MUH441 Bilişimde Güvenlik – 1

Prof. Dr. Hasan Hüseyin BALIK

(12. Hafta)

İçerik

- 3.Yazılım Güvenliği ve Güvenilir sistemler
  - 3.1.Arabellek Taşması
  - 3.2.Yazılım Güvenliği
  - 3.3.İşletim Sistemi Güvenliği
  - 3.4.Bulut Güvenliği
  - 3.5.IoT Güvenliği

3.3. İşletim Sistemi Güvenliği

3.3.İçerik

- İşletim Sistemi Güvenliğine Giriş
- Sistem Güvenliği Planlaması
- İşletim Sistemleri daha güvenli hale getirme
- Uygulama Güvenliği
- Güvenlik Bakımı
- Linux/UNIX Güvenliği
- Windows Güvenliği
- Sanallaştırma Güvenliği

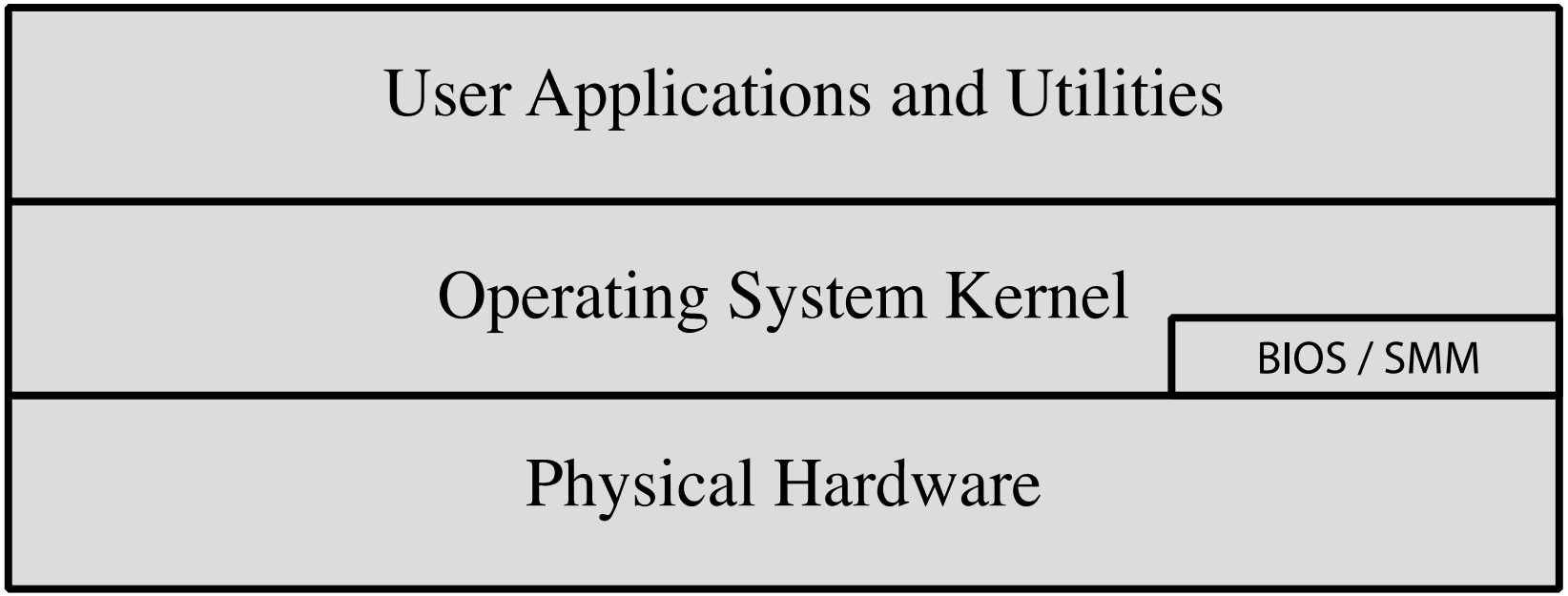


Figure 12.1 Operating System Security Layers

Stratejiler

- 2010'da Avustralya Sinyal Müdürlüğü (ASD), "En İyi 35 Azaltma Stratejisini" listelemiştir.
- 2009 yılında ASD tarafından araştırılan hedefli siber saldırıların %85'inden fazlası önlenebilirdi
- Önleme için ilk dört strateji şunlardır:
  - Beyaz liste onaylı uygulamalar kullanın
  - Üçüncü taraf uygulamalarına ve işletim sistemi güvenlik açıklarına yama yapın
  - Yönetici ayrıcalıklarını kısıtlayın
  - Kapsamlı bir savunma sistemi oluşturun
- Bu stratejiler, DHS, NSA, Enerji Bakanlığı, SANS ve Amerika Birleşik Devletleri'ndeki diğerler kurumlar tarafından geliştirilen "20 Kritik Kontrol"dekilerle büyük ölçüde uyumludur.

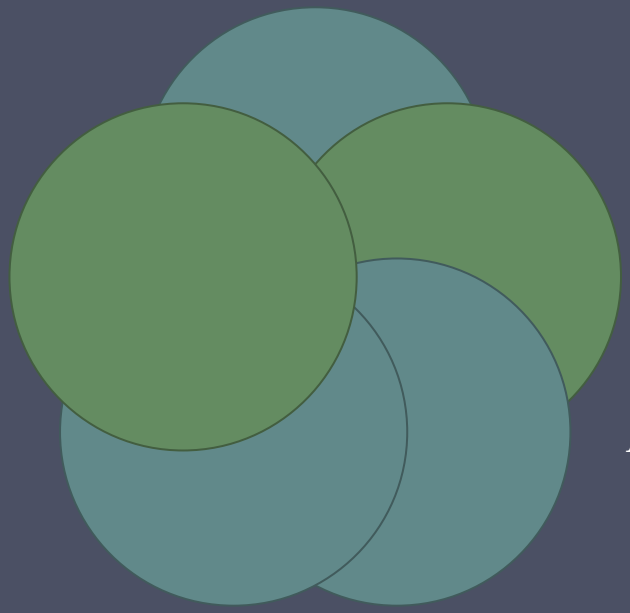
İşletim Sistemi Güvenliği

- Bir sistem, en son yamaları yüklemeden önce kurulum işlemi sırasında tehlikeye girebilir
- Bir sistem kurmak ve hizmete almak, bu tehdide karşı koymak için tasarlanmış planlı bir süreç olmalıdır.
- Süreç:
  - Riskleri değerlendirin ve sistem dağıtımını planlayın
  - Altta yatan işletim sistemini ve ardından önemli uygulamaları koruyun
  - Herhangi bir kritik içeriğin güvenli olduğundan emin olun
  - Uygun ağ koruma mekanizmalarının kullanıldığından emin olun
  - Güvenliği sürdürmek için uygun süreçlerin kullanıldığından emin olun

