BSM 471-AĞ GÜVENLİĞİ

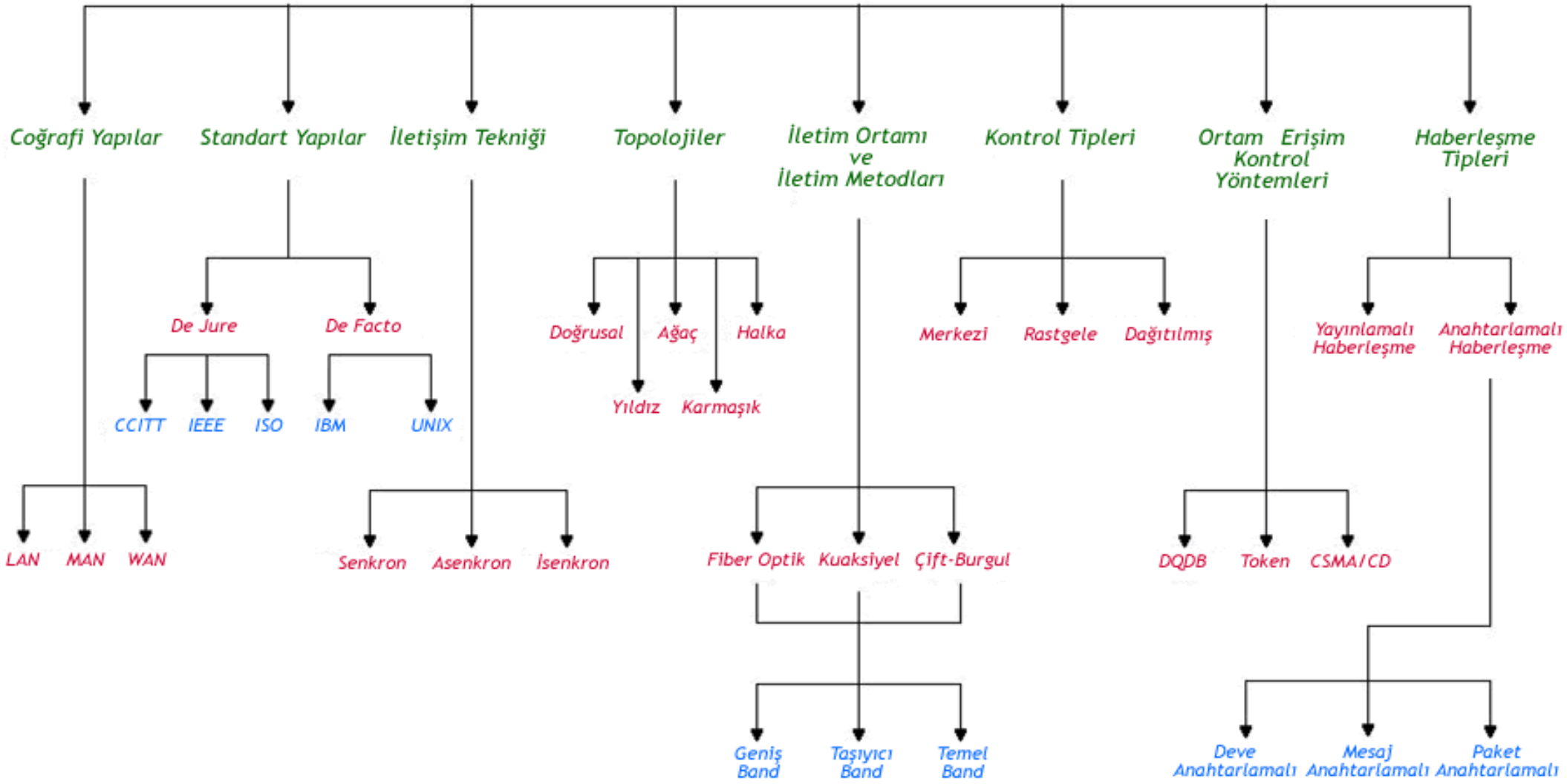
Hafta1: Ağ Güvenliği Temelleri ve Kavramlar

Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Haftalık İçerik

- Bilgisayar Ağları Temel Bilgileri
- Sınıflandırma Ağacı
- OSI Referans Modeli ve Çalışma Yapısı
- Arabağlantı Cihazları
- Güvenlik Kavramı
- Siber Güvenlik ve Ağ Güvenliği Temel Kavramlar

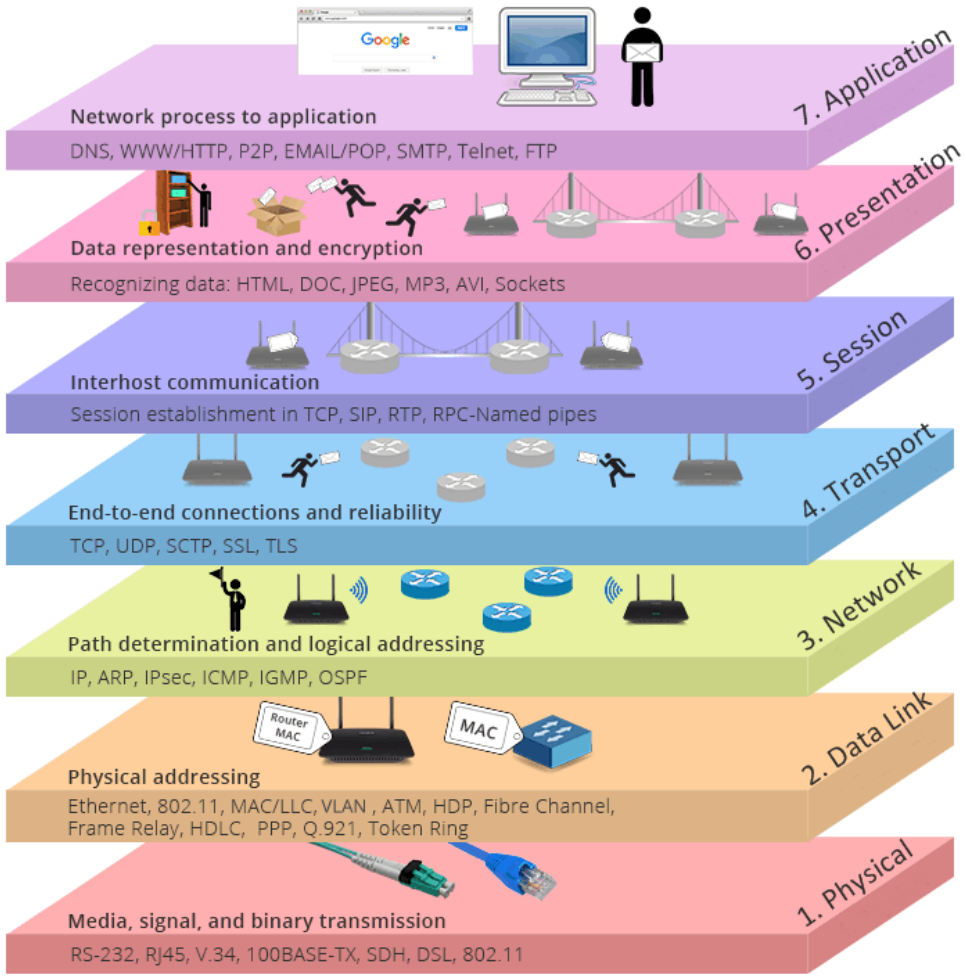
Bilgisayar Ağlarının Sınıflandırma Ağacı

