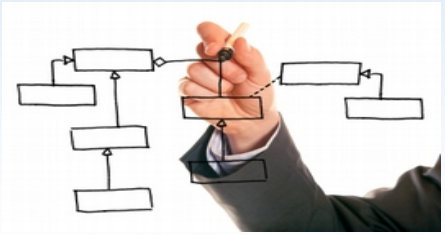
Kurumsal Bilgi Sistemleri ve Güvenlik

harezmi
it solutions

Kenan Sevindik Kimdir?

- 15 yıllık kurumsal uygulama geliştirme deneyimi var
- Bir çok kurumsal projenin hemen her fazında görev aldı
- Spring, Spring Security, Hibernate, Vaadin gibi kurumsal Java teknolojilerinde kapsamlı bilgi birikimi ve deneyime sahip



spring

Java

Spring SECURITY

Hibernate JPA

vaadin

Kenan Sevindik Kimdir?

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

harezmi bilişim çözümleri

Speedy Framework

JAVA Eğitimleri

Mimari Nedir?

Mimari, bir sistemin **yapısal organizasyonu**nu ifade eder

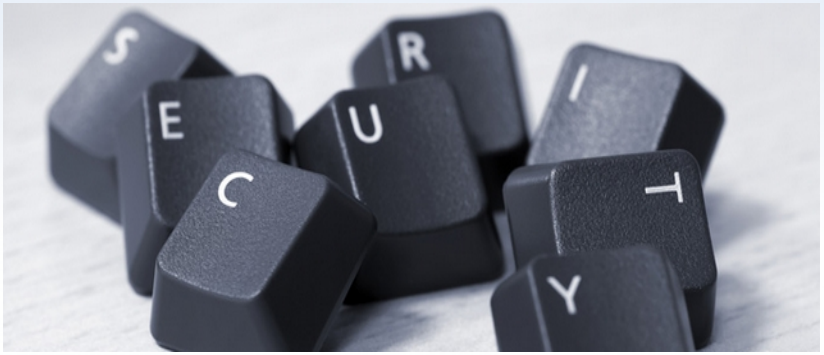
Sistemin bütüncül biçimde ortaya çıkması ve idame ettirilebilmesi için yapılması gereken faaliyetlerinin belirli **prensipler** üzerine oturtulmasını sağlar

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

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

Kurumsal Güvenlik Mimarisi

- Kurumsal bilgi sistemleri mimarisinin **temel yapı taşı**dır
- Kurumsal mimari oluşumunda güvenlik ihtiyaçlarını **ilk andan** itibaren ele almak önemlidir
- Bu sayede kurumun fonksiyonlarının **emniyetli** ve **kesintisiz** biçimde sürdürülmesi sağlanabilir



- Farklı uygulamaların ve hizmetlerin **kendine özgü veya eksik güvenlik yaklaşımları** nedeni ile bilgi sistemleri altyapısını zafiyete uğrama ihtimali azalacaktır
- Sistemde uçtan uca **tutarlı** ve **standart** bir güvenlik modeli hakim olacaktır

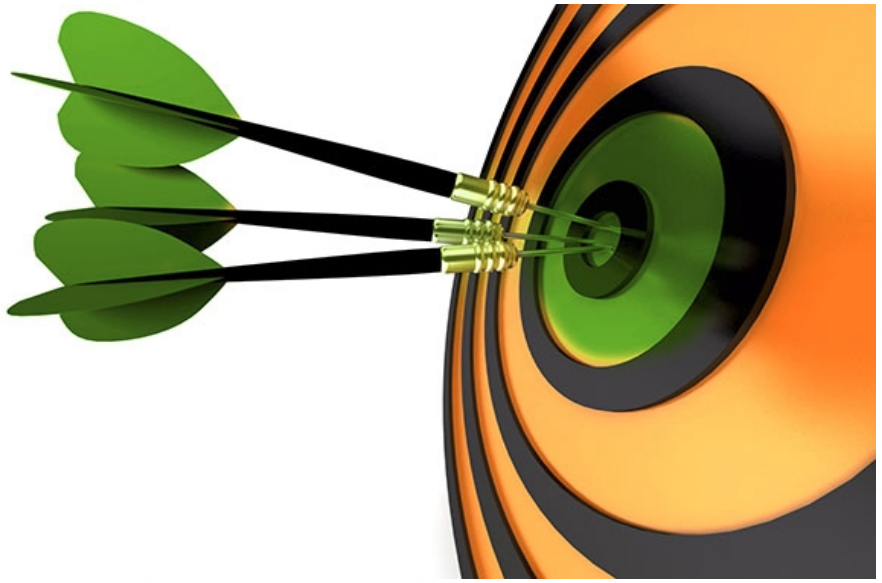
Kurumsal Güvenlik Mimarisinin Amacı Nedir?