Sistem Güvenliği Planlaması

Yeni bir sistemi devreye almanın ilk adımı planlamadır

Planın, sistemi kurmak ve yönetmek için uygun personeli ve eğitimi belirlemesi gerekiyor



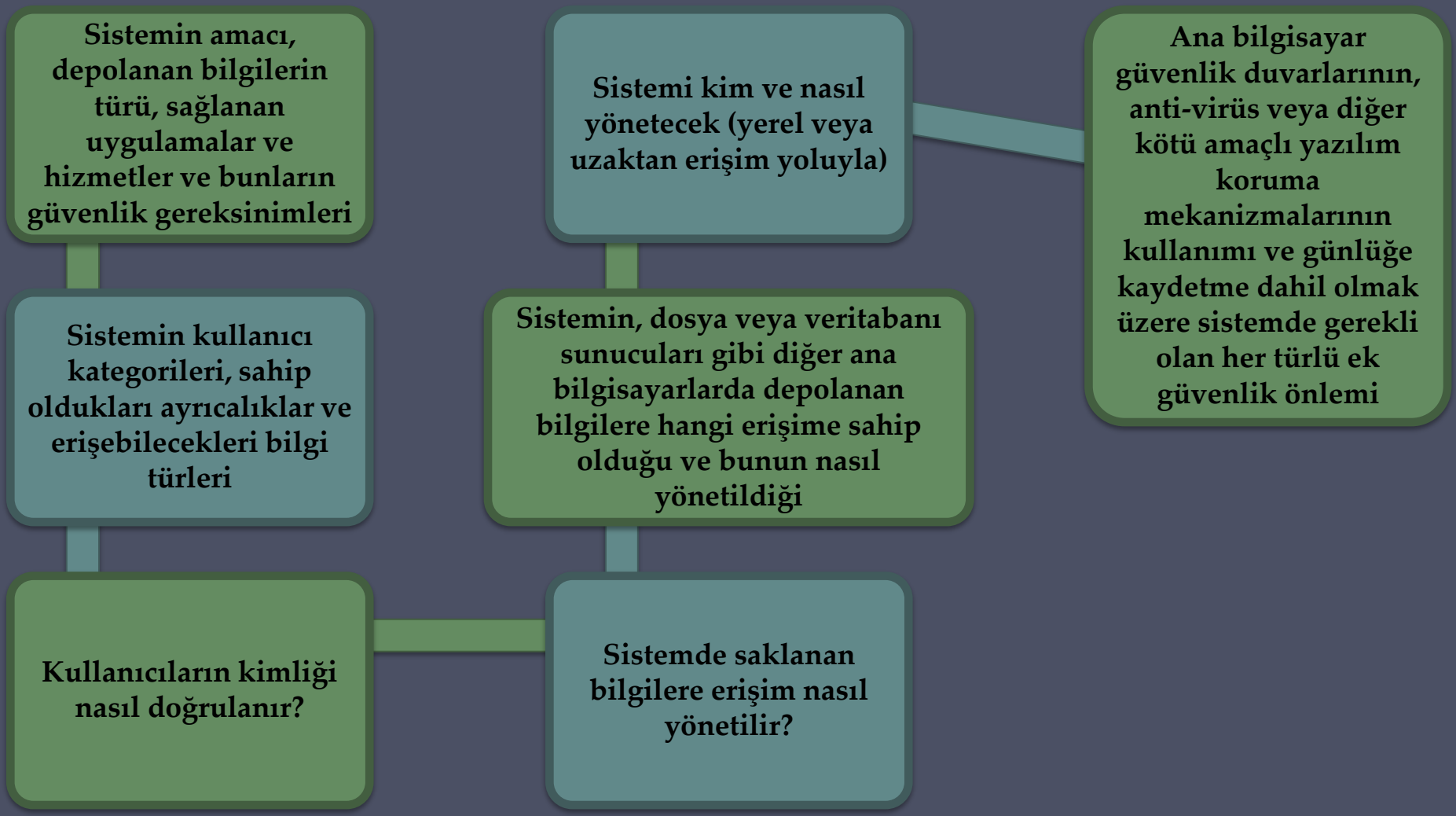
Planlama, kuruluşun geniş bir güvenlik değerlendirmesini içermelidir

Planlama sürecinin sistem, uygulamalar, veriler ve kullanıcılar için güvenlik gereksinimlerini belirlemesi gerekir

