Pooja Mewada

CYBER SECURiTY ANALYST
Ahmedabad, Gujarat

(+91) 8320086664 | poojamewada511@gmail.com | Pooja-Mewada

Summary

Detail-oriented and results-driven Security Analyst with a strong foundation in computer science and expertise in threat analysis, cyber protection, risk management and SOC analysis. Eager to apply my technical skills and hands-on experience in mitigating complex cyber threats, ensuring regulatory compliance, and continuously learning to adapt to new challenges. Seeking a challenging position where I can contribute effectively to a collaborative and forwardthinking cyber team.

Education

M.E. in Cyber Security — ***CPI 9.17 / 10***
GTU-GRADUATE SCHOOL OF ENGiNEERiNG AND TECHNOLOGY — *Ahmedabad, IN*
GUJARAT TECHNOLOGiCAL UNiVERSiTY — *Aug. 2021 - Jun. 2023*

B.E. in Computer Engineering — ***CGPA 8.89 / 10***
GOVERNMENT ENGINEERING COLLEGE – GANDHINAGAR — Gandhinagar, IN
GUJARAT TECHNOLOGiCAL UNiVERSiTY — Aug. 2018 - Jun. 2021

Diploma in Compute Engineering — ***CGPA 8.63 / 10***
R.C. TECHNICAL INSTITUE — Ahmedabad, IN
GUJARAT TECHNOLOGiCAL UNiVERSiTY — Jul. 2015 - Jun. 2018

Work Experience

Eventus Security — ***Ahmedabad, IN***
ASSOCiATE CYBER SECURiTY ANALYST — *August 2023 - Present*

- Provide timely client updates and address security incident queries.
- Investigate incidents using Trend Micro (Apex One, XDR) and CrowdStrike.
- Analyze network traffic and logs via SIEM tools (Cyberal, ESDL). • Collaborate on risk reporting, RCA, and mitigation strategies.

Adani Transmission Ltd. — *Ahmedabad, IN*
CYBERSECURiTY INTERN — *August 2022- November 2022*

- Interned in a NOC, monitoring network performance using SolarWinds.
- Analyzed logs to identify and troubleshoot network issues.
- Performed daily security checks to ensure compliance and integrity. • Contributed to network management and issue resolution in a team environment.

Academic Projects

Enhanced Approach for Kernel Level Security using Intrusion Detection System *Ahmedabad, IN.*

M.E. DiSSERTATiON

- Designed a kernel-level IDS to detect unauthorized access and system modifications by monitoring system calls, providing enhanced security and visibility over malicious activities

Certification

- SOC Certifications

  SOC Level 1, SOC Level 2, The Fundamentals of SOC, Trend Campus SOC Fundamentals
- Networking Certifications

  Networking Essentials, Network Defense Essentials, Fundamentals of Networking Security
- Vendor Certifications

  Fast Track Program (Fortinet), Palo Alto, Cisco
- Practical Experience: TryHackMe

Technical Skills

- Hands-on experience on Tools: Trend micro tools , SolarWinds ,CrowdStrike, SOAR ticketing tool, Service Now
- Other Tools: Wazuh, Splunk , Snort , Burp suite , Nessus , Wireshark
- Incident response and management
- Log analysis
- Threat Intelligence
- Network Security
- Mail Investigation
- Security Operations Center (SOC) workflows, including threat detection, triage, and escalation procedures
- Knowledge of risk and compliance frameworks such as NIST, ISO 27001,HIPPA and GDPR

Languages

- English
- Gujarati
- Hindi