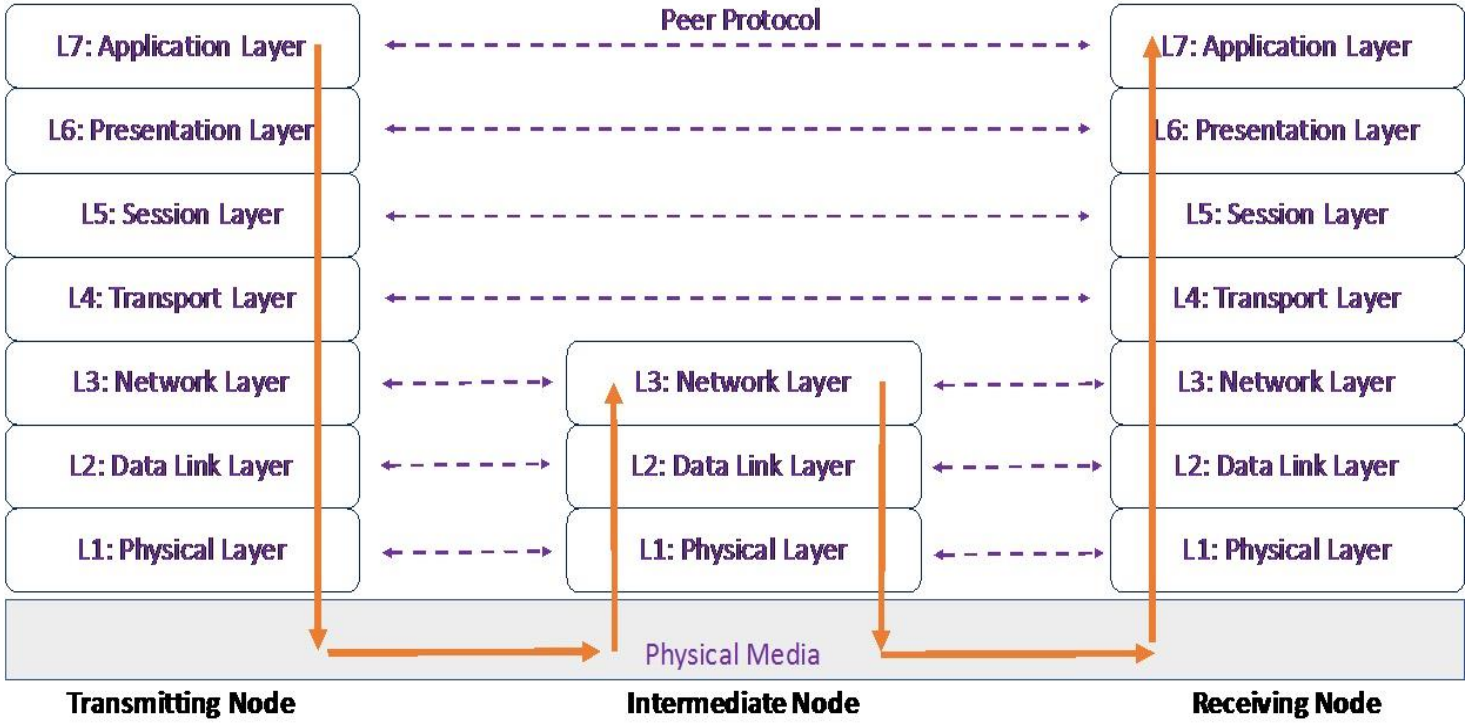


IEEE Standartları

Standart	Açıklama	Standart	Açıklama
IEEE 802.1	Üst Katman Ağ Yönetimi	IEEE 802.15	Kablosuz PAN
IEEE 802.2	Mantıksal Bağlantı Kontrolü	IEEE 802.15.1	**Bluetooth Sertifikasyon**
IEEE 802.3	**Ethernet**	IEEE 802.15.4	ZigBee Sertifikasyon
IEEE 802.4	**Token Bus**	IEEE 802.16	**Genişbant Kablosuz-WiMax**
IEEE 802.5	**Token Ring**	IEEE 802.16e	Mobil Genişbant Kablosuz
IEEE 802.6	Metropolitan Alan Ağları	IEEE 802.16.1	Yerel Multipoint Dağıtım
IEEE 802.7	Genişbant LAN-Coax Kablo	IEEE 802.17	Esnek Paket Ring
IEEE 802.8	**Fiber Optik TAG**	IEEE 802.18	Radyo Düzenleme TAG
IEEE 802.9	LAN Entegre Hizmetler	IEEE 802.19	Coexistence TAG
IEEE 802.10	LAN Birleştirilmiş Güvenlik	IEEE 802.20	Mobil Genişbant Kablosuz
IEEE 802.11	**Kablosuz LAN-Mesh (WiFi)**	IEEE 802.21	Ortam Bağımsız Handoff
IEEE 802.12	Talep Önceliği	IEEE 802.22	Kablosuz Bölgesel Alan Ağı
IEEE 802.14	**Kablo Modemler**	IEEE 802.23	Genişbant ISDN Sistemi

