NAZTEC®
INTERNATIONAL GROUP

Naztec Certified
Technical Skillset & Experience Guarantee
2023

Abdul Mateen

Security Solutions Consultant

abdulmsecops@gmail.com
Phone: 561-461-4959
LinkedIn: https://www.linkedin.com/in/shaikabdulm/

PROFILE SUMMARY

Experienced Security Solutions Consultant with over 10+ years of experience in Cyber Security seeking to acquire a challenging position in an organization, to offer solutions in security whilst protecting confidentiality, integrity and availability of information Assets along with safeguarding the enterprise against unauthorized access and misuse.

TECHNICAL SKILLS

SIEM Administration:	LogRhythm**,** Splunk, Q-Radar & ArcSight.
SOAR	IBM Resilience
Firewalls	Sonic Wall, Palo-Alto Networks, Juniper, Huawei USG & Fortinet.
Proxy	Blue Coat & Forcepoint
VA/PT	Accunetix, Metasploit, Nexpose & Nessus
Coding Languages	HTML & Python
Forensic Tools	Encase, Mandiant, AD Forensic Toolkit, San-dump.
Security Assessment	Netwitness, Security Analytics, Solera, Web Inspect, NMAP, Wireshark
EDR	FireEye & RSA.

EDUCATION & CERTIFICATIONS

Bachelor's Degree (B.Tech) in Information Technology | Jawaharlal Nehru Technological University Hyderabad, 2011

EC-Council:	Computer Hacking Forensics Investigator (CHFI)
	Certified Ethical Hacker (**CeH**).
HP:	Certified Advanced ArcSight Administrator
ISACA:	Certified Information Systems Auditor ***(CISA)***
LogRhythm:	Certified Security Analyst (**LRSA 305)**
	Certified Administrator (**LRPA 306**)

PROFESSIONAL TRAININGS

Cellebrite:	Certified Logical Operator (**CCLO**).
Cisco:	Cisco Certified Network Associate (**CCNA**).
EnCase:	Certified Examiner (**EnCE**).
IBM:	Certified Associate Analyst - Security QRadar SIEM.
Microsoft:	Certified Systems Engineer (**MCSE**).
Microsoft:	Certified IT Professional (**MCITP**).
SANS:	SEC 511: GIAC Continuous Monitoring & Security Operations (**GMON**).
	SEC 504: GIAC Certified Incident Handler (**GCIH**).
Splunk:	Fundamentals.

PROJECT SUMMARY

Naztec International Group
Role: *Security Consultant*
Client: Smart Poll Solutions – West Palm Beach, Florida **Nov 2022 - Present**

Responsibilities:

- Lead Security Consultant for SmartPoll project.
- Primary responsibilities include- aligning the Cyber Security controls to meet with the project charter.
- Leveraging internal tools to identify threat actors, victims, and potential targets.
- Working extensively with the Sales & Business Development departments to determine if any clients were subjected to spearhead phishing attacks and report clients.
- Proactively investigating online communities for phishing threats specifically targeting the IP.
- Identify / analyze security risks and propose mitigations and contingencies.
- Conducting organization-wide VA scanning and remediation processes.
- Stabilizing vulnerable systems by host hardening.
- Engaging with both the enterprise & customers in strategically modernizing and strengthening cybersecurity.
- Conducting reviews & reporting of Key Risk Indications (KRIs) associated with project to executive management and stakeholders.
- Providing inputs to modify existing intellectual property (IP) to minimize impact by the current threat landscape.
- Discover & mitigate false positives within data feeds to ensure continued development of security systems.
- Partner with internal teams to provide technology support in larger work engagements.
- Ensuring that all practices are followed in line with industry standards such as NIST.

