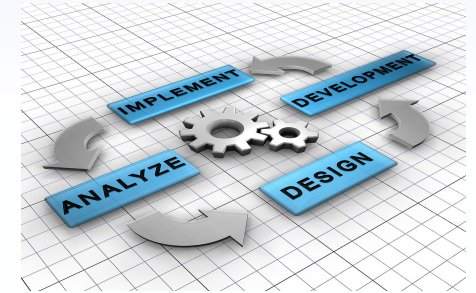
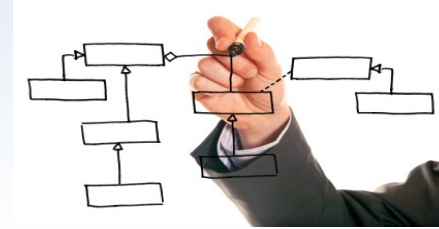


Kurumsal Bilgi Sistemleri ve Güvenlik

Kenan Sevindik Kimdir?

- 15 yıllık kurumsal uygulama geliştirme deneyimi var
- Çeşitli projelerin mimarilerinin oluşturulmasında görev aldı
- Spring, Spring Security, Hibernate, Vaadin gibi kurumsal Java teknolojilerinde kapsamlı bilgi birikimi ve deneyime sahip



Kenan Sevindik Kimdir?

- 2011 yılında **Harezmi Bilişim Çözümleri**ni kurdu
- Kurumsal uygulama geliştirme yapıyor
- Danışmanlık ve koçluk hizmetleri sunuyor
- Kurumsal Java Eğitimleri adı altında eğitimler düzenliyor
- **Beginning Spring** kitabının yazarlarından



Mimari Nedir?

Mimari, bir sistemin **yapısal organizasyonunu** ifade eder



Sistemin bütüncül biçimde ortaya çıkması ve idame ettirilebilmesi için yapılması gereken faaliyetlerinin belirli **prensip**ler üzerine oturtulmasını sağlar

Sistemi oluşturan bileşenleri ve bu **bileşenlerin** birbirleri ve çevreleri ile olan **entegrasyonunu** ortaya koyar

Kurumsal bilgi sistemleri mimarisi, bir organizasyonun iş süreçlerini ve faaliyetlerini yerine getirmek için kullandığı **teknolojileri** ve **bilgi sistemlerini** kapsar

Kurumsal Güvenlik Mimarisi

- Kurumsal bilgi sistemleri mimarisinin **temel yapı taşıdır**
- Kurumsal mimari oluşumunda güvenlik ihtiyaçlarını **ilk andan** itibaren ele almak önemlidir
- Kurumun fonksiyonlarının **emniyetli ve kesintisiz** biçimde sürdürülmesi sağlanabilir



- Farklı uygulamaların ve hizmetlerin **kendine özgü veya eksik güvenlik yaklaşımları** nedeni ile bilgi sistemleri altyapısının zafiyete uğraması ihtimali azalacaktır
- Uçtan uca **tutarlı ve standart** bir güvenlik modeli hakim kılınabilecektir

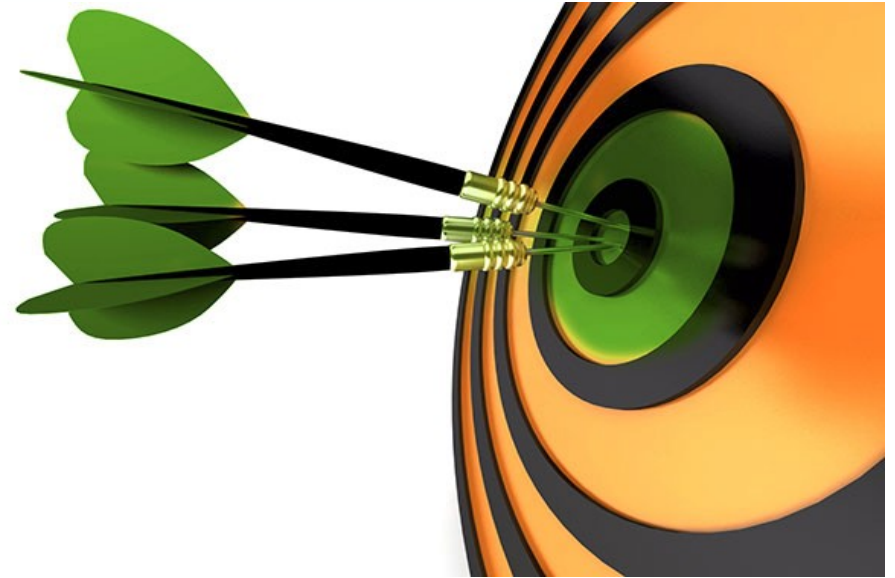
Kurumsal Güvenlik Mimarisinin Amacı Nedir?

Kurumsal güvenlik mimarisinde ana hedef
kurumun verisinin güvenliğini sağlamaktır

