Worked as IT Analyst Worked as IT Analyst Worked as IT Analyst Des Plaines, IL 5 years of experience as Security Analyst. This include the Domains like Security Information and Event Management (SIEM), Log Management, Vulnerability Assessment, Identification of threats & remediation, Proxy and Network Security Authorized to work in the US for any employer Work Experience Worked as IT Analyst Tata Consultancy Services - Pune, India September 2014 to May 2017 Project 1 Details Organization : Tata Consultancy Services Ltd. Pune, India Customer : Diligenta (Aviva), UK Role : Network Security Analyst Tool : Network devices -firewall, router, routing protocols. SIEM LogRhythm and Qradar Vulnerability Scanner- Qualys Guard Team Size : 10 Period : Nov 2015 May 2017 Role and Responsibilities: Network Architecture and design review and approval based on defined security guidelines. Representing Security team in weekly CAB meetings to address any security concerns and provide inputs. Planned, evaluated, and implemented network security measures To review, approve or reject all network and firewall changes. Security Team is the mandate authority to approve/reject network changes. Analyze and define security requirements of network system Provide Security inputs on new project activities like New Application/tool implementation. Maximized the effectiveness of vulnerability scanning by using Qualys Guard. Responsible for specialized investigation and remediation in response to notifications using SIEM- Qradar. Working on SIEM migration from RSA Envision to LogRhythm. Project 2 Details ? Organization : Tata Consultancy Services Ltd. Pune, India ? Customer : Cargill, US ? Role : SIEM Administrator, SOC Analyst ? Tools : SIEM LogRhythm and QRadar, McAfee Web Gateway, Microsoft ISA ? Team Size : 10 ? Period : Sep 2014 to Oct 2015 Role and Responsibilities: Project involved security event monitoring, analysis, triage incident alerting and reporting using SIEM QRadar for 2800 Critical log sources. QRadar Administration which includes new log source integration, SIEM health check, fine tuning of correlation rules, access control and log source management. To prepare and present SIEM metrics in monthly meetings. Responsible to maintain availability for SIEM. To analyze daily offenses and take required remediation actions Monitoring of all endpoint devices such as servers, desktop and laptop (Anti-virus, Anti-Spam and filtering) through Symantec Endpoint Protection Analyze McAfee Web

Gateway End User's request and provide access. Security Analyst Zensar Technologies - Pune, India August 2011 to August 2014 Project Details ? Organization : Zensar Technologies Ltd. Pune, India ? Customer : Investec Private Bank, South Africa ? Role : System Engineer ? Tools : SIEM Symantec Security Information Manager(SSIM) Symantec Antivirus, Nmap ? Team Size : 10 ? Period : Aug 2011- Aug 2014 Role and Responsibilities: Contributed in Implementation and Configuration SSIM for Real Time Logging, Monitoring and Reporting Monitored customer networks using SIEM SSIM to identify and remediate security breaches. Investigate potential or actual security violations in an effort to identify issues and areas that require new security measures or policy changes. Troubleshooting and deep analysis of Security alerts. Configured Log Monitoring for Critical log sources. To identify and resolve agent communication issues. Prepare weekly and monthly alert analysis reports. Conduct vulnerability assessments using Nmap to evaluate attack vectors, identify system vulnerabilities and develop remediation plans and security procedures Education B.E. in Computer Technology Kavikulguru Institute of Technology and Science 2011 H.S.C. in PCM Group Vidyaniketan Jr. College 2007 Skills IBM Qradar (5 years), Network Security (5 years), Logrhythm SIEM (1 year), Firewalls and Proxy (2 years), Wireshark (Less than 1 year), DLP (1 year)

Name: Victor Brown

Email: mariecook@example.org

Phone: 323-660-4567x807