Imtinan Saad

SOC Analyst | Information Security Graduate

✉ emtnansaadmhm@gmail.com 📞 +966 544127660 in www.linkedin.com/in/imtinan-saad

Objective

Information Security graduate with hands-on experience in a Security Operations Center (SOC). Experienced in threat detection, alert analysis, and incident response using SIEM tools. Seeking to work in a SOC environment to further develop skills in security event analysis and incident handling, with an interest in supporting threat intelligence activities within the security team.

Experience

Cybersecurity Operations Center (SOC) – COOP Training
Security Matterz

06/2025 – Present | Riyadh, Saudi Arabia

- Conducted in-depth **alert analysis and incident investigations** within a professional SOC environment, ensuring accurate detection and timely response to security events.
- Utilized **SIEM tools** such as *Splunk, RSA NetWitness, LogRhythm,* and *IBM QRadar* to monitor logs, correlate security events, and identify suspicious network and firewall activities.
- **Created incident tickets**, documented findings, and contributed to **monthly SOC reports** summarizing key alerts, false positives, and recommendations for improving detection rules and response workflows.

Certifications

- Cyber Incident Response Analysis
Misk Skills & STC — 7 hours
07/02/2025

- CCNA Development Course
Technical and Vocational Training Corporation 60 hours
09/07/2023 – 08/08/2023

- CompTIA Security+ Fundamentals
Technical and Vocational Training Corporation — 60 hours
27/08/2023 – 26/09/2023

- Cybersecurity Basics Technical Meeting
Ministry of Communications and Information Technology — 2 hours

Projects

CTI Flow - Threat Intelligence Management Platform
Training Project
- Developed a platform to manage and track IOCs with YARA and Sigma integration, duplication prevention, private IP filtering, and status tracking.

WhatsApp Forensics Tool
Graduation Project
- Currently developing a forensic tool to extract, decrypt, and analyze WhatsApp data for organized digital evidence.

Home SOC Lab - Splunk Environment
- Built a local SOC environment using Splunk for log analysis and attack pattern detection.

TryHackMe Practical Labs
- Completed SOC Level 1, Windows, Linux, and Network fundamentals with hands-on alert triage and incident response.

RADDAD
Smart Electrical Fault Prediction System
- Developed an AI-based model to predict electrical faults and improve power reliability.

Malware Detection System
- Built a Decision Tree model to classify Android apps as benign or malicious using static analysis.

SmartPath - Intelligent Educational Platform
Designed an AI-powered adaptive learning platform focused on personalized learning and modern UI/UX design.

Education

Bachelor of Science in Information Security
University of Hail
2022 – 2026 | Hail, Saudi Arabia
Expected Graduation: 2026
GPA: 3.57 / 4

Skills

Technical Skills
- **Programming & Scripting:** Java, SQL
- **Web Development:** HTML, CSS
- **Operating Systems:** Windows, Linux, Kali Linux
- **Networking & Log Analysis:** Firewall log analysis, DNS analysis
- **SIEM Tools:** Splunk, RSA NetWitness, LogRhythm, IBM QRadar
- **Threat Intelligence & Detection:** YARA, Sigma, Group-IB, IOC tracking, MITRE ATT&CK mapping
- **SOC Operations:** Alert triage, Incident response, SIEM content tuning, False positive reduction, Use case creation

Soft Skills
- Analytical thinking and problem-solving
- Research and information gathering
- Teamwork and time management

Volunteer Experience

AI Club - University of Hail
2025 – Present
- Designed UI/UX and visual content for AI projects.

Aj'a Space Initiative
2024 – 2025
- Conducted cybersecurity research and awareness reports.
- Awarded the title Aj'a Space Community Ambassador.

Artwaa Platform
2023 – 2024
- Contributed to UI/UX design projects and earned a certificate of appreciation.

Languages

- Arabic
- English