ALIEU KAMARA

DETAILS

ADDRESS

Glen Burnie MD
United States

PHONE

(240) 478-4032

EMAIL

amaratech@outlook.com

LINKS

LinkedIn
https://www.linkedin.com/in/alieukamara/

SKILLS

EXECUTIVE LEADERSHIP ADVISORY

Data Analytics and
Business Intelligence

●●●●●

Client-Centric Needs Analysis
Cybsecurity Advisory

●●●●●

SELECTED SPEAKING

Hosted a Networking Submit and presented the Topic of Benefits of Cybsecurity to small business in Columbia Maryland.

-04-27 – Presented a topic on Digital Transformation: Thriving in the Digital Age of Digital at African Stake Holder Meetings in Maryland

●●●●●

SIEM

Splunk, Qradar, Graylog

●●●●●

TICKETING

ServiceNow & Remedy,
Phantom, XSOAR

●●●●●

EDR

CrowdStrike EDR, Carbon Black, Sentinel One Threat Intelligence: Threat connects, OSINT Analysis

●●●●●

AV

Wildfire, McAfee endpoint, Windows Defender ATP

●●●●●

PROFILE

Focused and skilled IT Security professional individual with over 10 years of experience in the Information Technology industry seeking a challenging and rewarding position as a Cybersecurity Leader with proficiency in cloud orchestration, security, Identity and access management, monitoring and event management, governance & compliance, application delivery, data protection, self-service, and analytics. Comfortable working both autonomously and as part of a larger team, with a proven record of driving projects forward, managing incidents, and producing service-focused solutions to technical faults. Previous roles include infrastructure development, support, and project management for a diverse range of businesses including international organizations, e-commerce, and Consulting Service companies.

PROJECTS

Ransomware Detection Engineering - Reviewing Ransomware process evaluation against WBG controls, recommending best practices. Reviewing the tactics, technology, and process view around the detection of ransomware and bad actors. Testing rules and mapping it to a Kill Chain and understanding WBG Visibility Development of OSINT Tool (Spider foot)- Gathering information collected from the public regarding a target, E-mail addresses, IP addresses, domains, phone numbers, usernames, etc. Setting up of the application and API's.

Playbook Development: Leading the development of PB and effectively applying a structural analytical approach to resolving Missing PB that was identified. Demonstrated Quality Control and accuracy throughout the PB creation by other team members.

Security Process & Vulnerability Management: Leading Zero trust initiatives and activities that address security Processes and reporting. Refining SOPs documentation for all our tools and creating a SNOW dashboard to improve tracking task visibility and reporting to senior management. Contributing valuable input to incident monitoring, and Tickets Reviews. Implementing a Ticket creation for Security Advisory Alerts and working to streamline our manual reporting through the use of Power BI which provides reporting visibility across our security.

PROFESSIONAL EXPERIENCE

Lead - Security Process & Vulnerability, National Institute of Health (Zero Trust)

Rockville Campus — March 2024 - Present

As a lead, I was involved with the coordination of Security Incidents, and assisting with implementation plans, procedures, and standards that are reviewed, supported, and deployed most effectively and efficiently and are consistent with overall risk management of the organization.

Key Achievements:

- Documented business processes and analyzed procedures to ensure alignment with changing business needs.
- Identify/recommend controls to effectively close IT Security requirements and process gaps, through the development of modularity automation and creating a reporting dashboard through Power BI and Service Now to provide visibility.
- Improving our security productivity level by 90% through continuous monitoring, refinement of analyses, and identification of opportunities for the security team
- Develop vulnerability and remediation progress reports as a component of the Program Management & Reporting suite of deliverables & reports.

