Ensuring Security and Compliance in DevOps

Part 1: Office Roleplay Dialogue

Scenario: A DevOps Engineer, Takeshi, is working with his colleague, Ananya, to ensure the security and compliance of their infrastructure and code.

Ananya: Takeshi, we need to review our **security policies** before the next deployment. Have you checked the latest updates?

Takeshi: Yes, I did. We need to ensure that our pipeline follows the required **compliance** standards.

Ananya: Good. What about **vulnerability scanning**? Are we running it on every deployment?

Takeshi: Yes, we've automated scans, but we should also review **access control** settings to limit unauthorized changes.

Ananya: Agreed. Also, is our data **encryption** up to date? We can't risk any security breaches.

Takeshi: I checked that too. We're using the latest encryption protocols.

Ananya: Perfect. Then let's document everything to show compliance for audits.

Takeshi: Yes, I'll update the security logs. Do you want to schedule a final review before deployment?

Ananya: That's a good idea. Let's meet in an hour to go through everything one last time.

Takeshi: Sounds like a plan. I'll bring the security checklist.

Part 2: Comprehension Questions

1. What is the team reviewing before deployment?

(A) Performance benchmarks
(B) Security policies
(C) Marketing strategies
(D) Customer feedback

2. What does Takeshi suggest reviewing in addition to vulnerability scans?

(A) Network speed
(B) Database size
(C) Access control
(D) UI design

3. How is the team handling encryption?

(A) They are ignoring it
(B) They are using outdated encryption
(C) They are using the latest encryption protocols
(D) They are switching to manual encryption

4. What is the last step before deployment?

(A) A final security review
(B) Skipping all compliance checks
(C) Removing encryption
(D) Disabling all security policies

Part 3: Key Vocabulary Definitions in Japanese

1. **Security policies (セキュリティポリシー)** – IT システムやデータを保護するためのルールや手順。
2. **Compliance (コンプライアンス)** – 法規制や業界基準に従うこと。
3. **Vulnerability scanning (脆弱性スキャン)** – システムのセキュリティ上の弱点を検出するプロセス。
4. **Access control (アクセス制御)** – ユーザーのシステムやデータへのアクセスを管理する方法。
5. **Encryption (暗号化)** – データを保護するために情報を変換する技術。

Part 4: Questions & Correct Answers

1. **What is the team reviewing before deployment?**
   ✅ (B) Security policies
2. **What does Takeshi suggest reviewing in addition to vulnerability scans?**
   ✅ (C) Access control
3. **How is the team handling encryption?**
   ✅ (C) They are using the latest encryption protocols

4. **What is the last step before deployment?**

   ✅ (A) A final security review