ABDULLAH KHAN

Junior SOC Analyst | SolarWinds SIEM · CrowdStrike EDR

Dera Ghazi Khan, Pakistan |+92-336-2238524|khan.abdulah@hotmail.com
Portfolio: https://abdullahkhan-nuxt-portfolio.netlify.app/,
LinkedIn: http://www.linkedin.com/in/abdullah-khan-2001y11m15d

EDUCATION

Ghulam Ishaq Khan Institute (*Sep 2021 – Jul 2025)*
BS Computer Engineering
Superior College DG Khan *(Sep 2018 – Jul 2020)*
FSC: 75%

PROFESSIONAL EXPERIENCE

CareCloud – Junior SOC Analyst *(May 2025 – Present)*

- Proactively monitor **SolarWinds SIEM** for **~3,000 users**, **correlating** security events to reduce **mean time to detect/respond**.
- Developed a **Python automation script** for **brute-force attack detection,** cutting triage time from **15 minutes to under 5 minutes**.
- Evaluated **SOAR platforms** (Splunk SOAR, IBM QRadar SOAR, Cortex XSOAR) and recommended the **optimal solution** to **automate incident handling** and **improve response workflows**.
- Investigate **CrowdStrike EDR** telemetry across **750+ workstations**, performing **endpoint hunts** and **IOC enrichment** to validate alerts.

NetSol Technologies – Technical Intern *(Jun 2024 – Aug 2024)*

- Coordinated with **cross-functional teams** to design and deploy the **company's website using Nuxt 3**, enhancing **SSR performance** and **SEO optimization**.
- Developed a **personal portfolio** with **100+ reusable components**, integrating best **UI/UX practices** and **debugging strategies**.
- **Refactored** and **optimized** codebases to ensure **maintainability**, **scalability**, and **adherence** to coding standards.

LEADERSHIP AND EXTRACURRICULAR ACTIVITIES

- **Director Film Fest – Media Club GIKI** *(Sep 2022 – Feb 2023)* — Directed **main film** for **GIKI Film Fest 2023**; managed **50+ members** and hosted **500+** attendees.
- **Tech Head – Netronix GIKI** *(Oct 2021 – May 2023)* — Organized **cybersecurity hackathon** with **50+ participants** from **10+ institutions**, fostering **industry-academic collaboration**.
- **Football Team DG Khan District – Full Back** *(Sep 2019 – Nov 2019)* — Represented **district** in **all-Pakistan tournament**, ranking in **semi-final** 10 out of 70+ teams.

UNIVERSITY PROJECTS

COMPUTER ENGINEERING PROJECTS

- **SafeShe (FYP – 1st Place, Faculty of CSE)** — **Led development** of a **women's security app** with **SOS button**, **Safe Zones**, **Lawpath integration**, **community feature**, and **CNN-based voice recognition** (98% accuracy).
- **Password Manager (Python)** — Designed an encrypted **credential vault** with **local/cloud sync**, **autofill for 50+ websites**, and **self-destruct** mechanism triggered after **brute-force attempts**.
- **Remote-Controlled Spy Car (Arduino)** — Built a **mobile-controlled** surveillance car with **500+** lines of C, achieving **30m** real-time operational range.

CERTIFICATION & RECOGNITION

- SOC Level 1 — TryHackMe *(2025)*
- Google Cybersecurity Professional Certificate — (2025)
- Introduction to Cybersecurity — Coursera *(2024)*
- Certificate of Appreciation — NetSol Technologies (Eric Wagner, CMO) *(2022)*
- Certificate of Appreciation — CareCloud (CTO) *(2025)*

Technical Skills

Security & Networking: SIEM (SolarWinds), EDR (CrowdStrike), Incident Response, Threat Hunting, Log Analysis, IOC/IOA, MITRE ATT&CK, NIST CSF, TCP/IP, DNS, HTTP/HTTPS, SMTP, VPNs, Firewall Rules.
Programming & Automation: Python, PowerShell, Splunk SPL.
Tools: Splunk, SolarWinds SEM, Cortex XSOAR, Wireshark, Tcpdump, VirusTotal, Nmap, Burp Suite, MITRE Navigator.
Languages: English (Fluent), Urdu (Fluent), Punjabi (Fluent), Siraiki (Fluent).