Karim Chehab
Security Operations Center Analyst
Email: karimchehab0@gmail.com | **Mobile:** +966 598 717 099
Address: KFUPM, Dhahran, Saudi Arabia | **Nationality:** Lebanese

---

Summary

Security Operations Center Analyst with hands-on experience in monitoring, analyzing, and protecting systems against global threats. Currently studying for the **Certified Ethical Hacker (CEH)** certification, with proven expertise in identifying vulnerabilities, conducting vulnerability assessments, and implementing security measures to safeguard critical systems. Previous roles include responding to **APT attacks**, refining **incident response** strategies, and optimizing **SIEM** capabilities. Currently pursuing a **Master's in Security and Information Assurance** with a focus on **Smart Grid Security**.

Work Experience

Cyber Security Support Engineer
Log(N) Pacific – Seattle, Washington, USA | 08/08/2024 – Present

- Implemented secure cloud configurations using Azure Private Link, Network Security Groups, and Microsoft Defender for Cloud, adhering to Azure Regulatory Compliance (NIST 800-53), resulting in a 35% reduction in security incidents.

- Troubleshot and supported Microsoft Azure services, including Microsoft Sentinel (SIEM), Virtual Machines, Azure Monitor, and Azure Active Directory, resolving 25-30 issues per week on average.

- Developed and optimized KQL queries for Log Analytics and Microsoft Sentinel, resulting in 10-15 new SIEM dashboards and workbooks, improving threat detection and response capabilities.

- Monitored, detected, and responded to security events and incidents across the organization's global network, ensuring timely mitigation of risks.

Security Operations Center Analyst
Cyberploit – London, United Kingdom | 01/08/2023 – 01/08/2024

- Monitored and assessed security alerts and events from IDS, firewalls, and other security tools to identify and mitigate potential threats, contributing to the efficiency of SOC operations.

- Investigated suspicious activities, potential breaches, and conducted incident response, including root cause analysis and collaboration with teams for swift containment and resolution of APTs.

- Configured and optimized SIEM platforms such as Elastic and Splunk, performing log analysis and generating actionable reports to enhance security response capabilities.

- Utilized vulnerability assessment tools like Nessus to identify and address security weaknesses in systems, bolstering risk management and strengthening overall security posture.

Software Quality Assurance
FOO – Dubai, United Arab Emirates | 28/03/2023 – 30/06/2023

•Developed and executed test plans and cases for Fintech products using Testrail.

•Conducted manual testing and documented defects, improving product quality.

•Reported software defects using Jira and collaborated in an Agile environment.

Education

Master of Science in Security and Information Assurance
King Fahd University of Petroleum and Minerals – Dhahran, Saudi Arabia
27/08/2023 – 30/05/2025 | **GPA:** 3.4

Bachelor of Engineering in Computer and Communications Engineering
Rafik Hariri University – Mechrif, Lebanon
01/09/2019 – 26/05/2023 | **GPA:** 90.18

Skills

- **Cybersecurity Operations:** Incident Response, Splunk, Kali Linux, APT Simulation, Digital Forensics, Microsoft Sentinel (SIEM), KQL, Nessus, OSSEC, EDR, XDR, Firewalls, IDS, IPS, WAF.
- **Network Security:** Cisco (NAT, VLANs, Routing), TCP/IP, Packet Analysis (Wireshark)
- **Threat Analysis:** Splunk, Autopsy, Wireshark, Log Analysis
- **Security Tools:** Microsoft Defender for Cloud, Azure Sentinel
- **Programming:** Python, C++, SQL
- **Cloud Security:** Azure Security
- **Agile:** Agile Methodologies, Sprint Planning, Jira

Certificates

- **CCNAv7: Introduction to Networks** *(with merit)* – 2022-Present
- **CCNAv7: Switching, Routing, and Wireless Essentials** *(with merit)* – 2022-Present
- **CCNAv7: Enterprise Networking, Security, and Automation** *(with merit)* – 2022-Present
- **IELTS Academic Band 7 (C1)** – 2023-2025

Reference

Josh Madakor, CISSP
Owner, LOGN Pacific
6817 208th St SW, Unit 5761, Lynnwood, WA 98046
Phone: +1 (425) 319-0021 | Email: josh@lognpacific.com