***SUMMARY***

**Results-driven, security professional** offering 10+ years of experience in working with Cloud, SIEM, Unix/Linux, Cisco Firewalls. **Proficient** understanding of security frameworks and methodologies. **Proven** leader with excellent critical thinking, communication, and presentation skills. I excel at getting the job done in whether working in a self-motivated or team-based environment. **High aptitude** for leadership and learning with an **ability** to **adapt** to a fast – pace changing landscape. Looking to be an asset for your company/team.

***ACHIEVEMENTS***

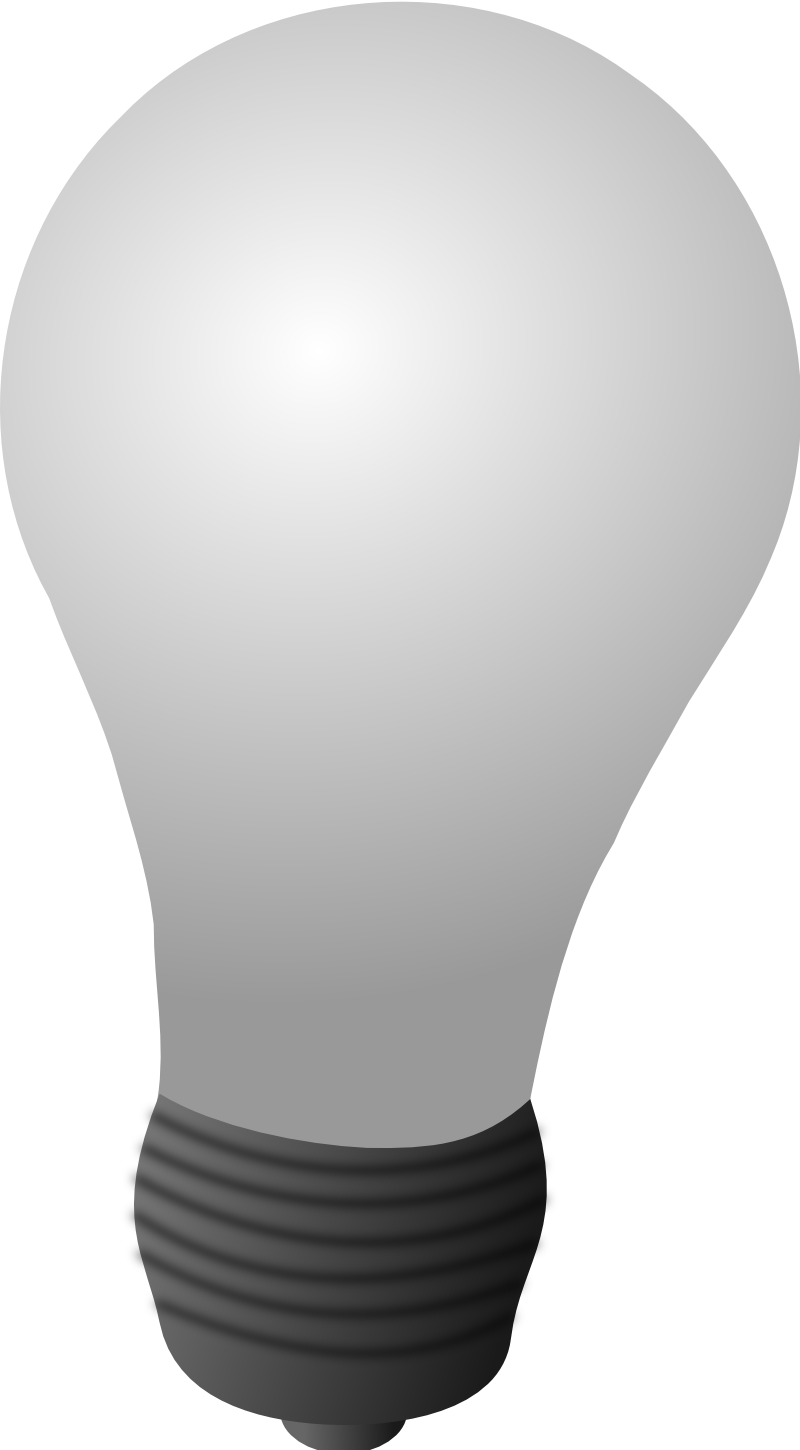
* Lead a Privilege Remote Access (PRA) project, that exceeded estimated deadlines by more than 3 months due to the sunset of Internet Explorer, while saving the company more than $1.1M in budgetary resources.

