Cloud and DevOps Security: Building Defences Against Cyberattacks

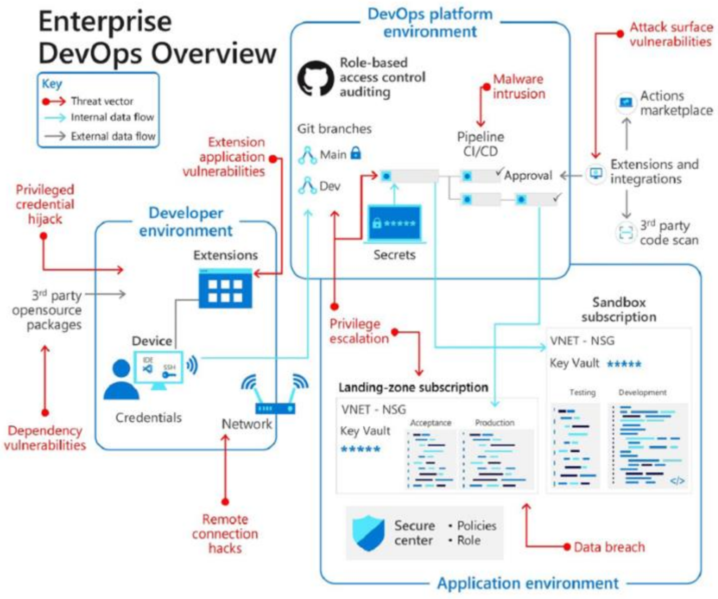
Name: Shenghan Gao

Tutorial group: W18A

Elevator Pitch

This project is to explore how modern cloud and DevOps components such as Infrastructure as Code (IaC), Identity and Access Management, CI/CD pipelines, monitoring and alerting can be configured to prevent cyberattacks. I am designing a simple cloud-hosted web service on AWS and integrating security tools and practices throughout its deployment lifecycle.

E.g. sample modern enterprise level system design graph



Why This Is Important

As more organisations or companies move to the cloud and adopt DevOps practices, misconfigurations and miss-placed security controls can leave systems vulnerable to attacks like brute force logins, privilege escalation, or data breaches. Understanding how to build security into systems from the designing phase rather than adding it as a patch fix is critical for cloud engineers to protect services and data in real-world deployments.

Planned Approach, Schedule, and Progress So Far

I am managing the project week by week according to this schedule:

- **Week 1**: Researched core topics and defined the project goals.
  Week 2: Explored DevOps fundamentals including CI/CD, Infrastructure as Code, and tools like GitHub Actions, CloudFormation, and Docker.
- **Week 3**: Investigated common cloud vulnerabilities, the shared responsibility model, and security best practices.
- **Week 4 (current)**: Working on integrating security into the CI/CD pipeline. I am testing GitHub Actions workflows with security scans such as static code analysis to catch vulnerabilities during deployment.

For the upcoming weeks:

- **Week 5**: Focus on IAM roles, least privilege principles, and analysing access logs.
- **Week 7**: Learn how to set up basic logging and monitoring using CloudWatch, possibly Splunk or Grafana, and create alerting rules for unusual events.
- **Week 8**: Consolidate all findings into a final report and presentation.

My deliverables will include a detailed journal, security design documents, summaries of best practices, architecture diagrams, and reflections on how to apply these principles in practice.

Challenges

My biggest challenge is balancing the wide scope of tools and security topics within the limited time frame of the project because there is a lot to cover. It can be harder to fully cover the practical details, limitations, or hidden complexities of certain tools or configurations. Another challenge is deciding how to make my designs so that they are realistic and useful without becoming overwhelming or too theoretical.