system maintenance to prevent, detect, analyze and respond to security incidents. Experienced and effective participant in hunt, computer network defense, real-time analysis and incident response activities, to include ability to reconstruct events from network, endpoint, and log data.

Work Experience Information Security Engineer Synovus Bank - Columbus, GA June 2017 to Present

- Review and assess risk to the environment by running vulnerability scans and remediating findings
- Deploy and setup Qualys for vulnerability management and compliance monitoring
- Ingestion of security logs and use cases development for the Security Operations Center
- Tuning various security tools to make sure it meets the required standards for the organization
- Interview business leaders, gathered requirements and built business use cases and essential sold solution to team ensuring acceptance from the top down
- Develop and document procedure and standard for the cloud security access for the organization
- Successfully federated various application using Okta for SSO and setup MFA
- Reviewing and configuring WAF changes using Akamai
- Deploy, setup, configure, manage, and maintain Splunk deployments to include clustering and high availability scenarios
- Collaborated with Network and IR Team to troubleshoot and remediate SOC
- Developed SOWs and POC for Client Integrations
- Research and advised on all matters relating to security vulnerabilities and threats to the organization
- Onboarding logs to Splunk and Qradar from various security tools
- Incident response and investigation using tools like Burp, Wireshark, Snort etc
- Proficient with Ariel Query Language and Splunk Query Language

Splunk Security Developer The Coca-Cola Company - Atlanta, GA January 2017 to June 2017

- Log forwarding into Splunk and creating custom dashboards from the data

Gathered requirement and developed reports, dashboards, and alerts using advanced searching
Analyzed security-based events using Splunk Building of Splunk lab environment for the organization
Data ingestion from different data sources to Splunk Configured dashboards to detect network and application anomalies
Maintained Splunk systems internal documentation, including SOP's and design documents Developed Splunk development environment with high availability and redundancy
Proficient with Regex and Splunk Query Language Created and installed Splunk applications
Troubleshoot deployment, bucket, and data ingestion issues in Splunk Information Security Analyst Norfolk Southern - Atlanta, GA August 2016 to December 2016
Monitored of the organizations network for security events to identify malicious activities and investigate
Gathered requirement, use cases and created rules for the SIEM Scanned statically and dynamically for applications vulnerability using HP Fortify Reviewed and tuned Email Gateway, Intrusion Detection and Intrusion Detection System (IPS/IDS) rules
Log forwarding into Splunk and creating custom dashboards from the data Security operations to research possible threats from system logs like IPS, IDS, firewalls IT Security Analyst Clayton County Water Authority - Stockbridge, GA March 2016 to August 2016
Responded to client needs by evaluating requests via telephone and ticketing system Participated in the deployment of devices to the whole organization
Worked with business stakeholders to gather requirement and improve systems
Documented technical issues and escalated incidents to the appropriate IT support level Worked with server backup for tape, disk, NAS, hard drive, FTP or REV drive etc
Troubleshooting server related problems including networking (wireless and LAN) Security operations around protecting customer PII and payment information.
Risk assessment and identity verification using manual and automated processes Coordinated the creation, modification, and removal of user accounts IT Analyst Clayton State University Technology Center - Morrow, GA July 2014 to March 2016
Coordinated virus protection software programs within departments and the assisted in the installation of software patches and upgrades
Troubleshoot access related issues for both student and staff Setup user awareness training for phishing campaigns and various security threats
Installed and troubleshoot of various OS to support the campus Worked with Active Directory to

provision access for student and staff members Education NIST September 2019 BSc. in Computer Science in Certifications and Trainings Clayton State University - Morrow, GA 2014 to 2017 Skills Siem, Network Security, Information Security, Cyber Security, Splunk Links <http://linkedin.com/in/olatundeawelega> Certifications/Licenses Security Guard

Name: Eric Jones

Email: clinechristine@example.org

Phone: 946-223-0594