**Denetim Tekniği İçin Örnek Senaryo**

**Örnek Senaryo: Bir Finansal Yazılım Sisteminin Güvenlik Denetimi**

**Proje:** Bir bankanın finansal yazılım sisteminin güvenlik kontrolleri.

**Amaç:** Yazılım sisteminin güvenlik standartlarına uygun olup olmadığını değerlendirmek ve olası güvenlik açıklarını belirlemek.

**Denetim Ekibi:**

* **Denetçi:** Bağımsız bir siber güvenlik uzmanı
* **Katılımcılar:** Yazılım geliştirme ekibi, IT yöneticisi, güvenlik uzmanı

**Denetim Süreci:**

1. **Planlama:**
   * Denetim ekibi, bankanın finansal yazılım sistemini güvenlik açılarından değerlendirmek için bir denetim planı oluşturur.
   * Denetimin kapsamı ve amaçları belirlenir; şifreleme, erişim kontrolleri ve veri bütünlüğü gibi güvenlik kriterleri odak noktası olarak belirlenir.
2. **Belge İncelemesi:**
   * Yazılımın güvenlik politikaları, erişim kontrol listeleri, veri şifreleme prosedürleri ve güvenlik test raporları gibi belgeler incelenir.
   * Mevcut güvenlik protokollerinin yeterliliği ve standarda uygunluğu değerlendirilir.
3. **Yerinde İnceleme:**
   * Yazılımın gerçek çalışma ortamında (bankanın veri merkezi) gözlemler yapılır.
   * Denetçi, sistem üzerinde belirli testler yaparak güvenlik açıklarını araştırır. Örneğin, SQL enjeksiyonu veya kimlik doğrulama testleri gerçekleştirilir.
4. **Sonuçların Raporlanması:**
   * **Tespit Edilen Güvenlik Sorunları:**
     + **Açık:** "Kullanıcı şifreleri yetersiz şifreleme ile saklanmaktadır."
     + **Öneri:** "Kullanıcı şifrelerinin SHA-256 gibi daha güçlü bir şifreleme algoritması ile korunması gerekmektedir."
   * **Uyumluluk Sorunları:** Mevcut sistem, sektör standartlarına (örneğin, PCI-DSS) tam uyum sağlamıyor.
5. **Düzeltici Faaliyetlerin Takibi:**
   * Yazılım geliştirme ekibine, güvenlik açıklarını düzeltmeleri için öneriler ve adımlar sağlanır.
   * Denetim ekibi, önerilen düzeltmelerin hayata geçirildiğini ve sorunların çözüldüğünü doğrulamak için tekrar bir değerlendirme yapar.