Katressa Cooper, CISM

5204 Taylor Lane Bessemer, Alabama 35022

Phone: (205) 253-4183 ♦ Email: katressaw3000@yahoo.com

SUMMARY

Results-driven, self-motivated, goal-oriented security professional offering 10+ years of accomplished experience in working with Cloud, SIEM, Unix/Linux, Cisco Firewalls. Heighten **Leadership** skills while being **Proficient** high-level understanding of security frameworks and methodologies that involve Governance, Risk or Vulnerability management with compliance requirements. **Proven** leader with excellent critical thinking, communication, and presentation skills. **High aptitude** for leadership and learning with an **ability** to **adapt** to a fast – pace changing landscape.

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)

CERTIFICATIONS, SKILLS & CORE COMPETENCIES

- Certified Information Security Manager (CISM)
- Splunk Certified Admin
- AWS Certified Solutions Architect (in-view)
- Project Management
- Data Analytics
- Coding/Scripting (Python, BASH, Terraform)
- Application Security
- Risk Management
- Strong Communication Skills
- Teamworking/Critical Thinking

PROFESSIONAL EXPERIENCE

Southern Company Services (Birmingham, AL.) Senior OT 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.

Project Management

- Led 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.
- Coordinated projects that minimize risk of malicious activity for the business using awareness with data analytics, vulnerability, patch management of (CIS) Critical Information Systems for a controlled infrastructure.
- Collaborate cross-functionally with Business partners for strategies, managed budgets and deployment plans that align with industry compliance and regulatory requirements.

Identity, Access Management (IAM)

RSA SECUREID

- Serve as a SME on IAM, partnering with the business to identify systems for management access solutions.
- Lead operational and strategic planning of authentication tools and systems, ensuring the alignment with applications for integration.
- Created procedural documentation that trained junior members of the team in task to leverage the on-boarding/off-boarding of user accounts associated with access entitlements fir infrastructure availability.

SPLUNK

- Designed, deployed, and managed a dynamically scalable logging and monitoring platform for content development to capture baseline performance deviations and implement proactive monitoring and alerting.
- Perform ISSM responsibilities around threat hunting to identify system updates, continuous monitoring to evaluate exposure to potential threats and vulnerabilities.
- Mastered onboarding of multiple data-sources to ingest security events into single or distributed instance.

- Administered, implemented, configured, and provided management on a RHEL/Linux-based or Windows platform for Splunk components in a distributed deployment or single enterprise instance.

PROFESSIONAL EXPERIENCE (CONTINUED)

  - Search-Head(s)
  - Indexer(s)
  - Cluster Master & Cluster Management
  - Splunk ES Foundational Knowledge

Security Support Specialist

- Lead security incident triage in investigating alerts for monitored security devices.
- Implement firewall rules in Cisco FirePower and Panorama to improve security communication of devices in a segmented network.
- Developed Standard Operating Procedures (SOP), policies and guidelines for advanced operational performance.
- Identify vulnerabilities that apply to specific managed network components to ensure applications operate effectively while providing appropriate performance toward the CIA triad.
  - SIEM Logging & Monitoring Platform
  - Palo Alto, Cisco firewall and switches
  - Dell Servers with ESXi host and guest deployment
  - RSA Multi-factor authentication

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

- Deployed IL (Impact Level) compute infrastructure using Terraform IaC deployments to establish monitoring an alerting for applications deployed.
- Leverage a fully managed Gitlab and JFrog Artifactory repositories with compiled source code to integrate with Concourse, Jenkins CI/CD pipeline service.
- Automated processes for scanning STIG images into a closed GAP environment.
- Collaborated, evaluate, and identify cloud technology alternatives using hands-on proof of concepts (POC) with IaaS cloud products.
- Administered Utilize Tenable.sc with Nessus scanners to triage risk of identified vulnerabilities with a closed gap infrastructure.

SPLUNK

- Consulted on visualization of security events from data sources building relevant dashboards or alerts to the overall big picture of stakeholders' awareness.
- Performed investigations and root cause analysis of issues/problems with the infrastructure while providing recommendations to implement changes to optimize performance.
- Experience in working with structured data formats, JSON, XML and Syslog to enhance custom log parsing using RegEX or field extractions for data appearance to end-users
- Developed procedural documentation for data ingestion with numerous application that supported audit procedures and CMMC requirements.

REFERENCE AVAILABLE UPON REQUEST