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**

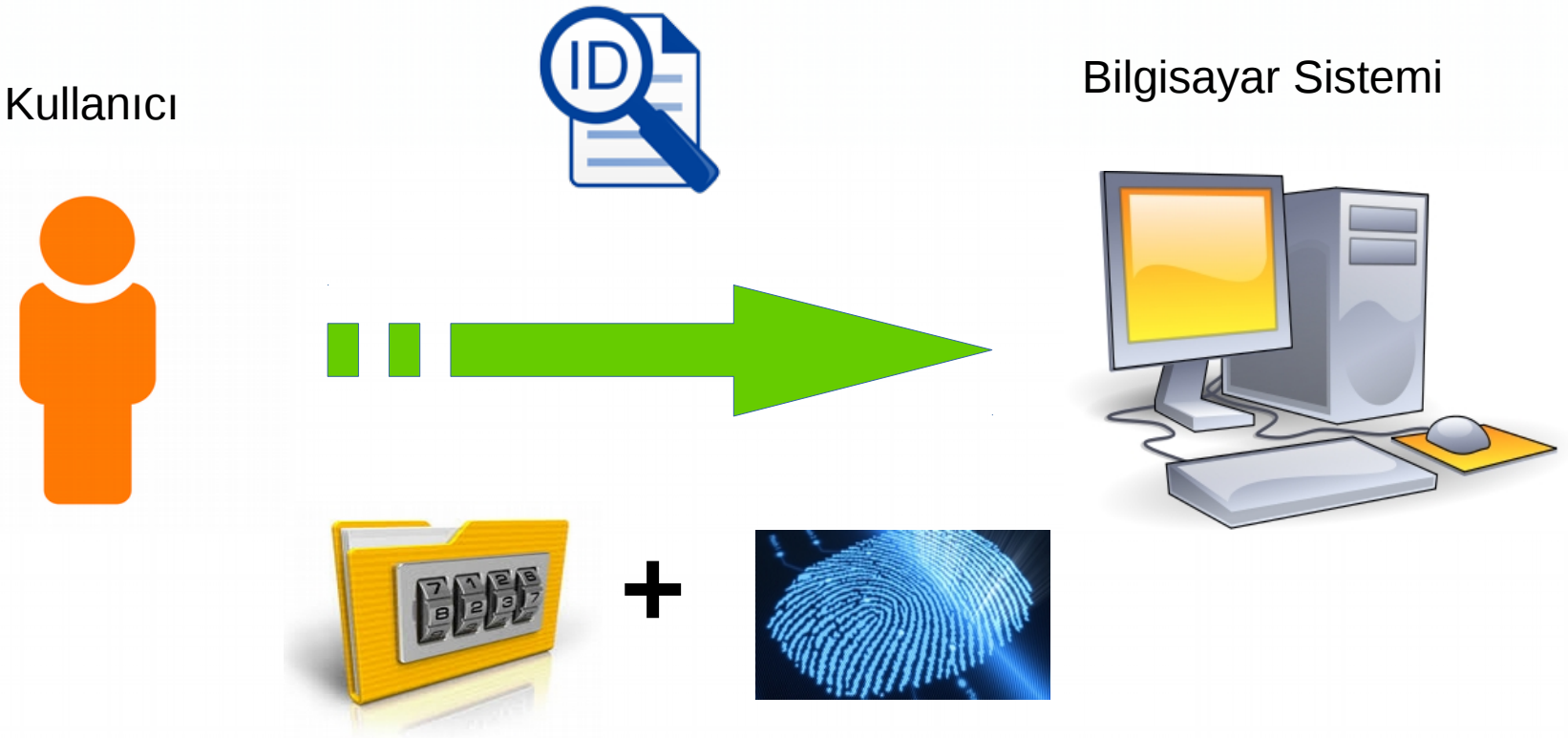
Kurumsal Güvenlik Mimarisinin Bölümleri

Kurumsal güvenlik mimarisi
üç ana bölümde incelenebilir

Kimliklendirme

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

Kullanıcı adı: Kullanıcıyı tanımlayan benzersiz niteleyici (identifier)

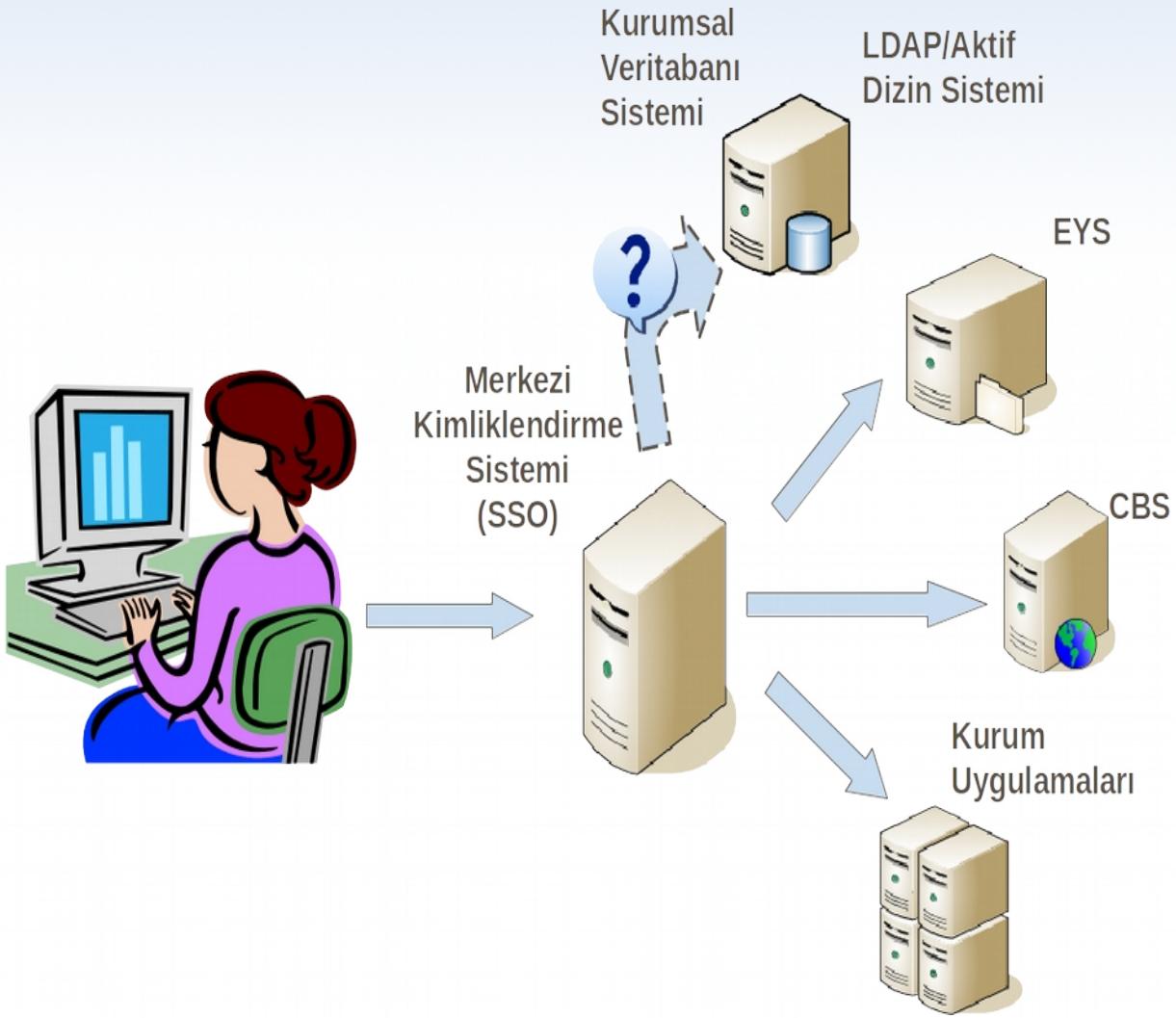


Şifre: Sadece kullanıcının bildiği veya sahip olduğu gizli bir bilgi veya özellik