Amaç, maliyetleri en aza indirirken güvenliği en üst düzeye çıkarmaktır

Sistem Güvenliği Planlama Süreci

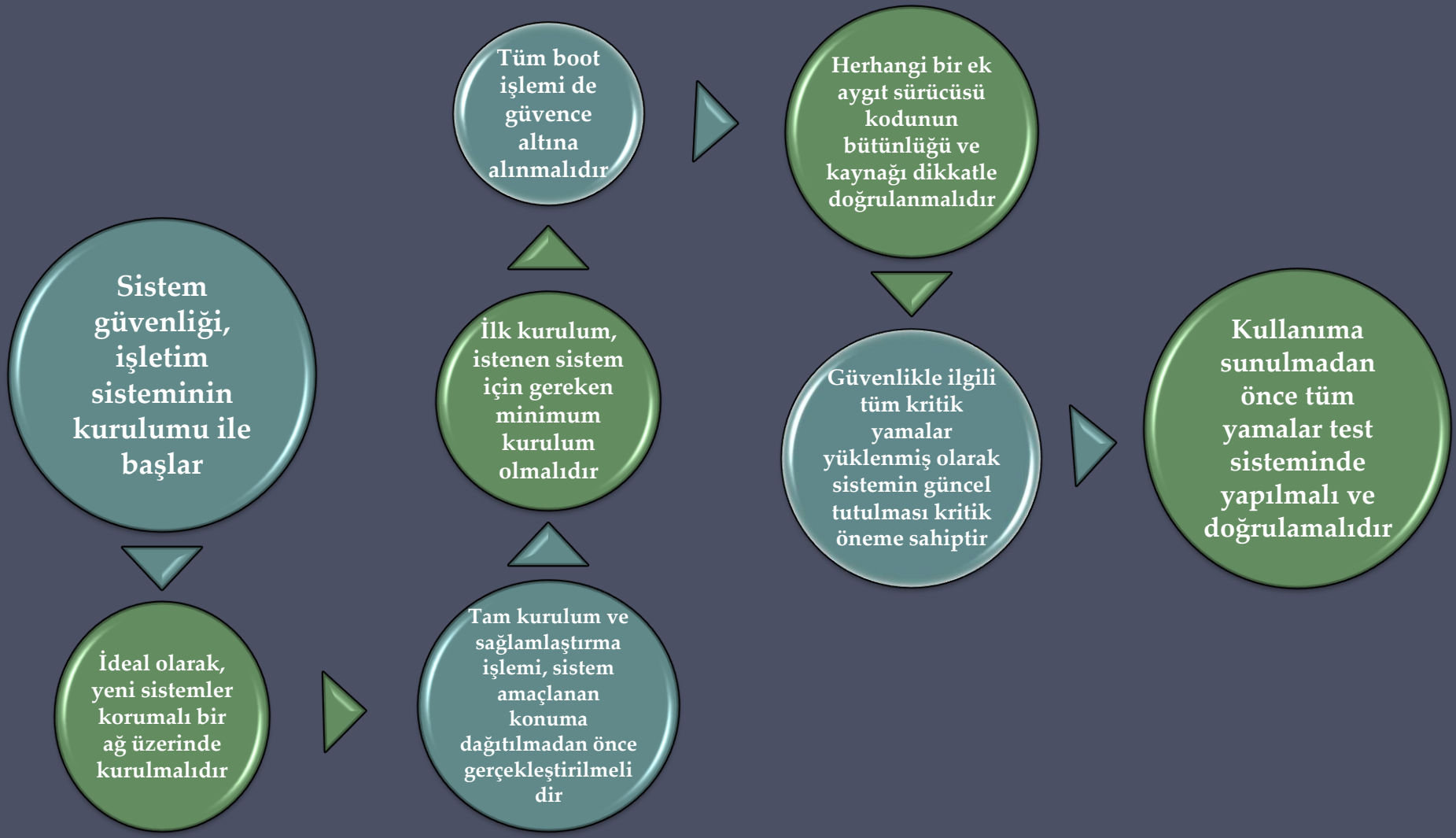
NIST SP 800-123, sistem güvenlik planlama sürecinde dikkate alınması gereken öğelerin bir listesini sağlar



İşletim Sistemlerini Güçlendirme

- Bir sistemin güvenliğinin sağlanmasındaki ilk kritik adım, temel işletim sisteminin güvenliğini sağlamaktır.
- Temel adımlar
  - İşletim sistemini kurun ve yamalayın
  - İşletim sistemini, sistemin belirlenmiş güvenlik gereksinimlerini yeterince karşılayacak şekilde aşağıdakileri gerçekleştirerek sağlamlaştırın ve yapılandırın:
    - Gereksiz hizmetleri, uygulamaları ve protokolleri kaldırma
    - Kullanıcıları, grupları ve izinleri yapılandırma
    - Kaynak denetimlerini yapılandırma
  - Virüsten koruma, ana bilgisayar tabanlı güvenlik duvarları ve izinsiz giriş tespit sistemi (IDS) gibi ek güvenlik denetimlerini kurun ve yapılandırın
  - Atılan adımların güvenlik ihtiyaçlarını yeterince karşıladığından emin olmak için temel işletim sisteminin güvenliğini test edin.

İlk Kurulum ve Yama Yapma



Gereksiz Hizmetleri, Uygulamaları, Protokolleri Kaldırma

- Çalıştırmak için daha az yazılım paketi varsa, risk azalır
- Sistem planlama süreci, belirli bir sistem için gerçekte neyin gerekli olduğunu belirlemelidir.

- İlk kurulumu gerçekleştirirken, var olan varsayılanlar kullanılmamalıdır.
  - Varsayılan yapılandırma, güvenlik yerine kullanım kolaylığını ve işlevselliği en üst düzeye çıkaracak şekilde ayarlanmıştır.
  - Daha sonra ek paketlere ihtiyaç duyulursa, gerektiğinde kurulabilirler.

Kullanıcıları, Grupları ve Kimlik Doğrulamayı Yapılandırma

- Bir sisteme erişimi olan tüm kullanıcılar, o sistemdeki tüm verilere ve kaynaklara aynı erişime sahip olmamalıdır
- Yükseltilmiş ayrıcalıklar, yalnızca onlara ihtiyaç duyan kullanıcılarla sınırlandırılmalı ve bu kullanıcılar bu yetkileri sadece görevi gerçekleştirmek için ihtiyaç duyulduğunda kullanmalıdır.

- Sistem planlama süreci şunları dikkate almalıdır:
  - Sistemdeki kullanıcı kategorileri
  - Sahip oldukları ayrıcalıklar
  - Erişebilecekleri bilgi türleri
  - Nasıl ve nerede tanımlanır ve doğrulanır?
- Sistem kurulumunun bir parçası olarak dahil edilen varsayılan hesapların güvenliği sağlanmalıdır.
  - Gerekli olmayanlar kaldırılmalı veya devre dışı bırakılmalıdır.
  - kimlik doğrulamada kullanılan politikalar yapılandırılmalıdır

Kaynak Denetimlerini Yapılandırma

- Kullanıcılar ve gruplar tanımlandıktan sonra, veriler ve kaynaklar üzerinde uygun izinler ayarlanabilir.
- Güvenlik güçlendirme kılavuzlarının çoğu, varsayılan erişim yapılandırmasında önerilen değişikliklerin listesini sunar.

