Pavan Sharma

Bharuch, Gujarat, India
pavansharma0603@gmail.com — +91 9662627746
LinkedIn: pavansharmacybersecurity

Objective

To work for an organization that offers opportunities to improve my skills and knowledge, enabling growth in alignment with the organization's objectives. I aim to contribute significantly to the security domain while enhancing my expertise in cybersecurity, incident response, and threat mitigation.

Technical Skills

Security Tools: Trend Micro Vision One, Trend Micro Apex Central, Trend Micro Apex One, Trend Micro Deep Security (Modules: Anti-Malware, Web Reputation, Intrusion Prevention System, Firewall, Log Inspection, Integrity Monitoring, Application Control, Anti-Bot), Trend Micro Cloud App Security, XDR & Email Security.
SIEM Tools: IBM QRadar, Cyberal.
Third-party Tools: IpVoid, URL Void, VirusTotal, Abuse IP DB, TrendMicro Reputation Check.
SOAR Tools: Sporact.
Networking: DNS, DHCP, AD, Email Server, Firewall, DMZ, IDS, IPS.
Protocols: TCP/IP.
Incident Response: Incident Investigation, Root Cause Analysis (RCA), Phishing Mail Processing.
Malware Analysis: Basic Malware Analysis, Threat Mitigation.
Operating Systems: Windows, Linux.
Others: XDR, Data Loss Prevention, Cyber Kill Chain, CIA Triad, AAA.

Certifications

- CompTIA Pentest+
- SOC Level 1 Learning Path (TryHackMe)
- Certified Ethical Hacker (Practical)
- Red Hat Linux
- Cyber Security Virtual Internship at AICTE
- Trend Micro Certifications: Apex Central for Administrators, Cloud One Workload Security Fundamentals, On-Premises Technical Essentials, Vision One Fundamentals, Deep Security for Administrators

Professional Experience

Security Engineer (SOC Analyst) **Protechmanize**
July 27, 2024 – Present *Thane, Maharashtra, India*

- Managed and responded to security alerts using Trend Micro Deep Security (modules like Anti-Malware, Web Reputation, Intrusion Prevention, Firewall, Integrity Monitoring, etc.) across a network of clients.
- Worked on P1, P2, P3, P4 cases, prioritizing critical incidents based on severity and impact, ensuring timely resolution according to SLA guidelines.
- Analyzed real-time network traffic logs from IDS and firewalls through SIEM tools.
- Conducted incident investigations, providing actionable insights for mitigation.
- Collaborated with clients and internal teams to design and implement security solutions.
- Monitored and responded to threats in a 24/7 rotational shift schedule.
- Worked with the Incident Response Team for root cause analysis (RCA) of incidents.
- Monitored security incidents for clients across multiple sectors (Finance, Healthcare, IT, etc.), ensuring timely detection and mitigation of threats.
- Collaborated with SOC teams to improve response time and threat detection rates.

Security Analyst **Eventus Security**
October 2023 – July 2024 *Ahmedabad, Gujarat, India*

- Monitored and analyzed security alerts for over 100 clients across various industries including healthcare, finance, education, and IT.
- Utilized Trend Micro Deep Security and Trend Micro Vision One for effective threat detection and response.
- Managed and prioritized P1, P2, P3, P4 cases, providing timely responses based on the criticality of the incident.
- Investigated and provided recommendations for threats based on severity levels.
- Conducted phishing mail investigations and collaborated with the Incident Response Team for RCA.
- Prepared weekly, monthly, and quarterly reports for clients on security status.

Network Engineer Intern **Geo Designs & Research Pvt. Ltd.**
February 2023 – April 2023 *Vadodara, Gujarat, India*

- Assisted in maintaining router and switch configurations, ensuring network availability and performance.
- Collaborated with the team to support network infrastructure.
- Documented network configurations and changes.
- Gained knowledge of basic network devices, OSI layers, and TCP/IP protocols.

Education

Bachelor of Engineering (B.E.), Information Technology Shri S'ad Vidya Mandal Institute of Technology
September 2020 – June 2023 *CGPA: 8.37*

Diploma in Information Technology **Parul University**
April 2017 – April 2020 *CGPA: 9.65*

Languages

- English: Proficient
- Hindi: Native
- Gujarati: Native

Projects

Security Monitoring and Response for 100+ Clients

- Monitored security incidents for clients across multiple sectors (Finance, Healthcare, IT, etc.), ensuring timely detection and mitigation of threats.
- Collaborated with SOC teams to improve response time and threat detection rates.