Verinin **gizliliğinin**
sağlanması

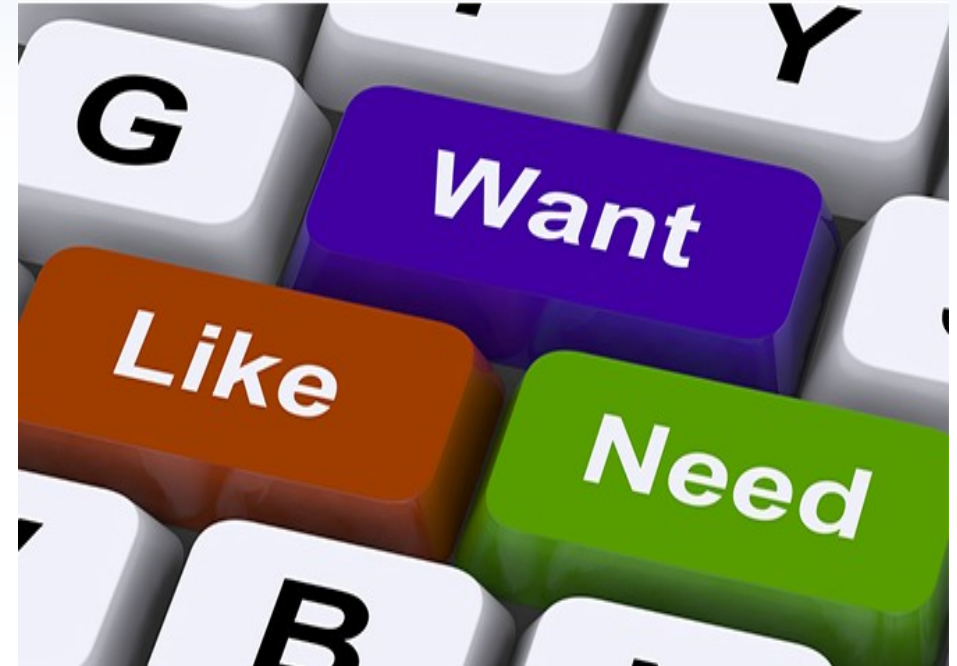
Verinin **tutarlılığının**
korunması

Verinin **sürekli**
erişilebilir kılınması



Güvenlik İhtiyaçları Nasıl Belirlenir?

- Kurumsal güvenlik gereksinimlerini belirleyen temel faktörler:
 - Kurumun yerine getirdiği **iş faaliyetleri**,
 - Dışarıdan veya içeriden kaynaklanacak **güvenlik tehditleri**,
 - Kurumun uyması veya yerine getirmesi gereken **yasal düzenlemeler** ve **standartlar**



Kurumsal Güvenlik Mimarisinin Bölümleri



Kurumsal güvenlik mimarisi
üç ana bölümde incelenebilir

Kimliklendirme

Kimliklendirme herhangi bir sisteme veya uygulamaya erişen kullanıcının kimliğinin tespit edilmesi sürecidir