Ek Güvenlik Denetimlerinin Kurulumu

- Ek güvenlik araçlarını kurarak ve yapılandırarak daha fazla güvenlik mümkündür:
  - Antivirüs yazılımı
  - Ana bilgisayar tabanlı güvenlik duvarları
  - IDS veya IPS yazılımı
  - Uygulama beyaz listesi

Sistem Güvenliğini Test Etme

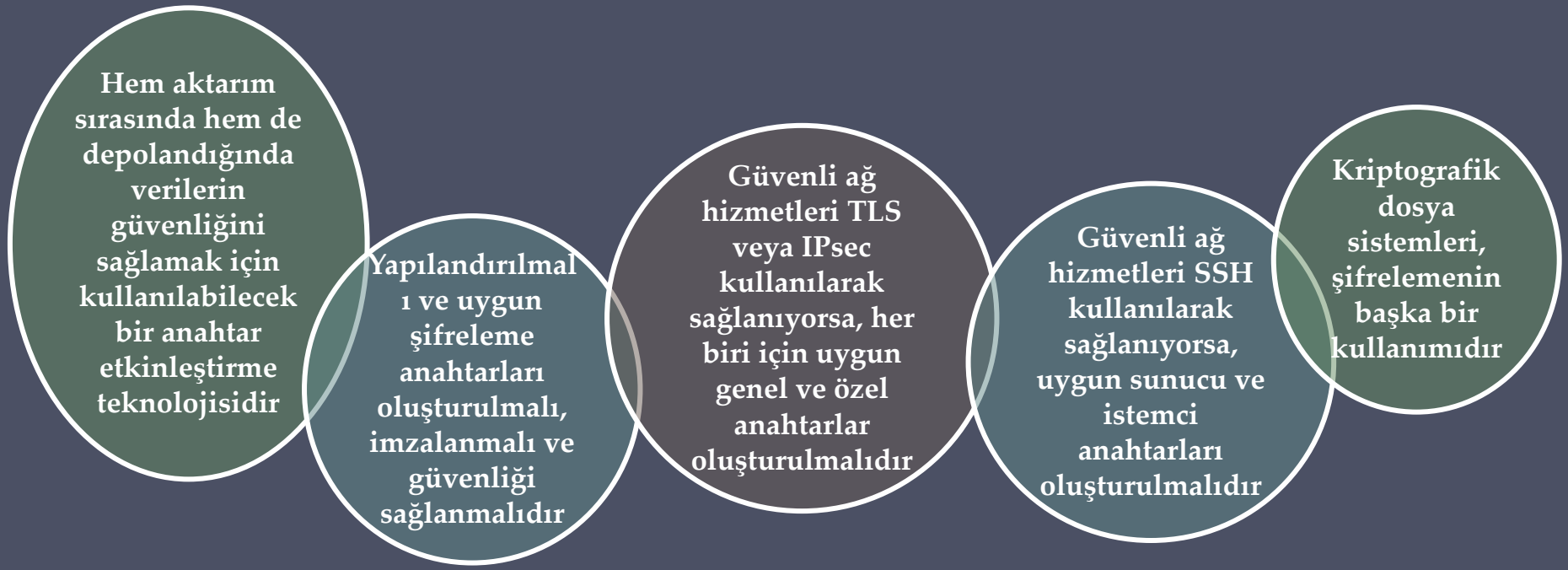
- Başlangıçta temel işletim sisteminin güvenliğini sağlama sürecindeki son adım, güvenlik testidir.
- Hedef:
  - Önceki güvenlik yapılandırma adımlarının doğru şekilde uygulandığından emin olun
  - Olası güvenlik açıklarını tanımlayın
- Kontrol listeleri, güvenlik güçlendirme kılavuzlarına dahildir
- Aşağıdakiler için özel olarak tasarlanmış programlar vardır:
  - Bir sistemin temel güvenlik gereksinimlerini karşıladığından emin olmak için bir sistemi gözden geçiren
  - Bilinen güvenlik açıklarını ve zayıf yapılandırma uygulamalarını tarayan
- Sistemin ilk güvenlik güçlendirmesinden sonra yapılmalıdır.
- Güvenlik bakım sürecinin bir parçası olarak periyodik olarak tekrarlanır

Uygulama Yapılandırması

- …… içerir:
  - Uygulamaya uygun veri saklama alanlarının oluşturulması ve belirlenmesi
  - Uygulama veya hizmet varsayılan yapılandırma ayrıntılarında uygun değişiklikleri yapma
- Bazı uygulamalar veya hizmetler şunları içerebilir:
  - varsayılan veri
  - Kodlar
  - Kullanıcı hesapları

  Bunlar gözden geçirilmeli ve yalnızca gerektiğinde ve uygun şekilde saklanmalıdır.
- Web ve dosya aktarım hizmetleri gibi uzaktan erişilen hizmetlerle özellikle ilgili
  - Bu tür saldırılardan kaynaklanan risk, dosyaların çoğunun sunucu tarafından yalnızca okunabilmesi, yazılmaması sağlanarak azaltılır.

