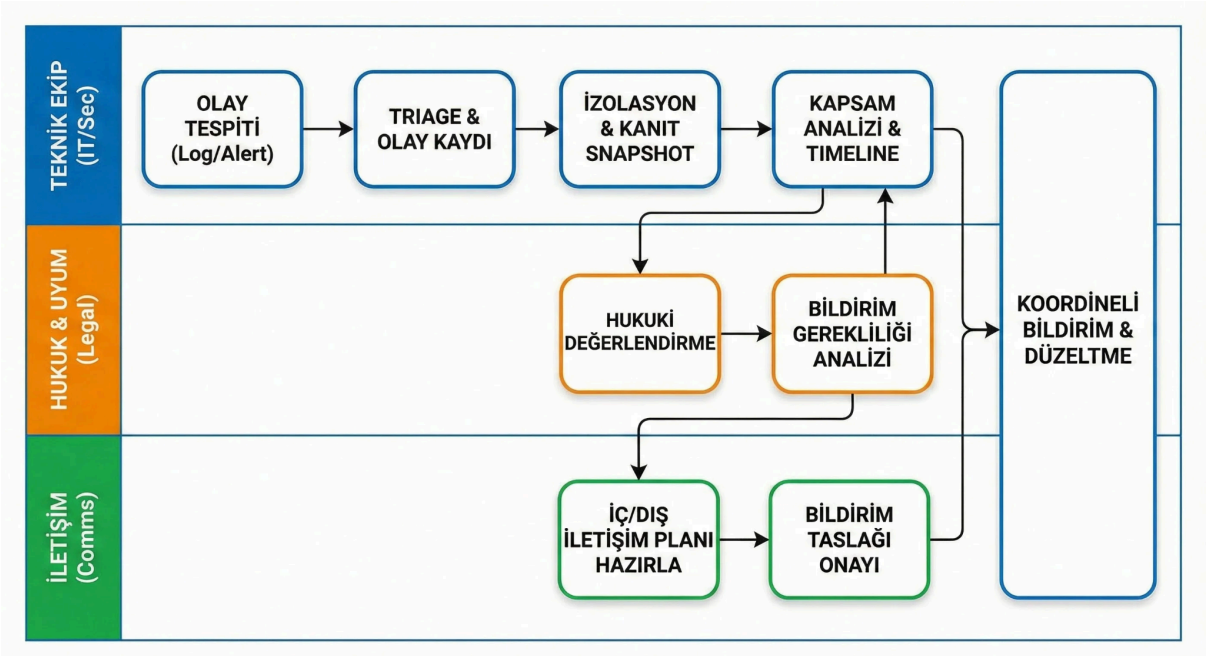
Veri İhlali (Incident Response) Akış & Rol Dağılımı Planlama Şablonu (v1.0)

Asset Amacı: Bu şablon, bir veri ihlali anında doğaçlama hareket edilmesini önlemek amacıyla ilk 60 dakika ve ilk 24 saatlik kritik süreci netleştirir. Teknik, hukuk ve iletişim ekipleri arasındaki rol dağılımını "Swimlane" (kulvar) akışıyla tek sayfada toplar; kapsam analizi ve kanıt koruma adımlarını standartlaştırır.

Kim Kullanır?: IT/BT ekipleri, hukuk danışmanları, iletişim departmanı ve operasyon liderleri (Otel & B2B).



Nasıl Kullanılır? (3 Adım)

1. **Tanımlama:** Kritik sistemlerinizi ve olay kaynaklarını (log, alarm, misafir şikâyeti vb.) önceden sisteme işleyin.
2. **Rol Ataması:** Incident Commander (Olay Komutanı), Legal ve Tech Lead gibi kritik rolleri ve yedeklerini belirleyin.
3. **Uygulama:** Hazırlanan akışı olay kartı checklist'iyle birlikte erişilebilir kılın ve yılda en az 1 kez tatbikat yapın.

TEMPLATE: Olay Müdahale Paketi

1) Olay Kartı (Incident Card)

- **Olay ID / Tespit Zamanı:** _____ / _____
- **Tespit Kaynağı:** (Alarm / Log / Şikâyet / Anomali) _____
- **Şüpheli Sistemler & Veri Türleri:** _____
- **Öncelik Seviyesi:** (P1: Kritik / P2: Yüksek / P3: Orta) _____

- **İlk Aksiyon:** (Hesap kilitle / Export kapat / Token rotate / WAF blok) _____
- **Kanıt Koruma:** Snapshot/Yedek alındı mı? [ ] Evet [ ] Hayır

2) Rol Dağılımı Tablosu

Rol	Birim	Sorumlu Kişi	Yedek
Incident Commander	Yönetim	_____	_____
Tech Lead	IT / Yazılım	_____	_____
Legal / Compliance	Hukuk	_____	_____
Comms / PR	Kurumsal İlt.	_____	_____

Zaman Bazlı Müdahale Akışı (Swimlane Özet)

- **0–15 dk (Tespit):** Olay kaydının açılması, önceliklendirme (triage) ve ilk log snapshot alımı.
- **15–60 dk (İzolasyon):** Şüpheli hesapların kilitlenmesi, WAF bloklama ve veri dışa aktarımının (export) kapatılması.
- **1–6 saat (Analiz):** Timeline oluşturma, etkilenen kayıt sayısının tespiti ve kök neden analizi.
- **6–24 saat (Düzeltme):** Güvenlik yamalarının uygulanması, RBAC (rol bazlı erişim) fix ve izleme sürecinin başlatılması.
- **24–72 saat (Kapanış):** Teknik özet paketinin hazırlanması, yasal bildirim hazırlığı ve "öğrenilen dersler" toplantısı.

Kontrol Listesi

- [ ] Olay ID açıldı ve tüm kronolojik kayıtlar tutuluyor.
- [ ] İzolasyon aksiyonları (hesap kilitleme vb.) uygulandı.
- [ ] Kanıt snapshot'ları alındı ve erişimleri sınırlandırıldı.
- [ ] Hukuk ve iletişim ekipleri için teknik özet paketi hazırlandı.
- [ ] Düzeltme sonrası takip metrikleri ve izleme süreci belirlendi.