Kullanıcıyı tanımlayan benzersiz niteleyici

Kullanıcı



Bilgisayar Sistemi

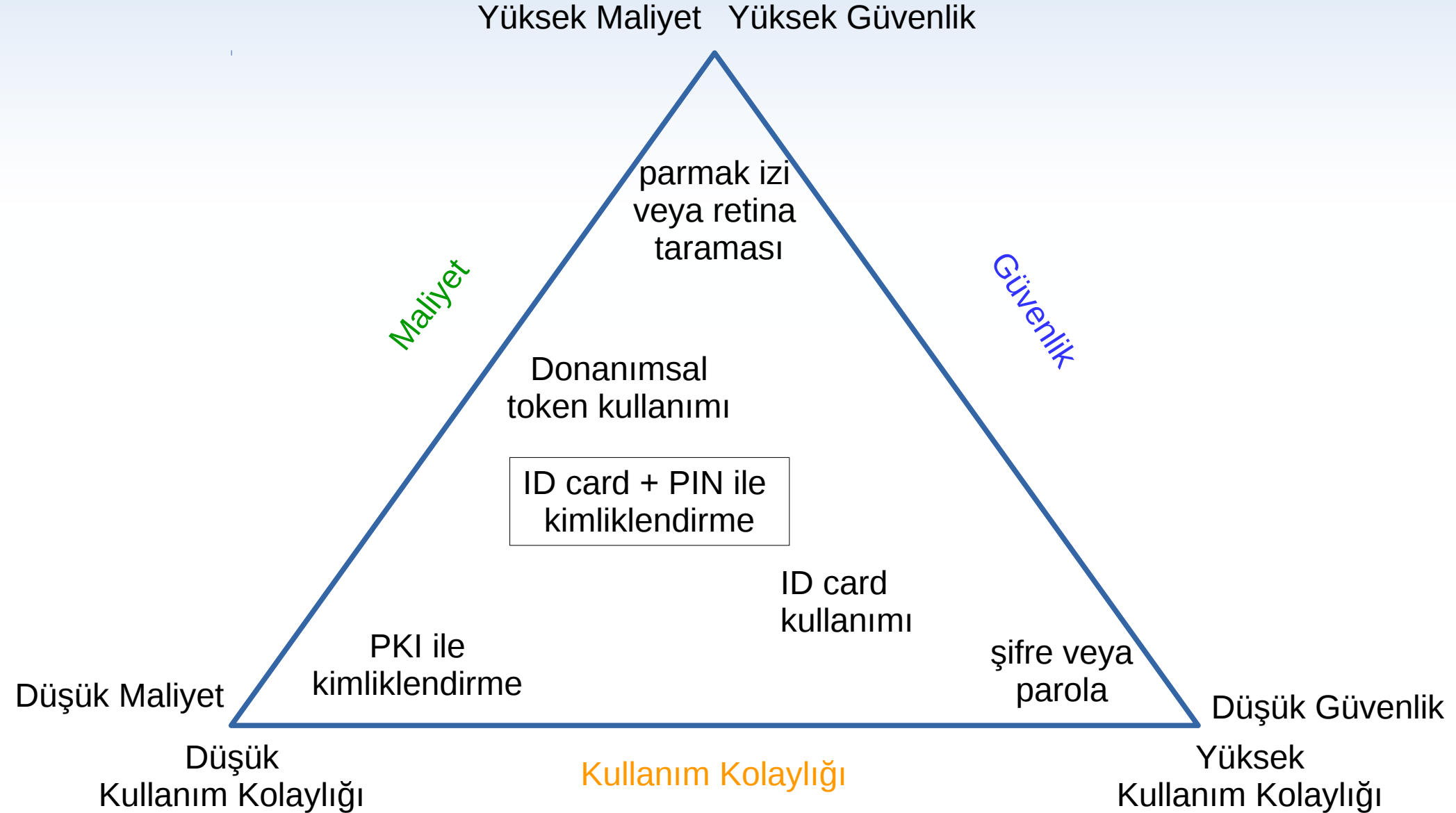


+



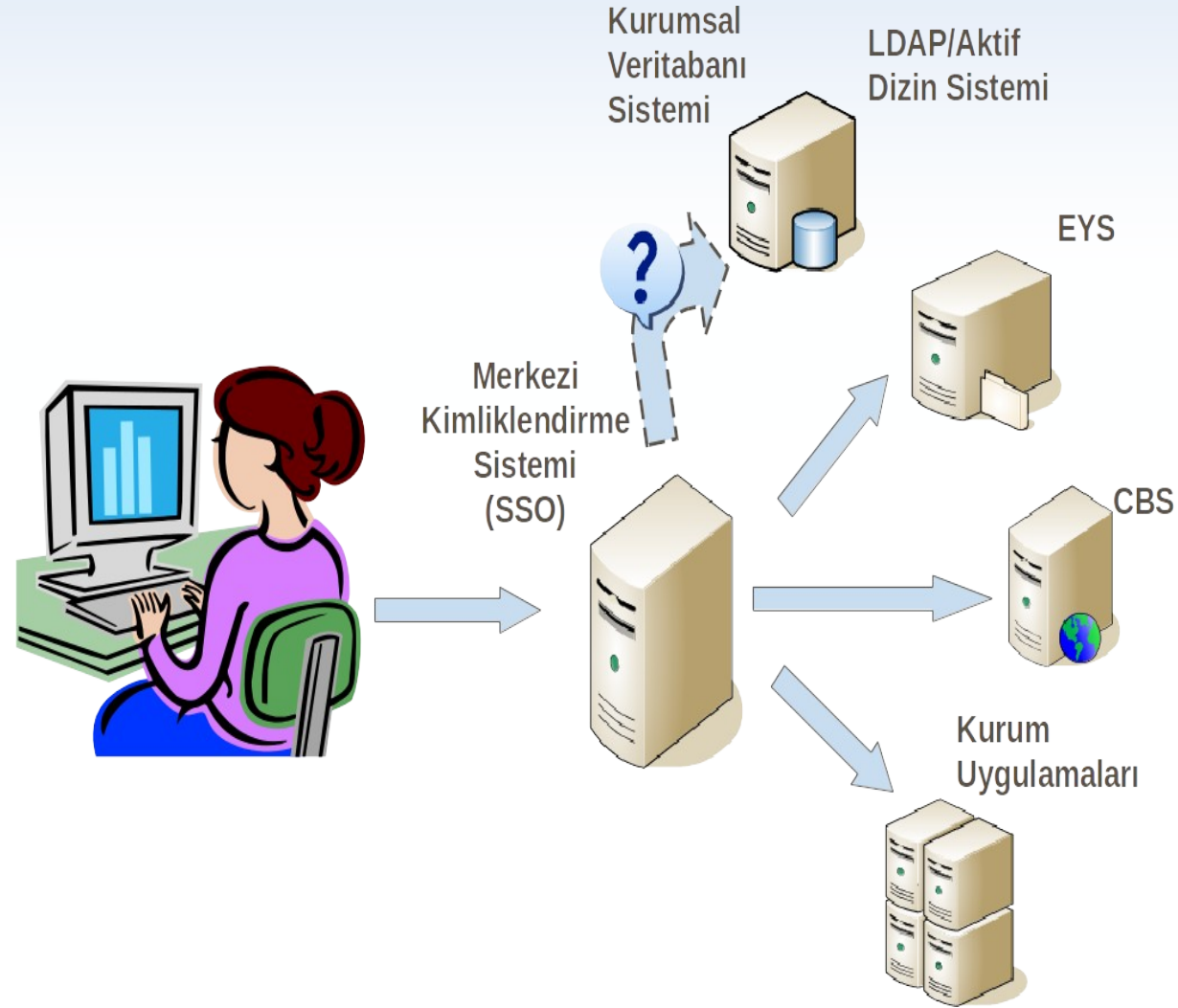
Sadece kullanıcının bildiği veya sahip olduğu
gizli bir bilgi veya özellik

