DYLAN SHIELD

Accomplished DevSecOps Engineer with 3 years industry experience. Led a 5-member DevOps team and coordinated with upper management for the successful deployment of Elastic as the global SIEM platform, £80,000 under budget. Skilled security practitioner with an understanding of SIEM, vulnerability management, and architecture. Headed 3 key projects in Red Bee Media's digital transformation.

EMAIL
dylan@scioshield.uk

PHONE
[REDACTED]

WEBSITE
https://www.scioshield.uk

WORK EXPERIENCE

2018-10 - 2021-09

DevSecOps Engineer

RED BEE MEDIA, LONDON

SIEM

- Developed the high- and low-level architectural designs for the **Elastic** SIEM. At a cost reduction of 60% over the previous system.
- Communicated key milestones with RBM's Global Head of Technology and other high-level managers.
- The system ingests ~2 billion events per week and historic data for at least 6 months.
- Ran a series of productive threat hunts, liaised with the security team to resolve the findings.
- Created custom **Logstash**/**Elasticsearch** ingest pipelines for Juniper and Cisco security devices, with a +99.999% success rate against 4 billion events.
- Refined **Filebeat** increasing ingest speed by 100%.
- Developed custom **Kibana** security dashboards, facilitating real time observation of ~1,800 network events per second.
- To test the features of the **Elastic Agent**, in a malware analysis lab samples were injected on Windows with a 99% detection rate.
- Analysed the Agent with **Kali Linux** and **Caldrea** to demonstrate the capacity to detect unsigned adversarial behaviour on Windows and Linux with a 95% detection rate.

Vulnerability Management

- Deployed **Nessus** as the global vulnerability assessment platform to 9 sites.
- Collaborated with the architecture team to design the solution for a secure and expandable platform.
- The platform automatically scans 50,000+ assets, including key network, play-out, and domain infrastructure.
- Communicated high level vulnerabilities to management in a timely manner.
- Designed the patch methodology to remediate vulnerabilities based on risk posed to the business.
- Influenced the rollout of **Red Hat Satellite** by providing the risk assessment and security architecture.
- Secured the PostgresSQL backend and resolved challenges including NTP stratum server drift.

Monitoring

- Led a 3-member team to fulfil the design and delivery of **Prometheus**.
- Modernized RBM's monitoring capability at a cost reduction of £230,000/year versus the previous solution.
- Architected the solution; providing high-level diagrams, undertook a security assessment to mitigate all operational security requirements.
- Implemented, with **Ansible**, to both green field and existing infrastructure.

Networking

- Successful on time delivery of a Meraki WiFi solution to four key hubs across the UK.
- The WiFi serves 150+ employees with zero down time, three separate SSIDs for role segregation including a guest network.
- Over the course of the project key challenges needed resolution including DHCP split brain, RADIUS certificate authentication, and OSPF route forwarding failures.

EDUCATION

2015-09 - 2018-09

BSc in Ethical Hacking and Network Security, First-Class Honours Degree

COVENTRY UNIVERSITY, COVENTRY