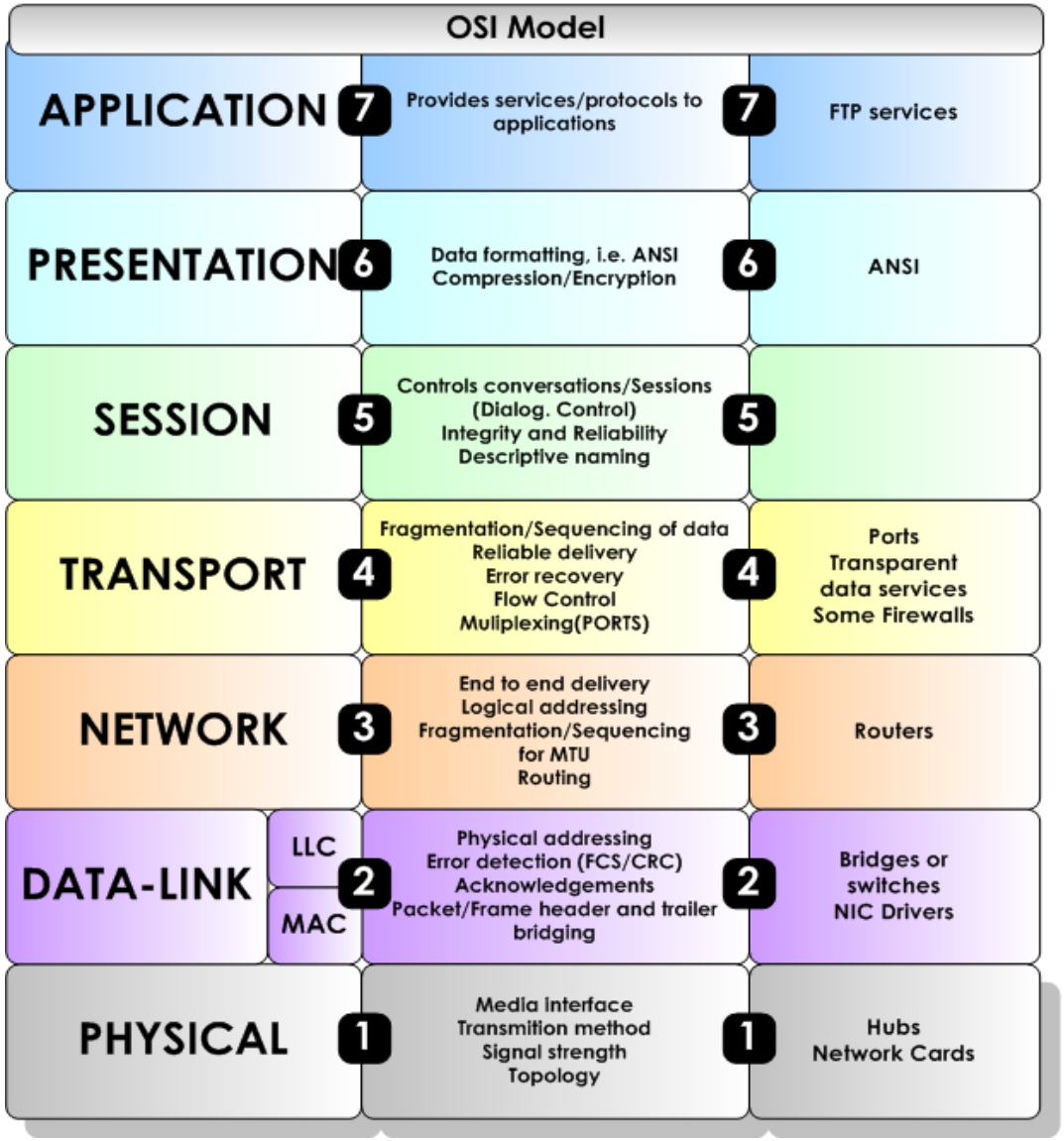
OSI Referans Modeli

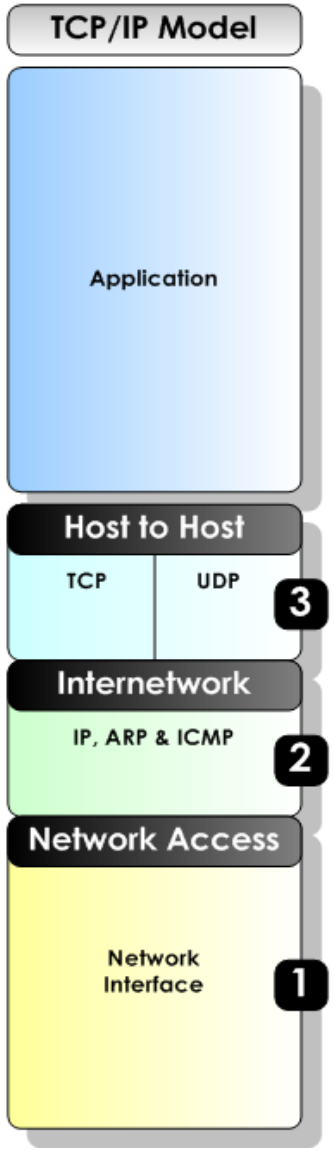


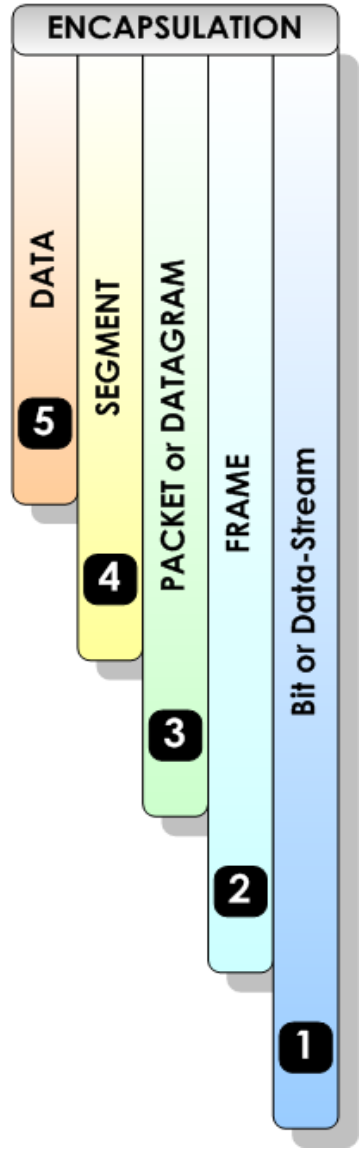


The OSI Model (Open Systems Interconnection)

© Copyright 2008 Steven Iveson
www.networkstuff.eu







Güvenlik Kavramları

- ***Bilgi güvenliği*;** izinsiz erişim, kullanım, kötüye kullanım, ifşa, yıkım, değişiklik veya bozulmaya neden olan, basılı, elektronik veya diğer herhangi bir türden gizli, özel ve hassas bilgiyi veya verileri korumak için tasarlanmış ve uygulanan süreçleri ve yöntemleri ifade eder. Bilgi güvenliğinin, siber güvenlikten farkı, siber uzayın dışındaki noktaları da içeren bir "bilgi sistemi" ve herhangi bir veri depolama noktasını içermesidir.

- ***Siber güvenlik;*** bilgi güvenliğinin bir alt kümesidir. Sistemleri, ağları ve programları dijital saldırılardan koruma pratiğidir. Bu saldırılar genellikle hassas bilgilere erişmeye, onları değiştirmeye veya yok etmeye yöneliktir.

- **Siber güvenlik yalnızca dijital verileri korumayı amaçlarken, bilgi güvenliği tüm verileri korumayı amaçlar.**

Güvenlik Kavramları (Devam)

- ***Ağ güvenliği;*** ağ altyapısını yetkisiz erişim, yanlış kullanım, arıza, modifikasyon ve imha gibi eylemlerden korumak için fiziksel ve yazılım önleyici tedbirler alma sürecidir. Böylece bilgisayarlar, kullanıcılar ve programlar için güvenli bir platform oluşturur.

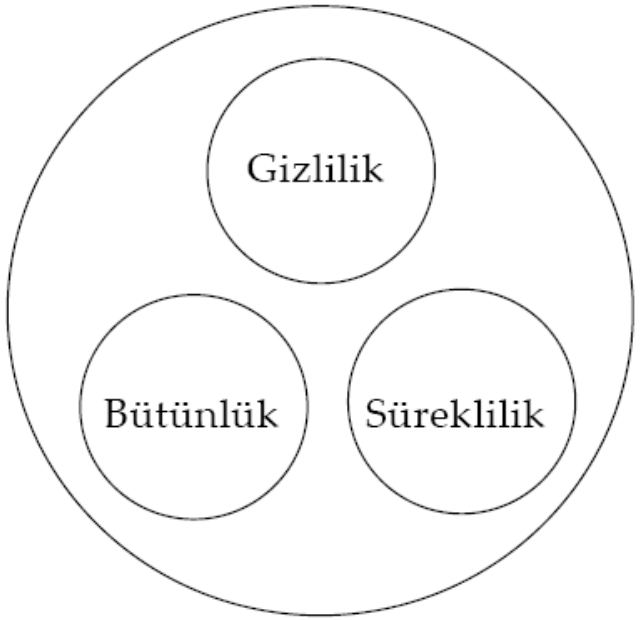
- Ağ güvenliği uzmanları şifreleri, güvenlik duvarlarını, internet erişimini, şifrelemeyi, yedeklemeleri ve daha fazlasını yakından takip ederek dahili korumaya odaklanır. Ana odakları, çalışan davranışlarını ve ağ erişimini izleyerek dahili bilgileri korumaktır. Siber güvenlik uzmanları, ağa sızmaya çalışan korsanları arayarak ve gelecekteki olası saldırılara karşı istihbarat kazanarak büyük olasılıkla dış tehditlere odaklanır. Ağ güvenliği uzmanları ise olası tehditleri tespit etmek ve ağı korumak için kullanılan yazılımları uygulamaya odaklanır.

Güvenlik Çeşitleri

- Bilgisayar/Uç Sistem Güvenliği
- Ağ Güvenliği
- Yazılım Güvenliği
- IoT Güvenliği
- Büyük Veri Güvenliği
- Bilişim Güvenliği
- Veri/Bilgi Güvenliği
- Sistem Güvenliği
- Veritabanı ve Uygulama Güvenliği
- Kablosuz Ağ Güvenliği
- ……

Güvenlik Prensipleri (Temel)

- **Gizlilik (Confidentiality):** Bilginin yetkisiz kişilerin eline geçmesini engellemektir. Bunu sağlamak için şifreleme yöntemleri kullanılır.
- **Bütünlük (Integrity):** Veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bunun için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar kullanılır.
- **Erişebilirlik (Availability):** Sistemleri, kurum içinden ve dışından gelebilecek tehditlere karşı korumaktır. Bunun için yedek sistemler, bakım, yedekleme, alternatif haberleşme kanalları kullanılır.



Güvenlik Prensipleri (Ek)

- **İzlenebilirlik (Accountability):** Sistemde gerçekleşen olayları, daha sonra analiz etmek üzere kayıt altına almaktır.
- **Kimlik Doğrulaması(Authentication):** Alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar, sertifikalar kullanılır.
- **İnkâr Edememe ((Non-repudiation):** Bilgiyi gönderen veya işleyen kişinin yaptığı işi sonradan inkar edememesidir. Bunun için sayısal (elektronik) imzalar, işlem kayıtları kullanılır.
- **Güvenilirlik (Reliability - Consistency):** Sistemin nasıl çalışması planlanmışsa, o şekilde çalışması ve her çalıştırıldığında aynı davranışı sergilemesidir.

OSI Güvenlik Mimarisi

- ITU-T, OSI için X.800 Güvenlik Mimarisi (Security Architecture) tanımlamıştır.
- X.800, güvenlik mimarisini 5 ana kategoriye ayırmıştır:
  - Kimlik Doğrulaması(Authentication)
  - Erişim Kontrolü (Access Control)
  - Veri Gizliliği (Data Confidentiality)
  - Veri Bütünlüğü (Data Integrity)
  - İnkar Edememe (Non-Repudiation)
- Kategorileri de alt başlıklara bölerek hangi güvenlik hizmetinin hangi katman(lar)da değerlendirilmesi gerektiğini belirlemiştir.