Kimliklendirme Yöntemleri



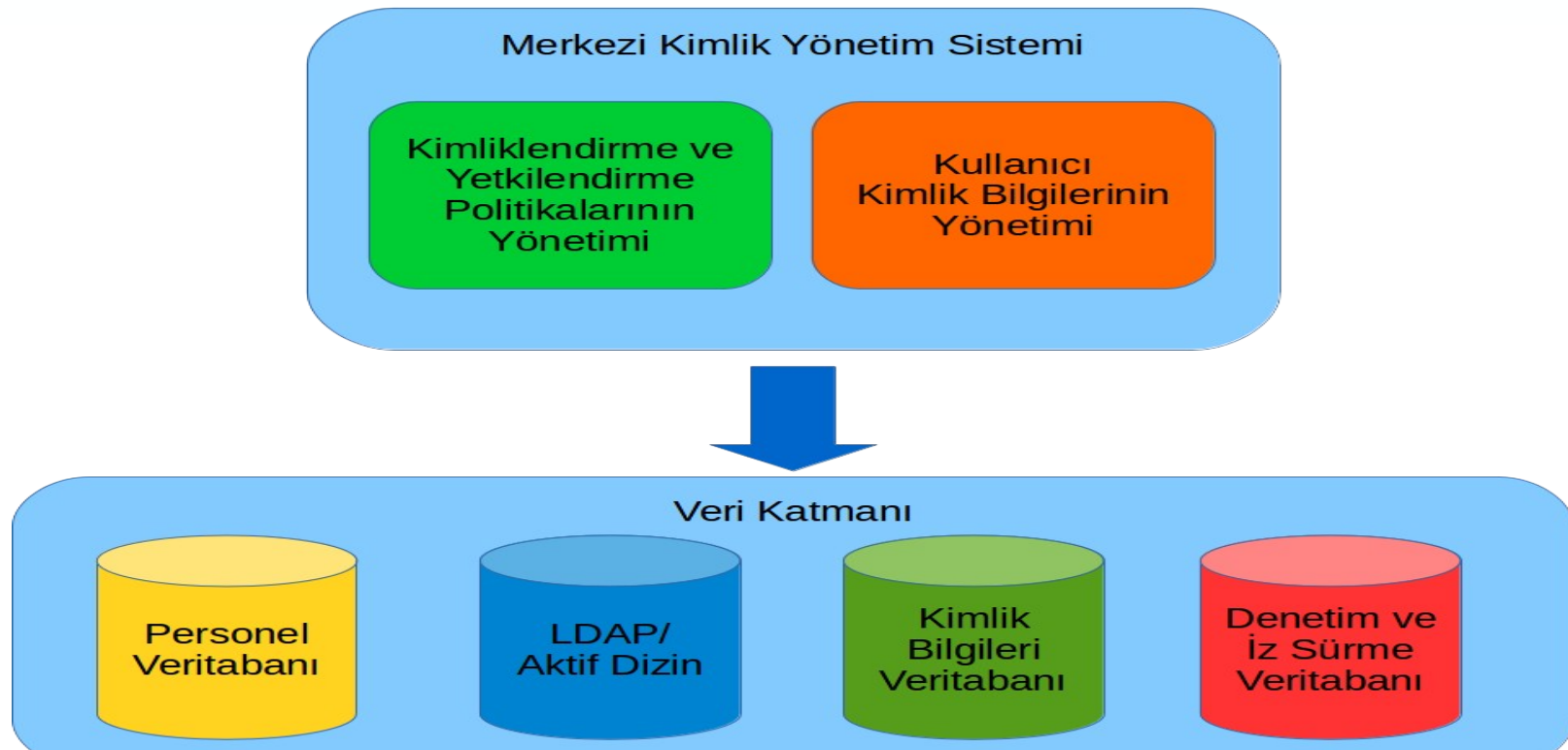
Merkezi Kimliklendirme Sistemi

- Her bir uygulamanın kendi **kimliklendirme işlemi**ni yapması yerine bunun merkezi bir kimliklendirme sunucusu tarafından sağlanması da mümkündür
- Bu sayede farklı uygulamaların kullanıcıya ait **gizli kimliklendirme bilgisi**ne erişme ihtiyacı ortadan kalkacaktır
- Kurum genelinde kimliklendirme hizmeti **standart**laşacak ve **daha emniyetli** bir hal alacaktır



Merkezi Kimlik Yönetim Sistemi

- Kurumsal bilgi sistemindeki farklı işletim sistemlerinin, ağ cihazlarının, sunucuların ve uygulamaların **kullanıcı bilgilerinin ortak bir sistem tarafından yönetilmesini** sağlar
- Kullanıcı bilgilerinin yanında kullanıcının kurum içindeki farklı sistemlere ve hizmetlere **erişim yetkileri** de bu sistem tarafından yönetilebilmektedir



Merkezi Kimlik Yönetim Sistemi

- **LDAP** ile kurum kullanıcı bilgisi, organizasyon hiyerarşisi ile beraber merkezi bir yerde depolanarak yönetilebilir. Bu yaygın bir pratiktir
- LDAP üzerinde **kullanıcının**, görev, ünvan, telefon, adres gibi **farklı öznitelikleri** tutulur
- LDAP türevi bir sistem kimliklendirme sürecinde yaygın içimde kullanılmasına rağmen, uygulama ve hizmetlerin **erişim yetkilerinin yönetimi** için uygun bir ortam değildir
- Bu tür veriler genellikle **ilişkisel veritabanı**nda tutularak, çalışma zamanında LDAP üzerinden elde edilen veri ile birleştirilmektedir

Yetkilendirme

Kullanıcının sistem üzerinde sadece yetkili olduğu işlemleri yürütmesi, kurumsal veriye izinler dahilinde erişebilmesi, yetkisi dışında kalan hizmetlere ve bilgiye erişiminin kısıtlanması işlemine **yetkilendirme** denir



Yetkilendirme Metotları

- Kurumsal güvenlik mimarisinde yetkilendirme kurallarının uygulanmasında **üç farklı metot** mevcuttur