Kimliklendirme Yöntemleri

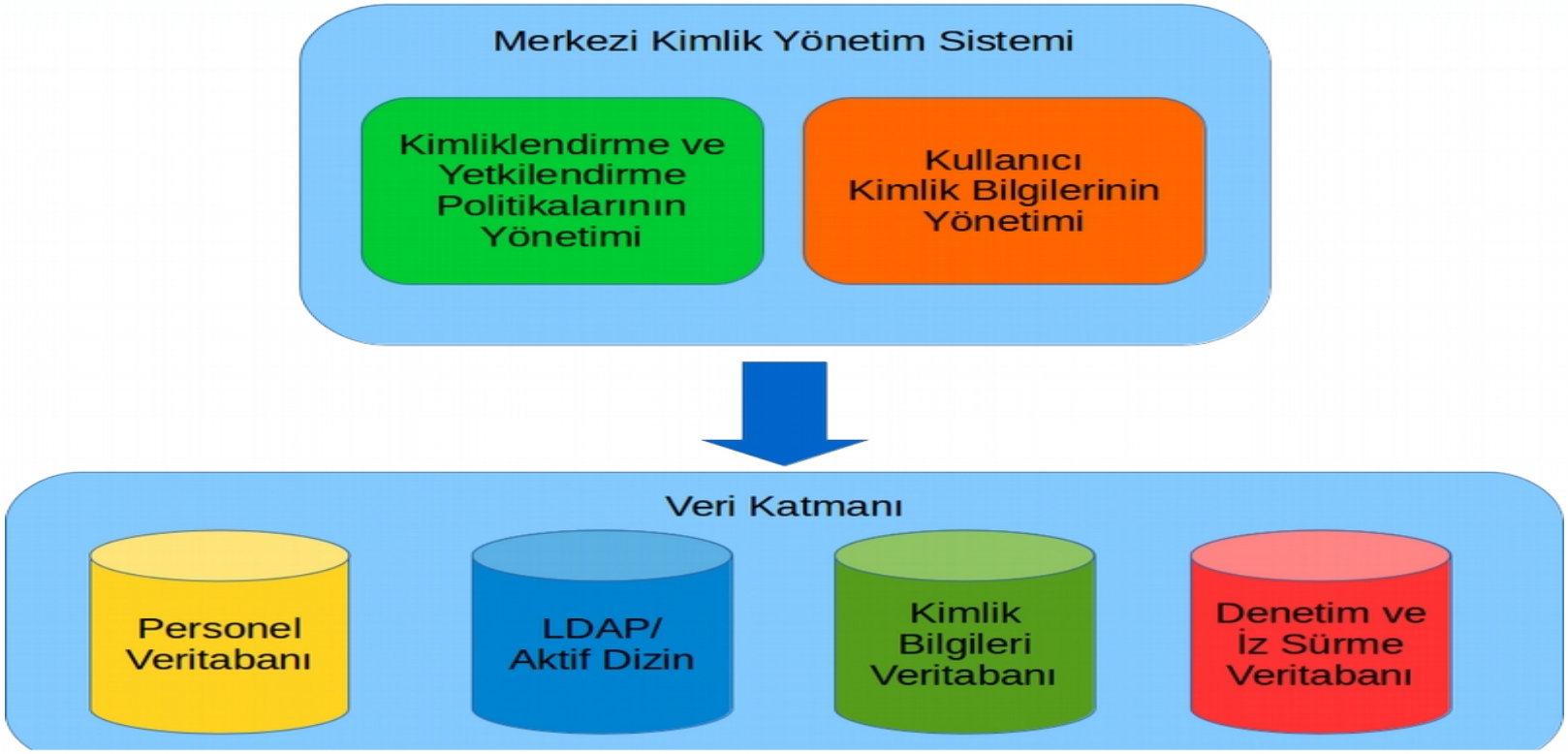
Merkezi Kimliklendirme Sistemi

- 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 yönetilmesi**ni sağlar
- Kullanıcı bilgilerinin yanında kullanıcının kurum içindeki farklı sistemlere ve hizmetlere **erişim yetkileri** de bu sistem tarafından yönetilebilmektedir



Merkezi Kimlik Yönetim Sistemi

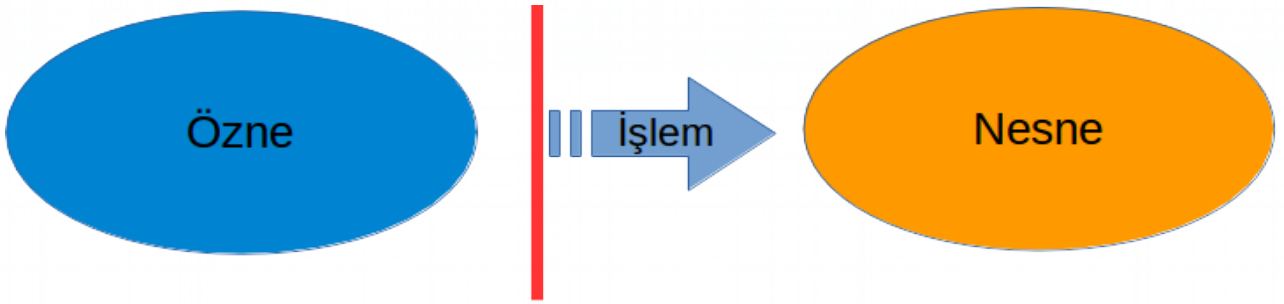
- Kurum kullanıcı bilgisi, organizasyon hiyerarşisi ile beraber **LDAP (Active Directory)** gibi merkezi bir yerde depolanarak yönetilebilir. Bu yaygın bir pratiktir
- LDAP üzerinde **kullanıcının**, görev, ünvan, telefon, adres gibi **farklı öznitelikleri** tutulur
- LDAP türevi bir sistem kimliklendirme sürecinde yaygın biçimde kullanılmasına rağmen, uygulama ve hizmetlerin **erişim yetkilerinin yönetimi** için uygun değildir
- Erişim yetkisi ile ilgili veriler genellikle **ilişkisel veritabanı**nda tutularak, çalışma zamanında LDAP üzerinden elde edilen kullanıcı ve organizasyon verisi 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