NETWORK SKILLS

Palo Alto, Wireshark, tcpdump,

●●●●●

CLOUD

Microsoft Azure, AWS, Microsoft EOATP, IOC: Anomali

●●●●●

PROGRAMMING LANGUAGES

Basic understanding of Bash Scripting, JSON, and YAML Sandbox: Cuckoo Sandbox, Joesandbox

OTHER TOOLS

Fiddler, Spider foot, Cyber Threat Intelligence IOC processing, Axiom Akamai Kona Connectome

●●●●●

CORES SKILLS IN DEVELOPMENT

PYTHON

●●●●●

CLOUD SECURITY (MICROSOFT AZURE)

●●●●●

OVERVIEW OF COMPETENCIES

- Handled Cyber security incidents through the IR lifecycle as part of security operations.
- Investigated a wide range of incidents from phishing, vishing, scams, malware activity, ransomware, DDOS, and more.
- Experienced in IOC analysis by performing OSINT on IOCs respective to incidents.
- Involved in the development of SOC-related procedures.
- Collaborated with system owners and IT teams to ensure timely remediation of high-risk vulnerabilities.
- Identity & Access Management: AWS Organization, AWS IAM, AWS AD Connector, Active Directory, AWS Workspaces, AWS Secrets Manager, etc.
- Experience with Microsoft Cloud Application Security (CAS).
- Experience with Microsoft Azure and AWS.
- Data Loss prevention identifies files with sensitive data including PII, PHI, financial, and other data types stored by clients.

Key Responsibilities:

- Implement security tools across NCATS network environments to enhance security operations & management
- Collaborate with other ITRB Teams to address the resolutions of vulnerability and compliance deficiencies
- Provide guidance, recommendations, and support to NCATS ITRB teams in reviewing processes and procedures requiring security input
- Training on operation security processes and procedures
- Develop (Electronic/Digital) Dashboards that provide meaningful information and performance indicators of the security landscape of NCAT IT environments
- Support threat and incident response management and provide visibility and insight into information technology activities that could present operations, security, and business risks to NCATS IT network environments
- Coordinate with other ITRB teams to confirm accuracy, drive remediation of vulnerabilities, and ensure compliance of IT assets across NCATS networks
- Support the NCATS applications and operations team with vulnerability remediation and mitigation through education, guidance, and technical assistance.
- Prioritize identified vulnerabilities based on risk utilizing a variety of metrics, including the Common Vulnerability Scoring System (CVSS), tool risk identification and prioritization, risk assessments, and internal assessments.

Lead Cybersecurity Engineer (Purple Team Specialist), Wells Fargo

Virginia — October 2022 — Feb 2024

Key Achievements:

- Led initiatives for refining tools and processes, identifying vulnerabilities, and developing mitigation strategies.
- 90% in resolving ticket fatigue by Incident Response Analyst.
- Analyze and determine the intent, and operational and technical capabilities of threat actors. Identify new threat TTPs and signatures used by cyber threat actors.
- Analyze threat actors' intent and capabilities, recommending preventive controls.
- Identify and close security gaps, improving the organization's overall security posture.
- Review technical documentation for Purple Team and other teams improving process and SLA responses and recommending corrective actions for stakeholders.

Key Responsibilities:

- Rationalize, refine, and document existing infrastructure, environment, and systems to enable preparation for new projects.
- Work as part of the team to advise the blue team and red team (OSRT) to refine tools and processes, and then actively work with them to identify vulnerabilities, test defenses, and develop mitigation strategies.
- Lead initiatives including research, analysis, design, testing, and implementation of protection technologies for Wells Fargo.
- Provide security consulting on medium projects for internal clients to ensure conformity with Wells Fargo information, security policy, and standards.
- Collaborate and consult with peers, colleagues, and managers to resolve issues and achieve goals.
- Coordinate with the client on network monitoring alerts and remediation.
- Training and mentoring of Junior Analyst.