Rol tabanlı
yetkilendirme

Erişim kontrol listesi
tabanlı
yetkilendirme

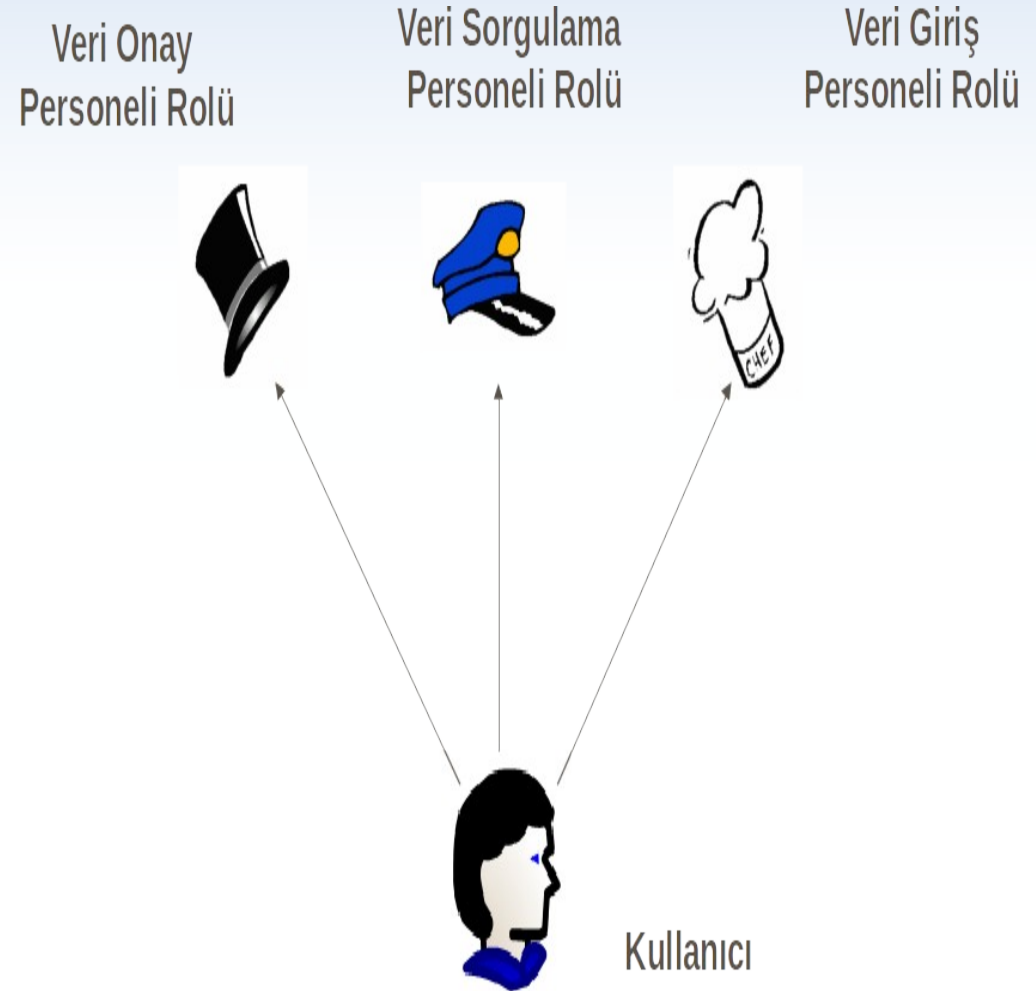
Durum tabanlı
yetkilendirme

Rol Tabanlı Yetkilendirme

- Sistem genelinde kullanıcılara veya kullanıcı gruplarına atanan bir veya birkaç **rol** vardır
- Kullanıcılar sahip oldukları bu **rollere göre** bir takım işlemleri gerçekleştirebilirler
- Bu yöntemle rol tabanlı yetkilendirme (**RBAC**) adı verilmektedir
- Rol tabanlı yetkilendirmede **kullanıcı, rol** ve kurumun **organizasyon hiyerarşisi** arasında birtakım yapılar temel teşkil etmektedir

Kullanıcı – Rol İlişkisi

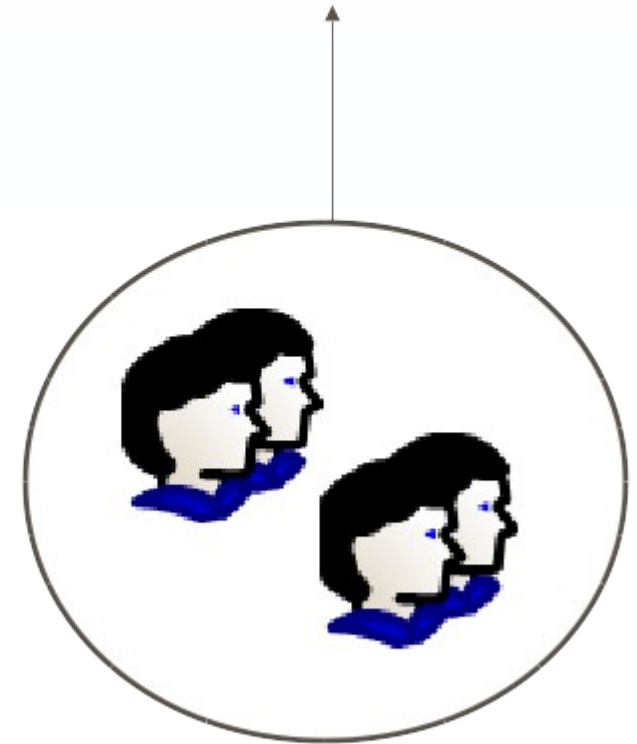
- Sistem kullanıcıları kendilerine atanmış rollerin izin verdiği ölçüde sistemi kullanabilirler
- Bir kullanıcı **birden fazla role** sahip olabilir
- Bir rol de **birden fazla kullanıcı** tarafından paylaşılabilir
- Roller arasında **hiyerarşi** oluşturmak da mümkündür



Kullanıcı, Rol ve Kullanıcı Grubu İlişkisi

- Kullanıcı grupları, **bir grup kullanıcının** bir araya getirilmesinden oluşur
- Rollerini teker teker kullanıcılara atamak yerine doğrudan bu kullanıcı gruplarına **rol ataması** yapılabilir
- Bu durumda o gruba dahil **kullanıcıların hepsi** atanan role sahip olurlar
- Kullanıcı gruptan çıkarıldığı vakit role sahip olması da sona ermiş olur
- Ayrıca kullanıcı grupları arasında da **hiyerarşi** olabilir

