Ahmed Mohamed Zamzam

SOC Team Lead

✉ Ahmadzamzam1997@gmail.com ☎ +201009635963 Cairo, Egypt

linkedin.com/in/ahmedmzamzam

PROFILE

Passionate about mentoring SOC analysts, threat-hunting methodologies, and aligning cybersecurity strategies with business objectives to improve overall security posture.

WORK EXPERIENCE

05/2023 – present

IP Protocol INC
SOC Team Lead

- **Lead and mentor** a team of SOC analysts, enhancing their technical expertise in threat detection, incident response, and threat hunting.
- **Manage daily SOC operations**, ensuring 24/7 security monitoring, incident triage, and escalation to mitigate potential threats efficiently.
- **Developed and optimized SOC** procedures, reducing false positives and enhancing incident response effectiveness.
- **Conduct proactive threat hunting**, leveraging **SIEM, EDR, TIP** and intelligence feeds to identify and neutralize advanced persistent threats (APTs).
- **Administer and maintain the SIEM platform**, ensuring optimal performance, scalability, and uptime.
- **Troubleshoot log sources issues**, ensuring seamless data flow and visibility for SOC analysts.
- **Integrated threat intelligence into** SOC workflows, improving detection accuracy and response
- **Collaborated with IT and security teams** to align security strategies with business objectives.
- **Prepared and delivered security reports** to executive leadership, providing actionable insights into emerging threats and security trends.

09/2022 – 05/2023

IP Protocol INC
SOC Analyst Tier 2

- **Responded to security incidents** by analyzing alerts, investigating threats, and escalating critical issues to minimize impact.
- **Created, fine-tuned, and assessed detection rules** in **QRadar SIEM**, improving threat detection accuracy and reducing false positives.
- **Assessed log sources** to ensure proper data ingestion, correlation, and visibility across network, endpoint, and cloud environments.
- **Integrated new log sources into QRadar**, configuring log ingestion, parsing, and normalization to enhance security event detection.
- **Performed Purple Team exercises**, collaborating with offensive security teams to test and improve detection capabilities against real-world attack scenarios.
- **Documented incident response processes**, ensuring knowledge transfer and continuous improvement within the SOC team.

06/2021 – 09/2022

IP Protocol INC
SOC Analyst Tier 1

- **Monitored security events and alerts** using SIEM QRadar to detect potential threats and suspicious activities.
- **Investigated security incidents**, analyzing logs, correlating events, and escalating critical threats to senior analysts for further action.
- **Generated and delivered operational reports** on security trends, incident findings, and SOC performance metrics.
- **Conducted threat intelligence activities**, gathering, analyzing, and integrating Indicators of Compromise (IOCs) into SOC workflows.
- **Created custom dashboards** in SIEM platforms, providing enhanced visibility into security events, threat trends, and operational performance.
- **Documented security incidents and investigation findings**, contributing to SOC knowledge sharing and continuous improvement.

EDUCATION

2015 – 2020

Bachelor of Communication and Computer Engineering
Faculty Of Engineering Helwan University

Graduation Project
Monitoring and analyzing system for cardiac data using ECG signals

WEB Development Intern
Udacity

Intern at Udacity WEB Developer Nanodegree Program

CERTIFICATES

Digital Forensics Professional (eCDFP)
eLearn Security (INE)

Splunk fundamentals 1
Splunk

Threat Hunting Professional (eCTHP)
eLearn Security (INE)

Incident Responder (eCIR)
eLearn Security (INE)

SKILLS

Experience in SIEM

- QRadar
- Splunk
- ELK

SIEM Administration

- QRadar

Experience in Scripting & Coding

- C
- C++
- Python
- Java
- Powershell

Experience in EDR

- FireEye Hx
- Fidelis
- SentinelOne

Experience in Vulnerability management

- Tenable

Experience in threat intelligence

- SOCRadar
- ThreatQ

Knowledge of Network Solutions

- Forcepoint
- Fortigate
- PaloAlto
- SonicWall
- F5

LANGUAGES

Arabic — Native/Bilingual

English — Fluent