# Jordan John-Phillip | Cyber Security PM

Location: London
Phone: 07919895059
Email: jordanjp1@hotmail.co.uk
LinkedIn URL: https://www.linkedin.com/in/jordan-john-phillip

## Professional Profile

A highly skilled Agile professional with a first-class honours degree in Project Management, I specialize in delivering design, development, and implementation projects for regulated B2C firms in the UK. My expertise spans Agile and Waterfall methodologies, covering all project phases, including requirements gathering, workshop delivery, testing, and handovers. Experienced with SDLC, GCP, SIEM environments and edge computing, I am proficient in tools like Splunk, Elastic, Virtual Machines, and VPNs. I integrate Machine Learning (LLM) and AI (LLM) solutions, and I excel in Microsoft Office, Cyber Essentials, CyberArk, and managing integration projects. My goal is to deliver exceptional results with strong communication and stakeholder engagement.

## Core Skills

- **Hashing, Nmap, Encryption, Cryptology, Syslog, Linux, GitHub.**
- Agile & Waterfall (Project Management)
- Project Management **(1st Class Honours Degree)**
- MS Teams Suite, Edge Computing.
- **Splunk, Elastic, Virtual Box, Virtual Machines. Event Viewer, VPN's.**
- Machine Learning - LLM.
- Artificial Intelligence - LLM.
- Microsoft Office (Excel, Word PowerPoint)
- **Cyber Essentials, CyberArk.**
- **Top 12% Platform Ranking** on TryHackMe**.**
- Integration Projects
- Communication Skills.
- **SIEM, Linux & Ubuntu.**
- **GCP, SIEM, ISO 27001.**

## Project Labs

**Building my Own SIEM or SOC - IDS Environment**

- **Objective:** Develop a Security Information and Event Management (SIEM) or Security Operations Center (SOC) with an Intrusion Detection System (IDS).

**Approach:**

- Set up a virtual lab environment using VirtualBox and configure multiple virtual machines to simulate a network.
- Installed and configured IDS tools like Snort and Suricata on network nodes.
- Integrated the IDS with a centralized SIEM platform to collect and analyze security events.
- Implemented log collection using syslog and monitored real-time network traffic for anomalies.
- Tested the environment by generating various types of network attacks and verified IDS detection and SIEM alerting capabilities.
- Outcome: Successfully created a functional SIEM/SOC environment capable of detecting and responding to security incidents.

**Navigating and Responding to Security Incidents within the Splunk Platform**

- **Objective:** Enhance skills in navigating the Splunk platform and responding to security incidents.

**Approach:**

- Set up a Splunk environment and indexed logs from various sources including firewalls, IDS, and endpoint security tools.
- Developed custom dashboards and alerts to monitor critical security events.
- Created search queries to identify suspicious activities and potential security breaches.
- Simulated security incidents and conducted incident response drills to practice investigation and remediation steps within Splunk.
- Documented the incident response procedures and created playbooks for common security scenarios.
- Outcome: Improved proficiency in using Splunk for incident detection and response, and developed standardized procedures for handling security incidents.

**Building Your Own SIEM or SOC - IDS Environment**

- **Objective:** Develop a Security Information and Event Management (SIEM) or Security Operations Center (SOC) with an Intrusion Detection System (IDS).

**Approach:**

- Set up a virtual lab environment using VirtualBox and configure multiple virtual machines to simulate a network.
- Installed and configured IDS tools like Snort and Suricata on network nodes.
- Integrated the IDS with a centralized SIEM platform to collect and analyze security events.

- Implemented log collection using syslog and monitored real-time network traffic for anomalies.
- Tested the environment by generating various types of network attacks and verified IDS detection and SIEM alerting capabilities.
    - Outcome: Successfully created a functional SIEM/SOC environment capable of detecting and responding to security incidents.

**Masterschool - Cyber Security Program**
Aug 2023 – June 2023 - Activities and societies: 9 Training Units

**TF101**
Tech Foundations
Aug 7 - Sep 3

**CY102**
Cyber, Windows, and Linux
Sep 4 - Oct 1

**CY103**
Networking and Cryptography
Oct 2 - Oct 29

**CY104**
Windows Administrator
Oct 30 - Nov 26

**CY105**
Cybersecurity Beginner
Nov 27 - Dec 24

**CY106**
Cybersecurity Intermediate
Dec 25 - Jan 21

**CY107**
Cybersecurity Advanced
Jan 21 – Mar 15

**CY108**
Cybersecurity Advanced
Mar 21 – April 25

**CY109**
Cybersecurity Advanced
April 25 – June 30

**Cyber Security Course Breakdown:**

- **Objective:** Defend organizations: from cyber attacks in an ever-evolving, sophisticated and hidden digital world:

**Approach**:

- OS & networks architecture and security
- Implementing security solutions
- Threat intelligence and host security
- Digital forensics and risk management
- Cutting edge “AI related” topics
- CompTIA Security+ exam prep and voucher.
- CEH, AWS Certified Cloud Practitioner and Microsoft Azure Administrator certificates prep.

## Technical Skills & Vocational Qualifications

- **7 Month Masterschool Cyber Security Analyst Program** (Completing in June 2024)
- Business Management with Project Management **(1st Class Honours Degree)**

## Certifications

- CyberArk Certification with IAM & PAM Guidelines – Udemy
- The Complete Splunk Core Certified User Course - SPLK-1001 - Udemy
- AZ-900 Microsoft Azure Fundamentals – Cybrary
- AWS Cloud Practitioner – Cybrary
- Cybersecurity Roles, Processes & Operating System Security - Coursera / IBM