Mohammed Faisal Khan

SOC Analyst | EDR & AV Engineer | IT Support

Dubai, UAE • +971 50 170 1165 • faisalkhan78612@gmail.com

linkedin.com/in/mohammedfaisalkhan • github.com/samfaiz

PROFILE SUMMARY

SOC Analyst with 3+ years of experience in security monitoring, incident triage, and threat response. Skilled in monitoring SIEM dashboards (Microsoft Sentinel) and EDR platforms (Microsoft Defender, CrowdStrike, SentinelOne) in real time, classifying alerts, correlating logs and indicators of compromise, and escalating high-severity incidents with full documentation. Experienced in phishing and malware analysis, threat-intelligence enrichment, root cause analysis, and producing incident reports with remediation recommendations.

CORE SKILLS

- **SIEM & Monitoring:** Microsoft Sentinel, Splunk, real-time dashboard & alert monitoring, log correlation
- **EDR / EPP:** Microsoft Defender for Endpoint, CrowdStrike Falcon, SentinelOne, McAfee MVision, Trellix EPO, Symantec
- **Incident Response:** Alert triage (true vs false positive), device isolation, password resets, IP/domain blocking, escalation to L2/L3
- **Threat Analysis:** phishing analysis, malware analysis, VirusTotal, Hybrid Analysis, MITRE ATT&CK
- **Documentation & Reporting:** Incident tickets, RCA, investigation notes, incident timelines, trend reporting, SOPs (ServiceNow)
- **Endpoint Management:** Microsoft Intune, vulnerability management, policy configuration & hardening
- **Scripting / OS:** PowerShell, scripting; Windows, macOS, Linux

PROFESSIONAL EXPERIENCE

Cruise Motors

Jan 2025 – Present

IT & Cyber Security Engineer — Dubai, UAE

- Monitor SIEM dashboards (Microsoft Sentinel) and security alerts in real time, tracking and analyzing events from Microsoft Defender to identify suspicious activity, anomalies, and policy violations.
- Perform initial investigation and classification of alerts, distinguishing true positives from false positives by reviewing logs, event details, reputation data, and indicators of compromise.
- Initiate predefined response actions including isolating compromised endpoints, forcing password resets, and blocking malicious IPs and URLs, then escalate confirmed or high-severity incidents to L2/L3 with proper documentation.
- Check IOC hits against threat-intelligence sources and analyze phishing emails, malware infections, malicious URLs, attachments, credential-harvesting attempts, and unauthorized access events.
- Conduct root cause analysis and create detailed incident tickets, investigation notes, and incident reports with remediation recommendations, maintaining accurate timelines in the ticketing system.
- Identify trends across alerts to support early-stage threat detection and generate reports for repeated or trending issues.
- Orchestrated end-to-end configuration and deployment of Microsoft Defender for Endpoints and Servers, ensuring proactive incident resolution and infrastructure hardening.
- Leveraged Microsoft Intune to enforce security protocols, including browser lockdowns and elevated-privilege requirements for software installation.
- Proposed custom detection rules in SIEM and EDR tools to improve detection accuracy and reduce false positives, collaborating with cross-functional teams to mitigate threats.
- Provide Tier 2/3 technical support, resolving complex hardware and software issues, and manage the full hardware lifecycle including procurement, inventory, and upgrades.

Eviden – Atos

Oct 2022 – Sept 2024

Associate Engineer (SOC) — Mumbai, India

- Provided Level 1 SOC operations in a 24x7 shift environment, using SOC tools to continuously monitor and analyze system activity and identify malicious activity via dashboards.
- Monitored, analyzed, and responded to new CrowdStrike detections classified as Unsafe/Abnormal, performing security incident handling, investigation, and escalation with mitigation recommendations.
- Handled phishing emails and endpoint security alerts triggered by various security tools, and performed threat analysis using third-party tools such as VirusTotal and Hybrid Analysis.
- Detected devices running outdated software, default configurations, or services with known vulnerabilities, and flagged unusual activity such as login attempts on exposed RDP ports.
- Reduced false alerts by 30% by tuning policies to vendor recommendations and standards; configured prevention and mobile policies.

- Developed a PowerShell script to automate CrowdStrike sensor repair, reducing manual intervention by 50–60% and receiving formal appreciation.
- Worked P1 & P2 incidents within defined SLAs, resolved problem incidents with RCA, and managed changes through CIP preparation and CAB meetings (ITSM Incident, Problem & Change Management).
- Migrated clients from traditional AV to EDR solutions and designed SOPs that improved team efficiency across Government, Healthcare, and Green Energy projects.

SECURITY PROJECTS

EDR/XDR Compliance Dashboard — Laravel, MySQL, Next.js (React), Tailwind, Sanctum

- Built a multi-tenant SaaS that lets security teams connect their EDR/AV vendor APIs (CrowdStrike, Defender, SentinelOne, etc.), normalize the data, and monitor endpoint compliance posture across their fleet from one vendor-agnostic dashboard.
- **Problem:** Organizations had no single, vendor-agnostic view of endpoint security compliance, and the platform needed to safely serve many companies without their data ever mixing.
- Architected multi-tenant organization isolation with a secure-by-default global query scope, guaranteeing one tenant can never access another's data, settings, or logs; added a platform-owner role for cross-org administration.
- Built a configurable connector + ingestion pipeline that pulls, normalizes, and snapshots data from any EDR/AV API, powering customizable dashboards, trend charts, and compliance rules.
- Implemented role-based access, MFA, and audit logging, plus per-organization email/SMTP and notification settings.
- Added a self-service 1-hour demo that provisions an isolated, sample-loaded workspace on one click and auto-expires (server enforced + scheduled cleanup) to drive frictionless trials.
- Live: https://compliancedashboard.faisalkhan.cloud/

Home SOC Lab (Active Directory)

- Designed and deployed a multi-VM Active Directory home SOC lab on VMware Workstation — Windows Server 2022 domain controller, Windows 11 client, Ubuntu server, pfSense firewall, and Kali attacker — instrumented with Sysmon, PowerShell block logging, and advanced audit policies to enable safe attack simulation and detection-engineering practice.
- GitHub: https://github.com/samfaiz/home-soc-lab-build-Project-1

Wazuh SIEM & Detection Engineering

- Built an all-in-one Wazuh SIEM on Ubuntu, integrated 4 agents (Windows DC, workstation, Linux server, pfSense), and wrote 10 custom detection rules mapped to MITRE ATT&CK (T1003.001 LSASS access, T1059.001 encoded PowerShell, T1566.001 Office macro abuse), validated with Atomic Red Team.

OTHER PROJECTS

AI-Built CMS Websites

- Designed and built full CMS-driven websites end-to-end using AI-assisted development, handling layout, content management, and deployment with unique per AI SEO Optimization and AI SEO Algorithm section to improve the SEO performance for future audit runs
- Live: https://wmd.faisalkhan.cloud/ & https://finper.faisalkhan.cloud/

EDUCATION

B.E., Information Technology — Mumbai University (CGPI: 8.51) 2019 – 2022

Diploma, Information Technology — VPM's Polytechnic, Thane (Score: 80%) 2016 – 2019

CERTIFICATIONS & TRAINING

- Certified CrowdStrike Falcon Administrator (CCFA)
- Certified Ethical Hacker v12 (CEH)
- Trellix EPO | Endpoint Security