Sr. Cybersecurity Engineer – Detection & Response Team, Coupang

California — April 2020 – Sept 2022

Key Achievements:

- Reviewed and tuned signature sets for optimal event volume and minimal false positives.
- Periodically reassess the incident management process and revise as needed work with MSIR with threat hunting analysis, to provide visibility on IOCs, IPs/domains, host artifacts, and analysis. (Improve the threat hunting process).
- **SOC Infrastructure**: Overseeing the efforts of writing new security policies developing, engineering, and implementing solutions for security requirements. This process involves gathering and organizing technical information about an organization's critical security goals and needs, existing security products, and ongoing programs within CSOC.
- **Leading CSOC initiatives**: (SOC Monitoring and SOC Infrastructure) and activities that address potential or existing issues. Modification of Playbooks and creation of BTS dashboard to improve visibility. Grouping playbooks to make data more searchable by refining the search logic in BTS.
- **Level 3 Escalation**: Effectively and professionally manages escalations complaints taking appropriate follow-up actions. Responding to Escalations and maintaining security changes within CSOC support is a top priority for Coupang. Effectively managed Level 3 escalations, resolving 15% of submitted tickets.
- Review at least 90% of Critical and Major severity security event response cases every month and document findings on cases where analysis needs to be improved.

- Experienced with Active Directory and Group Policy Objects (GPO).
- AWS Security: AWS Security Hub, AWS Guard Duty, AWS Inspector, MFA, access key rotation, security groups and NACLs, S3 bucket policies, mitigating DDOS attacks, etc.

CERTIFICATIONS & PROFESSIONAL TRAINING

- Certificates in Advanced Diploma for IT Practitioners (System Support Networking)
- Certified Information Security Management Systems Auditor (ISO/IEC 27001:2005 Standard).
- CCNA1 – Networking Basics
- CCNA2 – Router and Routing Basics
- CCNA3 – Switching and intermediate Routing
- CCNA4 – Wan Technologies
- CCNS – Cisco Certified Network Security.
- Security + Certification
- Cisco telepresence Management Suite Certification (TMS) (Training) Windows 10 deployment (Training)
- SCCM (Training)
- Microsoft Advanced Threat Protection
- Amazon Developer Associate (AWS)

Key Responsibilities:

- Review Playbook, improvement and recommendation & Self-Assessment, and contact information (POC)
- Identify and validate the revised approach for recently created Use Case capabilities already in production to provide a visibility report for PB creation.
- Manage Microsoft Defender Antivirus and Windows Defender Firewall configurations across a large Windows-based environment.
- Responsible for vulnerability scanning and assessment programs, identifying and prioritizing security vulnerabilities across the organization's infrastructure.
- Development and maintaining standardized PB Operations pipelines for close coordination with other IT Team • Spearheaded the deployment and configuration of CrowdStrike Falcon for endpoint protection, achieving advanced threat detection and response capabilities.
- Implemented and managed vulnerability scanning tools to conduct regular scans and assessments.
- Periodically reassess the playbook management process and revise as needed.
- Establish performance indicators to track the Playbook management process.
- Worked on fine-tuning CrowdStrike policies and rules to optimize security coverage and reduce false positives.
- Experienced in all the phases of Incident Response and have been effectively involved in several critical Incidents. Analyze and determine the intent, and operational and technical capabilities of threat actors. Identify new threat TTPs and signatures used by cyber threat actors.
- Developed and maintained vulnerability management policies and procedures to align with industry best practices.
- Implemented and maintained Microsoft Defender Advanced Threat Protection (ATP) to enhance threat detection and response capabilities.
- Conducted vulnerability trend analysis to identify recurring issues and proactively address systemic weaknesses.
- Review containment and mitigation procedures for incidents.
- Conducted threat hunting and analysis using CrowdStrike's Threat Intelligence to proactively identify and mitigate potential security risks.
- Raise awareness of the SOC's services and help CSOC members correctly report incidents.
- Secure Infrastructure on AWS using IAM, KMS, API Gateway, Cloud Trail, MFA, VPC, Roles, Policies, Cloud Watch, Config, Trusted Security Groups, ACL.
- Perform system performance monitoring and tuning; participate in capacity planning and systems configuration.

Information Security Analyst (ISOC) (Tier III), WorldBank Group

Washington, D.C. May 2016 – March 2020

Key Achievements:

- Reduced threat intel attack surface by 65%, collaborating with external partners.
- Successfully reduced phishing email responses by 35%.
- Conducted detailed IR investigations and recommended solutions to reduce PII exposure risk.

