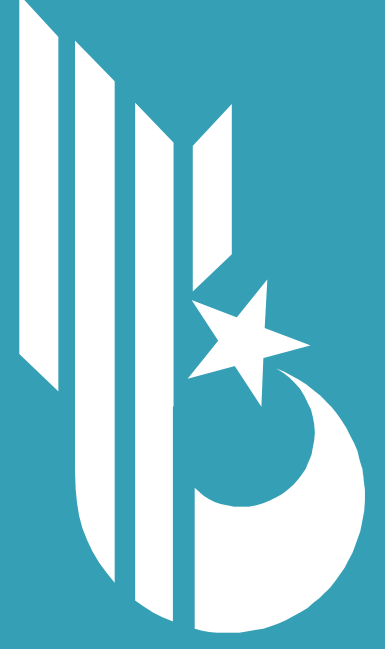




BTK
AKADEMİ

SİBER GÜVENLİĞE GİRİŞ

ATIL SAMANCIOĞLU

EĞİTİMİN HEDEFİ / AMACI



- Bu dersin amacı, katılımcıların siber güvenlik hakkında giriş seviyesinde bilgi edinmelerini sağlamaktır.

EĞİTİMİN SEVİYESİ



- Bu dersin seviyesi, katılımcıların siber güvenlik hakkında giriş seviyesinde bilgi edinmelerini sağlamak amacıyla oluşturulmuş 'Temel Seviye' düzeyinde bir müfredatı kapsamaktadır.

HEDEF KİTLE



- Siber güvenlik alanına giriş yapmak ve bilgisini artırmak isteyenler,
- Lise öğrencileri,
- Üniversite öğrencileri,
- Mezunlar ve çalışanlar.

ÖN KOŞULLAR



- İyi düzeyde Bilgisayar Okuryazarlığı,
- Bilgi Teknolojilerine Giriş Eğitimi'ni almış olması tavsiye edilir.
- Bilgi Güvenliğine Giriş Eğitimi'ni almış olması tavsiye edilir.

SIK SORULAN SORULAR



SORU: Bu eğitim siber güvenlik farkındalık eğitimi midir?

CEVAP: Hayır. Bu eğitim bir mesleki saha olan siber güvenliği temel seviyede ve genel kapsamda öğretmektedir. Kullanıcıların dikkat etmesi gereken konuların açıklandığı farkındalık eğitimi değildir.

SIK SORULAN SORULAR



SORU: Bu eğitimi sadece siber güvenlik alanında ilerlemek isteyenler veya çalışanlar mı almalı?

CEVAP: Hayır. Bu eğitim, bilgi teknolojileri alanında çalışan herkes için uygundur. Siber güvenlik alanına yönelenler için ise en baştan gereklidir.

SIK SORULAN SORULAR



SORU: Ağ yöneticisi, Yazılım Geliştirici, Veri tabanı Uzmanı veya Sistem Yöneticisi olmak istiyorum. Bu eğitimi ilk başta almam zorunlu mu?

CEVAP: Hayır. Bu eğitimi kariyerinizin en başında almanız zorunlu değildir. Ancak ilerleyen aşamalarda bu eğitimi almak tavsiye edilir.

EĞİTİM KAZANIMLARI



Eğitim sonunda;

- Siber güvenliği ve ilgili kavramları temel seviyede ifade edebilir,
- Siber güvenliğin alt alanlarının(sistem güvenliği, uygulama güvenliği, ağ güvenliği, veri tabanı güvenliği vb.) ne olduğunu ifade edebilir,
- Siber zafiyetlerin ne olduğunu ve kaynaklarını ifade edebilir,
- Siber tehdit, risk ve saldırı kavramlarını ayırt edebilir,

EĞİTİM KAZANIMLARI



Eğitim sonunda;

- Siber güvenliği sağlamak için yönetimsel süreçler hakkında bilgi sahibi olur,
- Siber güvenliği sağlamak için teknik bileşenler ve işlemler hakkında bilgi sahibi olur,
- Siber güvenlik alanındaki pozisyonların / rollerin neler olduğunu bilir,
- Siber güvenlik alanındaki standart ve sertifikalar hakkında bilgi sahibi olur,
- Siber güvenlik alanında hangi alana yöneleceğini kavrayabilirsiniz.



Bölüm 1

SİBER GÜVENLİĞE GİRİŞ SİBER GÜVENLİK NEDİR?

SİBER GÜVENLİK NEDİR?



- Siber, sadece internet değildir. Çok daha fazlasıdır.
- **Siber güvenlik ise** dijital ortamda bilginin ve verinin güvenliği için yapılan tüm çalışmalardır.
- Ağ yapısına bağlı sistemleri ve bu sistemlerle ilişkili verileri yetkisiz kullanım veya zararlardan korumak için sarf edilen sonsuz bir çabadır.



Bölüm 2

VERİ NEDİR? KİŞİSEL VERİLER NELERDİR?

VERİ NEDİR?

- Veri, bilgisayarların işleyebileceği bir forma dönüştürülmüş gerçekler (sayılar, kelimeler, ölçümler, gözlemler, vb.) topluluğudur.



KİŞİSEL VERİLER NELERDİR?

1. **Çevrimdışı Kimliğiniz**
2. **Çevrimiçi Kimliğiniz**
3. **Tıbbi Kayıtlar (Hasta Kayıtları)**
 - Fiziksel, zihinsel ve diğer kişisel bilgiler
 - Reçeteler
4. **Eğitim Kayıtları**
 - Notlar, sınav puanları, alınan dersler, ödüller ve dereceler
 - Devamlılık
5. **İstihdam ve Finansal Kayıtlar**
 - Gelir ve giderler
 - Vergi kayıtları - maaş çekleri, kredi kartı ekstreleri, kredi notu ve bankacılık ekstreleri
 - Geçmiş istihdam ve performans bilgileri





Bölüm 3

BİLGİ GÜVENLİĞİ NEDİR?

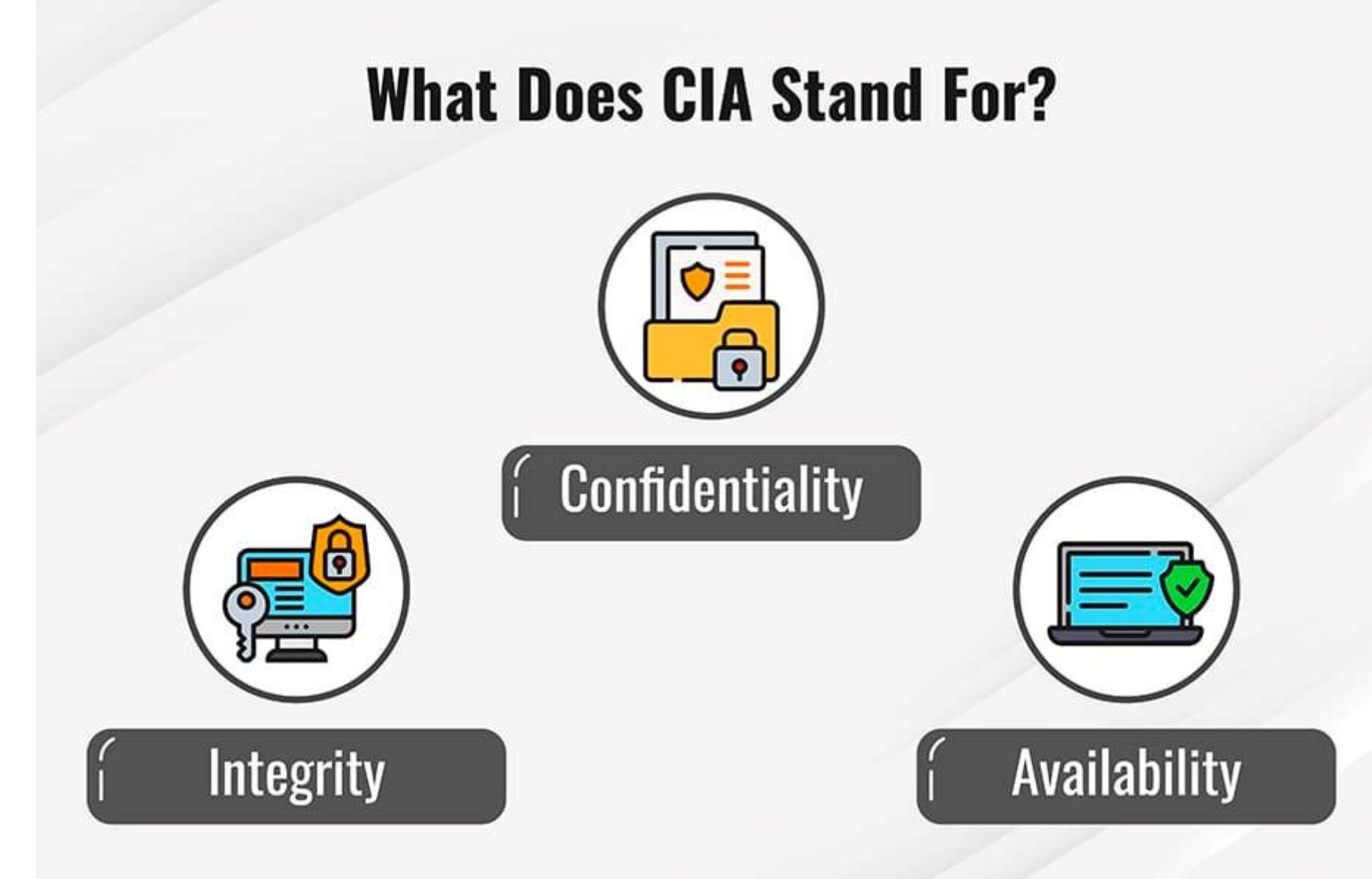
BİLGİ GÜVENLİĞİ NEDİR?



- Bilgi güvenliği, bir organizasyonun veya bireyin hassas bilgilerini, verilerini ve bilgi kaynaklarını, yetkisiz erişim, değiştirme, ifşa veya zarar verme gibi tehditlere karşı koruma sürecidir.
- Bilgi güvenliği, bilgiyi gizli, bütünlüklü ve erişilebilir şekilde koruma amacını taşır. Bu kapsamda bilgi güvenliği, fiziksel güvenlik önlemlerini, teknik önlemleri ve insan kaynaklarına yönelik politikaları içerir.

BİLGİ GÜVENLİĞİNİN TEMEL HEDEFLERİ

- **Gizlilik:** Hassas bilgilerin yetkisiz kişiler tarafından erişilmesini önlemek.
- **Bütünlük:** Bilgilerin değiştirilmesini veya bozulmasını engellemek.
- **Erişilebilirlik:** Yetkilendirilmiş kullanıcıların bilgilere güvenli bir şekilde erişimini sağlamak.
- **Süreklilik:** Bilgilerin sürekli olarak kullanılabilir ve erişilebilir olmasını sağlamak.
- **İzlenebilirlik:** Bilgiye kimin eriştiğini ve ne zaman eriştiğini izleyebilme yeteneği.



SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ

- **Bilgi Güvenliği Genel Bir Yaklaşım:** Bilgi güvenliği, organizasyonların genel olarak bilgi varlıklarını korumak için aldıkları önlemleri kapsar.
- **Siber Güvenlik Özel Bir Alan:** Siber güvenlik, bilgi sistemlerini ve ağları korumak için alınan spesifik önlemleri ifade eder. Siber güvenlik, bilgi güvenliğinin bir parçasıdır ve bilgi sistemlerinin çevrimiçi tehditlere karşı korunmasına odaklanır.
- **Karşılıklı Bağımlılık:** Bilgi güvenliği ve siber güvenlik arasındaki ilişki karşılıklıdır. Siber güvenlik, organizasyonların bilgi güvenliğini sağlama çabalarının önemli bir bileşenidir. Bilgi güvenliği politika ve prosedürleri, siber güvenlik tedbirlerini içerirken, siber güvenlik önlemleri de bilgi güvenliğini destekler.



HACKER TÜRLERİ

Junior
Hackers



Script
Kiddies



Green Hat
Hackers



Blue Hat
Hackers

Types of Hackers



Black Hat:
Criminal
Hackers



White Hat:
Authorized
Hackers



Gray Hat:
"Just for Fun"
Hackers



Green Hat:
Hackers-in-Training



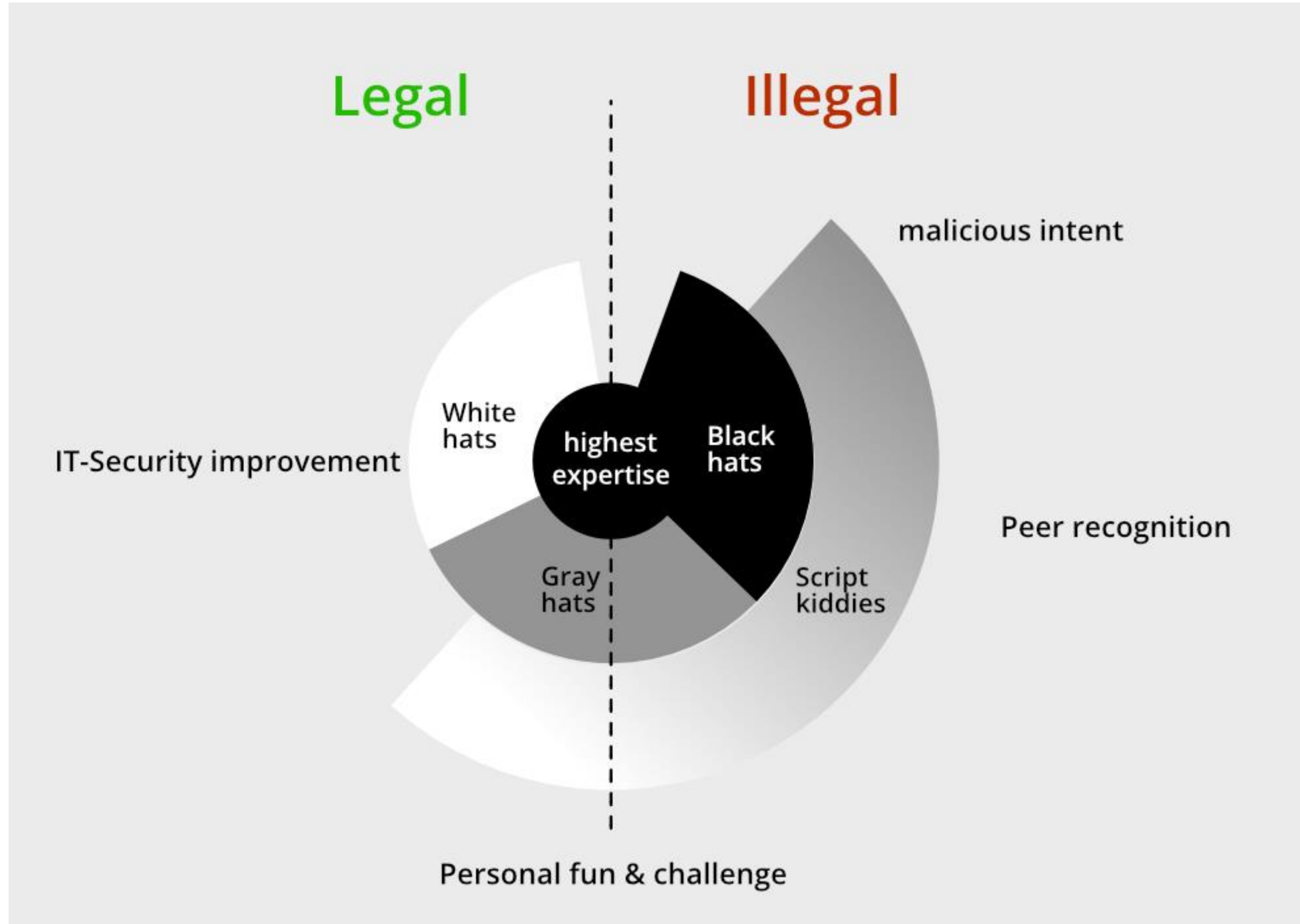
Blue Hat:
Authorized
Software Hackers



Red Hat:
Government-Hired
Hackers

- Siber güvenliğe karşılaşılabileceğiniz çeşitli saldırgan türleri bulunur. Bu saldırganlar farklı amaçlarla hareket ederler ve farklı yeteneklere sahiptirler.
- İşte siber güvenlikteki bazı saldırgan türleri ve detayları:

SİYAH ŞAPKALI HACKER (BLACK HAT HACKERS)

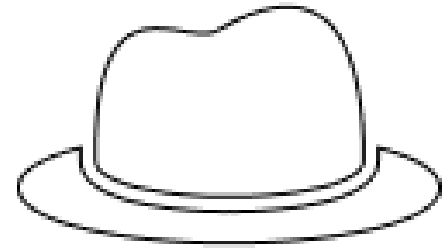


KAYNAK: <https://www.geeksforgeeks.org/what-are-white-hat-gray-hat-and-black-hat-hackers/>

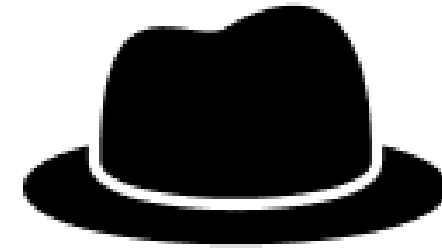
- Amaçları kötüdür.
- Bilgisayar sistemlerine izinsiz erişmek, bilgileri çalmak veya zarar vermek gibi kötü niyetli eylemleri gerçekleştirirler.
- Saldırganlar, kişisel kazanç veya zarar verme amaçlarıyla hareket edebilirler.

BEYAZ ŞAPKALI HACKER (WHITE HAT HACKERS)

White hat hacker VS Black hat hacker



- Increases the security framework
- Develops a high-security structure
- Updates and regularly checks the security
- Develops systems like firewall, ad blocker, etc.



- Reduces security by stealing data
- Gains access to accounts and sensitive data
- Steals valuable data from the organization
- Gains access to restricted areas

- Amaçları iyidir.
- Bilgisayar sistemlerinin güvenliğini test etmek veya zafiyetleri tespit etmek için izin almış güvenlik uzmanlarıdır.
- Sorunları tespit edip düzeltme konusunda organizasyonlara yardımcı olurlar.

GRİ ŞAPKALI HACKER (GREY HAT HACKERS)

White, gray and black hat comparison



WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws



GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes

Prioritize their own perception of right versus wrong over what the law might say



BLACK HAT

Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong

Exploit security flaws for personal or political gain—or for fun

KAYNAK: <https://lahjaty.com/white-hat-vs-black-hat/>



KAYNAK: <https://techcrunch.com/sponsor/king-university/different-types-of-hackers/>

- Amaçları karmaşıktır ve genellikle belirsizdir.
- İzin almadan bilgisayar sistemlerini test edebilirler, ancak bu işlemi kötü niyetli amaçlarla yapmazlar.
- Sistem zafiyetlerini tespit edip sahiplerine bildirirler, ancak izin almadan test yapma eğilimindedirler.

SOSYAL MÜHENDİSLER (SOCIAL ENGINEERS)

Social Engineering

The Art of Human Manipulation

Definition

Social engineering is the act of manipulating people into divulging sensitive information or performing acts that compromise security.

Techniques

Phishing, pretexting, baiting, and tailgating

Targets

Employees, customers, and vendors

Goals

Obtain sensitive information, gain unauthorised access, or commit fraud

Prevention

Awareness, training, and robust security measures



- Teknik bilgisayar becerileri yerine insanları manipüle etmeye odaklanan saldırganlardır.
- Kişisel bilgileri, kimlik bilgilerini veya giriş bilgilerini elde etmek için insanların güvenini kazanmaya çalışırlar.

SCRIPT KIDDIES

- Genellikle teknik bilgiye sahip olmayan veya sınırlı bilgiye sahip olan amatör saldırganlardır.
- Hazır yazılımları veya saldırı araçlarını kullanarak basit saldırılar gerçekleştirirler.
- Genellikle popüler olmayan hedeflere yönelirler.

Hackers vs. script kiddies		
	HACKERS	SCRIPT KIDDIES
Experience	More experienced	Inexperienced
Knowledge	- Skilled and knowledgeable - Well researched - Persist through challenges	- Limited knowledge and skills - Launch exploits without knowing much about them - Apt to quit
Methods	Use off-the shelf exploits but also can code their own and adapt methods to challenges	Use off-the-shelf and beginner programs written by other people

Script Kiddies



Motivation: Use existing malware to break into personal devices and private networks

Potential Targets: Internet users and businesses

KAYNAK: <https://us.norton.com/blog/emerging-threats/types-of-hackers>

HACKER GRUPLARI (HACKTIVIST GROUPS)

ATTACK CYCLE OF HACKTIVISM



- Belirli bir sosyal veya politik amaç için siber saldırılar gerçekleştiren gruplardır.
- Örnek olarak Anonymous gibi gruplar, çevrimiçi aktivizm veya sansür karşıtı eylemler için siber saldırılar düzenlerler.

SİBER GÜVENLİK UZMANLARI



SİBER GÜVENLİK YETENEKLERİ



Linux
Python
Network
Şifreleme
Yazılım Geliştirme
Bulut Bilişim
Donanım
Adli Bilişim
Sosyal Mühendislik



Bölüm 4

SİBER GÜVENLİK KATEGORİLERİ

SİBER GÜVENLİKLE İLGİLİ TEMEL KAVRAMLAR

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Siber Tehdit (Cyber Threat):** Bilgisayar sistemlerine veya dijital ortama zarar verme veya hassas bilgilere erişme amacıyla gerçekleştirilen herhangi bir potansiyel zararlı aktiviteyi ifade eder.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Siber Saldırı (Cyber Attack):** Bilgisayar sistemlerine veya dijital altyapılara yönelik saldırılar, siber tehdidin gerçekleştirildiği eylemlerdir.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Firewall:** Ağ trafiğini izleyen ve izin verilen trafiği geçiren, izin verilmeyen trafiği engelleyen bir güvenlik cihazıdır.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Şifreleme (Encryption):** Bilgilerin açık metin halinden, anlaşılması zor hale getirerek güvenli bir şekilde saklanmasını veya iletilmesini sağlayan bir güvenlik yöntemidir.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Kimlik Doğrulama (Authentication):** Kullanıcıların veya sistemlerin kimliklerini doğrulama sürecidir. Parola, biyometrik veriler veya iki faktörlü kimlik doğrulama bu kavrama örnek olarak verilebilir.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Yetkilendirme (Authorization):** Kimlik doğrulama sonrasında kullanıcılara veya sistemlere belirli kaynaklara erişim izni verilmesi sürecidir.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Güvenlik Güncellemeleri (Security Patch):** Yazılım veya işletim sistemlerindeki güvenlik açıklarını kapatmak için yayınlanan düzeltmelerdir. Bu güncellemeler, bilgisayarların güvenliğini artırmak için önemlidir.

GENEL SİBER GÜVENLİK KAVRAMLARI



KAYNAK: https://www.barewalls.com/art-print-poster/phishing-word-cloud_bwc72992591.html



- **Sosyal Mühendislik (Social Engineering):** Siber saldırganların insanları manipüle ederek hassas bilgilere veya sistemlere erişmeye çalıştığı bir saldırı taktiğidir. Örnekler arasında sahtekârlık, telefon dolandırıcılığı ve phishing (oltalama) yer alır.
- **Sosyal Mühendislik Testleri:** İnsanların güvenlik önlemlerini manipüle etmeye çalışan saldırılar veya testler. Bu, sahtekarlık ve insanların duygusal tepkilerini kullanma stratejilerini içerebilir.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Veri Sızıntısı (Data Breach):** Hassas veya kişisel bilgilerin izinsiz bir şekilde sızdırılması veya çalınmasıdır. Bu, kullanıcıların gizliliğinin ihlal edilmesine neden olabilir.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Ağ Güvenliği (Network Security):** Bilgisayar ağlarını, ağ trafiğini ve verileri koruma amacıyla alınan önlemleri ifade eder.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Güvenlik Politikası (Security Policy):** Bir organizasyonun veya bireyin siber güvenlikle ilgili belirlediği kurallar, prosedürler ve yönergelerdir.
- **Güvenlik Bilinci (Security Awareness):** Kullanıcıların siber güvenlik risklerini ve önlemlerini anlama ve bu konuda eğitilmiş olma durumunu ifade eder.

GENEL SİBER GÜVENLİK KAVRAMLARI



404
NOT FOUND

- **Ofansif Güvenlik (Hacking):** Sistemlerin veya ağların güvenlik önlemlerini aşmayı amaçlayan siber saldırılar veya testler için kullanılan teknikler ve stratejiler.
- **Defansif Güvenlik (İyileştirme-Güçlendirme):** Bilgisayar sistemlerini ve ağları koruma amacıyla güvenlik önlemlerini geliştirme ve iyileştirme süreçleri.

GENEL SİBER GÜVENLİK KAVRAMLARI

- **Sızma Testi (Penetrasyon Testi / Penetration Test):** Bilgisayar sistemlerinin veya ağların güvenlik açıklarını ve zafiyetlerini belirlemek için yapılan kontrollü saldırı ve testler.
- **İç Ağ Sızma Testi (Internal Test):** Bir organizasyonun iç ağındaki güvenlik açıklarını ve riskleri değerlendirmek için gerçekleştirilen sızma testleri.
- **Dış Ağ Sızma Testi (External Test):** Bir organizasyonun dış ağındaki güvenlik açıklarını ve riskleri değerlendirmek için gerçekleştirilen sızma testleri.



GENEL SİBER GÜVENLİK KAVRAMLARI

- **Uygulamaya Yönelik Sızma Testleri (+Mobil):** Web uygulamaları veya mobil uygulamalar gibi yazılım uygulamalarının güvenlik açıklarını ve zafiyetlerini tespit etmek için yapılan testler.
- **Bilgi Toplama Yöntemleri (Pasif / Aktif):** Siber saldırganların veya güvenlik uzmanlarının hedef sistem veya organizasyon hakkında bilgi toplama işlemleri. Pasif bilgi toplama, kamu kaynaklarından veri toplamayı içerirken, aktif bilgi toplama, hedef sistemle doğrudan etkileşim gerektirebilir.



GENEL SİBER GÜVENLİK KAVRAMLARI

0 1 0 1 0 1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0
0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 1 0 0 0 0 1 0
1 1 0 1 1 1 0 0 0 0 0 0 1 1 0 0 0 0 1 0 1 1 0 1
1 0 0 0 0 0 1 0 1 0 1 1 1 1 1 1 0 1 0 1 1 0 0 1
0 0 0 1 0 1 0 1 0 0 0 0 1 1 1 0 1 0 1 0 0 0 0 0
0 1 1 0 1 0 1 0 1 1 1 0 0 0 0 1 0 1 0 0 0 1 1 0
1 0 1 1 0 1 0 1 0 0 0 0 0 0 1 0 1 0 1 1 1 0 1 1
0 1 1 0 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 0 0 1 1 0
0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 1 1 1 1 0 0 1 0
0 1 0 0 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 0 0 1 0 0
1 0 0 0 1 1 1 0 0 1 0 0 0 0 0 0 1 1 1 1 0 0 1
0 1 1 0 0 1 0 1 0 0 1 1 1 1 1 1 1 1 0 0 1 1 0
0 0 0 0 0 1 1 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0
0 1 0 1 1 0 0 0 1 1 0 0 1 0 1 1 0 1 0 1 0 0
0 0 1 0 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0 1 0
1 1 1 1 1 0 1 0 1 1 1 1 0 1 1 1 1
0 1 0 1 1 0 0 1
1 0 1
0 0 1
1



- **Sızma Testi Yöntemleri (Black Box – Gray Box – White Box):** Sızma testi sırasında test edilen sistem veya uygulamanın bilgilendirilme düzeyine göre kullanılan yaklaşımlar.
- **Siyah kutu (Black Box),** hiçbir önceden bilgiye sahip olunmadan test edilirken, **beyaz kutu (White Box)** tam bilgiye sahip olunarak test edilir. **Gri kutu (Gray Box)** ise kısmi bilgiye sahip olunarak yapılan bir yaklaşımı ifade eder.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Zafiyet Taraması (Vulnerability Assessment):** Bilgisayar sistemlerinde ve ağlarda potansiyel güvenlik zafiyetlerini belirlemek ve sınıflandırmak için kullanılan bir süreç.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Exploit:** Güvenlik açığı veya zafiyeti kullanarak bir sisteme veya uygulamaya sızmayı veya kontrol etmeyi amaçlayan yazılım veya kod parçası.

GENEL SİBER GÜVENLİK KAVRAMLARI



KAYNAK: <https://stock.adobe.com/>

- **Google Hacking (Google Dork):** Google gibi arama motorları kullanarak hassas veya gizli bilgilere erişmeye çalışan siber saldırılar veya arama sorguları.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Siber terör**, siber alanlarda yasa dışı veya tehlikeli eylemleri teşvik eden veya gerçekleştiren bir grup veya bireyler tarafından gerçekleştirilen eylemleri tanımlayan bir terimdir.
- Siber terör, geleneksel terörizmin dijital ortamda gerçekleşen bir uzantısıdır.

GENEL SİBER GÜVENLİK KAVRAMLARI



- **Siber suç**, bilgisayarlar, ağlar ve dijital teknoloji kullanarak yasa dışı faaliyetlerde bulunma eylemidir. Bu faaliyetler genellikle finansal kazanç, veri çalma veya zarar verme amaçları taşır.



Bölüm 5

SİBER GÜVENLİK FARKINDALIĞINI TEHDİT EDEN UNSURLAR

SİBER GÜVENLİK TEHDİT UNSURLARI

- Eskiden siber saldırılar sadece büyük kuruluş ve sistemlere yapılırdı. Artık kötü niyetli saldırganlar, kişi veya kuruluş ayırt etmiyor.
- Reklamlar veya masum görünen paylaşımlara kontrolsüz tıklama.
- Halka açık bir internete bağlanma hatası.
- Siber güvenlik tehdit unsurları, bilgisayar sistemleri, ağlar ve dijital varlıklar için potansiyel risk oluşturan faktörlerdir.
- İşte siber güvenlik tehdit unsurlarının bazıları:



SİBER GÜVENLİKTE KARŞILAŞILAN SİSTEMSEL TEHDİTLERE ÖRNEKLER

Kötü Amaçlı Yazılım (Malware)

Virüs

Truva Atları (Trojans)

Casus Yazılım (Spyware)

Botnet'ler

Fidye Yazılımı (Ransomware)

Buffer Overflow

Cross-Site Request Forgery (CSRF)

Cross-Site Scripting (XSS)

Broken Access Control

Zero-Day Exploits (0 Days)

Port Configuration Hataları

RAT (Remote Access Trojan)

Man-in-the-Middle (MITM) Saldırıları

Denial-of-Service (DOS) Saldırıları



ZARARLI YAZILIM NEDİR?

- Zararlı yazılımlar, sistemleri parçalamaya, bilgi sızdırmaya, sistemi ele geçirmeye yönelik olabilir.
- Özünde her zararlı yazılım bir kod parçacığıdır.
- Onları kendi içerisinde kategorize eden şey bulaştıkları sistemde nasıl davranışlar sergiledikleridir.
- Bu davranışlara göre zararlı yazılım bir Trojan, Worm, Ransomware veya virüs olarak anılabilirler.



1- VİRÜS

Types of viruses



KAYNAK: <https://fpttelecom.com/blog/virus-may-tinh-la-gi/>

- Virüs, bilgisayarlar ve diğer dijital cihazlar için zararlı yazılımlardan biridir.
- Bir virüs, genellikle zararlı bir program veya kod parçasıdır ve başka bir programın içine veya dosyasına yerleştirilmiştir.
- Bilgisayarınıza bulaştığında, zararlı kodlar çalışır ve cihazınıza zarar verebilir.

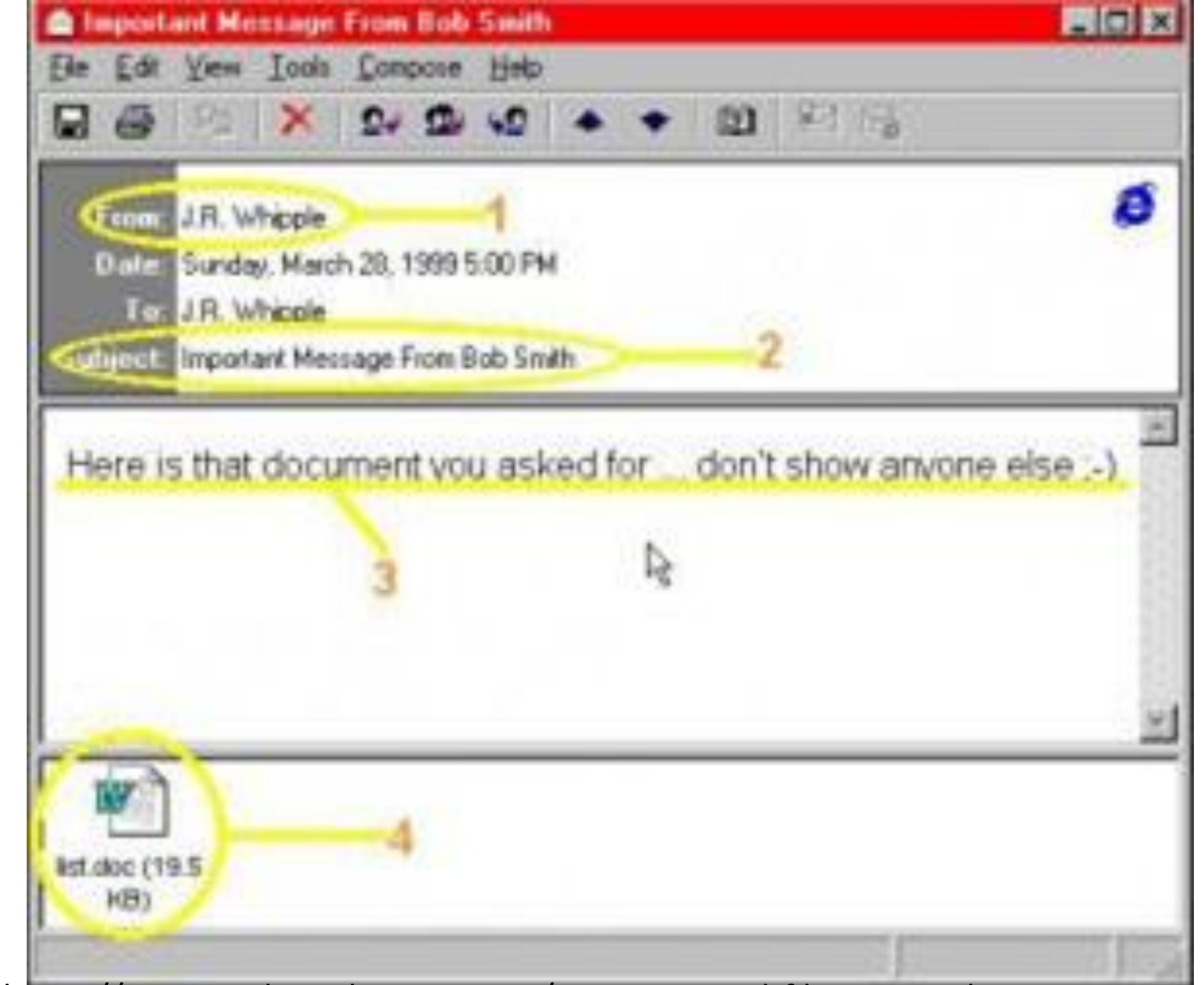
Nasıl Bulaşır?

- Virüsler, çeşitli yollarla bulaşabilirler. Bunlar arasında e-posta ekleri, kötü amaçlı web siteleri, yazılım güncellemeleri veya zararlı programların yasadışı kopyaları bulunabilir.

VİRÜS ÖRNEKLERİ



KAYNAK: <https://www.escapistmagazine.com/8-deadly-computer-viruses-that-shook-the-world/>



KAYNAK: <https://www.maketecheasier.com/2-unexpected-file-types-where-computer-viruses-can-exist/>

1. ILOVEYOU Virüsü (2000)
2. Melissa Virüsü (1999)
3. Conficker Worm (2008)
4. Stuxnet Worm (2010)
5. Sasser Worm (2004)

2- WORM (SOLUCANLAR)

- Worm (Solucan), bilgisayar ağlarında hızla yayılan ve çoğalan, zararlı bir yazılım türüdür.
- Bir Worm, bir bilgisayar ağı veya cihaz içindeki diğer cihazlara kendini kopyalayabilen bir zararlı yazılımdır.
- Worm'ler, kendilerini çoğaltarak hızla yayılır ve genellikle bilgisayar sistemlerine zarar verirler.

Nasıl Bulaşır?

- Worm'ler, genellikle bilgisayar ağlarında veya internet üzerindeki güvenlik açıklarını kullanarak yayılırlar.
- İnfekte edilmiş bir cihazdan diğer cihazlara otomatik olarak kopyalanabilirler.
- E-posta eklentileri veya indirilebilir dosyalar gibi bulaştırma yöntemleri de kullanılabilir.