Spearheaded the launch of with the implementation of Cribl. This improved Network Performance of the data pipeline by 20% and allowed a 30% increase in tool adoption of critical informational systems



[This Photo](https://game-icons.net/lorc/originals/trophy.html) by Unknown Author is licensed under [CC BY](https://creativecommons.org/licenses/by/3.0/)

Led advanced training for a team of 15 cyber security analyst, decreasing ticket resolution and becoming proactive in resolving issues for business stakeholders.



***CERTIFICATIONS & SKILLS***

* Certified Information Security Manager (CISM)
* Business Leadership McKinsey Academy
* Splunk Certified Admin
* Coding/Scripting (PowerShell, BASH, Terraform)
* Strong Communication Skills
* Teamworking/Critical Thinking

***EXPERIENCE***

**Southern Company Services (Birmingham, AL.) Cyber Security Specialist | 5 / 2011 to present**

*Senior Engineer instrumental inleading projects in Operational Technology (OT) environments structuring high-level technical design, implementation, and Operational support of cybersecurity platforms.*

*RSA SECUREID* 

* Configure, maintain and lead the enterprise identity management infrastructure and solution
* Coordinate user provisioning and identity management processes
* Responsible for deploying bulk user accounts using PowerShell scripting
* Create policies that grant RBAC/LDAP access to the right members while harvesting a least privilege mindset
* Integrate new technology to deploy a layered security format around accessing infrastructure applications/hardware.
* Implemented content (dashboards/reports) to assist with quality assurance of user’s accounts and infrastructure
* Develop standard operation procedure (SOP) documentation and packages that trained junior members of the team in task to leverage the on-boarding/off-boarding of user accounts associated with access requirements

**SPLUNK** 

* Hands on experience in Incident Response Plans (IRP) to brief upper management on security incidents Investigation and response that happened in controlled environments
* Spearheaded the integration of Cribl Log Stream with Splunk environment to optimize log data flow
* Researched new and evolving threats and vulnerabilities with potential impact to the business
* Mastered onboarding of multiple data-sources to ingest security events into single or distributed instance.
* Extensive knowledge of a tier installation of the SIEM infrastructure deployment while automating using BASH on:
* Search-Head(s), Indexer(s), Universal/Heavy Forward(s)
* Cluster Master & Cluster Management
* Splunk ES Foundational Knowledge

**Security Projects Support Specialist**

* Lead specialist in the implementation of a Privilege Remote Access (PRA) project, that met 100% of deadlines and goals, with completion of saving more than $1.1M in budgetary resources.
* Consult the business on security best stakeholders in vulnerability management to minimize risk to the business
* Perform audits on security designs, gap analysis, and documentation of technology tools to reduce vulnerability
* Developed Standard Operating Procedures (SOP), policies and guidelines for advanced operational performance.
* Collaborate cross-functionally with Business partners for strategies, managed budgets and deployment plans that align with industry compliance and regulatory requirements.
* Mentored, hired, and trained JR. analyst that improved process efficiency in day-to-day activities

**ICCYBER, LLC Entrepreneur (Independent) Contractor | 5 / 2020 to present**

*Senior Engineer instrumental inleading projects in Operational Technology (OT) environments structuring high-level technical design, implementation, and Operational support of cybersecurity platforms. Senior analyst that functioned as a SME in the overall engineering and administration of a distributes clustered environment to coach and develop Splunk skills across Cybersecurity Operations.*

**AWS Cloud Engineer** 

* In depth knowledge of cloud services like Compute, Network Storage and Identity Access Management
* Hands on experience in deploying an IL6 Network architecture with Terraform that included VPC, Subnets Internet gateway NAT and routing tables
* Worked with CI/CD pipelines for code deployment by engaging different tools like GIT, Jenkins, and Hashicorp
* Automated processes for scanning STIG images into a closed GAP environment.
* Implemented Infrastructure as Code (IaC) tools such as Terraform to automate cloud-based deployments
* Managed Tenable.sc with Nessus scanners to identify risk/vulnerabilities with a closed gap infrastructure.

**End-Point Protection**

* Implemented endpoint agents using McAfee/Trellix to monitor HIPS (Host Intrusion Prevention) restricted traffic
* Design, implement, and document Symantec Endpoint Protection solution in controlled environments
* Root cause analysis in the Problem Management lifecycle
* Participate in escalated incident response that included triage and containment, incident reporting, and stakeholder management
* Identify and analyze minor problems to distinguish between relevant and irrelevant information to make logical decisions or provide solutions for next steps

***Education***

Virginia College of Birmingham, Alabama

* **BS in Network Management, Minor in Business** June/2008 – May/2010 (GPA: 3.2)
* **AS in Network Engineering,** August/2006 – May/2008 (GPA:3.0)

***Reference Available Upon Request***