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

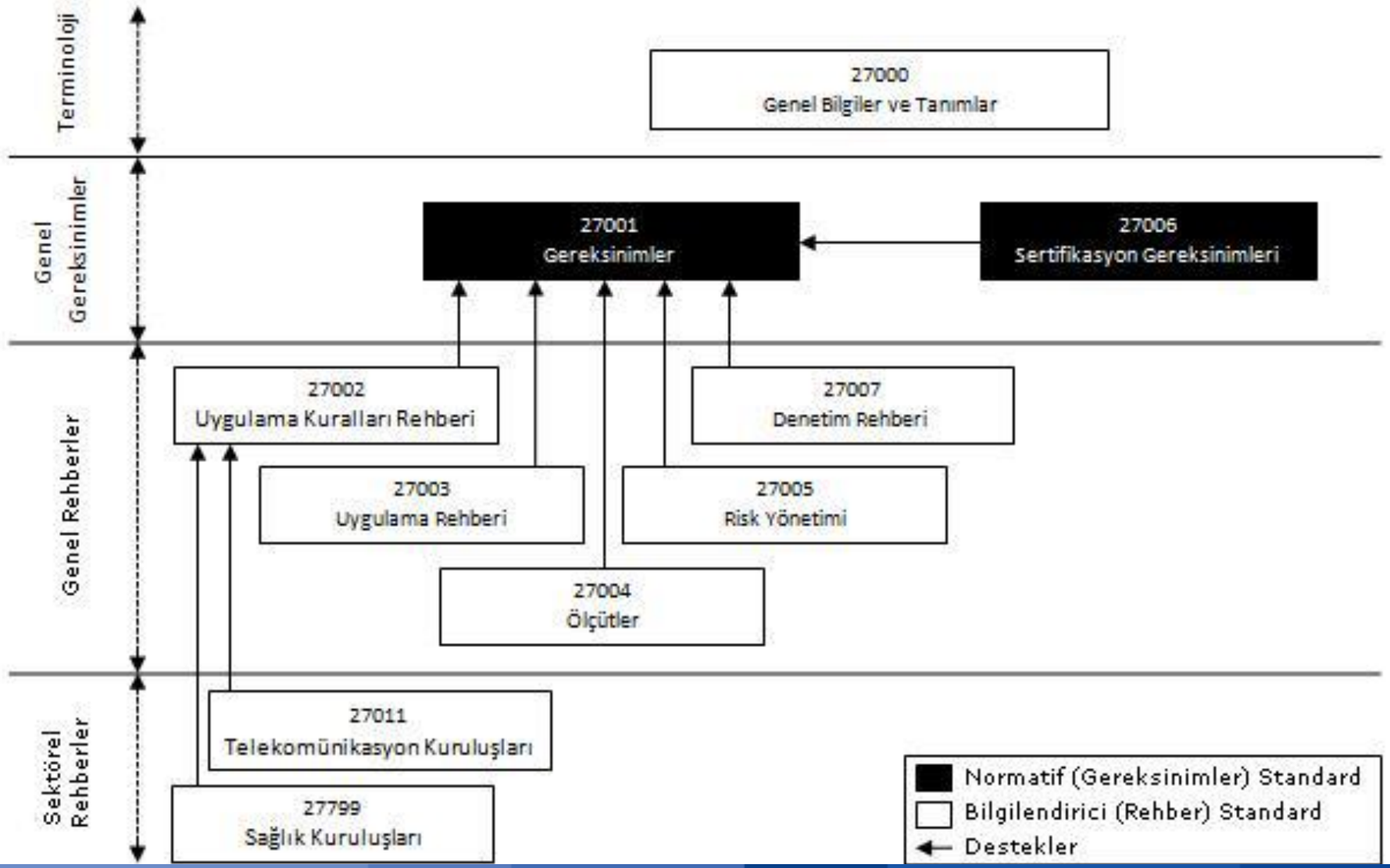
NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

ISO 27000 Güvenlik Serisi Ailesi



ISO 27001

- ISO 27001 BGYS standardı 39 kontrol hedefi ve 133 kontrol içeren toplam 11 güvenlik kontrol alanından oluşmaktadır. Burada geçen “kontrol”den kasıt politika, prosedür, rehber, pratikler veya organizasyon yapısı gibi risk yönetim araçları ve “kontrol amacı” ise kontrollerin uygulanması sonucu elde edilecek durumdur:
- ***1- Güvenlik Politikası:*** Bilgi güvenliği için yönetimin desteğini ve katılımını sağlamak, bilgi güvenliğinin önemini vurgulamak
- ***2- Bilgi Güvenliği Organizasyonu:*** Bilgi güvenliğinin koordinasyonu ve yönetimi için bir yönetim çerçevesi geliştirmek, bilgi güvenliği için sorumlulukları tahsis etmek
- ***3- Varlık Yönetimi:*** Tüm kritik veya hassas varlıklar için uygun bir koruma düzeyi belirlemek
- ***4- İnsan Kaynakları Güvenliği:*** Kullanıcı eğitimini ve bilincini teşvik ederek hırsızlık, dolandırıcılık veya bilgisayar kaynaklarının kötüye kullanılma riskini azaltmak
- ***5- Fiziksel ve Çevresel Güvenlik:*** Kuruluşun tesislerindeki bilgi işlem olanaklarına yetkisiz erişimi önlemek ve bilgilerin zarar görmesini engellemek

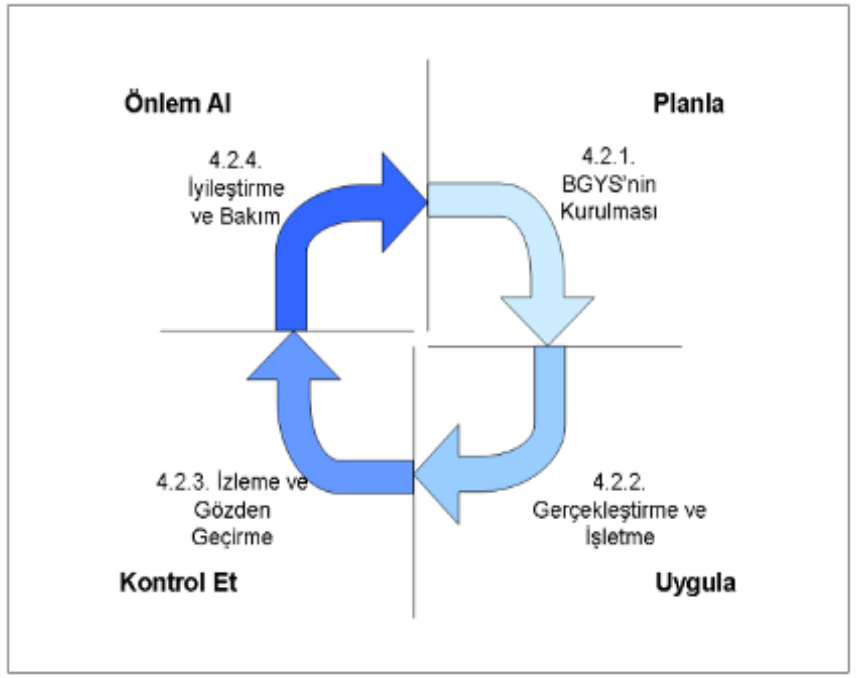
ISO 27001(devam)

- ***6- Haberleşme ve İşletim Yönetimi:*** Bilgi işlem tesislerinin uygun ve güvenli kullanımını sağlamak ve olay müdahale prosedürleri geliştirerek riski ve sonuçlarını azaltmak
- ***7- Erişim Kontrolü:*** Yetkisiz erişimlerin tespiti ve ağ sistemlerinin korunması için gerekli kontrol faaliyetlerini sağlamak
- ***8- Bilgi Sistemleri Edinim, Geliştirme ve Bakımı:*** İşletim sistemleri ve uygulama yazılımlarını bilgi kaybına karşı güncellemek ve kayıpları engellemek
- ***9- Bilgi Güvenliği İhlal Olayı Yönetimi***: Etkin bir bilgi güvenliği sağlamak için olayların zamanında tespit etmek ve gerekli önlemleri almak
- ***10- İş Sürekliliği Yönetimi:*** Kritik arızalar, olaylar, doğal afetler, felaketlerden kaynaklanan kesintilere karşı hızla müdahale edilebilmek için kapasite geliştirme faaliyetleri gerçekleştirmek
- ***11- Uyum:*** Mevcut güvenlik politikalarının tüm yasalara ve yönetmeliklere uygun olduğundan ve üst yönetim onayından geçtiğinden emin olmak

PUKÖ Döngüsü

- ISO 27001, BGYS'yi kurmak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için standart proses yaklaşımını benimsemiştir. Bu proses yaklaşımı güvenlik önlemlerinin belirlenip kurulması, uygulanması, etkinliğinin gözden geçirilmesi ve iyileştirilmesi süreçlerini ve bu süreçlerin sürekli olarak tekrarlanmasını içerir.