KAYNAK: <https://bkhost.vn/blog/worm-sau-may-tinh/>

WORM ÖRNEKLERİ

```
COUNTRY.S S    COUNTRY.TXT    DEBUG.EXE    EDIT.COM    EXPAND.
FDISK.EXEY    FORMAT.OM    KEYB.COM    KEYBOARD.SYS    MEM.EXEEXE
NETWORKS.X    NLSFUNCCE    OS2.TXT    QBASIC.EXE    README.T
SCANDISK.X    SYS.COM.E    XCOPY.EXE    CHOICE.C M    DEFRAG.EXT
DEFRAG.H T    DELOLDOS.E E    DOSHELP.HLP    EGA.CPI O    EGA2.CPIXE
EGA3.CPI E T    EMM386.EXE    KEYBRD2. YS    MSCDEX.E E    SCANDISK.INI
ANSI.SYSLP E    APPEND.E E    CHKSTATESSYS    DBLWIN.H    DELTREE.EXE
DISKCOMP. O    DISKCO M    DISPLAY.Y    DOSKEY. X    DRUSPACE EX
DRUSPACE.CL    DRUSPAPYX F    DRUSPACE S    MSD.EXECLP    REPL CE..XEE
STORE. H    HELP.HCE.C    DRIVER.SS S    EDIT.HLPOM    FAST ELPE X
STOPENEXE    FC.EXELP X    FIND.EXE.SYS    GRAPHICS COM    GR P I S
LP. OM.EX    HIMEM.SY.IO    INTERLNKYE E    I TER UR. XE    L . X
READF X C M    E MAKERS NE    MEMMAKER    M MMA ER N    M C M
FA OU B OM    E.COM.E    MOVE E H    OO L    P . X
HE C 3    DR UE.S S    SE E E    E    S E
LO I L 6P    R N.E E    M H
MON M X    O .C M    F X
QBASIC.    U B    O 6
SMARTDR. I ( M    X4,300    .    .    A H C .
TREE.CO. M M    Y9 0 4    TVER .    N S    ABEL E .
COMMANDH ROR X    ARTMXEX    E K .    ODE. O E
C:\DOS>U 8 SAM I T O    INTD.N.    MST LS..    OWER E E
C:\DOS>M.P E UMA TMac. M    S NFIG038 L    SHAR .EXDE    IZER.EXEE
C:\DOS>.CEME ANFORME3,01    Ubytes.UMBLP    SORT.EXEEI    UBST.EXEPRO
C:\DOS>930fi e s)UTOEX30,84 , 2 Cbytes.freeP    PRINT.EXEL F    UNDELETE.EXE
```

KAYNAK: <https://bestantivirus.com/blog/what-is-a-file-injector-virus.html>

MyDoom Virus

Type: Computer worm

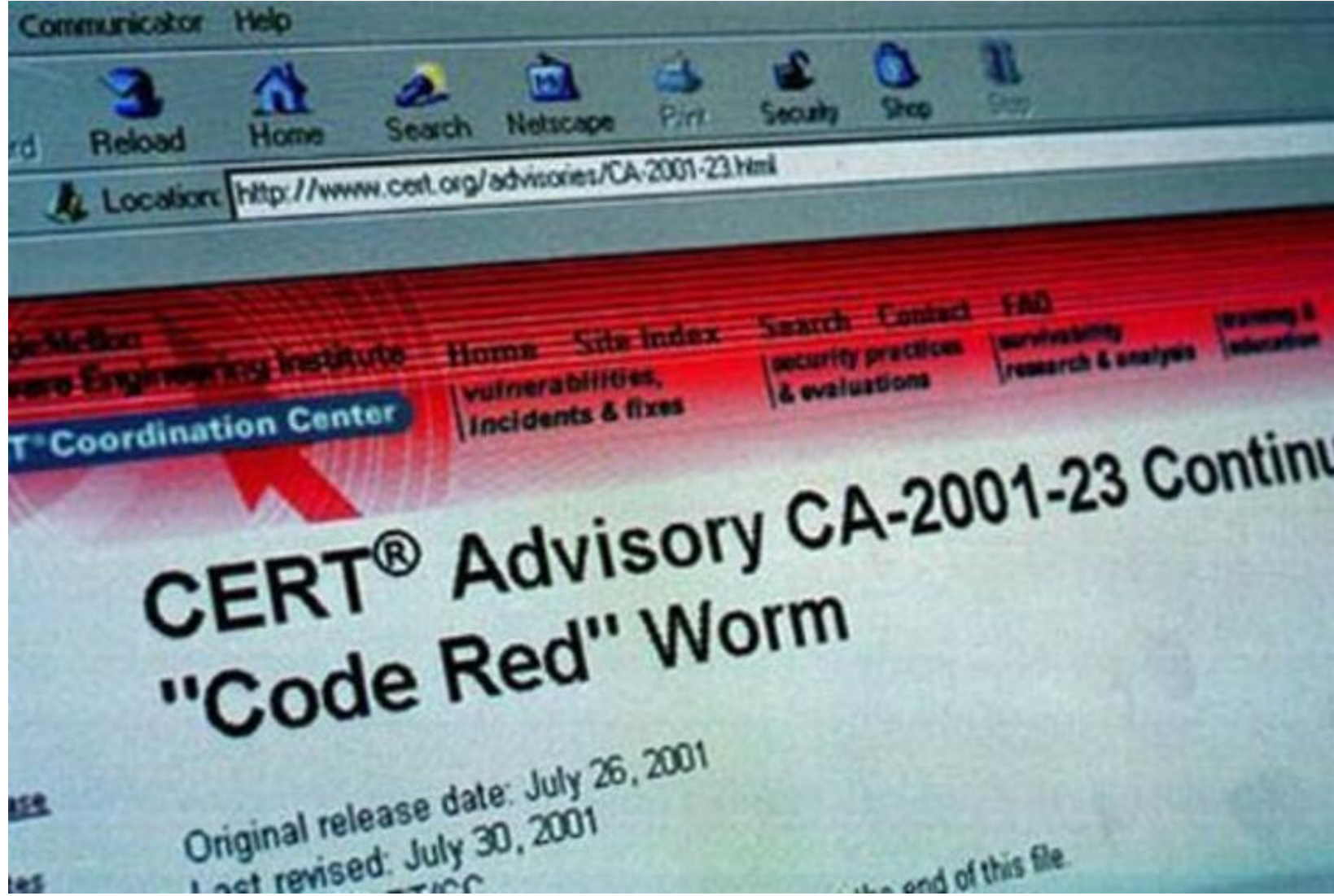
Creator: Unknown (named by Craig Schumgar)

Point of Origin: Russia - January 2004

Infected Users: 25% of global emails (at the time)

Estimated Damage: US\$ 38 billion

KAYNAK: <https://pbs.twimg.com/media/EZL1-BUXkAlIX7k?format=jpg&name=4096x4096>



KAYNAK: <https://tipsmake.com/what-is-virus-code-red-how-to-remove-like>

1. Blaster (MSBlast veya MS32.Blaster)
2. Conficker (Downadup)
3. Mydoom
4. Sasser
5. Code Red

3- SPYWARE (CASUS YAZILIM)

- Spyware (Casus Yazılım), kullanıcının bilgisayarını veya diğer cihazlarını izlemek, bilgi toplamak ve genellikle izinsiz olarak kişisel bilgileri çalmak amacıyla tasarlanmış zararlı yazılımlardır.
- Spyware, kullanıcının bilgisayar aktivitelerini izleyen ve toplayan bir yazılım türüdür. Bu yazılım, genellikle kullanıcının izni olmadan veya farkında olmadan kurulur.
- Spyware, kullanıcının gezdiği web sitelerini, klavye girişlerini, e-posta adreslerini, parolaları ve diğer kişisel bilgileri kaydedebilir.

Nasıl Bulaşır?

- Spyware, genellikle ücretsiz yazılımların veya uygulamaların içine gizlenmiş olarak gelir. Kullanıcılar bu yazılımları indirip kurduklarında spyware de sistemlerine bulaşır.
- Bazı web siteleri, zararlı pop-up reklamlar aracılığıyla da spyware bulaştırabilir.



KAYNAK: <https://www.fortinet.com/de/resources/cyberglossary/spyware>

SPYWARE ÖRNEKLERİ

HOW KEYLOGGING WORKS



KAYNAK: <https://vpnoverview.com/internet-safety/malware/keyloggers/>



KAYNAK: <https://techgator.in/what-is-browser-hijacking/>

1. Adware (Reklam Destekli Yazılım)
2. Keyloggers (Tuş Kaydediciler)
3. Trojan Horses (Truva Atları)
4. Web Browser Hijackers (Tarayıcı Kaçıranlar)
5. Mobile Spyware (Mobil Casus Yazılım)

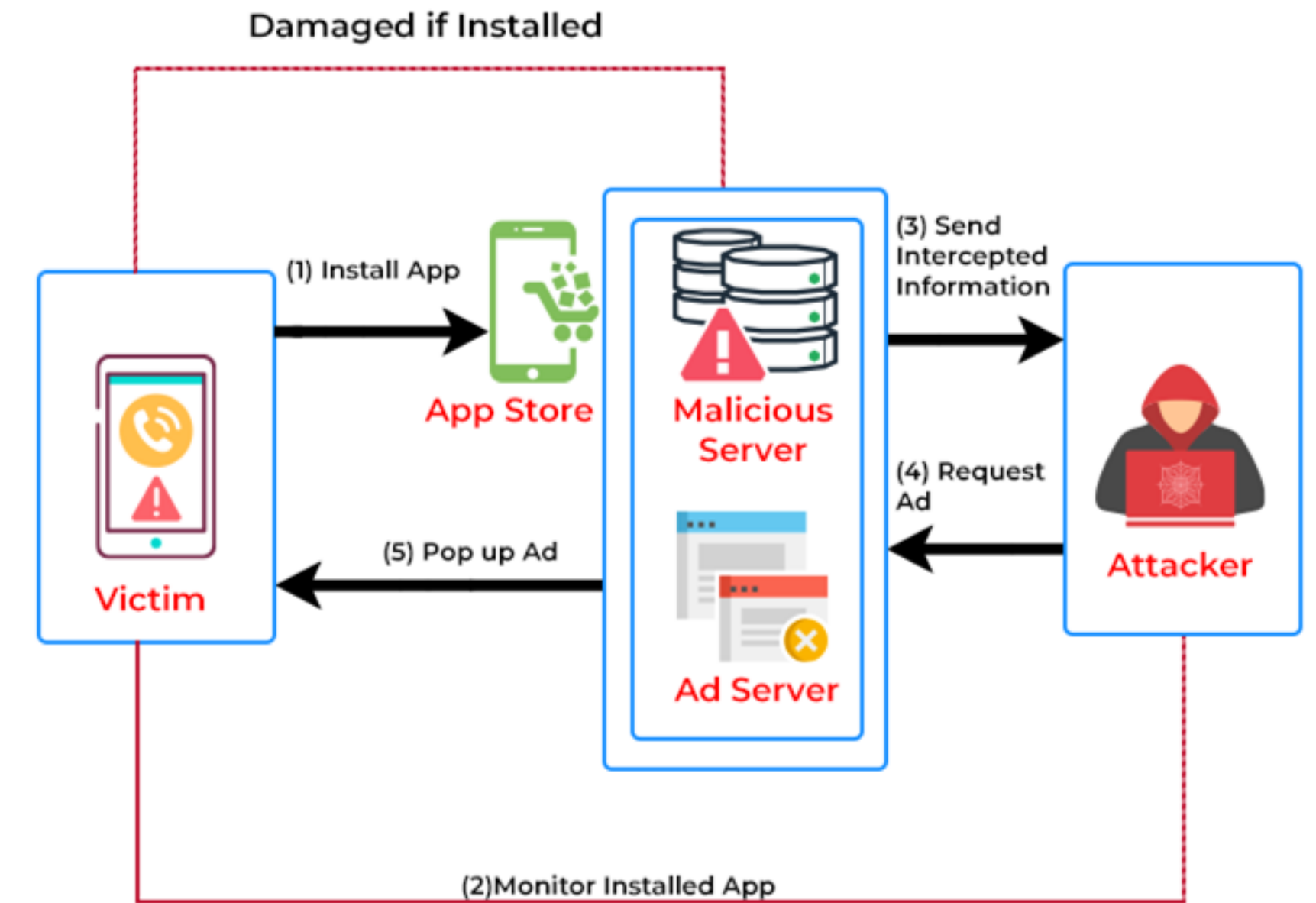
4- ADWARE(REKLAM YAZILIMI)

- Adware, "advertising-supported software" ifadesinin kısaltmasıdır ve reklam destekli yazılım anlamına gelir.
- Temel amacı, kullanıcının internet tarayıcısına veya bilgisayarına istenmeyen reklamlar eklemek ve bu reklamlar aracılığıyla gelir elde etmektir.
- Adware genellikle ücretsiz yazılımların veya uygulamaların bir parçası olarak bilgisayara bulaşır.

Nasıl Bulaşır?

- Adware, genellikle ücretsiz yazılımların veya uygulamaların içine gizlenmiş olarak gelir. Kullanıcılar bu yazılımları indirip kurduğunda adware de sisteme bulaşır.
- Bazı web siteleri, zararlı pop-up reklamlar aracılığıyla da adware bulaştırabilir.

HOW ADWARE WORKS

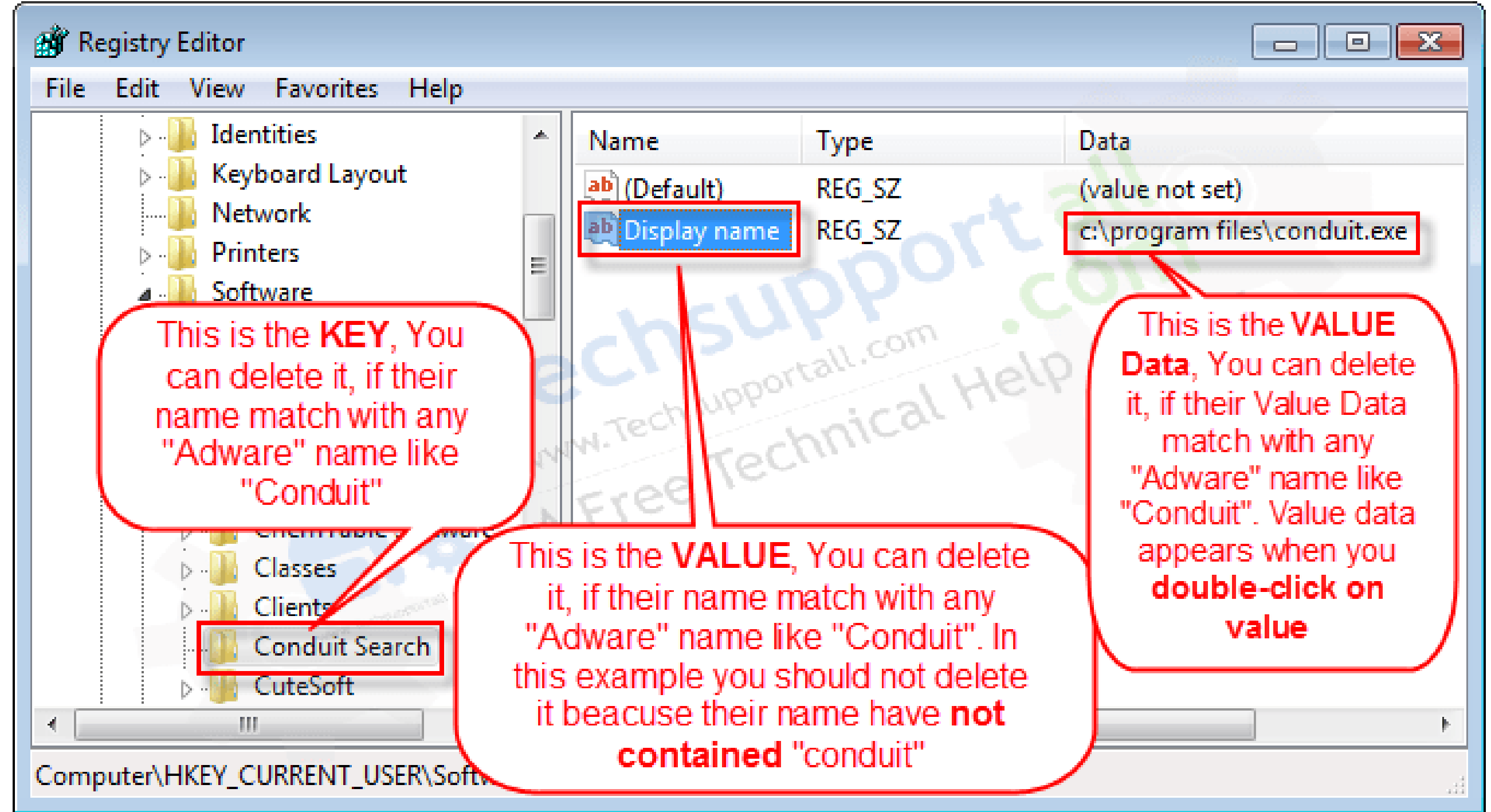


KAYNAK: <https://www.spiceworks.com/it-security/security-general/articles/what-is-adware/>

ADWARE ÖRNEKLERİ



KAYNAK: <https://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl/>

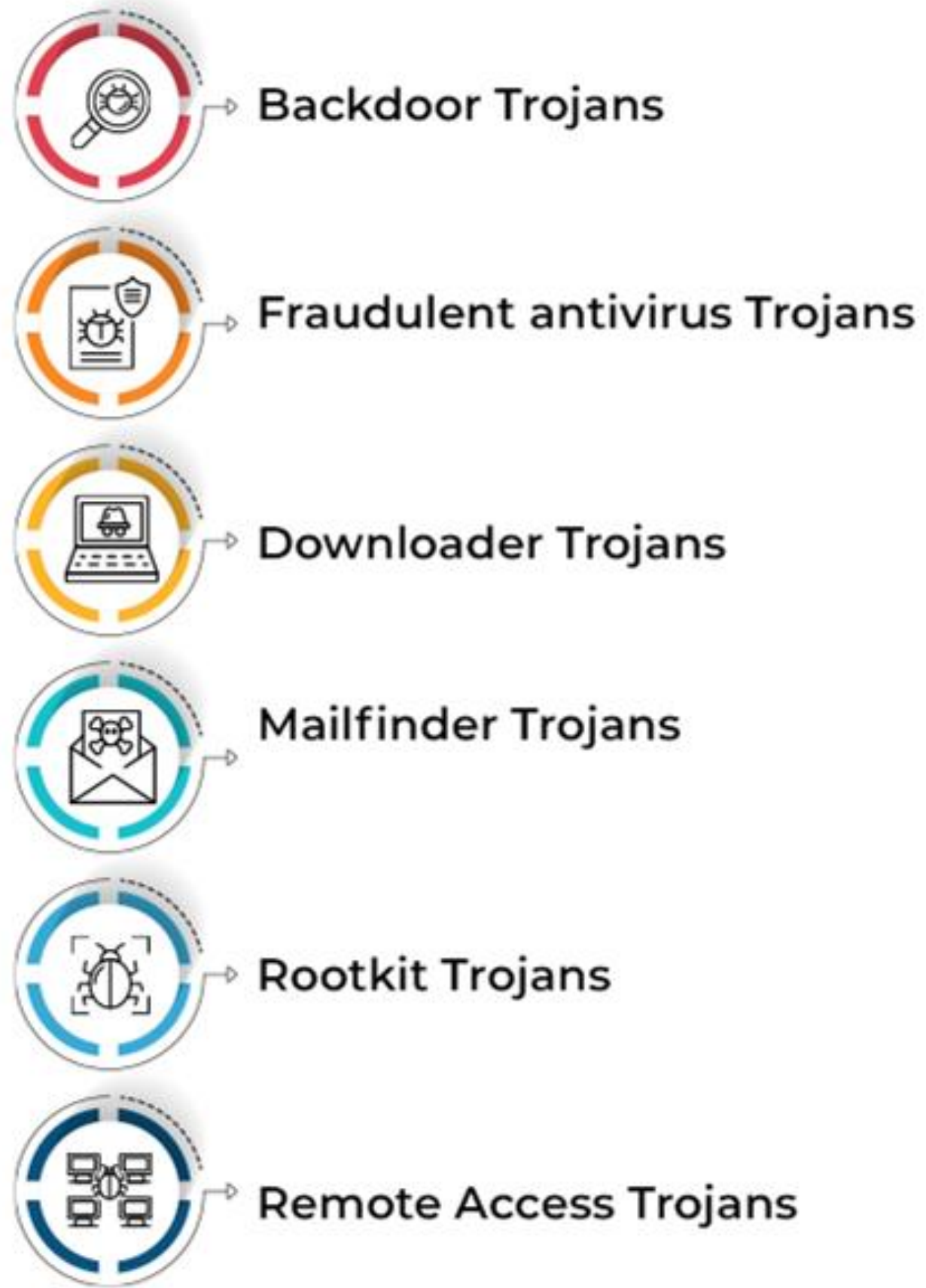


KAYNAK: <https://www.techsupportall.com/how-to-remove-safesurfs-com-homepage-removal-help/>

1. Superfish
2. MyWebSearch
3. Conduit Toolbar
4. Genieo

5- TROJAN (TRUVA ATI)

EXAMPLES OF TROJAN HORSE VIRUS

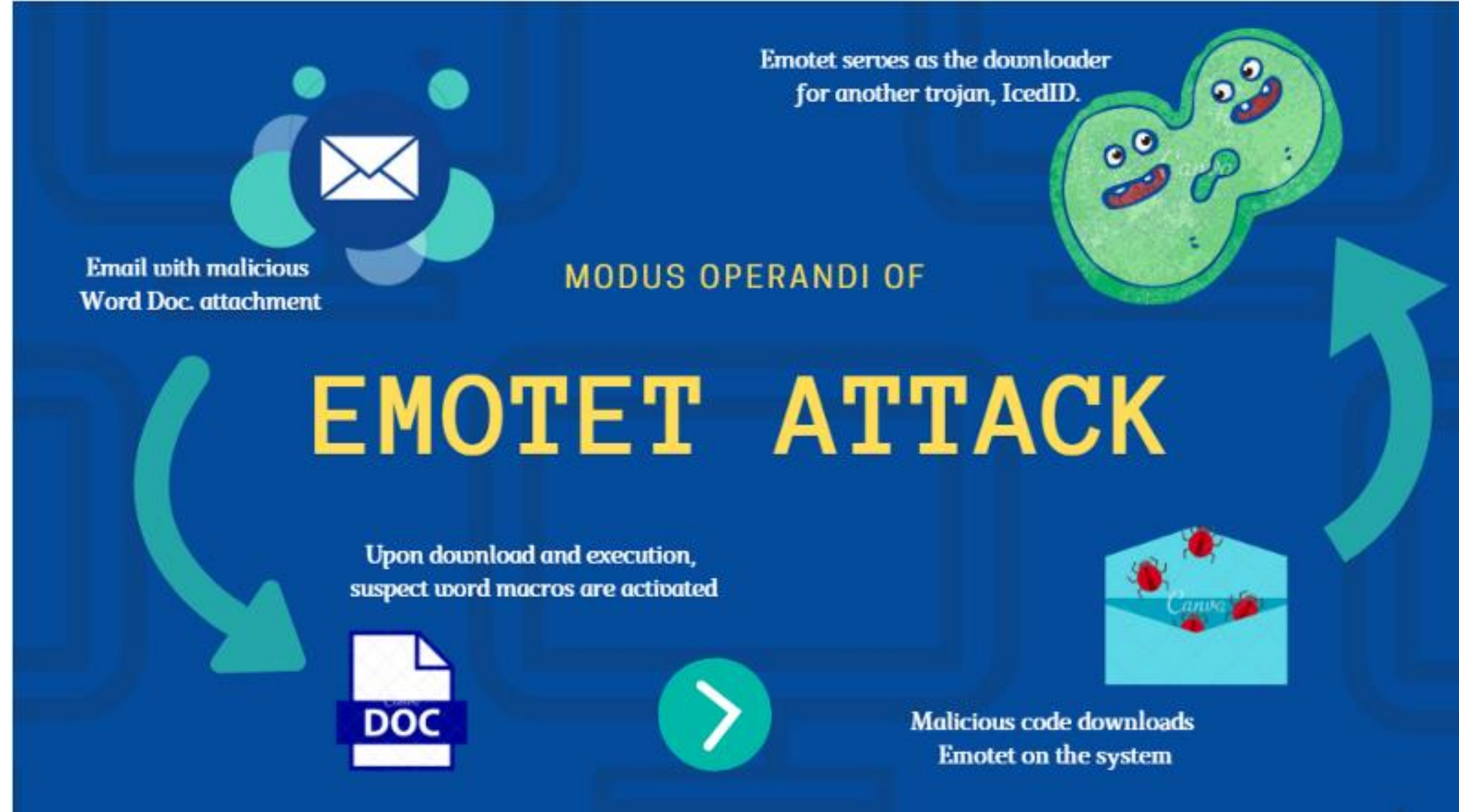


- Trojan (Truva Atı), görünüşte zararsız veya yararlı bir program veya dosya gibi davranarak, kullanıcının bilgisayarına kötü amaçlı yazılım bulaştırmak için tasarlanmış bir tür zararlı yazılımdır.
- Görünüşte zararsız bir program veya dosya gibi davranır, bu nedenle kullanıcılar tarafından kolayca kurulabilir.
- Amaçları, bilgisayara kötü amaçlı yazılım, casus yazılım veya diğer zararlı işlevleri yüklemektir.

Nasıl Bulaşır?

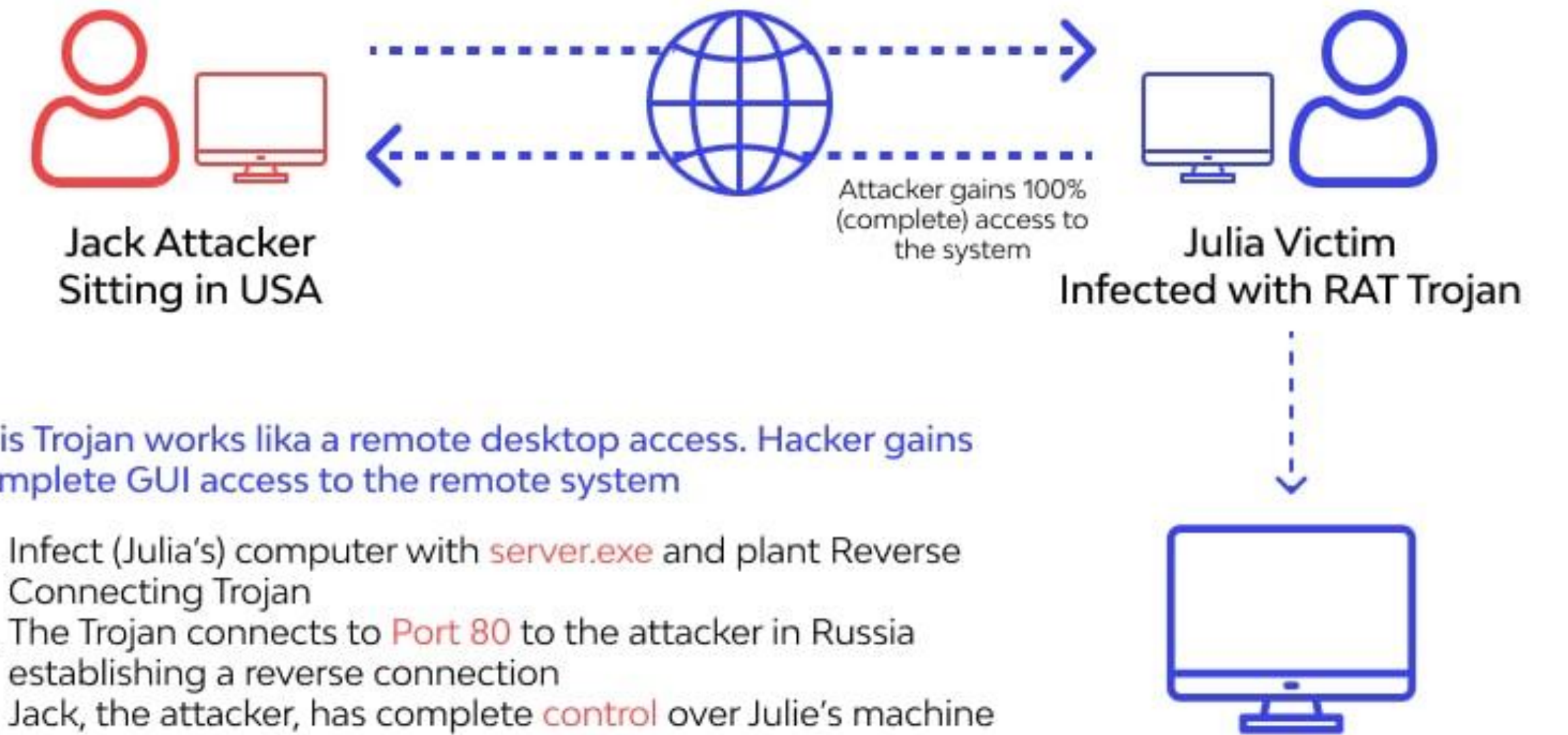
- Trojanlar, genellikle bilgisayar kullanıcılarına güvenilir ve çekici görünen e-posta ekleri, indirilebilir dosyalar veya uygulamalar aracılığıyla bulaştırılır.
- Kullanıcılar, bu dosyaları veya uygulamaları indirip açtıklarında Trojan bilgisayarlarına bulaşır.

TROJAN ÖRNEKLERİ



KAYNAK: <https://www.riskcompliance.biz/news/worlds-most-dangerous-malware-emotet-disrupted-through-global-action/>

Remote Access Trojans



KAYNAK: <https://www.thetechadvocate.org/how-to-prevent-remote-access-trojan-attacks-and-stay-in-control-of-your-pc/>

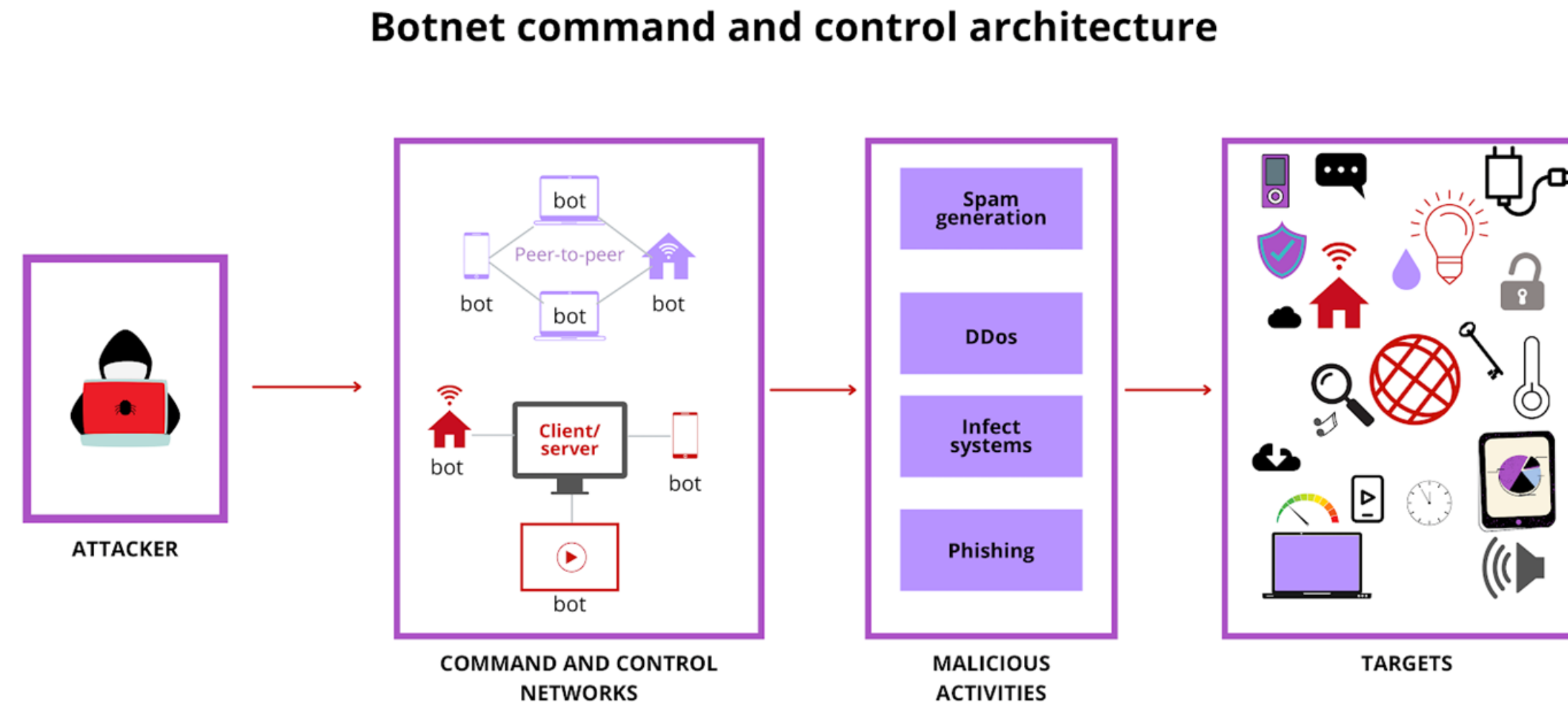
1. Zeus Trojan
2. DarkTequila
3. Emotet
4. RAT (Remote Access Trojan)
5. CryptoLocker

6- BOTNETS

- Bot terimi robotun kısaltmasıdır.
- Amacı, bilgisayarınızı bir bot'a (zombi olarak da bilinir) çevirebilen kötü amaçlı yazılımları dağıtmaktır. Böyle bir durumda bilgisayarınızı, sizin haberiniz olmadan internet üzerinden otomatik görevleri gerçekleştirebilir.

Nasıl Bulaşır?

- Botnetler, bilgisayarlara veya cihazlara bulaşmak için genellikle kötü amaçlı e-posta ekleri, bulaşmış web siteleri, güvensiz uygulamalar veya diğer kötü niyetli yazılımlar aracılığıyla yayılırlar.
- Kullanıcılar, bu bulaşmış dosyaları veya bağlantıları açtıklarında botnet bilgisayarlarına bulaşabilir.



 **WANTED
BY THE FBI**

**EVGENIY MIKHAILOVICH
BOGACHEV**

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

The diagram illustrates the Botnet Attack Process, showing the flow of commands and data between various components. A legend defines the color-coding for the actions:

- Scan:** Green arrow
- Infection:** Orange arrow
- Control:** Blue arrow
- Attack:** Red arrow

The process involves the following steps and components:

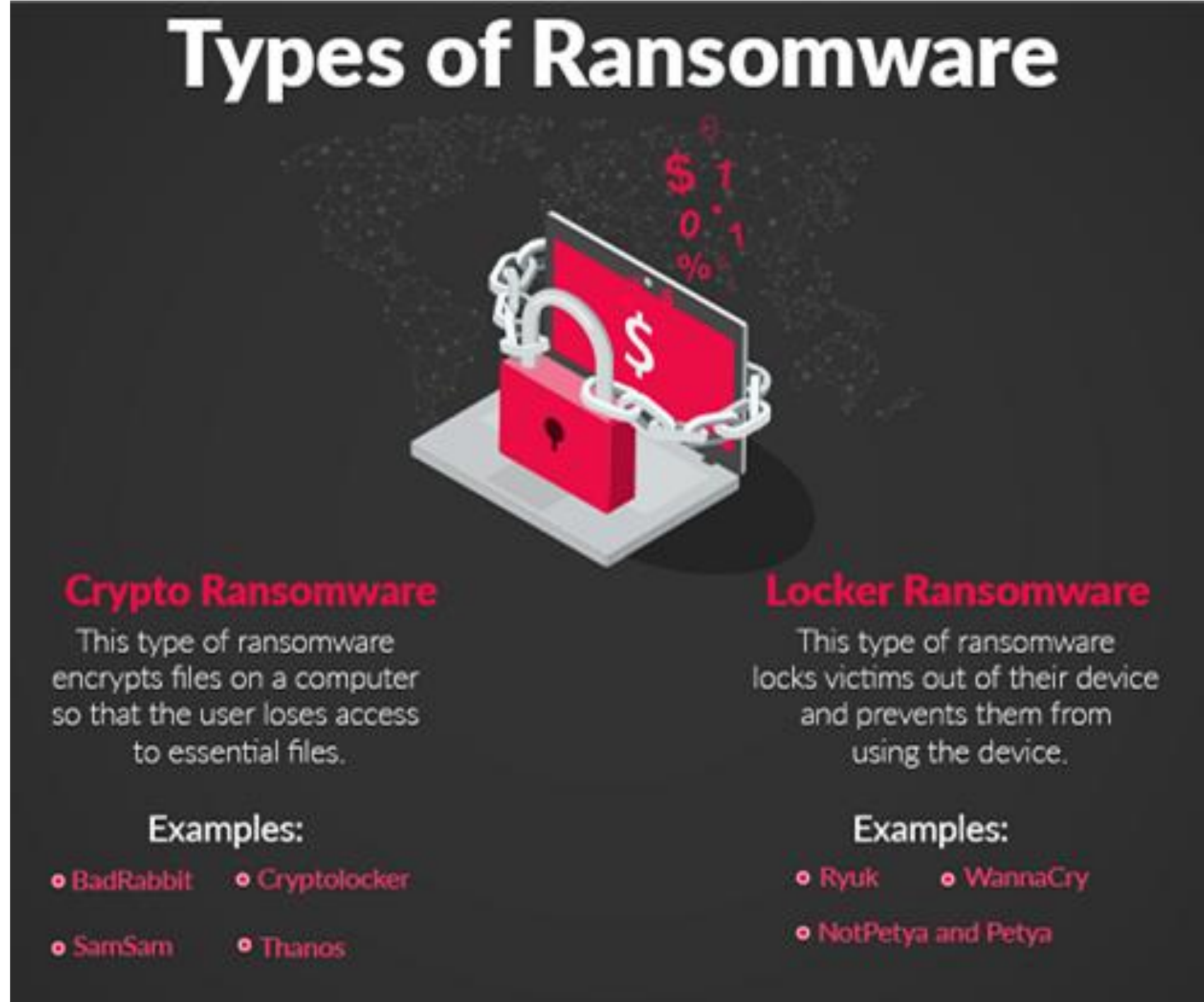
- Bot Master:** Initiates the attack.
- Scan / Loader:** Receives the initial connection and performs scans.
- CnC (Command and Control):** The central hub for bot management.
- 1st IoT Bot, 2nd IoT Bot, 3rd IoT Bot:** The infected devices used for scanning and attacking.
- Target:** The destination of the DDoS attack.

The sequence of actions is as follows:

- 1. Connect:** Bot Master connects to Scan / Loader.
- 2. Telnet Scan:** Scan / Loader scans the 1st IoT Bot.
- 3. Report IP:** 1st IoT Bot reports its IP to CnC.
- 4. Infect Command:** CnC sends an infect command to Scan / Loader.
- 5. Load Bot:** Scan / Loader loads the bot.
- 6. Attack Command:** CnC sends an attack command to 1st IoT Bot.
- 7. DDoS:** 1st IoT Bot performs a DDoS attack on the Target.
- 8. TelnetScan:** 1st IoT Bot scans the 2nd IoT Bot.
- 9. Report IP:** 2nd IoT Bot reports its IP to CnC.
- 10. Infect Command:** CnC sends an infect command to Scan / Loader.
- 11. Load Bot:** Scan / Loader loads the bot.
- 12. Attack Command:** CnC sends an attack command to 2nd IoT Bot.
- 13. DDoS:** 2nd IoT Bot performs a DDoS attack on the Target.
- 14. TelnetScan:** 2nd IoT Bot scans the 3rd IoT Bot.

1. Conficker
2. Mirai
3. Storm Worm
4. Gameover Zeus

7- RANSOMWARE(FİDYE YAZILIMI)



KAYNAK: <https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-a-ransomware-attack/>

- Ransomware, kötü amaçlı bir yazılım türüdür ve adını rehine verileri fidye karşılığında serbest bırakma eyleminden alır.
- Ransomware, dosyaları veya bilgisayarın tamamını şifreleyerek kullanıcının erişimini engeller.

Nasıl Bulaşır?

- Ransomware, genellikle sahte e-posta ekleri, kötü amaçlı web siteleri, güvensiz indirme kaynakları veya açıkları kullanarak bilgisayarlara bulaşır.
- Kullanıcılar, kötü amaçlı dosyaları veya bağlantıları açtıklarında ransomware bulaşabilir.