Şifreleme Teknolojisi



Güvenliğin Korunması

- Güvenliği sağlama süreci süreklidir
- Güvenliğın korunması şunları içerir:
  - Log kayıtlarını izleme ve analiz etmek
  - Düzenli yedeklemeler gerçekleştirmek
  - Güvenlik ihlallerinden kurtarmak
  - Sistem güvenliğini düzenli olarak test etmek
  - Tüm kritik yazılımları yamalamak, güncellemek ve yapılandırmayı gerektiği gibi yapmak ve revize etmek için uygun yazılım bakım süreçlerini kullanmak

Loglama

Sadece daha önce olmuş kötü şeyler hakkında bilgi verebilir

Bir sistem ihlali veya çökmesi durumunda, sistem yöneticileri ne olduğunu daha hızlı belirleyebilir

Anahtar, doğru verileri yakaladığınızdan ve ardından bu verileri uygun şekilde izleyip analiz ettiğinizden emin olmaktır

Bilgi sistemi, ağ ve uygulamaları tarafından üretilebilir

Elde edilen veri aralığı, sistem planlama aşamasında belirlenmelidir

Önemli miktarda bilgi üretir ve bunlar için yeterli alan ayrılması önemlidir

Otomatik analiz tercih edilir

Veri Yedekleme ve Arşivleme

Verilerin düzenli olarak yedeklenmesi, sistemin ve kullanıcı verilerinin bütünlüğünü korumaya yardımcı olan kritik bir kontroldür

- Verilerin saklanması için yasal veya operasyonel gereklilikler olabilir

Yedekleme

- Verilerin düzenli aralıklarla kopyalanması sürecidir

Arşivleme

- Geçmiş verilere erişmek için yasal ve operasyonel gereklilikleri karşılamak amacıyla verilerin kopyalarını uzun süreler boyunca saklama sürecidir

Yedekleme ve arşivleme ile ilgili ihtiyaçlar ve politika, sistem planlama aşamasında belirlenmelidir

- Çevrimiçi veya çevrimdışı tutulur
- Yerel olarak depolanır veya uzak bir siteye taşınır
  - Farklı tehditlere karşı daha fazla güvenlik ve sağlamlığa karşı uygulama kolaylığı ve maliyeti içerir

Linux/Unix Güvenliği

- Yama yönetimi
  - Güvenlik yamalarını güncel tutmak, yaygın olarak tanınan ve kritik bir güvenliği sağlamak için kontrol ekanizmasıdır
  - Modern Unix ve Linux dağıtımları genellikle otomatik olarak indirme ve yüklemeiçin gerekli mekanizmaları sunar
    - Red Hat, Fedora ve CentOS: up2date veya yum
    - SuSE: yast
    - Debian : apt-get

    kullanır
- Uygulama ve servis yapılandırması
  - En yaygın olarak her uygulama ve hizmet için ayrı metin dosyaları kullanılarak uygulanır
  - Genellikle /etc dizininde veya belirli bir uygulama için kurulum ağacında bulunur
  - Sistem varsayılanlarını geçersiz kılabilen bireysel kullanıcı yapılandırmaları, her kullanıcının ana dizinindeki gizli “nokta” dosyalarında bulunur
  - Sistem güvenliğini artırmak için gereken en önemli değişiklikler, gerekli olmayan hizmetleri ve uygulamaları devre dışı bırakmaktır

Linux/Unix Güvenliği

- Kullanıcılar, gruplar ve izinler
  - Erişim, her kaynak için sahibin, grubun ve diğerlerinin her birine okuma, yazma ve yürütme izinleri vermek olarak belirtilir.
  - Kılavuzlar, kritik dizinler ve dosyalar için erişim izinlerinin değiştirilmesini önerir.
  - Yerel istismar
    - Yükseltilmiş ayrıcalıklar elde etmek için bir saldırgan tarafından istismar edilebilecek yazılım güvenlik açığı
  - Uzaktan istismar
    - Bir ağ sunucusunda, uzaktaki bir saldırgan tarafından tetiklenebilecek yazılım güvenlik açığı

Linux/Unix Güvenliği

Uzaktan erişim kontrolleri

- Birkaç ana bilgisayar güvenlik duvarı programı kullanılabilir
- Çoğu sistem, hangi hizmetlerin sisteme erişmesine izin verileceğini seçmek için bir yönetim yardımcı programı sunar

Loglama ve log rotasyonu

- Varsayılan ayarın mutlaka uygun olduğu varsayılmamalıdır

Linux/Unix Güvenliği

- Ağdan erişilebilen bazı hizmetler, tam dosya sistemine erişim gerektirmez, bunun yerine işlemleri için yalnızca sınırlı bir dizi veri dosyasına ve dizine ihtiyaç duyar (ör. FTP)
- Unix ve Linux sistemleri, bu tür hizmetleri tek bir ağda çalıştırmak için bir mekanizma sağlar. chroot jail
- chroot jail
  - Sunucunun dosya sistemi görüşünü yalnızca belirli bir bölümle sınırlar
  - Dosya sisteminin kökünü başka bir dizine eşleyerek bir işlemi sınırlamak için chroot sistem çağrısını kullanır.
  - Chroot jail dışındaki dosya dizinleri görünmez veya erişilebilir değildir
  - Ana dezavantaj ek karmaşıklıktır

Windows Güvenliği

Yama yönetimi

- "Windows Update" ve "Windows Server Update Service" düzenli bakıma yardımcı olur ve kullanılmalıdır
- Üçüncü taraf uygulamaları da otomatik güncelleme desteği sağlar

Kullanıcı yönetimi ve erişim denetimleri

- Sistemler isteğe bağlı erişim kontrol kaynakları uygular
- Vista ve sonraki sistemler zorunlu bütünlük denetimleri içerir
- Nesneler düşük, orta, yüksek veya sistem bütünlük düzeyi olarak etiketlenir
- Sistem, öznenin bütünlüğünün nesnenin seviyesine eşit veya bundan daha yüksek olmasını sağlar
- Biba Bütünlük modelinin bir biçimini kullanılır

Windows Güvenliği Kullanıcı Yönetimi ve Erişim Kontrolleri

Windows sistemleri ayrıcalıkları da tanımlar

- Sistem genelinde ve kullanıcı hesaplarına verilir

Paylaşılan bir kaynaktaki dosyalara erişirken ek güvenlik ve ayrıntı düzeyi sağlamak için paylaşım ve NTFS izinlerinin birleşimi kullanılabilir

Kullanıcı Hesabı Denetimi (UAC)