Veriye erişim, uygulamanın çalıştırılması, dosya kopyalama, çıktı alma vb

Son kullanıcı, Uygulama, Proses, Başka bir sistem



Veri, Uygulama, Süreç, Disk veya network erişimi

Yetkilendirme

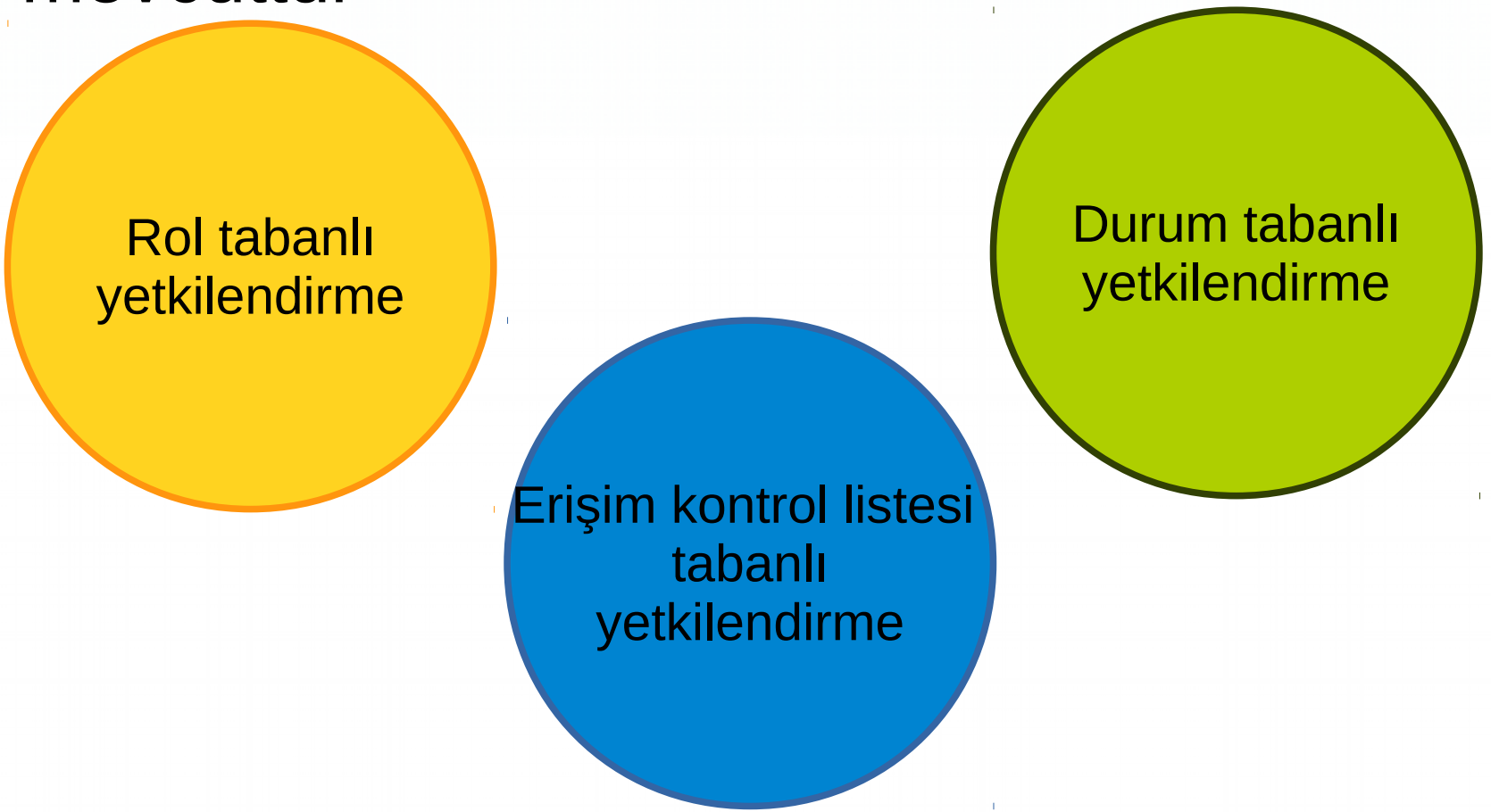
Roller ve erişim kontrol listeleri

Nesne ve öznenin içinde yer aldığı ortamla ilgili durum ve şartlar

İşlem sırasında uyulması gereken kurallar, düzenlemeler

Yetkilendirme Metotları

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

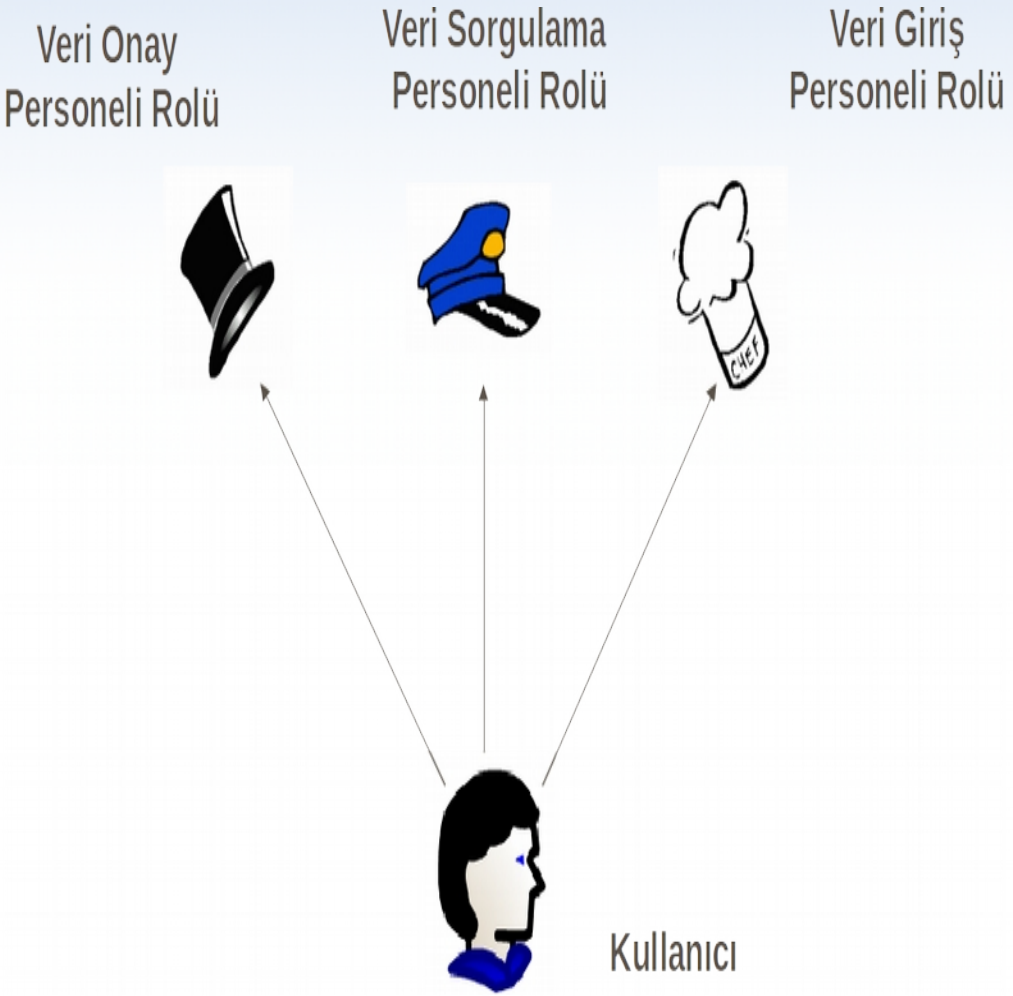


Rol Tabanlı Yetkilendirme

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

