Ismael Gaton

Data Analyst

ismaelgatongg@gmail.com

+34 637614010

Gliwice, Poland

https://www.linkedin.com/in/ismael-gaton-32651a238/

https://tryhackme.com/p/ismaelggm

github.com/ismaelggm1

LANGUAGES

Spanish ●●●●●

English ●●●●○

Polish ●●○○○

CERTIFICATES

- Google Cybersecurity Professional
- Soc Level 1 (Tryhackme)
- Jr Penetration Tester (Tryhackme)

SKILLS

- Vulnerability Assessment and Remediation
- Strong problem solving & attention to detail
- Incident Handling
- SIEM & Log analysis: Splunk, Qradar, Sentinel
- Network & Firewalls (Palo Alto), IDS/IPS (Snort, Suricata, Zeek)
- Malware analysis and digital forensics
- Endpoint & threat detection: CrowdStrike, SentinelOne

ABOUT ME

Aspiring SOC Analyst with hands-on experience in threat detection, incident response, and SIEM tools. Actively preparing for **CompTIA Security+**, completing daily labs and challenges on **TryHackMe** and **LetsDefend**, gaining practical exposure to blue team operations and log analysis. Strong foundation in monitoring, vulnerability assessment, and proactive threat hunting.
Check my Github link for my personal projects about SOC analyst

PROFESSIONAL EXPERIENCE

Data Analyst
Microsoft
10/2024 – Present | Poland (Remote)

- Monitored and processed large volumes of data, applying statistical analysis to detect irregularities and trends
- Conducted data validation and quality checks, ensuring reliable inputs for analysis and security decision-making.
- Prepared clear, actionable reports from complex datasets, enabling efficient identification of anomalies and supporting incident response.
- Hands-on experience with relational databases and large datasets, useful for correlating events and supporting investigations in security operations.

Data Annotator
THOTH AI
04/2025 – 10/2025 | Poland (Remote)

- Analyzed and labeled large datasets with precision, ensuring high-quality outputs
- Identified patterns, inconsistencies, and quality issues, assisting in problem resolution
- Collaborated with internal teams and clients to align on policy guidelines, reinforcing experience with security policies, standard operating procedures, and compliance practices.
- Provided actionable feedback to improve processes

Finance and Accounting
Capgemini
06/2022 – 10/2024 | Poland, Katowice

- Managed client accounts and performed regular reconciliations, honing attention to detail and accuracy
- Handled sensitive information and escalated discrepancies, reinforcing skills in risk identification and compliance.
- Collaborated cross-functionally with teams to streamline processes and implement improvements, demonstrating analytical thinking and operational efficiency

PROJECTS

Vulnerability Assesment Lab

- Set up and configured Windows virtual machine on Virtualbox.
- Installed and configured Nessus vulnerability scanner on the VM
- Conducted comprehensive vulnerability scans using Nessus, including credential scans.
- Identified and analyzed vulnerabilities in the system and installed vulnerable software for testing purposes.
- Developed and implemented effective remediation strategies to address indentified vulnerabilities.

Multi Honeypot Platform

- Deployed T-Pot on Azure Cloud to enchance security measures
- Configured virtual machine and network to support the installation and operation of the T-Pot
- Monitored and analyzed honeypot data to detect and respont to potential cyber threats
- Gained experience with cloud security configurations, intrusion detection, and proactive threat monitoring.

Microsoft Sentinel SIEM

- Successfully deployed Microsoft Sentinel a Siem solution in Azure Cloud.
- Implemented advanced techniques and configurations to enhance the SIEM solution's threat detection capabilities
- Created customer analytics rules using KQL to enable the detection of specific security events and patterns.
- Conducted incident investigations using SIEM tools and techniques to analyze cybersecurity indicents
- Implemented remediation actions to mitigate and resolve indentified cybersecurity incidents

Password Management System in AWS

- Created Passbolt, a self-hosted password manager, to securely store and manage complex passwords.
- Utilized AWS cloud services to host Passbolt, ensuring scalability, availability and reliability
- Implemented HTTPS encryption to safeguard sensitive data transmitted to and from the password manager.
- Configured and maintained the domain hosting for the password manager, ensuring accessibility and securit.
- Provided funcionality within Passbolt, for secure storage of comples passwords, enhancing data protection and user convenience

AI Enabled Incident Response Automation

- Developed a ChatGPT solution on the Azure Cloud platform designed to enhance cybersecurity indicent management.
- Implemented strict access controls and persmissions ensuring a secure enviroment for handling sensitive incident data and response activities.
- Conducted necessary fine-tuning and optimizations to maximize AI performance, ensuring its ability to deliver valuable insights and recommendations.
- Created an automation within the SIEM system to seamlessly integrate AI andstreamline overall cybersecurity operations.