

# BTRisk

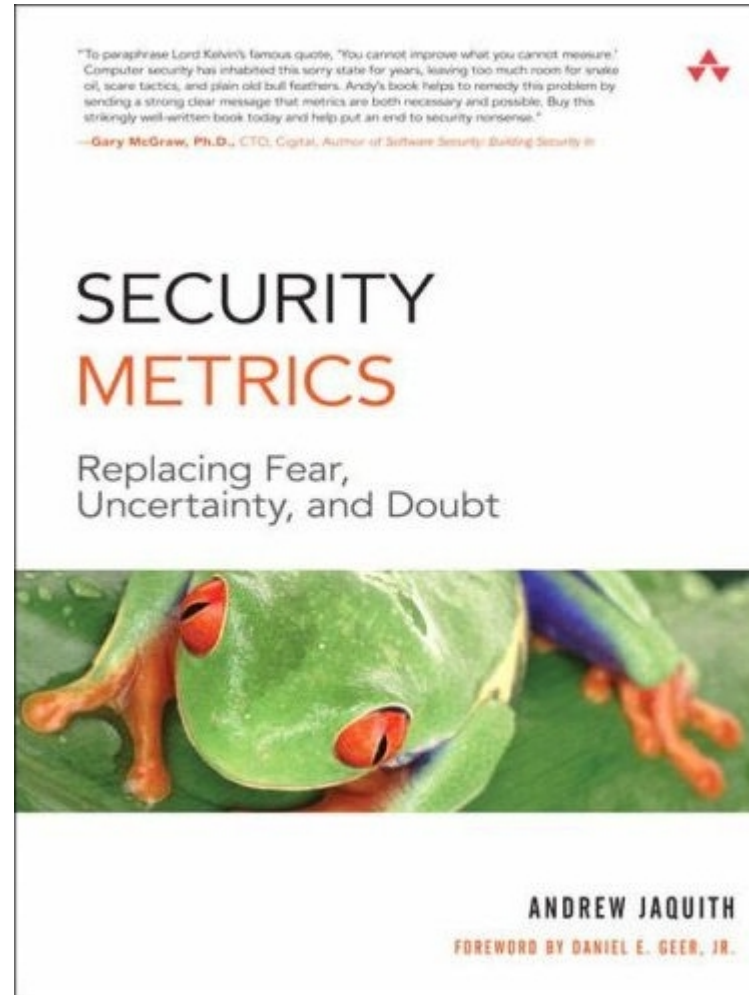
## Güvenlik Metrikleri

İstanbul Bilişim Kongresi

Fatih Emiral, CISSP, CISA, CIA, CEH

9 Haziran 2007

# Kredi

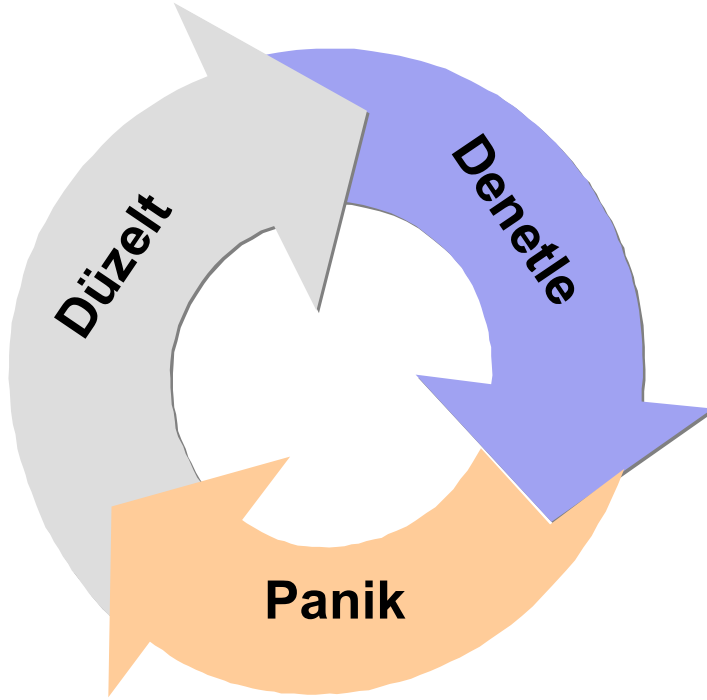


# Gündem

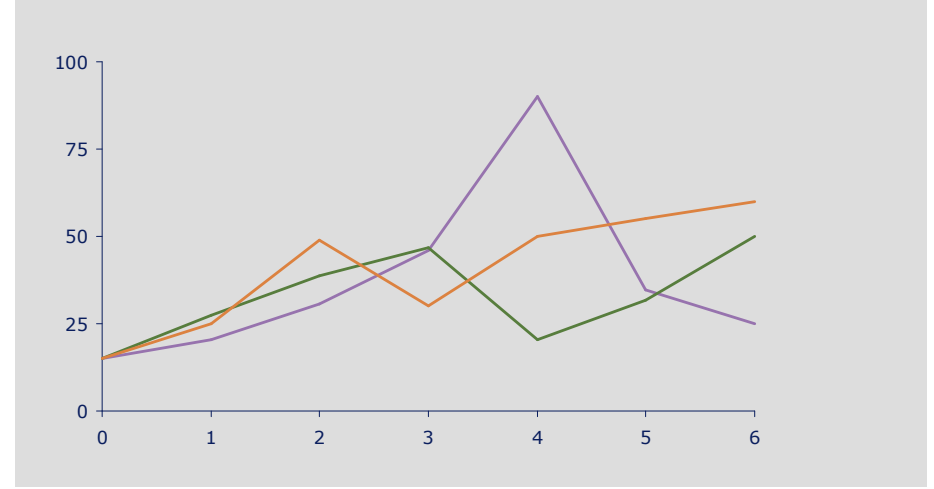
1. İyi Metriklerin Özellikleri
2. Problem Teşhis ve Teknik Güvenlik Metrikleri
3. Güvenlik Program Metrikleri
4. Dengeli Güvenlik Puan Tablosu