Kafaat Business Solutions
Role: *Security Solutions Lead Consultant*
Client: National Information Center - SDAIA Riyadh **Nov 2018 - Aug 2022**

Responsibilities:

- Technical Lead for deploying & maintaining Security Operation Center Solutions & Tools.
- Oversaw the Configuration and tuning of SIEM system to collect and process relevant data from various sources.
- Led troubleshooting and resolving of issues related to the SIEM system's performance, availability, and functionality.
- Provided daily, weekly and monthly reporting for all EDR.
- Conducted audits and reviews of the SOC system's configuration and reports to ensure compliance with industry standards and regulations.
- Augmented SOC staff capability by continuously supporting with the implementation, maintenance, and continual improvement activities of EDR solution.
- Created Custom Collectors and Parsers for log sources which are not out-of-box supported by Vendor.
- Developed and implemented security rules, policies, dashboards, reports, and alerts based on the system's development life cycle (SDLC).
- Oversaw change management for SOC Administration activities like Patch upgrade onboarding log sources etc.
- Provided Break/Fix support on demand.
- Maintaining, restoring configuration/data backups based as per requirements.
- Overseeing if the SLA Requirements were met w.r.t Managed SOC services & Vendors.
- Recommended security improvements to ensure that technological decisions made are compliant with Security Architecture.
- Provided solutions to complex challenges on projects centered around security operations.
- Deploy & Evaluate POC of various vendor products on customer premises.

- Provided on-site, full-time support in a client environment.
- Responsible for team management & effective use of resources.

Technology Control Company
Role: *Level-3 SOC Administrator*
Client: National Information Center - SDAIA Riyadh **Sep 2015 - Nov 2018**

Responsibilities:

- Provided Tier-3 level support for Security Operations.
- Oversaw Cyber Kill Chain Process in SOC Team such as Events Monitoring, IR & Threat Intelligence.
- Ensured that the Security Operation Center (SOC) procedures and protocols were properly fulfilled by the team.
- Lead respondent for incidents where IR was needed.
- Leveraged various security technology & tools such as SIEM, AV, Firewalls, Intrusion Prevention, Packet Capture, DLP proxy etc. tools for escalated incidents.
- Provide root-cause analysis to support any escalated incidents.
- Handled end-to-end incident response investigations.
- Revised and strengthened the Security Operations Framework.
- Created and maintained Runbooks and Playbooks.
- Provided MITRE ATT&CK modelling inputs to be enriched within SOC Tools.
- Built tools & techniques to automate threat response tasks.
- Worked with stakeholders to improve security posture post investigations.
- Handled monthly QA review of incidents and service requests.
- Conducted risk analysis, impact analysis & dependencies on demand.
- Carried out – of the box threat hunting from various log sources.
- Ensured compliance, policy & procedures were followed to achieve the SOC's mission objectives.
- Coached and mentored junior team members with IR procedures.

Starlink Middle East - Riyadh **Feb 2015 - Aug 2015**
Role: *Information Security Consultant*

Responsibilities:
- Executed consulting projects.
- Worked on client engagements, supporting delivery and offering solutions expertise.
- Ensured client needs and obligations were met successfully by providing custom solutions & Implementation plans.
- Verified security controls to ensure protection of client systems.
- Develop best practices and security standards for the organization based on compliance models.
- Collaborate with client-side engineers to identify gaps & create custom use cases on Security solutions.
- Worked alongside clients to help them mitigate risk with the use of security monitoring & IR.
- Perform security audits and provide reports to clients.
- Develop and implement strategy for vulnerability Assessment & Management.
- Enhanced cyber awareness for clients.

Tata Consulting Services
Role: *Systems Engineer / SOC Analyst*
Client: Microsoft India - Hyderabad **Jun 2014 - Jan 2015**

Responsibilities:
- Conduct Level 2 triage of escalated Incidents.
- Perform cyber reconnaissance to illuminate a potential attack surface area.
- Advanced analysis of suspicious URLs, emails, network anomalies and binaries.

