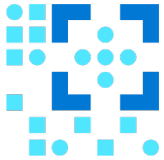
[答] C : Azure Sentinel

- **組織全体のセキュリティを分析**する SIEM と SOAR サービス
- SIEM : セキュリティ情報イベント管理
- SOAR : セキュリティ運用の自動化

収集

- オンプレミスとクラウドの セキュリティデータを収集
- Azure AD や Office 365
- パートナー製品

検出



- 機械学習を使用した 脅威の検出
- アラートルール対応

分析

- インシデントを ビジュアルで表示
- ハンティングクエリ
- Jupyter ノートブック対応

対応

- オートメーションによる インシデントの迅速な対応
- Azure Logic App ベースの プレイブック