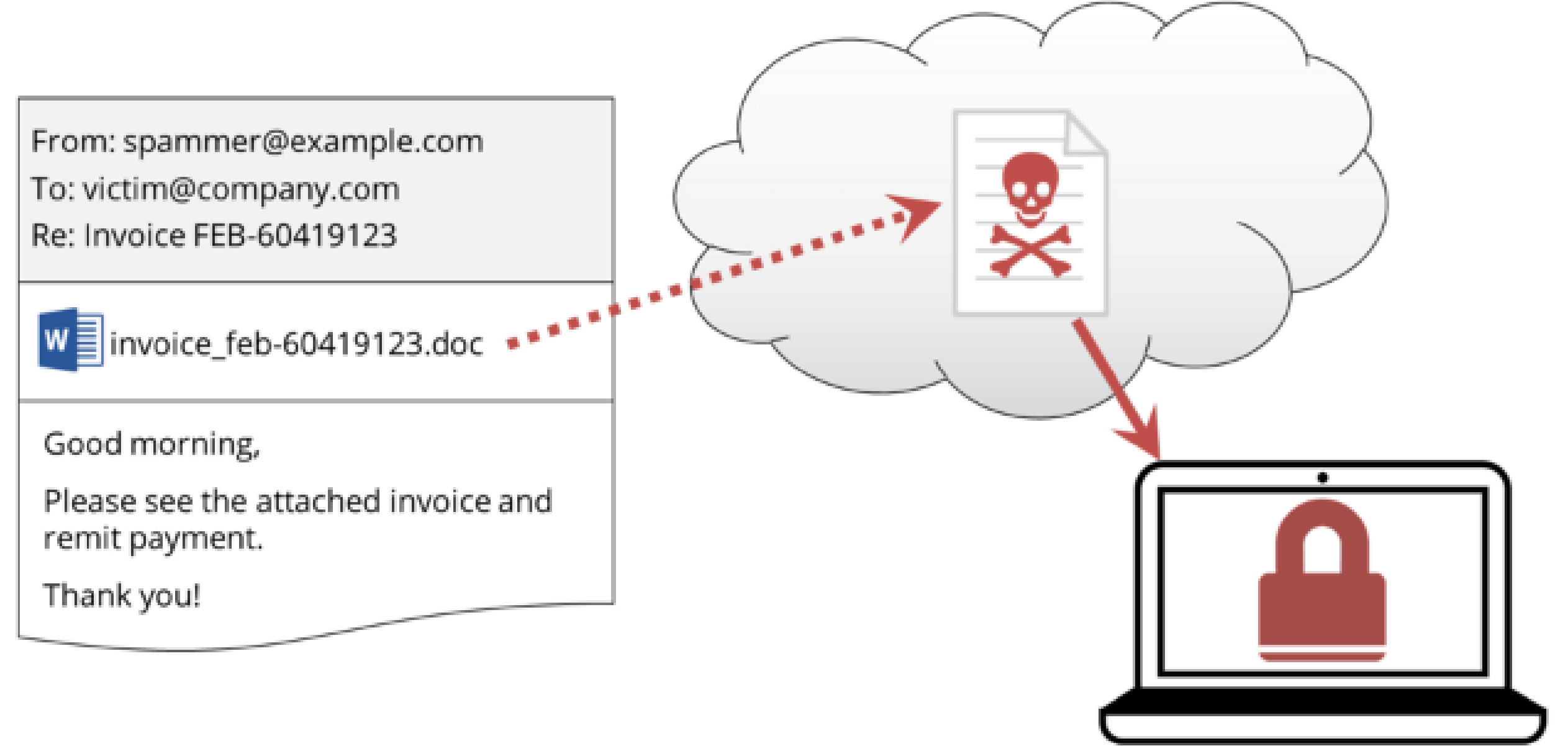
RANSOMWARE ÖRNEKLERİ

WannaCry Ransomware Attack

Name	: WannaCry, WannaCrypt, Wana Decrypt0r 2.0, WanaCrypt0r 2.0, and Wanna Decryptor.
Born	: May 12, 2017
Point of origin	: Pyongyang, North Korea
Invented by	: Lazarus Group (not confirmed)
Type of Attack	: Crypto-Ransomware
Subtype	: Ransomware
Operating Systems	: Microsoft Windows Affected
Outcome	: 300,000+ Computers Infected

KAYNAK: <https://www.ssl2buy.com/cybersecurity/wannacry-ransomware-attack>

Fake Invoice Email Installs Locky Ransomware



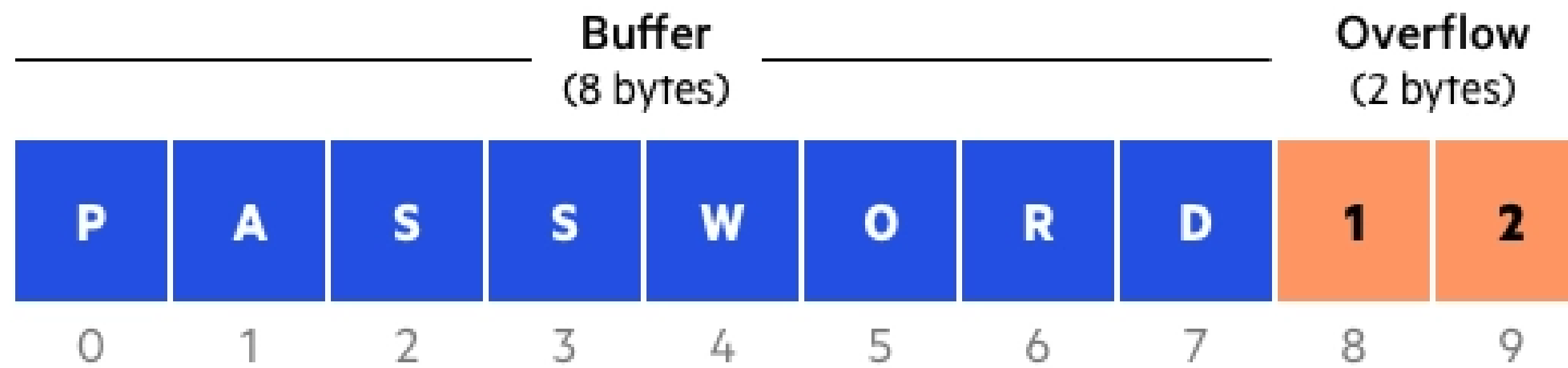
KAYNAK: <https://www.greenviewdata.com/blog/security/blocking-locky-ransomware-virus-update-and-tips>

1. WannaCry
2. Locky
3. CryptoLocker
4. Ryuk
5. NotPetya (Petya/ExPetr)

8. BUFFER OVERFLOW:

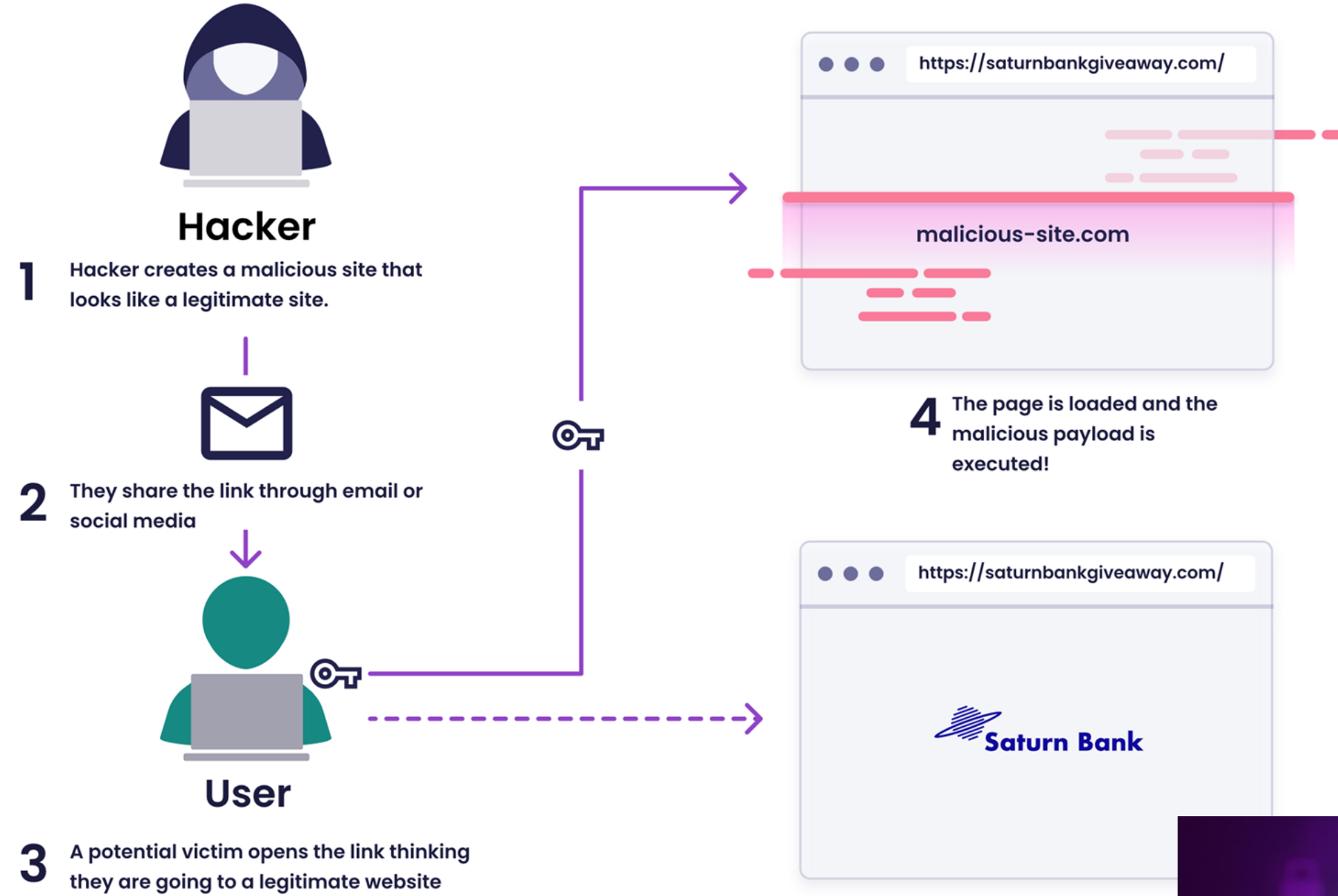


- Bir programın bellek alanının sınırlarının dışına çıkılarak kötü amaçlı kodların çalıştırılmasına izin veren bir güvenlik açığı.
- Örnek: Morris Worm, buffer overflow açığı kullanarak ilk büyük çaplı internet saldırısını gerçekleştirmiştir.



KAYNAK: <https://www.imperva.com/learn/application-security/buffer-overflow/>

9. CROSS-SITE REQUEST FORGERY (CSRF):

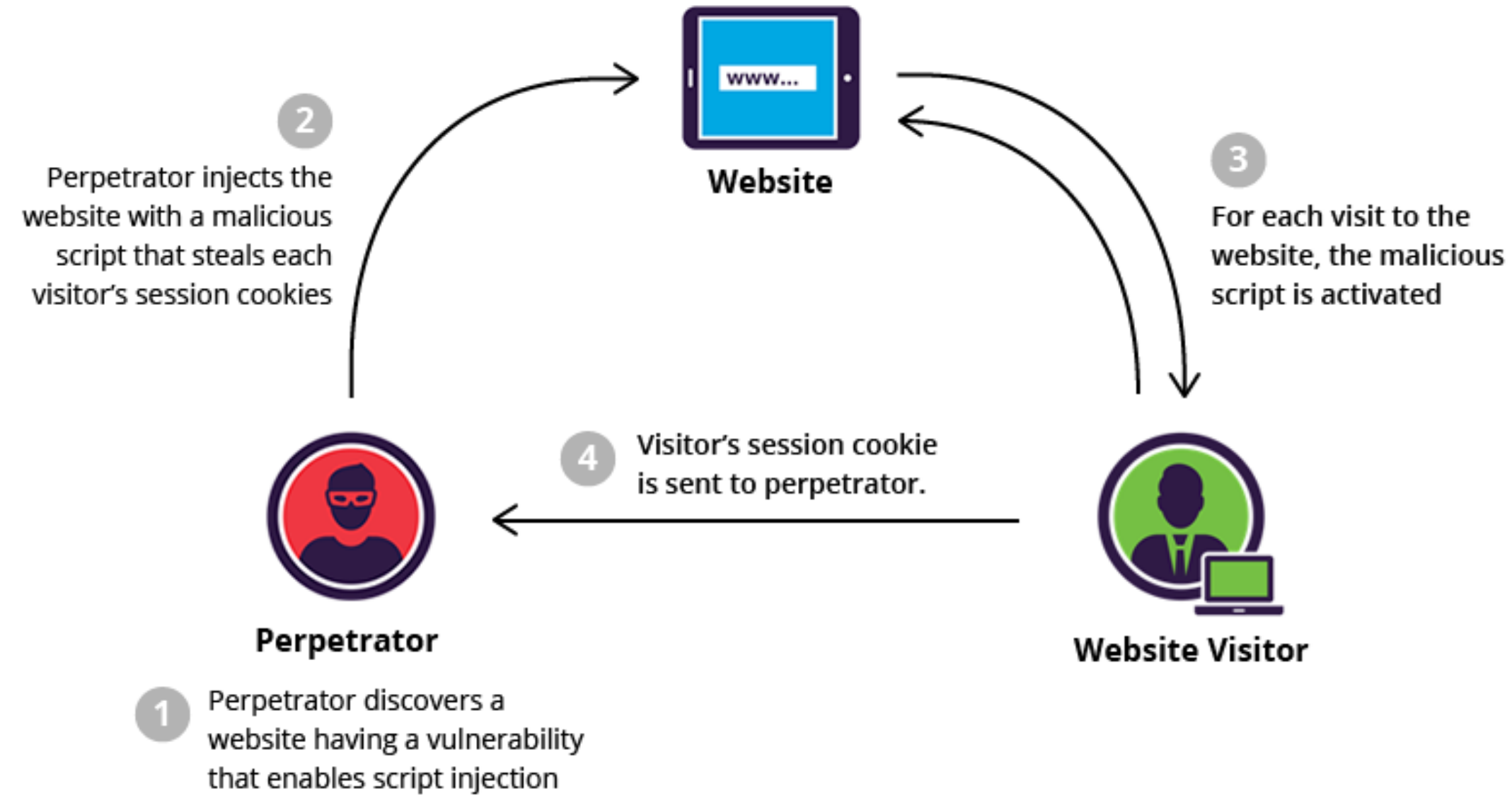


- Saldırganların kullanıcıların hesaplarını izinsiz olarak farklı bir web sitesi üzerinden işlem yapmaya zorladığı bir saldırı türü.
- Örnek: Bir saldırgan, kullanıcının banka hesabından para transferi yapmasını isteyen sahte bir web sayfası oluşturabilir.

KAYNAK: <https://learn.snyk.io/lesson/csrf-attack/>



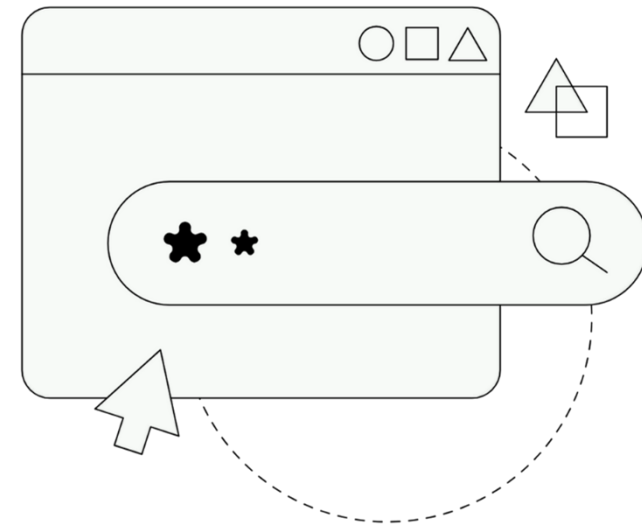
10. CROSS-SITE SCRIPTING (XSS):



- Saldırganların web sitelerine zararlı kodlar ekleyerek kullanıcıların tarayıcılarında çalışmasını sağladığı bir saldırı türü.

- Örnek: Bir saldırgan, kullanıcılara zararlı bir JavaScript kodu içeren sahte bir e-posta gönderebilir.

KAYNAK: <https://www.mobindustry.net/blog/11-web-application-security-best-practices-you-need-to-know/>



11. BROKEN ACCESS CONTROL:

Access Control Types

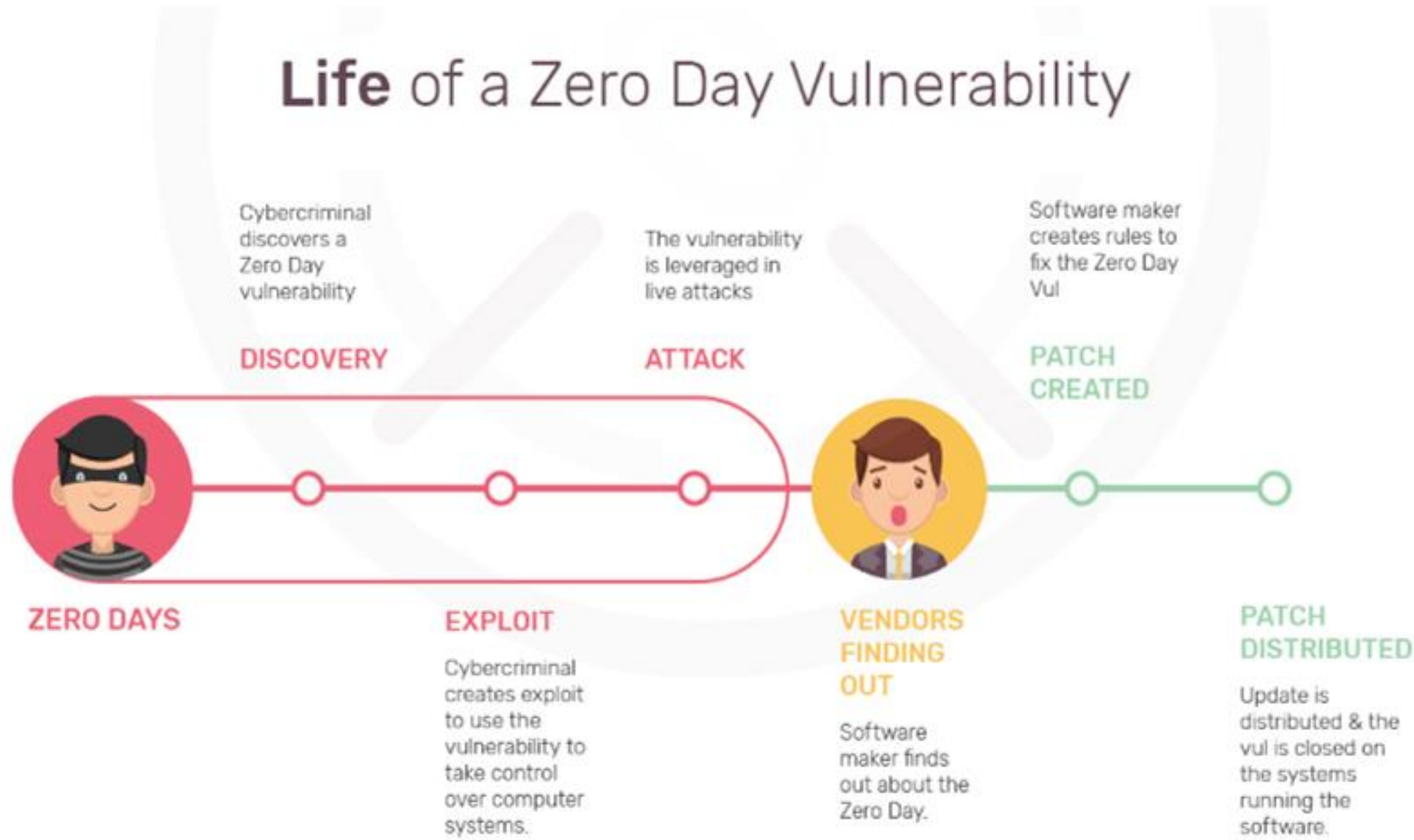


- Kullanıcıların izin verilmeyen kaynaklara veya işlevlere erişim sağlamasına izin veren bir güvenlik açığı.
- Örnek: Bir kullanıcının hesap ayarlarını değiştirmesi gereken bir işlevin, yetkisiz erişime açık olması.



KAYNAK: [https://medium.com/@cyber_kid12/day-83-cyber-chronicles-from-broken-access-control-to-risk-manAğement-revisited-2408008628c](https://medium.com/@cyber_kid12/day-83-cyber-chronicles-from-broken-access-control-to-risk-management-revisited-2408008628c)

12. ZERO-DAY EXPLOITS (0 DAYS):

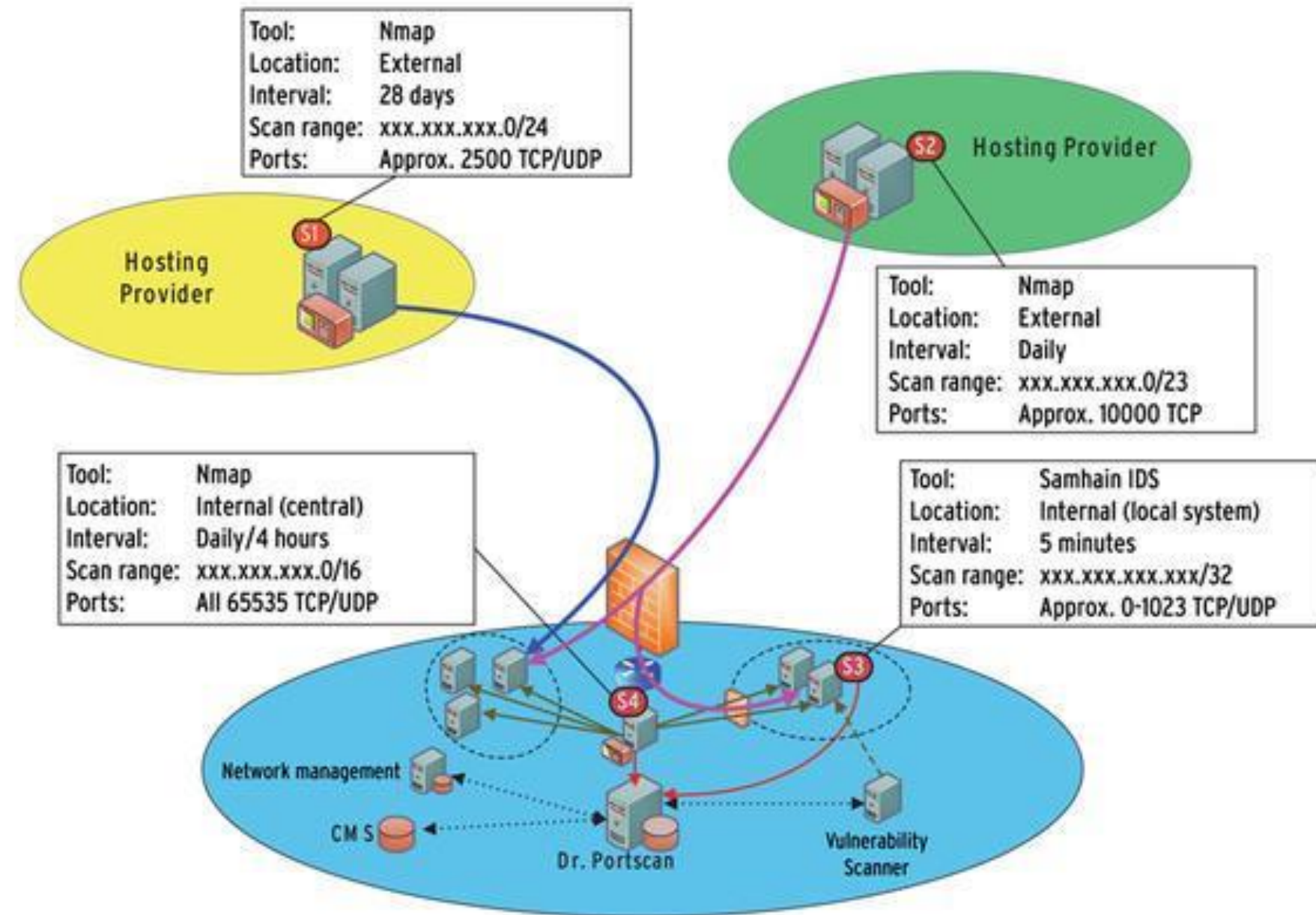


KAYNAK: <https://www.indusface.com/blog/prevent-zero-day-attacks/>

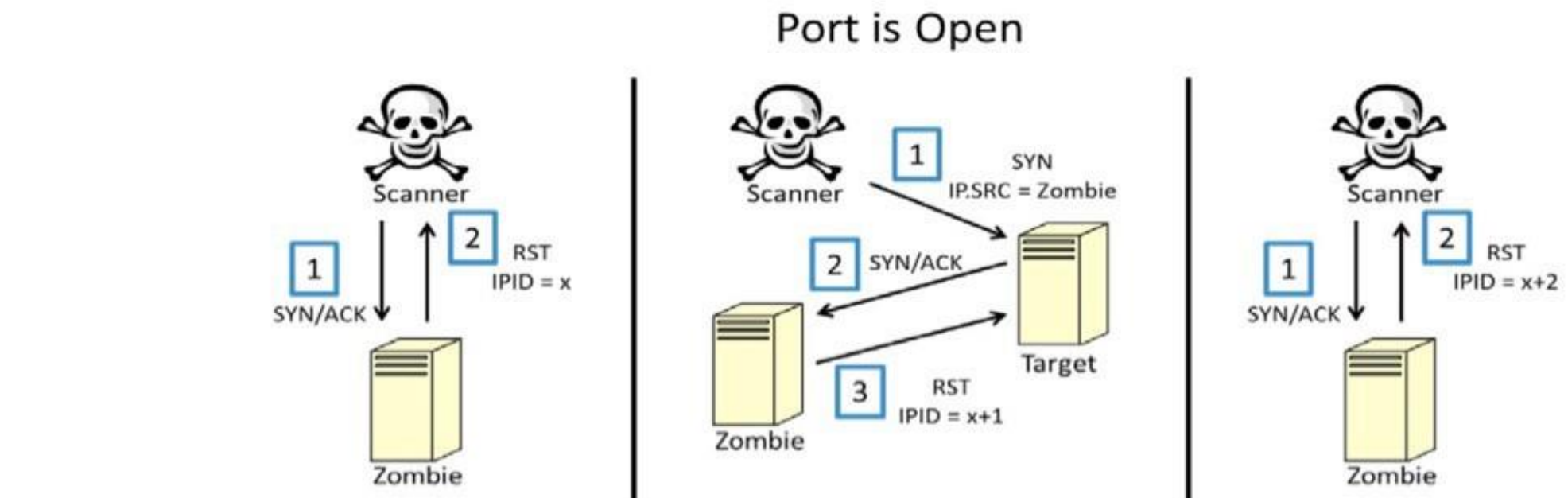
- Yazılım veya sistem güvenlik açıklarının keşfedildiği ve henüz üretici tarafından düzeltilmediği durumlar.
- Örnek: Saldırganlar, henüz açığı kapatılmamış bir yazılık veya işletim sistemi güvenlik açığından faydalanabilirler.

13. PORT CONFIGURATION HATALARI:

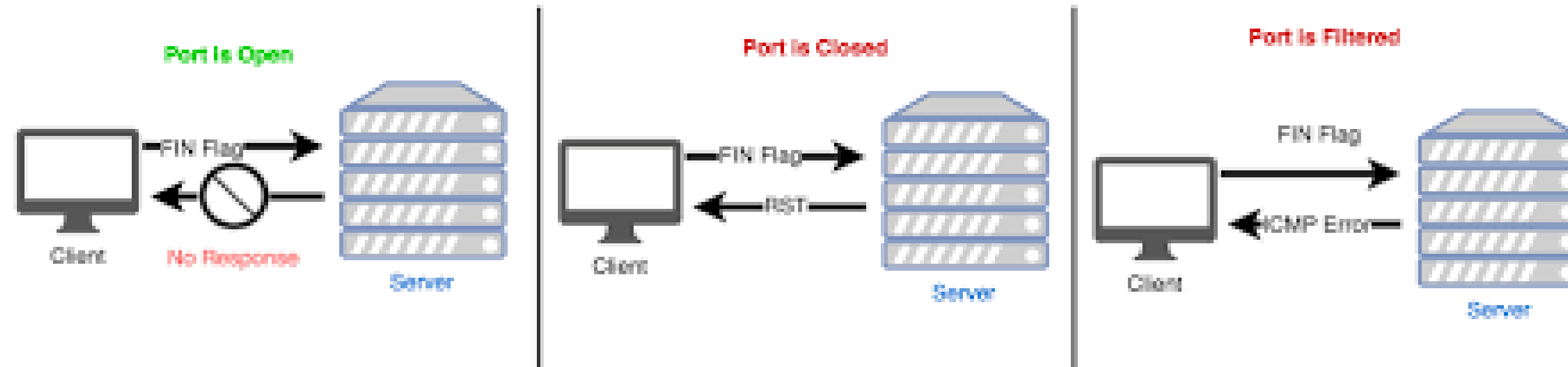
- Ağ cihazlarının yanlış yapılandırılması sonucu ağ güvenliğinin tehlikeye girmesi.
- Örnek: Açık bir ağ bağlantısı, yetkisiz erişimlere yol açabilir.



KAYNAK: <https://www.admin-maGazine.com/Articles/ManAging-Port-Scan-Results-with-Dr.-Portscan>

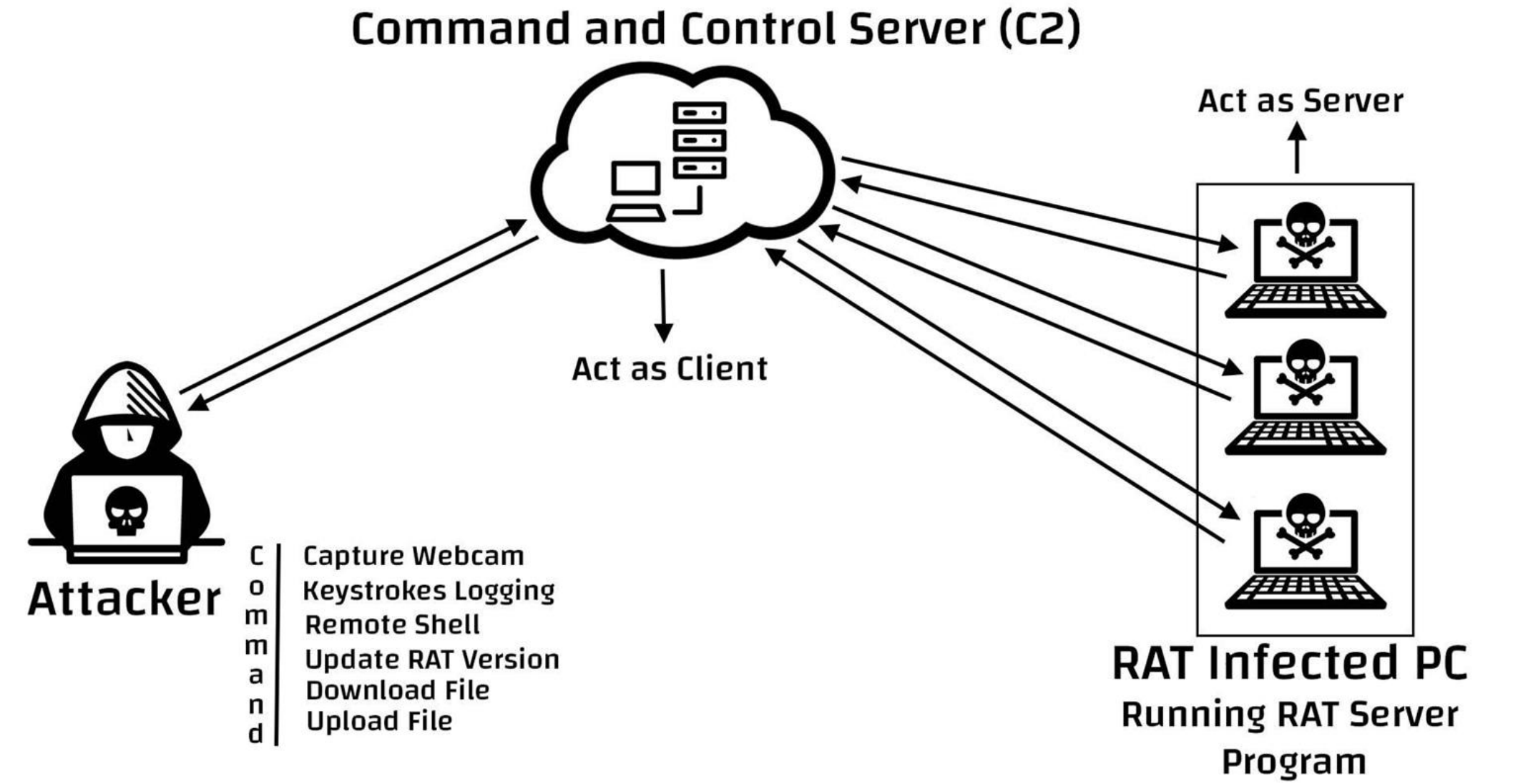
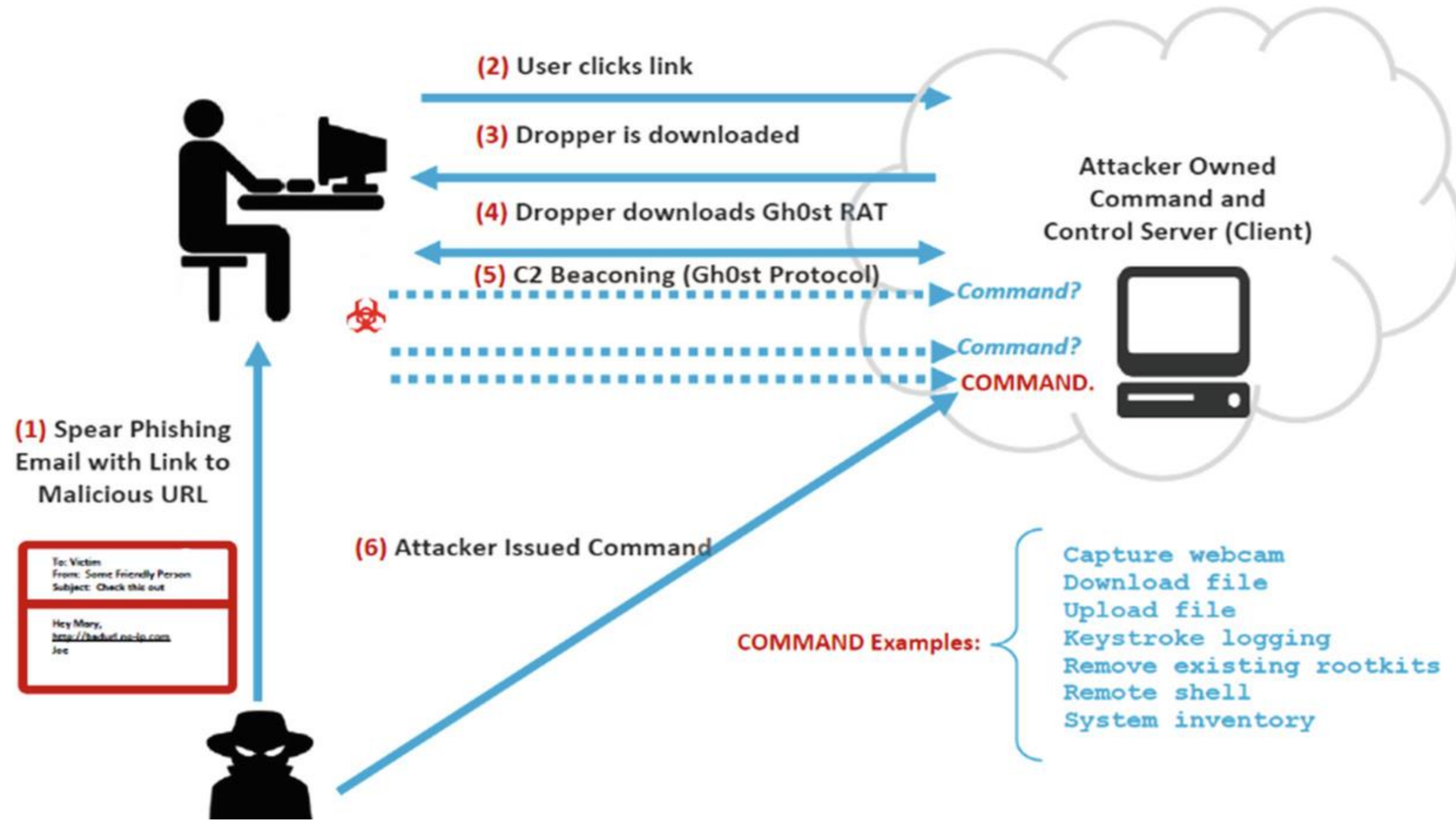


KAYNAK: <https://www.networkcomputing.com/network-security/port-scanning-techniques-introduction>



KAYNAK: <https://subscription.packtpub.com/book/security/9781784399771/6/ch06lv11sec34/fin-scanning>

14. RAT (REMOTE ACCESS TROJAN):

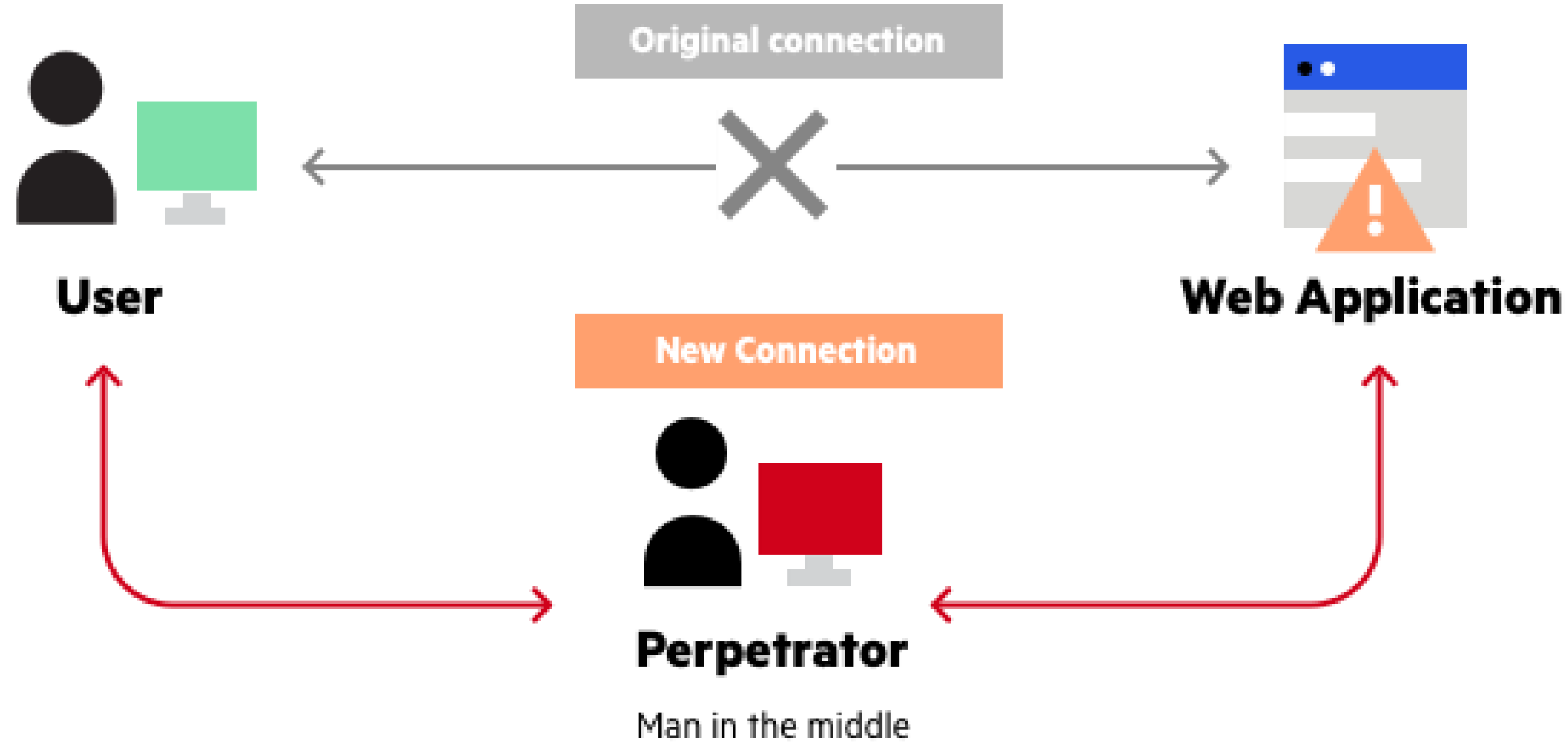


KAYNAK: <https://hackerterminal.com/what-is-remote-access-trojan/>

KAYNAK: <https://medium.com/codex/the-birth-and-rise-of-remote-access-trojans-rats-2819d7ab2b06>

- Saldırganların bir bilgisayar sistemine uzaktan erişim sağlamak amacıyla kullanılan truva atları.
- Örnek: Poison Ivy RAT, uzaktan bilgisayar kontrolü sağlayan bir RAT örneğidir.

