

PRADEEP GURJAR

Sikar, Rajasthan, India | +91 7877688211 | pgurjarsec@gmail.com
[linkedin.com/in/pgurjarsec](https://www.linkedin.com/in/pgurjarsec) | github.com/pgurjarsec | pradeepgurjar.tech

PROFESSIONAL SUMMARY

B.Tech CSE (Cyber Security) student and Certified SOC Expert with hands-on experience in SIEM-based log analysis, alert triage, and incident documentation. Practical exposure to cloud security (Azure Sentinel, Microsoft Defender for Office 365, Microsoft Entra ID), endpoint security (CrowdStrike EDR, phishing analysis), and vulnerability assessment. Microsoft Azure Fundamentals (AZ-900) certified. Seeking a SOC L1 Analyst role to apply strong fundamentals in threat monitoring, alert triage, and incident response.

TECHNICAL SKILLS

- SOC Operations: SOC monitoring, alert triage and escalation, true/false positive classification, log analysis, event correlation, threat detection, incident documentation
- SIEM Tools: Splunk Enterprise, Microsoft Sentinel (Azure Sentinel)
- Endpoint and Network: CrowdStrike EDR, phishing email analysis, vulnerability assessment, network scanning (Nmap), Wireshark
- Cloud and Identity: Microsoft Defender for Office 365, Microsoft Entra ID, MFA, Conditional Access, IAM, Microsoft 365 Security
- Container Security: Kubernetes Security Posture Management (KSPM), Kubernetes manifest hardening (CIS Benchmark)
- Operating Systems: Windows Server, Linux
- Programming: Python (PyYAML, MongoDB)

EXPERIENCE

SOC Analyst Training Program | SIEM XPERT

Apr 2026 – Sep 2026

- Practiced real-time SOC alert monitoring and triage in a simulated SIEM environment using Splunk Enterprise and Microsoft Sentinel, classifying true positives, false positives and benign activity.
- Performed log analysis, event correlation and incident documentation across endpoint and network sources following standard SOC escalation procedures.

Cloud Infrastructure and Security Intern | Celebal Technologies, Jaipur

Jun 2025 – Aug 2025

- Supported configuration and monitoring of Azure Sentinel for centralized log ingestion, alerting and security event correlation across cloud workloads.
- Administered Microsoft Defender for Office 365, Multi-Factor Authentication (MFA) and Conditional Access policies to strengthen email and identity security.
- Gained hands-on exposure to Microsoft Entra ID and Microsoft 365 security administration through daily configuration and troubleshooting tasks.

Cyber Security Intern | Eximius Tech Innovations Pvt. Ltd.

Jun 2024 – Jul 2024

- Analyzed reported phishing emails and investigated CrowdStrike EDR alerts and tickets to identify indicators of compromise (IOCs).
- Performed vulnerability assessments and network scanning across internal assets to identify security gaps and support remediation recommendations.

PROJECTS

KubeGuard: Kubernetes Security Assessment Tool | Personal Project

2026

- Built a Kubernetes manifest scanner using Python and PyYAML that evaluates manifests against CIS Kubernetes Benchmark, NSA and CISA hardening guidelines.
- Detects privileged containers, host namespace sharing, root escalation and missing resource limits.
- Integrated MongoDB for scan history logging and built on-demand PDF vulnerability assessment reporting.

EDUCATION

B.Tech, Computer Science Engineering (Cyber Security) | Sobhasaria Group of Institutions, Sikar (BTU) | 2023 – 2027 | CGPA: 8.17/10.0

Higher Secondary (PCM) | Gyandev Public School, Sikar (RBSE) | 2023 | 85.20%

CERTIFICATIONS

- Certified SOC Expert, SIEM XPERT (Cert. No. SOCAPR26031, Sep 2026)
- Microsoft Certified: Azure Fundamentals (AZ-900)
- Google Cybersecurity Professional Certificate

LANGUAGES

English (Advanced), Hindi (Advanced)