**EMMANUEL APPIAH**

4eappiah@gmail.com

+1 571 575 5491

 Harvard Cir, Melbourne, Florida, 32905

 Professional Summary

Experienced Cybersecurity Professional with a demonstrated history of supporting the government and Private organizations. Skilled in installing, configuring, integrating, troubleshoot QRadar SIEM solution and other SIEM Solutions, Network Security and over 3 years’ experience in performing SOC monitoring, Intrusion Detection, Threat, and Malware Analysis and participating in Security Incident Response process until remediation. Strong Information Technology professional with Master of Science Degree in Systems Engineering and a Bachelor of Science in System Engineering. Self-motivated and goal-oriented cyber security professional, with demonstrated ability to handle complex responsibilities in a demanding environment. A team player with good written and verbal communication.

 CLEARANCE

* + - * **Secrete Clearance**

 Education

**08/2015 – 12/2017**

**Bachelor of Science, Systems Engineering.**

George Mason University, Fairfax, VA

Major: Systems Engineering, BS

**10/2018 – 07/2021**

**Master of Science, Systems Engineering.**

Florida Institute of Technology, Melbourne, FL

Major: Systems Engineering, MS

 CERTIFICATIONS

|  |  |
| --- | --- |
| * **CASP+ CE**

* **Security+ CE.**

 | * **Certified Information System Security Professional (CISSP)**

**(In progress)** |

 Skills

|  |  |  |
| --- | --- | --- |
| * Windows, Linux
* Critical Thinking
* Webservice (SOAP/REST)
* JIRA/Bitbucket/ServiceNow
* Security Control Assessment
* System Auditing and ATO package processing
 | * Python/Powershell
* User Behavior Analytics
* IDS/IPS
* Nessus,Rapid7 VM
* IBM Qradar SIEM
* Splunk
* Bitbucket
 | * AI Analytics & Correlation
* Malware & Phishing Analysis
* Incident Response/Cyber Threat Intelligence
* Data Loss Prevention (DLP)
* TCP / IP
* RMF, FISCAM, NIST, FISMA
* Enterprise Risk Assessment
 |

 Professional experience

**03/2022– Present IBM Qrader SIEM Engineer at Apria Healthcare, Melbourne FL**

* Expert knowledge of IBM Qradar SIEM
* Install & Configure IBM QRadar SIEM
* Tuning and troubleshooting QRadar to deliver optimal performance
* Technology escalation point for QRadar SIEM and underlying event collection components
* Implement and test custom parsers in QRadar SIEM
* Configure and tune SIEM platform to ensure optimal performance
* Provide expertise in event collection and parsing related to SIEM platform
* Assess existing SIEM platform and identify key system flaws and areas of improvement
* Perform annual assessment of SIEM configuration and custom content
* Develop detailed supporting documentation regarding technical projects (such as materials to support an architecture review board)
* Manage customer expectation and attend all mandatory review / regulatory discussions related to the specific project being delivered
* Help establish baseline and plan for improvement of a large enterprise deployment of QRadar SIEM and event collection platform
* Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks
* Operates with appreciable latitude in developing methodology and presenting solutions to problems
* Contributes to deliverables and performance metrics where applicable
* Experience in administration of operating systems (Linux and Windows)
* Experience with Windows Event Forwarding Service
* Ensure IBM QRadar SIEM is configured as per cyber security policies
* Analyze offenses/Incidents using IBM Qradar.

**10/2018 – 03/2022 Security Engineer (IBM QRadar) at Northrop Grumman, Melbourne, FL.**

* I worked as part of a security team responsible for protecting the company's IT assets
* Experienced with the traditional use of SIEM tools such as QRADAR but will also be able to advise Company staff SIEM plans with an eye toward virtualization
* Support all aspects of Company's Security Information and Event Management initiative
* Participate in the operation of QRADAR Security Information and Event Management systems to include QRADAR ESM, Logger appliances, Windows and Linux servers, network devices and backups
* Configure rules within QRADAR ESM to correlate events from various devices throughout the network and identify anomalies that require further investigation
* Participate in the design and implementation of QRADAR architecture upgrades and changes
* Establish plans to implement architecture changes
* Life-cycle management of the QRADAR platforms including coordination and planning of upgrades, new deployments, and maintaining current operational data flows
* Apply Configuration Management disciplines to maintain hardware/software revisions, QRADAR content, security patches, hardening, and documentation
* Develop content for a complex and growing QRADAR infrastructure
* This includes use cases for Dashboards, Active Channels, Reports, Rules, Filters, Trends, and Active Lists
* Provide optimization of data flow using aggregation, filters, etc
* Create periodic reports for management showing the health of the SIEM program
* Working closely with Company team to maintain security requirements for operation of
* Drive the development and the establishment, enhancement, and continual improvement of an integrated set of correlation rules, alerts, searches, reports, and responses
* Responding to day-to-day security requests relating to QRADAR operations
* Tunes QRADAR performance and event data quality to maximize QRADAR system efficiency
* Assists with analyst using QRADAR and other tools to detect and respond to IT security incidents
* Perform routine equipment checks and preventative maintenance
* Act as SME for all questions related to the QRADAR SIEM implementation
* Maintaining up to date documentation of designs/configurations
* Create shell and perl scripts to facilitate automated tasks
* Work with other Service Providers to support areas of common interest
* Working with software and hardware vendors
* On-call support may be required
* Perform other duties as assigned

**04/2015 – 09/2018 System Administrator at AWS Data Center at AWS, Manassas, VA.**

* Design infrastructure and automation improvements
* Provisioning of servers and environments
* Maintain and improve configuration management templates
* Monitor system performance and respond to alerts
* Take part in on-call rotation
* Support a team of developers and QA engineers
* Participate in software releases and patches
* Ensure compliance with security standards and practices
* Manage user access
* Keep current on relevant technologies; continually push the company and the team
* Leverage the best possible tools and resources
* Secure the operations and data of the applications against theft, loss and/or disasters
* Partner with external services and companies for seamless integration

**05/2014 – 04/2016 Cyber Security Analyst at G4S Secure Solutions, Manassas, VA.**

* Monitoring and safeguarding the log sources and security access
* Planning for disaster recovery in the event of any security breaches
* Monitor for attacks, intrusions and unusual, unauthorized, or illegal activity
* Performs moderately complex log reviews and forensic analysis to identify unauthorized or unacceptable access to data or systems
* Conduct security assessments, risk analysis and root cause analysis of security incidents
* Handling incidents escalated by the L1 team in 24x7 rotational shifts
* Use advanced analytics tools to determine emerging threat patterns and vulnerabilities
* Completing all tactical security operations tasks associated with this engagement.
* Analyses all the attacks and come up with remedial attack analysis
* Conduct detailed analysis of incidents and create reports and dashboards