# Sonsuz Endişe Döngüsü

## Güvenlik Açıkları Denetim Döngüsü



## Metrik İzleme



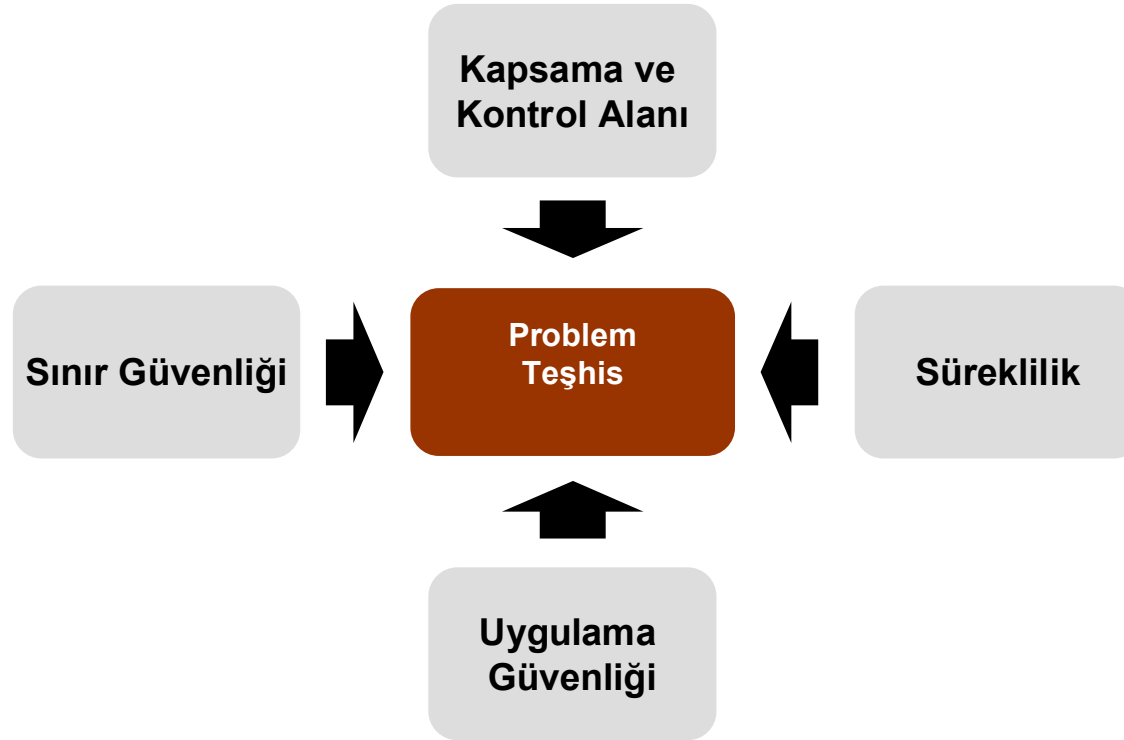
## İyi Metriklerin Özellikleri



# Gündem

1. İyi Metriklerin Özellikleri
2. Problem Teşhis ve Teknik Güvenlik Metrikleri
3. Güvenlik Program Metrikleri
4. Dengeli Güvenlik Puan Tablosu

# Problem Teşhis ve Teknik Güvenlik Metrikleri



# Sınır Güvenliđi

- E-Posta
  - Gnlk mesaj sayısı (#) (Normal mesaj hacmini takip edip anormallikleri tespit edebilme)
  - Yakalanan istenmeyen mesajlar (#, %) (E-posta kirlilik oran belirteci)
  - Yakalanamayan istenmeyen mesajlar (#,%) (İçerik filtreleme yazılım etkinliđinin takibi)
- Anti-Virs/Casus Yazılım
  - Kullanıcı dosyalarında tespit edilen virsler (sunucularda, masa st ve diz st bilgisayarlarda) (#) (Enfeksiyon oranı belirteci)
  - Manuel mdahale gerektiren virs olayları (#, %) (Temizlik iin manuel mdahale gereklilik oranı)
  - Virs olayları temizlik masrafı (iř birimi bazında) (YTL) (Virs olaylarının neden olduđu personel masrafı)
- Ađ Sınır Güvenliđi
  - Koruma duvarı kural deđiřiklik sayıları (iř birimi bazında) (#) (Gvenlik ihtiya karmařıklık belirteci)
  - Sınır gvenlik araları bakımı personel kaynađı (# tam zamanlı personel) (Destek iin gerekli personel sayısının takibi)
  - İnternet sunucularına dıřarıdan bađlantılar (TCP/UDP port bazında, sunucu tip veya grubu bazında) (#) (İeri dođru internet aktivite belirteci)
  - Merkezi sistemlere koruma duvarı olmaksızın bađlanan uzak yerleřkeler (#) (Ađ gvenlik blmleme seviyesi)
- Saldırıları
  - Saldırı sayıları (#) (Tehdit dzeyi)
  - Bařarılı saldırı sayıları (iř birimi, cođrafi yerleřim bazında) (#,%) (Sınır gvenlik nlemlerinin etkinlik derecesi)

# Kapsama ve Kontrol Alanı

- Anti-Virüs/Casus Yazılım
  - Anti-Virüs yüklü bilgisayarlar (çalışma istasyonu ve sunucu bazında) (#,%) (Anti-Virüs kontrollerinin kapsamı)
  - Güncel virüs imzalarına sahip bilgisayarlar (#,%) (Anti-Virus kontrolünün etkinlik belirteci)
- Yama Yönetimi
  - Yama politikasını karşılamayan bilgisayarlar (sunucu tipi, yerleşim, vd. bazında) (%) (Yama sürecinin etkinlik belirteci)
  - Dönemsel olarak uygulanan yamalar (#, bilgisayar başına #) (Yama iş yükü belirteci)
  - Uygulanmamış yamalar (kritik yamalar, iş birimleri, coğrafi dağılıma göre) (ortalama ve medyan) (Bekleyen yama iş yükü belirteci)
  - Uygulanmamış yama bekleme süreleri (her bilgisayar için) (gün) (Potansiyel zayıflık penceresi belirteci)
- Konfigürasyon
  - Bilgisayar karşılaştırma puanları (Güvenlik standart konfigürasyonu uygulama derecesi)
  - Standart imaj ile kurulan bilgisayarlar (%) (Çalışma istasyonları ve dizüstü bilgisayarların standart kurulum imajına uyum derecesi)
  - Uzak yerleşimlerdeki bilgisayarlar yönetilebilme yüzdesi (%)
  - Loglama kapsama alanı (# bilgisayar, %)
  - Aktif olarak izlenen kritik sistem oranı (%)