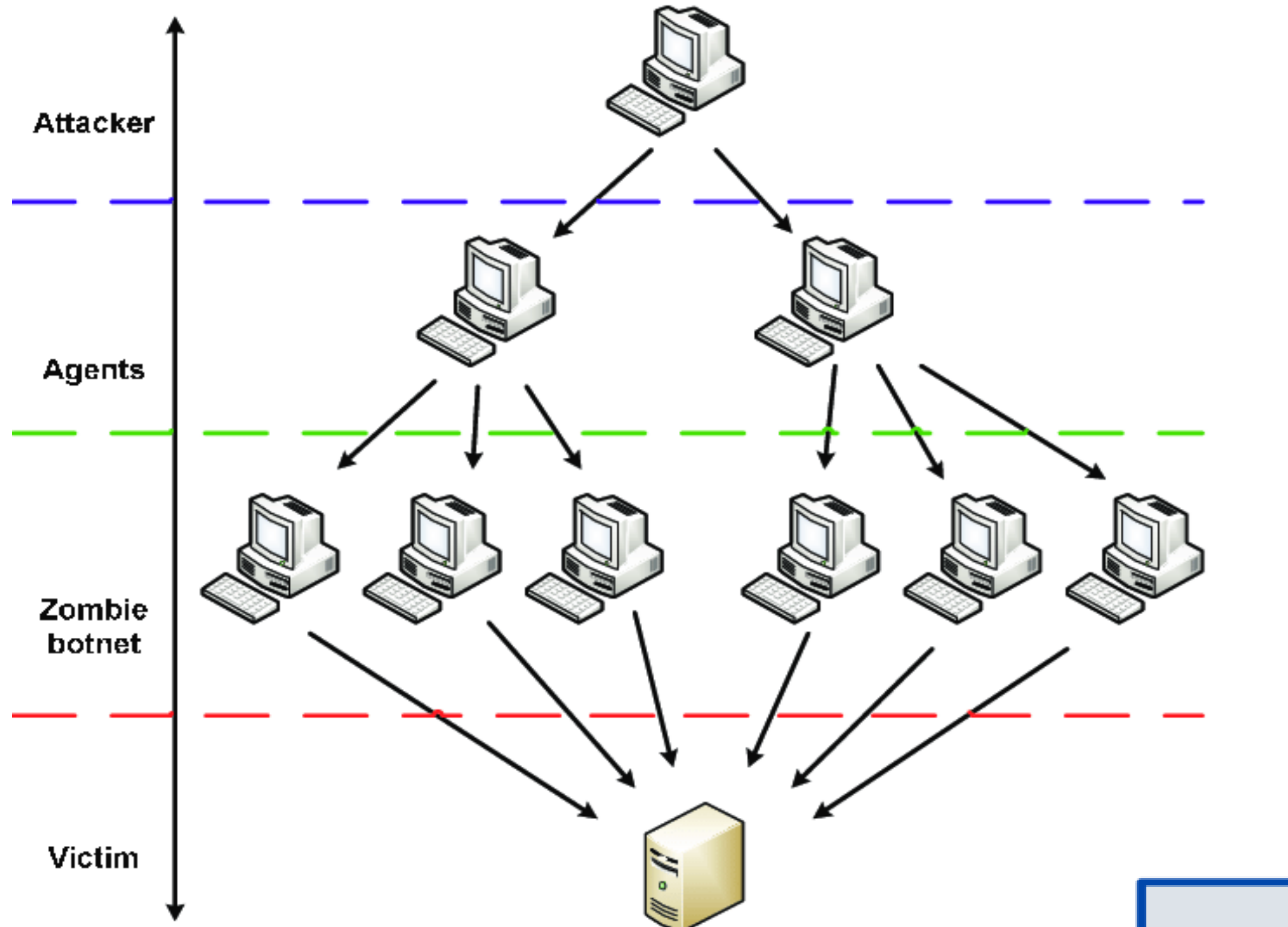
15. MAN-IN-THE-MIDDLE (MITM) SALDIRILARI:



KAYNAK: <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>

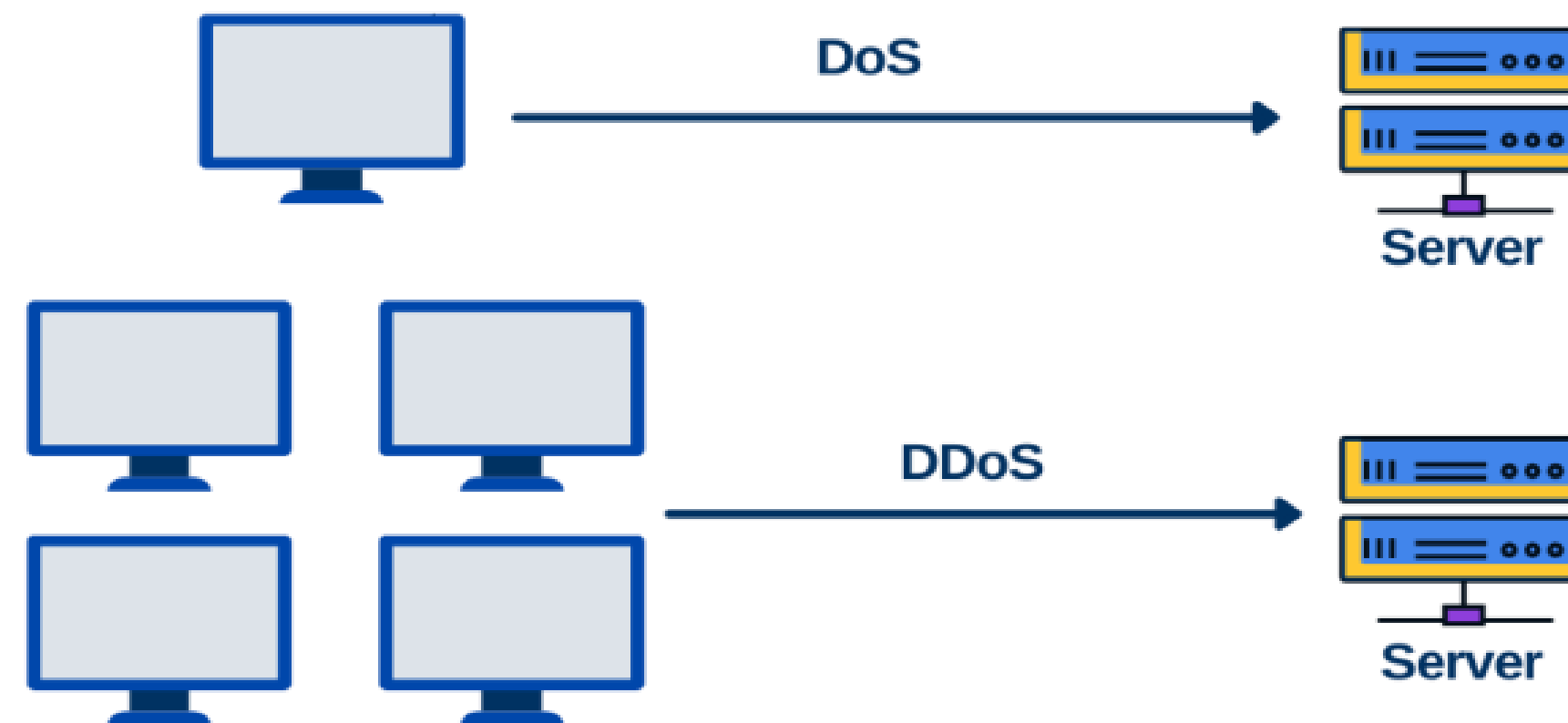
- Saldırganların iki iletişen tarafın arasına girerek iletileri izlemesine veya manipüle etmesine olanak tanıyan saldırı türü.
- Örnek: Bir kişi, halka açık bir Wi-Fi ağı üzerinden verileri izleyebilir veya değiştirebilir.

16. DENIAL-OF-SERVICE (DOS) SALDIRILARI:



KAYNAK: <https://www.globalsign.com/en/blog/10-cybersecurity-challenges-healthcare>

- Hedeflenen sistem veya ağı yoğun talep gönderilerek hizmetin kesilmesine neden olan saldırılar.
- Örnek: SYN Flood saldırısı, bir sunucunun hizmet veremeyecek kadar çok bağlantı isteği aldığı bir tür DOS saldırısıdır.



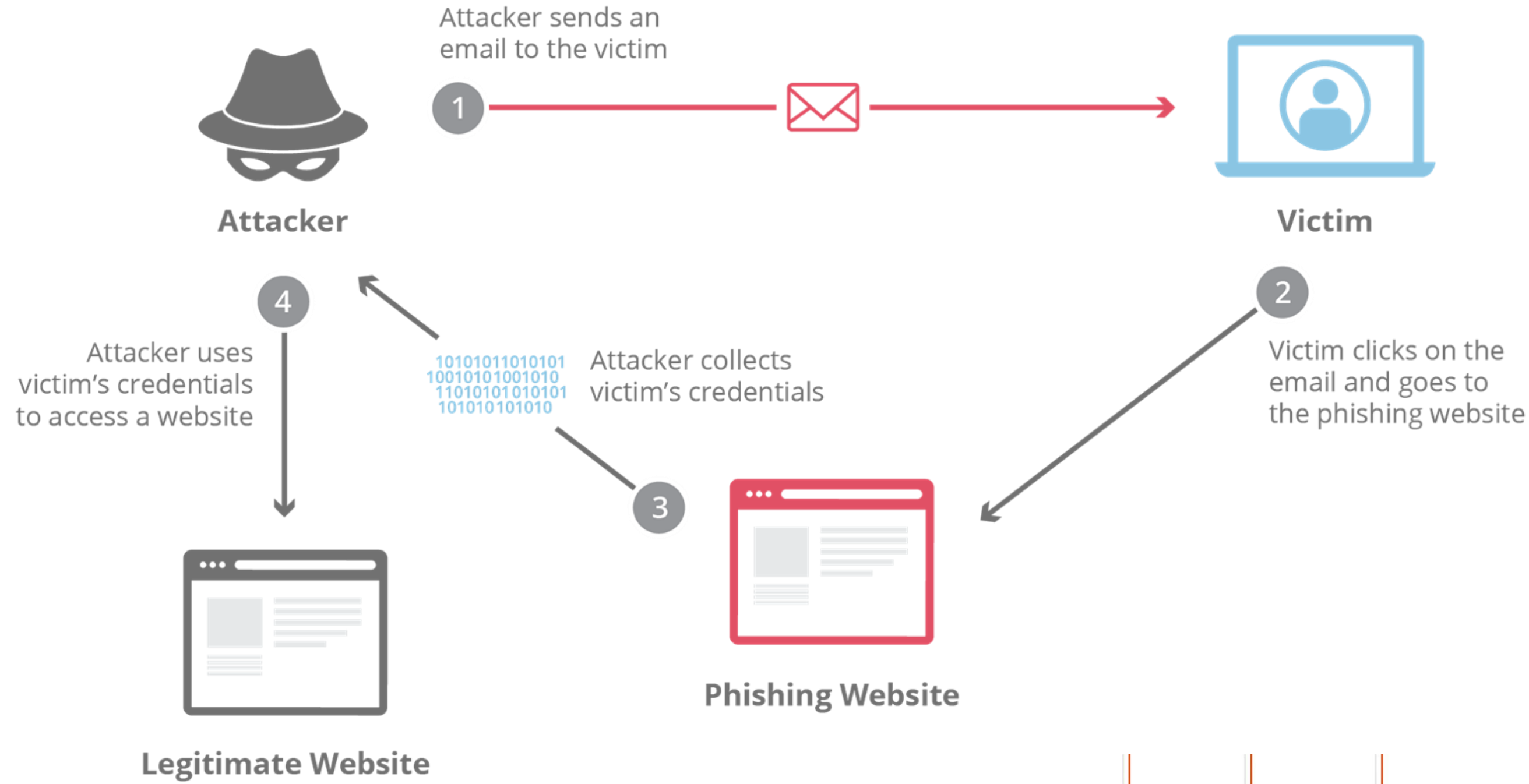
KAYNAK: <https://www.cobalt.io/blog/what-is-denial-of-service-attack>

17. SOSYAL MÜHENDİSLİK & SİBER GÜVENLİKTE KARŞILAŞILAN SOSYAL MÜHENDİSLİK TEHDİTLERİ

- I. Phishing (Yemleme):
- II. Spear Phishing:
- III. Shoulder Surfing (Omuz Sörfü):
- IV. Dumpster Diving (Çöp Karıştırma):
- V. Role Playing (Rol Yapma):
- VI. Pretexting (Bahane Uydurma):
- VII. Baiting (Yemleme):
- VIII. Tailgating (Kuyrukta Sürünme):
- IX. Quid Pro Quo (Karşılık Bekleme):
- X. Impersonation (Kimlik Taklidi):
- XI. Pharming (Çiftçilik):
- XII. Vishing (Sesli Fishing):
- XIII. Water Holing



I. PHISHING (YEMLEME)



KAYNAK: <https://cyberhoot.com/cybrary/phishing/>

- Saldırganlar, sahte e-postalar, web siteleri veya mesajlar kullanarak kullanıcıları kişisel bilgileri ifşa etmeye veya kötü amaçlı yazılımları indirmeye ikna etmeye çalışır.
- Örnek: Kullanıcılara sahte bir banka e-postası göndererek, hesap bilgilerini paylaşmalarını isteyen bir phishing saldırısı.



II. SPEAR PHISHING

Phishing vs. spear phishing vs. whaling

Phishing

A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.



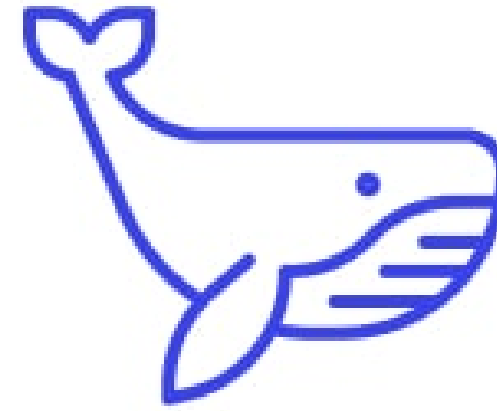
Spear phishing

A type of phishing that targets individuals



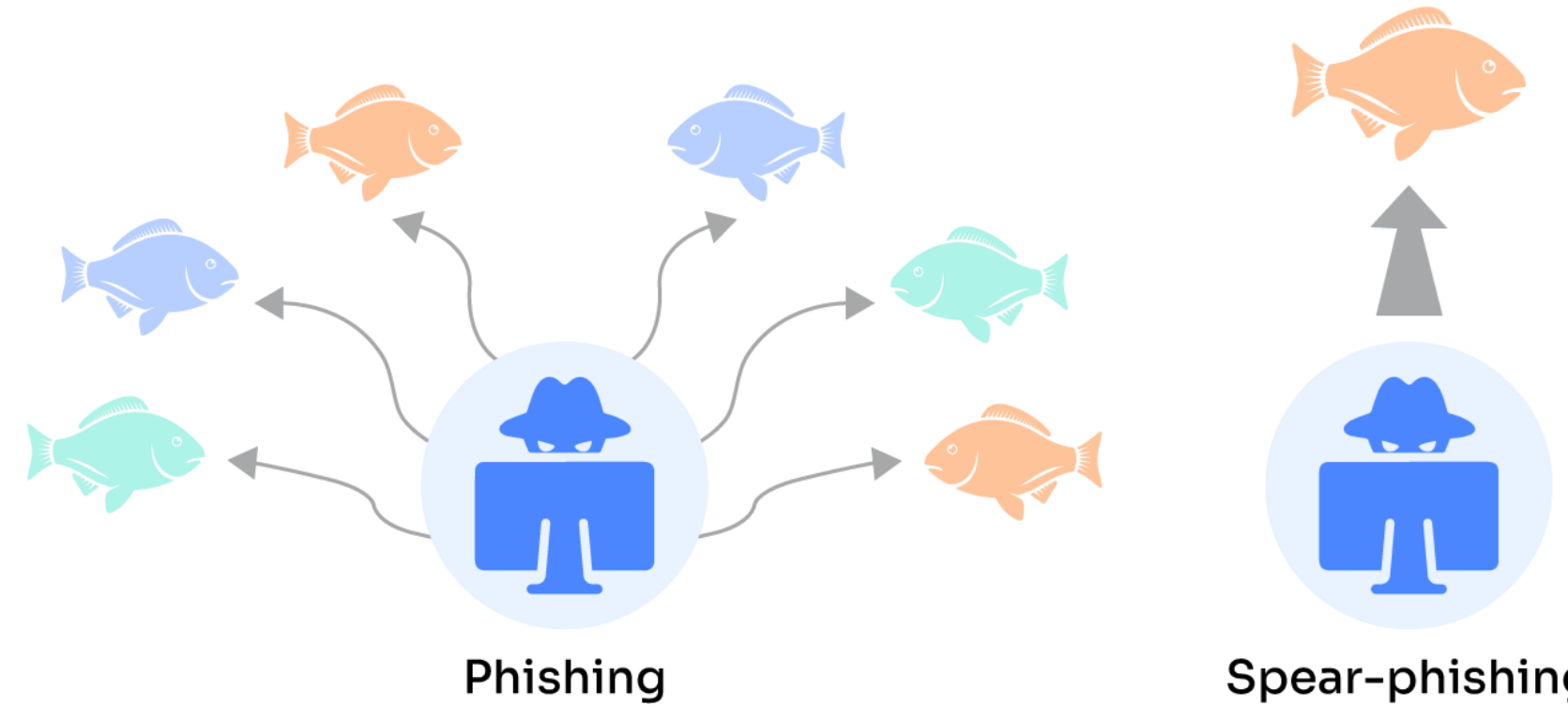
Whaling

A form of spear phishing that targets high-ranking victims within a company.



- Phishing'in özelleştirilmiş bir türüdür; saldırganlar belirli kişileri hedef alarak daha inandırıcı mesajlar gönderir.
- Örnek: CEO'yu taklit eden bir e-posta göndererek finans müdürünü para transferi yapmaya ikna etmeye çalışan bir spear phishing saldırısı.

KAYNAK: <https://www.wallarm.com/what/what-is-a-spear-phishing-attack-how-to-prevent-one>

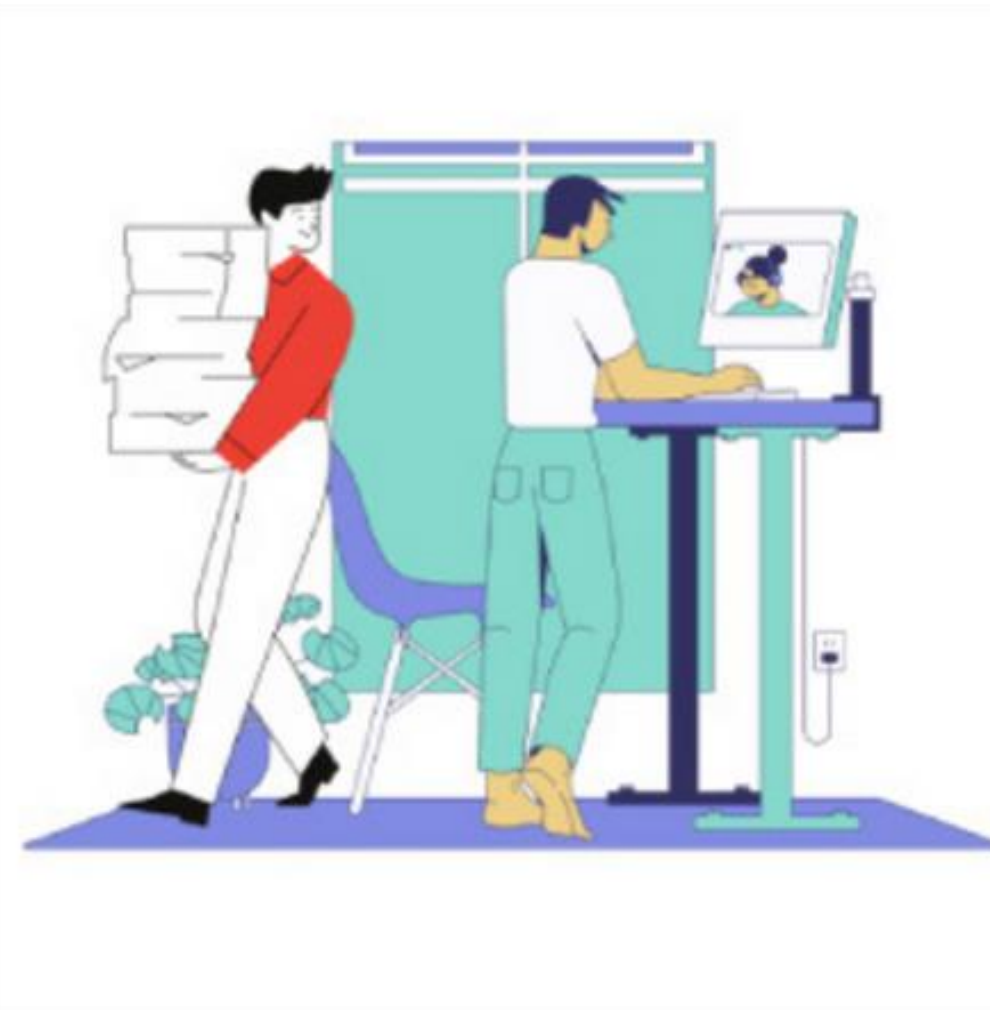


KAYNAK: <https://www.valimail.com/guide-to-phishing/spear-phishing-vs-phishing/>

III. SHOULDER SURFING (OMUZ SÖRFÜ)



- Saldırganlar, birisinin bilgisayar ekranını veya klavyesini izleyerek hassas bilgilere erişim sağlamaya çalışır.
- Örnek: Halka açık bir Wi-Fi ağına bağlıken, yan masada oturan kişinin şifresini izlemek.



IV. DUMPSTER DIVING (ÇÖP KARIŞTIRMA)



KAYNAK: <https://www.techtarget.com/searchsecurity/definition/dumpster-diving>

- Saldırganlar, kurumların veya bireylerin çöplerini karıştırarak hassas bilgilere ulaşmaya çalışır.
- Örnek: İşyerinin atıklarını karıştırarak, bilgisayarların atılan belgeleri üzerinden önemli bilgilere erişmeye çalışan bir saldırgan.



V. ROLE PLAYING (ROL YAPMA)



- Saldırganlar, güven kazanmak veya inandırıcılıklarını artırmak için sahte bir rol üstlenirler.
- Örnek: Teknik destek uzmanı gibi davranarak, kullanıcılardan uzaktan bilgisayarlarına erişim izni talep eden bir role playing saldırısı.

VI. PRETEXTING (BAHANE UYDURMA)

Pretexting Attack Techniques



Impersonation



Piggybacking



Tailgating



Scareware



Vishing and
Smishing



Phishing



Baiting



1.

A fraudster
**impersonates a
trusted authority**
and crafts a scenario
to reach out
to their victims.



2.

The victim
**believes the
scenario** and shares
any information
the 'trusted'
authority requests.



3.

The fraudster
**gains valuable
information**
from their victim
and often uses
it maliciously.

KAYNAK: <https://www.wallarm.com/what/pretexting-types-and-prevention-methods>

KAYNAK: <https://us.norton.com/blog/online-scams/what-is-pretexting>

- Saldırganlar, inandırıcı bir bahane uydurarak kişilerden bilgi veya yardım talep ederler.
- Örnek: Sahte bir müşteri temsilcisi gibi davranarak, bir kişinin banka hesabı bilgilerini çalmaya çalışan bir pretexting saldırısı.

VII. BAITING (YEMLEME)



Scareware



Email hacking



Access tailgating



Phishing



DNS spoofing



Baiting



Physical breaches



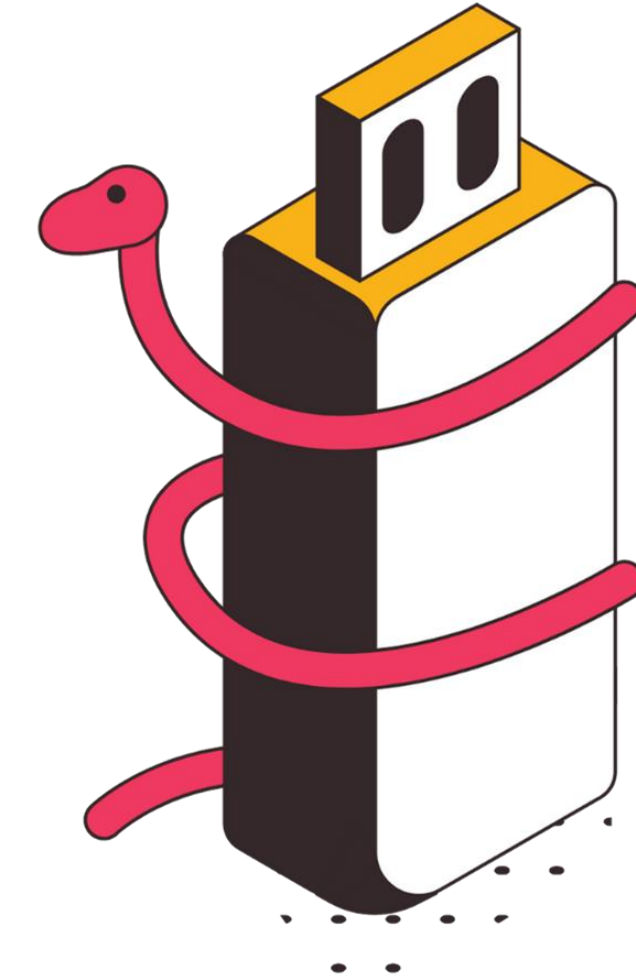
Pretexting



Watering hole attacks



Quid pro quo

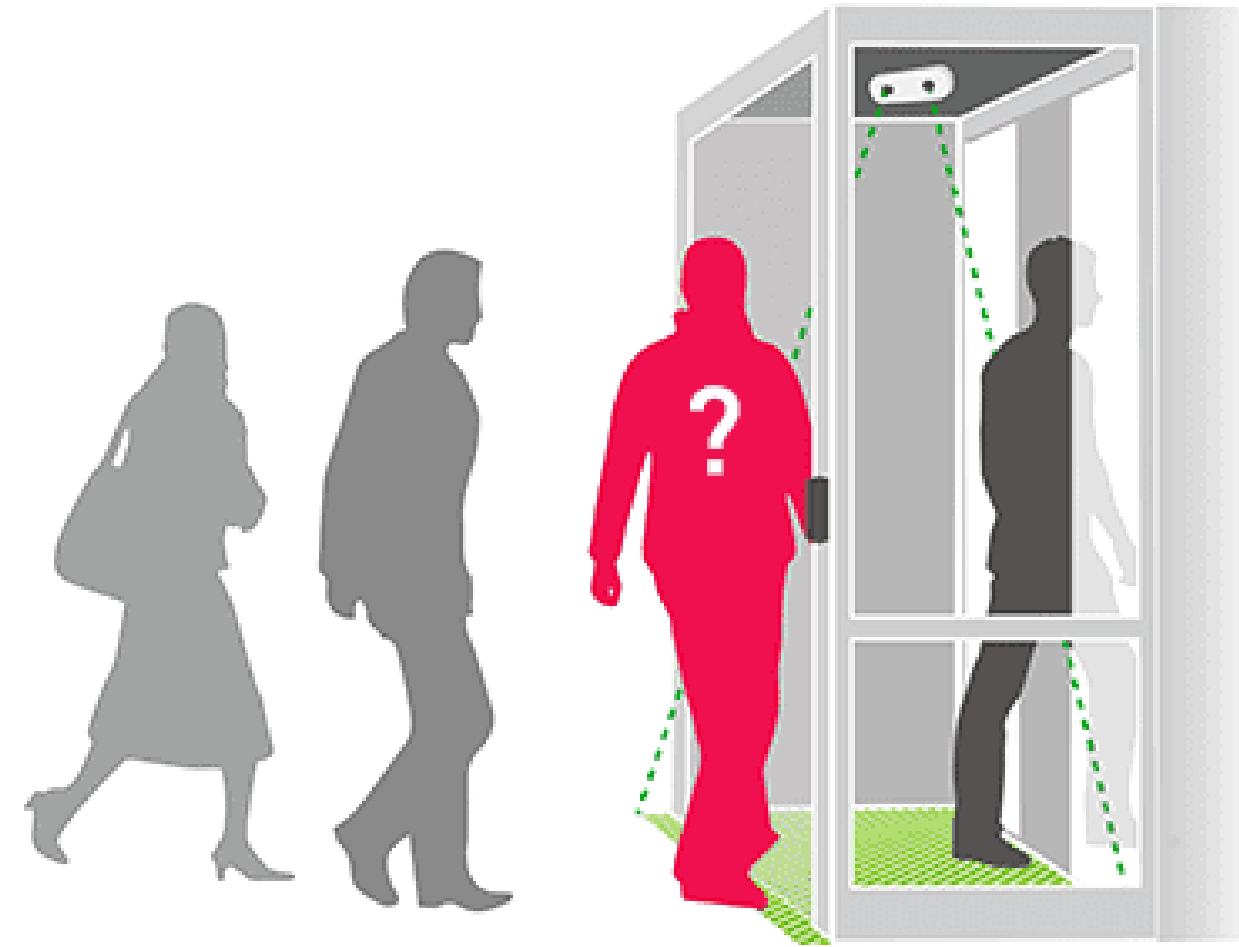


- Saldırganlar, kullanıcıları kötü amaçlı yazılım içeren çekici dosyalar veya cihazlarla cezbetmeye çalışır.
- Örnek: USB belleği park halindeki bir araçta bırakarak, bulan kişinin bilgisayarına kötü amaçlı yazılım bulaştırmaya çalışan bir baiting saldırısı.

VIII. TAILGATING (KUYRUKTA SÜRÜNME)



- Saldırganlar, birisinin yetkili bir alana girmesine izin vermesini bekleyerek güvenlik önlemlerini atarlar.
- Örnek: Bir işyerinin girişinde başkasının arkasından girerek içeri sızma girişimi.



KAYNAK: <https://huperlab.com/products/3d-ai-video-analytics/3d-tailgating-detection/>

KAYNAK:
<https://arindamcctvaccesscontrol.blogspot.com/search/label/Globally%20Tailgating?m=0>

IX. QUID PRO QUO (KARŞILIK BEKLEME)

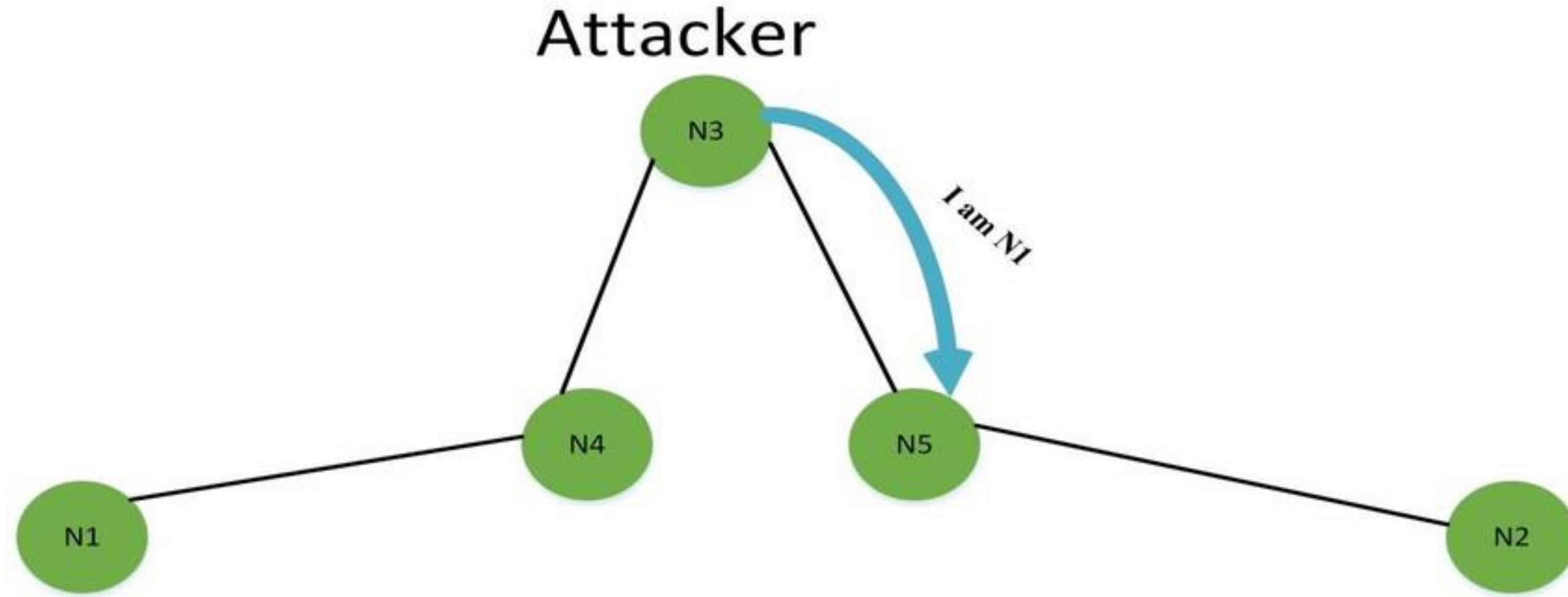


KAYNAK: <https://legal.thomsonreuters.com/blog/quid-pro-quo-social-engineering-infographic-and-explanation/>



- Saldırganlar, kullanıcıları bir hizmet sunmaya veya yardım etmeye söz vererek bilgi elde etmeye çalışır.
- Örnek: Sahte bir teknik destek uzmanı olarak arayan saldırgan, bilgisayarın şifresini öğrenmek için yardım isteyebilir.

X. IMPERSONATION (KİMLİK TAKLİDİ)



KAYNAK: https://www.researchgate.net/figure/A-simple-impersonation-attack-behavior_fig5_282856952

- Saldırganlar, başkasının kimliğini taklit ederek güven kazanmaya çalışır.
- Örnek: Birinin telefon numarasını taklit ederek, sahte bir kimlikle banka işlemi yapmaya çalışan bir impersonation saldırısı.

