NAVEEN PACHANGI

SOC Analyst L2 | Security Operations | Threat Hunting | Incident Response

📍 Pune, India | 📞+91 7204231882 | 📧naveenpachangi666@gmail.com
🔗LinkedIn: www.linkedin.com/in/naveenpachangi6

PROFESSIONAL SUMMARY

Results-driven **SOC Analyst with 4+ years of experience** in Security Operations, incident response, threat hunting and log analysis across multi-tenant environments. Skilled in analyzing complex security alerts, performing root-cause investigations, improving detection logic, and coaching SOC teams. Experienced in SIEM/EDR technologies, threat intelligence, and MITRE ATT&CK-based investigation and detection engineering. Proven ability to reduce false positives, strengthen SOC maturity and drive high-impact security outcomes.

CORE SKILLS & EXPERTISE

- **Security Monitoring & Incident Response**
- **Threat Hunting & Use Case Development**
- **False Positive Reduction & Rule Fine-tuning**
- **Endpoint & Network Security Analysis**
- **Log Analysis (Windows Events, Sysmon, Firewall, Proxy, Email Security)**
- **MITRE ATT&CK Framework & IOC Analysis**
- **Leadership & SOC Support**, Mentoring Interns
- **Documentation & Customer Communication**

TOOLS & TECHNOLOGIES

- **SIEM:** Elastic SIEM, Splunk, Azure Sentinel (Basics)
- **EDR:** CrowdStrike, Windows Defender, Trend Micro Apex One / Apex Central
- **Network:** Fortigate Firewall, Palo Alto (Traffic/Threat Logs), VPN, Proxy (Zscaler)
- **Vulnerability:** Qualys, SSL certificate management
- **Email & Cloud:** O365 Security, CloudTrail basics
- **Threat Intel:** OSINT, AbuseIPDB, VirusTotal, AnyRun, Hybrid Analysis
- **Supporting Tools:** Wireshark, Sysinternals, Procmon, AD, Sysmon logs

---

CERTIFICATIONS & TRAINING

- **CEH – Certified Ethical Hacker (EC-Council)**
- **Mandiant Practical Threat Hunting Certification**
- **Fortinet NSE 1, NSE 2 & NSE 3 Certifications**

ACHIEVEMENTS & RECOGNITION

- Honored with the **Airtel ACE Award by Management for outstanding performance, operational excellence and significant contribution to SOC operations.**
- Recognized organization-wide with appreciation message from leadership for **managing critical customers, leading Pune SOC team, and training interns** simultaneously with dedication and excellence.
- Received **multiple Kudos and client appreciation** for onsite visits, troubleshooting major issues, and delivering impactful security training.
- Acknowledged for **enhancing SOC operational efficiency** through proactive threat hunting and use-case improvements.
- Awarded excellence recognition for **mentoring interns and building SOC team skill capability**.

PROFESSIONAL EXPERIENCE

Deputy Manager – SOC Analyst L2

Bharti Airtel Ltd | Nov 2023 – Present | Pune

- Lead investigation and response for security incidents across multi-tenant environments involving SIEM, EDR, Firewall, O365, and endpoint telemetry.
- Reduced SOC alert noise and **improved true positive accuracy** by performing rule fine-tuning and false positive reduction initiatives.
- **Improved investigation efficiency & response time (MTTD/MTTR)** by enhancing alert playbooks and data enrichment.
- Developed **MITRE ATT&CK mapped detection use cases** for brute force, PowerShell encoded commands, credential dumping, C2 callbacks, and lateral movement attempts.
- Conducted deep-dive analysis of **4624/4625 brute force**, suspicious PowerShell, LSASS access, encoded commands, and EDR process tree investigations.
- Led multiple major incident investigations including **account compromise and malware threat containment**, coordinating isolation, IOC blocking, and forensic evidence collection.
- Improved SOC maturity by enhancing monitoring coverage, tuning noisy detections, optimizing pipelines, and documenting investigation playbooks.
- Mentored SOC interns and analysts through technical knowledge sharing and review of investigation quality.
- Collaborated with cross-functional IT & risk teams to implement preventive controls, defense hardening, MFA enablement, and access security improvements.

Security Operations Center Analyst

Melange Systems Pvt Ltd | Sep 2021 – Aug 2023

- Monitored and analyzed security alerts including Antivirus, proxy, EDR, and firewall traffic to identify cyber threats.
- Performed vulnerability assessment using Qualys and supported remediation tracking.
- Investigated endpoint and network-based threat alerts, conducted escalation and RCA reporting.
- Participated in threat hunting activities to proactively identify potential attacks.
- Managed SSL certificates and performed periodic security posture checks.

- Collaborated with senior analysts and acquired hands-on IR exposure through assessments and shadow investigations.

KEY SECURITY INCIDENTS HANDLED

- **Brute-force authentication attack leading to account compromise:** Detected abnormal spike in 4625 failures followed by 4624 success; performed IP reputation checks, isolated impacted endpoint, reset credentials, enforced MFA, blocked malicious IOC at firewall, and prevented further lateral movement.
- **Suspicious PowerShell Base64-encoded execution via Outlook process chain:** Analyzed EDR process tree, identified malicious payload execution attempts, isolated endpoint, collected forensic artifacts, and recommended additional PowerShell execution restrictions.
- **Malware execution and endpoint compromise event:** Contained infection using EDR quarantine, performed signature-based and behavioral scans, collected persistence artifacts, eliminated scheduled tasks / registry modifications, and restored secure operational state.
- **Threat hunting initiative identifying unauthorized remote access attempts:** Conducted hypothesis-based hunting using SIEM queries across login patterns, lateral movement behaviors and privilege escalation; contributed to creation of new MITRE-aligned detection logic and dashboarding.

PERSONAL DETAILS

- Languages: English, Hindi, Kannada and Marathi
- Current Location: Pune, India
- Willing to Relocate: Yes

SIGNATURE

Signature: Naveen Pachangi

Date: 05/12/2025

Place: Pune, India