- Vista ve sonraki sistemlerde vardır
- Yönetici haklarına sahip kullanıcıların bunları yalnızca gerektiğinde kullanmasına yardımcı olur, aksi takdirde sisteme normal bir kullanıcı olarak erişir

Düşük Ayrıcalıklı Servis Hesapları

- Dosya yazdırma ve DNS hizmetleri gibi uzun ömürlü hizmet süreçleri için kullanılır

Windows Güvenliği

Uygulama ve servis yapılandırması

- Yapılandırma bilgilerinin çoğu Kayıt Defterinde (Registry) merkezileştirilmiştir
  - Uygulamalar tarafından sorgulanabilecek ve yorumlanabilecek bir anahtar ve değer veritabanı oluşturur
- Registery anahtarları, «Registery Editor" kullanılarak doğrudan değiştirilebilir
  - Toplu değişiklikler yapmak için daha kullanışlıdır

Windows Güvenliği

Diğer güvenlik kontrolleri

- Virüsten koruma, casus yazılımdan koruma, kişisel güvenlik duvarı ve diğer kötü amaçlı yazılım ve saldırı algılama ve işleme yazılım paketlerinin yüklenmesi ve yapılandırılması önemlidir
- Mevcut nesil Windows sistemleri, temel güvenlik duvarı ve kötü amaçlı yazılımlara karşı önlem yetenekleri içerir
- Kullanılan ürün setinin uyumlu olmasını sağlamak önemlidir

Windows sistemleri ayrıca bir dizi şifreleme işlevini destekler:

- Dosyaları ve dizinleri Şifreleme Dosya Sistemini (EFS) kullanarak şifrelenir
- BitLocker kullanarak AES ile tam disk şifreleme yapılır

"Microsoft Baseline Security Analyzer"

- Microsoft'un güvenlik önerileriyle uyumluluğu kontrol eden ücretsiz, kullanımı kolay araçtır

Sanallaştırma

- Sanal makine (VM) adı verilen simüle edilmiş bir ortamda çalışan bazı yazılımlar tarafından kullanılan kaynakların soyutlanmasını sağlayan bir teknolojidir
- Faydaları arasında fiziksel sistem kaynaklarının kullanımında daha iyi verimli olması vardır
- Tek bir fiziksel sistem üzerinde birden çok farklı işletim sistemi ve ilişkili uygulama için destek sağlar
- Ek güvenlik endişelerini artırır