Veri Giriş
Personeli Rolü

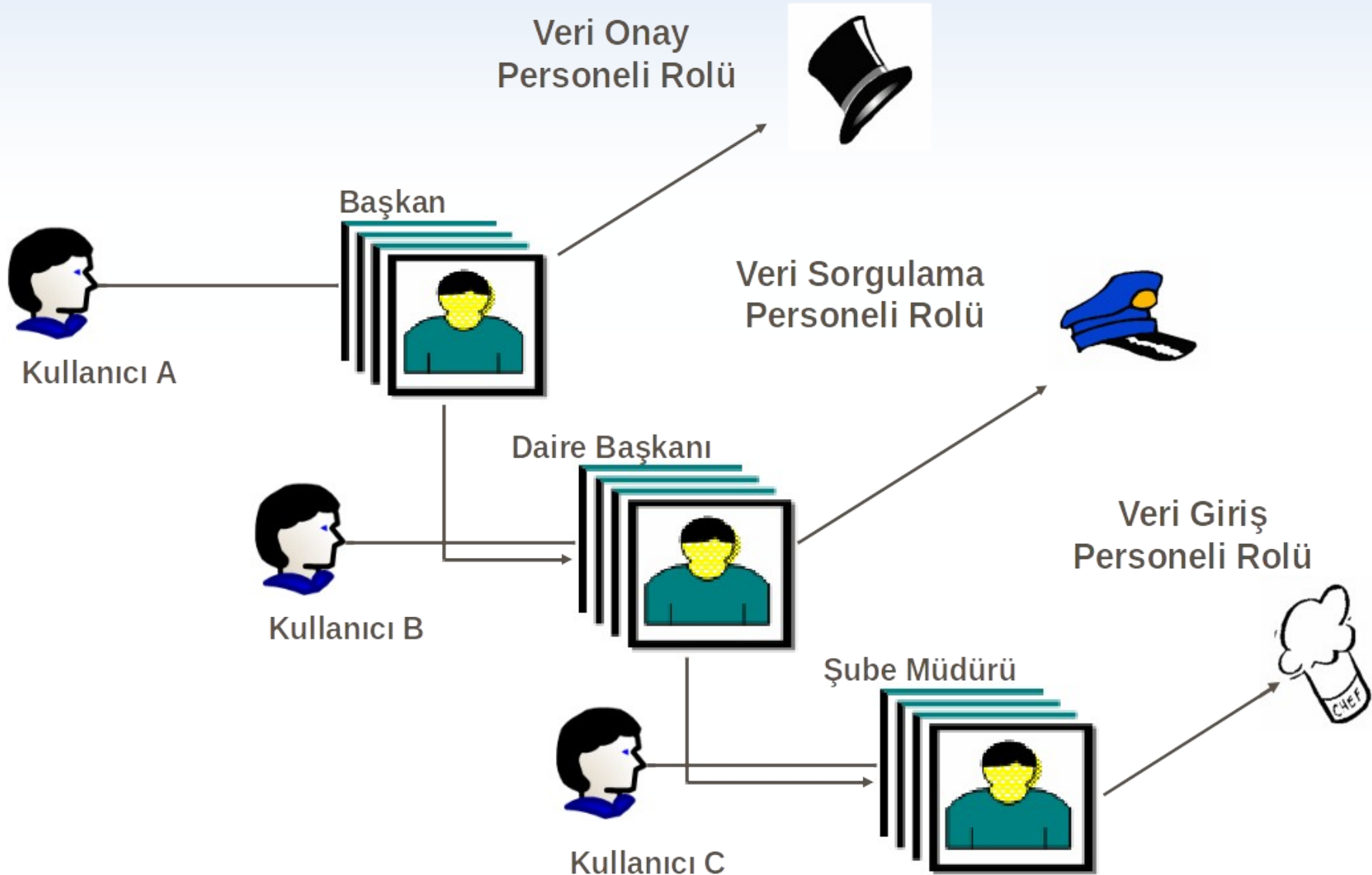


Veri Giriş Kullanıcı
Grubu

Kullanıcı, Organizasyon Hiyerarşisi, Makam ve Rol İlişkisi

- Kurumun organizasyon hiyerarşisindeki her bir **birim** bir **makam** olarak ele alınabilir
- Her makamın sahip olduğu bir takım **roller** olabilir
- Bir rol birden fazla makama da atanabilir
- Organizasyon hiyerarşisinde **üstteki bir makam** alttaki makamların sahip olduğu rollere otomatik olarak sahip olabilir
- Her makama **asaleten** veya **vekaleten** atanmış kullanıcılar olabilir
- Kullanıcı aynı anda **birden fazla makamla** ilişkili olabilir

Kullanıcı, Organizasyon Hiyerarşisi, Makam ve Rol İlişkisi



Erişim Kontrol Listesi Tabanlı Yetkilendirme

- **UNIX** işletim sisteminin yetkilendirme modeline benzer
- Bu yöntemle isteğe bağlı erişim kontrolü (**DAC**) adı da verilmektedir
- UNIX işletim sisteminde **özne** kendimiz, ait olduğumuz gruplar veya diğerleri şeklinde üçe ayrılmaktadır
- **Nesne** ise burada dosya veya uygulamadır
- Dosya veya uygulama üzerinde gerçekleştirilebilecek **işlemler** okuma, yazma, silme ve çalıştırma olarak tanımlanmıştır

Erişim Kontrol Listesi Tabanlı Yetkilendirme

- **Nesnenin sahibi** ilgili öznelerle bu yetkilerden uygun gördüklerini atamadan sorumludur
- Atanan bu yetkiler dahilinde özne de nesne üzerinde **izin verilen işlemleri** gerçekleştirebilir
- Nesne üzerinde kimin hangi izinlere sahip olduğu bilgisine de erişim kontrol listesi (**ACL**) adı verilir

Erişim Kontrol Listesi Tabanlı Yetkilendirme

- Kullanıcıların yetki atama işlemlerinde yapabilecekleri **hataları azaltmak** ve atama işlemine birtakım **sınırlar getirmek** amacı ile **zorunlu erişim kontrol yöntemi** (MAC) uygulanabilir
- Bu yöntemde erişim izinlerinin atanmasında kullanıcılar tamamen **bağımsız ve özgür değildir**
- Kendilerine verilen **izin doğrultusunda** yetkiler atayabilirler

