node101 Yazılım Geliştirme Güvenlik Politikaları Özet

01. IAM

2FA ve SSH/token kullanımı zorunludur. Yetkiler düzenli denetlenmelidir.

02. BRANCH & COMMIT

İmzalı commit kullanımı zorunludur. Doğrudan push veya force-push yapmak yasaktır.

03. KOD İNCELEME

En az bir onay alınmalı ve kendi PR'ını onaylamak yasaktır. Yeni commitlerle onaylar sıfırlanmalı ve testler geçilmelidir.

04. SECRET YÖNETİMİ

Sırlar hiçbir koşulda commitlenmemeli ve gitignore'da tutulmalıdır. Sızıntı durumunda rotasyon hemen yapılmalı ve uzun ömürlü sırlar yıllık yenilenmelidir.

05. BAĞIMLILIK

Lock dosyaları depoda tutulmalı ve kritik açıklar 7 gün içinde kapatılmalıdır. Dinamik sürüm belirteçleri ve bakımsız paketler yasaktır.

06. CI/CD

Action'lar commit hash ile sabitlenmelidir. Dağıtımlar sadece korumalı daldan yapılmalıdır.

07. UYGULAMA GÜVENLİĞİ

OWASP Top 10 esas alınarak girdi doğrulaması ve parametreli sorgu uygulanmalıdır. Kimlik doğrulama ile yetkilendirme ayrı tutulup stack trace gizlenmelidir.

08. KRİPTOGRAFİ

Üretim anahtarları HSM gibi yöntemlerle korunmalı ve düz metin saklanmamalıdır. Özel kriptografi yazılmamalı, Argon2/bcrypt gibi standartlar kullanılmalıdır.

09. ALTYAPI

SSH anahtarıyla giriş zorunlu olup servisler non-root çalıştırılmalıdır. Loglar 90 gün saklanmalı ancak içlerine sır veya kişisel veri yazılmamalıdır.

10. OLAY MÜDAHALESİ

Şüpheli durumlar derhal bildirilmeli ve müdahalede erişimi kesip kanıt korunmalıdır. Post-Mortem 7 gün içinde yazılmalı ve SECURITY.md talepleri 72 saatte yanıtlanmalıdır.

EK: AI KULLANIMI

Gizli veriler AI araçlarına girilmemeli ve üretilen kodlar standart güvenlik süreçlerinden geçirilmelidir.

NODE101 TEKNOLOJİ A.Ş. (Inc.)
Karanfil Sokak, Villa 13 Levent, Beşiktaş, Istanbul /
Turkiye, 34330