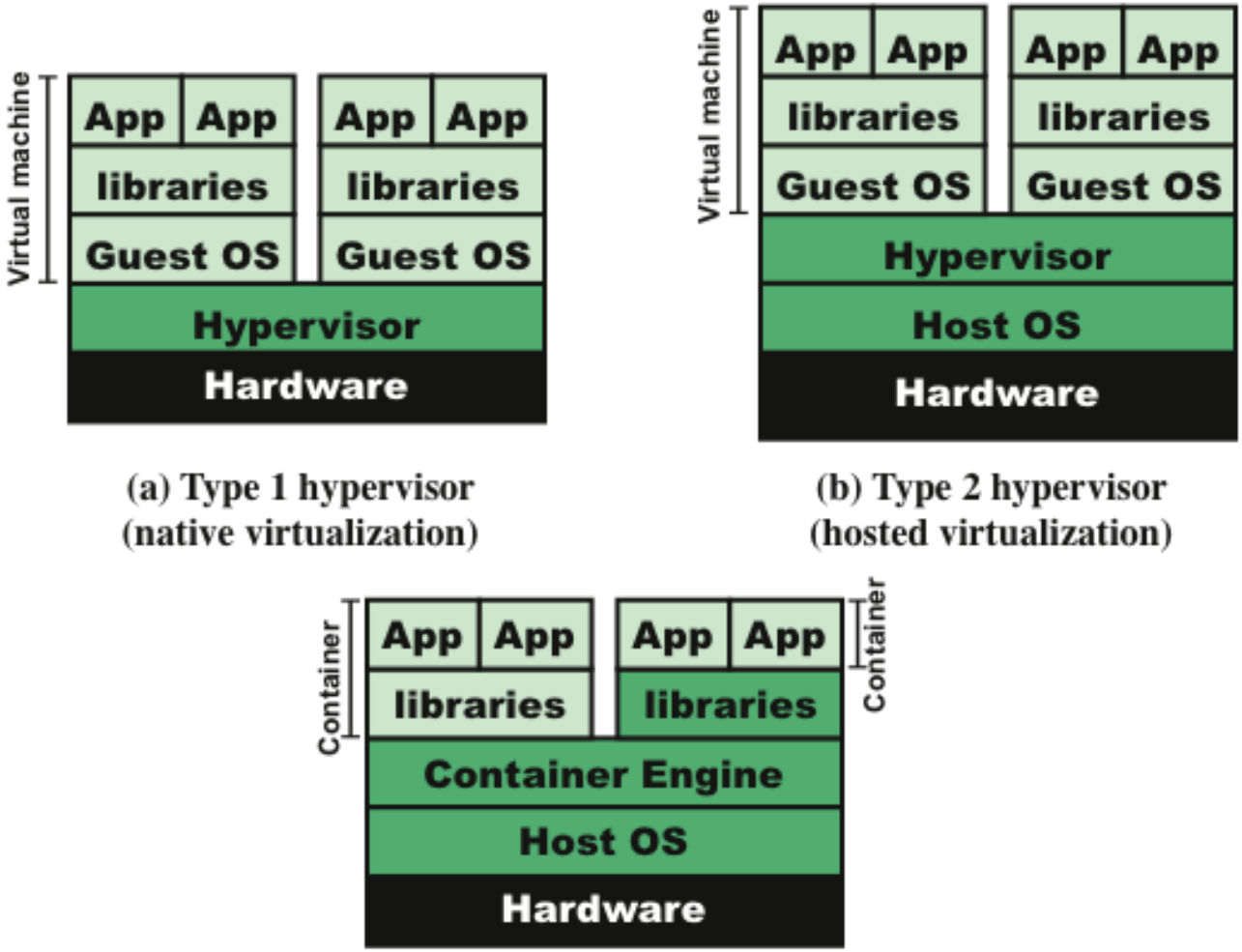
Hipervizör/Hypervisor

- Donanım ve sanal makineler arasında yer alan yazılım
- Bir kaynak komisyoncusu olarak hareket eder
- Birden çok VM'nin tek bir fiziksel sunucu ana bilgisayarında güvenli bir şekilde bir arada bulunmasına ve bu ana bilgisayarın kaynaklarını paylaşmasına izin verir.
- Sanallaştırma yazılımı, tüm fiziksel kaynakların soyutlanmasını sağlar ve böylece sanal makineler adı verilen çoklu bilgi işlem yığınlarının tek bir fiziksel ana bilgisayarda çalıştırılmasını sağlar.
- Her sanal makine, konuk işletim sistemi adı verilen bir işletim sistemi içerir.
    - Bu işletim sistemi, varsa, ana işletim sistemi ile aynı veya farklı bir işletim sistemi olabilir.

Hipervizör İşlevleri

Bir hipervizör tarafından gerçekleştirilen başlıca işlevler şunlardır:

- VM'lerin yürütme yönetimi
- Cihaz emülasyonu ve erişim kontrolü
- Konuk VM'ler için hipervizör tarafından ayrıcalıklı işlemlerin yürütülmesi
- VM'lerin yönetimi (VM yaşam döngüsü yönetimi olarak da adlandırılır)
- Hipervizör platformunun ve hipervizör yazılımının yönetimi



(a) Type 1 hypervisor (native virtualization)

(b) Type 2 hypervisor (hosted virtualization)

(c) Container (application virtualization)

Figure 12.2 Comparison of Virtual Machines and Containers

Sanallaştırılmış Sistemler

- Sanallaştırılmış sistemlerde, mevcut donanım kaynakları çeşitli konuk işletim sistemleri arasında uygun şekilde paylaşılmalıdır.
- Bunlar CPU, bellek, disk, ağ ve diğer bağlı cihazları içerir.
- CPU ve bellek genellikle bunlar arasında bölünür ve gerektiğinde programlanır.
- Disk depolama, her konuğun bazı disk kaynaklarını özel olarak kullanması ile bölümlenebilir.
- Alternatif olarak, her konuk için kendisine tam bir dosya sistemine sahip bir fiziksel disk gibi görünen ancak harici olarak alttaki dosya sisteminde tek bir "disk görüntüsü" dosyası olarak görüntülenen bir "sanal disk" oluşturulabilir.
- Optik diskler veya USB aygıtları gibi bağlı aygıtlar genellikle aynı anda tek bir konuk işletim sistemine tahsis edilir.

Yazılım Tanımlı Ağlar (SDN'ler)

SDN'ler, aynı temel fiziksel ağı kullanırken, ağ segmentlerinin veri merkezleri içinde ve arasında birden çok sunucuyu mantıksal olarak kapsamasını sağlar

Bindirmeli ağların kullanımı da dahil olmak üzere, SDN'leri sağlamaya yönelik birkaç olası yaklaşım vardır

- Bunlar, temeldeki fiziksel ağdan tüm katman 2 ve 3 adreslerini gerekli olan mantıksal ağ yapısına soyutlar
- Bu yapı ihtiyaca göre kolayca değiştirilebilir ve genişletilebilir
- VXLAN (Sanal Genişletilmiş Yerel Alan Ağı) kullanan IETF standardı DOVE (Dağıtılmış Bindirmeli Sanal Ağ), bu tür bir yer paylaşımlı ağ uygulamak için kullanılabilir
- Bu esnek yapı ile sanal sunucuları, sanal IDS'leri ve sanal güvenlik duvarlarını gerektiği gibi ağ içinde herhangi bir yere konumlandırmak mümkündür

Konteynerler

- Sanallaştırmaya yönelik yeni bir yaklaşım, *konteyner sanallaştırması* veya *uygulama sanallaştırması* olarak bilinir
- Bu yaklaşımda, sanallaştırma konteyneri olarak bilinen yazılım, ana işletim sistemi çekirdeğinin üzerinde çalışır ve uygulamalar için yalıtılmış bir yürütme ortamı sağlar
- Hipervizör tabanlı VM'lerin aksine, konteynerler fiziksel sunucuları taklit etmeyi amaçlamaz
- Bir ana bilgisayardaki konteynere alınmış tüm uygulamalar, ortak bir işletim sistemi çekirdeğini paylaşır
- Konteynerler için, konteynerlere destek olarak sadece küçük bir konteyner motoru gereklidir.
- Konteynerleştirme, işletim sistemi ile uygulamalar arasında yer alır ve daha düşük ek yüke neden olur, ancak potansiyel olarak daha büyük güvenlik açıkları ortaya çıkarır

Sanallaştırma Güvenlik Sorunları

- Güvenlik endişeleri şunlardır:
  - Konuk işletim sistemi izolasyonu
    - Konuk işletim sistemi içinde çalışan programların yalnızca kendisine tahsis edilen kaynaklara erişebilmesini ve bunları kullanabilmesini sağlamak
  - Hipervizör tarafından konuk işletim sistemi izleme
    - Her konuk işletim sistemindeki programlara ve verilere ayrıcalıklı erişime sahip olan
  - Sanallaştırılmış ortam güvenliği
    - Özellikle saldırganların görüntülemeye veya değiştirmeye çalışabilecekleri imaj ve shapshot yönetimi