- ***Planla:*** BGYS'nin kurulması: Sonuçları kuruluşun genel politikaları ve amaçlarına göre dağıtmak için, risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, hedefler, prosesler ve prosedürlerin kurulması.
- ***Uygula:*** BGYS'nin gerçekleştirilmesi ve işletilmesi: BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesi.
- ***Kontrol Et***: BGYS'nin izlenmesi ve gözden geçirilmesi: BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi.
- ***Önlem Al:*** BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi: BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi



Siber Tehdit Kavramı

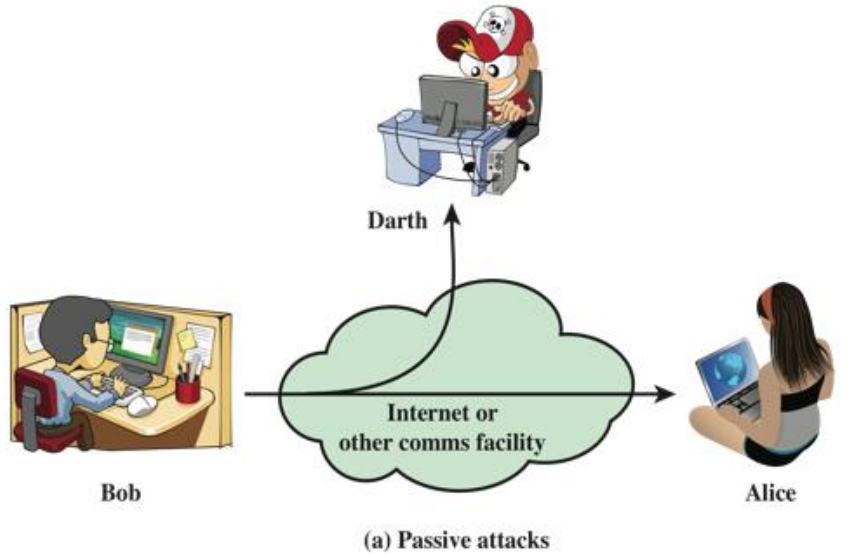
- Siber tehdit kavramı genel olarak, yetkisiz kişi veya kurumların başka bir kişi veya kurumların bilişim altyapılarının (ağ sistemlerine, veri tabanı, ağ cihazlarına vb.) kullanılabilirliği, bütünlüğü veya gizliliğine zarar vermek amacıyla erişmeleri anlamına gelmektedir.

Siber Tehdit Aktörleri

- ***Devlet destekli tehdit aktörler:*** politik, ekonomik, askeri vb. nedenler sebebiyle hedef ülkelerin kurum/kurumlarına saldırı düzenleyen ilgili devlet kontrolünde kapsamlı ve nitelikli bir gruptur.
- ***Hacktivistler:*** Herhangi bir kurum veya kuruluşa bağlı olmadan, bir propaganda doğrultusunda hedef kuruma saldırı düzenleyen gönüllü gruplardır.
- ***Siber teröristler:*** Gerçek hayattaki ideolojik ve siyasi kazanımlar amacıyla barışçıl olmayan yöntemlerle hedef kişi veya kurumları yıldırma veya zarar verme eyleminin siber dünyada gerçekleştirilen kişilere denir. Kimlik avı, zararlı yazılım, virüs vb. çok farklı teknik ve yöntem kullanabilirler.
- ***Ticari rakipler:*** Aynı sektörde çalışan kurumların ekonomik açıdan birbirlerine üstünlük sağlamak amacıyla gerçekleştirilen siber saldırıları yöneten tehdit aktörleridir.
- ***Fırsatçı kişi/kişiler:*** Bu grupta bulunan siber tehdit aktörleri genellikle profesyonel olmayan yöntemlerle, siber dünyada isimlerini duyurabilmek amacıyla hedef sistemlere saldırı yapan kişilerdir.

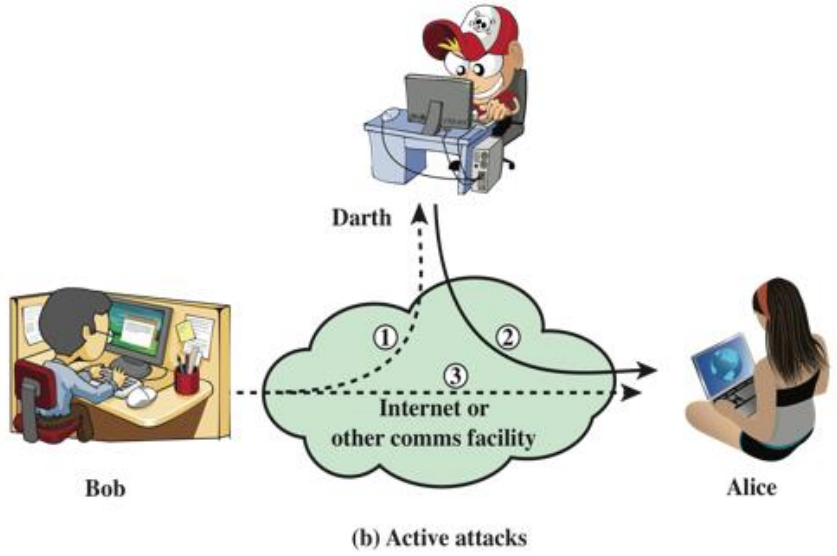
Siber Saldırıların Sınıflandırılması

- ***Pasif bir saldırı,*** sistemden bilgi öğrenmeye veya sistemden yararlanmaya çalışır ancak sistem kaynaklarını etkilemez.
  - Mesaj içeriğinin serbest bırakılması
  - Trafik analizi



(a) Passive attacks

- ***Aktif bir saldırı***, sistem kaynaklarını değiştirmeye veya onların çalışmasını etkilemeye çalışır.
  - Çok çeşitli potansiyel fiziksel, yazılım ve ağ güvenlik açıkları nedeniyle önlenmesi zor

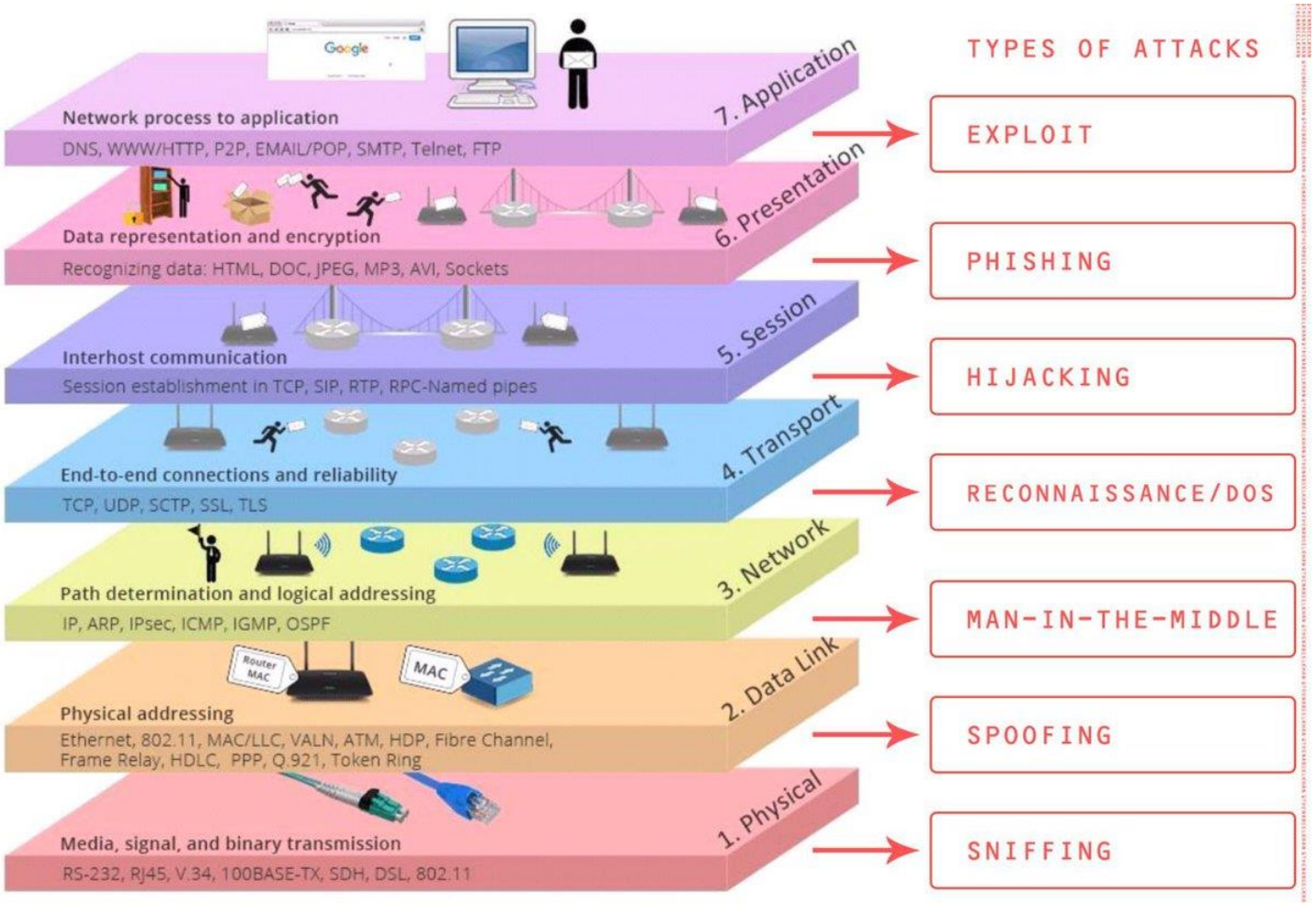


(b) Active attacks

Aktif Saldırı Yöntemlerinin Karakteristikleri

Interruption (Engelleme)	• Kaynak ve hedef sistemler arasında bilgi akışı engellenmektedir. Böylece, bilgiye erişim engellenmiş olmaktadır.
Intecept (Dinleme)	• Kaynak ile hedef sistemler veya bilgisayarlar arasındaki iletişimin dinlenmesi yolu ile verinin okunmasıdır.
Modification (Değiştirme)	• Kaynak bilgisayardan hedef bilgisayara gönderilen verinin, araya giren saldırgan tarafından değiştirilmesi ve içeriği değiştirilen verinin hedef bilgisayardan geliyormuş gibi gönderilmesidir.
Fabrication (Uydurma)	• Bu saldırı türünde, saldırgan tarafından üretilen yeni bir veri söz konusudur.

