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
- Performed end to end root cause analysis for every incident by effectively using EDR, ATP and MCAS tools
- Data loss prevention: Addressed an average of 175 incidents per day among all data channels. Reduced 1025 false positives per month
- Automated different security use cases using playbooks and SOAR
- Created SOPs for several malware use cases
- Collaborated with other IT teams to detect vulnerabilities and fix them on time
- Maintained active certifications and followed current security news, trends and best practices
- Created and analyzed daily reports in Sentinel

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

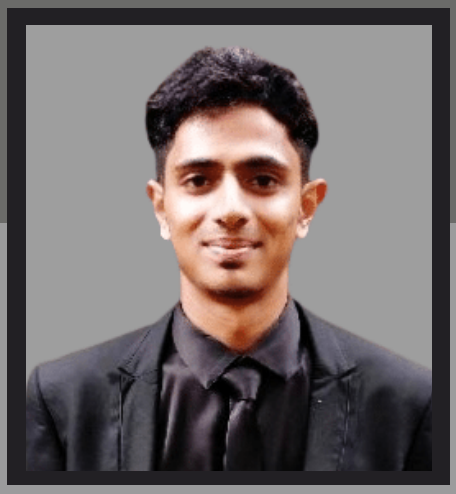
Bachelor of Engineering (ECE), 2013- 2017 8.15 GPA

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



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