Key Responsibilities:

- Monitor and analyze data using various security tools and data feed from various network devices (switches, firewalls, and router.
- Conduct Malware analysis and investigate behavioral characteristics of each incident utilizing IDS monitoring tools.
- Leveraged Risk Sense for vulnerability management with prioritized remediation, an exercise to exorcise exploitable finds appertained to exfiltration, RCE, and ransomware.
- Perform and participate in the incident handling process, incident discovery, analysis and verification, incident tracking, containment and recovery, incident response coordination, and notifications.
- Analyze and determine the intent, and operational and technical capabilities of threat actors. Identify new threat TTPs and signatures used by cyber threat actors.
- Collaborated with incident response teams to contain and eradicate threats identified by CrowdStrike, minimizing the impact of security incidents.
- Regularly reviewed CrowdStrike dashboards and reports to ensure the security posture of the organization's endpoints.
- Conducted investigations and responded to security alerts generated by Microsoft Defender ATP, effectively mitigating security incidents.
- Perform threat monitoring – monitor industry resources and observe new technical developments, intruder activities, and related trends to help identify threats to WBG environment.
- Utilized SIEM and other tools for monitoring security events, identifying threats, and conducting threat analysis.
- Recommended preventive, mitigating, and compensating controls to ensure the appropriate level of protection and adherence to the goals of overall information security strategy.
- Experience with endpoint monitoring solutions such as Microsoft Threat Defender, CrowdStrike, and Splunk technologies and applying them creatively and effectively.
- Assisted with review of policy, security alerts, guidance, regulations, and technical advances in IT Security Management.
- Utilized processes within the Security Assessment and Authorization environment such as system security categorization, development of security and contingency plans, security testing and evaluation, system accreditation, and continuous monitoring.
- Monitoring security events using a SIEM and other feeds, looking for significant events, and processing reports of unexpected network activity.
- Identify adversary's activities, including attribution, tactics, techniques, and campaigns, support ongoing tracking and remediation of security issues, ensuring that tickets are closed, and issues are addressed promptly.
- Detailed analysis, documentation, and a strong understanding of the attack vectors, persistence mechanisms, and detection avoidance tactics.

Technical Support Analyst (Tier II), **WorldBank Group**

Washington, D.C. Sept. 2014 – April 2016

Key Achievements:

- Project-managed Windows 7 to Windows 10 migration for 1100 endpoints.
- Transformed mobile device management, reducing workload by 75% and costs by 30%,
- using Intune.
- Configured and maintained audio-visual equipment, virtual meeting tools, and collaboration tools.

Key Responsibilities:

- Providing daily operational support and system administration for core network infrastructure and desktops.
- Providing excellent technical support and training to the Bank complex users, located in multiple buildings.
- Implement policies with various IT Teams to analyze information related to a client support service, identifying, and reporting on trends, anomalies, etc. Identify opportunities for improvements and escalate to management.
- Documents maintains, and enhances work processes and standards in the area, including documenting procedures for troubleshooting and incident resolution/solution.
- Implement and define system IT needs, current state, proposed future state, and transition roadmap(s).
- Configure and maintain audio-visual equipment including virtual meeting tools, Jabber, WebEx, and Polycom.
- Configured E360 Fiber link and Cisco any connect.
- Configured and re-imaged workstations with Windows Enterprise Desktop software.
- Configured Lotus Notes Client for users' email and ensured proper connectivity.
- Processes software purchases and deployment requests.
- Collaborates with Remedy and eService providers for issues or enhancements impacting ISAM activities.
- Monitors compliance and produces software licensing reports against deployed and takes corrective actions if needed.
- Analyses information related to a client support service, identifying, and reporting on trends, anomalies, etc. Identify opportunities for improvements and escalate to management.
- Escalation points for Directors and VIP's.
- Maintain a high level of security for all clients, minimize the attack surface, and hold regular audits.
- Client-facing, full-spectrum support, incident management & service management.
- Liaise and maintain working relationships with the Cheshire East IT department.
- Remote and desk-side technical support (2nd & 3rd line), Windows 7 to Windows 10.
- Use ADFS & AD to sync data between Office 365 and on-premises servers.
- Regular consultation with VIPs and stakeholders to review IT provision, purchasing, software, and licenses.

