**Zeshan Tariq**

**SOC - SRE - DEVOPS - SEC OPS - KUBERNETES - DOCKER**

**Contact Information**

* **e: zt@baa3.org**
* **w: zt.baa3.org**

**Profile**

**An Azure Certified DevOps Engineer with over 8 years of experience in various sectors including Government, Consultancy, Audit, and Finance. Skilled in application development, configuration management, and deploying to public clouds with open-source technologies. I've effectively bridged business and technology teams, defining requirements and translating them into specific software solutions.**

**In addition to my DevOps expertise, I bring a wealth of knowledge in Security Operations Center (SOC) practices and Site Reliability Engineering (SRE) principles. This includes experience in threat monitoring, security incident response, automation of production systems for reliability and performance, and ensuring system security and stability through rigorous testing and deployment methodologies.**

**Key Strengths**

* **Support software deployment using Kubernetes, AKS, Docker, and GitHub Actions, creating procedures to minimize technical incidents.**
* **Deliver CI/CD pipelines, IAC using Terraform, and collaborate with development, test, and product teams for defect root cause analysis.**
* **Implement project changes, possessing extensive skills in analysis, development, and reporting.**
* **Confidently communicate with clients, leading software deployment projects to enhance user experiences and improve service in line with operational objectives.**

**Professional Experience**

**Azure SecOps Engineer - DEFRA (Department for Environment, Food and Rural Affairs)**

**From: April 2024 – Current**

* **Threat Detection & Hunting: Proactively hunted for threats across Azure cloud environments using Azure Sentinel and Microsoft Defender for Cloud. Utilized advanced analytics and custom KQL queries to uncover indicators of compromise (IOCs) and detect anomalous behavior.**
* **Real-Time Alerting & Triage: Monitored security alerts and telemetry data, prioritized incidents based on severity and impact, and performed initial triage and investigation. Tuned detection rules to reduce false positives and improve signal-to-noise ratio.**
* **Automated Remediation & Playbooks: Developed automated incident response workflows using Sentinel playbooks and Logic Apps to contain threats rapidly. Integrated remediation actions such as user isolation, token revocation, and alert suppression.**
* **Compliance Monitoring & Reporting: Ensured continuous compliance with DEFRA’s regulatory requirements by leveraging Azure Policy, regulatory compliance dashboards, and audit logs. Produced actionable reports for stakeholders and auditors.**
* **Use Case Development & Detection Engineering: Designed and implemented new detection use cases aligned with the MITRE ATT&CK framework. Continuously refined analytic rules to stay ahead of emerging threats.**
* **Team Development & Mentoring: Provided hands-on support, mentoring, and performance appraisals for junior SOC analysts. Promoted knowledge sharing and best practices in threat analysis, incident handling, and security tooling.**

**L3 Security Engineer (SOC) – National Crime Agency**

**From: July 2023 – March 2024**

* **Established and led a newly formed SOC team, mentoring junior analysts, setting performance goals, and embedding a culture of continuous improvement and security excellence.**
* **Monitored and investigated security alerts using Microsoft Sentinel and Huntsman, leveraging Kusto Query Language (KQL) to develop advanced hunting queries and custom analytics rules.**
* **Led incident response efforts across the full lifecycle—identification, triage, containment, eradication, and recovery—coordinating with cross-functional teams to minimize business impact.**
* **Conducted in-depth security assessments of on-premise infrastructure, identifying risks and aligning systems with organizational and national cybersecurity standards.**
* **Performed malware analysis and supported digital forensic investigations to determine attack vectors and assist with legal or disciplinary outcomes.**
* **Supported and enhanced vulnerability management processes by analyzing scan results, prioritizing threats, and tracking remediation efforts.**
* **Developed detection use cases, tuned alert logic, and implemented automated response playbooks in Microsoft Sentinel to streamline threat response.**
* **Regularly reviewed and optimized SOC operations, staying abreast of evolving threats, tactics, and tools, and integrating threat intelligence into daily workflows.**

**Senior Azure DevSecOps and SRE Engineer - UK Hydrographic Office**

**From: July 2021 – July 2023**

* **Led infrastructure automation projects using PowerShell, CloudFormation, ARM, and Terraform, including Kubernetes orchestration.**
* **Implemented robust security measures with Microsoft Defender, Sentinel, Splunk, and integrated vulnerability scanning.**
* **Managed and secured Kubernetes clusters, ensuring scalability and adherence to security best practices.**
* **Utilized monitoring tools like Log Analytics, Grafana, and Elastic Stack for comprehensive infrastructure monitoring.**
* **Collaborated on B2C SSO architecture projects, coordinated overseas initiatives, and provided architectural support.**
* **Led appraisals and set compliance goals for junior members of the team and remained the point of contact for clarifications of any queries raised.**

**DevSecOps L2 Engineer - UK Home Office**

**From: April 2021 – July 2021**

* **Served as a Level 3 Security, Logging, Reporting, and Troubleshoot Engineer, monitoring the DSAB infrastructure based on Kubernetes Microservice Architecture and hosted on AWS.**

**DevOps Engineer - South Gloucestershire Council**

**From: February 2021 – April 2021**

* **Managed build and release pipelines, including deployment to Azure App Service and Dynamics 365. Involved in administering Azure AD, Dynamics 365, and Power Platform, and implementing practices to shift security left.**

**DevSecOps Consultant - General Dynamics**

**From: March 2019 – February 2021**

* **Worked with Technical Architects and Information Security Officers, designed and implemented robust procedures for deployment to internal and external environments to minimize downtime and proactively address information security risks through principles of shared responsibility across Microsoft Azure.**

**DevOps Engineer - Bristol City Council**

**From: September 2018 – March 2019**

* **Developed DevOps principles and recommended approaches for the development and delivery of the system by using the best practices of DevOps. Introduced SonarQube into the Azure DevOps CI/CD system, GitHub repository management for open-source and closed-source systems.**

**Core Competencies**

**Cloud Services:**

* **Azure: Azure VMs, Networking, IaaS, PaaS Services, Azure Sentinel, Azure DevOps, Azure CLI, Azure Kubernetes Service**
* **AWS: IAM, EC2, RDS, S3, CloudFront, CloudTrail, CloudWatch**

**Version Control:**

**Git, GitHub, BitBucket**

**Continuous Integration/Deployment:**

**TeamCity, Jenkins, Octopus Deploy**

**Containerization:**

**Docker, Kubernetes**

**Infrastructure as Code and Deployment:**

**Terraform, Ansible, Puppet**

**Web Servers:**

**IIS, Nginx, Apache**

**Security:**

**OWASP, White Source Bolt, Fortinet, Palo Alto, Azure Sentinel, Splunk**

**Logging and Monitoring:**

**Kibana, Grafana, Prometheus, Azure Monitor, Azure Log Analytics, Azure Application Insights, Azure Monitor for Containers, Azure Security Center, Azure Sentinel**

**Programming Languages:**

**C#, PowerShell, Python, Bash**

**Databases:**

**Azure SQL Database, Cosmos DB, MySQL, PostgreSQL, Aurora DB**

**Others:**

**VMWare, Hyper-V, Dynatrace**

**Certifications**

* **Microsoft Certified: AZ-400 – Microsoft Azure DevOps Expert**
* **AWS Certified: AWS Cloud Practitioner**