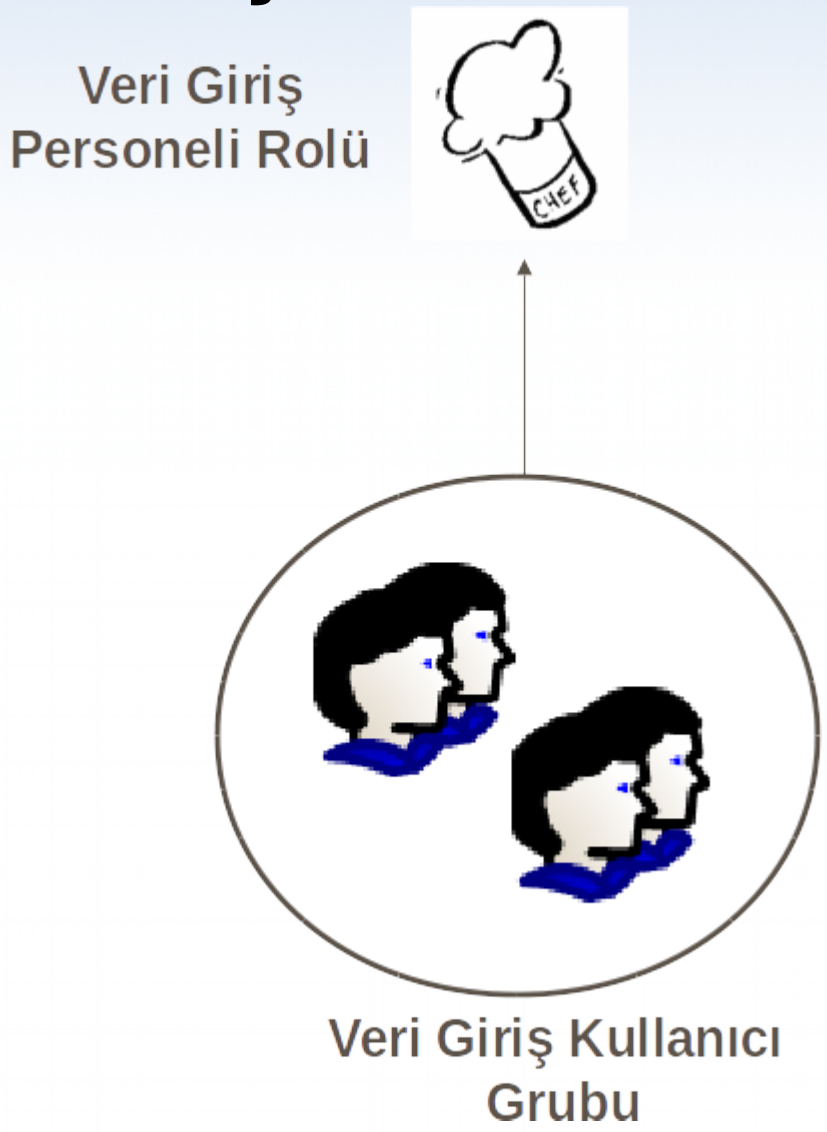
Kullanıcı – Rol İlişkisi

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



Kullanıcı, Rol ve Kullanıcı Grubu İlişkisi

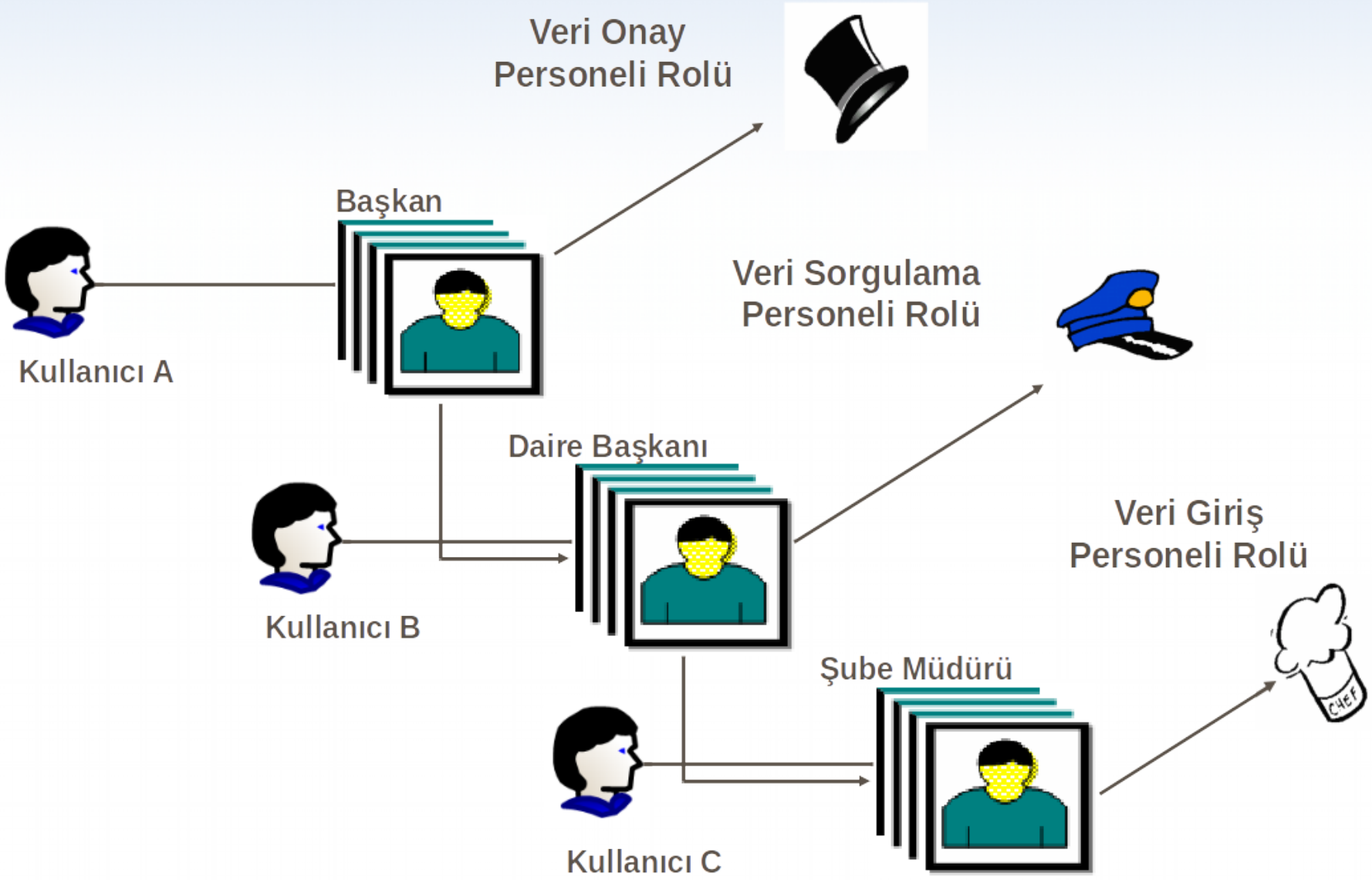
- Kullanıcı grupları, **bir grup kullanıcı**nın bir araya getirilmesinden oluşur
- Rolleri teker teker kullanıcılara atamak yerine, doğrudan kullanıcı gruplarına da atanabilir
- Bu durumda o gruba üye **kullanıcıların hepsi** atanan role sahip olurlar
- Kullanıcı gruptan çıkarıldığı vakit role sahip olması da sona ermiş olur
- Kullanıcı grupları arasında da **hiyerarşi** olabilir



Kullanıcı, Organizasyon Hiyerarşisi, Makam ve Rol İlişkisi

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

Kullanıcı, Organizasyon Hiyerarşisi, Makam ve Rol İlişkisi



Erişim Kontrol Listesi Tabanlı Yetkilendirme

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

Erişim Kontrol Listesi Tabanlı Yetkilendirme

- **Nesne sahibi**, ilgili öznelere bu yetkilerden uygun gördüklerini atar
- Atanan bu yetkiler dahilinde ilgili özne de artık hedef nesne üzerinde **izin verilen işlemler**i 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 değiller**dir
- Kendilerine verilen **izin doğrultusunda** yetkiler atayabilirler