# Kapsama ve Kontrol Alanı

- Açıklık Yönetimi
  - Zayıflık tarayıcı kapsamı (#, %, sıklık frekansı) (Bilgisayar sayısı ve süre göz önüne alındığında denetim kapsam ve yoğunluk belirteci)
  - Aylık zayıflık sayıları (kritiklik, iş birimi, coğrafi dağılım bazında) (#)
  - Zayıflık sayılarındaki aylık net değişim (%)
  - Zayıflık tespit gecikme süresi (zaman)
  - Tespit edilen zayıflıkların kapatılma süresi (zaman)

# Süreklilik

- Ayakta kalma süresi
  - Sunucu ayakta kalma süreleri (kritik sunucular ve tüm sunucular için) (% , zaman)
  - Planlanmamış kesintiler (%) (Büyük yüzdeler daha az kontrollü ortamlara işaret eder)
  - Güvenlik olaylarına bağlı planlanmamış kesintiler (% , zaman)
  - Sistem tarafından desteklenen gelir miktarı (kritik sunucular için) (saatlik maliyet) (Kesintilerle birlikte yorumlanmak için kullanılır)
  - Kesintiler arasındaki ortalama zaman (zaman)
- Sistem Kurtarma
  - Destek müdahale zamanı (ortalama zaman)
  - Kurtarma süreci ortalama zamanı (ortalama zaman)
  - Son kurtarma testinden bu yana geçen zaman (süreç kritik sistemler için) (gün)
- Değişiklik Kontrolü
  - Dönem başına gerçekleşen değişiklik sayısı (#) (Normal gerçek ortam değişiklik yoğunluğu hakkında fikir verir)
  - Dönem başına acil değişiklik sayısı (#, %) (Özel durumların hangi sıklıkta gerçekleştiğine dair fikir verir)
  - Değişiklik prosedür ihlalleri (#, %)