Siber Tehdit Aktörleri-Saldırı Yöntemleri (Katmansal Gösterim)



APT (Advanced Persistent Threat-Gelişmiş Israrcı Tehdit) Kavramı

- APT kavramı, bir siber saldırganın hedefe yetkisiz olarak erişim yapması ve uzun süre tespit edilmeden hedef sistemde kalmasına denir.
- Bir APT saldırısının ana amacı genellikle hedef ağ sistemine, kuruma zarar vermekten ziyade o sistemdeki ağ trafiğini/harekelerini izlemek ve verileri elde etmektir.
- APT saldırılarında izlenen yol aşağıdaki gibidir:

Tehlike Göstergeleri (Indicator of Compromise)

- Tehlike Göstergeleri (IoC) bir siber saldırının gerçekleştirildiğinin adli kanıtıdır.
- IoC'ler, gerçekleştirilen siber saldırıları hakkında ağ ve sistem yöneticilerinin bilgi sahibi olmalarını sağlar. Ayrıca yapılan saldırıların analiz edilerek yorumlanmasıyla bir sonraki saldırılara karşı tedbir alınmasını sağlamaktadır.
- Ağ yöneticileri ve sistem analistlerinin siber saldırılara karşı dikkate aldıkları bazı uzlaşma göstergeleri şu şekildedir:
  - Olağan dışı ağ trafiği
  - Yönetimsel hesaplardaki olağan dışı hareketler
  - Yetkisiz girişler
  - Farklı kaynaklardan aynı noktaya çok fazla istek
  - Veri tabanına erişim boyutundaki artış

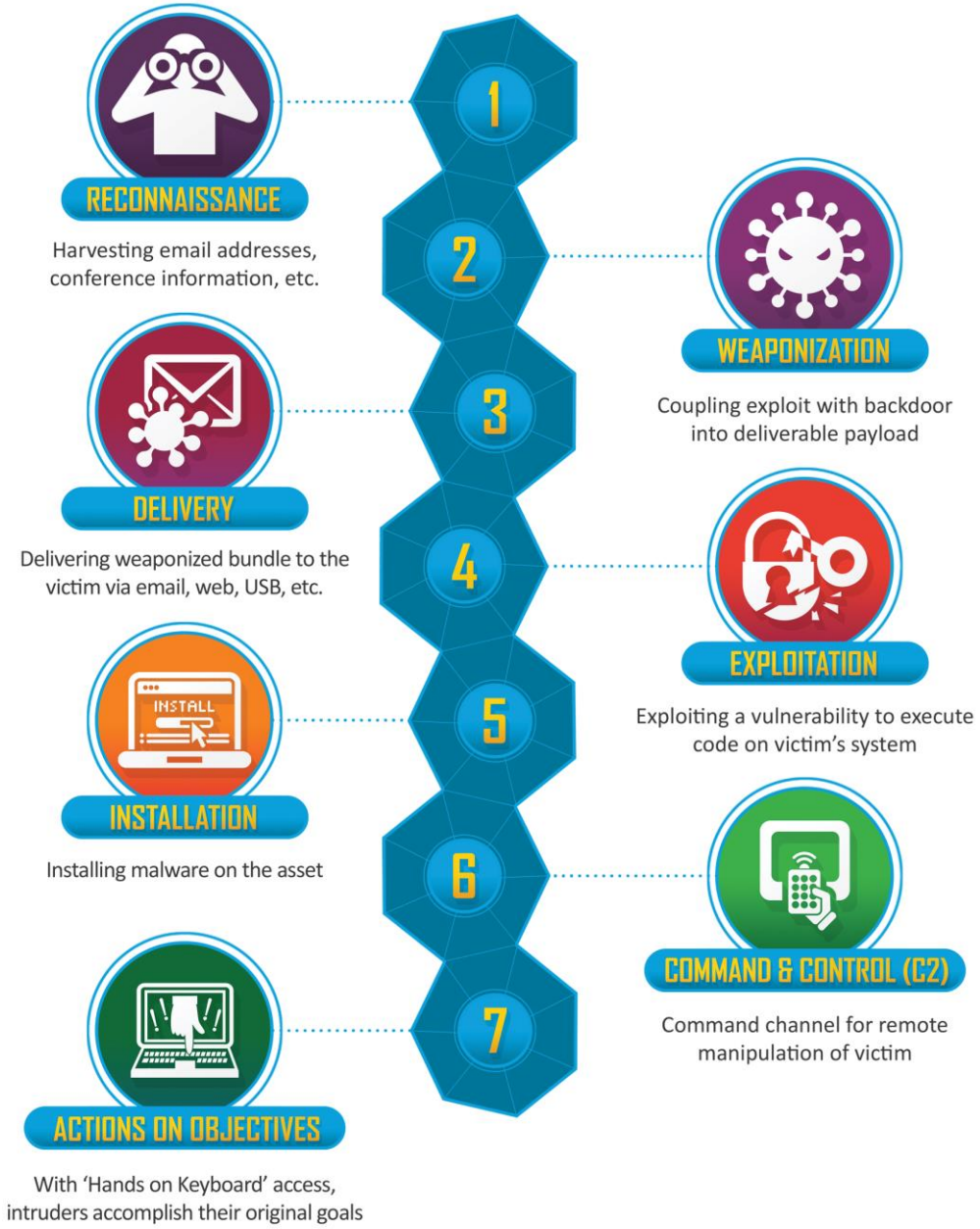
“Pyramids of Pain” Kavramsal Modeli

TTP (Taktik, Teknik ve Prosedürler)

- Taktikler, teknikler ve prosedürler terimi, bir APT saldırısını analiz etme veya mevcut bir tehdit aktörünün profilini belirlemeye yarar.
- ***Taktik kelimesi,*** bir saldırganın saldırısını başından sonuna kadar gerçekleştirmeyi seçtiği yöntemi belirtir.
- ***Teknik kelimesi*** ise saldırı işlemi sırasında ara sonuçlara ulaşmanın teknolojik yaklaşımı saldırganın kullandığı yöntemler ile tanımlanmaktadır.
- ***Prosedür kelimesi*** ise de, saldırının örgütsel yaklaşımı belirtilmektedir.

Atak Modelleri

- Atak modelleri veya saldırı yaşam döngüleri saldırıları analiz etmek ve analiz sonuçlarına bağlı olarak benzer saldırıları engellemek amacıyla geliştirilmiş yöntemlerdir.
  - Cyber Kill Chain
  - Mandiant Attack Life Cycle
  - MITRE ATT&CK