Durum Tabanlı Yetkilendirme

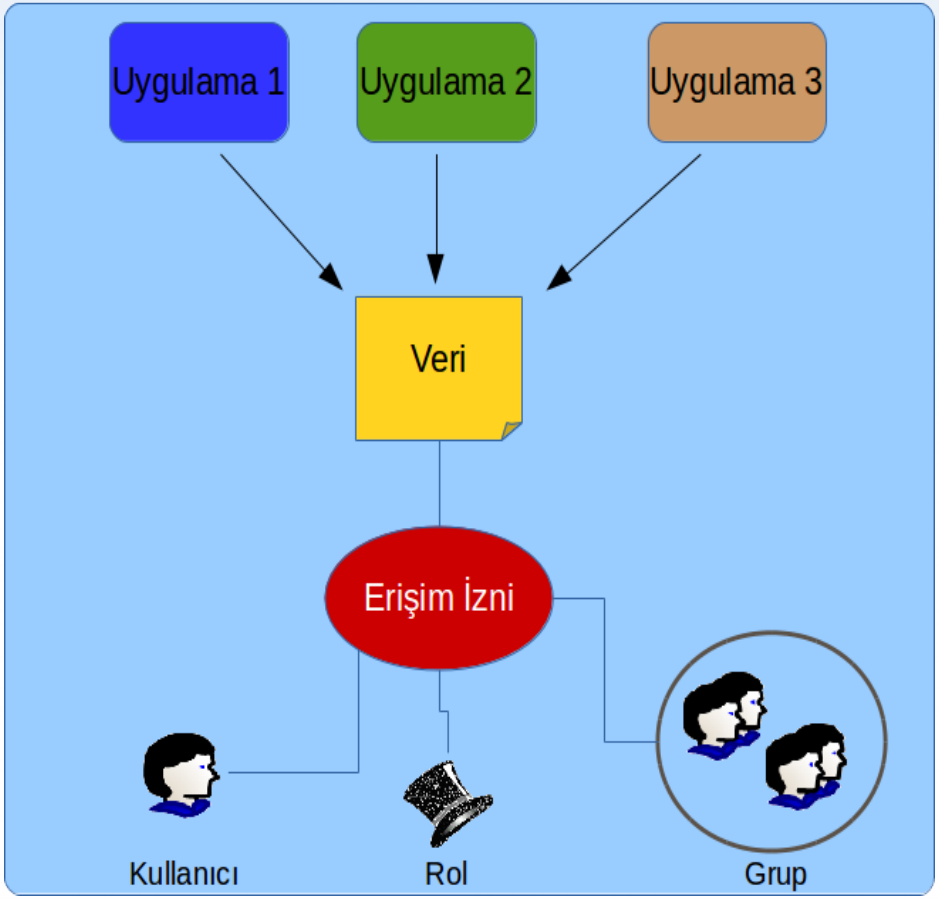
- Sistem ve kullanıcı ile ilgili bir takım **durumsal ifadeler**i kontrol ederek yapılan yetkilendirmedir
- Durumsal ifadelere örnekler
  - Kullanıcının erişim IP'si 192.168.1.0/24 aralığında ise,
  - erişim zamanı 08:00 ile 17:00 arası ise veya kullanıcı BMO üyesi ise,
  - dokümanın günlük çıktı alma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

Durum Tabanlı Yetkilendirme

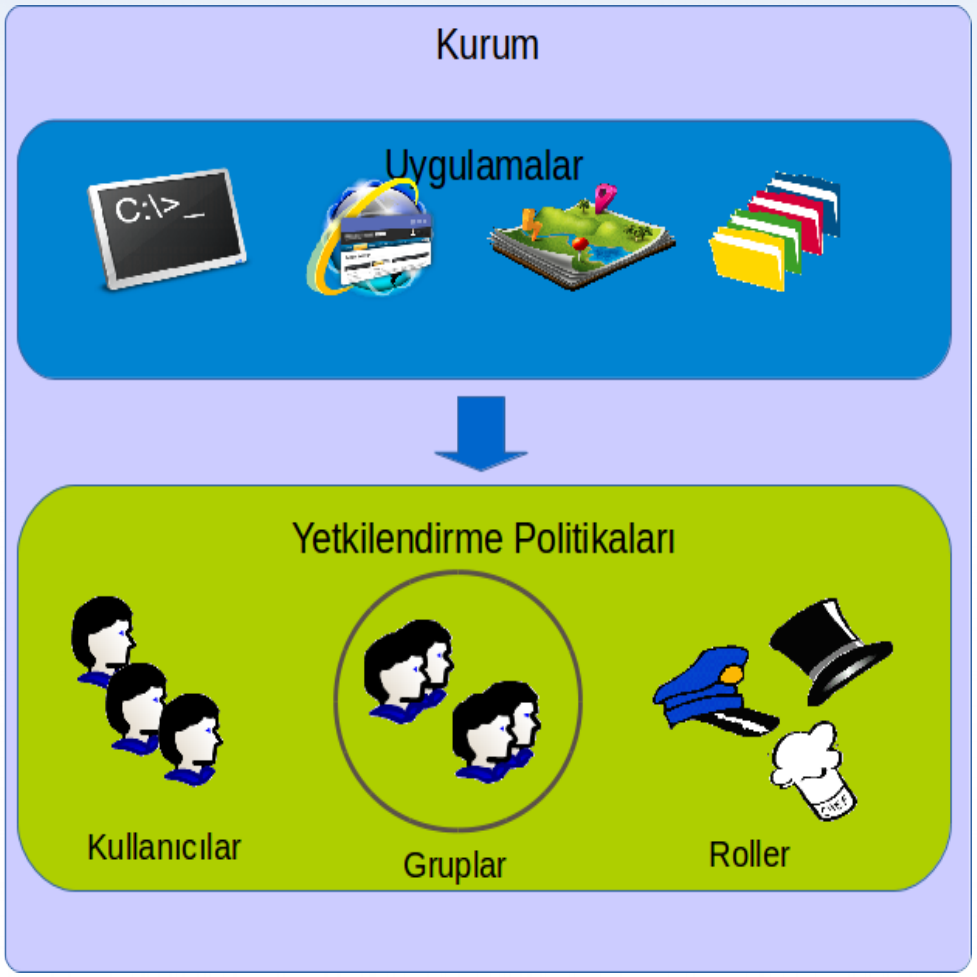
- Durumsal ifadeler **çalışma zamanında** kullanıcının erişim bilgisi, sistem zamanı gibi bilgiler ile değerlendirilerek erişim kararı verilir
- İki veya daha fazla durumsal ifade mantıksal operatörler yardımı ile bir araya getirilerek **bileşke durumsal ifadeler** de oluşturulabilir
- Durum tabanlı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

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 veriyi odak noktasına alan, **uygulamalardan bağımsız** bir güvenlik mimarisine ihtiyaç vardır



Kurumsal Verinin Güvenliği



- Veri düzeyinde hangi kullanıcının ne türde yetkilere sahip olduğu bilgisi **tek bir nokta**dan yönetilmelidir
- Bu sayede yetkilendirme politikaları ve veri üzerindeki yetkilendirme işlemleri, kolayca kurumun sahip olduğu **uygulamalar arasında paylaşılabilir**