XI. PHARMING (ÇİFTÇİLİK)

Phishing

VS

Pharming



Easier to identify

Trickier to identify

Targets a single person

Multiple simultaneous targets

Malicious e-mail sent to inbox

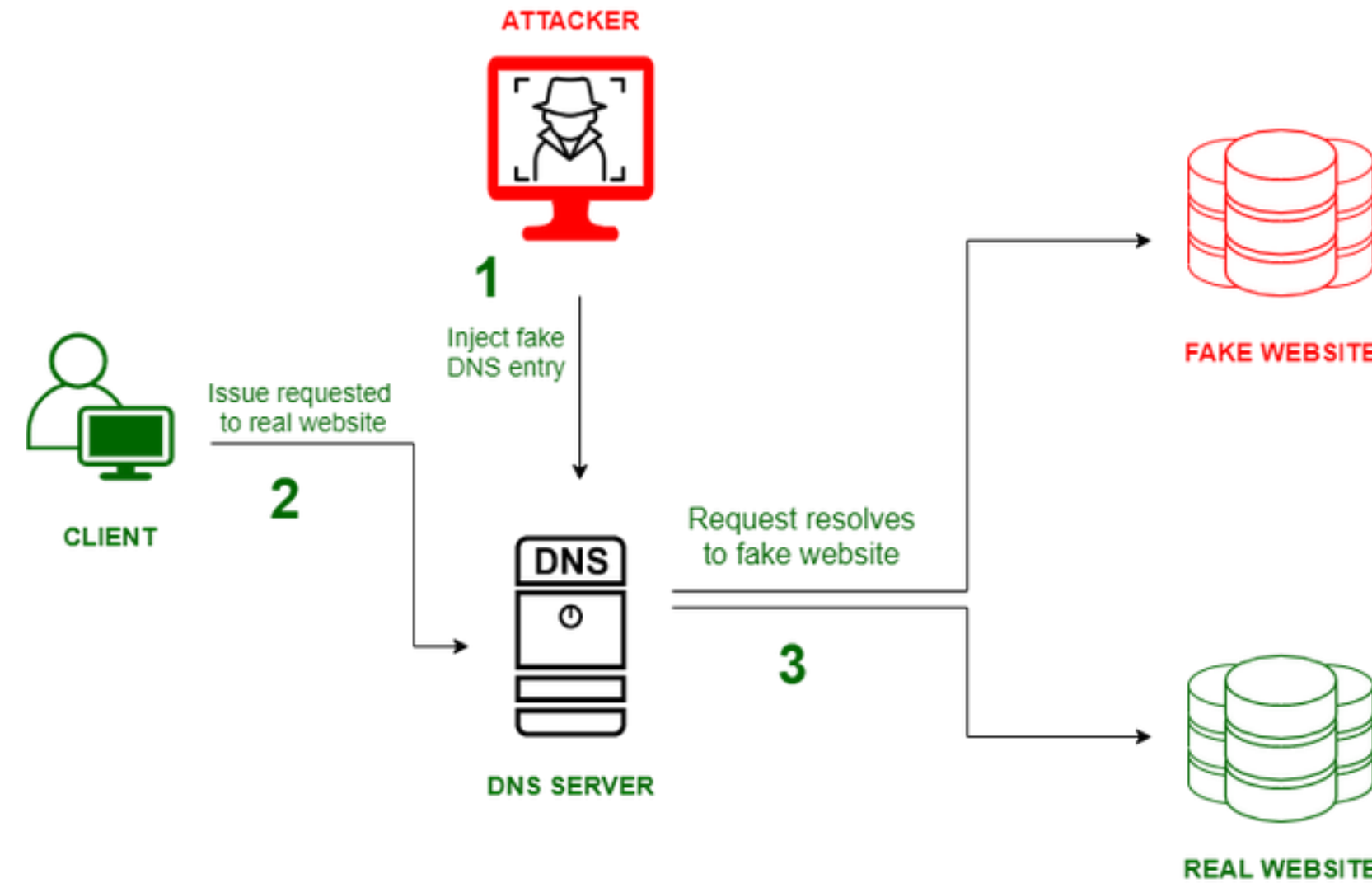
Malicious code installed on computer

Requires the user to manually click the link to activate code

Redirects automatically without user needing to click

KAYNAK: <https://www.linux-wlan.org/what-is-the-difference-between-phishing-and-pharming>

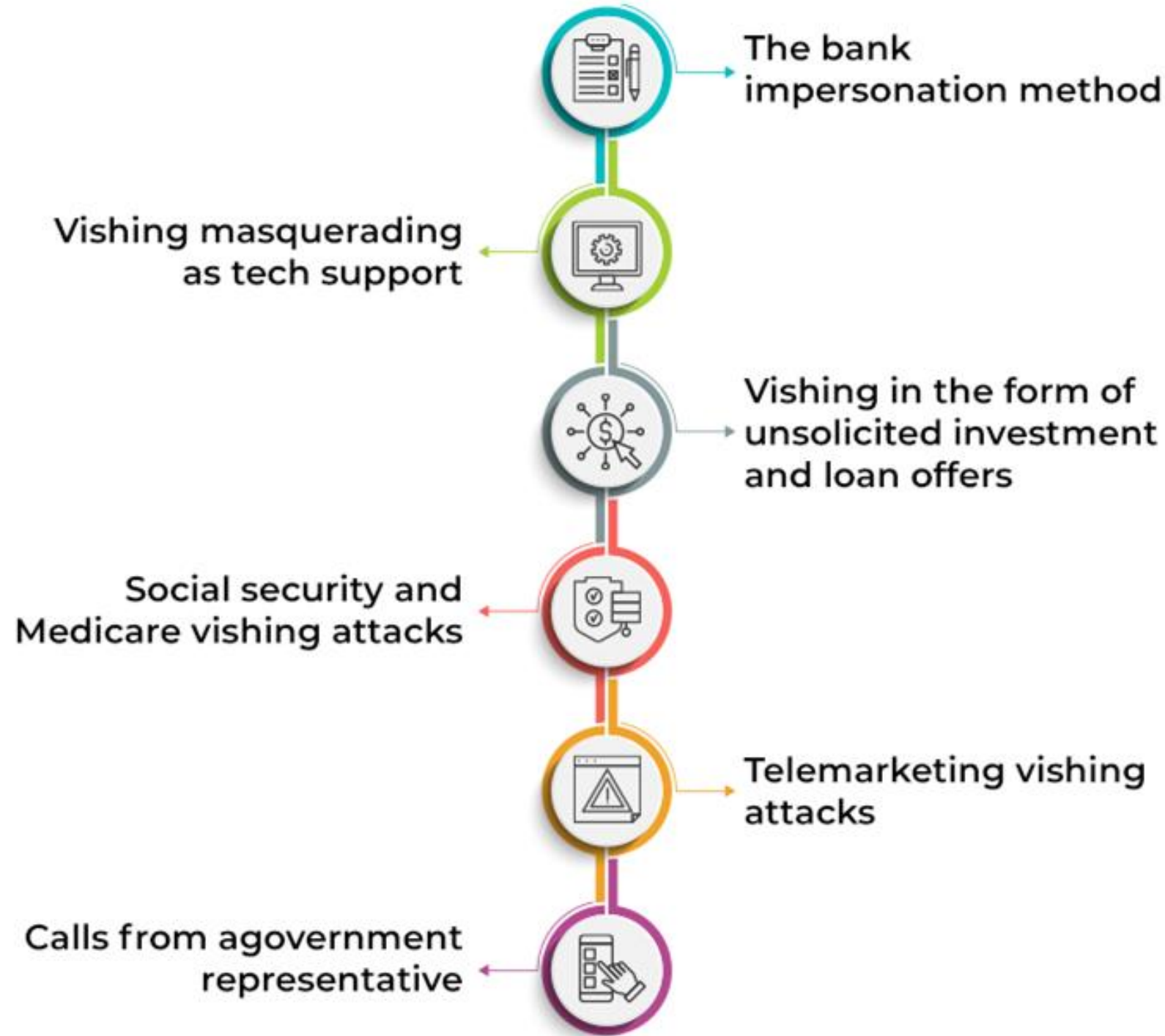
- Saldırganlar, kullanıcıları sahte web sitelerine yönlendirerek kişisel bilgilerini toplamaya çalışır.
- Örnek: Kullanıcıları sahte bir banka web sitesine yönlendiren ve giriş bilgilerini çalmaya çalışan bir pharming saldırısı.



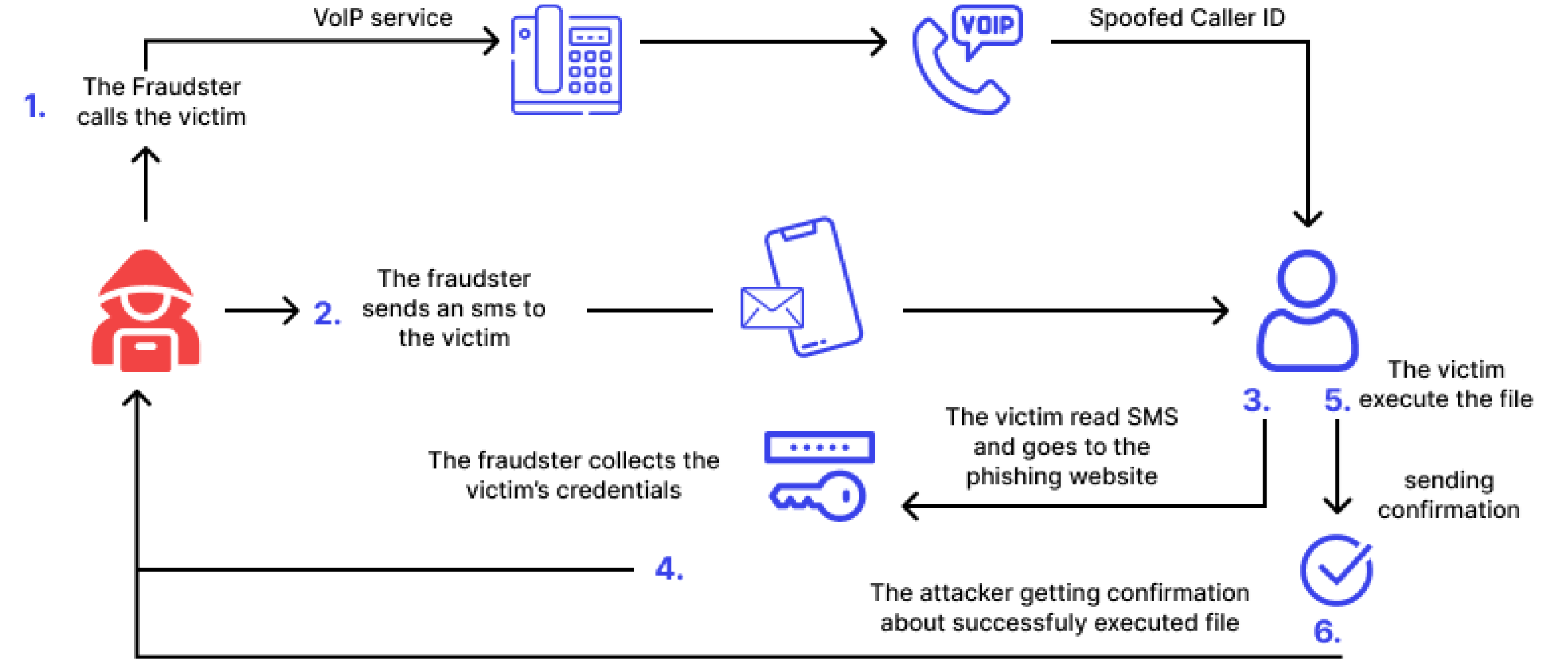
KAYNAK: <https://www.geeksforgeeks.org/pharming-attack-prevention-and-examples/>

XII. VISHING (SESLİ FISHING)

COMMON VISHING METHODS



KAYNAK: <https://bkhost.vn/blog/vishing/>

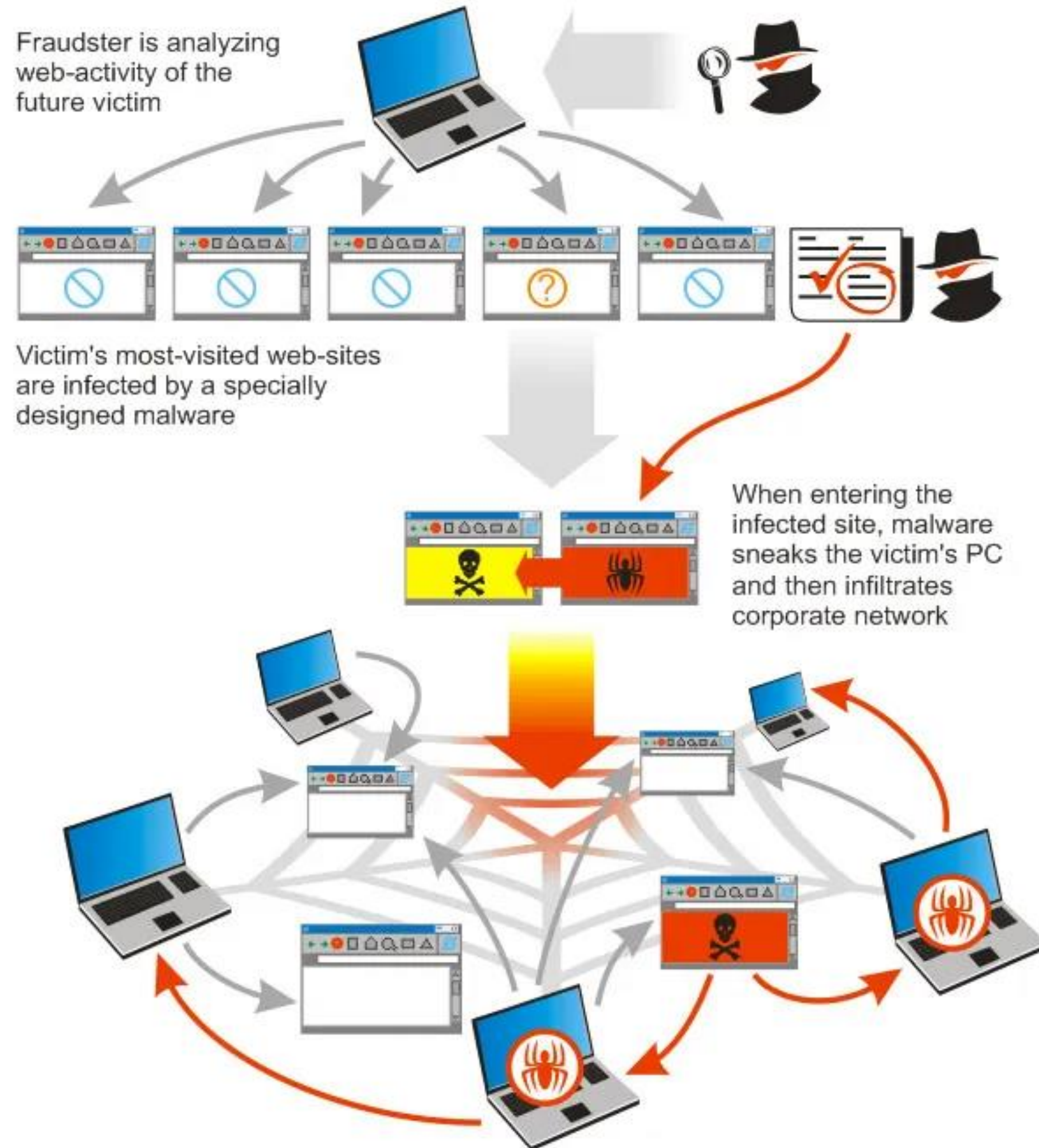


KAYNAK: <https://www.wallarm.com/what/vishing-attack>

- Saldırganlar, telefonla arayarak kurbanları kişisel bilgileri veya finansal bilgileri vermek konusunda kandırmaya çalışır.
- Örnek: Sahte bir banka temsilcisi olarak arayan saldırgan, müşterilerden hesap bilgilerini vermesini isteyebilir.

XIII. WATER HOLING

The “Watering hole” attack



- Saldırganlar, kurbanlarının sık kullandığı web sitelerini hedef alarak kötü amaçlı yazılım veya phishing kampanyaları düzenler.
- Örnek: Bir sektörün ilgi çekici bir web sitesini hackleyen ve ziyaretçilerini kötü amaçlı yazılım ile enfekte etmeye çalışan bir water holing saldırısı.



Bölüm 6

HACKER METODOLOJİSİ

HACKER METODOLOJİSİ



KAYNAK: <https://vishnushivalalp.medium.com/phases-of-hacking-dfa65b3d1505>



Bölüm 7

SİBER SALDIRILARI ÖNLEME & BASİT GÜVENLİK TAVSİYELERİ

SİBER SALDIRILARI ÖNLEME VE BASİT GÜVENLİK TAVSİYELERİ

- Firewall Kullanımı
- Güncel Yazılımlar ve Yama Yüklemeleri
- Güçlü Parolalar ve Kimlik Doğrulama
- Eğitim ve Farkındalık
- Anti-Virüs ve Anti-Malware Yazılımları:
- Saldırı İzleme ve İncelenmesi
- Ağ Güvenliği Duvarları (Intrusion Detection and Prevention Systems - IDPS)
- Veri Yedeklemeleri
- Fidye Ödememe Politikası
- Ayrıcalıklı Erişim Kontrolleri
- Gelişmiş Güvenlik Ekipmanları
- Siber Güvenlik Politikaları ve Prosedürler



SİBER SALDIRILARI ÖNLEME VE BASİT GÜVENLİK TAVSİYELERİ

- Çift Faktörlü Kimlik Doğrulama Kullanın
- Şifre Yöneticisi Kullanın
- Güçlü ve Benzersiz Şifreler Kullanın
- Kişisel Bilgilerinizi Paylaşmaktan Kaçının
- Bilinmeyen E-postalara ve Bağlantılara Dikkat Edin
- Yazılım Güncellemelerini İhmal Etmeyin
- Sosyal Mühendislik Saldırılarına Karşı Bilinçli Olun
- Bilinmeyen USB Cihazlarından Kaçının
- Ağ Güvenliği İçin Firewall Kullanın
- Bilgilerinizi Düzenli Olarak Yedekleyin



SİBER SALDIRILARI ÖNLEME VE BASİT GÜVENLİK TAVSİYELERİ

PEKİ, ÖNEMLİ BİR BELGEYE ARTIK İHTİYACINIZ YOKSA NE YAPMALIYIZ? DİREKT ÇÖPE Mİ ATMALIYIZ?

- Çöplük Dalışını hatırlayalım.
- **Bu tür belgelerle nasıl başa çıkmanız gerektiği hakkında bazı öneriler:**
 - Belgeyi Güvenli Bir Şekilde İmha Edin
 - Dijital Kopyaları Silin
 - Veri Güvenliği İlkelerine Uyun
 - Çöp Kutusu İle Dikkatli Olun



SİBER SALDIRILARI ÖNLEME VE BASİT GÜVENLİK TAVSİYELERİ



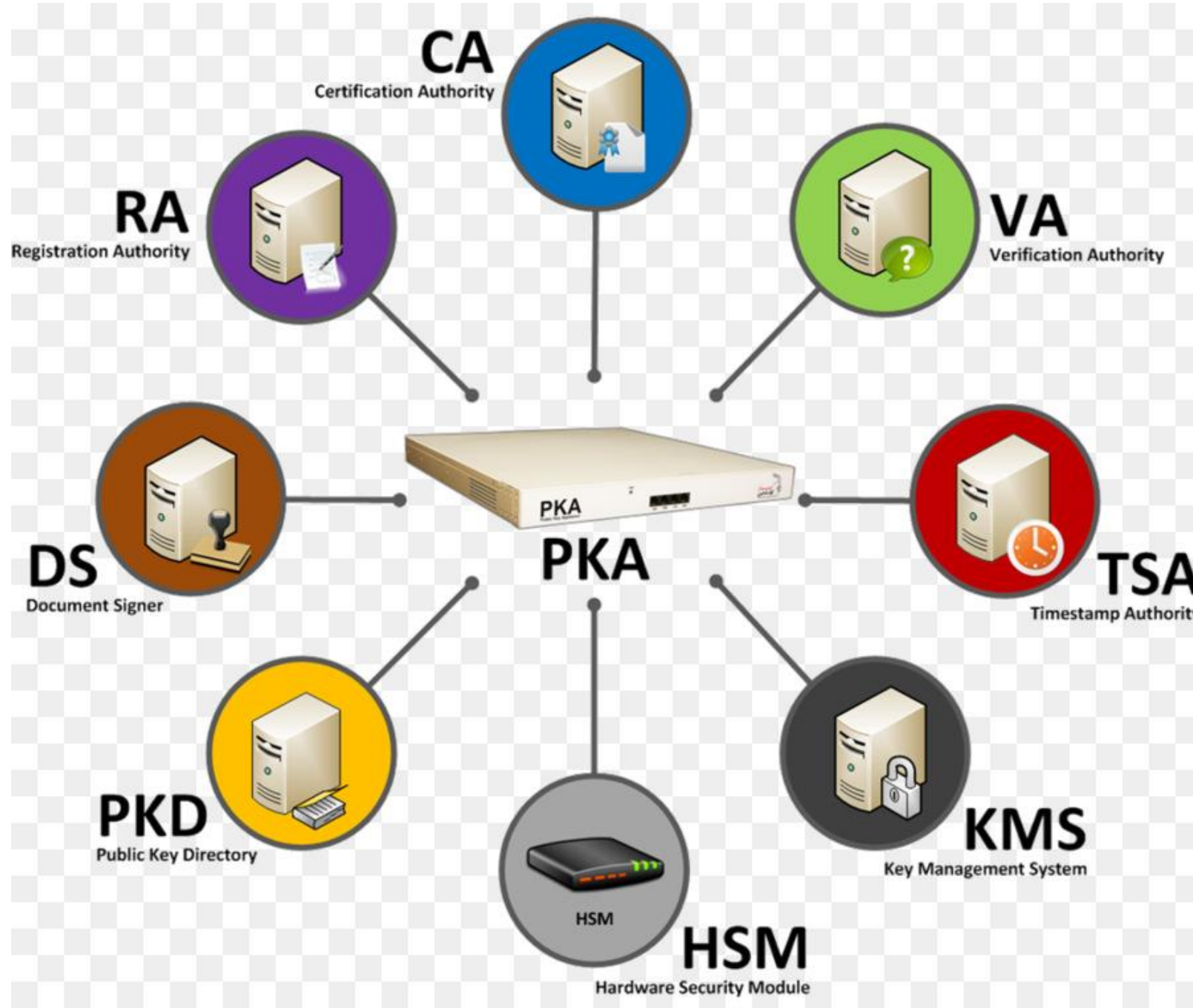
- Zayıf halka olmak istemezsiniz.
- Hele ki iş arkadaşınızın, en yakın arkadaşınızın veya aile üyenizin güvenliğini tehlikeye sokan kişi olmak ve onların mahremiyetini kaybetmesinin nedeni olmak asla istemezsiniz.



Bölüm 8

DONANIM GÜVENLİĞİ
ALTYAPI GÜVENLİĞİ
İŞLETİM SİSTEMİ GÜVENLİĞİ
UYGULAMA SUNUCUSU GÜVENLİĞİ

DONANIM GÜVENLİĞİ



KAYNAK: <https://www.pngindir.com/png-6hst3o/>

Güvenlik Açıkları



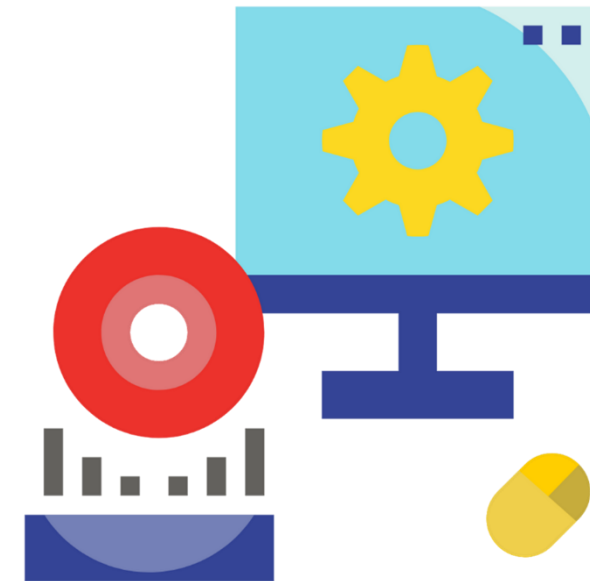
KAYNAK: <http://www.bilgiguvenligi.gov.tr/kilavuz-dokumanlar/index.php>

- Donanım güvenliği, bilgisayar sistemlerinin ve cihazlarının donanım bileşenlerinin, yazılım saldırılarına veya fiziksel tehditlere karşı korunmasını sağlayan bir bilgi güvenliği dalıdır. Temel amaç, donanımın gizlilik, bütünlük ve erişilebilirlik açısından güvende olmasını sağlamaktır.

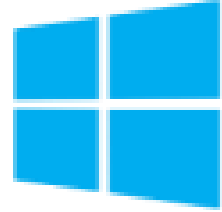
ALTYAPI GÜVENLİĞİ



- Alt yapı güvenliği, bir organizasyonun bilgisayar ağlarının, sunucularının, yönlendiricilerinin ve diğer altyapı bileşenlerinin güvende olduğundan emin olma sürecini ifade eder. Bu, ağ erişiminin sınırlandırılması, güçlü kimlik doğrulama ve veri iletişiminin şifrelenmesi gibi önlemleri içerir.
- Örnek: Bir şirketin ağının güvenliği için güvenlik duvarı (firewall) kullanmak, yetkilendirilmemiş erişimi engellemek için ağ anahtarlarını ve yönlendiricilerini yapılandırmak.



İŞLETİM SİSTEMİ GÜVENLİĞİ

	windows	android	macOS/ iOS	linux	pardus
Logo					
Geliştirici	Microsoft	Google	Apple	Linux Vakfı	Tübitak
Lisans Durumu	Ücretli Lisanslı	Ücretsiz Lisanslı	Ücretli Lisanslı	Ücretsiz, Genel Kamu Lisansı	Ücretsiz
Kullanılan Cihazlar	Bilgisayarda Windows, Telefon ve Tabletlerde Windows Phone	Tablet ve Telefonlarda	Mac bilgisayarlarında macOS, iPhone ve iPad lerde iOS	Bilgisayarda	Bilgisayarda
Kaynak Kodu	Kapalı Kaynak	Açık Kaynak	Kapalı Kaynak	Açık Kaynak	Açık Kaynak
Güvenlik Düzeyi	Orta	Orta	Yüksek	Yüksek	Yüksek

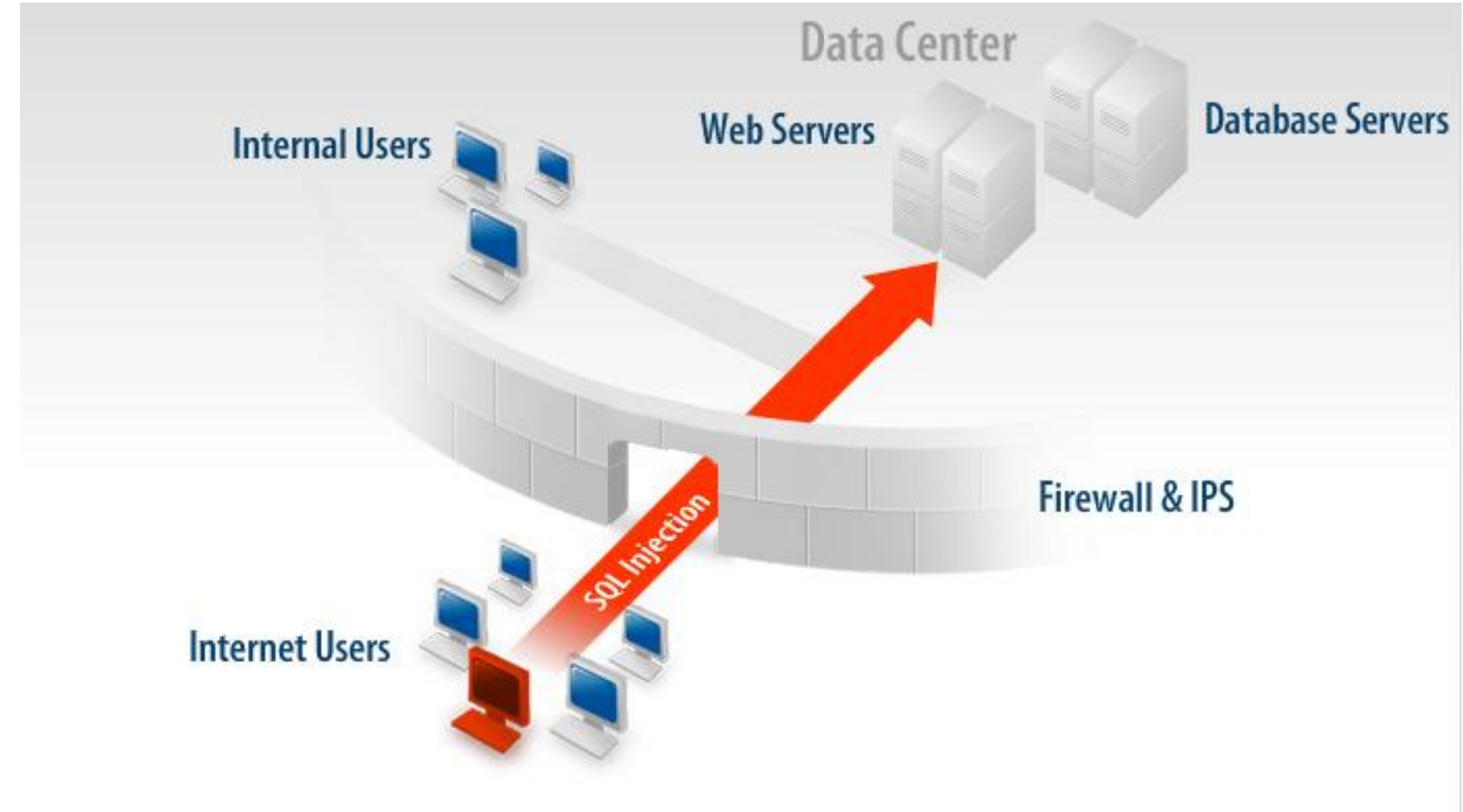
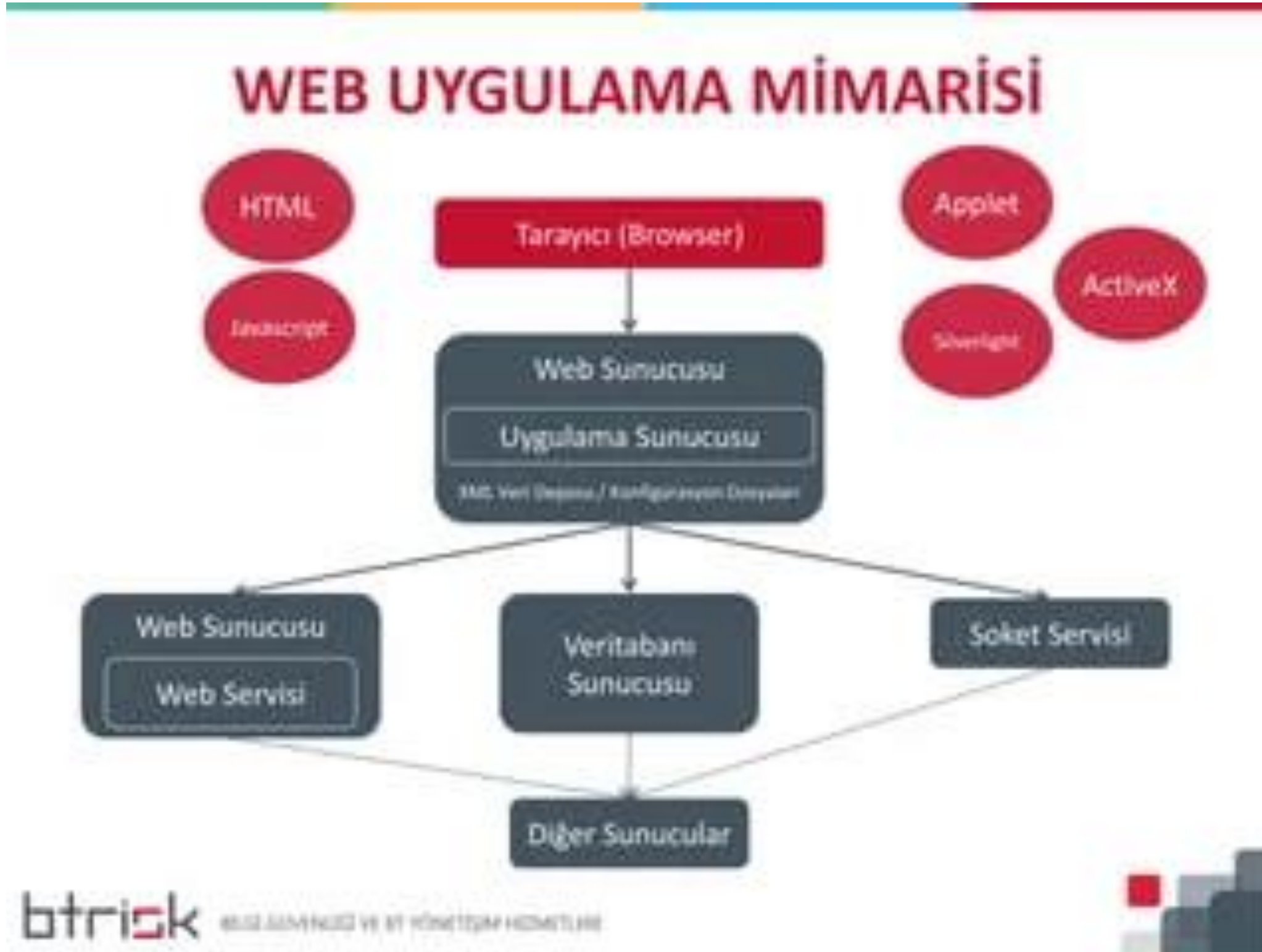


KAYNAK: <https://diyot.net/isletim-sistemi-nedir/>

KAYNAK: <https://btydersnotlari.com/2023/09/20/1-donem-2-hafta-6-sinif-isletim-sistemi/>

- İşletim sistemi güvenliği, bilgisayar veya sunucu üzerinde çalışan işletim sistemlerinin güvende olduğundan emin olma sürecini ifade eder. Bu, güncellemelerin düzenli olarak uygulanması, gereksiz hizmetlerin kapatılması ve güçlü parola politikalarının uygulanması gibi önlemleri içerir.

UYGULAMA SUNUCUSU GÜVENLİĞİ



KAYNAK: <https://www.qtsc.com.vn/en/product-n-solution/qtsc-provides-information-security-services>

KAYNAK: <https://www.slideshare.net/btrisk/web-uygulama-guvenligi-sunumu>

- Uygulama sunucusu güvenliği, web sunucuları, veritabanı sunucuları veya diğer uygulama sunucularının güvende olduğundan emin olma sürecini ifade eder. Bu, güvenlik yamalarının uygulanması, gereksiz hizmetlerin kapatılması ve sıkı erişim kontrolünün sağlanması gibi önlemleri içerir.



Bölüm 9

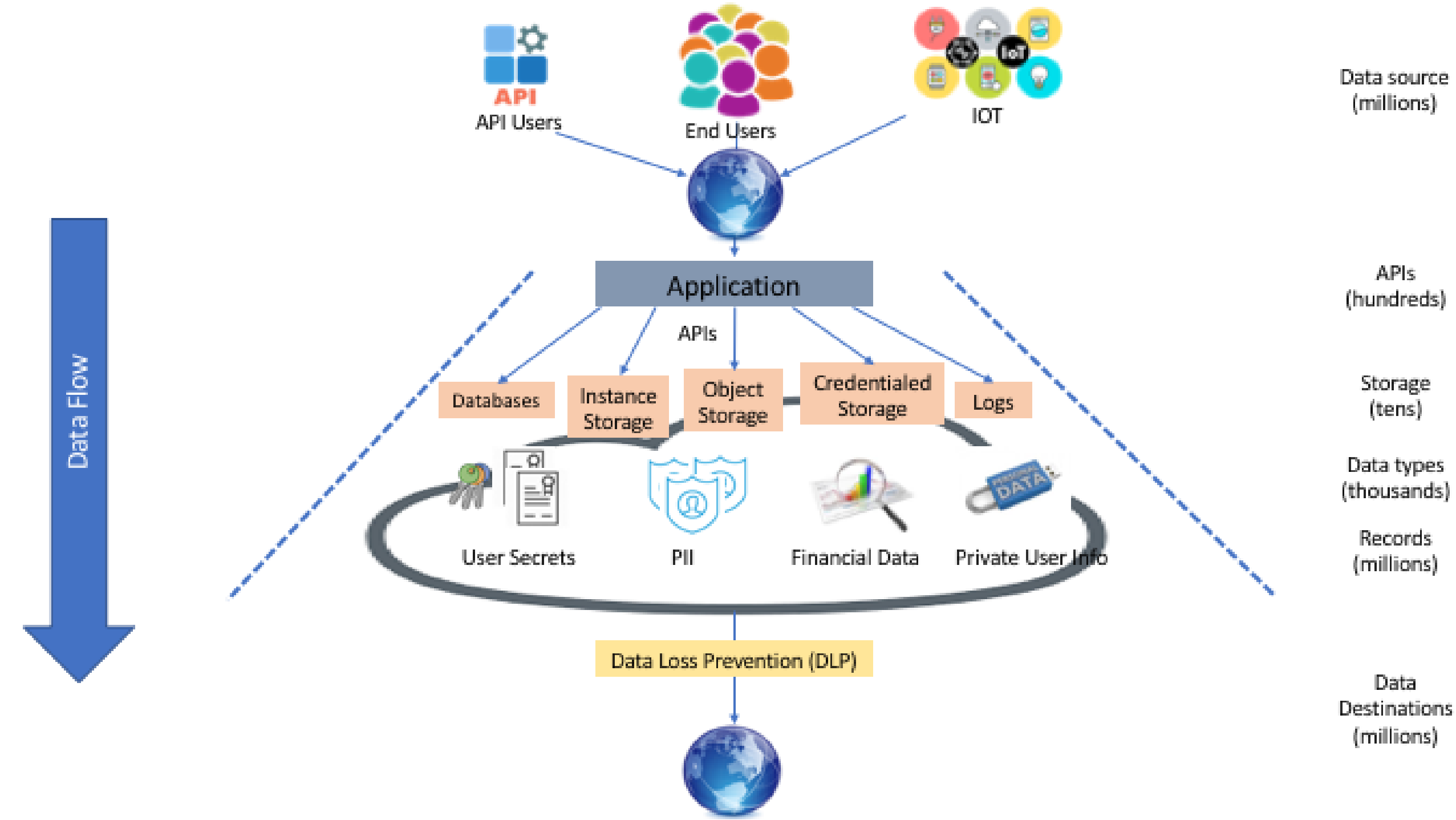
VERİ SIZINTISI (KAZARA/İSTEM DIŞI - KASITLI/İSTEMLİ) VERİ SIZINTISINI ÖNLEME

VERİ SIZINTISI (DATA BREACH)

- Veri sızıntısı, hassas veya kişisel bilgilerin yetkisiz erişim veya ifşa sonucu sızdırıldığı bir olaydır.
 - Bu tür bir sızıntı, kişisel bilgilerin, finansal bilgilerin, sağlık kayıtlarının veya diğer hassas verilerin yetkisiz kişilerin eline geçmesi durumunda meydana gelir.
 - Veri sızıntıları, organizasyonların veya bireylerin güvenliğini ve gizliliğini tehlikeye atabilir.
- a. İstem Dışı-Kazara Veri Sızıntısı
 - b. İstemli-Kasıtlı Veri Sızıntısı



İSTEM DIŞI-KAZARA VERİ SIZINTISI



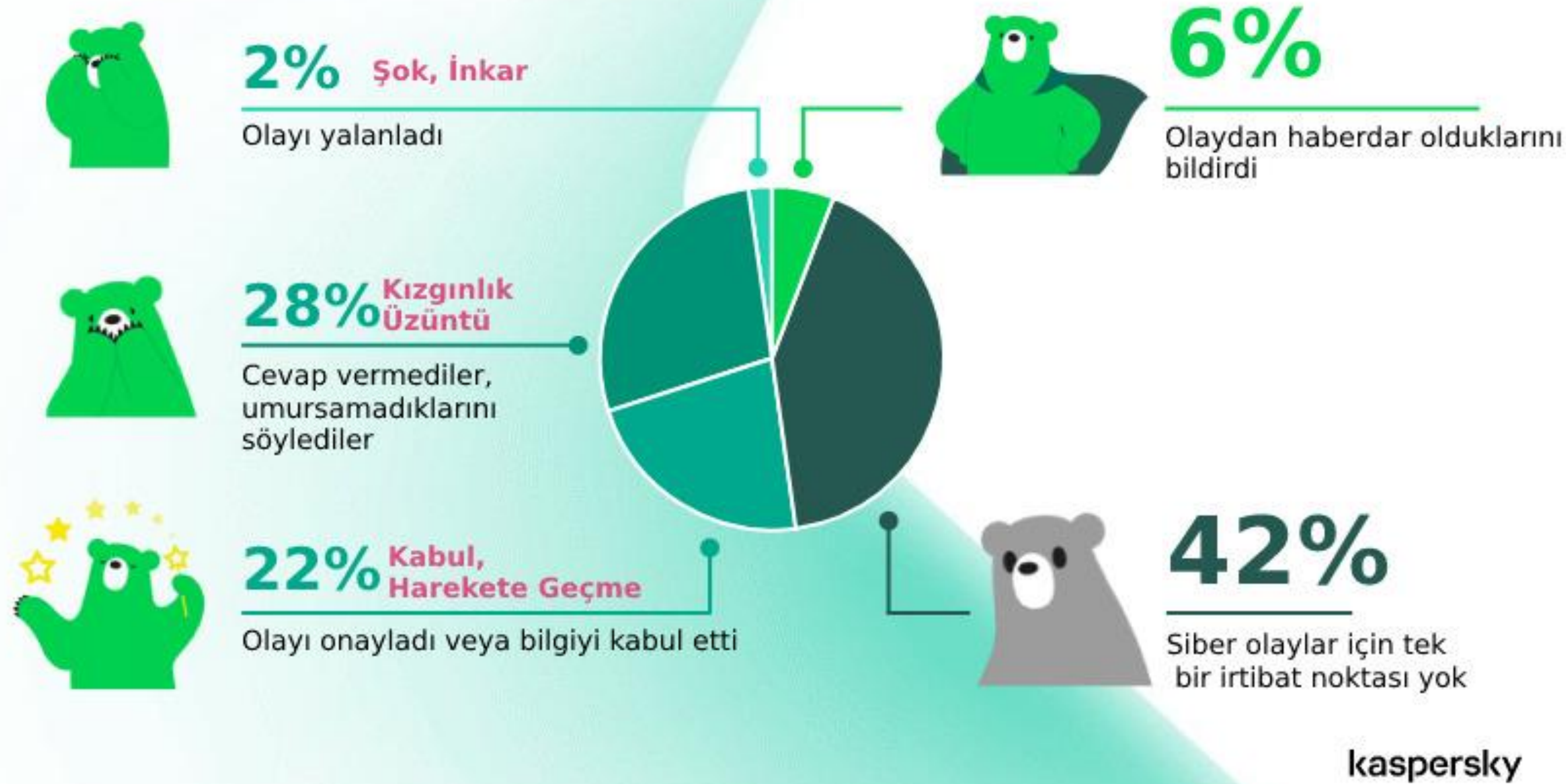
KAYNAK: <https://blog.shiftright.io/why-data-loss-prevention-dlp-must-evolve-for-modern-applications-e653dc661be0>

- Kazara veri sızıntısı, verinin yetkisiz bir şekilde ifşa edilmesine veya kaybedilmesine neden olan istem dışı olayları ifade eder.
- Bu tür sızıntılar genellikle insan hataları, teknik arızalar veya kötü niyetli olmayan ihlaller sonucu meydana gelir

İSTEMLİ-KASITLI VERİ SIZINTISI

Şirketler, Darkweb'de verilerinin gizliliğinin ihlal edilmesine nasıl tepki veriyor?