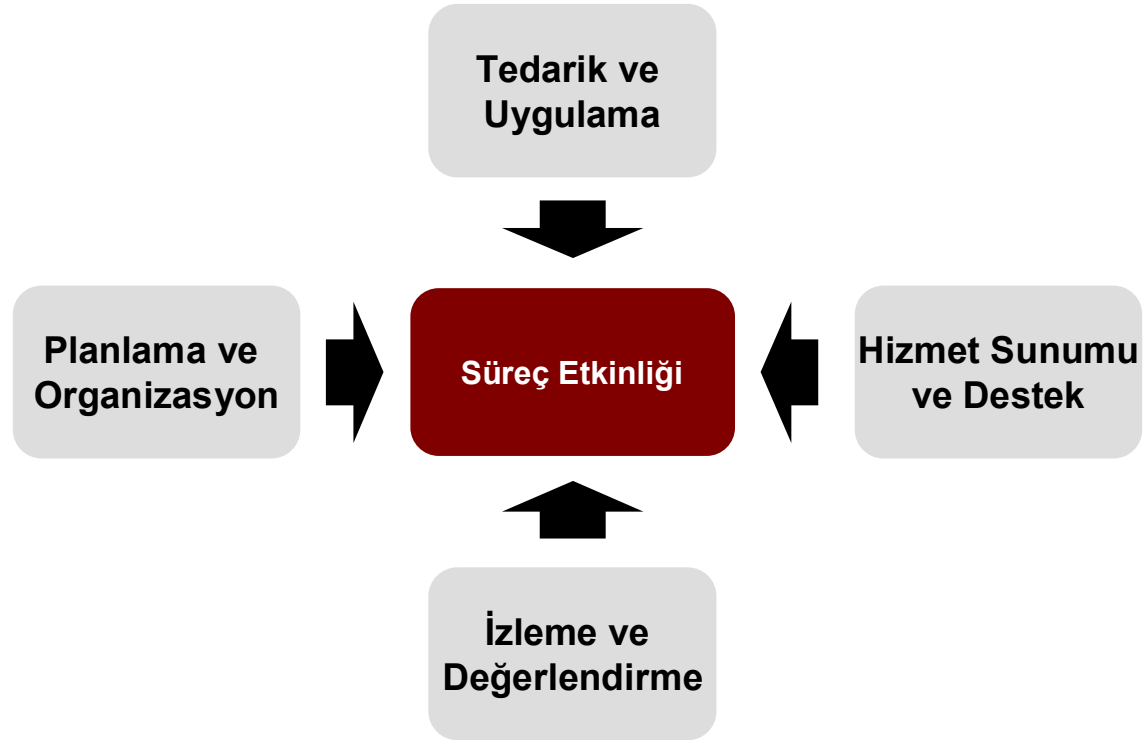
# Uygulama Güvenliđi

- Kara kutu testi bulgu metrikleri
  - Uygulama başına tespit edilen zayıflık sayısı (iş birimi ve kritikliğe göre) (#)
- Kalitatif süreç metrik ve endeksleri
  - Göreceli iş riski (zayıflığın derecesi ve iş kritikliği çarpımı sonucu ulaşılan sonuç)
  - Uygulama güvenlik risk endeksi (erişim profili, kritik veri barındırma, vb. gibi çeşitli risk faktörlerine göre uygulama bazında risk endeksi)
- Kaynak kodu güvenlik metrikleri
  - Uygulama geliştirme sürecindeki değerlendirme sıklığı (tasarım, kod inceleme ve gerçek ortam öncesi saldırı testleri bazında) (%)
  - Satır sayısı (bin satır bazında)
  - Her bin kod satırı başına düşen zayıflık sayısı (#)
  - Karmaşıklık değeri (cyclomatic complexity)

# Gündem

1. İyi Metriklerin Özellikleri
2. Problem Teşhis ve Teknik Güvenlik Metrikleri
3. Güvenlik Program Metrikleri
4. Dengeli Güvenlik Puan Tablosu

# Güvenlik Program Metrikleri



# Planlama ve Organizasyon

- BT risklerinin değerlendirilme ve yönetimi
  - Güvenlik standartlarına uyumlu sistemler üzerinde bulunan kritik varlık / fonksiyonların yüzdesi (%)
  - Fiziksel güvenlik riskleri değerlendirilmiş kritik varlık / fonksiyonların yüzdesi (%)
  - Saldırı sonucu oluşabilecek hasar tahmini yapılmış kritik varlık / fonksiyonların yüzdesi (%)
  - Risk analizi dokümante edilmiş kritik varlık / fonksiyonların yüzdesi (%)
  - Risk tedavi planı dokümante edilmiş kritik varlık / fonksiyonların yüzdesi (%)
