BHARAT PATEL VELARAM

✉ bharat8511patel@gmail.com| 📞 8511850044 | https://www.linkedin.com/in/bharat-patel-3b1822223

Summary

Diligent cybersecurity professional with hands-on SOC experience and specialization in FortiSIEM and FortiSOAR integrations. Experienced in log collection, parser/tuning, detection rule creation, incident triage, and automation using custom scripts. Strong practical knowledge of network security devices, endpoint protection, identity services, and PAM solutions. Comfortable working with cross-vendor environments and building integrations to ingest, normalize, and enrich security telemetry.

CORE COMPETENCIES

- SOC Operations, Log Analysis & Threat Hunting
- Security Information & Event Management (FortiSIEM)
- Security Orchestration & Automation (FortiSOAR)
- Incident Detection, Triage & Response
- Firewall & Network Security (Fortinet, Palo Alto, Cisco, Sophos)
- Endpoint & Email Security (Trend Vision One, SentinelOne, Sophos Central, Netskope)
- Privileged Access Management (PAM) Solutions
- Active Directory Integration & Hardening
- ManageEngine Endpoint Central Administration
- Python Scripting for Log Collection & Automation
- Custom API Integration (Netskope, SentinelOne, ManageEngine, Sophos)
- Linux & Windows Server Administration
- Network Protocols: TCP/IP, DNS, DHCP, NAT, VLANs
- Cloud & Hybrid Log Integration

Experience

Security Analyst — TechOwl Infosec ***(Nov 2024 – Present)***

- Working in SOC operations focusing on FortiSIEM and FortiSOAR integration and automation.
- Integrated multiple security solutions including firewalls, switches, Active Directory, Trend Vision One, PAM solutions, ManageEngine, Netskope, SentinelOne, and Sophos Central into FortiSIEM.
- Developed and deployed custom log collection scripts (Python) for Netskope, SentinelOne, ManageEngine, and Sophos Central.
- Automated FortiSOAR workflows for enrichment, ticketing, and IOC correlation using APIs.

Network Engineer — Cyber Hospitality **(Apr 2024 – Sep 2024)**

- Configured and managed gateways, switches, and wireless devices across multiple properties.
- Monitored network health and coordinated with SOC for security events and incidents.

SOC & VAPT — Tech Defence Labs(Intern) **(Jan 2024 – Mar 2024)**

- Assisted SOC workflows, performed vulnerability scanning, and contributed to threat hunting exercises using Nessus, BurpSuite, Metasploit, and Wireshark.
- Worked on CTF challenges to validate detection logic and response playbooks.

Lab Technician — Parul University (Intern) **(May 2022 – Nov 2022)**

- Maintained Windows lab environment, installed and deployed antivirus across domain-joined systems and performed routine troubleshooting.

Skills

SIEM / SOAR: FortiSIEM, FortiSOAR, Splunk (basic)
Security Tools: Nessus, BurpSuite, Nmap, Metasploit, Wireshark, Trend Micro (Trend Vision)
Log & Parsing: Syslog, CEF, LEEF, JSON logs, regex for parsing, field mapping, event normalization
Scripting & Automation: Python (API integration, data parsing, batching), shell scripting
Networking / Systems: TCP/IP, DNS, DHCP, NAT, routing, Windows, Linux
Identity & Access: Active Directory, PAM solution basics, LDAP integrations
Soft skills: Communication, teamwork, problem solving, time management

Education

Bachelors in computer science and engineering (**cybersecurity specialization**) 2020-2024
Parul university Vadodara, Gujarat

Certificates

- Certified in cybersecurity by ISC2
- Google Cloud Cybersecurity Certificate
- Introduction of Cybersecurity by Cisco.
- Fortinet Certified Fundamentals in Cybersecurity by Fortinet.
- NSE1: Information Security Awareness (by FORTINET)
- NSE2: The Evolution of Cybersecurity (by FORTINET)
- FCF - Introduction to the Threat Landscape 2.0
- The Cybersecurity Threat Landscape
- Azure fundamentals by Microsoft
- Cybersecurity Job Simulation by MasterCard