Kaspersky 258 şirketi, çalınmış kimlik bilgileri, veri sızıntısı, ilk erişim izni gibi verilerinin Darkweb'de kullanımıyla ilgili bilgilendirildi



- İstem dışı kasıtlı veri sızıntısı, verinin kötü niyetli bir eylem sonucu ifşa edilmesine neden olan bir durumu ifade eder.
- Bu tür sızıntılar, bilinçli bir şekilde veri çalmayı veya ifşa etmeyi amaçlayan kişiler veya gruplar tarafından gerçekleştirilir.
- Saldırganlar, hassas verilere erişmek veya bu verileri kötü amaçlı olarak kullanmak için çeşitli yöntemler kullanabilirler.

VERİ SIZINTISINI ÖNLEME

- Veri sızıntısını önleme, hassas veya kişisel bilgilerin yetkisiz erişim veya ifşa sonucu sızdırılmasını engellemeyi amaçlar. Bu, organizasyonların veya bireylerin gizliliğini ve verilerinin güvenliğini korumak için alınan önlemleri içerir.

Veri Sızıntısını Önlemenin Temel Prensipleri ve Önerileri:

- Eğitim ve Farkındalık
- Güçlü Kimlik Doğrulama
- Veri Şifreleme
- Güncel Yazılımlar ve Yama Yüklemeleri
- Siber Güvenlik Yazılımı Kullanımı
- Veri Erişim Kontrolleri
- Veri Yedeklemeleri
- Ağ Güvenliği





Bölüm 10

PAROLA / ŞİFRELER

PAROLA / ŞİFRE NEDİR?

- Parola bir kullanıcının belirli bir hesaba veya sistemde kimliğini doğrulamak için kullandığı gizli karakter dizisidir.
- Parolalar, kullanıcı adı ile birlikte kullanılarak hesaba erişim sağlar. Genellikle harf, rakam ve sembollerin kombinasyonlarından oluşurlar ve gizliliklerinin korunması önemlidir.

Örnek: "P@ssw0rd123" veya "MySecretCode2023!"



PAROLA GÜVENLİĞİ

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

- Parola güvenliği, kullanıcıların parolalarını güvende tutma ve kötü niyetli kişilerin hesaplara yetkisiz erişimini engelleme pratiğini ifade eder.
- Güçlü parola güvenliği, zorlukla tahmin edilebilecek karmaşık parolaların kullanılmasını içerir. Ayrıca, parolaların düzenli olarak değiştirilmesi ve güvende tutulması da önemlidir.
- Güçlü bir parola, büyük harf, küçük harf, rakam ve sembollerin karışımını içerir ve kişisel bilgilere dayanmaz.

PAROLA SALDIRILARI NEDİR?

- Parola saldırıları, kötü niyetli kişilerin veya yazılımın bir hesaba veya sistemdeki parolayı tahmin etmeye veya kırarak yetkisiz erişim elde etmeye çalıştığı siber saldırı türleridir.

Aşağıda bazı parola saldırısı türleri ve örnekleri verilmiştir:

1. Brute Force Saldırısı:

Örnek: "aaaaa", "aaaab", "aaaac", ...

2. Dictionary Saldırısı:

Örnek: "password", "admin", "123456".

3. Phishing Saldırısı:

Örnek: Kullanıcıların banka hesap bilgilerini girmelerini isteyen sahte bir banka web sitesi.

4. Rainbow Table Saldırısı:

Örnek: Önceden hesaplanmış MD5 veya SHA-1 karma değerlerini içeren bir veritabanı.



KAYNAK:

<https://preview.redd.it/273uascsf4r41.jpg?width=1080&crop=smart&auto=webp&s=7b8d997fa7f42682a8277ea916f0ea82b6672a9e>



Bölüm 11

VERİ TABANI VERİ TABANI GÜVENLİĞİ

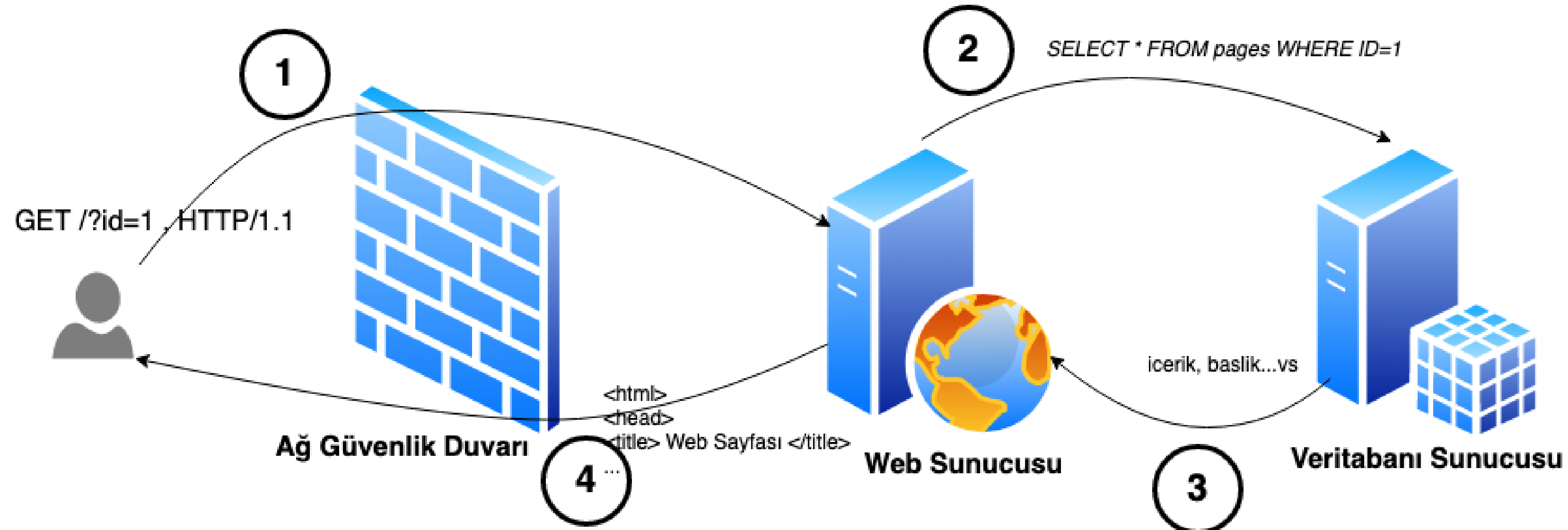
VERİ TABANI (DATABASE) NEDİR?

- Veri tabanı, yapılandırılmış bir şekilde bilgi saklamak, düzenlemek, erişmek ve sorgulamak için kullanılan bir elektronik depolama sistemidir.
- Veri tabanları, büyük miktarda verinin güvenli ve düzenli bir şekilde yönetilmesine olanak tanır. Bu veriler, metin, sayılar, resimler, sesler veya diğer veri türlerini içerebilir.

Örnek: Bir şirketin müşteri bilgilerini, ürün envanterini ve işlemlerini saklamak için bir veri tabanı kullanabilir. Bu veri tabanı, tüm bu bilgilere hızlı ve güvenli bir şekilde erişim sağlar.



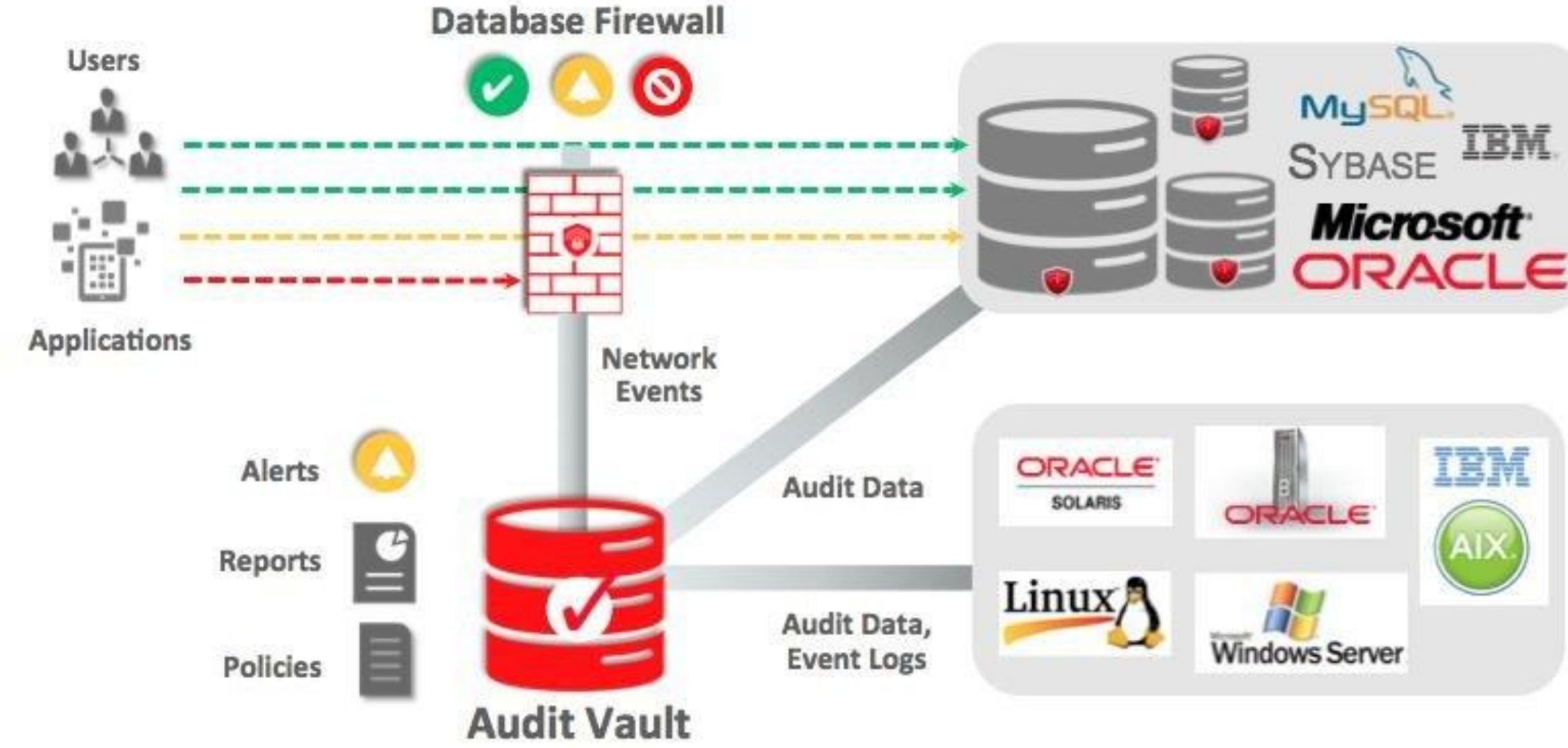
VERİ TABANI GÜVENLİĞİ NEDİR?



KAYNAK: <https://docs.ahtapot.org.tr/kullanım-klavuzlari/web-uygulama-guvenlik-duvari-kullanimi/>

- Veri tabanı güvenliği, bir veri tabanının içerdiği bilgilerin ve yapıların yetkisiz erişimden, değiştirilmeden veya yok edilmeden korunmasını sağlamayı amaçlar.

VERİ TABANI GÜVENLİĞİ UNSURLARI



KAYNAK: <https://iicybersecurity.wordpress.com/2016/02/>

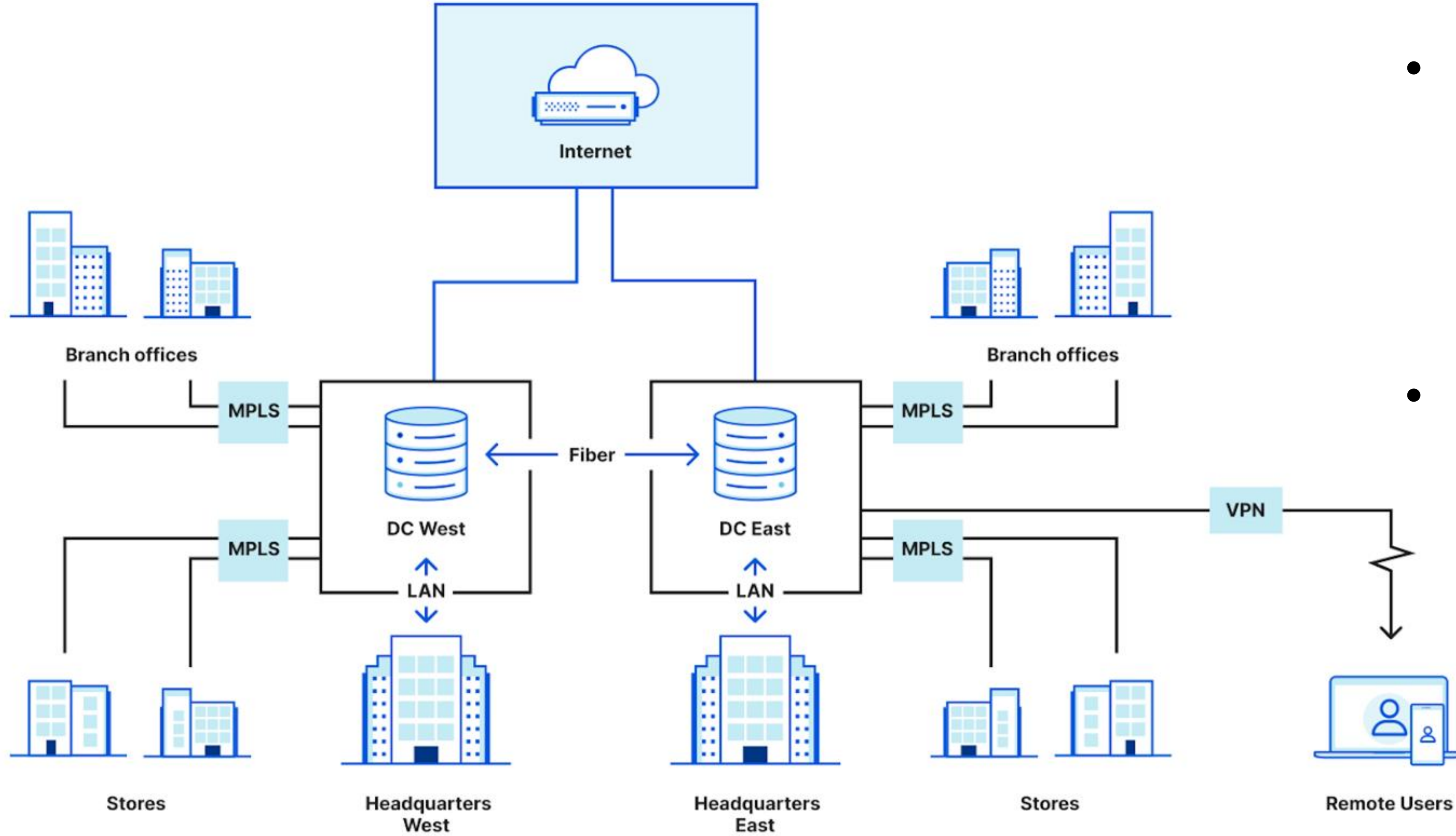
- Veri tabanı güvenliği, bilgi güvenliğinin önemli bir parçasıdır ve aşağıdaki unsurları içerir:
1. Erişim Kontrolleri
 2. Şifreleme
 3. Günlük Kayıtları
 4. Yedeklemeler
 5. Güncel Yazılım ve Yama Yüklmeleri
 6. Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)



Bölüm 12

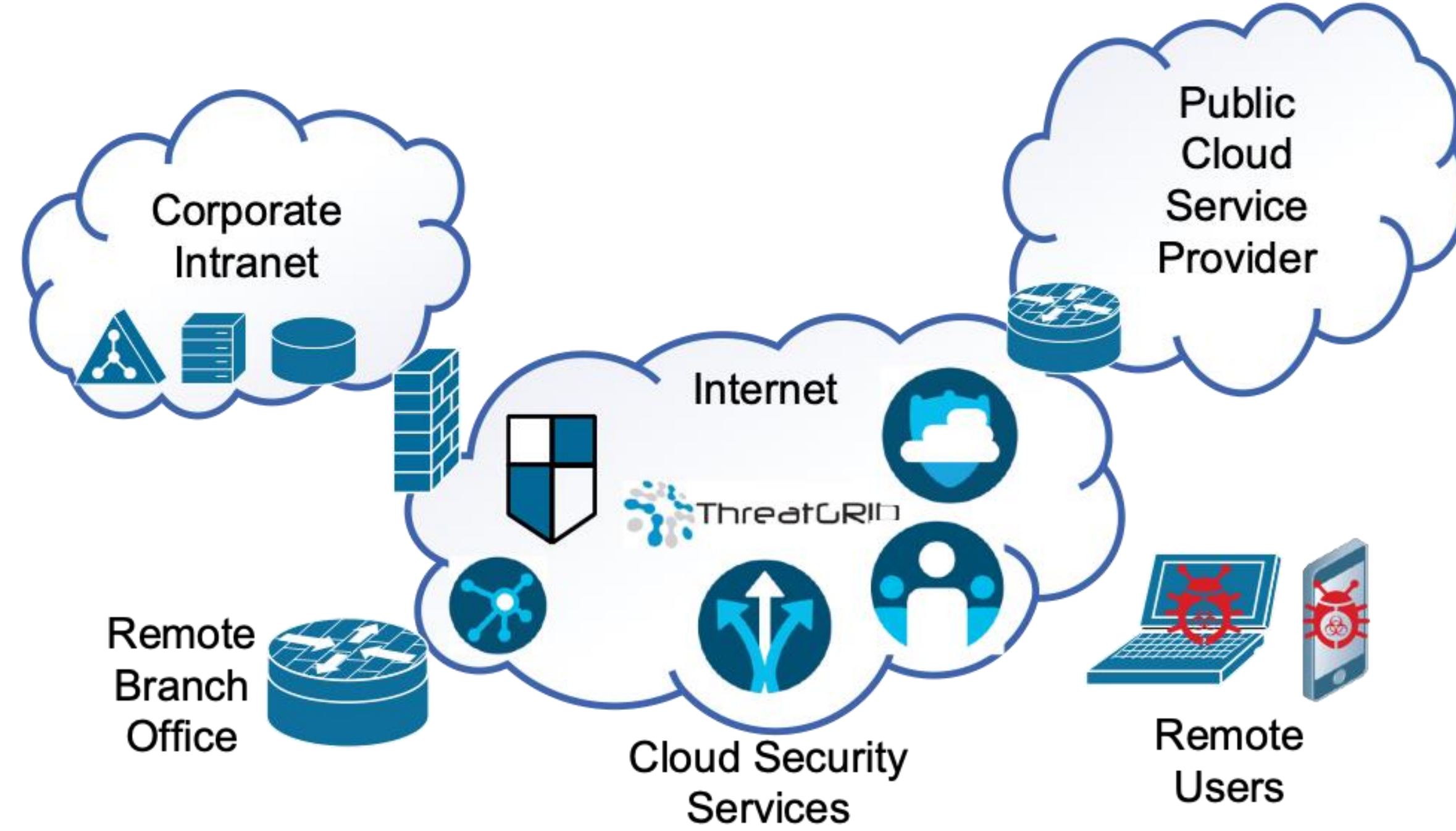
KURUMSAL AĞ KURUMSAL AĞ GÜVENLİĞİ

KURUMSAL AĞ (CORPORATE NETWORK) NEDİR?



- Kurumsal ağ, bir organizasyonun veya işletmenin içindeki bilgisayarların ve diğer cihazların birbiriyle iletişim kurduğu, bilgi ve veri paylaştığı özel bir iletişim altyapısını ifade eder.
- Kurumsal ağlar, çalışanların işbirliği yapması, veri ve dosya paylaşımı, e-posta iletişimi gibi günlük iş süreçlerini desteklemek için kullanılır.

KURUMSAL AĞ GÜVENLİĞİ NEDİR?



KAYNAK: <https://zivaro.com/enterprise-network-security-architecture-transformation/>

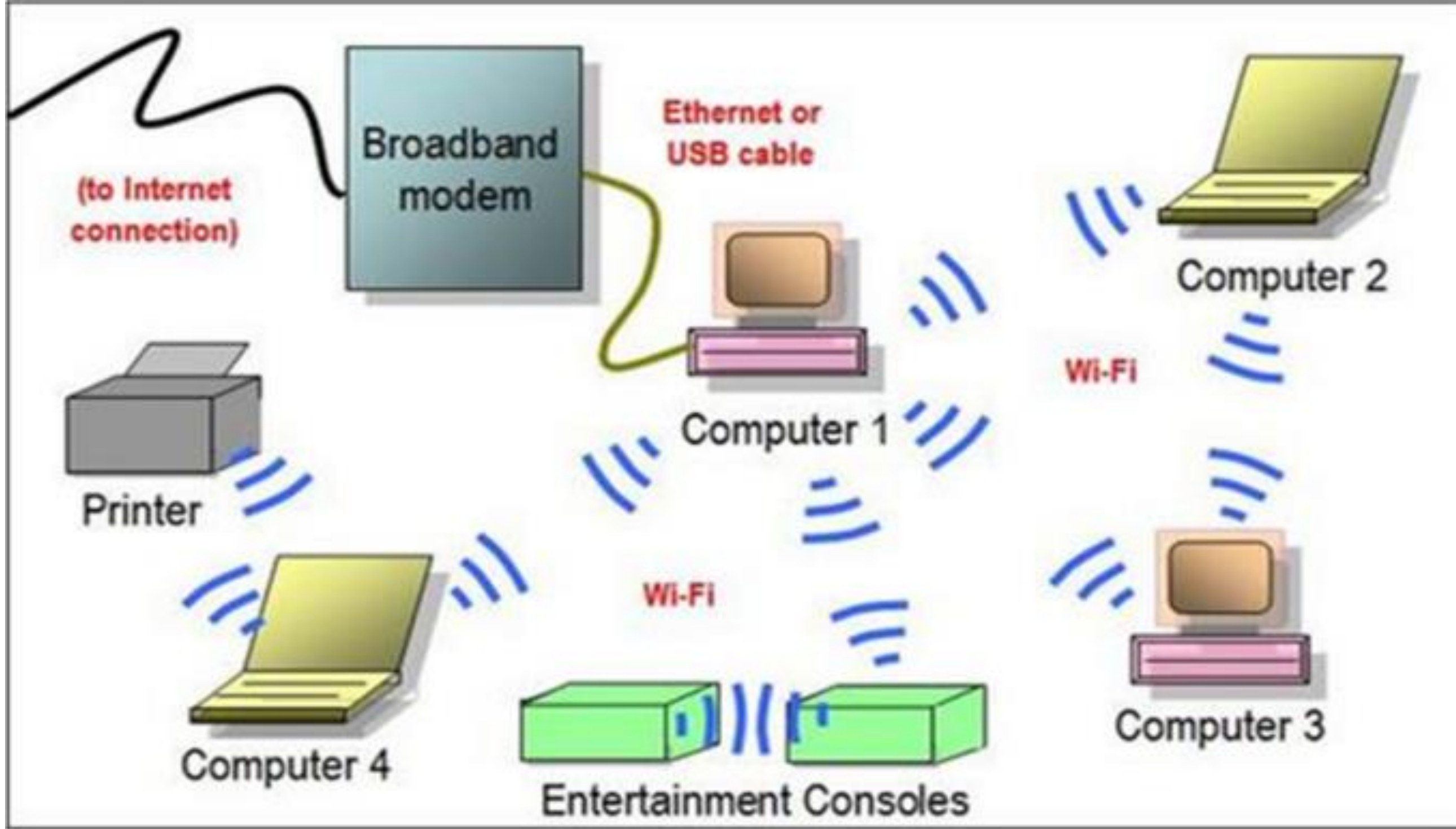
- Kurumsal ağ güvenliği, bir organizasyonun iç ağına yönelik tehditlere karşı koruma sağlama pratiğini ifade eder.
- Bu, ağa yetkisiz erişimden, veri sızıntısından veya diğer siber saldırılardan korunmayı içerir. Ayrıca, çalışanların ve organizasyonun veri güvenliği politikalarına uygun davranmalarını teşvik etmek de önemlidir.



Bölüm 12

KABLOSUZ AĞ KABLOSUZ AĞ GÜVENLİĞİ WEP, WPA, WPA3

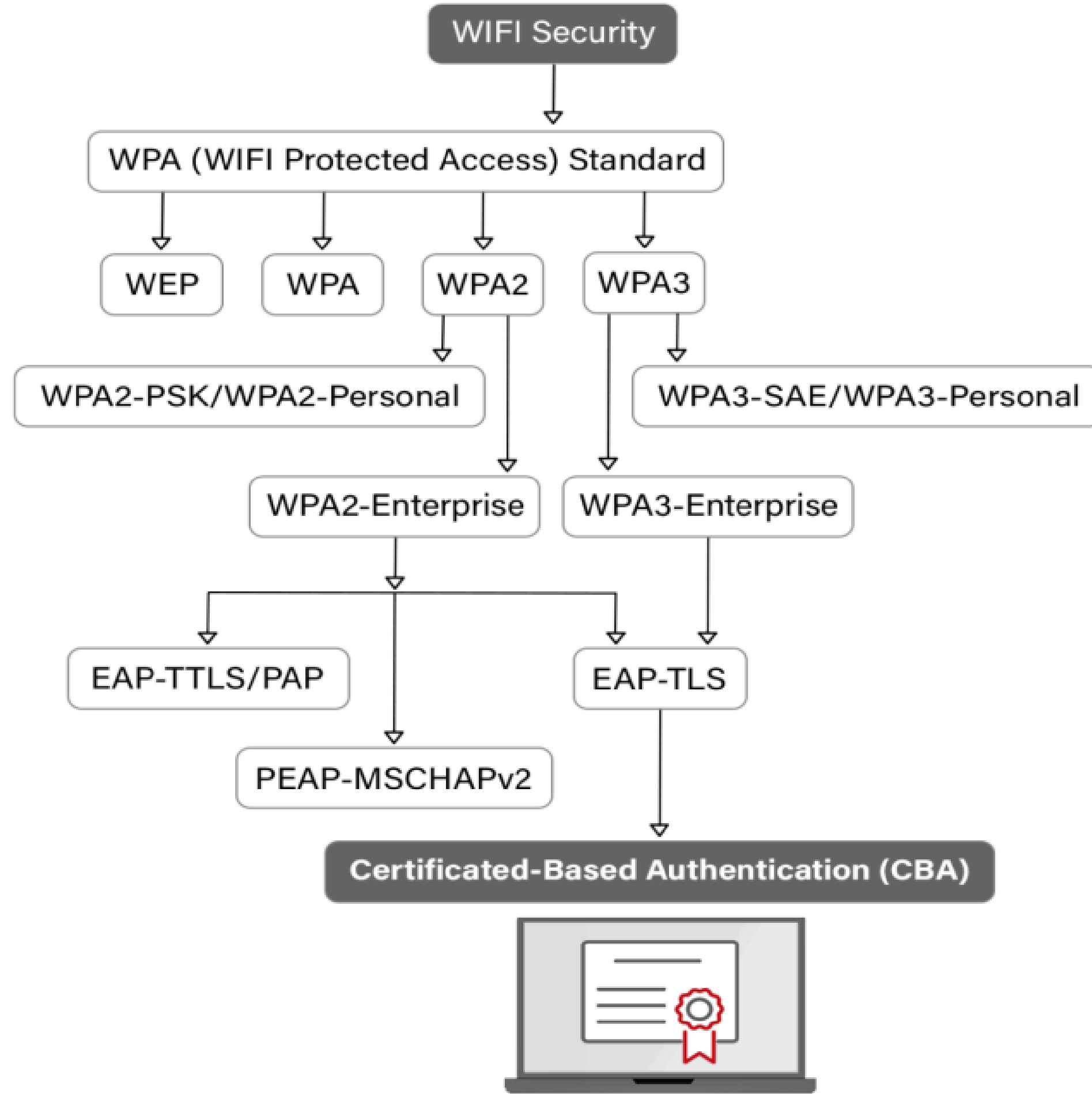
KABLOSUZ AĞ (WIRELESS NETWORK) NEDİR?



KAYNAK: <https://link.springer.com/article/10.1007/s11831-021-09631-5>

- Kablosuz ağ, bilgisayarlar, telefonlar, tabletler ve diğer cihazların kablosuz iletişim teknolojileri aracılığıyla birbirleriyle veya internetle iletişim kurmasını sağlayan bir ağ türüdür. Bu iletişim Wi-Fi, Bluetooth veya diğer kablosuz iletişim protokollerini kullanarak gerçekleşir.
- Kablosuz ağlar, telli (kablolu) ağlara göre daha esneklik ve mobilite sağlar.

KABLOSUZ AĞ GÜVENLİĞİ NEDİR?



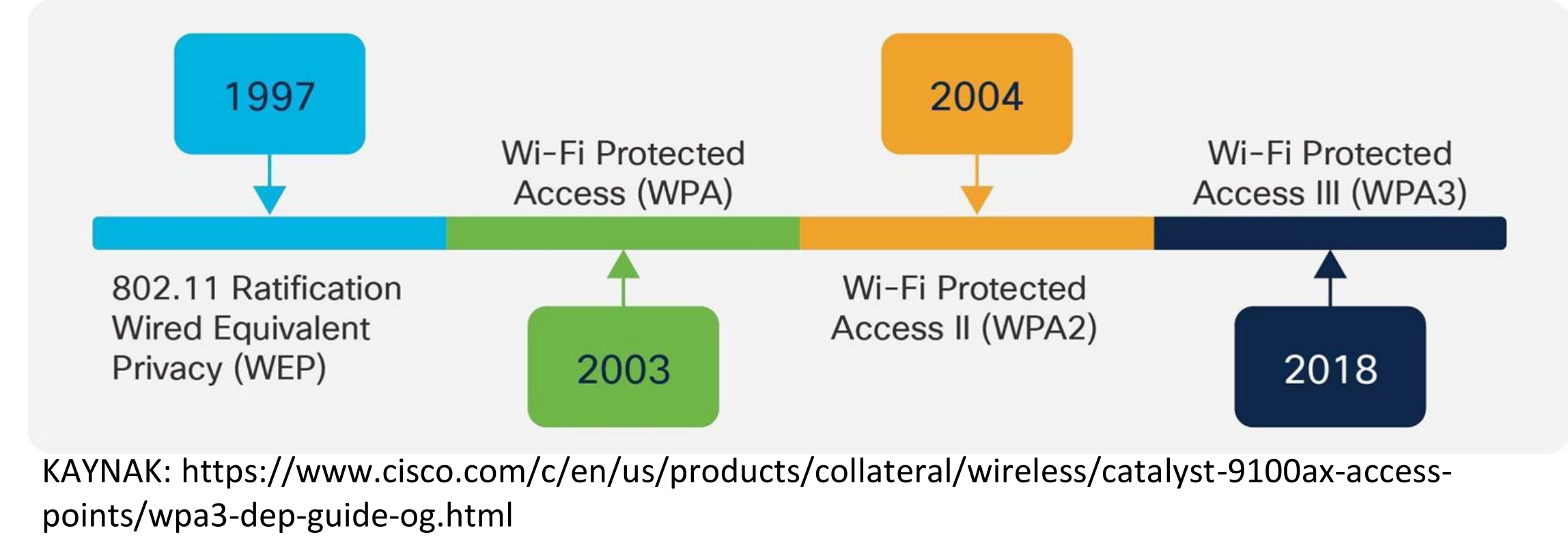
- Kablosuz ağ güvenliği, kablosuz ağları yetkisiz erişim ve siber saldırılardan koruma pratiğini ifade eder.
- Kablosuz ağlar, yaygın olarak kullanıldıkları için güvenlikleri önemlidir çünkü kötü niyetli kişiler veya cihazlar bu ağlara kolayca erişebilirler.
- Kablosuz ağ güvenliği, ağın gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlar.

KABLOSUZ AĞ GÜVENLİĞİ TEMEL PROTOKOLLER : WEP, WPA ve WPA3

Wi-Fi security algorithms comparison

WEP	WPA	WPA2	WPA3
• Earliest security protocol(1999) • Vulnerable, not secure, easily hackable <i>(Wired Equivalent Privacy)</i>	• Uses TKIP (temporal key integrity protocol) • Increased security from WEP <i>(Wi-Fi Protected Access)</i>	• Uses AES(advanced encryption standard) • Very secure, and adopted by the US government	• Most advanced

KAYNAK: <https://www.thetechadvocate.org/wep-wpa-wpa2-or-wpa3-how-to-tell-what-security-type-your-wi-fi-uses/>



- Kablosuz ağ güvenliği, kablosuz (Wi-Fi) ağların yetkisiz erişime karşı korunması ve güvende tutulması anlamına gelir.
- Bu koruma yöntemleri ağ trafiğinin şifrelenmesi ve yetkisiz erişimlere karşı savunma sağlar. Kablosuz ağ güvenliği için kullanılan temel protokoller şunlardır: WEP, WPA ve WPA3.



Bölüm 13

OWASP (Open Web Application Security Project)

OWASP NEDİR?



KAYNAK: <https://blog.kakaocdn.net/dn/5IKzS/btqCwXfSvHC/GSVaRMwSCF5DNsZUkSNSTK/img.png>



- OWASP, "Open Web Application Security Project" kelimelerinin baş harflerinden oluşan bir kısaltmadır ve açık kaynaklı bir topluluk tarafından yönetilen bir projeyi ifade eder.
- OWASP, yazılım ve web uygulamalarının güvenliğini artırmayı amaçlayan bir dizi kaynak ve rehber sunar. OWASP, web uygulama güvenliği alanında dünya genelinde tanınan bir otoritedir.

OWASP NEDİR?



A01:2021
Broken Access
Control



A02:2021
Cryptographic Failures



A03:2021
Injection



A04:2021
Insecure Design



A05:2021
Security Misconfiguration



A06:2021
Vulnerable & Outdated
Components



A07:2021
Identification &
Authentication Failures



A08:2021
Software & Data
Integrity Failures



A09:2021
Security Logging &
Monitoring Failures



A10:2021
Server-Side Request
Forgery

KAYNAK: <https://www.sprocketsecurity.com/resources/owasp-top-10-risks-of-2022>

- OWASP, geliştiricilere, güvenlik profesyonellerine ve organizasyonlara aşağıdaki konularda yardımcı olur:

Güvenli Uygulama Geliştirme
Siber Tehditlere Karşı Koruma
Eğitim ve Bilinçlendirme

KİMLER KULLANIR VE ÖNEMİ NEDİR?

