**Cybersecurity Engineer**

**Name**: **SelamNigatu**

**Email**: **nigatuselam09@gmail.com**

**Contact**: **214-716-8712**

**Current Location**: **Wylie, TX**

**Professional Summary**

* Cyber Security Engineer with 4+ years of experience in implementation, administration, operation, and troubleshooting of enterprise data networks.
* Experienced IT Security Professional in IT Infrastructure, DLP, Vulnerability, Risk security, GRC, SOC Analyst, SIEM, Information Security, and Cyber Security.
* Manages security tools including DLP, SIEM, Vulnerability scanner, and ServiceNow Security Operation and Penetrations test.
* Experience in developing innovative security controls and processes to protect information Familiar with industry tools such as Encase Enterprise, Encase eDiscovery, Symantec Clearwell eDiscovery Platform, Discovery Attender, Splunk, Access Data’s ForensicToolkit, MS SQL 2005/2008, MS Visual Studio, VMWare, and SIFT Workstation.
* Experienced with Symantec DLP Policies (DLP templates) compliance andregulation standards such as SOX, PCI, and HIPAA
* Conducted assessments using Radiant logic VDS, OIM, RACF, MFA, SailPoint, ArcSight, Burp suite, Qualys, SiteMinder, Securonix (UEBA), and conducted MRA and Splunk.
* Integrated SAP data with ServiceNow using JavaScript API, and Web services, and created a table to capture the data.
* Engineered and deployed global Splunk SIEM solution and deployed global CarbonBlack Response EDR solution.
* Experienced in SAST and DAST applications using tools like Burp Suit and Check Marx. ∙ Worked with system owners to achieve FISMA compliance and Authorization to Operate
* Experienced in SAST and DAST applications using tools like Burp Suit and Check Marx Worked with system owners to achieve FISMA compliance and Authorization to Operate
* Utilise Splunk SIEM threat analyst in a managed service security operation centre (SOC), triaging cyber threats usingSplunk and various Cloud security tools.
* Conducted penetration tests and vulnerability assessments to identify and mitigate potential security risks. Experienced in managing and implementing various security controls, including firewalls, intrusion prevention systems, and access controls
* Proficient in creating and maintaining security policies, procedures, and guidelines.
* Developed and implemented security awareness and training programs for employees.
* Knowledgeable in regulatory compliance standards such as GDPR, CCPA, and NISPOM. Strong understanding of cloud security and experience securing cloud architectures.
* Worked with system owners to achieve FISMA compliance and Authorization to Operate
* (ATO) for systems based on guidance from the Federal Financial Institutions Examination Council (FFIEC) andNIST SP. ∙Collaborated with IT and business teams to assess security risks and develop risk management strategies.
* Experienced in incident response and handling security incidents, including data breaches and cyber-attacks. Stayed up to date with the latest security trends,technologies, and threats and implemented best practices accordingly
* Possessed strong analytical and problem-solving skills, with the ability to identify and address complex security issues.

**Technical Skills:**

|  |  |
| --- | --- |
| DLP | Websense, Symantec & McAfee |
| Endpoint Security | McAfee Suits (VSE, HIPS & HDLP), McAfee MOVE AV, Safe boot |
| SIEM | Splunk ES, McAfee, ArcSight, Qader, LogRhythmRSA Envision, ArcSight, Splunk security manager, IBM Qader |
| IPS/IDS | McAfee IPS, HP Tipping Point, Cisco IDS, SecureWorks IDS/IPS |
| Antivirus | McAfee virus scan Enterprise, Symantec, Endpoint Protection Suite |
| Cloud Security | AWS, Azure, OpenStack, Docker, Ansible, Chef, Ansible, CI/CD, Terraform |
| **MSS** | Vulnerability Assessment, Content Filter, Antispam, IDS/IPS Management |
| **Vulnerability Management Tools** | Foundstone, QualysGuard, Nessus, Nmap, Nexpose, Wireshark**SecurityTools:** Splunk ES, McAfee Vulnerability management solutions, Burp suite, OpenVAS, Nessus, Qualys, SolarWinds, Fore scout |
| **Programming Language** | SQL, R, Python, PowerShell |
| **Cyber Security** | STIX, TAXII, TRISTAR |
| **Operating Systems** | Microsoft Server, 2012,  2008R2, 2003, 2000 Advanced Server, Windows 10,7, Vista, XP, Netware, Red Hat, Unix  Solaris, VMWareESXi/vSphere v5.1, 5.5, and 6.5 |

