WORK EXPERIENCE

CYBER SECURITY ANALYST

MINDTREE LTD • April 2021 - Present

- Worked on an average of 23 Azure Sentinel (SIEM) incidents per week with 9% True Positive rate and 39% False Positive rate
- Reduced a total of 384 false positive Sentinel incidents (~190 manual hours) by automation/ recommendations
- Automated different security use cases using playbooks and SOAR
- Performed end to end root cause analysis for every incident by effectively using EDR, ATP and MCAS tools
- Created SOPs for several malware use cases

SOFTWARE DEVELOPER

RACETRACK.AI • Oct 2020 - Apr 2021

- Developed, maintained & deployed chatbots for multiple clients in BFSI & Real Estate sectors
- Handled entire backend of multiple chatbots simultaneously, while working on Python, RASA, NLU, ML, Falcon,APIs, MongoDB, Gunicorn & Docker

PROJECT ENGINEER

WIPRO LTD • Oct 2017 - Aug 2019

- Monitored & remediated malware incidents on client-side SIEM application
- Updated SOPs for use cases and provided recommendations to reduce false detections
- Acquired analytical & collaborative skills while working in a geographically distributed team

EDUCATION

BMS COLLEGE OF ENGINEERING

Bachelor of Engineering (ECE), 2013- 2017 8.15 GPA

EXPERT PRE- UNIVERSITY COLLEGE

Pre-University (Science), 2011- 2013 96 %

AWARDS AND RECOGNITION

1. SPOT-ON- HATS OFF	Nov 2021
2. SPOT ON - A-TEAM	Dec 2021
3. SPOT ON - MASTERMIND	Apr 2022

Ranjan Khyadad

CYBER SECURITY ANALYST

3.5+ years in Cybersecurity with a focus on Security Operations- Incident response, Malware analysis and Forensics Investigation.

☎ +91-8147545560

📍 Bengaluru

✉ ranjankhyadad@gmail.com

CORE SKILL SETS

CyberSecurity
SIEM tools- Azure Sentinel, Splunk
EDR- Microsoft Defender, MDATP
Cloud Security- MCAS
DLP- ForcePoint DLP
Hacking OS- Kali Linux, TAILS

Networking:
DNS, DC, DHCP, RDP, Cisco, Palo Alto, Zscaler, Checkpoint

Programming:
Python, Flask, Django