- BT insan kaynakları yönetimi
  - Bilgi güvenliği sorumluluklarını da içeren performans değerlendirme yüzdesi (%)
  - Bilgi güvenliği sorumluluk ve yetkinliklerini içeren iş tanımlarının yüzdesi (%)
  - Özgeçmiş ve sabıka kontrolü yapılmış personelin yüzdesi (%)
  - İş birimlerindeki (gölge) bilgi güvenliği sorumlularının merkezi bilgi güvenliği personeline oranı (%)
- BT yatırım yönetimi
  - Güvenlik bütçe tutarı (YTL)

# Tedarik ve Uygulama

- Otomasyon çözümlerinin tanımlanması
  - Müşteri ve iş ortakları ile yapılan alışverişlerdeki gizlilik kontrolleri uygulanma oranı (%)
  - Müşteri ve iş ortakları ile yapılan alışverişlerdeki bütünlük kontrolleri uygulanma oranı (%)
  - Kurum dışına açık uygulamaları geliştiren personel ile güvenlik ekibi arasındaki görüş alışverişlerinin sayısı (#)
  - İş birimleri ile güvenlik ekibi arasındaki görüş alışverişlerinin sayısı (#)
  - Güvenlik riskleri proje başında değerlendirilmiş yeni sistemlerin oranı (%)
- Çözümlerin akreditasyonu, kurulumu ve değişiklik yönetimi
  - Kurum dışına ve müşteriye açık akredite edilmiş (iş sahibi tarafından risk kabulü imzalanmış) uygulamaların oranı (%)
  - Güvenlik akreditasyonu yapılmış uygulamaların oranı (%)
  - Güvenlik sertifikasyonu yapılmış (test edilip uygunluğu görüşmüş) sistemlerin oranı (%)
  - Güvenlik kontrol maliyetleri bütçeye konulmuş sistemlerin oranı (%)
- Operasyon ve kullanıma geçiş
  - Operasyonel politika ve kontrolleri tanımlı sistemlerin oranı (%)