Cyber Kill Chain

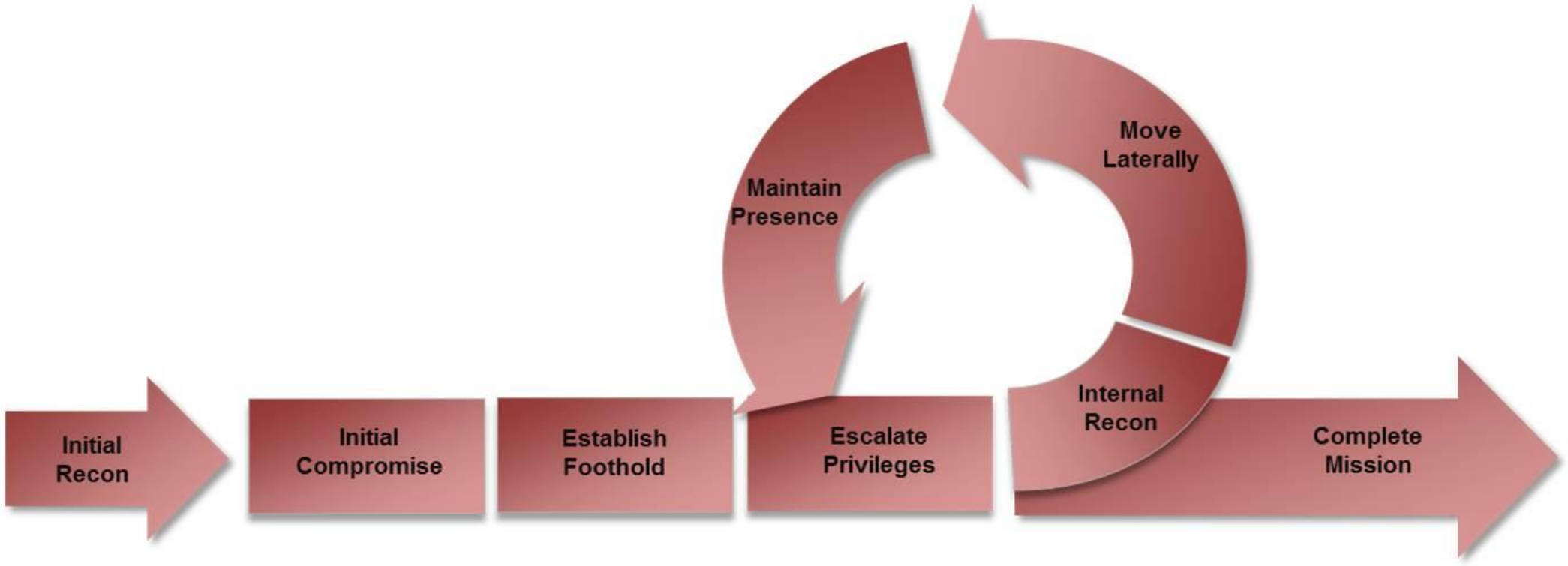
- Hedefli saldırıların aşamalarını tanımlamak için kullanılmaktadır.
- Lockheed Martin silah firması, tarafından önerilmiştir.

Cyber Kill Chain Aşamaları

1. **Keşif (Reconnaisance):** Sistemlere giriş yapılacak noktalar belirlenir ve gerekli bilgiler toplanır.
2. **Silahlanma (Weaponization):** Silahlanma aşaması, kullanılacak silahın belirlendiği, zararlı yazılımların oluşturulduğu ve paketlendiği aşamadır.
3. **İletme (Delivery):** Zararlı yazılımların kurum/kuruluş ağına nasıl sızdırılacağına karar verilir.
4. **Sömürme (Exploitation):** Hedef sistemlerdeki zafiyetten yararlanma aşamasıdır.
5. **Yükleme (Installation):** Saldırganların sistemlere uzaktan bağlanabilmesi için gerekli uygulama kurulumlarının yapıldığı aşamadır.
6. **Komuta Kontrol (Command&Control)**
7. **Eyleme Geçme (Actions on Objectives)**

Mandiant Attack Lifecycle

- “APT1 Exposing One of China’s Cyber Espionage Units”



Mandiant Attack Lifecycle Aşamaları

1. **İlk Keşif (Initial Recon):** Sistemlere giriş için ilk keşif faaliyetlerini kapsar.
2. **İlk İstila (Initial Comprimise):** Hedef ve saldırı vektörleri belirlendikten sonra denemeler.
3. **Yerleşme (Establish Foothold):** Zararlı yazılımların kurum/kuruluş ağına sızdırılması.
4. **Yetki Yükseltme (Escalate Priviliges)**
5. **İç Keşif (Internal Recon):** Ağdaki diğer sistemleri keşfetme işlemi.
6. **Yayılma (Move Laterally)**
7. **Yerini Sağlamlaştırma (Maintain Presence)**
8. **Görevi Tamamlama (Complete Mission)**

MITRE ATT&CK

- MITRE ATT&CK Framework, saldırıları daha iyi sınıflandırmak ve bir kurumun riskini değerlendirmek için tehdit avcıları, kırmızı takım ve savunucuların kullandığı kapsamlı taktik ve teknikler matrisidir.
- Bu çerçeve yapısının asıl amacı tehdit aktörlerinin bir saldırıdaki davranışlarını sistematik olarak kategorize etmektir.
- 3 farklı ATT&CK matrisi bulunmaktadır:
  - Kurumsal ATT&CK
  - PRE-ATT&CK
  - Mobil-ATT&CK

MITRE ATT&CK-Devam

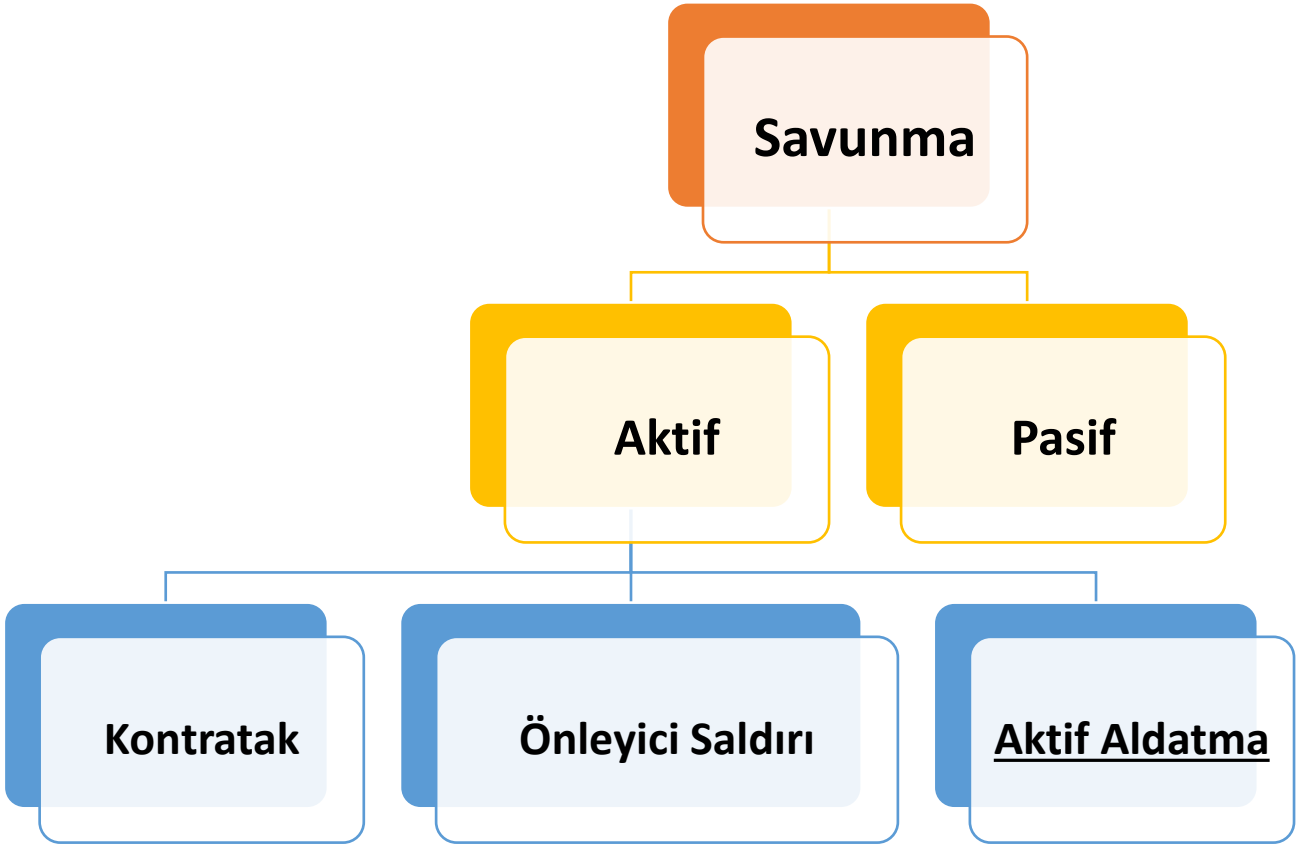
1. Başlangıç Erişimi Sağlama
2. İcra Etme
3. Kalıcılık Sağlama
4. Ayrıcalık Kazanma-Hak Yükseltme
5. Savunma Sisteminden Kaçınma
6. Kimlik Bilgisi ile Erişim Sağlama
7. Keşif Yapma
8. Yanal Hareket Yapma
9. Toplama
10. Komut ve Kontrol Sunucusu ile Haberleşme
11. Sızıntı Oluşturma
12. Etki Oluşturma

