



Dış Kaynaklı Uygulamaların Güvenliđi

Yunus ADIRCI
Güvenlik Mimarı
Haberleşme Mühendisi
Türk Telekom

Ajanda

- Hakkında
- Giriş
- Uygulama Temin Metotları
- Güvenli Yazılım Geliştirme Yaşam Döngüsü
- Dış Kaynaklı Uygulamalar ve Güvenlik
 - Şartname Hazırlama
 - Güvenlik Kontrolleri
 - Zafiyet Giderme Süreci
- Soru Cevap

Hakkında

- Haberleşme Mühendisi/2004
- 4 Yıldır Telekomünikasyon Sektöründe
- Developer Kökenli
 - Series 60, Web Uygulamaları
 - SIP, RTP, HTTP
- Kötü Kod Nasıl Yazılır
- Güvenli Yazılım Geliştirme Yaşam Döngüsü

www.yunuscadirci.com

[@yunuscadirci](https://twitter.com/yunuscadirci)

Giriş

- ❑ Saldırıları Uygulama Katmanına Yayılıyor
 - ❑ %80
 - ❑ Security by Layer
- ❑ İstihbarat Servisleri Tarafından Kötü Amaçlı Kullanılan Yazılımlar
 - ❑ PROMIS (Prosecutors Management Information Systems)
- ❑ Kişisel Bilgiler Hedefte (PII- Personal Identifiable Information)
 - ❑ Sony PSN – 77 Milyon
 - ❑ WordPress – 18 Milyon
 - ❑ Kişisel Verilerin Korunması Kanun Tasarısı (Bakanlar Kurulu 7/4/2008)
- ❑ Kamu Hedefte
 - ❑ Maliye.gov.tr
 - ❑ Tek olayda onlarca gov.tr uzantılı hastane sitesi
 - ❑ Aynı firmanın ürünü

Uygulama Temin Metodları

In-house

- Tüm süreç kurum içerisinde
- Güvenlik uçtan uca kontrol edilebilir
- Zafiyet Giderme süreci yönetilebilir

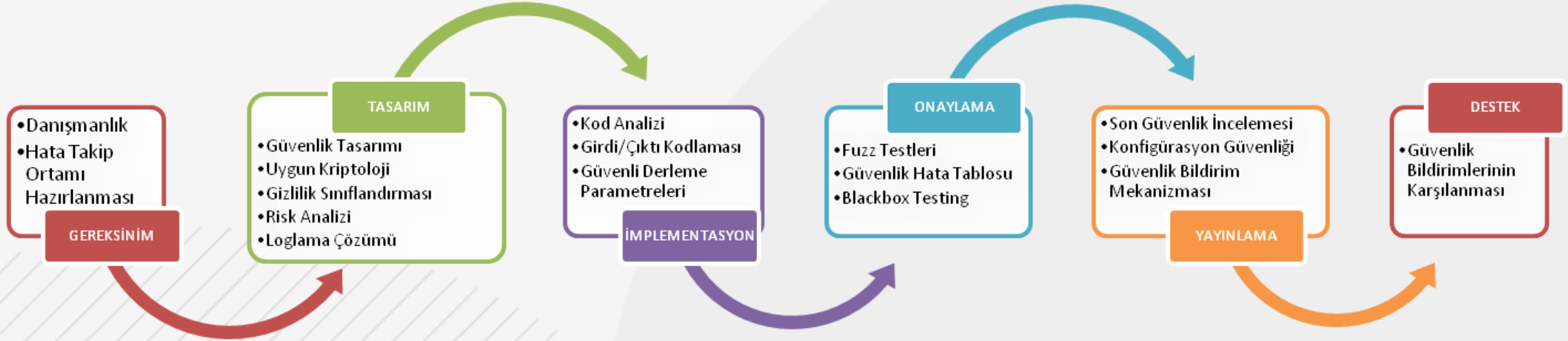
Outsourcing

- Firma yetenekleri önemli
- Geliştirme sürecinde kontrol düşük
- Zafiyet giderme süreci az yönetilebilir

