Serverless Fonksiyonlar İçin IAM & Secrets Güvenlik Checklist Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu asset; serverless (*FaaS - Function as a Service*) mimarilerde güvenliğin üç kritik bileşenini (IAM yetkilendirmeleri, secrets yönetimi ve event kaynakları) standartlaştırmak için hazırlanmıştır. "Cloud altyapı sağlayıcısı her şeyi halleder" yanılgısını ortadan kaldırarak paylaşılan sorumluluk (*shared responsibility*) sınırlarını teknik olarak netleştirmeyi hedefler. Loglama ve denetim (*audit*) yaklaşımını KVKK/GDPR teknik tedbirleriyle ve veri minimizasyon ilkeleriyle tam uyumlu hale getirecek kontrol maddelerini içerir.

Kim Kullanır?: Backend / DevOps Mühendisleri, Platform Ekipleri, Otel / B2B Entegrasyon Sorumluları.

Nasıl Kullanılır?

1. Serverless fonksiyon envanterinizi çıkarın; her fonksiyon için bağımsız IAM politikalarını, kullanılan secrets yapılarını ve event kaynaklarını tanımlayın.
2. En az yetki (*least privilege*) politikasını ve gizli bilgi (*secrets*) saklama/şifreleme modellerini uygulayın.
3. Event imza doğrulama, rate limiting ve izlenebilirlik (*observability*) mekanizmalarıyla konfigürasyon sapması (*drift*) ve kötüye kullanım (*abuse*) risklerini anlık izleyin.

CHECKLIST & SPRINT PLAN — Serverless IAM & Secrets Güvenliği

1) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **Fonksiyon Bazlı IAM Policy Ayrıştırması:** Her serverless fonksiyon için ortak rol kullanımı engellendi, fonksiyona özel bağımsız IAM rol ve politikaları kurgulandı.
- [ ] **En Az Yetki (Least Privilege) Kuralları:** IAM politikalarında wildcard (*) kullanımı kaldırıldı; yalnızca ilgili servisin ihtiyaç duyduğu aksiyon ve kaynaklar (*action/resource*) tanımlandı.
- [ ] **Secrets Saklama Modeli (Vault / KMS):** Hassas veriler, API anahtarları ve veritabanı parolaları ortam değişkenlerinde (*environment variables*) açık metin olarak saklanmak yerine KMS ile şifrelendi veya Secret Manager / Vault sistemlerine taşındı.
- [ ] **Secrets Rotation & Revocation Planı:** Otomatik parola ve API key yenileme (*rotation*) mekanizmaları ile sızıntı anında hızlı iptal (*revocation*) runbook'ları oluşturuldu.
- [ ] **Event Kaynakları Allowlist & Doğrulama:** Webhook ve event tetikleyicilerinde ip kısıtlaması, istek imzası doğrulama (*HMAC / JWT validation*) ve şema kontrolleri zorunlu kılındı.
- [ ] **Rate Limit & Throttling Yapılandırması:** API Gateway, HTTP endpoint ve mesaj kuyruğu (SQS/PubSub) seviyelerinde eşzamanlı çağrı ve bant genişliği limitleri ayarlandı.
- [ ] **Concurrency & Timeout Limitleri:** Yanlışlıkla oluşabilecek sonsuz döngü veya DoS maliyetlerini engellemek için fonksiyon seviyesinde maksimum *concurrency* ve *timeout* süreleri kilitlendi.

- [ ] **İdempotency & Retry Stratejisi:** Mükerrer event tetiklenmelerine karşı işlemler *idempotent* hale getirildi; başarısız istekler için *Dead Letter Queue (DLQ)* ve üstel geri çekilme (*exponential backoff*) tanımlandı.
- [ ] **Correlation ID & Audit Log Yapısı:** Distributed tracing için uçtan uca istek takibi sağlayacak Correlation ID standartlaştırıldı ve denetim logları merkezi ortama aktarıldı.
- [ ] **KVKK Veri Minimizasyonu & Log Politikası:** Log verileri içerisindeki kişisel verilerin (PII) otomatik maskelenmesi ve KVKK saklama/imha sürelerine uygun retention ayarları yapıldı.

2) Problem $\rightarrow$ Kök Neden $\rightarrow$ Çözüm Tablosu

Problem	**Kök Neden**	**Çözüm (Serverless Security)**
Fonksiyon Çok Yetkili (Geniş Erişim)	Ortak geniş IAM rollerinin kullanılması	**Policy Daraltma** $\mathbf{+}$ **Permission Boundary**
Secrets Sızıyor (Açık Metin)	Şifrelerin env var veya kod/log içinde tutulması	**Vault / KMS Entegrasyonu** $\mathbf{+}$ **Log Masking**
Event Flood / Aşırı Maliyet	Tetikleyici kaynaklarda rate limit olmaması	**API Gateway Limitleri** $\mathbf{+}$ **Reserved Concurrency**
Downstream Sistemlerin Çökmesi	Hızlı ölçeklenen fonksiyonların veritabanını boğması	**Queue (Kuyruk Katmanı)** $\mathbf{+}$ **Circuit Breaker**

