* Explain your project? What was your role?
* what programming languages are you comfortable?
  + Python
* What is your understanding of DevSecops why people are more tending towards it
* What is Black Duck
* What is your understanding about ArgoCD.
* I see you working on various roles, how come you were promoted as a Devops manager how did this transition happen
* How do you segregate your activities technically as well as from people management? What is the percentage you work technically and what is the percentage you manage people
* How did you give constructive feedback to your reportees and how the disagreement was solved?
* Have you fired anyone?
* What is the architectural change you proposed and how was it handled and presented to the relevant srakeholders
* How were your test stages configured, how were the automated test results interpreted, what was the criteria to pass or fail this step.There is already a Devops toolchain used, what would be your approach to analyse and propose a cost effective approach
* How do you propose the new solution to your management and how do you convince them
* what is your roles and responsibility  
  describe recent issue you faced and your contribution you maid to fixed that issue ?  
  tell me what was the cause for that issue and wat is the resolution you took to fix that issue?
* what is dry?  
  ANS: DRY stands for "Don't Repeat Yourself," which is a software development principle aimed at reducing repetition of code and promoting code reusability

ANSWERS:

**Explain your project? What was your role?**

**what programming languages are you comfortable?**

* Python

**What is your understanding of DevSecops why people are more tending towards it**

* + DevSecOps is an approach that integrates security practices into DevOps workflows, aiming to prioritize security throughout the software development lifecycle (SDLC). It involves collaboration and shared responsibility between developers, operations teams, and security teams right from the start of the development process.  
      
    The increasing popularity of DevSecOps can be attributed to several factors:
  + Shift Left Mentality: DevSecOps promotes the idea of addressing security concerns earlier in the development process, rather than treating it as an afterthought. By integrating security practices into the entire SDLC, organizations can identify and address vulnerabilities at an early stage, reducing the likelihood of security breaches or major issues later on.
  + Continuous Security: DevSecOps emphasizes continuous monitoring, testing, and security analysis throughout the software development process. This proactive approach helps in identifying security weaknesses, vulnerabilities, or configuration issues before they can be exploited, improving overall security posture.
  + Agile and Efficient Collaboration: DevSecOps promotes collaboration between developers, operations teams, and security teams, blurring the traditional boundaries between them. This collaborative environment enables faster communication, knowledge sharing, and problem-solving, leading to more efficient and secure development practices.
  + Automation and Tooling: DevSecOps relies on automation and specialized security tools to seamlessly integrate security measures into the development pipeline. Automated security testing, code analysis, vulnerability scanning, and continuous monitoring help in identifying and addressing security issues in a timely manner.
  + Compliance and Risk Reduction: To comply with regulations and standards, organizations need to demonstrate the implementation of robust security practices. DevSecOps provides a framework for building security into the development process, ensuring compliance and reducing risk.
  + Enhanced Customer Trust: As security breaches and data leaks become more frequent and damaging, customers and users are increasingly concerned about the security of the software they use. Implementing DevSecOps practices demonstrates an organization's commitment to security, building trust and credibility among users.
  + Overall, the adoption of DevSecOps can help organizations improve the security of their software, reduce vulnerabilities, and respond more effectively to security threats in today's rapidly evolving technology landscape.

**What is Black Duck?**

**What is your understanding about ArgoCD.**

**I see you working on various roles, how come you were promoted as a Devops manager how did this transition happen**

**How do you segregate your activities technically as well as from people management? What is the percentage you work technically and what is the percentage you manage people**

**How did you give constructive feedback to your reportees and how the disagreement was solved?**

**Have you fired anyone?**

**What is the architectural change you proposed and how was it handled and presented to the relevant srakeholders**

**How were your test stages configured, how were the automated test results interpreted, what was the criteria to pass or fail this step.There is already a Devops toolchain used, what would be your approach to analyse and propose a cost effective approach**

**How do you propose the new solution to your management and how do you convince them**

**what is your roles and responsibility  
describe recent issue you faced and your contribution you maid to fixed that issue ?  
tell me what was the cause for that issue and wat is the resolution you took to fix that issue?**

**what is dry?**  
ANS: DRY stands for "Don't Repeat Yourself," which is a software development principle aimed at reducing repetition of code and promoting code reusability