## Hizmet Sunumu ve Destek

- Kullanıcı eğitimi
  - Güvenlik farkındalık eğitimini almış yeni personel oranı (%)
  - Farkındalık eğitimi tazelenmiş eski personel oranı (%)
  - Profesyonel güvenlik sertifikası sahibi güvenlik personel oranı (%)
  - Parola kalitesi ile son eğitim süresi arasındaki korelasyon değeri (iş birimi bazında)
  - Fiziksel giriş kontrolleri ihlal oranları ile son eğitim süresi arasındaki korelasyon değeri (ofis bazında)
- Sistem güvenliğinin sağlanması
  - Tek kişiye bağlı maksimum aktif kullanıcı kodu değeri (#)
  - Yüksek erişim yetkisine sahip olup son dönemde erişim hakları gözden geçirilmiş personel yüzdesi (%)
  - İşten ayrılmış yüksek yetkili personelin son dönemde erişim hakları gözden geçirilme oranı (%)
  - Üzerinde rollerin ayrımı ilkesinin uygulandığı sistem ve uygulama oranı (%)
  - Parola politikasının uygulandığı sistem ve uygulama oranı (%)
- BT maliyetlerinin belirlenmesi ve atanması
  - Gelir sürecini destekleyen sistemler için gerçekleşen güvenlik maliyeti
  - İş birimlerine yansıtılan güvenlik masraflarının oranı (%)
  - Gerçekleşmiş güvenlik ihlalleri sonrası oluşan maliyetlerin tutarı (YTL)

## Hizmet Sunumu ve Destek

- Veri yönetimi
  - Müşteri ve iş ortakları ile alıp verilen veri miktarı (MByte)
  - Müşteri verisinin toksiklik oranı (kişiyeye bağlanabilen bilgilerin toplam veriye oranı)
  - Kurum dışında saklanan veri yedeklerinin oranı (%)
  - İmha ve temizlik prosedürüne uygun olarak işlem görmüş veri saklama araçlarının oranı (%)
- Tedarikçi yönetimi
  - Tedarikçi ve iş ortağı erişim hakları verilme ve geri alınma süreç zaman ortalamaları (zaman)
  - Tedarikçi ve iş ortakları kontratlarında güvenlik gereksinimlerinin belirtilme oranı (%)
  - Tedarikçi ve iş ortakları kullanıcılarının erişim hakları son dönem gözden geçirilme oranı (%)

