Jordan John-Phillip | Cyber Security Analyst

Location: London | 07919895059 | jordanjp1@hotmail.co.uk | My LinkedIn | My Portfolio |

Professional Profile

Proven experience as a Project Cyber Security Analyst from large-scale organizations, identifying and mitigating cyber risks. Expertise in cybersecurity management, risk assessment methodologies, and managing risks within business appetite. Proficient in assessing and mitigating controls across various technologies and data flows. Familiar with ISO 27001 and Cyber Essentials (Audits), with strong communication and presentation skills. Able to convey complex technical risks in clear, commercial language.

Core Skills

- **Agile & Waterfall**
- (Project Management)
- **RAID, RACI, RASCIO & Action Trackers.**
- SDLC, GCP.
- JIRA (Confluence).
- **Exercises Playbooks.**
- CCTV - Cameras (DWGs) Reviews.
- **DBS and SC Cleared. (DV Clearance upon request)**
- **Log & PCAP Analysis.**
- Communication Skills.
- **RAID, RACI, RASCIO &** Action Trackers.
- **Mitre ATT&CK,** TTPs.
- **Splunk –** Reports, Dashboards.
- **IR – Incident Response and ID – Incident Detection.**
- Event Viewer, Active Directory.
- **Cyber Detection.**
- Autodesk (DWGs), VPN's.
- **Cyber Detection.**
- **CSIRT Policies.**
- Machine Learning - LLM.
- **OSI Stack.**
- Artificial Intelligence - LLM.
- **FIA/NSI/LPCB/C&G**
- OWASP, CVSS etc.
- **Project Management (1st Class Honours Degree)**
- **Playbooks Policies.**
- Supplier Assurance.
- Microsoft Office (Excel, Word PowerPoint).
- **Cyber Essentials, CyberArk, APIs,**
- **SIEM**, Linux & Ubuntu.
- Client VDI Access.
- **ISO270001, PCI DSS, GDPR, NIST Framework Compliance.**

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 analyse 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.

Jan 2024 to June 2024 - Role Title: Security Operations Analyst
Company Name: QCIC

- Minimized cybersecurity incident damage and coordinated recovery efforts by 15%, preventing future incidents. Monitored and analysed security controls and alerts, managing incidents according to policies. Investigated and resolved complex security issues, enhancing situational awareness by 20% through reports and dashboards. Provided security guidance and managed security tools, ensuring compliance and continuous improvement by 10%.

Business Management with Project Management Degree – Grade 1st Class Honours

Nov 2021 to Nov 2022 - Role Title: Project Manager Intern / Contractor Role.
Company Name: Qumind

- Worked in the Customer Success Team at Qumind, managing projects for clients like Guardian and Nestle. Led testing, and improved translation edits by 15%, and improved website changes by 25% while collaborating using Google tools. Achieved Employee of the Month (Feb 2022) and contributed to cybersecurity practices through senior management meetings increasing security practices by 20%.

March 2021 to Oct 2021 - Role Title: Junior Project Manager
Company Name: Sharpshot Digital

- Supported Sharpshot Digital's digital transformation efforts, delivering bespoke process improvement projects for startups. Led project control by managing and improving RAID logs by 10%, facilitated and improved discovery sessions using Jira by 20%, and coordinated key meetings. Managed workload and daily stand-ups provided project support during sprints and enforced best practices in reporting and improved quality assurance by 25%.

Jun 2014 to Jun 2018 - Role Title: Project Manager/ Business Owner
Company Name: Jordan JP Plastering

- Produced schedules in MS Project to prioritize and improve critical tasks by 25%, managed RAID logs, and created stakeholder maps. Demonstrated in-depth knowledge of housing services and performed initial client assessments to increase client base by 30%. Developed business cases for funding and underwent procurement processes and improving company systems by 15%. Achievements include exceptional service delivery, increased client satisfaction, and a 10% annual growth in client portfolio.

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

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

Certifications

- Official ISC2 CC Certification - ISC2
- Official ISC2 GRC Certification – Supply Chain Risk Management (SCRM) through Governance, Risk, and Compliance (GRC) – ISC2
- CyberArk Certification with IAM & PAM Guidelines – Udemy
- The Complete Splunk Core Certified User Course - SPLK-1001 – Udemy
- APIs and RESTful APIs Crash Course – Udemy
- PCI DSS Compliance Certification – Udemy
- AZ-900 Microsoft Azure Fundamentals – Cybrary
- AWS Cloud Practitioner – Cybrary