**Professional Experience:**

**Role: Cyber Security Engineer July 2022 - Present**

**Client-AMEN RA SECURITY**

**Responsibilities**:

* Lead the implementation of IT Audit GRC Compliance workflow automation process in Cyber One using Salesforce.
* Plan, develop, and execute security data analytics using Business Intelligence tools (TibcoSpotfire, Extraction, Tableau) to support the IT Compliance team, Risk Management team, Information Security team, and all other functional units regarding IS security data.
* Manage third-party/vendor risk assessment oversight for security applications/tools, check for data security protection mechanisms (data-at-rest & data-in-transit), data retention, application authentication, access control, incident response, media protection, and regulatory and compliance standards the vendor adheres to.
* GathersecuritythreatintelligencefromvarioussecuritytoolssuchasSecurity InformationandEvent Management (SIEM) Systems, RSA Net witness, RSA e CAT, CyberArk, ActiveDirectory,IdentityManagement(IDM),Nexpose,and Infoblox
* Perform the review of the RSA Security SIEM log and Net Witness Security Event Log, analyse various logs from various appliances such as Cisco IDS, Proofpoint, Big-IP, Snort, and application firewalls, and provide a strong threat intelligence security data point forthe Information Security team.
* Work extensivelyon various streams of Identity and Access Management (IAM) compliancewithregardto account management, web access management (Citrix VDI), passwordmanagement,anduserprovisioning systems using LANDesk, CyberArk, and Active Directory (AD).
* Develop and monitor Risk Management central data repository to identify potential threats and vulnerabilities, track identified gaps, and recommend technical remediation.
* Assess and review periodically over 24 enterprise and security endpoint agents to evaluate and track the agent deployment process on all active endpoints and ensure swift agent
* deployment for non-compliant endpoints. ∙Be the subject matter expert and training facilitator for IS Security and Compliance data analyses, using data to drive theorganisation's Security, Risk, and Compliance exercises.
* Perform security monitoring, vulnerability management, risk management, and security incident response in identifying, coordinating, and remediating various identified vulnerabilities.
* Have knowledge of AWS cloud computing concepts and cloud infrastructure technologies services such as config, IAM, CloudWatch events, Guard Duty,CloudTrail, etc.
* Have strong knowledge and experience with IT Security and Compliance Tools such as Tripwire, Net Witness, Cylance, Beyond Trust, McAfee E Policy Orchestrator (McAfee epos), McAfee DLP, RSA MFA, RSA SIEM, CyberArk, and AirWatch MDM.
* Develop and maintain IT policies and procedures related to information security, ITrisk management, and ITcompliance in accordance with regulatory requirements (e.g., GDPR, HIPAA, PCI DSS). ∙Conduct periodic risk assessments of IT systems andapplications to identify potential vulnerabilities and recommend appropriatemitigation strategies.
* Work closely with IT and business teams to identify and evaluate new technologies and services, and ensure they meet the organisation's security and compliance requirements.
* Collaborate with internal and external auditors to provide evidence of IT compliance and address any identified issues.
* Maintain awareness of emerging threats and vulnerabilities, and ensure that the organisation's security controls are updated accordingly.
* Develop and deliver security awareness training programs to educate employees on information security best practices.

**Role: Cyber Security Engineer Dec 2019 – July 2022**

**Client: CARMEL LOGISTICS, LLC**

**Responsibilities**

* Develop and refine cybersecurity policies and procedures to protect the company's data and systems Monitor and assess security risks and vulnerabilities, and develop strategies to mitigate them Configure and manage security controls, such as firewalls and intrusion detection/prevention systems, to protect against cyber-attacks
* Investigate security incidents and breaches, determine their scope and cause, and develop and implement strategies to prevent similar incidents in the future.
* Manage user access to company systems and data, ensuring that only authorised personnel have access to sensitive information.
* Provide training and support to employees on cybersecurity best practices, such as how to identify and avoid phishing scams and other common cyber threats.
* Stay current with the latest cybersecurity threats and trends in the logistics industry, and incorporate new security measures and technologies as needed.
* Collaborate with other members of the IT team to ensure that cybersecurity practices are aligned with overall ITstrategies and goals
* Monitor and maintain the company's network and system infrastructure, including performing routine maintenance and upgrades as necessary.
* Continuously improve cybersecurity practices by staying up-to-date with the latest technologies and techniques, and by seeking out and implementing best practices from industry peers.
* Develop and maintain disaster recovery and business continuity plans in the event of a cybersecurity incident or other disaster.
* Conduct regular security assessments and audits to identify potential vulnerabilities and areas for improvement
* Implement and manage security information and event management (SIEM) systems to collect, analyse, and report on security-related dataWork with external auditors and assessors to ensure that the company is compliant with relevant regulations and industry standards (such as PCI DSS or HIPAA)
* Collaborate with third-party vendors and partners to ensure that their systems and processes meet the company's cybersecurity standards and requirements
* Conduct penetration testing and vulnerability assessments to identify potential security weaknesses in the company's systems and infrastructure.
* Manage and respond to security incidents, including coordinating with internal teams and external partners as needed to contain and resolve the incident.
* Monitor emerging cybersecurity threats and trends, and provide regular updates and recommendations to management on how to mitigate those threats.

**CERTIFICATIONS:**

* CompTIA Security+ ce Certification (Issued Sep 2022 · Expires Sep 2025)
* AWS Certified Solutions Architect – Associate (Issued Jun 2022 Expires June 2025) ∙
* Cisco Certified Network Associate Routing and Switching (CCNA)
* Microsoft Azure Security Technologies – 500