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Savunma

- *Saldırıyı önlemek için yapılan her türlü eylem*



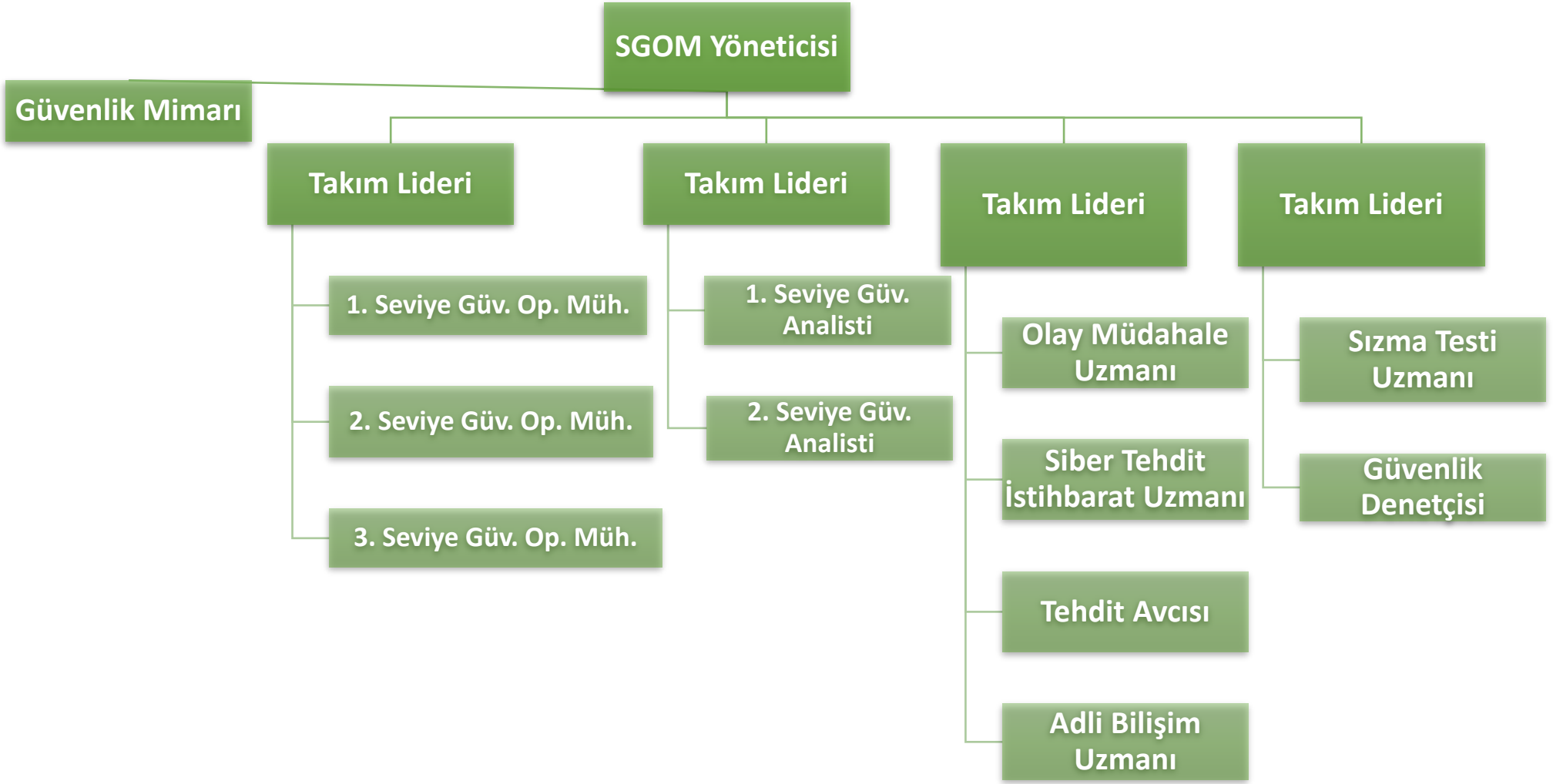
Pasif Savunma

- Saldırgan/lar tarafından yapılan/yapılacak eylemlerin kurum için sebep olacağı zararların etkisini azaltmak için alınan önlemlerdir.
- Pasif savunma teknikleri;
  - Güncelleme/yamalama/sıkılaştırma
  - Güçlü parola kullanımı
  - Şifreleme
  - Erişim yönetimi uygulaması
  - Anti-zararlı yazılım
  - Güvenlik duvarı
  - IDS/IPS
  - SIEM

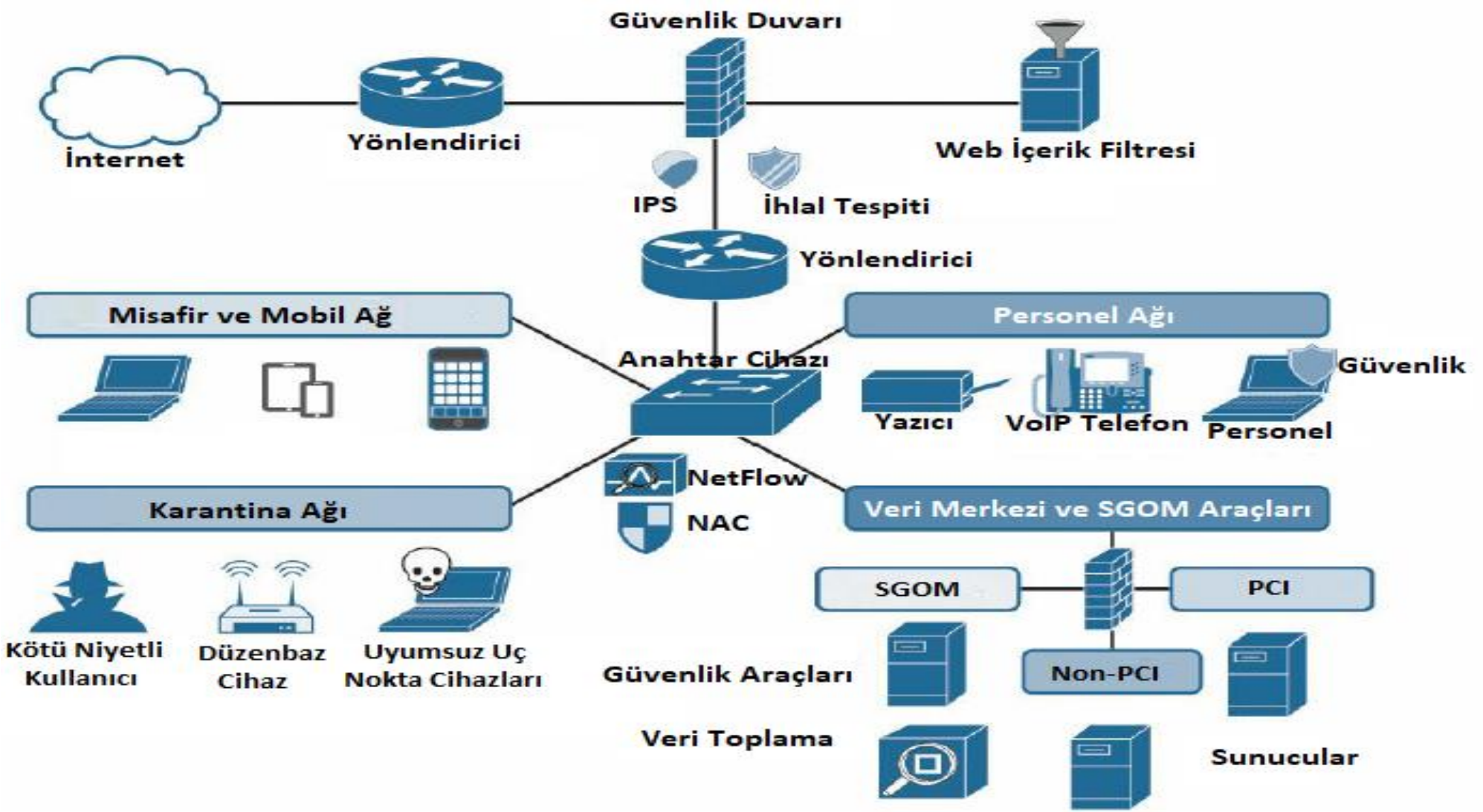
Aktif Savunma

- ***Kontratak;*** Bir saldırının hemen ardından veya saldırı esnasında saldırganların dikkatlerini dağıtarak, motivasyonlarını kırma amacıyla başlatılan karşı saldırı.
- ***Önleyici saldırı;*** siber istihbarat verilerine göre bir saldırıdan önce, saldırganın saldırmasına olanak vermeden yapılan karşı saldırı.
- ***Aktif aldatma;*** Saldırganları hedef sistem içerisinde sahte kaynaklara yönlendirmek.

Büyük Ölçekli SGOM-Organizasyon Yapısı



Örnek Bir Güvenli Ağ Mimarisi



Network Security Logical Architecture