Sanallaştırma Sistemlerini Güvenli Hale Getirme

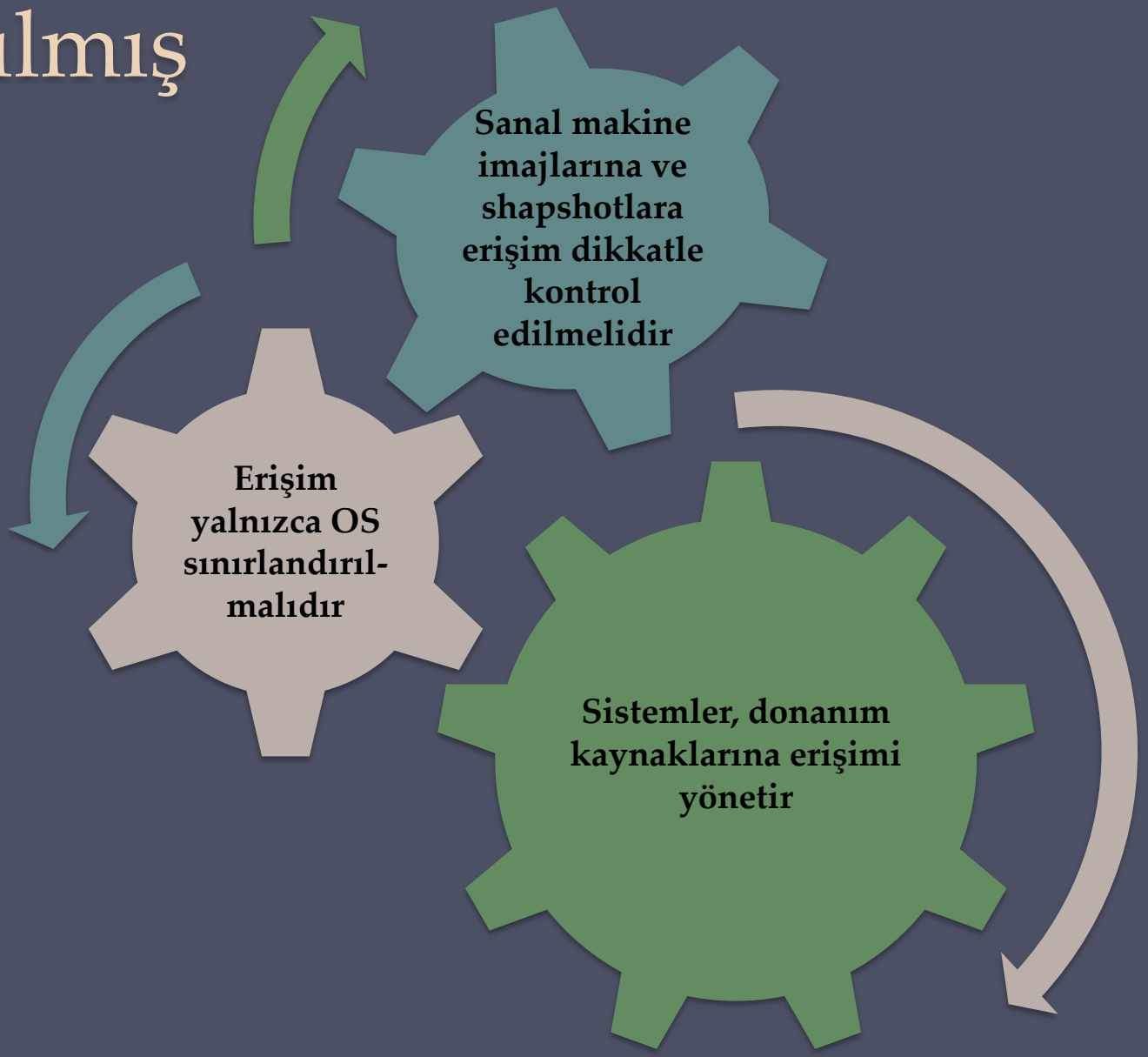
Sanallaştırmayı kullanan kuruluşlar:

- **Sanallaştırılmış sistemin güvenliğini dikkatlice planlamalı**
- **Eksiksiz bir sanallaştırma çözümünün tüm öğelerini emniyete almalı ve güvenliklerini sürdürmeli**
- **Hipervizörün uygun şekilde sabitlendiğinden emin olmalı**
- **Sanallaştırma çözümüne yönetici erişimini kısıtlamalı ve korumalı**

Hipervizör Güvenliği

- Yapılması gerekenler
  - Bir işletim sisteminin güvenliğini sağlamaya benzer bir işlem kullanılarak güvenlik altına alınır
  - Yalıtılmış bir ortama kurulur
  - Otomatik olarak güncellenecek şekilde yapılandırılır
  - Herhangi bir ele geçirme belirtisi için izlenir
  - Yalnızca yetkili yönetici tarafından erişilir
- Hem yerel hem de uzaktan yönetimi destekleyebilir, bu nedenle uygun şekilde yapılandırılmalıdır
- Uzaktan yönetim erişimi, kullanımda olan herhangi bir ağ güvenlik duvarı ve IDS yeteneğinin tasarımında dikkate alınmalı ve güvenliği sağlanmalıdır.
- İdeal olarak yönetim trafiği, kuruluş dışından sağlanan çok sınırlı erişime sahip ayrı bir ağ kullanmalıdır.

Sanallaştırılmış Altyapı Güvenliği



Sanal Güvenlik Duvarı

Sanallaştırılmış veya bulut ortamında barındırılan sistemler arasında akan ağ trafiği için, bu trafiğin geleneksel güvenlik duvarı hizmetlerini destekleyen fiziksel olarak ayrı bir ağa yönlendirilmesini gerektirmeyen güvenlik duvarı özellikleri sağlar

VM Kale Sunucu

IDS ve IPS hizmetleri de dahil olmak üzere fiziksel olarak ayrı bir kalede çalışacak şekilde yapılandırılabilecek aynı güvenlik duvarı sistemlerini ve hizmetlerini destekleyen ayrı bir VM'nin kale ana bilgisayarı olarak kullanıldığı durum

VM Sunucu tabanlı Güvenlik Duvarı

VM üzerinde çalışan Konuk İşletim Sistemi tarafından sağlanan ana bilgisayar tabanlı güvenlik duvarı özelliklerinin, bu ana bilgisayarı fiziksel olarak ayrı sistemlerde kullanılanla aynı şekilde güvence altına alacak şekilde yapılandırıldığı durum

Hipervizör Güvenlik Duvarı

Güvenlik duvarı özelliklerinin doğrudan hipervizör tarafından sağlandığı duruml