# Oladotun Joseph - Cybersecurity Engineer

Ottawa, ON | 6132661783 | ojebode@gmail.com | https://www.linkedin.com/in/oladotun-joseph/
https://www.oladotun.space/

## SUMMARY & HIGHLIGHTS

A **Cybersecurity SOAR Engineer** with 7+ years of experience designing and implementing security orchestration and automation workflows within enterprise SOC environments.

- ❖ Spearheaded SOAR engineering for clients' SOC implementations.
- ❖ Architects large-scale, automation-driven SOC capabilities using SOAR technologies.
- ❖ Transforms security challenges into practical automation solutions through creativity, collaboration, and communication.

## SKILLS

- SOAR Platforms: FortiSOAR (CyberSponse), Chronicle SOAR (Siemplify)
- Automation & Integration: SOAR Playbook Development, Workflow Automation, API Integrations (REST), SOAR Connector Development, Security Tool Integration, Task Scheduling (Crontab)
- Security Operations: Incident Response, Threat Detection, Security Event Analysis
- Programming & Scripting: Python, Jinja, Regex
- Data Platforms: Elasticsearch, Solr, MongoDB
- SIEM: RaptorX, Wazuh
- Cloud: AWS
- Security Frameworks: MITRE ATT&CK, Cyber Kill Chain, Diamond Model, Pyramid of Pain
- Operating Systems & Networking: Linux, Windows, TCP/IP, OSI Model
- Security Testing Tools: Kali Linux, Vulnerability Assessment Tools
- Analytical Problem Solving
- Attention to Detail
- Communication & Stakeholder Engagement
- Cross-functional Collaboration
- Ownership & Accountability
- Adaptability

## PROFESSIONAL EXPERIENCE

**Cybersecurity Engineer (SOAR & Security Automation)** **Nov 2018 – June 2026**
Maguire Security Solutions (Mubadala, Injazat, UAE Federal Ministry)

- Lead the deployment and engineering of enterprise SOAR capabilities supporting SOC operations for large-scale environments, improving investigation efficiency and operational consistency across security workflows.
- Designed and implemented 100+ SOAR playbooks that automated triage, enrichment, and investigation workflows, processing ~200 daily alerts and generating 350,000+ executions in 17 months, while reducing manual analyst workload by ~60% and accelerating MTTR by ~50%.
- Developed SOAR connectors and integrations across detection, CTI, and telemetry platforms (e.g., CrowdStrike, ForeScout, Endgame, Elasticsearch, Solr, MongoDB), collaborating closely with security architects, detection engineers, and operational teams to ensure automation pipelines integrated seamlessly into broader SOC workflows.
- Engineered custom automation modules in CyberSponse SOAR platform to support GSOC operations across 10 onboarded tenants, enabling multi-tenant orchestration and MongoDB-based data handling.
- Applied threat intelligence and detection validation techniques to improve alert fidelity and reduce false positives across SOC investigations by ~25%, collaborating with detection engineers to identify process gaps and drive targeted playbook improvements.

- Architected multi-stage SOAR pipelines for indicator extraction, enrichment, and investigative workflows, automating triage for ~200 daily security detections and significantly reducing manual SOC analysis effort.
- Automated investigation and response actions using Python and Jinja, improving investigation and remediation speed by ~50% faster.
- Built proactive threat-hunting playbooks leveraging security telemetry and intelligence feeds, partnering with the threat hunting team to develop and update workflows addressing new attack vectors.
- Trained SOC analysts on SOAR platform operations, enabling consistent execution of automated incident response workflows and improved alert triage efficiency.

**Network Security Engineer -** Sanitas Data Security **July 2016 – Dec 2016**

- Reviewed the information security policy of client systems and networks.
- Implemented secure configuration of boundary firewall and internet gateways to enhance enterprise network security posture.
- Performed vulnerability assessment on client's network with Kali Linux tools and recommended remediation measures.
- Ensured client compliance with Cyber Essentials by implementing five key technical controls: Firewall, Secure Configuration, Access Control, Malware Protection, and Patch Management.

## EDUCATION (WES-Assessed – Canadian Equivalency)

**MSc Information Security & IT Management (1st class)** **2015 – 2016**
Edge Hill University (UK)

**BSc IT \ Networking and Security (1st class)** **2010 – 2014**
Ajman University of Science & Technology (UAE)

## CERTIFICATIONS

| | |
|---|---|
| CISSP, ISC2 | **2026** |
| CompTIA CSAP, CySA+ | **2022** |
| CompTIA Security+ | **2020** |
| CCIE (Security version 5 written) | **2017** |
| CCNP (Routing and Switching) | **2016** |
| CCNA (Routing and Switching) | **2014** |

## PROFESSIONAL DEVELOPMENT

- Built and maintained personal cybersecurity lab environments for hands-on exploration of SOC and SOAR technologies, including Wazuh and Shuffle.
- CompTIA SecAI+ – AI security, AI-driven security operations, and AI risk & governance (Ongoing Courses on Udemy)
- French – Beginner (Ongoing Courses on Udemy)