

Siber Gvenlik Temelleri – Daphne Kariyer Online Eđitim

Kurumlar İin Savunma ve
Farkındalık Odaklı Bařlangı Rehberi

Kimin İçin & Yaklaşım



Kurum çalışanları, yöneticiler, alana yeni başlayanlar.



Teknik olmayan, tamamen savunma ve farkındalık odaklı.



Yaklaşık 10–12 saat, başlangıç düzeyi, kendi hızında.

Öğrenme Hedefleri

- ✓ Gizlilik, bütünlük ve erişilebilirlik ilkelerini (CIA) kavramak.
- ✓ Fidyeye yazılımı ve oltalama gibi tehditleri tanımak.
- ✓ Güçlü parola, MFA ve en az yetki ilkelerini uygulamak.
- ✓ Güvenlik duvarı ve ağ segmentasyonu mantığını anlamak.
- ✓ Yedekleme (3-2-1 kuralı) ve iş sürekliliğini planlamak.
- ✓ Güvenlik olaylarına müdahale aşamalarını kavramak.
- ✓ ISO 27001 ve KVKK standartlarında güvenlik kültürü oluşturmak.

MODÜL 1

Bilgi güvenliğinin temeli

Gizlilik
Yalnız yetkili kişiler görebilir

Bütünlük
Doğru ve izinsiz
değiştirilmemiş



Erişilebilirlik
İhtiyaç anında
ulaşılabilir

[Varlık] + [Tehdit] + [Zafiyet] = RİSK

Azaltmak
Önlem almak

Aktarmak
Sigorta/Dış Kaynak

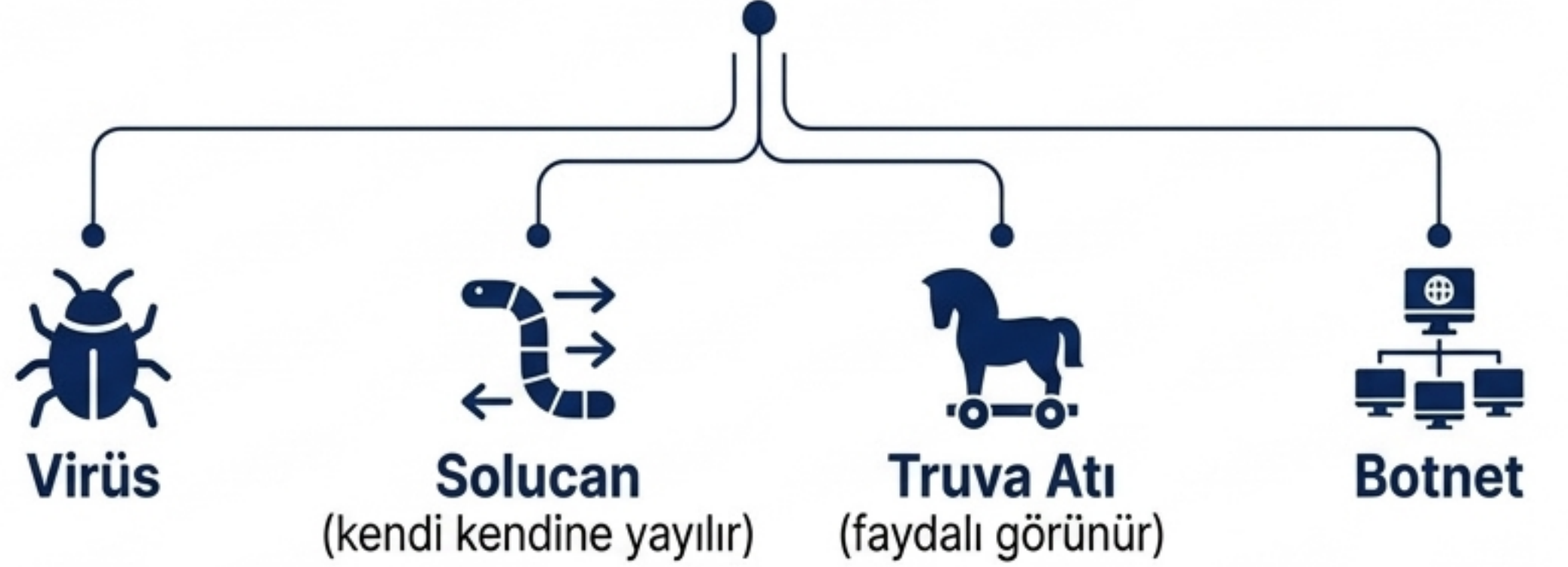
Kaçınmak
İşi yapmamak

Kabul Etmek
Yazılı onay ile üstlenmek

MODÜL 2

Tehdit türleri

Zararlı Yazılım Spektrumu



İnsan Odaklı Tehditler

1 Oltalama (Phishing)	Sahte mesaj/e-posta (Aciliyet ve baskı içerir).
2 Sosyal Mühendislik	Telefon/Yüz yüze güven istismarı (Kuyruk takibi, bahane uydurma).
3 İş E-postası Dolandırıcılığı	Sahte yönetici/tedarikçi talimatı.

Fidye Yazılımı ve Çifte Şantaj:
Saldırgan sistemi şifreler + dışarı çıkardığı veriyi yayımlamakla tehdit eder.

MODÜL 3

Kimlik ve erişim yönetimi

Erişim Hunisi



Parola Güvenliği



Uzunluk
karmaşıklıkla
önemlidir
(en az 12 karakter)