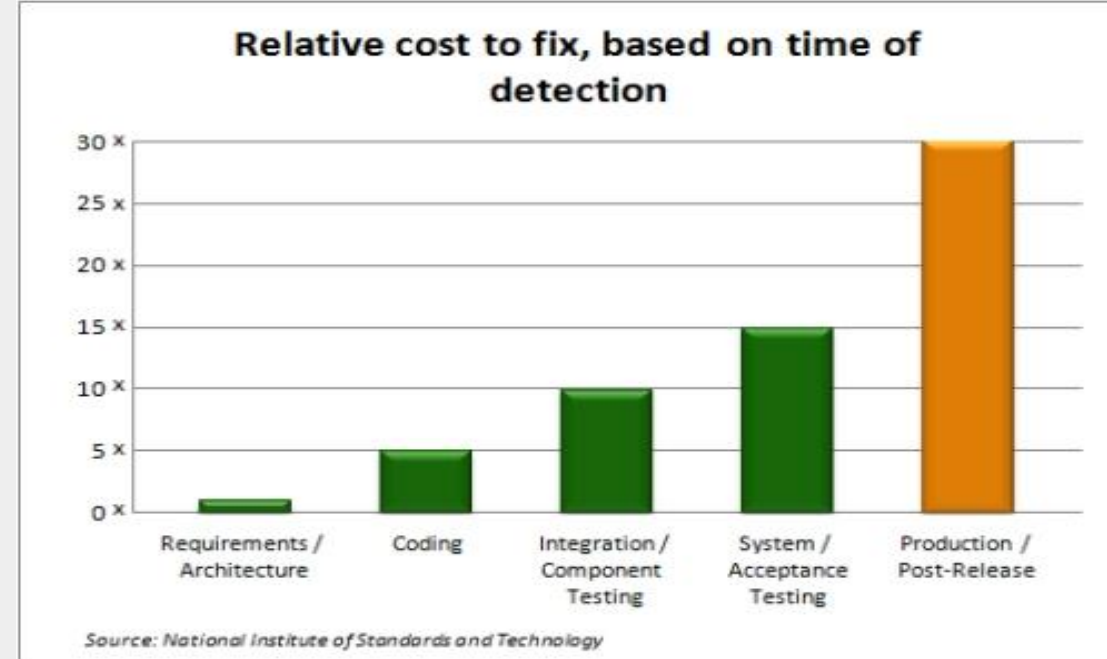
COTS

- Commercially available Off-The-Shelf (Paket Program)
- Geliştirme sürecinde kurum kontrolü dışında
- Zafiyet giderme süreci yönetilemez

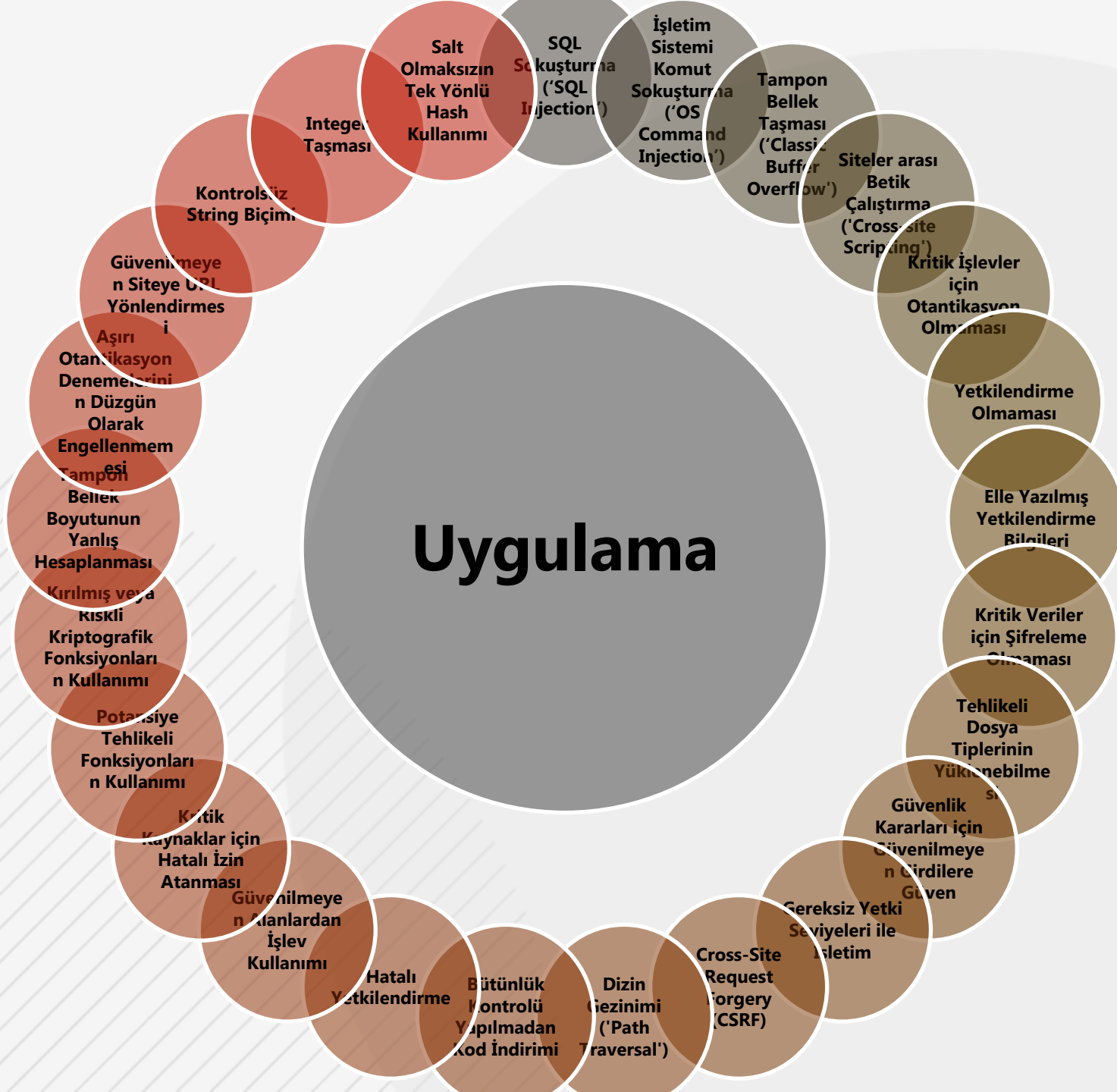
Güvenli Yazılım Geliştirme Yaşam Döngüsü (S-SDLC)



