



OMAR MALAS

Cyber Security Defense Analyst - SoC Analyst

📍 Zagreb, 21 10000 ✉️ omarmalas.1561999@gmail.com

PROFESSIONAL SUMMARY

Cybersecurity professional with thorough understanding of threat landscapes and defensive measures. Recognized for ability to quickly identify security breaches and implement timely solutions. Highly collaborative, known for working effectively within teams and adapting to evolving security challenges, bringing strong analytical and problem-solving skills to table. Experienced with monitoring and analyzing security events to protect organizational assets. Utilizes strong analytical skills to identify threats and vulnerabilities. Knowledge of cybersecurity protocols and effective incident response techniques, ensuring robust defense against potential breaches.

WEBSITES, PORTFOLIOS, PROFILES

- <https://www.linkedin.com/in/omar-malas-5a9541206/>
- <https://www.credly.com/badges/e60a8e4c-f9ef-4ca5-b306-31f43008987a>
- <https://github.com/omarmalas>

WORK HISTORY

CYBER SECURITY DEFENSE ANALYST INTERN

06/2024 to 12/2024

PwC | Remote

- Maintained accurate documentation of all SOC activities, facilitating knowledge sharing across the organization.
- Reduced false alarms by fine-tuning intrusion detection system configurations based on historical analysis of incidents.
- Implemented automated tools for continuous monitoring of system logs, reducing manual efforts by the team.
- Enhanced network security by monitoring systems for potential threats and vulnerabilities.
- Identified root causes of security breaches through thorough investigation and analysis of log data.

CYBER SECURITY WEBINAR COORDINATOR

01/2020 to 01/2023

IronPath | Remote

- In my role as a Cyber Security Webinar Coordinator at IronPath, I was responsible for inviting companies to attend our cyber security webinars
- My main responsibilities included:
- Identifying and reaching out to potential attendees through various channels such as email, LinkedIn, and phone calls
- Creating and sending out personalized invitations
- Following up with potential attendees to ensure they received the invitations and answering any questions they may have

EDUCATION

- Coordinating with the marketing team to create promotional materials and social media posts
- Tracking responses and attendance for each webinar
- Providing feedback and suggestions to improve future webinars
- I have developed a good understanding of the cyber security industry and the companies that are interested in attending webinars
- I had the opportunity to work closely with the marketing and sales team which helped me to build my communication and teamwork skills
- I was able to successfully increase attendance at our webinars and received positive feedback from attendees

The Art of Investigation | SIEM

01/2025 to CURRENT

Splunk, Remote

Understanding the Investigation Process

- Defined the purpose and scope of an investigation
- Identified key stakeholders (SOC analysts, incident responders, forensic teams)
- Differentiated between proactive and reactive investigations

Using Splunk for Investigations

- Understood the role of **Splunk Enterprise Security (ES)** in threat detection
- Learned how to use the **Incident Review Dashboard** for triaging security events
- Used **Investigation Workbench** to track incidents and analyze artifacts
- Worked with notable events and risk-based alerting (RBA)

Threat Intelligence and Data Enrichment

- Utilized **Threat Intelligence Framework** to enrich security events
- Applied **LOOKUP** and **ASSET & IDENTITY** frameworks for context
- Correlated events across different data sources using Splunk SPL

Advanced SPL Techniques for Investigations

- Used **TSTATS** for efficient data searches
- Applied **TRANSACTION** to group related events
- Extracted critical details using **REX** and **EVAL**
- Used **LOOKUP** to enrich data with external threat feeds

Investigative Workflows & Best Practices

- Followed a structured approach: **Detection - Triage - Investigation - Containment**
- Maintained proper documentation for each investigation
- Leveraged Splunk's built-in playbooks for common threats
- Used Splunk dashboards and reports to communicate findings

Hands-on Practice & Real-world Scenarios

- Worked on simulated incidents in Splunk ES
- Investigated phishing, malware, and insider threats using Splunk
- Identified patterns in logs and alerts using correlation searches

Certificate CompTIA Security+ | Security+

01/2025 to CURRENT

CompTIA, Remote

- Building foundational knowledge in network security, threat management, and cryptography.
- Gaining expertise in identity and access management, vulnerability management, and incident response.
- Learning to implement and monitor security controls for systems and networks.
- Preparing for certification exam and aiming to gain proficiency in industry standards and best practices for securing systems and data.

Certificate Cyber Threat Detection And Analysis | 01/2025 to 01/2025
Cyber Threat Detection And Analysis

Splunk, Remote

- Gained expertise in identifying and analyzing cyber threats using advanced detection tools and methodologies.
- Developed skills in threat intelligence, intrusion detection systems (IDS), and log analysis.
- Learned proactive threat hunting techniques to identify and mitigate potential security risks.
- Acquired hands-on experience in incident response strategies to manage and contain cyber incidents.
- Enhanced ability to strengthen organizational defenses against evolving cyber threats.

Certificate (SC-900) | Security, Compliance And Identity 07/2022 to 08/2022
Fundamentals (SC-900)

Microsoft, Remote

Gained foundational knowledge of security, compliance, and identity principles within cloud-based environments, particularly Microsoft solutions. Demonstrated understanding of core security and compliance concepts, including Microsoft 365 security features and Azure security solutions. Learned the essential components of identity management using Azure Active Directory (Azure AD), ensuring the implementation of robust identity and access management (IAM) protocols.