Her hesap için
farklı parola



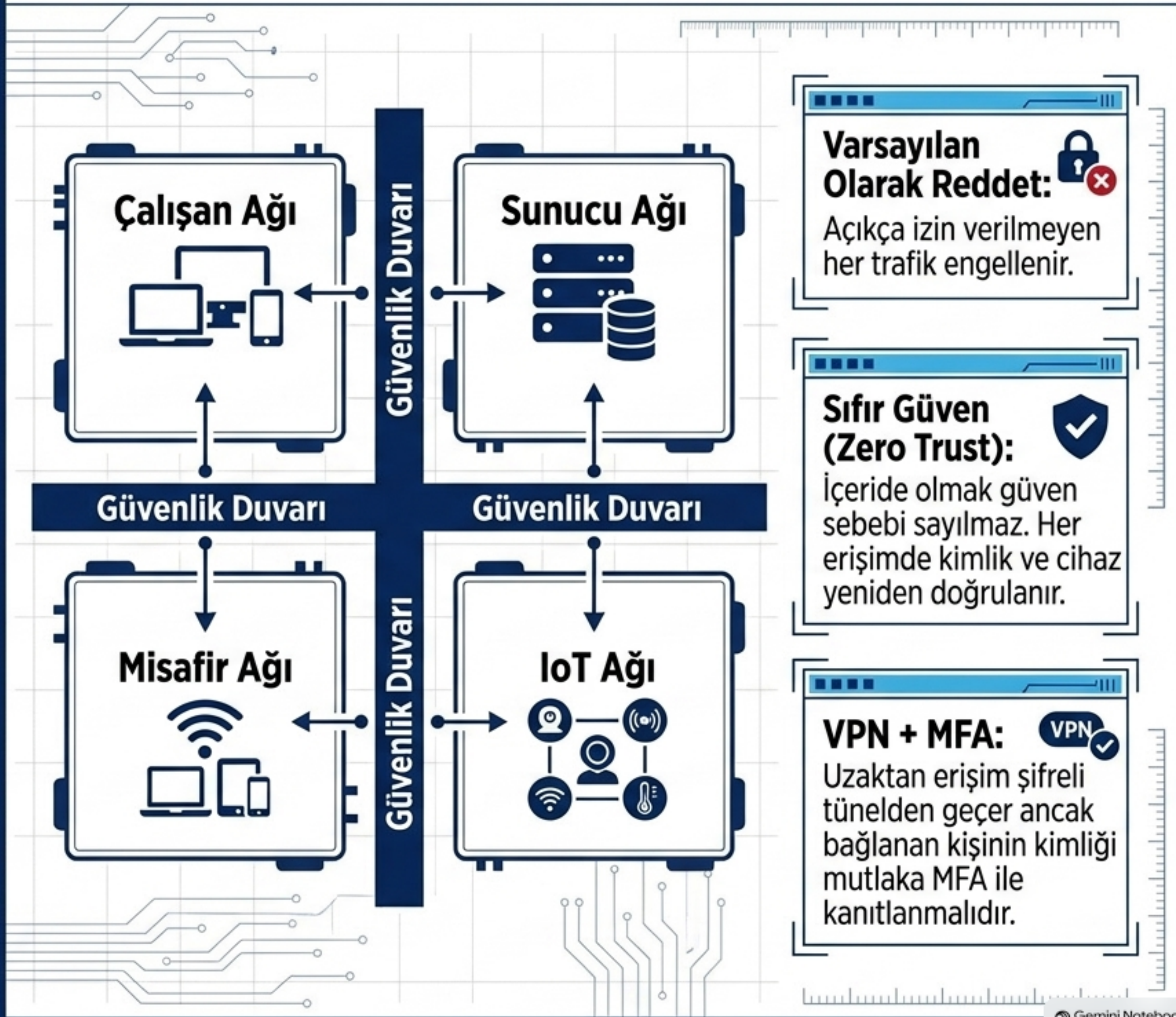
Parola yöneticisi
kullanımı



Kişisel bilgi
içermemesi

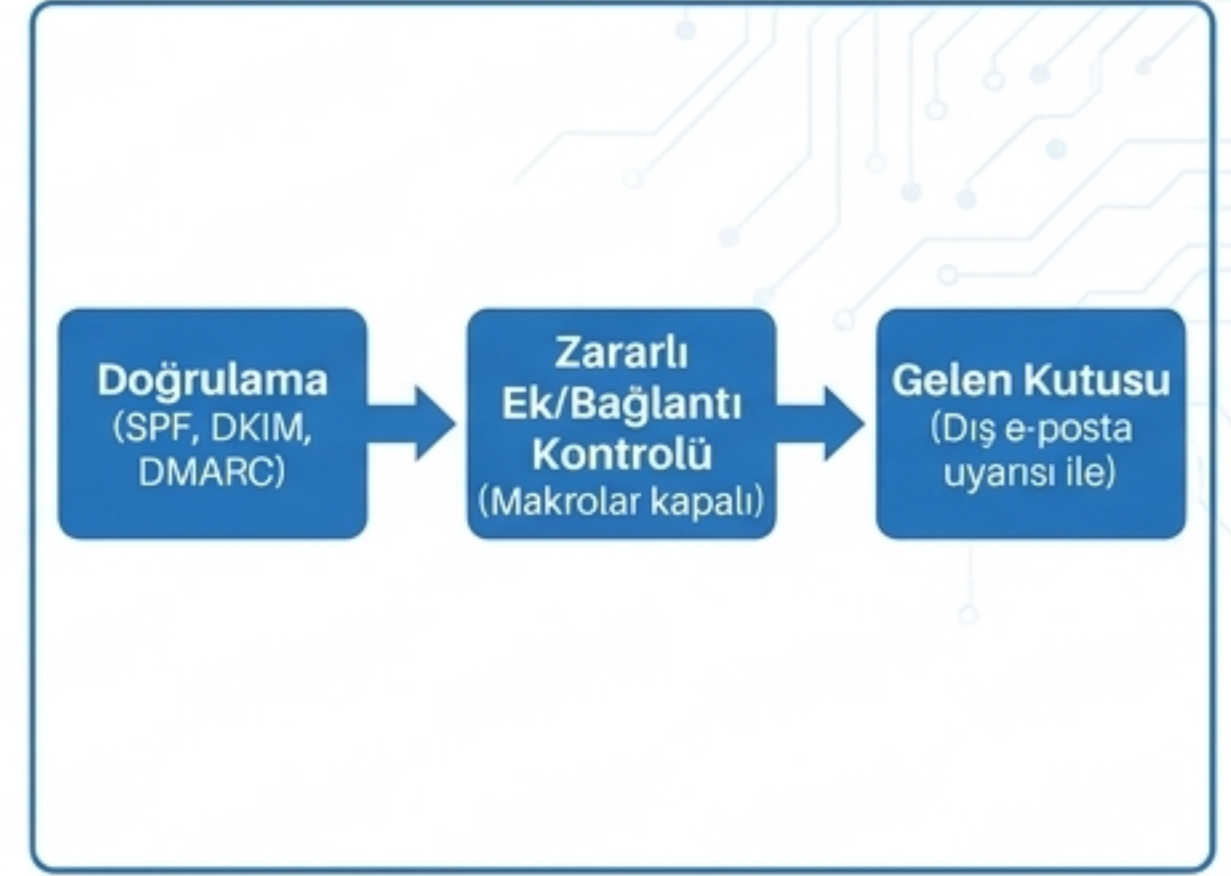
MODÜL 4

Ağ güvenliğine giriş



MODÜL 5

Uç nokta ve e-posta güvenliği,
güncelleme yönetimi



Yama Yönetim Döngüsü



MODÜL 6

Yedekleme ve iş sürekliliği