Durum Tabanlı Yetkilendirme

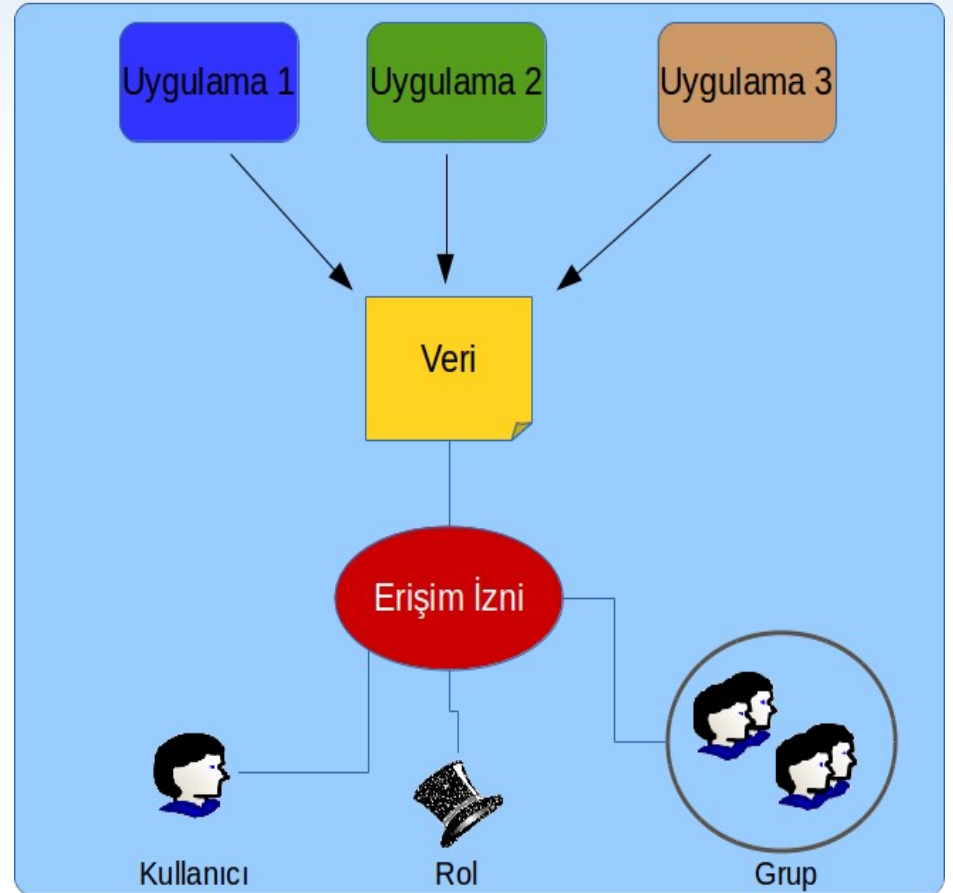
- Sistem ve kullanıcı ile ilgili bir takım **durumsal ifadeleri** kontrol ederek yapılan yetkilendirmedir
- Durumsal ifadelere örnekler
 - Kullanıcının erişim IP'si 192.168.1.0/24 aralığında ise,
 - erişim zamanı 08:00 ile 17:00 arası ise veya kullanıcı AJUG üyesi ise,
 - dokümanın günlük print etme sayısı aşılmamış ise,

Durum Tabanlı Yetkilendirme

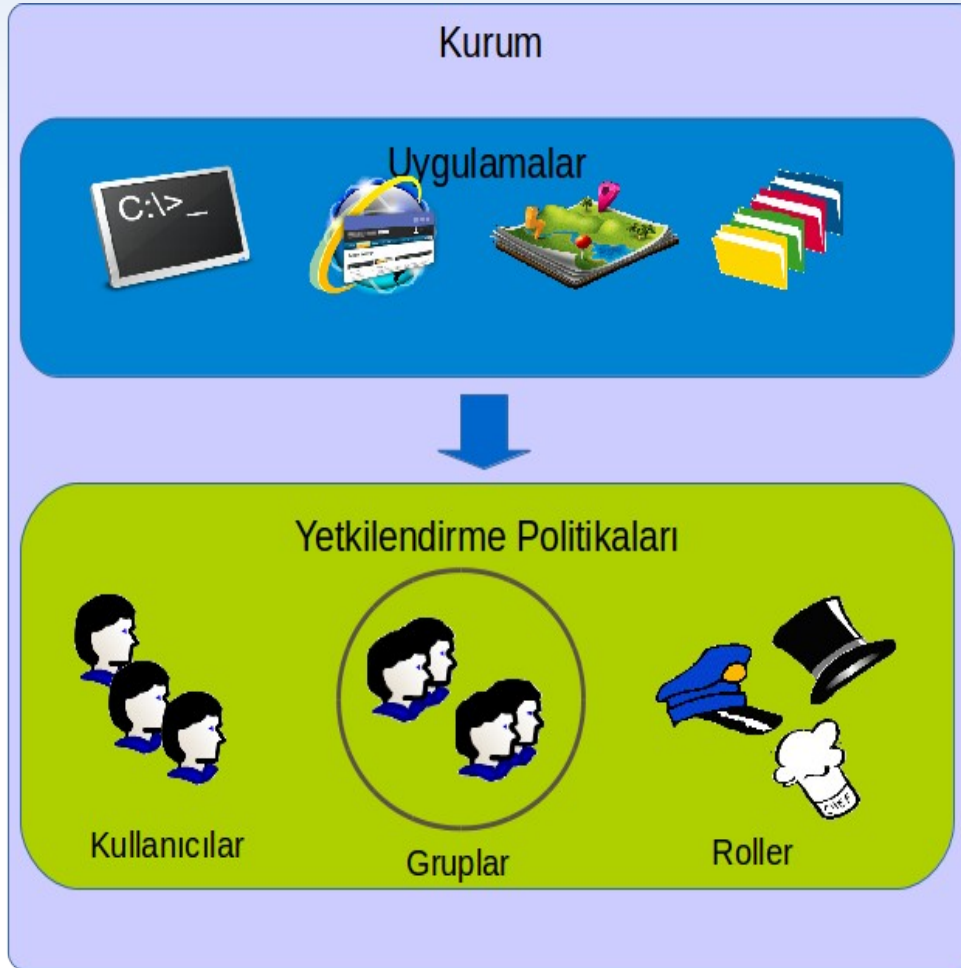
- Durumsal ifadeler **çalışma zamanında** kullanıcının erişim bilgisi, sistem zamanı gibi bilgiler ile değerlendirilerek erişim kararı verilir
- İki veya daha fazla durumsal ifade mantıksal operatörler yardımı ile bir araya getirilerek **bileşke durumsal ifadeler** de oluşturulabilir
- Durum tabanlı yetkilendirme diğer iki yetkilendirme yöntemi ile birlikte, bunları **tamamlayıcı biçimde** de kullanılabilir

