Kushlendra Singh

Cyber Security Consultant (Professional Services)
Ahmedabad, India,380061 | +91 8401783081 | Kushlendra02@gmail.com

Security Consultant and Cyber Security Engineer with hands-on experience delivering enterprise SIEM and SOAR solutions across hybrid and cloud environments. Proven expertise in Microsoft Sentinel and Splunk, including large-scale use case development, log onboarding, custom parser creation, and security automation using Azure Logic Apps. Strong background in cloud security monitoring, incident detection and response, high-availability and disaster recovery architectures, and professional services delivery. Experienced in penetration testing, vulnerability management, and offensive security across web, API, network, and cloud systems, with a solid foundation in security architecture design, documentation, and customer-facing consulting for public and private sector organizations.

Experience

ICPES Technologies, Bangalore, IN

Security Consultant | Dec 2023 – Present

- Led enterprise-grade SIEM and SOAR implementations using Microsoft Sentinel and Splunk, delivering end-to-end security monitoring solutions for multiple client environments.
- Designed and developed 1,000+ SIEM detection use cases using KQL, aligned to MITRE ATT&CK, covering endpoint, identity, network, cloud, and SaaS threat scenarios.
- Onboarded and normalized logs from Windows, Linux, firewalls, switches, cloud platforms, and SaaS applications, ensuring complete visibility across hybrid and multi-cloud environments.
- Built and maintained custom log parsers and data connectors for 50+ OEM products, enabling accurate log ingestion, enrichment, and correlation.
- Developed SOAR automation playbooks using Azure Logic Apps, automating alert triage, enrichment, containment, ticketing, and notification workflows to reduce MTTR.
- Designed High-Level Design (HLD) and Low-Level Design (LLD) documents for enterprise SOC architectures, including SIEM, SOAR, log ingestion, and threat response workflows.
- Architected and deployed high availability (HA) and disaster recovery (DR) SIEM/SOAR solutions to meet enterprise resilience and compliance requirements.
- Implemented cloud security monitoring and threat detection across Azure environments, integrating Defender signals, activity logs, and identity telemetry into Sentinel.

- Worked closely with customers in a professional services and consulting capacity, translating business and compliance requirements into scalable security solutions.
- Delivered professional documentation, operational runbooks, architecture diagrams, and executive-level security reports to support audits, handover, and long-term operations.

Attack Box, Ahmedabad, IN

Cyber Security Engineer | Jan 2023 – Dec 2023

- Designed and developed custom security tools and vulnerable machines for hands-on cybersecurity training, Capture The Flag (CTF), and offensive security labs.
- Built and maintained CTF platforms, including vulnerable web applications, APIs, networks, and systems to simulate real-world attack scenarios.
- Planned and executed CTF competitions, bug bounty programs, and security workshops, supporting large-scale cybersecurity events and community engagement.
- Performed penetration testing and Vulnerability Assessment & Penetration Testing (VAPT) across web applications, APIs, mobile apps, networks, and infrastructure.
- Conducted source code reviews and manual exploitation aligned with OWASP Top 10, identifying critical security flaws and providing remediation guidance.
- Deployed and managed Tenable vulnerability management solutions, including Nessus and Tenable Security Center, for infrastructure and application security assessments.
- Produced clear, actionable security assessment reports, including risk ratings, proof of concept (PoC), impact analysis, and remediation recommendations.
- Collaborated with red team members to simulate real-world attack techniques using tools such as Metasploit, Nmap, Burp Suite, and SQLMap.

Digz Placements, Ahmedabad, IN

Jr Cyber Security| Sep 2022 – Jan 2023

- Delivered CEH and CCNA cybersecurity training, supporting candidates with hands-on labs, real-world demonstrations, and guided attack-defense scenarios.
- Assisted students in practical penetration testing labs, covering web applications, APIs, networks, and basic cloud security concepts.
- Demonstrated real-world hacking techniques, including reconnaissance, exploitation, privilege escalation, and post-exploitation activities in controlled environments.
- Performed practical VAPT exercises on target systems, identifying vulnerabilities and misconfigurations across applications and network services.
- Conducted OSINT investigations, gathering intelligence from public sources to support attack surface analysis and threat modeling.
- Created professional vulnerability assessment and penetration testing reports, documenting findings, evidence, impact, and remediation steps.

- Supported documentation, lab setup, and training material development to ensure consistent learning outcomes.

Education

Ganpat University, Gujarat

BTech in Computer Science Spec. in Cyber Security | June 2020 – June 2024

- CGPA: 8.4

Certificates

- SC100 - Microsoft Cybersecurity Architect
- SC200 - Microsoft Certified: Security Operations Analyst Associate
- Google Cloud SecOps Technical
- Google Cloud SecOps Sales
- Google Security Operations - Deep Dive
- Google Security Operations - Fundamentals
- Chronicle SIEM Fundamentals
- Google Security Operations - SIEM Rules
- SOAR Fundamentals
- Security Practices with Google Security Operations - SIEM
- Mandiant Fundamentals
- Google Security Operations - SOAR Developer
- Google Security Operations - SOAR Analyst
- AWS Cloud Foundations
- Microsoft Cloud Security Hackathon
- Cisco Cybersecurity Essentials
- Cisco CCNA

Skills

- Linux
- Fortify SAST
- Fortify DAST
- Tenable
- Threat Research
- Threat Hunting
- Burp Suite
- Red Teaming
- Penetration Testing
- Web Application Security
- Mobile Application Security
- API Testing
- Vulnerability Management
- DevSecOps
- Metasploit
- Nmap
- SQLMap
- Nessus
- Python
- Source Code Review
- Container Security

- Security Automation
- OWASP Top 10
- Splunk
- Vulnerability Assessment
- Security Monitoring
- Cloud Security
- SIEM
- SOAR
- Incident Response
- Threat Detection
- Sentinel
- Chronicle
- SIEM Rules
- SOAR Development
- SOAR Analysis

OEM Expertise

Sr no	Cybersecurity	OEM Products
1.	Application Security	OpenText™ Fortify Static Code Analyzer OpenText™ Fortify WebInspect Tenable Web Application Scanning Tenable Nessus
2.	Vulnerability Management	Tenable Security Center Tenable Vulnerability Management
3	Cloud Security	Tenable CS Tenable Attack Surface Management Microsoft Sentinel Google Chronicle
4	OT Security	Tenable OT Security
5	Enterprise Security	Splunk ArcSight

* Specialized in solution design, deployment, system health assessments, and seamless integration of the aforementioned OEM products. Experienced in deploying solutions across small, medium, and large enterprises, including both public and private sectors.