3 2 1 +1

Kopya Veri
(Asıl + 2 Yedek)

Farklı Ortam
(Disk, Bulut, vb.)

Uzak Konum
(Bina dışı)

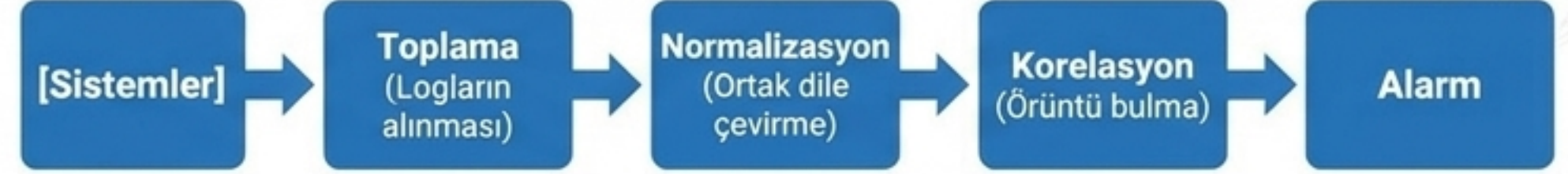
**Çevrimdışı /
Değiştirilemez**
(Fidye yazılımına
karşı korumalı)



MODÜL 7

Güvenlik izleme ve
SOC'un işleyişi

Log'dan Alarma SIEM Süreci



Triyaj Hunisi



MODÜL 8

Olay müdahalesi süreci



ALTIN KURAL:
Şüpheli bir
bilgisayarı kapatma!
Bellekteki delilleri
korumak için doğrudan
ağ bağlantısını
(kablo/wi-fi) kes.

MODÜL 9

Etik hackerlık ve sızma testi



Zafiyet Taraması

Otomatik araçlar, geniş kapsam, düzenli, doğrulanmamış açıklar.

Sızma Testi (Penetration Test)

Uzman onayı, hedeflenmiş, kontrollü istismar.

