Sharique Hussain

Senior SOC Analyst | Detection Engineer | Cloud Security Engineer

SUMMARY

Senior Cybersecurity professional with 6+ years of enterprise-scale experience protecting platforms serving 50M+ users. Proven track record of measurable security outcomes including improving detection Signal-to-Noise Ratio from 50% to 90%, expanding endpoint visibility from 68% to 99%, and reducing MTTR by approximately 40%. Deep technical expertise spanning SIEM detection engineering, SOAR automation, EDR, cloud security, and Infrastructure as Code, with strong ability to communicate technical findings to engineering, legal, and executive stakeholders.

SKILLS

Google SecOps/Chronicle | LogRhythm | Elastic SIEM | Splunk | Microsoft Sentinel | Incident Response | Digital Forensics | CrowdStrike Falcon | Tines SOAR | AWS GuardDuty | AWS Config | Lacework CSPM | GCP Security Command Centre | Cloudflare WAF | Cloudflare Zero Trust | Terraform | GitHub Actions | CI/CD | Mandiant | Google Threat Intel | CrowdStrike Falcon Recon | CTM360 | ImmuniWeb | Recorded Future | MITRE ATT&CK; | Nessus | IDS/IPS | DMARC | DKIM | DLP | Dynatrace | Python | PowerShell | KQL | YARA-L | SPL | FQL | JSON | YAML | REST APIs | NIST CSF | ISO/IEC 27001 | SOC 2 | JIRA | Confluence

EXPERIENCE

Senior Cyber Security Operations Engineer — Careem (An Uber Company)

Mar 2024 – Present • UAE / Remote

Leads enterprise-scale 24×7 SOC operations for an Uber subsidiary platform serving 50M+ users, owning end-to-end incident response for critical security events and engineering advanced SIEM detection logic. Architect of security automation infrastructure including Terraform-based IaC framework managing 100+ Cloudflare edge security rules and zero-touch CI/CD pipelines. Serves as technical escalation point and delivers structured post-incident analysis to cross-functional stakeholders including engineering, legal, and executive leadership.

- Engineered and refined SIEM correlation rules in Google SecOps (Chronicle), improving Signal-to-Noise Ratio from 50% to 90% and eliminating 40% of false positives
- Deployed DMARC, DKIM, and sandboxing controls reducing phishing delivery by 95%; implemented DLP policies blocking unauthorized exfiltration
- Identified and remediated 30+ critical AWS misconfigurations; maintained continuous cloud security posture monitoring via Lacework CSPM and AWS GuardDuty
- Conducted MITRE ATT&CK-aligned; threat hunting; hunt outputs directly generated 8 new SIEM detection rules, reducing MTTD
- Architected Terraform-based IaC framework managing 100+ Cloudflare edge security rules across multiple production zones, eliminating manual configuration drift
- Built zero-touch CI/CD pipeline (GitHub Actions + Terraform) enforcing plan/apply separation and automated security validation
- Mentored junior analysts and acted as shift lead during major incidents

Cyber Security Operations Engineer II — Careem (An Uber Company)

Jan 2023 – Mar 2024 • UAE / Remote

Architected and executed enterprise-wide endpoint security deployment and led adversary emulation exercises to strengthen detection capabilities. Expanded organizational security visibility and external attack surface management while supporting compliance initiatives. Delivered measurable improvements in endpoint coverage, detection capabilities, and security posture scoring.

- Architected enterprise-wide CrowdStrike Falcon EDR deployment across Production, Staging, and Development environments, expanding endpoint visibility from 68% to 99%
- Led adversary emulation (purple team) exercise simulating real-world attack chains; gap analysis produced 15+ new SIEM detection rules and reduced MTTD
- Evaluated and deployed CTM360 EASM platform enterprise-wide, lifting external security posture score from 90 to 96
- Deployed Cloudflare WAF neutralizing active brute-force campaigns targeting API endpoints
- Supported ISO 27001 and SOC 2 compliance initiatives through gap assessments, evidence collection, and control alignment verification

Cyber Security Operations Engineer I — Careem (An Uber Company)

Nov 2021 – Dec 2022 • UAE / Remote

Performed Tier-1/Tier-2 SIEM alert monitoring and triage in high-volume 24×7 enterprise SOC environment, producing structured incident reports and operationalizing threat intelligence feeds. Contributed to security framework implementation and maintained incident response documentation and standard operating procedures.

- Performed SIEM alert monitoring and triage in high-volume 24×7 enterprise SOC; produced structured incident reports with IOCs, attack timelines, and containment recommendations
- Operationalized threat intelligence feeds within SIEM, flagging 30+ malicious domains and IPs in first quarter, reducing dwell time on known-bad infrastructure
- Maintained incident response runbooks and SOPs; contributed to security framework implementation and SOC process documentation

Information Security Engineer — RapidCompute Pvt. Ltd.

Aug 2019 – Nov 2021 • Karachi, Pakistan

Deployed and managed enterprise SIEM infrastructure while driving organization-wide security initiatives including multi-factor authentication rollout and vulnerability management programs. Monitored security infrastructure in real-time, investigated anomalies with full root-cause analysis, and developed incident response documentation adopted for team onboarding.

- Deployed and managed LogRhythm SIEM; built custom correlation rules improving alerting accuracy by 20% and reducing analyst false-positive workload
- Drove organization-wide MFA rollout across 500+ users, achieving 98% adoption in 60 days
- Conducted quarterly Nessus vulnerability scans with coordinated remediation, achieving zero open critical CVEs per sprint
- Monitored IDS/IPS, firewalls, and endpoint protection in real-time; investigated anomalies with full root-cause analysis and post-incident reporting
- Developed incident response plans and coordinated multi-departmental response during active security events; produced documentation adopted as onboarding material

Technical Support Engineer — Multinet Pakistan Pvt. Ltd.

Feb 2019 – Aug 2019 • Karachi, Pakistan

Managed enterprise networking infrastructure including IP/MPLS, secure VPN, SMTP, and DNS services for major clients including British Telecom, Verizon, and financial institutions. Served as Shift In-charge and QA Engineer, producing root-cause analysis documentation for all escalated anomalies.

- Managed IP/MPLS, secure VPN, SMTP, and DNS for enterprise clients including British Telecom, Verizon, and major financial institutions
- Served as Shift In-charge and QA Engineer, producing RCA documentation for all escalated anomalies

EDUCATION

Master of Science, Information Security — NED University of Engineering & Technology

2021 – 2023 • Completed part-time while employed full-time

Bachelor of Engineering, Telecommunications Engineering — Iqra University

2015 – 2018 • Gold Medalist — 1st Position, Class of 2018. Final Year Project: Network Security & Redundancy Model — GNS3 and physical cisco switches

CERTIFICATIONS

Certified Ethical Hacker (CEH)

EC-Council • 2021

Certified AppSec Practitioner (CAP)

The SecOps Group • Feb 2023

Foundation Level Threat Intelligence Analyst

arcX • Apr 2023

ISO/IEC 27001 Information Security Associate

SkillFront • May 2021

CCNA Security

Cisco • Oct 2018

NSE 1 Network Security Associate

Fortinet • Sep 2021

LANGUAGES

English (Full Professional Proficiency) | Urdu (Native)