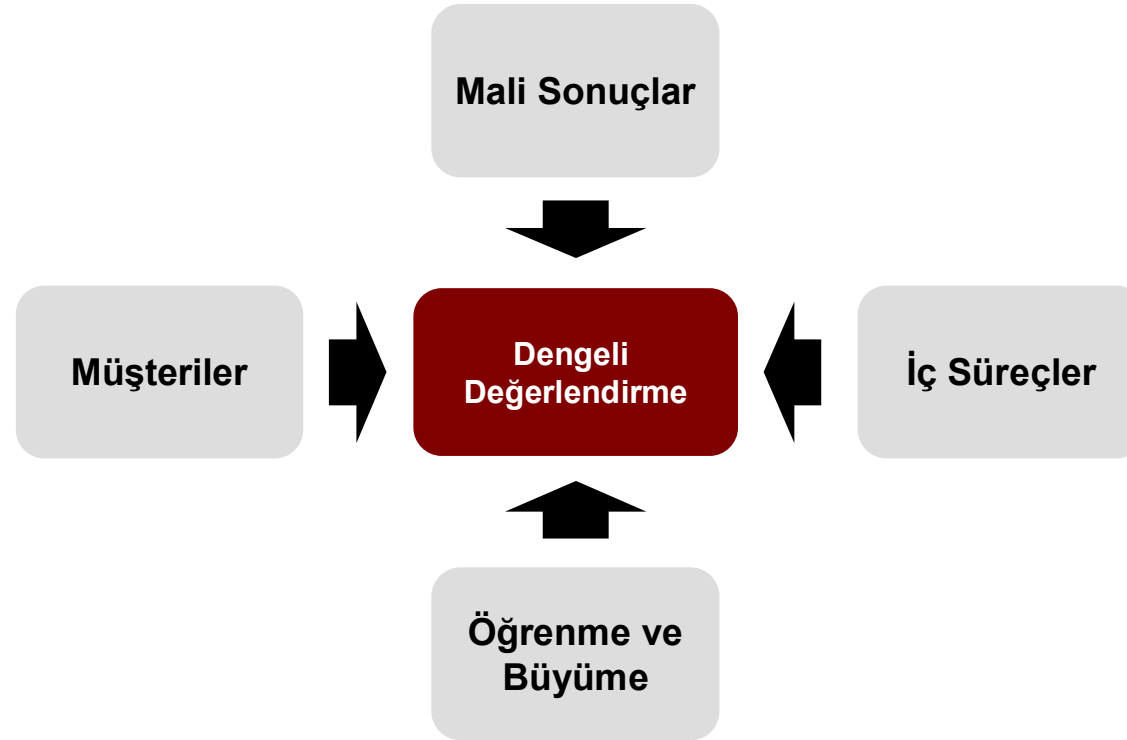
# İzleme ve Değerlendirme

- Sürecin izlenmesi
  - Logları izlenen sistemlerin oranı (%)
  - Müşterilere ve internete açık sistemlerin log izleme oranı (%)
  - Güvenlik konfigürasyonlarının kurumsal standartlara uygunluğu izlenen sistemlerin oranı (%)
- İç kontrollerin izlenmesi ve değerlendirilmesi
  - Kontrol uyumluluğu gözden geçirilen kritik sistemlerin oranı (%)
  - Kontrol uyum kontrolü yapılan üçüncü taraf ilişkileri oranı (%)
  - Tasarlandığı gibi çalışan kontrol oranı (%)
  - En az bir kritik zayıflığı bulunan sistemlerin oranı (%)
- Düzenlemelere uyumun sağlanması
  - Başarı ile tamamlanan kanuni denetimlerin sayısı (#)
  - Düzeltilmeyi bekleyen denetim bulguları (#) ve yaklaşık maliyetleri (zaman, YTL)
  - Düzenlemelere uyumlu anahtar kontrollerin oranı (%)
  - Kritik bulgu içeren güvenlik uyum denetimlerinin oranı (%)

# Gündem

1. İyi Metriklerin Özellikleri
2. Problem Teşhis ve Teknik Güvenlik Metrikleri
3. Güvenlik Program Metrikleri
4. Dengeli Güvenlik Puan Tablosu

## Dengeli Güvenlik Puan Tablosu



## Mali Sonular

- Gvenlikle iliřkili hedefler:
  - Gelir srecini destekleyen sistemlerin yksek kullanımı
  - Gelir srecini destekleyen sistemlerin btnlğnn ykseltilmesi
  - Gelir muhasebe srecinin btnlğnn ykseltilmesi
  - Gelir srecini destekleyen sistemlerin kullanımından doėabilecek risklerin azaltılması
  - Gvenlik maliyetlerinin dřrlmesi
  - Sistem kesinti maliyetleri ve gvenlik ihlalleri ile doėrudan iliřkili maliyetlerin dřrlmesi
- Mali sonuları etkileyen rnek gvenlik metrikleri
  - Gelir srecini destekleyen sistemlerle verilen sipariř sayı ve miktarları (#, YTL)
  - Sistem ayakta kalma zamanı (zaman)
  - Hizmet kesintisi saldırıları nedeniyle oluřan gelir kayıpları (YTL)
  - Mřteriler, tedarikiler ve iř ortakları ile veri alıř veriř miktarı (MByte)
  - Gelir srecini destekleyen sistemlerin gvenlik maliyeti (YTL)
  - Gvenlik ihlalleri sonucu oluřan maliyetler (YTL)
  - Gvenlik btesi (YTL)
  - Gelir srecini destekleyen sistemlerin risk indeksleri