OWASP API Security Top-10 2019		OWASP API Security Top-10 2023
API1 Broken Object Level Authorization		API1 Broken Object Level Authorization
API2 Broken User Authentication		API2 Broken Authentication
API3 Excessive Data Exposure		API3 Broken Object Property Level Authorization
API4 Lack of Resources & Rate Limiting		API4 Unrestricted Resource Consumption
API5 Broken Function Level Authorization		API5 Broken Function Level Authorization
API6 Mass Assignment		API6 Unrestricted Access to Sensitive Business Flows
API7 Security Misconfiguration		API7 Server-Side Request Forgery (SSRF)
API8 Injection		API8 Security Misconfiguration
API9 Improper Assets Management		API9 Improper Inventory Management
API10 Insufficient Logging & Monitoring		API10 Unsafe Consumption of APIs

Removed Updated New

KAYNAK: <https://appsentinels.ai/blog/owasp-api-top-10-2023-what-changed-and-why-its-important/>

- OWASP kaynakları, yazılım geliştiricileri, siber güvenlik profesyonelleri, bilgi güvenliği uzmanları ve organizasyonlar tarafından kullanılır.
- Güvenli yazılım geliştirme uygulamalarını benimsemek, organizasyonların siber saldırılardan kaynaklanan veri sızıntıları ve maddi kayıpları önlemelerine yardımcı olabilir.
- OWASP, yazılım güvenliği için bir standart oluşturur ve bu nedenle büyük bir öneme sahiptir.



Bölüm 14

GÜVENLİK AMAÇLI KOD ANALIZI (STATİK VE DİNAMİK)

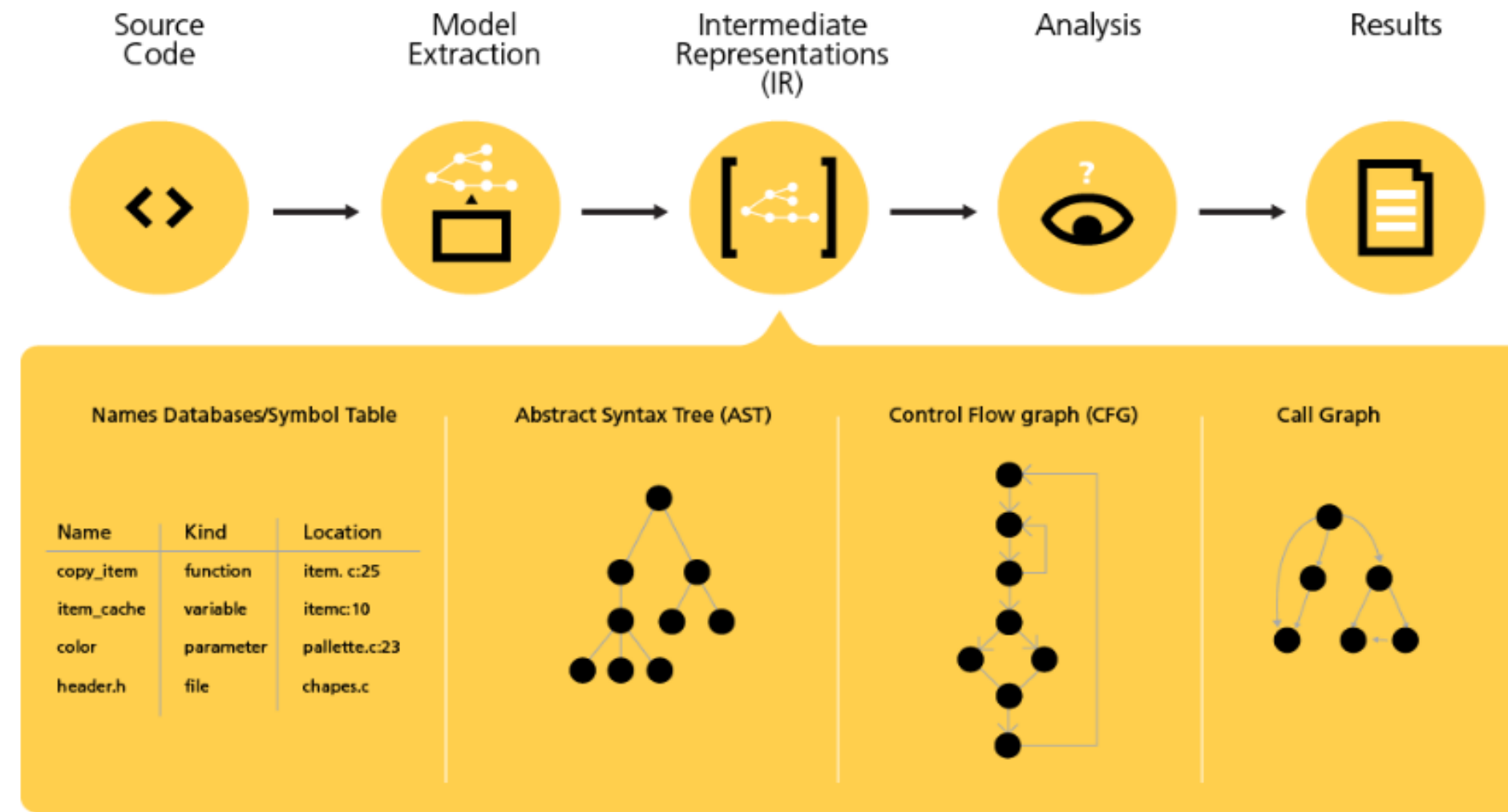
GÜVENLİK AMAÇLI KOD NEDİR?



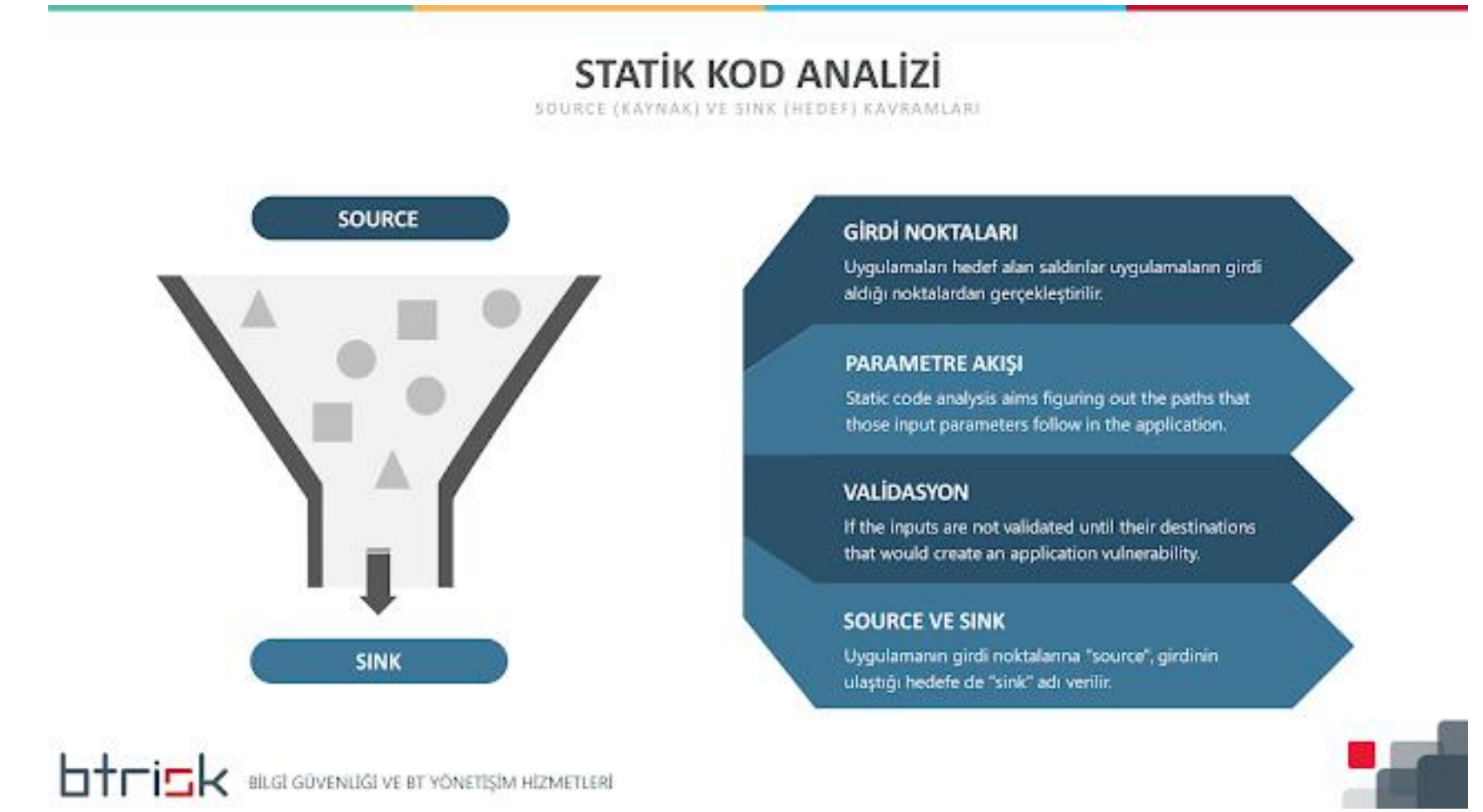
- Güvenlik amaçlı kod, yazılım geliştirme sürecinde güvenlik açıklarını tespit etmek ve önlemek amacıyla eklenen programlama kodlarını ifade eder. Bu kodlar, yazılımın siber saldırılara ve güvenlik ihlallerine karşı daha dayanıklı olmasını sağlar.
- Güvenlik amaçlı kodlama uygulamaları, yazılımın zayıf noktalarını tespit eder ve düzeltilmesine yardımcı olur.



GÜVENLİK AMAÇLI KOD ANALİZİ NEDİR?



KAYNAK: <https://sourceforge.net/software/compare/CodeSonar-vs-ReSharper/>



KAYNAK: <https://www.btrisk.com/statik-kod-analizi-nedir/>

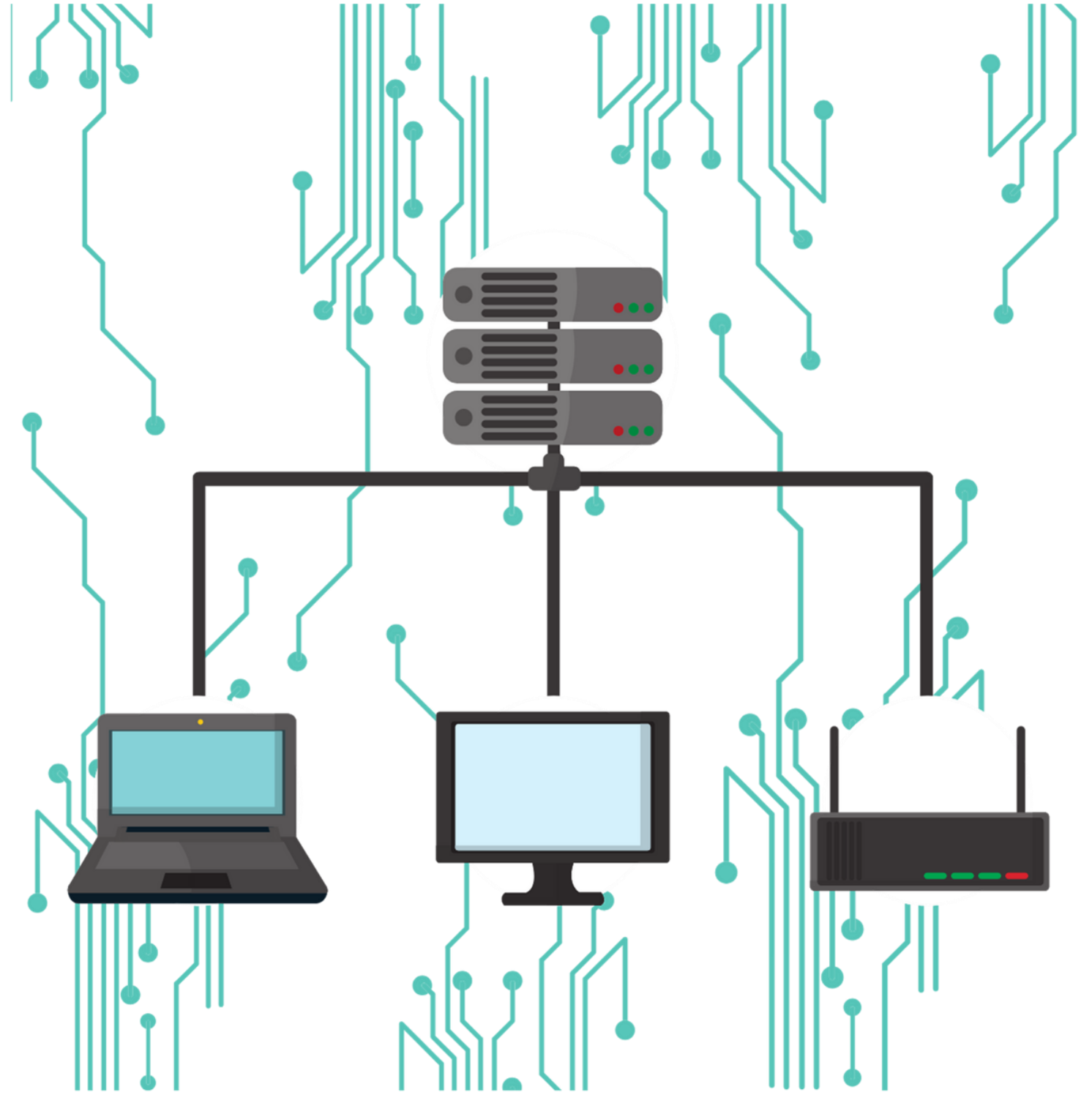
- **Statik Kod Analizi:** Bu, yazılımın kaynak kodunun incelemesiyle gerçekleştirilen bir güvenlik testidir.
- Otomatik analiz araçları kullanılarak kod üzerinde potansiyel güvenlik açıkları ve hatalar tespit edilir.
- Bu analiz, kodun yazılım geliştirme aşamasında yapıldığı için daha erken tespit ve düzeltme imkanı sağlar.

GÜVENLİK AMAÇLI KOD ANALİZİ NEDİR?



- **Dinamik Kod Analizi:** Bu, yazılımın çalışma zamanında test edilmesini içerir.
- Uygulama çalışırken güvenlik açıkları ve zayıf noktalar test edilir.
- Bu analiz, uygulamanın gerçek dünya koşullarında nasıl davrandığını değerlendirmeye yardımcı olur.

KMLER KULLANIR VE ÖNEMİ NEDİR?



- Güvenlik amaçlı kod analizi, yazılım geliştiricileri, siber güvenlik uzmanları ve organizasyonların güvenlik ekipleri tarafından kullanılır.
- Bu analizlerin önemi şunlardır:
 1. Güvenlik Açıklarının Erken Tespiti
 2. Saldırılara Karşı Direnç
 3. Veri Koruma

NASIL UYGULANIR?



KAYNAK: https://media.licdn.com/dms/imAĞe/D4D12AQEY-CoN4SegtA/article-inline_imAĞe-shrink_1500_2232/0/1677153390836?e=1700697600&v=beta&t=PS065NWTiqtgGZOmX4jaBAtyhZErINTJjUt_tRarziQ

- **Statik Kod Analizi:** Statik kod analizi araçları kullanılarak yazılımın kaynak kodu taranır. Bu araçlar, potansiyel güvenlik açıkları ve hataları tespit ederler. Örnek araçlar arasında "Fortify" ve "Checkmarx" bulunur.
- **Dinamik Kod Analizi:** Uygulama çalıştırılır ve güvenlik açıkları simüle edilir. Bu testler sırasında uygulamanın yanıtı ve davranışı izlenir. Örnek araçlar arasında "Burp Suite" ve "Nessus" yer alır.

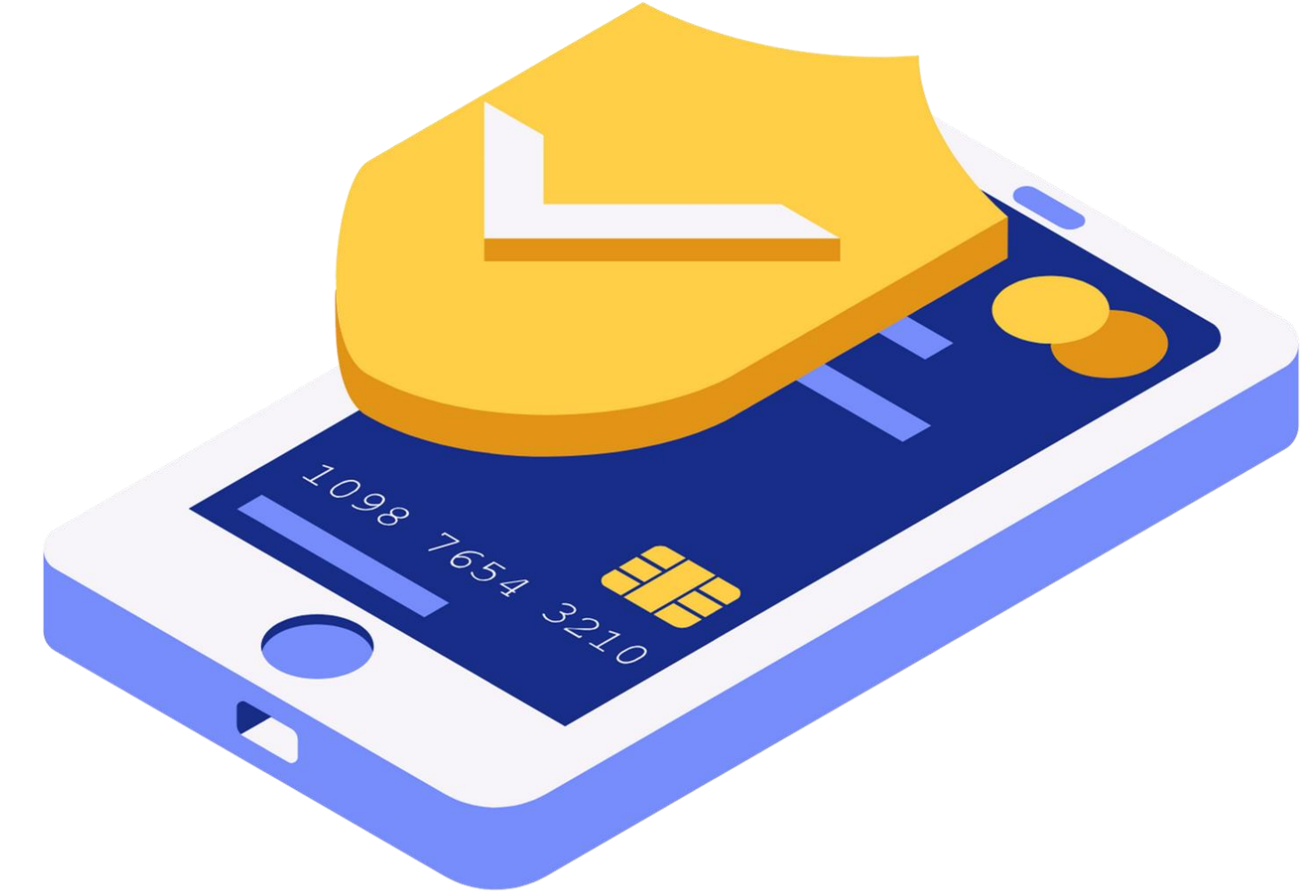
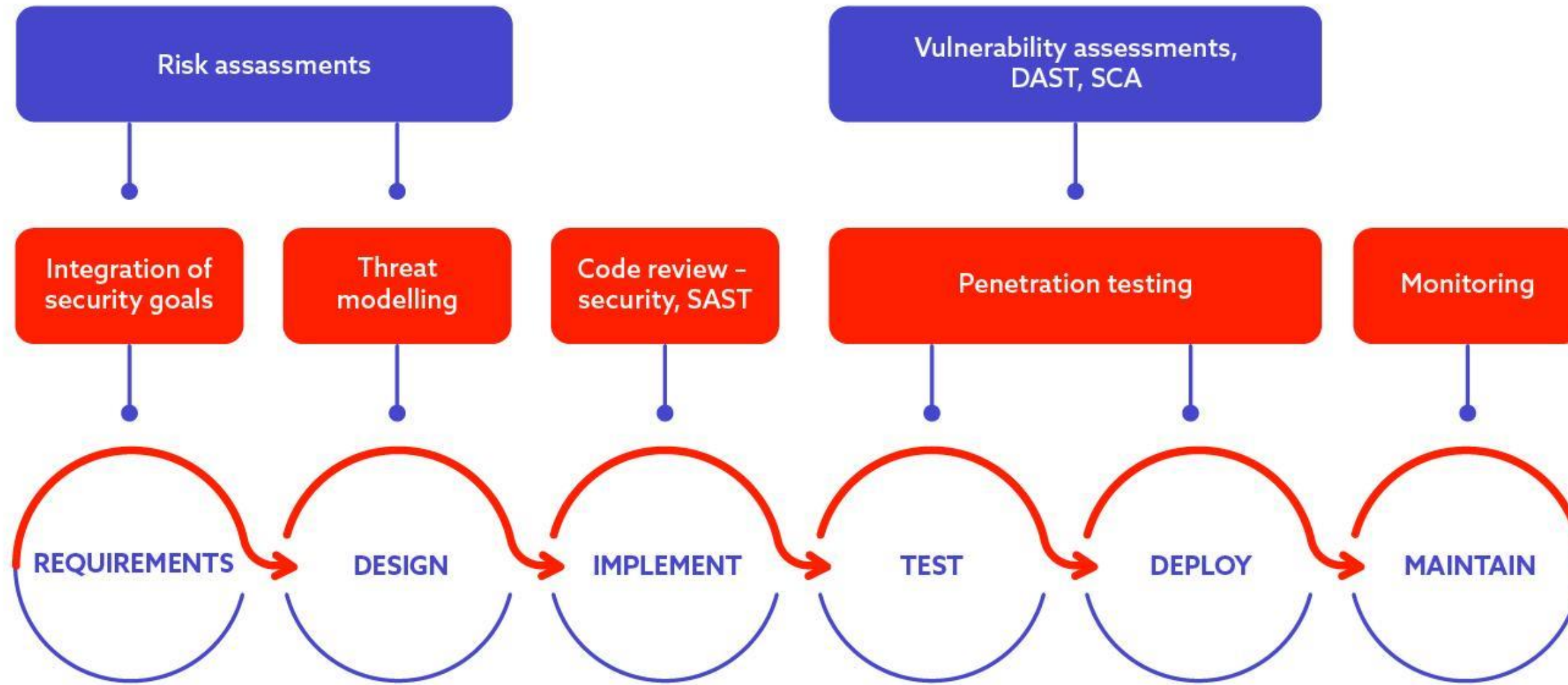


Bölüm 15

GÜVENLİ YAZILIM GELİŞTİRME YASAM DÖNGÜSÜ (SSDLC)

GÜVENLİ YAZILIM GELİŞTİRME YAŞAM DÖNGÜSÜ (SSDLC) NEDİR?

Secure software development lifecycle (SSDLC)

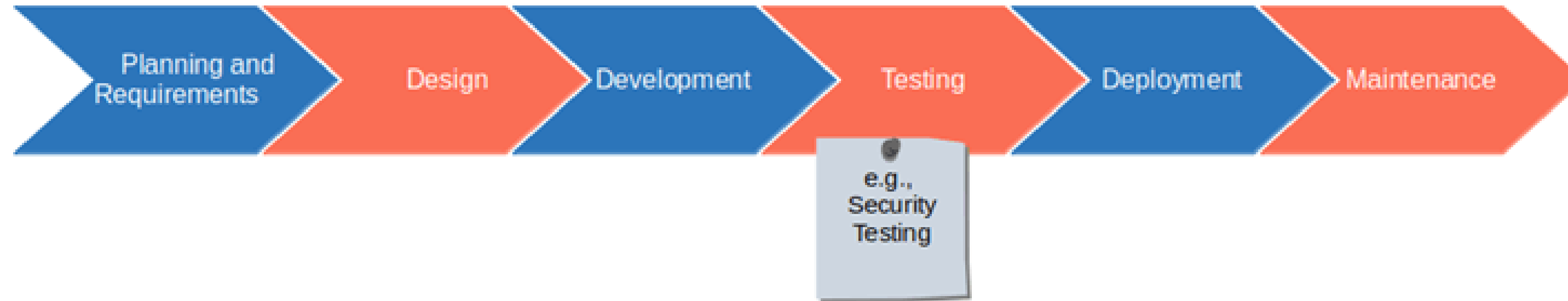


KAYNAK: <https://spyro-soft.com/blog/secure-software-development-lifecycle-ssdlc-why-is-it-important>

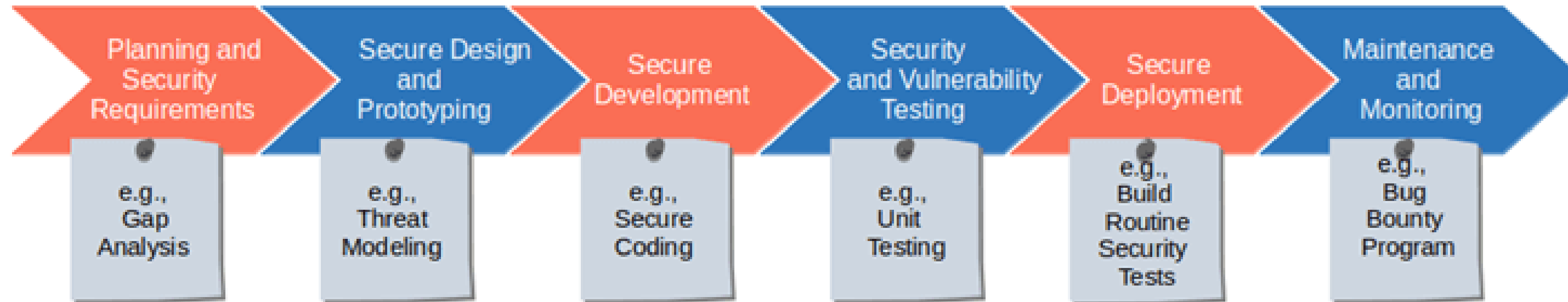
- Güvenli Yazılım Geliştirme Yaşam Döngüsü (Software Security Development Life Cycle - SSDLC), yazılım geliştirme sürecinin her aşamasında güvenlik önlemlerinin ve uygulamalarının entegre edilmesini sağlayan bir metodoloji veya süreçtir.
- SSDLC, yazılımın tasarımından başlayarak kodlama, test, yayınlama ve bakım aşamalarını içerir ve güvenlik açıklarının erken tespitini ve düzeltilmesini hedefler.

SSDLC NE İŞE YARAR?

Software Development Life Cycle (SDLC) Process



Secure Software Development Life Cycle (SSDLC) Process



- Güvenlik açıklarının erken tespiti: Yazılım geliştirme sürecinin her aşamasında güvenlik değerlendirmeleri yaparak potansiyel tehditleri erken tespit eder.
- Yazılım güvenliği kültürünü teşvik eder: Geliştiricilerin ve diğer ekip üyelerinin yazılım güvenliği konusunda bilinçlenmelerine ve eğitilmelerine yardımcı olur.



Bölüm 16

SİBER RİSKLER RİSK YÖNETİMİ (SİBER RİSKLERİN YÖNETİMİ)

SİBER RİSKLER

- Siber riskler, bilgi teknolojileri ve internetin kullanımıyla ilişkilendirilen potansiyel tehlikeleri ifade eder.

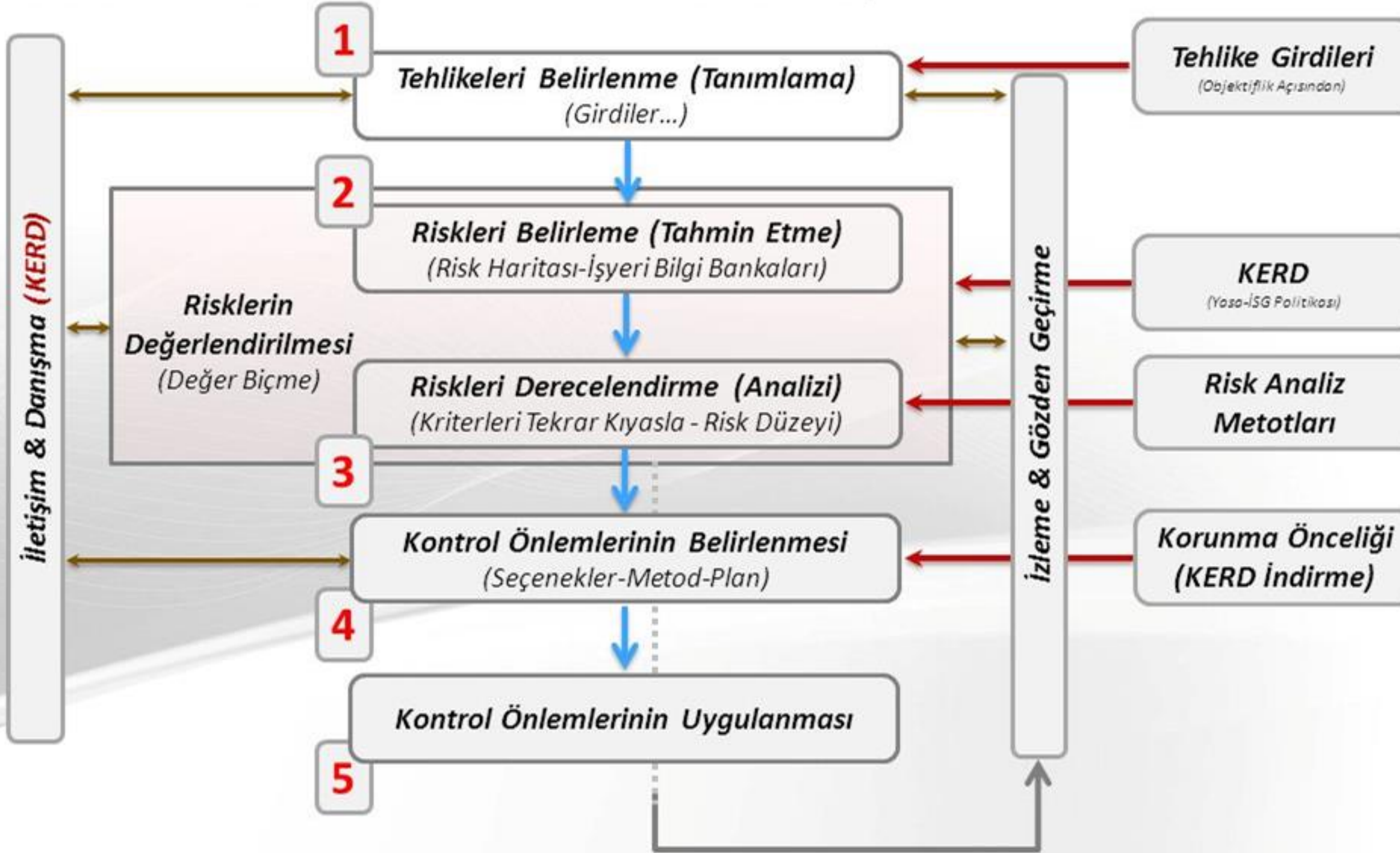
İşte siber risklerin bazıları:

1. Veri Sızıntısı Örnek: Bir kuruluşun müşteri bilgilerinin sızdırılması.
2. Malware (Kötü Amaçlı Yazılım) Örnek: Bir ransomware saldırısı.
3. Phishing Örnek: Bir çalışanın sahte bir e-postaya tıklaması.
4. DDoS Saldırısı Örnek: Bir e-ticaret sitesinin saldırıya uğraması ve erişilemez hale gelmesi.
5. İç Tehditler Örnek: İçeriden bir saldırganın gizli bilgilere erişimi.



SİBER RİSKLER

RİSK YÖNETİM PROSESİ-SÜRECİ / GENEL



- Risk yönetimi, organizasyonların karşılaştığı riskleri tanımlama, analiz etme, değerlendirme, azaltma veya kabul etme sürecini ifade eder.
- Siber risk yönetimi, organizasyonların siber tehditleri ve riskleri belirlemesine, bu riskleri azaltmasına veya kabul etmesine ve uygun güvenlik önlemlerini uygulamasına yardımcı olur.

KİMLER KULLANIR VE ÖNEMİ NEDİR?



NIST Cyber Security Framework

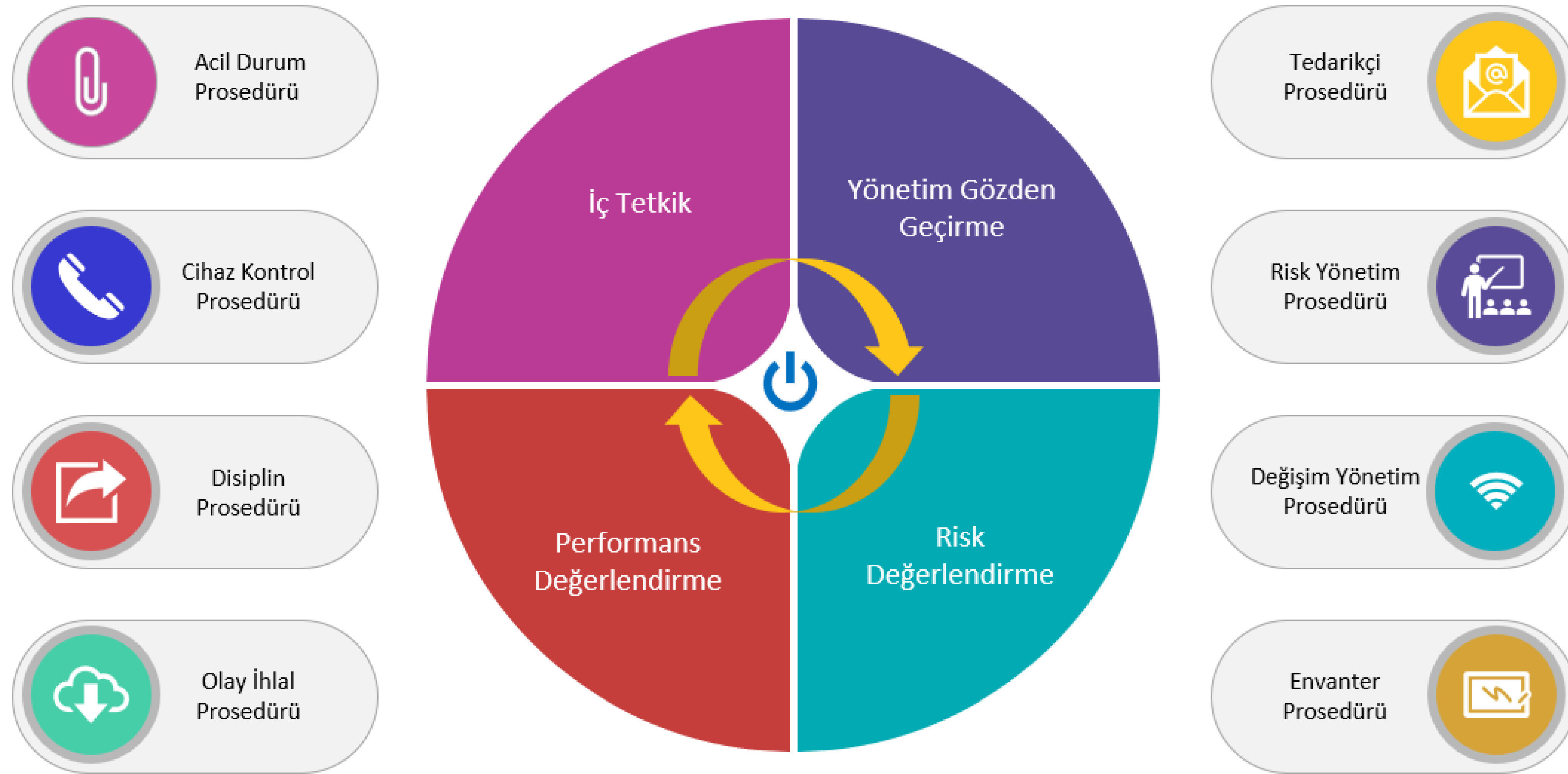


KAYNAK: <https://www.wallarm.com/what/nist-cybersecurity-framework-csf>

- Siber risk yönetimi, tüm organizasyonlar için önemlidir, özellikle büyük kuruluşlar, finans kurumları ve sağlık sektörü gibi hassas verilere sahip olanlar için daha kritiktir.
- Bilgi güvenliği profesyonelleri, risk yöneticileri ve üst düzey yöneticiler siber risk yönetimi süreçlerini uygular.

TSE ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ STANDARDI

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Prosedürleri



- Türk Standartları Enstitüsü (TSE) tarafından kabul edilen bu standart, Türkiye'de bilgi güvenliği için en yaygın olarak kullanılan standarttır.
- ISO/IEC 27001, bilgi güvenliği yönetim sistemi kurmak ve sürdürmek isteyen organizasyonlar için rehberlik sunar.

KVKK

Kişisel Veri Nedir?

Kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veridir.

- Ad - Soyad
- Doğum Tarihi/Yeri
- Anne Kızlık Soyadı
- Medeni durumu
- Ana/Baba adı
- Cinsiyet

Kimlik Bilgileri

- Özgeçmiş
- Mesleki bilgileri
- SGK Bilgileri
- Disiplin cezaları
- Askerlik bilgisi
- Adli sicil bilgisi

Özlük

- Telefon
- Adres
- E-Posta
- KEP Adresi

İletişim

- Kazanç
- Harcama/Vergi
- Malvarlığı/Yatırım
- Sigorta/Banka/Kart Bilgileri-Hareketleri
- Kredi Oranları,

Finans

- IP Adres
- SSID
- IMEI
- BLUETOOTH ID
- MAC Adresi

İşlem Güvenliği

- Güvenlik kamerası
- İşe giriş-çıkış kayıtları
- Araç plakası

Fiziksel Mekan Güvenliği

- Alışveriş Geçmişi
- Alışkanlık raporları, kampanya bilgileri
- İstatistiki analizler
- Pazarlama anketleri
- Cerez kayıtları

Pazarlama Bilgileri

- Fotoğraf
- Ses kaydı
- Kamera kaydı (mülakat, etkinlik vb.)

Görsel ve İşitsel Kayıtlar

- Kurumsal telefon görüşmesi kayıtları
- Kurumsal e-posta yazışmaları
- İnternet erişim logları

Haberleşme Kayıtları

- GPS
- HGS/OGS geçişleri
- Taşıt tanıma
- Yemek kartından konum bilgisi

Lokasyon



KAYNAK:

https://commons.wikimedia.org/wiki/File:KVKK_logo.svg

- Türkiye'de kişisel verilerin korunmasını düzenleyen bu kanun, siber güvenlikle de ilgilidir.
- Organizasyonlar, kişisel verilerin güvenliğini sağlamak için çeşitli siber güvenlik önlemleri almak zorundadır.