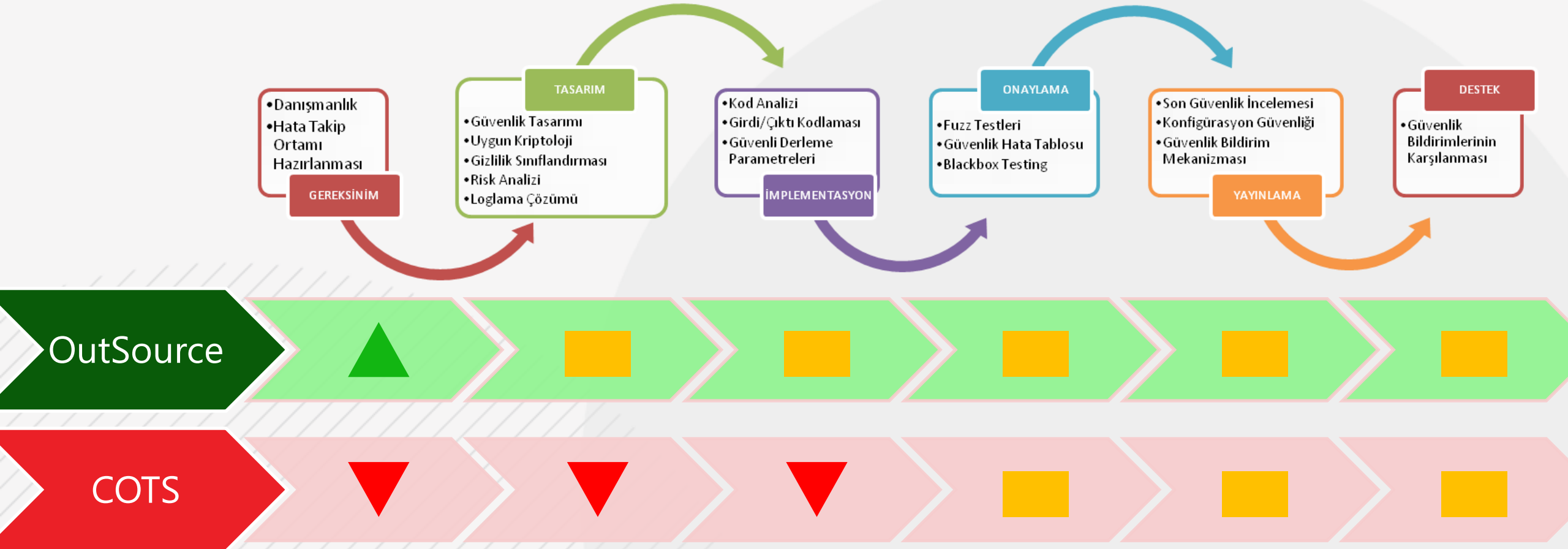
- Yazılımın her aşamada güvenlik kontrolü
- Minimum maliyetle maksimum güvenlik



