Web Altyapısı Güvenlik Loglama & SIEM Checklist Şablonu (v1.0)

Asset Amacı: Bu şablon; Web, App, WAF, DB ve PMS/CRM entegrasyon loglarını standardize ederek SIEM (Güvenlik Bilgisi ve Olay Yönetimi) sistemlerinde anlamlı uyarılar oluşturmak için hazırlanmıştır. Hedef; gürültüsüz bir alarm setiyle siber olaylara müdahaleyi hızlandırmak ve KVKK uyumlu log saklama standartlarını korumaktır.

Kim Kullanır?: BT/DevOps, Güvenlik Operasyonları (SecOps) ve teknik liderler.

Nasıl Kullanılır? (3 Adım)

1. **Envanter:** Katman bazlı (Web/App/DB/API) log setlerini işaretleyin ve eksik alanları tanımlayın.
2. **Kural Seti:** SIEM üzerinde çalışacak 5-10 adet yüksek sinyal kuralını ve eşik değerlerini belirleyin.
3. **Sprint:** 14 günlük planla sistemleri devreye alın ve yanlış alarmlara (false-positive) göre optimize edin.

Güvenlik Loglama & Denetim Kontrol Listesi

- [ ] **Web Access/Error:** Endpoint, HTTP Status ve Latency (gecikme) verileri mevcut mu?
- [ ] **App Audit:** Login denemeleri, rol değişimleri ve kritik CRUD işlemleri kayıt altında mı?
- [ ] **WAF/Firewall:** Tetiklenen kural ID'si ve alınan aksiyon (Block/Pass) loglanıyor mu?
- [ ] **Entegrasyon:** PMS/CRM auth/scope ve rate limit hataları sınıflandırıldı mı?
- [ ] **Log Masking:** Token, anahtar ve parolaların log dosyalarında gizlendiğinden (mask) emin misiniz?
- [ ] **KVKK/KVYS:** Gereksiz kişisel veri tutuluyor mu? Erişim ve saklama politikası tanımlı mı?
- [ ] **SIEM & Dashboard:** İlk 5-10 kritik kural hazır mı? Operasyonel paneller çizildi mi?

Problem → Kök Neden → Çözüm Matrisi

Problem	Kök Neden	Çözüm
Yüksek MTTD (Geç Tespit)	Loglarda standart yok; arama zor.	Log alanlarını (standardize) eşitle.
Alert Fatigue (Yorgunluk)	Eşik değerleri çok düşük; her şey alert.	Eşik değerlerini (threshold) normalize et.
Veri Sızıntısı Riski	Masking eksik; logda açık şifre var.	RegEx tabanlı dinamik masking uygula.
Görünürlük Kaybı	Entegrasyon (PMS/API) logları kapalı.	Entegrasyon hata kodlarını SIEM'e bağla.

14 Günlük Güvenlik İzleme Sprint'i

Gün	Aşama	Aksiyon
G 1-2	**Analiz**	Log alan standartlarının ve katman envanterinin çıkarılması.
G 3-5	**App & WAF**	Kritik işlem loglama ve WAF/Firewall formatının netleştirilmesi.
G 6-7	**Politika**	Entegrasyon hata sınıfları ve KVKK saklama politikası (Masking).
G 8-10	**SIEM & Dash**	İlk 5 kuralın tanımlanması ve Executive/Ops panellerinin oluşturulması.
G 11-14	**Optimizasyon**	False-positive ayarları, Runbook hazırlığı ve final raporlama.

Öncesi / Sonrası KPI Hedefleri

KPI	Mevcut (Tahmini)	Hedef (30 Gün Sonra)
MTTD (Tespit Süresi)	> 24 Saat	< 1 Saat
Gürültü Oranı (Alerts)	%100	%20 (Sadece kritik)
Log Kapsamı	Parçalı	Tam (End-to-end)

Deliverables

- Log Standart Dokümanı, SIEM Kural Seti & Runbook, 3 Katmanlı Dashboard, KVKK Erişim Politikası.