



SHARON DSOUZA

SUMMARY

Cybersecurity professional with 9+ years of experience across threat hunting, digital forensics, incident response, security monitoring and SIEM/EDR operations. Experienced in leading hypothesis-driven threat hunts, investigating adversary behavior, correlating endpoint and network telemetry, and translating technical findings into actionable detection and response improvements. Strong hands-on exposure to Microsoft Defender, CrowdStrike, Splunk, Microsoft Sentinel and forensic tooling, with a practical understanding of MITRE ATT&CK, detection engineering, incident investigation and threat-led security assessments. Seeking Security Threat Hunter, Threat Detection, DFIR, Incident Response or Cyber Defense opportunities in the UAE and international markets.

EXPERIENCE

April 2024 - Current

Security Threat Hunter - Team Lead Accenture Pvt Ltd | Mumbai, India

- Led proactive, hypothesis-driven threat-hunting engagements for global enterprise clients focusing on advanced adversary behaviors.
- Designed and executed behavior-based hunting strategies utilizing EDR and SIEM telemetry to identify stealthy threats.
- Conducted deep-dive investigations into suspicious endpoints and network activities, validating findings to enhance incident response effectiveness.

June 2022 - April 2024

Senior Cyber Security Associate Ankura Consulting | Mumbai, India

- Conducted in-depth forensic analysis of security incidents, preserving digital evidence to identify root causes and inform preventive measures.
- Collaborated with MDR team to analyze network traffic, review security alerts, and investigate anomalies, enhancing threat assessment using SIEM and endpoint detection tools.

December 2021 - June 2022

Senior Cyber Security Analyst Network Intelligence India | Mumbai, India

- Oversaw network operations, utilizing specialized security instruments to analyze and detect potential threats and vulnerabilities.
- Conducted initial triage, declared incidents, created incident cases, gathered evidence, tracked, and updated incident status.

January 2021 - December 2021

Solution Architect Inspira-Enterprise Pvt Ltd. | Mumbai, India

- Designed and implemented security information and event management (SIEM) solutions using Azure Sentinel, customizing configurations to address client requirements and enhance security posture.

September 2019 - February 2020

Cyber Security Consultant PricewaterhouseCoopers (PWC) | Mumbai, India

- Collaborated on Cloud Investigations, Memory Forensics, Mobile Forensics, and Email Investigations to support case resolutions.

March 2017 - September 2019

Cyber Forensic Analyst Specialist Advisory and Intervention Group | Mumbai, India

- Conducted investigations into communication patterns, analyzed email headers, and created narrative frameworks to illustrate communication timelines and patterns.

📍 India | Open to work in UAE

📞 +91 9987265119

✉️ sharonndsouzaa@gmail.com

SKILLS

- **Threat Hunting**
- **Incident Response**
- **Endpoint Detection and Incident Response:** Defender, Morphisec, Rapid7, Nessus, CrowdStrike, Carbon Black
- **SIEM Tools:** Splunk, Azure Sentinel, ArcSight, Obsidian
- **Cyber Forensics Tools:** Nuix, Encase, FTK, Autopsy, Volatility

EDUCATION

January 2016

Master's | Information Technology
University Department of
Information Technology, Santacruz
GPA: 4.33 / 7

January 2014

Bachelor's | Information
Technology
ICLES Motilal Jhunjhunwala
College, Vashi
GPA: 4.77 / 7

CERTIFICATIONS

- CHFI - EC-Council
- AZ 900 - Microsoft
- CIFR (Cyber Investigation and Forensic Response) - Accenture Certification