3) 14 Günlük Uygulama Sprint Planı (Gün 1–14)

[Gün 1–5: Envanter & IAM/Secrets Refactor] ⟶ [Gün 6–9: Event Güvenliği & Throttling] ⟶ [Gün 10–12: Observability & KVKK Compliance] ⟶ [Gün 13–14: Tatbikat & Takvim]

- **Gün 1:** Mevcut serverless fonksiyon envanterinin ve bağlı oldukları kritik iş akışlarının haritalandırılması.
- **Gün 2:** Mevcut IAM rollerinin ve erişim politikalarının denetlenip aşırı yetkilerin tespit edilmesi.
- **Gün 3:** Pilot fonksiyonlar üzerinde *least privilege* ilkelerine göre IAM politikalarının daraltılması.

- **Gün 4:** Ortam değişkenlerindeki hassas verilerin KMS/Vault servislerine taşınması ve şifrelenmesi.
- **Gün 5:** Otomatik secrets rotation süreçlerinin ve acil durum iptal (*revocation*) prosedürlerinin hazırlanması.
- **Gün 6:** Event tetikleyicileri için imza doğrulama (*HMAC*) ve girdi şema kontrollerinin devreye alınması.
- **Gün 7:** API Gateway ve event kaynakları seviyesinde Rate Limit ve Throttling kurallarının tanımlanması.
- **Gün 8:** Fonksiyon özelinde Concurrency sınırlarının ve Timeout sürelerinin belirlenerek kilitlenmesi.
- **Gün 9:** Mükerrer istek yönetimi için Idempotency kütüphanelerinin entegrasyonu ve DLQ kurgusu.
- **Gün 10:** Uçtan uca izlenebilirlik (*X-Ray / OpenTelemetry*) ve merkezi log yönetimi altyapısının kurulması.
- **Gün 11:** Anomali durumları için alarm eşiklerinin tanımlanması ve olay müdahale (*incident*) akışlarının kurgulanması.
- **Gün 12:** Loglanan verilerde KVKK/GDPR uyumlu PII maskeleme ve log saklama (*retention*) ayarlarının yapılması.
- **Gün 13:** Olay simülasyonu: Beklenmeyen event akışlarına ve yüksek trafiğe karşı *Event Flood* tatbikatının icra edilmesi.
- **Gün 14:** Yönetimsel sonuç raporunun oluşturulması ve 180 günlük periyodik denetim takviminin kilitlenmesi.

4) Öncesi / Sonrası KPI Tablosu

KPI Metriği	**Önce (Mevcut Durum)**	**Sonra (Sprint Sonrası)**	**Hedef Yönü**
IAM Policy Kapsamı (Geniş Yetki Riski)	Geniş/Ortak Roller (Wildcard *)	Fonksiyon Bazlı Daraltılmış Policy	**Hedef ↓ (Düşüş)**
Timeout Oranı (%)	$\%4.2$ (Uzun çalışan istekler)	$< \%0.1$ (Optimize sınırlarla)	**Hedef ↓(Düşüş)**
Yetkisiz Çağrı / Event İhlali	Yüksek (İmzasız event alımı)	0 (İmza doğrulamalı)	**Hedef ↓(Düşüş)**

Secrets Rotation Uyumu (%)	$\%0$ (Manuel/Sabit)	$\%100$ (Otomatize KMS/Vault)	**Hedef ↑ (Yükselme)**

Deliverables (Teslim Edilecek Çıktılar)

- **Serverless IAM Policy & Least Privilege Seti:** Her fonksiyon türüne özel daraltılmış izin şablonları ve permission boundary kuralları.
- **Secrets Yönetim Standardı & Rotation Runbook'u:** KMS/Vault entegrasyon rehberi ve otomatik parola/key yenileme prosedürleri.
- **Event Koruma & Throttling Planı:** API Gateway rate limit, concurrency sınırları ve imza doğrulama mimarisi dokümanı.
- **Observability Dashboard & KVKK Audit Log Altyapısı:** Merkezi izleme panelleri, PII maskeleme kuralları ve olay müdahale kılavuzu.

[Checklist Card]

DevOps/Backend mühendisleri, platform ekipleri ve entegrasyon sorumluları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Serverless Güvenlik Checklist Kartı. Koyu karbon gri ve parlak turuncu/siyan tonlarındaki teknolojik zemin üzerinde; AWS Lambda / Cloud Functions simgeleri, IAM kilit ve KMS anahtar sembolleri, event flood koruma grafikleri ve

14 günlük serverless sprint takvimi yer alıyor. Kartın üzerinde; "Least Privilege IAM & Permission Boundaries", "Encrypted Secrets & Automated KMS Rotation", "Event Signature Validation & Rate Limiting", ve "KVKK Compliant PII Masking & Observability" teslimat kalemi başlıkları, yanlarında parlak turuncu onay işaretleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.