Developed knowledge of Microsoft compliance tools, including Compliance Manager, Microsoft Information Protection, and Microsoft Defender.

Gained skills in protecting sensitive data through policies, encryption, and data loss prevention (DLP).

Acquired knowledge on identity protection, including multi-factor authentication (MFA), conditional access, and identity governance.

Familiarized with Security Operations processes, helping organizations effectively manage and mitigate security risks.

Developed a basic understanding of security governance frameworks and industry standards for compliance, including ISO/IEC 27001 and GDPR.

Bachelor's Degree | Cyber Security 10/2019 to 02/2024

The World Islamic Science And Education University, Remote

- Gained a comprehensive understanding of network security, cryptography, incident response, ethical hacking, and risk management.

- Completed hands-on projects involving penetration testing, firewall configuration, and vulnerability assessments.
- Studied security protocols, data protection, and security governance to build a strong foundation for securing systems and networks.
- Participated in hands-on projects, including designing and implementing a secure network for a local business, applying theoretical knowledge to real-world scenarios.

Current GPA: 3.0

PROJECTS

1) Project Title: Virtual Environment Penetration Testing and Log Analysis

- **Description:** Developed a controlled virtual environment to simulate cyber-attacks using Metasploit, analyzed system logs with Splunk, and implemented remediation strategies to enhance security posture.
- **Key Activities:**
- **Environment Setup:** Configured a virtual lab environment using Metasploitable, an intentionally vulnerable Linux distribution, to serve as the target system.
- **Vulnerability Exploitation:** Utilized Metasploit Framework to identify and exploit known vulnerabilities, such as: **VSFTPD v2.3.4 Backdoor:** Exploited a backdoor vulnerability in the VSFTPD service to gain unauthorized shell access.
Unpatched Samba Service: Leveraged a vulnerability in the Samba service to execute arbitrary code remotely.
- **Log Collection and Analysis:** Ingested system and application logs into Splunk to monitor and analyze malicious activities. Created dashboards to visualize attack patterns and identify indicators of compromise.
Performed searches to correlate events and trace the attacker's actions.
- **Remediation and Hardening:** Implemented security measures to mitigate identified vulnerabilities: Applied necessary patches and updates to vulnerable services.
Configured firewall rules to restrict unauthorized access.
Enhanced logging and monitoring to detect future intrusion attempts.

2) Project Title: Simulated Cyber Incident Response

- Deployed and configured SIEM platforms, including **Splunk** and Microsoft Sentinel.
- Used tools like **Splunk** to simulate and respond to security incidents, including phishing, ransomware, and DDoS attacks.
- Documented the entire incident response process, including detection, analysis, containment, eradication, and recovery.
- Correlated events to detect anomalies and potential breaches, improving threat detection efficiency.
- Built and participated in cyber range exercises to simulate attacks based on the **MITRE ATT&CK** framework.

- Improved response strategies by analyzing tactics, techniques, and procedures (TTPs) used in simulated attacks.
- Built custom dashboards, alerts, and reports to detect suspicious activities and enhance visibility across networks.

3) Project Title: Network Traffic Analysis Lab

- Captured and analyzed network traffic using **Wireshark** and **tcpdump**.
- Identified patterns, anomalies, and potential threats, such as malware-infected packets and unauthorized access.

4) Project Title: Vulnerability Management Program

- Set up a vulnerability management process using tools like **Nessus** and **OpenVAS**.
- Conducted scans, prioritized vulnerabilities, and implemented remediation measures to minimize security risks.

5) Project Title: Active Directory Hardening Project

- Enhanced Active Directory security by implementing **Restricted Admin Mode**, **Admin Tiering**, and **LAPS** (Local Administrator Password Solution).
- Conducted regular audits and applied hardening techniques to minimize attack surface.

6) Project Title: Python Web Scanning Tool

Description: Developed a Python-based web scanning tool designed to identify vulnerabilities in web applications.

Key Features:

- **URL Scanning:** Analyzes specified URLs to detect potential security issues.
- **Template Utilization:** Employs predefined templates to standardize scanning processes.
- **Wordlist Integration:** Incorporates wordlists to enhance the detection of common vulnerabilities.
- **Database Management:** Manages scan results and configurations using a structured database system.

Project Link: <https://github.com/omarmalas/python-web-scanning-tool>

7) Project Title: PS-PortProbe

Description: Created a PowerShell script to perform efficient port scanning, aiding in network security assessments.

Key Features:

- **Port Scanning:** Probes specified IP addresses to identify open TCP ports.


- **Asynchronous Operations:** Utilizes asynchronous processing to enhance scanning speed and efficiency.
- **Result Reporting:** Generates detailed reports of open ports and associated services.

Project Link: <https://github.com/omarmalas/PS-PortProbe>

SKILLS

- Vulnerability Assessment
- Knowledge of Cyber Defense Systems
- Problem solving
- Digital forensic
- Proficiency in Python programming.
- Proficiency in PowerShell scripting.
- Ability to design and implement automated security tools.
- Expertise in log analysis and visualization with Splunk.
- Threat Analysis
- Communication
- Cyber Threat Detection and Analysis
- SIEM management
- SQL
- Knowledge of network protocols and port scanning methodologies.
- Proficiency in using Metasploit for penetration testing and exploit development.

LANGUAGES

Arabic Native language
English C2

Proficient