DANIELLE DEFEUGAING

Greenbelt, MD 20770
202-202-4029 - danielledefeugaing919@gmail.com

PROFESSIONAL SUMMARY

A results-driven security professional with over years of experience and focus on vendors onboarding process, vulnerability management, compliance, risk management, security assessment and authorization, security control management, assessment, and authorization, RTP management, continuous monitoring, and Risk Management Framework. Understanding of business unit needs, vendors selection as well as Vendors tiering and classification, Analyzing SOC reports and creating risk assessment report. Proven ability to lead and direct, solve problems creatively, and make strategic decisions in fast paced environments. Excellent with organizing, planning analytical and technical skills. Demonstrate teamwork with IT and business unit departments. US Citizen.

SKILLS

- Customer Communication
- Trend Analysis
- Time management.
- Attention to details.
- Microsoft 365
- HITRUST/ HITECH
- Fast Learner
- Analytical skills.
- Teamwork.
- Multitasking Abilities
- Dependable and Responsible

Work History

08/2019 to Current

Third-party Risk Management Analyst
Marathon Petroleum – San Antonio, TX

- Assists Operational Risk Management and Sr. Risk Analyst, Operations in maintaining effective and professional relationships with senior management, business and support areas, internal and external auditors, Federal and State regulators, and others dealt with in a professional capacity.
- Acts as Subject Matter Expert for Program questions from Business Units. Provides prompt follow-up and accurate information.
- Assist with various Third-Party Risk Management program initiatives working closely with the Third-Party Risk Management Leads
- Promote effective teamwork and manage the resolution of interpersonal issues. Support People Management related initiatives
- Identify opportunities for improving third party risk posture as well as third party risk management processes, including expanded monitoring.
- Assist the Team Lead in overseeing risk assessment and due diligence processes and ensure they are properly performed in selecting new third parties!
- Work with the Vendor Management Office and Head Strategic Sourcing & Vendor Management to formulate holistic strategy around key third parties.
- Develops competence by performing structured work assignments.

- Engage with the Third-Party Information Risk Managers (TPRM), in developing the Wholesale (CIB, AM and CB) and Firmwide Critical Supplier portfolio Book of Work.

02/2018 to 07/2019 **Senior third-party Risk Analyst**
MetLife, Citigroup – Greenbelt, MD

- Participate in suppliers' onboarding process with Business, Procurement, Privacy, and legal teams.
- Provide support to Business unit in scouting IT related vendors.
- Support Procurement with vendor due diligence activities, with inherent questionnaires.
- Review SLAs, RFPs, and Inherent questionnaires responses in support of vendors' categorization (Tier)
- Conduct risk assessments on assigned vendors, taking into consideration business needs and Data mapping.
- Review security related evidence such as SIG questionnaires responses, SOC reports, latest scans results and policies documentations to identify gaps in vendors' environment.
- Communicate with suppliers through VRM to discuss findings and possible treatment solutions.
- Review and update company risk register in support of weekly risk status reports.
- Develop Risk Assessment Reports {RAR} documents for upper management review.
- Conduct continuous monitoring of approved vendors in bit sight tool.
- Support Legal team in contract writing.
- Conduct contracts exit meetings prior to contract termination.
- Support internal and external audit review by gathering and making available all evidence associated in controls catalog.
- Partake in daily meetings with upper management.
- Review and update internal security documentation.

12/2016 to 12/2017 **Cybersecurity Analyst/ Compliance**
Universal Care Medical Group – WASHINGTON, DC

- Assisted in developing, reviewing, implementing and maintenance of policies, procedures, standards, and guidelines in accordance with applicable regulations including ISO 27001, NIST 800-53 Framework Controls, HIPAA, and PCI DSS
- Created security documentation and workflows to assist with incident response, audits, and vendor requirements.
- Lead training of new employees on Vendor Risk Assessment
- Acted as a Liaison between external auditors in conjunction with Audit support project.
- Helped Environment obtain and maintained regulatory compliance.

- Conducted internal controls review, identified gaps, and developed treatment solutions.
- Responded to clients' requests in relation to audit reports requests.
- Reviewed all company SOPs to ensure compliance.
- Supported environment TPRM processes.

11/2015 to 11/2016 **ISSO**
W.T SOLUTION – Norfolk, VA

- Prepared and reviewed Authorization to Operate (ATO) packages (SSP, RA, CMP, CP, DRP, IRP and PIA, E-Authentication, and POA&M) per NIST 800 guidelines in support of assigned systems.
- Conducted risk management framework activities in collaboration with Analysts, SO and AO.
- Provided support for security related FedRAMP compliance controls; and audit systems, services, and processes to verify adherence to company security policies and procedures.
- Conducted systems categorization, controls selection and implementation, following NIST guidelines.
- Supported systems assessments and audits processes, in collaboration with ATO process.
- Developed plan of action and milestones to track and remediate vulnerabilities.
- Conducted monthly security meetings to provide status reports on assigned systems.
- Researched and reviewed Vulnerability reports with Developers, System Admins, and Engineers to remediate Vulnerabilities identified from scans and create POA&M to track the remediation process per classification (Critical, High, Medium, and low)
- Maintained up-to-date knowledge of cyber threats by researching top vulnerability database website, National Vulnerability database, OWASP Top 10
- Supported ATO processes and conducted continuous monitoring of systems, following NIST 800-137.
- Conducted patch, change, scans, risk, and vulnerability managements activities to maintain CIA of information systems.
- Created, maintained, and reviewed policies and standards operational procedures in relation to company business needs.
- Conducted awareness training, and IR, DR, and CP tabletop tests.

EDUCATION

2013 **Bachelor of Science**: **Computer Science**
University of Buea Cameroon - Cameroon

CERTIFICATIONS

CompTIA Security+ Scrum Certificate Certified Information Systems Auditor (CISA)
SAFe Certification CAP (in progress)

TOOLS

- XACTA.

- TENABLE
- SLPUNK.
- QUALYS.
- SCOUT.
- VENMINDER
- JIRA AND SIG
- CYBERGRX
- SERVICE NOW