SATYAJEET SINGH PATEL

SECURITY ENGINEER | SIEM ADMINISTRATION | EDR/XDR | VULNERABILITY MANAGEMENT

📧 receive.satyajeet@gmail.com | 📞 +91-7906085790 | 🌍 Sonbhadra, India
Linkedin

SUMMARY

Results-driven Security Engineer with 7+ years of experience in Security Operations Center (SOC), SIEM engineering, EDR/XDR monitoring, vulnerability management, incident response, and OT/ICS cybersecurity. Skilled in QRadar, Splunk, CrowdStrike, Microsoft Defender ATP, Rapid7, and Zscaler technologies. Proven expertise in threat hunting, log correlation, malware analysis, phishing investigation, and security monitoring across enterprise environments. Adept at reducing false positives, automating security workflows, and improving incident response efficiency.

CORE COMPETENCIES

- SIEM Engineering: IBM QRadar, Splunk, Perchybana
- EDR/XDR Security: CrowdStrike, Microsoft Defender ATP, Cisco AMP, RedCloak, Taegis, McAfee
- Threat Hunting & Incident Response
- Vulnerability Management & Risk Assessment
- Malware Analysis & IOC Enrichment
- Firewall & Network Security
- Zscaler Administration & DNS Security
- OT/ICS Security Monitoring
- Security Log Analysis & Correlation
- Security Operations Center (SOC)
- Cloud Security Fundamentals (Azure Security Center)
- Scripting: Bash, PowerShell
- Windows & Linux Administration

PROFESSIONAL EXPERIENCE

L2 Security Engineer, Norsk Hydro — Jaipur, India **June 2022 - Present**

- Monitored, analyzed, and responded to threats using EDR (CrowdStrike, Windows Defender ATP, RedCloak, McAfee, SEP) and SIEM tools (QRadar, Splunk).
- Investigated phishing incidents, triaged alerts, and coordinated remediation across email and endpoint platforms.
- Deployed and maintained log sources, created parsing rules, event mappings, and maintained SIEM health.
- Managed Zscaler proxy configurations, firewall policies, and DNS monitoring (OpenDNS).
- Handled OT and ICS security systems including Claroty CTD & SRA for industrial environments.
- Led vulnerability management and patching initiatives using Rapid7 and Windows Defender.
- Documented incidents and coordinated with global SOC teams for escalations.

Key Achievements

- Successfully migrated enterprise security tooling across 1200+ devices with minimal operational downtime.
- Improved threat visibility and incident detection through SIEM optimization and log source enhancement.

Reduced weak password vulnerabilities remediation backlog by 90%.

Senior Security Engineer, SecurView Systems Pvt. Ltd. — Pune, India **July 2019 - June 2022**

- Implemented and optimized SIEM use cases, event correlation rules, and alert workflows.
- Conducted vulnerability assessments using Nmap, Nessus, Burp Suite, and Kali Linux.
- Performed phishing investigations and endpoint threat analysis across enterprise environments.
- Automated security log ingestion pipelines to improve SOC operational efficiency.
- Investigated indicators of compromise (IOCs) using threat intelligence platforms including Cyware and Anomali.
- Performed malware analysis and security event triaging for critical incidents.
- Coordinated with infrastructure and security teams for remediation and containment activities.

Key Achievements

- Reduced incident investigation time through automation and enhanced SIEM rule tuning.
- Improved SOC operational efficiency by minimizing repetitive manual analysis tasks.
- Received client and organizational appreciation for high-impact security operations support.

EDUCATION

Post Graduate Diploma in IT Infrastructure & System Security (PG-DITISS) **Aug 2018 – Feb 2019**
CDAC Acts, Pune

B.Tech in Computer Science & Engineering **2013 – 2017**
Sir Chhotu Ram Institute of Engineering and Technology, Meerut

---

TECHNICAL SKILLS

- Security Information & Event Management (SIEM):QRadar, Splunk, Perchybana
- EDR/XDR Platforms: CrowdStrike, Microsoft Defender ATP, Cisco AMP, McAfee, Taegis
- Vulnerability Management: Rapid7 InsightVM, Nessus, Nmap, Burp Suite
- Network & Security Tools: Palo Alto, Fortigate, Zscaler, OpenDNS, Wireshark
- Threat Intelligence Platforms: Cyware, Anomali, Claroty CTD
- Operating Systems & Platforms: Windows, Linux, Azure Security Center
- Scripting: Bash, PowerShell

CERTIFICATIONS

- ✅ Certified Ethical Hacker (CEH)
- ✅ Zscaler Zero Trust Associate
- ✅ Zscaler Delivery Specialist
- ✅ Claroty Implementation Engineer (CIE 401)
- ✅ Claroty Cybersecurity Analyst (CCA 601)
- ✅ Malware Analysis Skill Path (LetsDefend)

PROJECTS & ACHIEVEMENTS

- Reduced weak password vulnerabilities remediated up to 90%.
- Led successful migration of Security tool across 1200+ devices with minimal downtime.
- Designed automated vulnerability scan reports integrated with ticketing system.
- Recognized by organizations for outstanding contributions to cybersecurity operations.