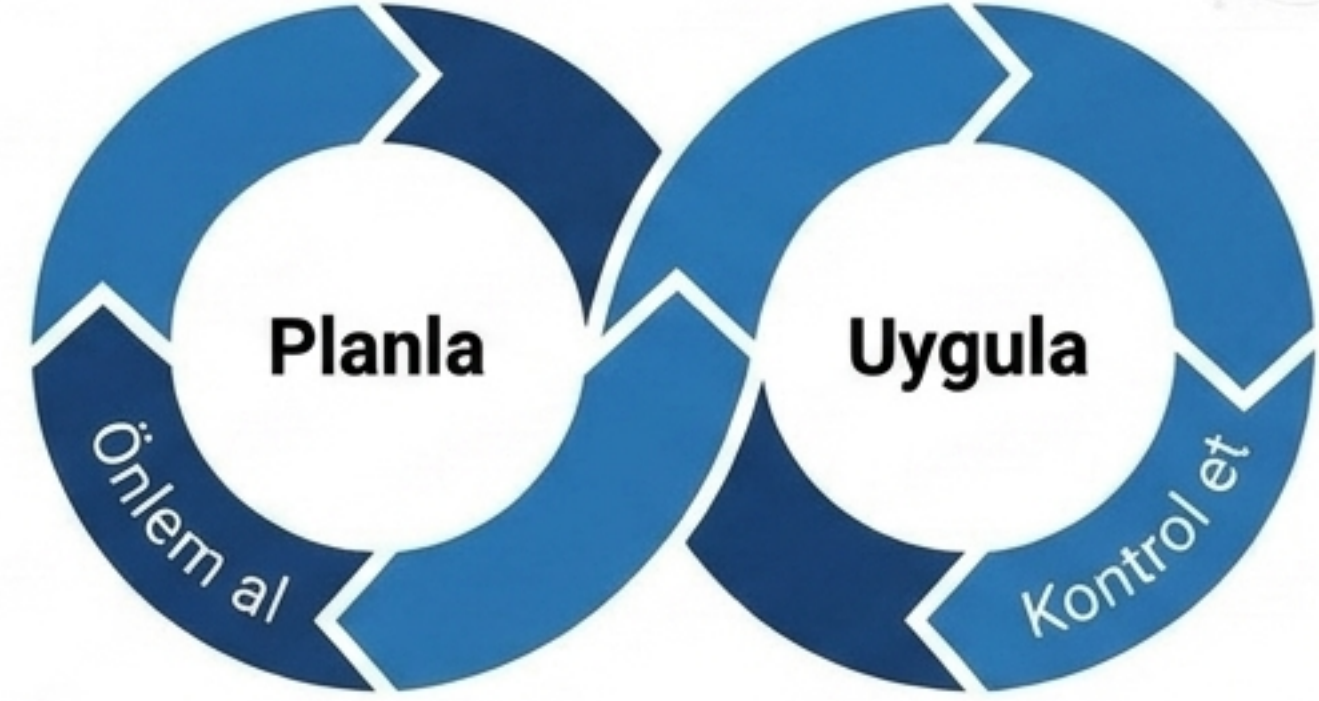
Kırmızı Takım

Gerçekçi saldırgan simülasyonu, savunma ekibini (mavi takım) sinama amaçlı.

MODÜL 10

Standartlar, mevzuat
ve güvenlik kültürü

ISO 27001 (PUKÖ Döngüsü)



KVKK Kuralı: Kişisel veri ihlallerinde, öğrenildiği andan itibaren en geç 72 saat içinde kurula bildirim yapılmalıdır.

Güvenlik Kültürü Sütunları

**Bildirim
Cezalandırılmaz
(Hata saklanmaz).**

**Yönetim
Örnek Olur
(Kurallara istisna
istenmez).**

**İşi
Kolaylaştıran
Çözümler
(Uygulanabilir
kurallar).**

Sonraki Adım: Bilginizi Doğrulayın

- Daphne Kariyer platformundaki ücretsiz testlerle öğreniminizi pekiştirin.
- Siber Güvenlik, Bilgi Güvenliği, Ağ Güvenliği, SOC Analistliği ve Siber Olay Müdahalesi testlerine katılın.
- Başarı durumunda doğrulanabilir dijital sertifikanızı alın.

daphnekariyer.com/dijital-yetkinlikler