# İç Süreçler

- Güvenlikle ilişkili hedefler:
  - Bilgi varlıklarının korunması
  - Kullanıcı erişim hakları verilme ve geri alma işlemlerinin hızlı biçimde yapılması
  - Gereksiz erişim haklarının en aza indirilmesi
  - Teknolojik gelişmelere uyum kabiliyetinin artırılması
  - Güvenlik risklerinin anlaşılması, kabul edilmesi veya iyileştirme yoluna gidilmesinin sağlanması
  - Güvenlik zayıflıklarının tespit edilmesi
- İç süreçleri etkileyen örnek güvenlik metrikleri
  - Güvenlik maliyetlerinin bütçelendiği iş yatırımlarının oranı (%)
  - Yama gecikme süresi (teknoloji ortamı bazında) (zaman)
  - Son dönemde gözden geçirilen kritik erişim haklarına sahip kullanıcı oranı (%)
  - Logları izlenen sistem oranı (%)
  - Güvenlik akreditasyonuna sahip sistem oranı (%)
  - İş sürekliliği planına sahip iş birimi oranı (%)
  - Yeni kullanıcı ekleme ve kullanıcı erişim hakları kaldırma süreleri (zaman)
  - Güvenlik ihlalleri dolayısı ile oluşan kesintiler arası ortalama zaman (zaman)

# Öğrenme ve Büyüme

- Güvenlikle ilişkili hedefler:
  - Güvenlik farkındalığının yayılması
  - Güvenlik imkanların anlaşılması ve kullanımının etkinleştirilmesi
  - Güvenlik yönetim sorumluluklarının iş birimlerine delege edilmesi
  - Bilgi güvenliği ekibi ve iş birimleri arasındaki iş birliğinin güçlendirilmesi
  - Güvenlik ekibinin yetkinlik ve sertifikasyon düzeyinin artırılması
- Öğrenme ve büyümeyi etkileyen örnek güvenlik metrikleri
  - İş birimlerinde güvenlik sorumluluğu taşıyan personelin merkezi güvenlik ekibine oranı (%)
  - Güvenlik farkındalık eğitimini tamamlayan yeni personelin oranı (%)
  - İş birimleri ile güvenlik ekibi arasında gerçekleşen görüş alış verişi sayısı (#)
  - Güvenlik sertifikasyonuna sahip güvenlik personel oranı (%)
  - İş tanımında güvenlik sorumluluk ve yetkinlik tanımları bulunan personel oranı (%)
  - Operasyonel prosedürleri tanımlı iş birim oranı (#)

# Müşteriler

- Güvenlikle ilişkili hedefler:
  - Kurum hizmet ve ürünlerinin çekiciliğini artırmak
  - Müşteri siparişlerinin sayısının artırılması
  - Müşteriler ve iş ortakları ile yapılan elektronik işlemlerin artırılması
  - Elektronik iletişim imkan ve alternatiflerinin artırılması
  - İşlem bütünlüğü güvencesinin artırılması
  - Kaza sonucu müşteri ve iş ortakları verilerinin istenmeyen kişilerin eline geçme riskinin azaltılması
- Müşteri memnuniyetini etkileyen örnek güvenlik metrikleri
  - Müşteri kazanma ve kaybetme oranları (%)
  - Güvenlik konusunun önemli bir kriter olduğu yeni kazanılan işlerin sayısı (#)
  - Güvenlik konusundaki problemler dolayısı ile kaybedilen müşteri sayısı ve oranı (#, %)
  - Bilgi sistemlerine müşteri erişim hakları verme ve alma süreleri (zaman)
  - Dışarıya açık sistemlerin ayakta kalma süreleri (zaman)
  - Müşteri ve iş ortakları ile işlem sayısı (#)
  - Müşteri ve iş ortaklarının karıştığı güvenlik ihlal sayısı (#)
  - Kritik erişim haklarına sahip iş ortakları son dönem gözden geçirme oranı (%)