- Perform in-depth log analysis and reporting.
- Aided Level-1 Analysts with threat Hunting inputs during the active incidents.
- Updating each security related incident with incident ticket in the SOC moments sheets.
- Provided Identification of attacker tools, tactics, and procedures (TTPs).
- Provided IOC's, Counter Threat Database & Collective Intelligence to be fed in SOC Systems for Incident enrichment. Assist in the tuning of proxy policy, in-line malware tools based on threat feeds, trust and reputation data, incidents, or vulnerabilities.
- Analyzed software vulnerabilities provided workarounds or mitigation techniques & patch prioritization.
- Responsible for Application Whitelisting.
- Provided On Call support for Security Incidents as needed.
- Participated in the enhancement of process and technologies impacting the Cyber Defense Operations function.

Depository Trust & Clearing Corporation, DTCC - Chennai **Jul 2013 - Jun 2014**
Role: *Cyber Security Event Analyst*

Responsibilities:
- Provided first layer of defense; Responsible for quick detection of incidents via SIEM Tool.
- Responsibilities Included Monitoring, Analyzing & Assessing External & Internal Threats for DTCC Organizational Environment.
- Perform analysis and correlation of network traffic, OS and application-level events via security tools.
- Identified, Investigated and escalated potential security threats to senior SOC resources when needed.
- Investigated compromised hosts and reported the impact of discovered incidents.
- Utilized threat analysis tools to identify potential threats within DTCC Environment.
- Provided Actionable Intelligence from various sources on Existing & upcoming threats to various Tech & Tools Teams
- Prepared comprehensive Threat & Vulnerability Report for Senior Management on Latest Developments.
- Provided escalation and communication to Security Incident Response teams.
- Kept updated on current & ongoing changes of threat landscape.

E2-Labs Information Security Pvt. Ltd., - Hyderabad **Feb 2011 - Jun 2013**
Role: *Security Engineer*

Responsibilities:
- Performed VA scans & Lead Corrective Measures for clients.
- Conducted Audits on demand.
- Prepared and presented briefings on Security findings and actively participated with client’s day-to-day interactions.
- Developed & monitored network infrastructure, perimeter & system logs on demand basis.
- Participated in client’s incident handling processes such as incident discovery, analysis and verification, incident tracking, containment and recovery, incident response coordination and escalation.
- Forensically analyzed client’s systems and servers suspected to have possible indicators of compromise.
- Provided consultation and assessment on perceived security threats.
- Participated in legal / Law enforcement investigations requiring forensic reporting.
- Created and delivered effective presentations and sales tools for the sales team.
- Supported recruiting efforts of clients by identifying potential candidates and participating in interviews for personnel selection.
- Training members of teams in security solutions.

SunSys India IT Services - Hyderabad **Dec 2009 - Dec 2010**
Role: *Network & Systems Engineer*

Responsibilities:

- Deploy & provide Initial setup of equipment’s such as routers, switches, firewalls, access points, and voice communication platforms and audio/video solutions for client offices.
- Monitoring System health for outages/disruptions.
- Tuning FWs to ensure compliance at client’s premises.
- Ensuring availability of WAN Circuit, monitoring devices for no outages.
- Coordinated with ISPs vendors to resolve circuit outage issues.
- Monitor performance including monitoring link utilization, Packet loss, latency, errors and discards.
- Monitor and Generate health check point, Performance and capacity reports.
- Ensured appropriate performance tuning, preventive maintenance of internet and Wi-Fi troubleshooting as needed.
- Hardware and software installation and management.
- MS Windows & Linux OS setup, upgrades for client environment Devices such as workstations, BYOD’s, servers etc.
- Performance Management, User Account Management.
- VPN tunnel setup and troubleshoot as per client needs.
- General security patching and bug fixes.
- Ad hoc queue management.
- Handle day to day IT related query / issue in given timeline.
- Providing desktop support services to clients on demand.
- Assist end-users with network-related issues and provide timely support.