IT System Administrator, **2nd Chance College**

United Kingdom (UK) Aug. 2013 – April 2014

Key Achievements:

- Reviewed existing infrastructure, highlighted areas for improvement, and implemented new telephony systems.
- Managed Google Apps and intranet site for staff and students.
- Replace/upgrade all office PCs and equipment.
- Develop a disaster recovery plan.
- Migrate emails from onsite exchange server to Office 365.

Key Responsibilities:

- Installed Windows Server 2008 alongside various Microsoft software applications.
- Installed, and managed Trend Micro anti-virus on desktops using Windows server management to update definitions on the LAN enterprise environment.
- Conducted technical risk evaluation of hardware, software, and installed systems and networks.
- Implemented Helpdesk solutions to track inventory using Spiceworks.
- Implemented ICT Security Policies for various groups.
- Migrated user data from Google Apps administration to Windows server 2008.

IT & Business Support, Digibridge CIC

United Kingdom (UK) Nov 2012– March 2013

Key Achievements:

- Analyze business requirements and provide IT Infrastructure development plans.
- Products covered include Network, AD, Server 2008, SBS 2011, Windows 7 & 10.
- Researched and streamlined the Wake-UP LAN project with senior network managers to deploy within the company reducing network logon times for existing technologies and implementation for future growth.
- Installed and/or troubleshooted software and applications including transition to new equipment.
- Installed and configured XP operating systems.
- Performed upgrades to the network and troubleshoot associated network problems.
- Perform and participate in the incident handling process, incident discovery, analysis and verification, incident tracking, containment and recovery, incident response coordination, and notification.
- Assess threats, risks, and vulnerabilities from emerging security issues.

IT Analyst, Evershed LLP

United Kingdom (UK) Sept. 2011 – Oct. 2012

Key Achievements:

- Planned and designed the creation of company policies and procedures governing corporate security, email and internet usage, and access control to reduce incident response, improving the performance of key business applications.
- Providing reports to the IT security Manager monitoring internet usage across the IT Estate.
- Managed incident requests from start to completion, communicating with users, subject matter experts, and other stakeholders involved.
- Researched, and designed documentation on system architectures, and functional designs to provide recommendations for cross-project integration and support for regional office Infrastructure.
- Configured workstation security parameters to register encryption with PGP encryption.
- Conducted technical risk evaluation of hardware, software, and installed systems and networks.
- Implemented and installed the Skype project @ desktop video conferencing and providing training to users across the UK offices.
- Identified and responded to change management integration with the existing infrastructure across the IT estate.
- Implemented VLAN Configuration setup with technical Architect to design risk assessment procedures for international Offices across Europe.
- Devised an internal structure for technical support and documented all office procedures.

IT System Support, Leap Training Ltd

United Kingdom (UK) Sept. 2010 – Oct. 2011

Key Achievements:

- Infrastructure development for small businesses including SBS 2011, Server Essentials 2012 & 2016, Exchange, and Office 365, delivering optimized systems whilst reducing operating costs.
- Installed Windows XP/ Vista Operating system on PCs.
- Installed operating system updates and configuration, performing backups of data.
- Installed drivers for various peripherals.
- Implemented anti-virus protection on PCs.
- Revised policies for monitoring security vulnerabilities on the network.
- A compiled report highlighting the risk of virus protection and rudimentary remedial action.
- Managed user accounts: adding, deleting, creating, and modifying.
- Resolved connectivity problems relating to the Windows Operating System and the Internet.

EDUCATION

Master Certificate MSc Network Information Security and Management. Studies, Kingston University 2012

B.S., Computer Networking
London Metropolitan University 2010