|  |  |
| --- | --- |
| Parth Khundiwala | +974 74094852 (Doha, Qatar)  +91-8956605443 (India)  [parthukhundiwala@gmail.com](mailto:parthukhundiwala@gmail.com)  Doha, Qatar  https://www.linkedin.com/in/parth-khundiwala-52641543/ |

**PROFILE**

Cybersecurity professional with 9+ years of managing diverse projects, leading teams with problem-solving and analytical capabilities, and ensuring Compliance with industry standards and regulations. Skilled in Risk Assessments, NIST-800, CIS, ITIL, and standards like PCI DSS, and ISO 27001. Proficient in Vulnerability Scanning, Log Management, and securing critical data with SIEM, IDS/IPS. Passionate about innovation, leading teams, and implementing effective Security Strategies to stay ahead of emerging threats.

Gears **KEY SKILLS**

* SIEM
* Vulnerability Management
* Policy & Procedures
* PCI DSS
* CIS/NIST
* AWS
* IT Security
* SOC Monitoring
* SANS
* IDS/IPS
* ISO 27001
* Security Audit
* Risk Monitoring
* ITIL
* Microsoft Azure Sentinel
* NIST
* Information Security
* Security Analysis
* Implement & Management
* Risk Register
* GRC
* Strategy
* Control Assessments
* Risk Identification
* Incident Response & Management
* CISA (pursuing)

**WORK EXPERIENCE**

**KBC Technologies | Contract Position - Atos LLC, Doha, Qatar – Senior Information Security Engineer July 2022 – December 2023**

* **Security Operations Centre (SOC):**
  + Monitor security events and incidents using the SIEM tool.
  + Identify and establish Key SOC metrics, such as SOC Key Performance Indicators (KPIs), Service Level Agreements (SLAs), etc., to measure the effectiveness and efficiency of the SOC.
  + Respond promptly to security incidents, conduct investigations, and implement corrective actions.
  + Advised team on security best practices and incident response procedures.
  + Oversaw the deployment and updates of security technologies.
  + Provide regular updates to management on Infrastructure security defining operational KPIs and metrics and building dashboards and reports.
    - **Use Case Management:** Perform Use Case Assessments, tracking false positives, customization, creation, fine-tuning, and testing to cover the Attack Surface
    - **Log Assessment:** Perform Log Analysis and Validations to ensure the received logs are valid. Troubleshoot issues with Log Sources or Systems with vendors, and report System defects.
* **Governance, Risk Management, and Compliance (GRC):**
  + Proven ability to establish effective governance frameworks, defining clear roles and responsibilities in cybersecurity management.
  + Ensure compliance with industry standards, regulations, and internal policies.
  + Participate in the development and enhancement of governance and risk management frameworks.
  + Manage to follow up, close, and report upon all department’s information security regulatory requirements, audits, nonconformity reports, compliance issues, and observations that arise during conducted internal and external assurance engagements.
  + Hands-on experience in strategic consultancy projects related to cybersecurity risk management, SOC consulting, and compliance with ISO/IEC standards, including ISO 27001, PCI DSS, NIST
  + Assess, evaluate, recommend, and implement IT Security controls to address key risks.
* **Cyber Risk Management:**
  + Develop and implement strategies to assess and mitigate cyber risks.
  + Conduct IT Security assessments regularly and take appropriate remedial actions.
  + Collaborate with cross-functional teams to comprehensively understand the organizational risk landscape.
* **Cyber Threat Intelligence (CTI):**
  + Research threat actor groups, malware, methods, and vulnerabilities.
  + Stay up to date on current cyber threats and vulnerabilities from different threat intelligence sources.
* **Vulnerability Management:**
  + Execute vulnerability assessments and prioritize and remediate identified vulnerabilities to enhance the overall security posture and collaborate with teams to address the security findings.

