

# KAUSHALSINH VALA

kibhavala9@gmail.com | 6359991555 | linkedin.com/in/kaushalsinhvala

## Summary

---

Experienced Security Analyst with nearly 4 years in the IT field, focusing on threat detection, incident response, and automation. Proficient in SIEM tools such as Microsoft Sentinel, ArcSight, Splunk, and Log360. Strong grasp on compliance, malware analysis, SOAR, and endpoint security.

## Technical Proficiency

---

**SIEM:** Cortex XDR, Microsoft Sentinel, ArcSight, Splunk, Log360

**Firewalls/WAF:** Sophos, Palo Alto, FortiGate

**IDS/IPS/XDR:** Suricata, Cortex XDR, Trend Micro

**Languages:** Python, PowerShell

**Vulnerability Mgmt:** Tenable, OpenVAS, Qualys

**Compliance:** GDPR, HIPAA, PCI DSS, NIST, MITRE ATT&CK

**Query Languages:** KQL, WQL

**Tools:** CMDB, Grafana, IDA, Volatility, Redline, Burp Suite

## Employment History

---

### SOC Analyst

Dev Information Technology Ltd – Ahmedabad (2025–Present)

- Manage SIEM tools (Sentinel, Coretex XDR, Splunk) including alert tuning, log monitoring, and event correlation.
- Analyze network traffic for anomalies; investigate incidents and perform forensic analysis.
- Implement automation using Wazuh, Shuffle, The Hive, VirusTotal API for detection and response.
- Conduct breach readiness drills, vulnerability assessments (Qualys), and incident documentation.
- Support audits and ensure compliance with PCI DSS, ISO 27001, SOC 2, and NIST.
- Develop playbooks, perform phishing simulations, train employees, and enforce IAM controls.
- Built automation pipelines that integrate VirusTotal and Wazuh.

## **SOC Analyst Team Lead**

Phoenix Technocyber – Surat (2020–2023)

- Developed SOC processes and led team for multi-device alert correlation.
- Led SOC operations, optimized client SIEM reports, and created real-time incident alerts.
- Implemented automation, documented incident processes, and handled escalations.
- Conducted security awareness campaigns and weekly threat reports.
- Investigate phishing emails, suspicious logins, and security concerns reported by users & soc team.
- Follow runbooks and playbooks for common threat scenarios like brute-force, malware detection, or data exfiltration.
- Maintain accurate incident logs, including timelines, actions taken, and outcomes.
- Assist in vulnerability scan reviews and coordinate with IT for patch updates.
- Stay up-to-date on threat trends, malware types, and attack vectors through threat intelligence feeds and internal briefings.
- Work closely with senior analysts to learn advanced detection and response techniques.
- Support security awareness efforts by identifying trends in user behavior and reporting suspicious activities.

## **Security Engineer**

Sequaretek IT Solutions – Mumbai (2019–2020)

- Managed SEP 12/14, handled malware mitigation, compliance reporting, and risk assessments.
- Performed IOC analysis, disaster recovery drills, and endpoint/server baseline reviews.
- Monitored events, investigated incidents, escalated threats, and closed tickets per SOP.
- Monitor security alerts from SIEM and other sources in real-time.
- Perform an initial alert triage to determine severity, priority, and possible impact.
- Document incidents and create tickets for investigation based on standard operating procedures (SOPs).
- Escalate threats to L2/L3 teams when indicators of compromise (IOCs) or suspicious behavior is detected.
- Conduct initial assessments on alerts to evaluate their severity, priority, and possible effects.
- Assist in deploying and maintaining security tools such as firewalls, endpoint protection platforms, and intrusion detection/prevention systems (IDS/IPS).
- Monitor system logs and alerts, supporting the detection and resolution of potential security incidents.

- Perform basic configuration and troubleshooting of security devices (e.g., firewalls, antivirus, proxies).
- Support vulnerability management efforts by running scans, analyzing results, and coordinating patching with relevant teams.
- Implement security policies and controls under the guidance of senior engineers or architects.
- Support network segmentation and access control configurations in alignment with zero-trust principles.
- Assist in endpoint hardening by applying baseline configurations and ensuring compliance with company security standards.
- Help maintain asset inventory and ensure visibility of all devices connected to the environment.
- Document security processes, configurations, and incident response actions for audit and compliance purposes.
- Collaborate with IT teams during security tool deployments and updates.
- Stay up-to-date with evolving threats, tools, and best practices in cybersecurity and share insights with the team.

## **Certifications & Education**

---

### **Certified Information Security & Ethical Hacker**

**M.Tech**, Cyber Security Raksha Shakti University, Ahmedabad (2019)

**B.E.**, Information Technology Gujarat Technological University, Ahmedabad (2017)