

Joseph Ojebode

Cybersecurity SOAR Engineer

Ottawa, Ontario

(613) 266-1783

ojebode@gmail.com

[LinkedIn](#) | [Personal Website](#)

PROFESSIONAL SUMMARY

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

- Spearheaded SOAR engineering for clients' SOC implementations.
- Architected large-scale, automation-driven SOC capabilities using SOAR technologies.
- Transformed security challenges into practical automation solutions through creativity, collaboration, and communication.
- Core Competencies: Analytical Problem Solving, Cross-functional Collaboration, Communication & Stakeholder Engagement, Continuous Learning & Curiosity

TECHNICAL & PROFESSIONAL SKILLS

- SOAR Platforms: FortiSOAR (CyberSponse), Chronicle SOAR (Simplify)
- Automation & Integration: SOAR Playbook Development, Workflow Automation, API Integrations (REST), SOAR Connector Development, Security Tool Integration, Task Scheduling (Crontab), Ansible (Lab)
- 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: Incident Response Frameworks (NIST, SANS), 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

WORK EXPERIENCE

Cybersecurity Engineer (SOAR & Security Automation)

Nov 2018 – June 2026

Maguire Security Solutions (Dubai, UAE)

- Led the deployment and engineering of enterprise SOAR capabilities across secure SOC environments, configuring platforms and automation workflows to meet operational and security requirements.
- Designed and implemented 100+ SOAR playbooks automating alert triage, enrichment, investigation, and response, processing ~200 daily alerts and 350,000+ executions in 17 months while reducing manual analyst workload by ~60% and accelerating MTTR by ~50%.
- Developed SOAR connectors across detection, CTI, and telemetry platforms (e.g., CrowdStrike, ForeScout, Elasticsearch, Solr, MongoDB), collaborating with security architects, detection engineers and operations teams to embed automation seamlessly into end-to-end SOC workflows.
- Engineered reusable playbook components in CyberSponse SOAR to identify, segregate and route detections across 10 GSOC tenants, enabling multi-tenant orchestration and MongoDB-based data handling.
- Applied threat intelligence and detection validation techniques to improve alert fidelity and accelerate false-positive disposition by ~25%, partnering with detection engineers to address process gaps and optimize playbooks.

- Automated investigation and response actions using Python and Jinja, improving investigation and remediation speed by ~50%.
- 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.
- Developed and maintained technical SOAR documentation covering data-flow architecture, connector configurations, and playbook catalogues, providing an operational reference for platform support, maintenance, and knowledge transfer.

Network Security Engineer

July 2016 – Dec 2016

Sanitas Data Security (Manchester, England)

- Implemented secure configurations for boundary firewalls and internet gateways, and assessed client networks for vulnerabilities using Kali Linux tools.
- Supported Cyber Essentials compliance by implementing five technical controls: firewall, secure configuration, access control, malware protection, and patch management.

EDUCATION (WES-Assessed – Canadian Equivalency) & TRAINING

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)

Professional Training – CCNA + CCNP + CCIE (Security)

Sep 2017 – Jan 2018

Network Bulls (Delhi, India)

CERTIFICATIONS

CompTIA SecAI+	2026
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 & ENGAGEMENT

- Rabitanoor | Part-time Contributor: Exploring Chakali's governed agentic AI platform and evaluating potential SOC automation use cases.
- French: Beginner (Ongoing learning)