Uygulama



Dış Kaynaklı Uygulamalar ve Güvenlik



▲ **Kontrol Edilebilir**

■ **Kısmen Kontrol Edilebilir**

▼ **Kontrol Edilemez**

Şartname Hazırlama

- ❑ Her kuruma uygun şartname yok
 - ❑ İhtiyaçlar ve öncelikler farklı
 - ❑ Kanun ve Regülasyonlar
- ❑ Güvenlik için bir baseline oluşturun
 - ❑ Ne güvenlik açığıdır ne değildir?
 - ❑ CWE/SANS Top 25 Most Dangerous Software Errors
- ❑ Kontrol edebileceğiniz maddeler
 - ❑ Maliyet etkin bir şartname
 - ❑ Ekibiniz/araçlarınız kontrolü gerçekleştirebilecek mi?
- ❑ Gerçekleştireceğiniz testleri belirtin
 - ❑ Statik Kod Analizi
 - ❑ Firma kaynak kodu paylaşacak mı?
 - ❑ Blackbox
 - ❑ Security Checklistinizi paylaşın



Şartname Hazırlama

- ❑ Kullanıcı Yönetimi ilkelerini belirleyin
 - ❑ IDM, SSO entegrasyonları
 - ❑ Parola kuralları, Hatalı girişler
- ❑ Entegrasyon Güvenliği
 - ❑ Uygulamanın bir parçası
 - ❑ Security by layer prensibince trust ilişkisinden kaçın
- ❑ Güvenlik Dökümantasyonu
 - ❑ Alınan önlemler
 - ❑ Kullanıcı Yönetim Mekanizması
 - ❑ Security by default prensibini sağlayacak konfigürasyonlar
 - ❑ PII içeren modüller
 - ❑ Firma desteği gerekmeden yürütülebilen Kurulum Kılavuzu
 - ❑ Güvenlik testleri için girdi parametreleri



Şartname Hazırlama

- ❑ Zafiyet giderme sürecini tanımlayın
 - ❑ Zafiyetler nasıl sınıflandırılacak
 - ❑ Zafiyet sınıflarına göre maximum giderme süreleri
- ❑ Uygulamada ihtiyaç duyacağınız loglama noktalarını belirtin
 - ❑ İşlemi gerçekleştiren kullanıcı
 - ❑ İşlemi gerçekleştirme zamanı
 - ❑ İşlemin gerçekleştirildiği modül/sayfa - servis
 - ❑ İşlemin gerçekleştirildiği kullanıcı aksiyonu/fonksiyonu
 - ❑ İşlemi gerçekleştiren kullanıcı IP'si
 - ❑ Aktif network cihazlarına dikkat edin
 - ❑ İşlem parametreleri



Güvenlik Kontrolleri

Uygulama devreye alınmadan önce gerçekleştirilmeli

- ❑ Test Ekibi
 - ❑ Kurum içi
 - ❑ Dış kaynak
- ❑ Araçlar
 - ❑ Blackbox
 - ❑ Kaynak Kod Analizi
 - ❑ Otomatize Olmayan (Pentest) Araçlar
- ❑ Kontrol Listeleri
 - ❑ CWE/SANS Top 25 Most Dangerous Software Errors
 - ❑ Portal Cheklisti (73 Madde)
- ❑ Karne
 - ❑ Uygulama bazlı



Zafiyet Giderme Süreci

- RFP'de tanımlı olmalı
- Bugfix sürecine paralel
 - Bedelsiz
 - Uygulama sahibinin bilgisi dahilinde
- Zafiyet giderilene kadar önlemleri sıkılaştırın
 - Web Application Firewall
 - XML Firewall
- Karne
 - Zafiyet giderme performansına göre Firma Bazlı



Soru