Kurumsal Verinin Güvenliği

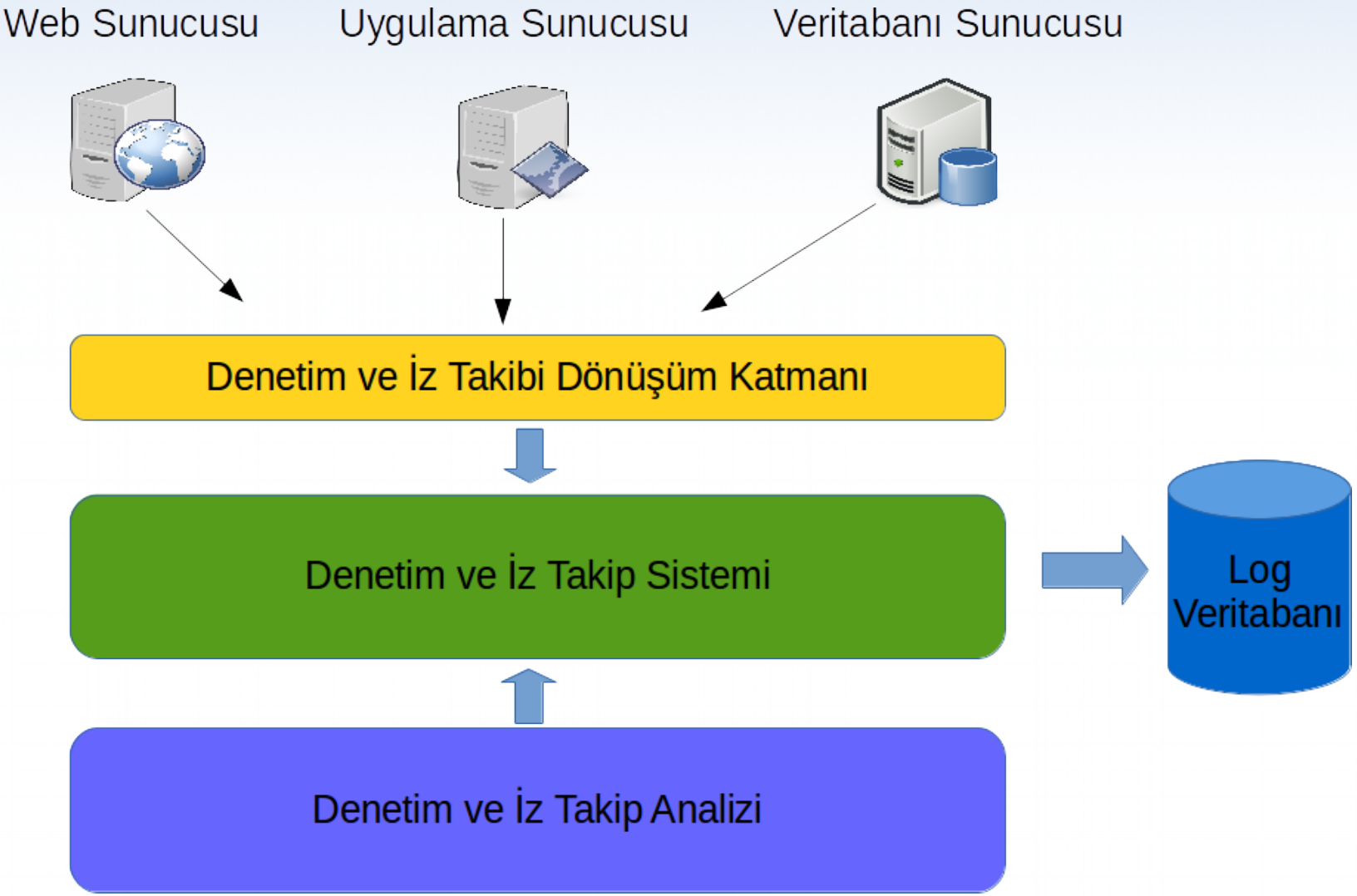
- İzin verilen işlemlerin ve bu işlemleri yapacakların yetkilendirilmesinin belirli bir **kapsam**a veya **etki alanı**na sahip olması istenebilir
- Bu durumda yetki tanımına ilaveten bir de **kapsama/etki alanı** (protection domain) bilgisinin erişim kontrol listelerine eklenmesi gerekecektir

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 takibi**nin ve **izinin sürülmesi**ni 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
- Bazı durumlarda ise sistem yöneticisinin **anlık olarak bilgilendirilme**si de gerekebilir

Denetim ve İz Sürme Sistemi



İz Kayıtlarının Oluşturulmasını Tetikleyen Durumlar

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

İz Kayıtlarının İçeriği ve Yapısı

- Herhangi bir sistemde iz kayıtları şu **sorulara cevap** üretebilmelidir:
  - Kim?
  - Nerede?
  - Ne Zaman?
  - Nasıl?
  - İşlem Türü Nedir?
  - İşlem Sonucu Nedir?
- Şifre gibi bazı **mahrem veriler**in kriptolu biçimde bile olsa iz kayıtları içerisinde yer almaması önem arz edebilir

İz Kayıtlarının Güvenliği ve Tutarlılığı

- İz kayıtları uygulamadan **ayrı bir yer**de toplanmalıdır
- **Zaman damgalı** olmalıdır
- Başkaları tarafından kesinlikle **değiştirilememeli**dir
- **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 sorgulanabilir
- İz kayıtları üzerinde **filtreleme**, **sıralama**, **arama** yapılabilmelidir
- Kullanıcılara sistemde gerçekleşen işlemlerle ilgili kullanıcılara **istatistiki bilgi** de sunmalıdır
- İşlemlerle ilgili **averaj değerler**i veya **işlenen veri miktarı**nı, **işlem sayısı**nı sunan istatistik kabiliyetleri olmalıdır
- Farklı **iz kayıtları arasındaki ilişkileri** gösteren analiz kabiliyetleri de faydalı olacaktır

Soru & Cevap

İletişim

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