**QuinStreet Software India Pvt Ltd, Pune, India - Senior Information Security Engineer December 2021 – July 2022**

* Managed and administered Cortex XDR Detection, Vulnerability Management program using Rapid7 InsightVM
* Provided support and collaboration to the Compliance team for Internal and External Audits
* Strategized the deployment of Managed Security Service to integrate logs from Technologies with the LogRhythm SIEM tool.
* Document Security-related policies like Change Management Policy, Incident Response Policy, Remote Access Policy, etc.
* Worked with the Compliance team to support Risk Assessment Procedures
* Worked closely with the cross-functional teams to ensure and maintain the organization's Security Posture.

**ZS Associates, Pune, India - Senior Information Security Analyst - SOC Lead March 2017 – December 2021**

* Helped and mentored Tier2 & Tier3 analysts to tune and set up SIEM and Vulnerability Management Solutions
* Managed daily operations (use case development, complex integrations, parsers development, etc.) for Threat and Vulnerability Intelligence, Investigations, and Security Monitoring
* Preparation of reports and Present biweekly to both the CISO and other Senior Management Groups, providing comprehensive updates on the company's Security Posture, Incident Handling, Vulnerability Management
* Strategized the deployment of Managed Security Service to integrate logs from 10+ Technologies.
* Supported 60+ customer RFPs and helped multiple business units, like the Legal and Knowledge Management (KM) team.
* Collaborated with the Compliance team for the client, External, and Internal Audits - SOC2 Audit, Security Incident Response, Security Awareness and Training Policy, Audit Evidence
* Given extensive support and collaboration in readiness to implement ISO:27001 and PCI-DSS, Business Impact Assessment (BIA) - Business Continuity and Disaster Recovery program.
* Managed CrowdStrike and McAfee ePolicy Orchestrator and worked as Rapid7 InsightVM and Tenable SME
* Conducted Proof of Concept (POC) of new tools and technologies for the replacement of the infrastructure

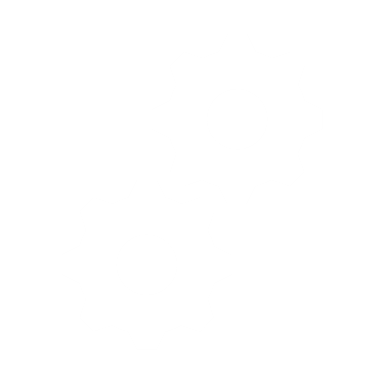
**Medline Industries India Pvt Ltd, Pune, India - IT Security Analyst August 2016 – March 2017**

**Systems Plus Technologies, Pune, India - Security Analyst - L1 May 2015 – August 2016**

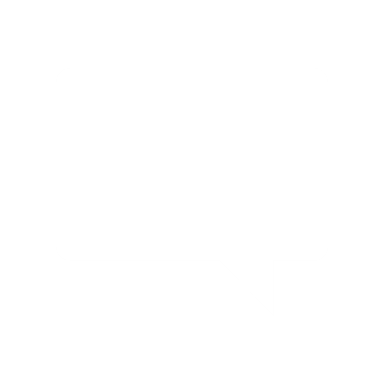
**Security Shells Infotech Pvt Ltd, Pune, India - Technical Support Engineer April 2014 – May 2015**

**EDUCATION**

* BE in Electronics and Communication Engineering - KNS Institute of Technology, Bangalore, India **June 2009 - July 2013**
* Diploma in Electronics and Communication Engineering – Bhagwan Mahavir Polytechnic, Surat, India **June 2006 - June 2009**

 **Certifications**

* EC-Council: Certified Ethical Hacking v9
* EC-Council: Certified Security Analyst v9
* CompTIA Security+
* AWS Certified Solutions Architect - Associate
* Splunk Enterprise Security
* Management & Governance Framework Security & Risk
* Certified Payment Security Practitioner (CPSP) (PCI-DSS)
* Enterprise Security Leadership: Managing Virtual Teams
* Rapid7 InsightVM Certified Administrator
* Coursera: Introduction to Cybersecurity for Business
* LogRhythm Platform Administrator (LRPA)
* Microsoft Certified: Azure Fundamentals
* Microsoft Certified: Security, Compliance, and Identity Fundamentals
* Certified Information Systems Auditor (CISA) (Pursuing)

 **Appreciations**

* Certificate of appreciation from CISO for extensive support and collaboration in developing the Application Security Governance Framework (ASGF)