SALJOOK HAIDER

Cyber Security Analyst | Security Operations | Incident Response

Dublin, Ireland | +353 87 034 9157 | seljukhaider77@gmail.com | linkedin.com/in/saljookhaider | Available immediately

PROFESSIONAL SUMMARY

SOC-focused Cyber Security Analyst with two years of experience triaging Splunk alerts, investigating endpoint, identity and email threats, and escalating confirmed incidents. BTL1 (Gold) and CompTIA Security+ certified with a First Class MSc in Cybersecurity, combining digital forensics and phishing analysis skills with Python and PowerShell automation to resolve alerts faster and document them clearly.

CERTIFICATIONS

- **Blue Team Level 1 (BTL1), Security Blue Team** | Gold Badge, 95/100 | Digital forensics, incident response, SIEM, malware analysis, threat hunting, phishing analysis, threat intelligence
- **CompTIA Security+ (SY0-701)** | Score 870/900 | Network security, endpoint protection, risk management, cryptography, cloud security, IAM

TECHNICAL SKILLS

SOC Operations: Alert monitoring and triage, incident investigation, escalation, root cause analysis, incident documentation

SIEM and Log Analysis: Splunk, Windows event logs, Sysmon, authentication logs, DNS and HTTP logs

Digital Forensics and IR: KAPE, FTK Imager, Autopsy, Volatility, DeepBlueCLI, evidence collection, timeline reconstruction

Threat Intelligence and Email: MITRE ATT&CK, IOC enrichment, phishing and URL analysis, VirusTotal, CyberChef, WHOIS, MXToolbox

Network Analysis: Wireshark, packet capture analysis, TCP/IP, DNS

Identity and Endpoint: Active Directory, Entra ID, Microsoft 365, access reviews, Windows, patch management

Automation and AppSec: Python, PowerShell, OWASP Top 10, secure code review, Semgrep, Bandit

PROFESSIONAL EXPERIENCE

Cyber Security Analyst | 3AM Technologies **Jan 2024 – Jan 2026**

Security Operations (SOC) & Incident Response

- Monitored and triaged 200+ security alerts per week in Splunk, correlating system, application, network and endpoint logs to separate true positives from false positives
- Investigated suspicious endpoint, identity and email activity by querying Windows event logs and Entra ID sign-in logs in Splunk, mapping attacker behaviour to the MITRE ATT&CK framework to determine scope and root cause
- Escalated 40+ confirmed incidents per runbooks and SLAs, supporting containment through account disablement, host isolation and malicious IP/domain blocking, and documenting findings in incident tickets
- Analysed 50+ reported phishing emails per month, extracting IOCs such as URLs, attachments and sender domains, and enriching them with VirusTotal, WHOIS and MXToolbox
- Tuned detection rules to cut false positives by 30% and automated triage tasks with PowerShell and Python, saving around 8 hours per week

Frontend Developer | Secure Web Solutions | kreativrudel GmbH & Co. KG **Jul 2021 – Sep 2023**

Remote, Germany | Application Security & Client Support

- Identified and remediated input validation failures and access permission misconfigurations in live client web environments
- Communicated technical security risk to non-technical stakeholders and third-party clients in Germany, Switzerland and Austria, aligning remediation with business requirements while working independently within a distributed team

HANDS-ON LAB INVESTIGATIONS

BTL1 certification labs and personal lab work in simulated environments; not production SOC experience.

- **Endpoint and network investigation:** Traced simulated incidents in Splunk using Windows authentication, process and Sysmon telemetry, tracing process chains and persistence, and corroborated findings with Wireshark packet captures
- **Digital forensics:** Acquired and analysed disk and memory images with FTK Imager, KAPE, Autopsy and Volatility, used DeepBlueCLI to surface suspicious event log activity, and reconstructed incident timelines from correlated artefacts

- **Phishing analysis:** Examined email headers, sender infrastructure, attachments and URLs, enriching indicators with VirusTotal, WHOIS and MXToolbox, decoding content in CyberChef, and classifying messages as benign, suspicious or malicious
- **Reporting:** Wrote structured investigation reports covering findings, evidence reviewed, IOCs, MITRE ATT&CK mapping and recommended containment and remediation actions

EDUCATION

MSc in Cybersecurity, First Class Honours | Dublin Business School, Dublin **Apr 2025 – Apr 2026**

- Dissertation: Built a Python pipeline using a large language model to evaluate Semgrep and Bandit static-analysis findings, triaging likely false positives and generating remediation guidance

BSc in Software Engineering, First Class Honours | University of Lahore **2019 – 2023**