Kurumsal Verinin Güvenliği

- Pek çok organizasyon için kurumsal mimari de **odak noktası** veridir
- Farklı uygulamalar **ortak veri setleri** üzerinde işlem yapabilirler
- Bu verinin gizliliği, tutarlı biçimde değiştirilmesi ve sürekli olarak erişilebilir kılınması için **uygulamalardan bağımsız**, veriyi odak noktasına alan bir güvenlik mimarisine ihtiyaç vardır



Kurumsal Verinin Güvenliği



- Veri düzeyinde hangi kullanıcıların ne türde yetkilere sahip olduğu bilgisi **tek bir noktadan** yönetilebilir
- Bu yetkilendirme politikalarının ve veri üzerindeki yetkilendirme işlemlerinin kurumun sahip olduğu **uygulamalar arasında paylaşılmasının** sağlar

Kurumsal Verinin Güvenliği

- İzin verilen işlemlerin ve bu işlemleri yapacakların yetkilendirilmesinin belirli bir **kapsama** veya **etki alanına** sahip olması istenebilir
- Bu durumda yetki tanımına ilaveten bir de **kapsama alanı** bilgisinin erişim kontrol listelerine eklenmesi gerekecektir

Nesne (OID)	Özne (SID)	İzin	Etki Alanı
Doküman:101	user1	R	app1
Doküman:555	user1	R,W	app2,app3
Doküman:101	user2	D,R,W	app1,app2,app3

Denetim ve İz Sürme Sistemi

- Kurumsal bilgi sistemlerinde kullanıcıların gerçekleştirdiği **işlemlerinin takibinin ve izinin sürülmesini** sağlar
- Kurum içerisinde meydana gelebilecek güvenlik problemlerinin **sorumlularını tespit edebilmek** için bu sistem tarafından üretilen kayıtlara ihtiyaç duyulur
- Bazı durumlarda gerçekleşen işlemlerle ilgili **detaylı bir iz kaydı** oluşturmak yeterlidir
- Diğer durumlarda ise sistem yöneticisinin **anlık olarak bilgilendirilmesi** de söz konusu olabilmektedir

Denetim ve İz Sürme Sistemi

Web Sunucusu

Uygulama Sunucusu

Veritabanı Sunucusu



Denetim ve İz Takibi Dönüşüm Katmanı

Denetim ve İz Takip Sistemi

Denetim ve İz Takip Analizi

Log
Veritabanı

İz Kayıtlarının Oluşturulmasını Tetikleyen Durumlar

- **Güvenlikli veya hassas veri** üzerinde gerçekleşen okuma, yazma veya silme işlemleri
- **Erişim kontrol verisi** ile ilgili değişiklikler
- **Sistem konfigürasyonu** üzerinde yapılan işlemler

İz Kayıtlarının İçeriği ve Yapısı

- İz kayıtları bu **sorulara cevap** üretebilmelidir:
 - Kim?
 - Nerede?
 - Ne Zaman?
 - Nasıl?
 - İşlem Türü Nedir?
 - İşlem Sonucu Nedir?
- Şifre gibi bazı **mahrem verilerin** kriptolu biçimde bile olsa iz kayıtları içerisinde yer almaması istenebilir

İz Kayıtlarının Güvenliği ve Tutarlılığı

- İz kayıtları uygulamadan **ayrı bir yerde** toplanmalıdır
- **Zaman damgalı** olmalıdır
- Başkaları tarafından kesinlikle **değiştirilememelidir**
- **Kriptolanarak** saklanmalıdır
- Sıkıştırma, arşivleme gibi işlemlere tabi tutulabilmelidir
- İz kayıtları üreten farklı sistemler ile merkezi denetim ve iz sürme sistemi arasında **zaman senkronizasyonu** da önemlidir

Denetim ve İz Kayıtlarının Analizi

- Üretilen denetim ve iz kayıtları geriye dönük olarak **farklı kriterler** ile incelenebilmelidir
- İz kayıtları üzerinde **filtreleme, sıralama, arama** yapılabilmelidir
- Kullanıcılara sistemde gerçekleşen işlemlerle ilgili kullanıcılara **istatistiki bilgi** de sunmalıdır
- İşlemlerle ilgili **averaj değerleri** veya **işlenen veri miktarını, işlem sayısını** sunan istatistik kabiliyetleri olmalıdır
- Farklı **iz kayıtları arasındaki ilişkileri** gösteren analiz kabiliyetleri de mevcut olmalıdır

Soru & Cevap

İletişim

- Harezmi Bilişim Çözümleri
- <http://www.harezmi.com.tr>
- info@harezmi.com.tr