SHUBHAM SHARMA

SOC Analyst | SIEM & Detection Engineering | Threat Hunting | Cloud Security

Delhi, India | shu6h4m@gmail.com | +91 8953322535 | LinkedIn

PROFESSIONAL SUMMARY

SOC Analyst with hands-on experience across SIEM engineering, detection engineering, threat hunting, endpoint and network security, and cloud log monitoring. At Mobisec Technologies, designs and deploys Wazuh-based SOC environments from architecture through production readiness, including endpoint onboarding, multi-source log collection, custom rules, decoders, correlation logic, alert tuning, vulnerability detection, TheHive integration and network security monitoring. Onboarded AWS cloud servers, collected logs from multiple sources and developed detection rules for observed cloud security events. Also deployed IBM QRadar, configured the QRadar Connect agent, onboarded endpoint logs and analysed security events. Previously at NodeSec Technology, handled GTB Technologies DLP operations, endpoint monitoring and DLP alert investigation, worked with SentinelOne EDR, and gained exposure to Forescout NAC and CyberArk PAM. Experienced with Windows/Linux telemetry, Sysmon and attack-vector-based detection across Active Directory, endpoint security, web, backup and VPN environments.

WORK EXPERIENCE

SOC Analyst — Apr 2026 – Present

Mobisec Technologies

- Owned the end-to-end creation of a Wazuh-based SOC platform, from architecture and deployment through production readiness, monitoring and operational tuning.
- Designed production SOC architectures, onboarded clients and implemented secure endpoint/log onboarding workflows.
- Onboarded AWS cloud servers and integrated logs from multiple cloud/server sources into centralized monitoring; validated ingestion and event visibility.
- Developed cloud-focused detection rules from available telemetry to identify suspicious or security-relevant activity, and analysed/tuned resulting alerts.
- Created automation scripts for Wazuh agent installation/onboarding, health diagnostics, Sysmon deployment and recurring operational tasks.
- Deployed and troubleshot containerized Wazuh environments using Docker; worked across Manager, Indexer, Dashboard, agents, log collection and service management.
- Engineered Wazuh detections using custom rules, built-in rule extensions, correlation logic and custom decoders; performed threat hunting and reduced alert noise/false positives.
- Implemented vulnerability detection and compliance-oriented monitoring; integrated The Hive for case management and configured dashboards and Slack/email alert routing.
- Worked with OPNsense, Tailscale, Cisco AnyConnect, OpenVPN, Wire Guard and IPsec; configured routing, port forwarding, VLANs, subnets and inbound/outbound traffic flows.
- Configured FortiGate static routes, firewall policies and VLANs; set up SPAN/mirror traffic and network monitoring with Zeek and Suricata.
- Configured rack-server infrastructure and Proxmox virtualization; worked with Nginx reverse proxy, DNS, backup workflows and operational scripting.
- Deployed IBM QRadar, configured QRadar Connect, onboarded endpoint log sources, validated event ingestion and analysed security events.
- Developed attack-vector-based detection use cases for Active Directory, antivirus/endpoint security, web servers, backup servers and VPN servers; worked with Windows/Linux telemetry and Sysmon.
- Contribute to an Agentic SOC AI initiative focused on security operations and automation.

Cybersecurity Associate — Jan 2026 – Apr 2026

NodeSec Technology

- Managed GTB Technologies DLP operations, including incident triage, event analysis and policy management.
- Performed inventory management and endpoint monitoring for data security compliance; investigated and closed DLP alerts with root-cause analysis and remediation recommendations.
- Supported threat monitoring and response using Sentinel One EDR; gained exposure to Forescout NAC and CyberArk PAM.

Cybersecurity Trainee — Sept 2025 – Dec 2025

Tata Strive (Offline)

- Assisted with vulnerability assessment simulations, log analysis and SOC-style monitoring using SIEM tools.
- Performed web application/lab vulnerability assessments using Nmap, Nessus and Burp Suite; monitored logs in Wazuh/Splunk for suspicious activity.

TECHNICAL SKILLS

SOC / SIEM: Wazuh, IBM QRadar, SIEM Monitoring, Log Analysis, Detection Engineering, Threat Hunting, Incident Detection, Alert Tuning

Cloud Security: AWS Cloud Server Onboarding, Multi-source Cloud Log Collection, Cloud Telemetry Validation, Cloud Detection Rules, Cloud
Security Monitoring

Wazuh Engineering: Custom Rules, Built-in Rule Extension, Decoders, Correlation Logic, Agent Onboarding, Sysmon, Dashboards, TheHive,
Slack/Email Integration, Automation, Backup(compressed).

Incident Detection: Active Directory, Endpoint Security, Web Server, Backup Server, VPN Server Attack Vectors, Rule Development, Detection Use Cases

Endpoint Security: Windows/Linux Telemetry, Sysmon, GTB Technologies DLP, Sentinel One EDR, CyberArk PAM, Forescout NAC

Network Security: FortiGate, OPNsense, Routing, Firewall Policies, VLANs, Subnetting, Port Forwarding, SPAN/Port Mirroring, Network Segmentation

VPN / Connectivity: IPsec, WireGuard, OpenVPN, Tailscale, Cisco AnyConnect

NSM / Network Analysis: Zeek, Suricata, Wireshark, TShark, Live Traffic Monitoring

Infrastructure / DevOps: Docker, Proxmox, Nginx Reverse Proxy, DNS, Rack Server Setup, Backup/Configuration Management

VAPT: Nmap, Nessus, Burp Suite, Metasploit, Hydra, SQLmap, OWASP Top 10

Scripting / Programming: Python, Bash, Powershell, C, C++, Java, SQL, JavaScript, MERN

PORTFOLIO & PROJECTS

Production Wazuh SOC, Cloud Log Monitoring & Detection Engineering

- Designed and deployed Wazuh Manager, Indexer and Dashboard in a Docker-based SOC environment; configured agents, log collection, dashboards, integrations and production monitoring.
- Onboarded Windows/Linux endpoints and Sysmon telemetry, plus AWS cloud servers; integrated logs from multiple sources and validated event flow into centralized monitoring.
- Developed custom rules, decoders and correlation logic; extended built-in detections, tuned alert conditions and created cloud-focused detections from available telemetry.
- Integrated TheHive for case management, configured Slack/email alert routing, and implemented vulnerability detection and SOC dashboards.

IBM QRadar — QRadar Connect & Endpoint Log Analysis

- Deployed IBM QRadar and installed/configured the QRadar Connect agent for endpoint log collection and forwarding.
- Onboarded endpoint log sources, validated event ingestion and analysed collected security events for suspicious and security-relevant activity.
- Worked across the endpoint → QRadar Connect → SIEM pipeline, including log-source connectivity, ingestion validation and event analysis.

Attack-Vector-Based Detection Engineering

- Active Directory: mapped authentication/security telemetry to detection use cases and SIEM rules for studied attack vectors.
- Antivirus / Endpoint Security: created detection rules from relevant endpoint-security telemetry.
- Web Server, Backup Server and VPN Server: developed detection use cases from relevant request, server, authentication, connection and security telemetry.
- Workflow: attack vector → attacker behaviour → observable telemetry → SIEM event → detection rule → alert analysis/tuning.

EDUCATION

Bachelor of Technology - Computer Science & Engineering **Graduated 2025**

Greater Noida Institute of Technology (GNIOT) *(CGPA – 7.7)*

Additional hands-on focus

SOC Engineering, Cloud log monitoring, SIEM detections, Endpoints telemetry and Network Security Monitoring