

Darshan Chauhan

+91 8238973356



devchauhan2950@gmail.com



Security Analyst

Ahmedabad



www.linkedin.com/in/darshan-chauhan-156874257



ABOUT ME

Experienced SOC Analyst skilled in the oversight, analysis, and response to cybersecurity incidents. Proficient in the use of advanced security tools, interpreting log data, and collaborating with cross-functional teams. Capable of proactively identifying and addressing security risks to safeguard the integrity of organizational information systems.

PROFESSIONAL EXPERIENCE

Eventus Security | 20th November 2023 - Present

Security Analyst

- Monitored and analyzed security alerts using Trend Micro products (Vision One, XDR, MDR, Apex One, SOAR) and SIEM tools to identify and respond to incidents in real-time.
- Conducted in-depth investigations of security events, assessed impact, and executed actions for containment, eradication, and recovery.
- Reduced false positives by fine-tuning detection logic and implementing whitelisting for trusted paths, enhancing alert accuracy and response efficiency.
- Analyzed logs from IDS, firewalls, and security appliances, leveraging OSINT tools for threat verification and IOC extraction.
- Prepared daily, weekly, and monthly reports to track incidents and enhance client security posture, ensuring SLA compliance.
- Managed and maintained EDR/XDR services, monitored infrastructure health, and implemented allow/block actions on IOCs based on investigation outcomes.
- Worked in a 24x7 rotational shift, handling escalations, participating in client meetings, and collaborating with cross-functional teams to improve detection logic and security processes.

TECHNICAL SKILLS

- Log Analysis
- Firewall and Intrusion Detection
- Malware Analysis
- Experience in handling critical cyber alerts
- Conducting Threat Vulnerability and Risk Assessments
- Email Analysis
- Networking : Routing & Switching

CERTIFICATIONS

- Attack IQ Certified Foundation of Operationalizing MITRE ATT&CK
- Attack IQ Certified Foundation of Purple Teaming
- Trend Micro Products Certification
- TryHackMe: SOC Level 1

EDUCATION

Master of Science in Network Security | 2022-2024

Gujarat University, Ahmedabad

Bachelor of Commerce | 2018-2021

Gujarat University, Ahmedabad

WORKED ON TOOLS

- EDR, XDR, Log Inspector
- Trend Micro Apex One
- Trend Micro Cloud One
- OSINT Tools
- Vulnerability Scanning Tool
- Network Sniffing Tool
- Splunk