Bölüm 18

SİBER GÜVENLİK ALANINDAKİ ULUSLARARASI SERTİFİKALAR

OFFENSIVE SECURITY (OSWE,OSCE,OSCP,OSWP)

- Offensive Security, siber güvenlik alanında eğitim ve sertifikasyon programları sunan bir şirkettir. Offensive Security'nin sunduğu bazı önemli sertifikalar şunlardır:
- **OSCP (Offensive Security Certified Professional):** OSCP, Offensive Security'in en popüler ve tanınmış sertifikasıdır.
- **OSCE (Offensive Security Certified Expert):** OSCE, bilgisayar güvenliği uzmanlarının bilgisayar sistemlerine sızma testleri yapma yeteneklerini daha derinlemesine göstermelerine olanak tanır.
- **OSWE (Offensive Security Web Expert):** OSWE sertifikası, web uygulamalarının güvenliğini test etme ve web uygulama sızma testleri yapma yeteneklerini ölçer.
- **OSWP (Offensive Security Wireless Professional):** OSWP sertifikası, kablosuz ağ güvenliği ile ilgilenen kişilere yöneliktir.



KAYNAK: <https://www.offsec.com/wp-content/uploads/2022/10/Artboard-1@2x.png>

CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL)

- CISSP, bilgi sistemleri güvenliği profesyonelleri için dünya genelinde tanınmış bir sertifikadır.
- Bilgi güvenliği yönetimi, risk yönetimi, güvenlik mimarisi ve diğer konularda uzmanlaşmış profesyonellere yöneliktir.



Certified Information
Systems Security Professional

KAYNAK: <https://www.cm-alliance.com/cissp-training-faqs>

CEH (CERTIFIED ETHICAL HACKER)



- CEH sertifikası, etik hackerlar için tasarlanmıştır.
- Bu sertifika, ağları güvenlik açıklarını tespit etmek ve kapatmak için yetenekli hale getirmek isteyen profesyoneller için geçerlidir.

COMPTIA SECURITY+



- CompTIA Security+, temel siber güvenlik kavramlarını ve uygulamalarını kapsayan bir sertifikadır.
- Bu sertifika, siber güvenlik kariyerine yeni başlayanlar veya temel bilgiye sahip olanlar için uygundur.

KAYNAK: <https://www.innovativelearning.eu/products/comptia-cybersecurity/comptia-security.html>

CCNA CYBEROPS (CISCO CERTIFIED NETWORK ASSOCIATE - CYBEROPS)



- CCNA CyberOps, ağ güvenliği ve siber güvenlik alanlarında uzmanlaşmak isteyen ağ profesyonelleri için Cisco tarafından sunulan bir sertifikadır.



KAYNAK: <https://www.fccmeredith.org/ccna-cyber-ops-certification>

CERTIFIED CLOUD SECURITY PROFESSIONAL (CCSP)



Certified Cloud
Security Professional

An (ISC)² Certification

- CCSP, bulut bilişim güvenliği uzmanları için tasarlanmış bir sertifikadır.
- Bulut ortamında güvenliği sağlamak için gereken bilgi ve becerileri ölçer.

KAYNAK: <https://cycubix.com/2022/04/04/isc2-ccsp-martina-costello/>



Bölüm 19

SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Bilgi Güvenliği Uzmanı (Information Security Specialist):

- Güvenlik duvarlarını yapılandırır, güvenlik yazılımını güncellerler.

Ağ Güvenliği Mühendisi (Network Security Engineer):

- Ağ içi iletişimin güvenli bir şekilde gerçekleştiğinden emin olurlar.
- DoS saldırılarına karşı savunma önlemleri geliştirirler.

Sızma Testi Uzmanı (Penetration Tester):

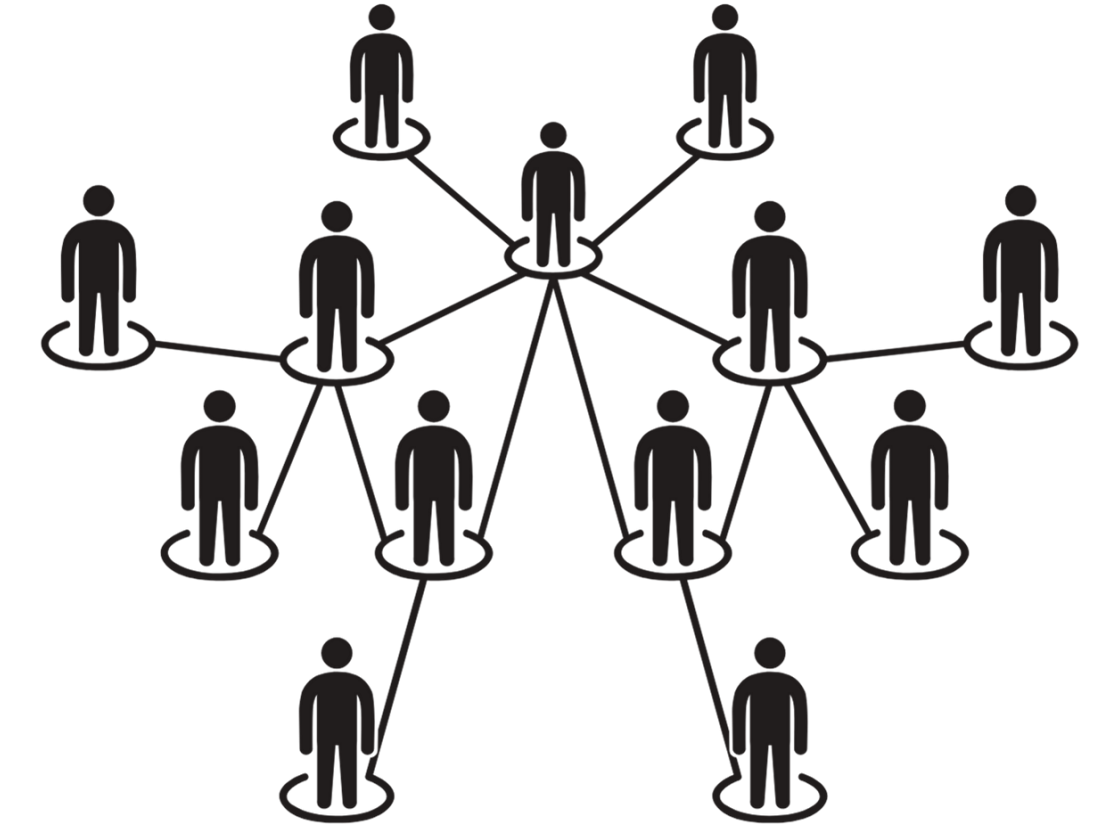
- Örneğin, organizasyonun web uygulamasında açıklar bularak güvenlik zafiyetlerini ortaya çıkarırlar.

Güvenlik Analisti (Security Analyst):

- Örneğin, bir kullanıcının hesabının ele geçirilmesini tespit edip bu olayı incelerler.

Kimlik ve Erişim Yönetimi Uzmanı (Identity and Access ManAĞement Specialist):

- Örneğin, bir işletme için tek oturum açma (Single Sign-On) sistemini uygularlar.



SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Veri Güvenliği Analisti (Data Security Analyst):

- Bir sağlık kurumu için hastaların tıbbi kayıtlarının güvenliğini sağlarlar.

Güvenlik Mimar (Security Architect):

- Bulut tabanlı bir hizmetin güvenliğini sağlamak için mimari planlar hazırlarlar.

Olay Yanıtı Uzmanı (Incident Response Specialist):

- Bir fidye yazılım saldırısına karşı hızlı bir kurtarma planı oluştururlar.

Uygulama Güvenliği Uzmanı (Application Security Specialist):

- Bir e-ticaret sitesinin web uygulamasının güvenliğini denetlerler.

Eğitim ve Farkındalık Uzmanı (Training and Awareness Specialist):

- Sahte e-posta kampanyaları düzenleyerek çalışanların dikkatini çekerler.



SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Yazılım Geliştirme Güvenliği Danışmanı (Secure Development Consultant):

- Yazılım geliştiricilere güvenlik açıklarını düzeltme konusunda rehberlik ederler.

Güvenlik Denetçisi (Security Auditor):

- Bir finans kuruluşunun güvenlik prosedürlerini denetlerler.

Mobil Uygulama Güvenliği Uzmanı (Mobile Application Security Specialist):

- Bir bankanın mobil bankacılık uygulamasının güvenliğini test ederler.

Güvenlik Ekip Lideri (Security Team Leader):

- Bir büyük organizasyonun güvenlik ekibinin liderliğini yaparlar.

Veri Gizliliği Danışmanı (Data Privacy Consultant):

- GDPR gibi düzenlemelere uyum sağlamak için bir şirkete danışmanlık yaparlar.



SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Endüstriyel Kontrol Sistemleri Güvenliği Uzmanı (Industrial Control Systems Security Specialist):

- Bir enerji santralinin ICS güvenliğini sağlarlar.

Blockchain Güvenliği Uzmanı (Blockchain Security Specialist):

- Bir kripto borsasının güvenliğini sağlarlar.

Yapay Zeka ve Makine Öğrenimi Güvenliği Uzmanı (AI and Machine Learning Security Specialist):

- Bir sağlık kuruluşu için hastaların sağlık verilerini korurken yapay zeka kullanırlar.

Uygulama Penetrasyon Testi Uzmanı (Application Penetration Testing Specialist):

- Bir e-ticaret uygulamasının güvenliğini test ederler.

Dijital Tehdit Analisti (Digital Threat Analyst):

- Bir siber casusluk saldırısını inceleyerek kimin arkasında olduğunu belirlerler.



SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR



Veri Analitiği ve Güvenlik Uzmanı (Data Analytics and Security Specialist):

- Veri madenciliği teknikleriyle güvenlik olaylarını önceden tahmin ederler.

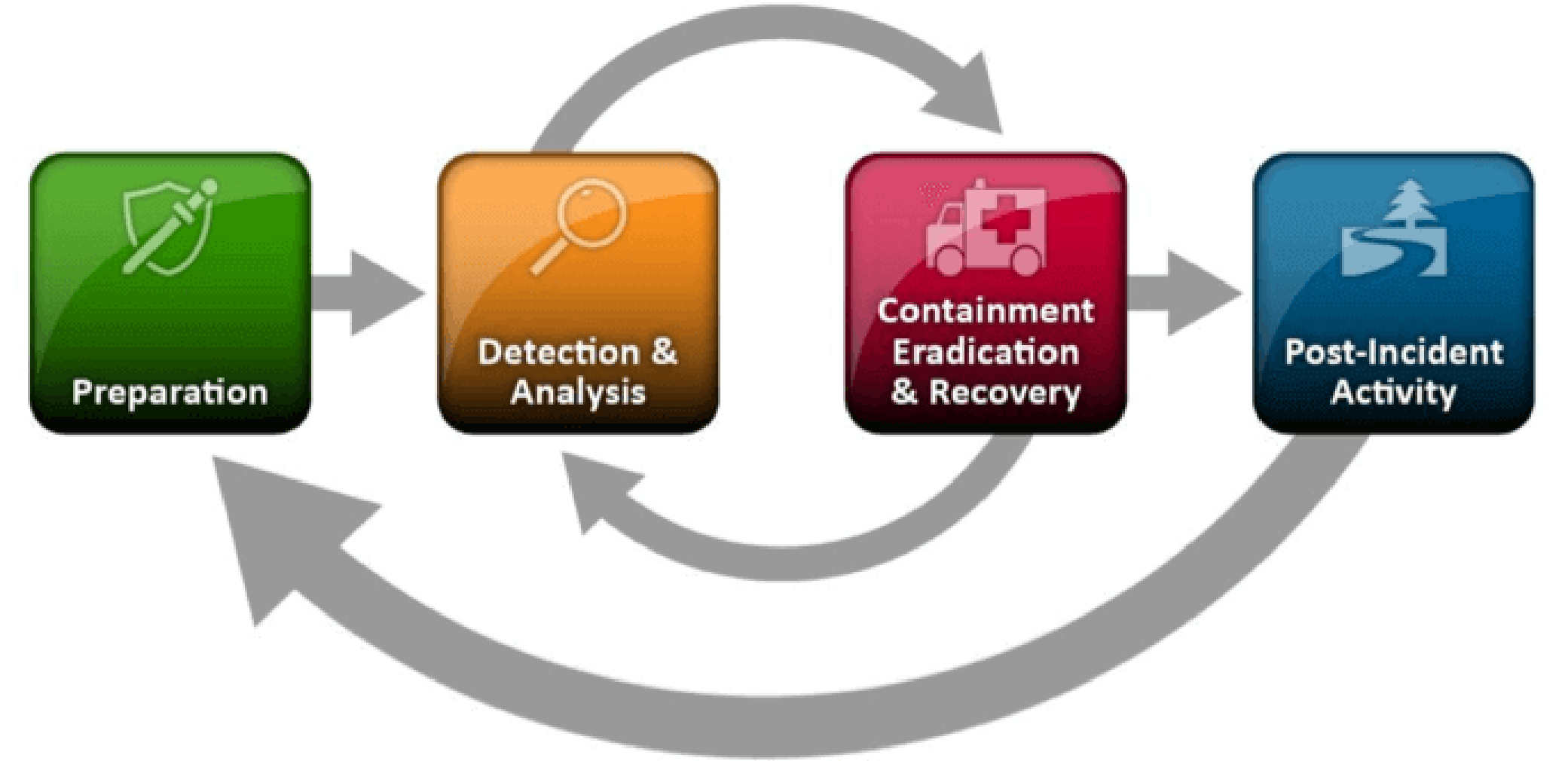
Siber Hukuk Uzmanı (Cybersecurity Lawyer):

- Bir şirketin bir veri ihlali sonucu maruz kaldığı yasal sorunları ele alırlar.



SOME (SİBER OLAYLARA MÜDAHALE EKİBİ)

- **SOME (Siber Olaylara Müdahale Ekibi)**, bir organizasyonun veya kurumun siber güvenliği ile ilgili olayları izlemek, tespit etmek, analiz etmek, yanıtlamak ve çözmek için kurulan bir ekiptir.
- Bu ekip, siber tehditlere karşı savunma sağlamak, olayları hızla çözmek ve potansiyel olarak zararlı etkileri en aza indirmek **amacıyla** çalışır.



KAYNAK: <https://www.barikatbv.com/services/csirt-services>

SOME (SİBER OLAYLARA MÜDAHALE EKİBİ)

SOME ekibi genellikle aşağıdaki **görevleri** yerine getirir:

- **Olay Tespiti:** SOME ekibi, ağlarını ve sistemlerini sürekli olarak izler ve potansiyel siber tehditleri tespit etmek için güvenlik olaylarını analiz eder.
- **Olay Analizi:** Ekip, tespit edilen olayları ayrıntılı bir şekilde analiz eder.
- **Olay Yanıtı:** SOME ekibi, bir siber olay tespit edildiğinde hızla yanıt verir.
- **Olayın Düzgün Kayıt Altına Alınması:** Ekip, tüm olayları ve müdahale süreçlerini ayrıntılı bir şekilde kayıt altına alır.

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

CSIRT Components



KAYNAK:

<https://www.wallsec.com.tr/cozumlerimiz/danismanlik/some-siber-olaylara-mudahale-ekibi/>

SOME (SİBER OLAYLARA MÜDAHALE EKİBİ)

- SOME ekibi, organizasyonların siber güvenliğini artırmak ve siber saldırılara karşı dirençli olmalarını sağlamak için çok önemlidir.

Önemli nedenler şunlar olabilir:

- **Siber Tehditlere Hızlı Yanıt:** SOME ekipleri, siber saldırıları hızla tespit edebilir ve yanıtlayabilir, bu da organizasyonların potansiyel olarak büyük zararları en aza indirmelerine yardımcı olur.
- **Veri ve Varlık Koruması:** SOME ekipleri, organizasyonların hassas verilerini ve diğer varlıklarını koruma görevini üstlenir. Bu, veri sızıntıları ve kayıplarının önlendiği anlamına gelir.
- **Siber Güvenlik Farkındalığı:** SOME ekibi, organizasyonun siber güvenlik farkındalığını artırır ve güvenlik politikalarını uygulamak için en iyi uygulamaları teşvik eder.
- **Uzun Vadeli Öğrenme:** SOME ekipleri, saldırılar hakkında bilgi toplar ve bu bilgileri gelecekteki olaylara karşı hazırlık olarak kullanır. Bu, organizasyonun siber güvenlik savunmasını sürekli olarak güçlendirmeye yardımcı olur.



KAYNAK:

<https://www.barikat.com.tr/hizmetler/olay-mudahale-hizmeti>

SOME EKİBİNDE ÇALIŞANLARA ÖRNEKLER

Temel Yetenek	Eğitimler
Açıklık Analizi	- Temel Güvenlik Denetim Eğitimi - Sistem Güvenlik Denetim Eğitimi - Sızma Testleri Eğitimi - Saldırı Teknikleri Eğitimi
Kayıt Yönetimi	- Saldırı Tespit Sistemi Eğitimi - Kayıt Yönetimi Eğitimi - Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi
Siber Olay Müdahale	- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi - Bilgi Sistemleri Adli Analizi Eğitimi - Bilgisayar Adli Analizi – Derinlemesine Windows Eğitimi - Karşı Adli Bilişim Eğitimi - İleri Bilgisayar Adli Analizi ve Olay Müdahale Eğitimi - Ağ Adli Analizi Eğitimi - Zararlı Yazılım Analiz Yöntemleri Eğitimi - DDoS Saldırıları ve Korunma Yolları Eğitimi - Bilişim Hukuku
Bilgi Güvenliği Yönetimi	- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi - ISO 22301 İş Sürekliliği / Felaket Kurtarım Planlaması Eğitimi

- **Siber Güvenlik Analisti:** Olayları izler ve analiz eder, yanıt planlarını uygular.
- **Siber Tehdit Avcısı:** Gelişmiş tehditleri tespit eder ve izler.
- **Kriz Yöneticisi:** Büyük olayların kriz yönetimini sağlar.
- **Siber Güvenlik Eğitmeni:** Çalışanları güvenlik konusunda eğitir ve farkındalık programları düzenler.

KAYNAK: <https://www.bgasecurity.com/2018/11/some-siber-olaylara-mudahale-ekibi-nedir/>

Temel Yetenek	Eğitimler	Eğitimden Beklenen Faydalar
Zafiyet Analizi	- Güvenli Yapılandırma Denetimi Eğitimi - Sızma Testleri Eğitimi - Saldırı Teknikleri Eğitimi	Kurumsal SOME personelinin bir siber olay gerçekleşmeden önce sistemlerindeki önemli zafiyetleri tespit etmesi ve karşı önlem uygulamasını koordine etmesi için gerekli yetenekleri kazanması
Kayıt Yönetimi	- Saldırı Tespit ve Kayıt Yönetimi Eğitimi - Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi	Kurumsal SOME personelinin sistemdeki kayıtları takip edebilmesi, sistemler ve tehditler ile ilgili farkındalık kazanabilmesi
Siber Olay Müdahale	- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi - Bilişim sistemleri Adli Analizi Eğitimi - Bilgisayar Adli Analizi - Derinlemesine Windows Eğitimi - Ağ Adli Analizi Eğitimi - Zararlı Yazılım Analiz Yöntemleri Eğitimi - DDoS Saldırıları ve Korunma Yolları Eğitimi - Bilişim Hukuku Eğitimi	Bir siber olay gerçekleşmesi durumunda gerekli olacak olay yönetimi ve koordinasyonu yeteneklerinin kazanılması, dijital delillerin geçerliliğinin bozulmaması için alınacak tedbirlerin öğrenilmesi. Adli analiz esasen kolluk makamının görevi olmakla birlikte, kurumların “sistem izleme” ve “kayıt yönetimi” kapsamında giriş seviyesinde adli analiz bilgisine sahip olması gerekmesi.
Bilgi Güvenliği Yönetimi	- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi	Bilgi güvenliği/siber güvenlik sürecinin kavratılması ve Bilgi Güvenliği Yönetim Sistemi ile ilgili farkındalık oluşması.

SOC (GÜVENLİK OPERASYON MERKEZİ)



KAYNAK: <https://cetark.com/soc.html>

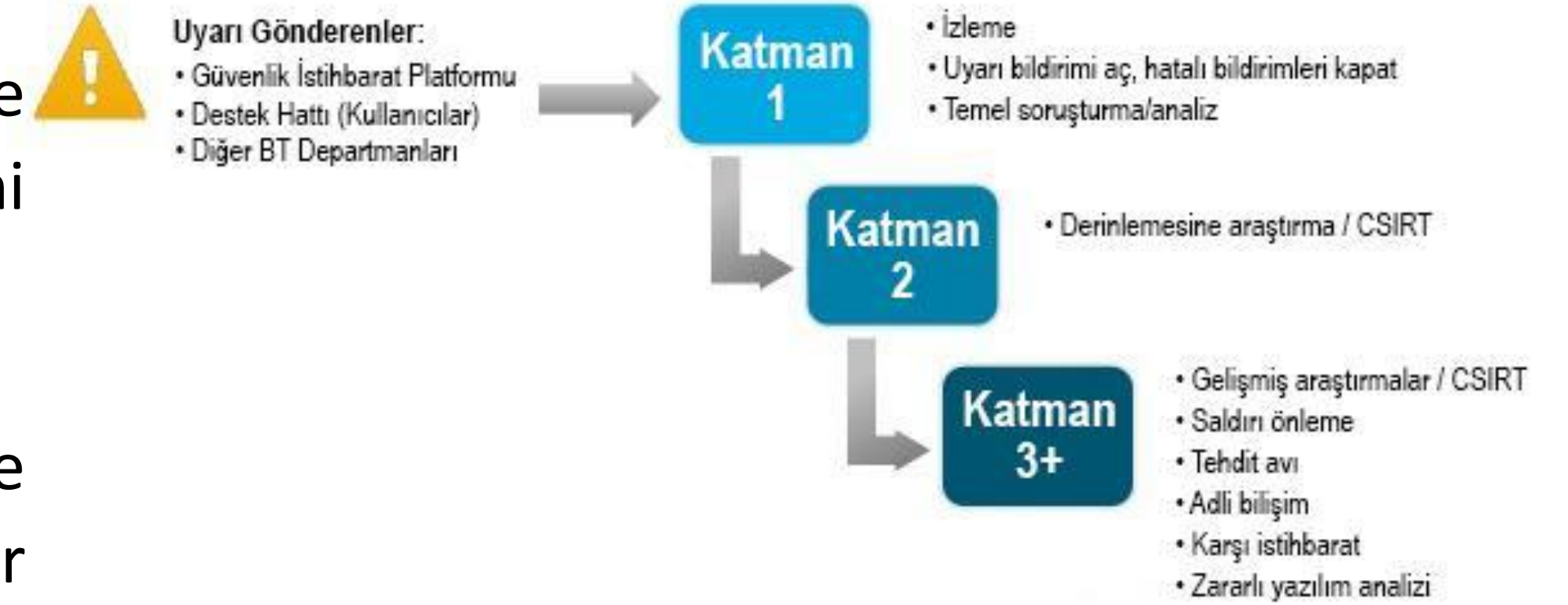
- **SOC (Güvenlik Operasyon Merkezi)**, bir organizasyonun veya kurumun siber güvenliği ile ilgili sürekli izleme, tehdit tespiti, yanıt verme ve güvenlik olaylarını yönetme **amacıyla** kurulan bir merkezdir.
- SOC, siber tehditlere karşı savunma sağlamak ve siber güvenliği artırmak için tasarlanmış bir operasyonel birimdir.

SOC (GÜVENLİK OPERASYON MERKEZİ)

Görevleri:

- **Siber Tehdit İzleme:** SOC, organizasyonun bilgisayar ağları ve sistemlerini sürekli olarak izler ve siber tehditlerin erken tespitini sağlar.
- **Tehdit Analizi:** SOC, tespit edilen tehditleri analiz eder ve bunların ne kadar ciddi olduğunu ve organizasyona ne tür zararlar verebileceğini belirlemeye çalışır.
- **Olay Yanıtı:** SOC, siber güvenlik olaylarını hızla yanıtlar. Tehditlerin etkisini sınırlamak ve organizasyonun sistemlerini korumak için gerekli aksiyonları alır.
- **Olay Kayıt ve Raporlama:** SOC, tüm güvenlik olaylarını ayrıntılı bir şekilde kayıt altına alır ve bu kayıtları organizasyonun yasal gereksinimlerine ve raporlama ihtiyaçlarına uygun olarak saklar.

Basitleştirilmiş SOC Katmanları



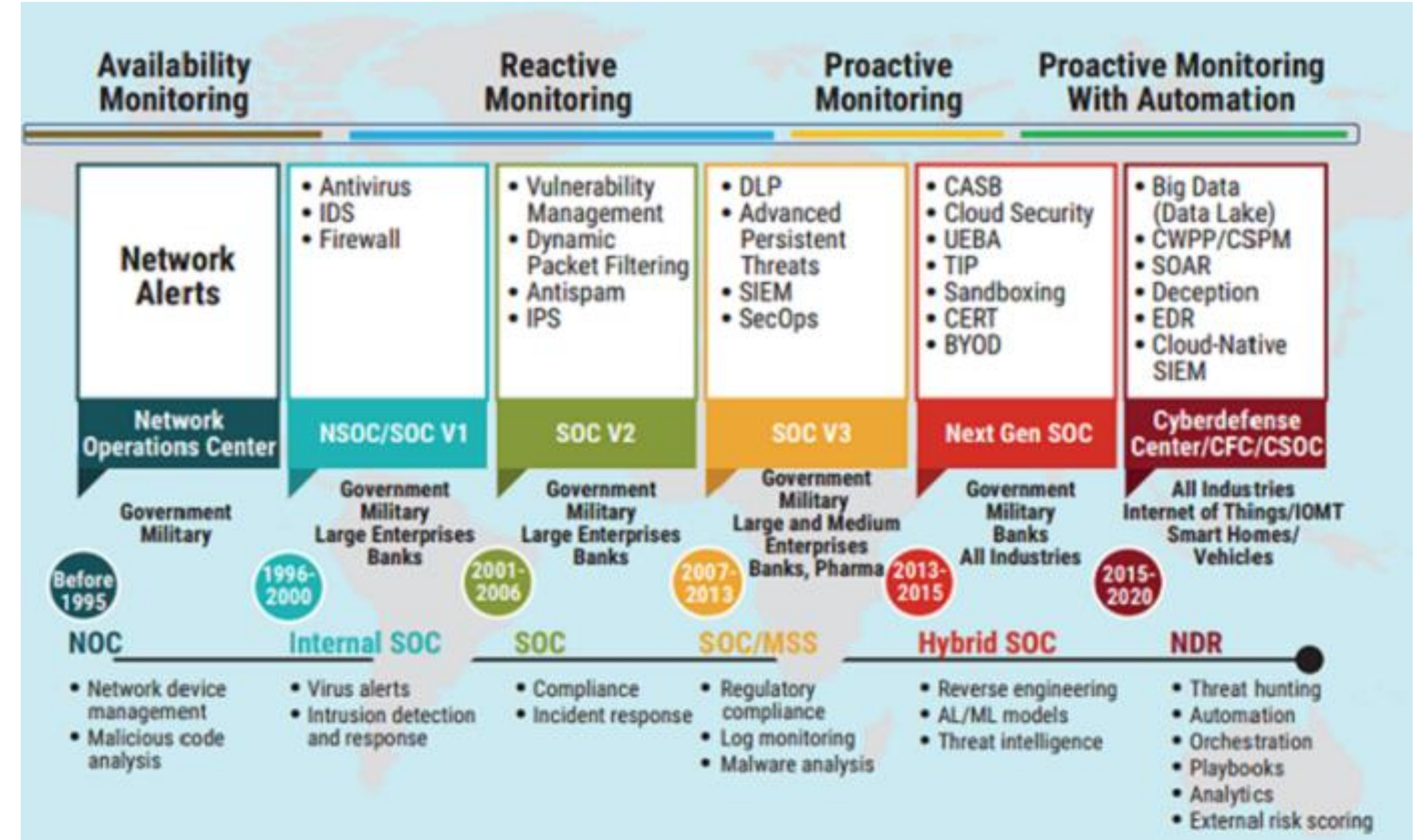
KAYNAK: <https://cağlar-celik.com/tAğ/siber-guvenlik-operasyonlari-merkezi/>

SOC (GÜVENLİK OPERASYON MERKEZİ)

İşleyişi:

SOC, genellikle birkaç ana bileşenden oluşur:

- **Monitörleme ve Algılama Sistemleri:** Bilgisayar ağları ve sistemlerini sürekli olarak izlemek ve tehditleri tespit etmek için kullanılan güvenlik araçları ve yazılımları içerir.
- **Analiz ve Yanıt Ekibi:** Tehditleri analiz eden ve olaylara yanıt veren siber güvenlik uzmanlarından oluşur.
- **Olay Kayıt ve Yönetim:** Olayların kaydedildiği ve raporlandığı bir veritabanını içerir.
- **İletişim ve İşbirliği:** İlgili paydaşlarla iletişim kurma ve işbirliği yapma yeteneklerini içerir. Bu, diğer organizasyon birimleri, üçüncü taraf güvenlik hizmet sağlayıcıları ve yetkilendirilmiş makamlarla iletişimi içerebilir.

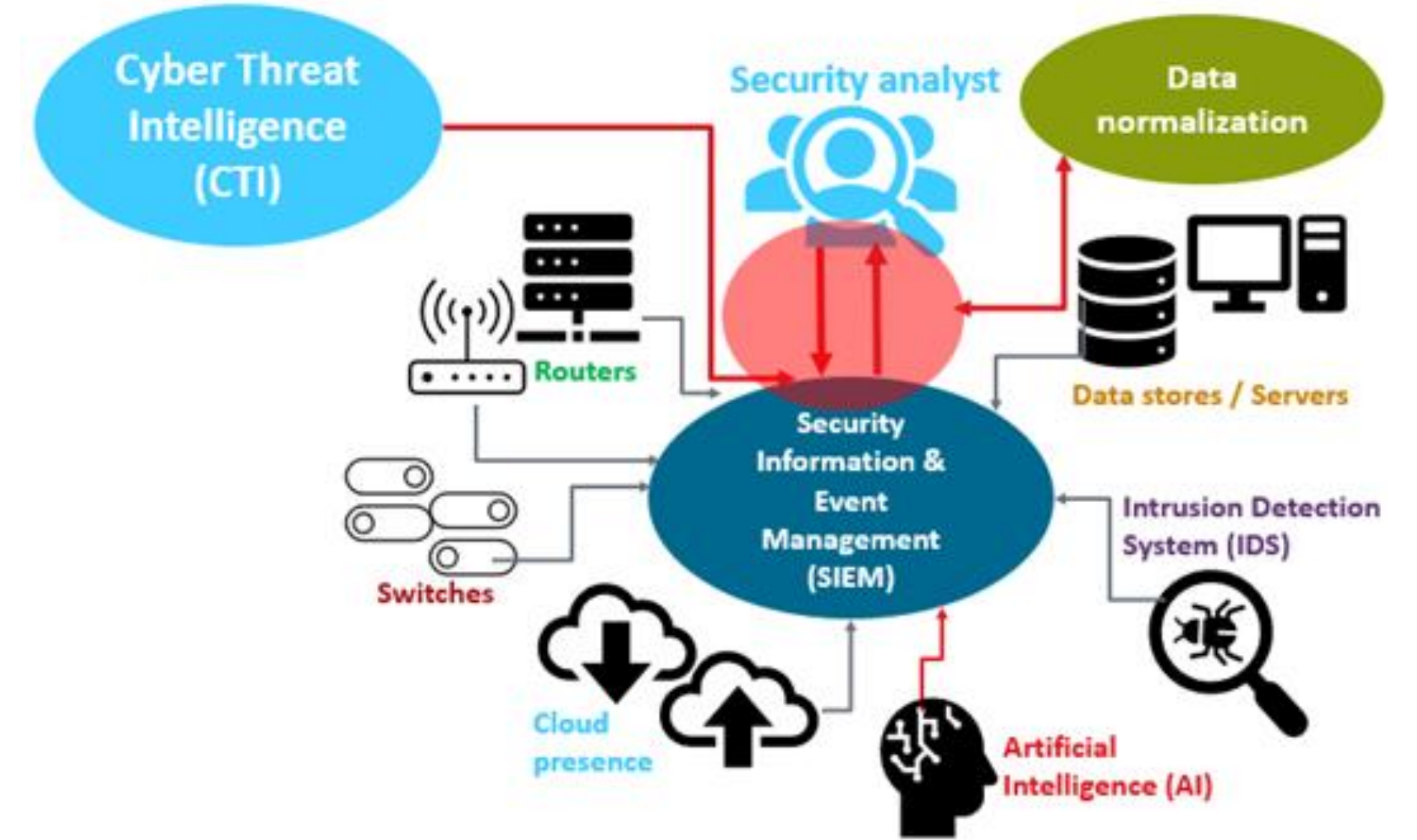


KAYNAK: <https://www.xenexsoc.com/blog/51bpom4k8jm7jdaxc3u5zr75ung4kj>

SOC (GÜVENLİK OPERASYON MERKEZİ)

Önemi:

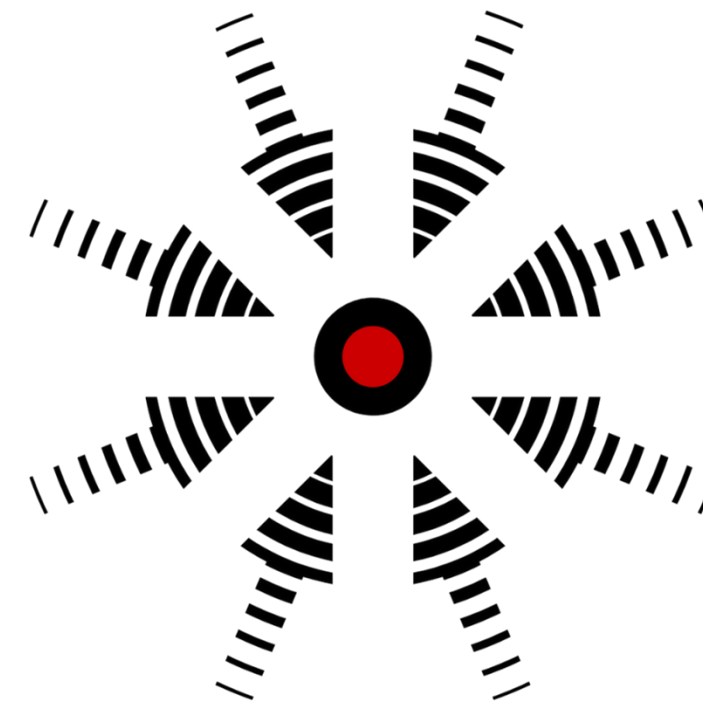
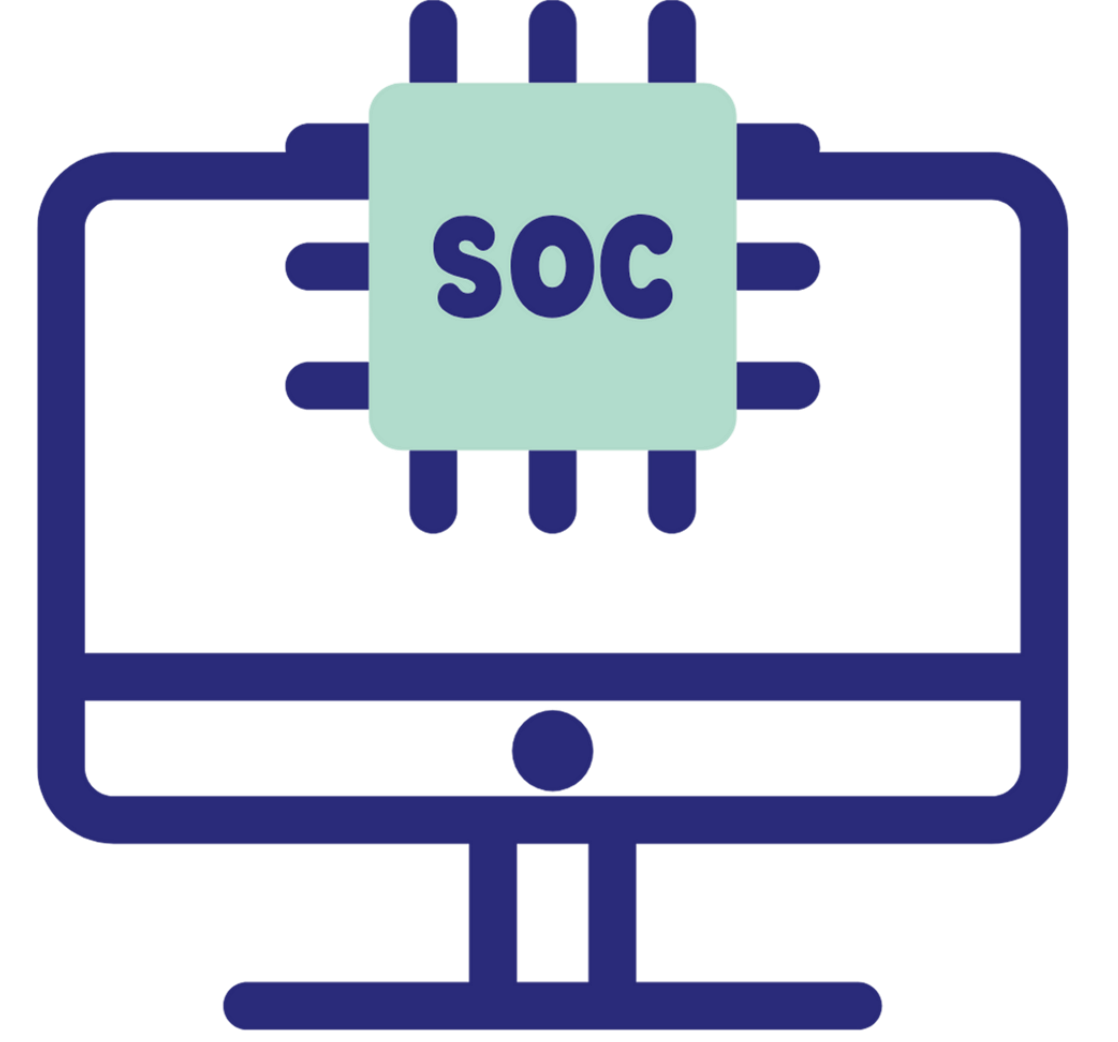
- **Siber Tehditlere Hızlı Yanıt:** SOC, organizasyonların siber tehditlere hızlı bir şekilde yanıt vermesini sağlar, bu da potansiyel hasarın en aza indirilmesine yardımcı olur.
- **Veri ve Varlık Koruması:** SOC, organizasyonların hassas verilerini ve diğer varlıklarını koruma görevini üstlenir, böylece veri sızıntıları ve kayıpları önlenabilir.
- **Siber Güvenlik Bilinci:** SOC, organizasyon içinde siber güvenlik farkındalığını artırır ve güvenlik politikalarının uygulanmasına yardımcı olur.
- **Sürekli İyileştirme:** SOC, güvenlik olaylarından öğrenir ve organizasyonun siber güvenlik savunmasını sürekli olarak güçlendirmeye yardımcı olur.



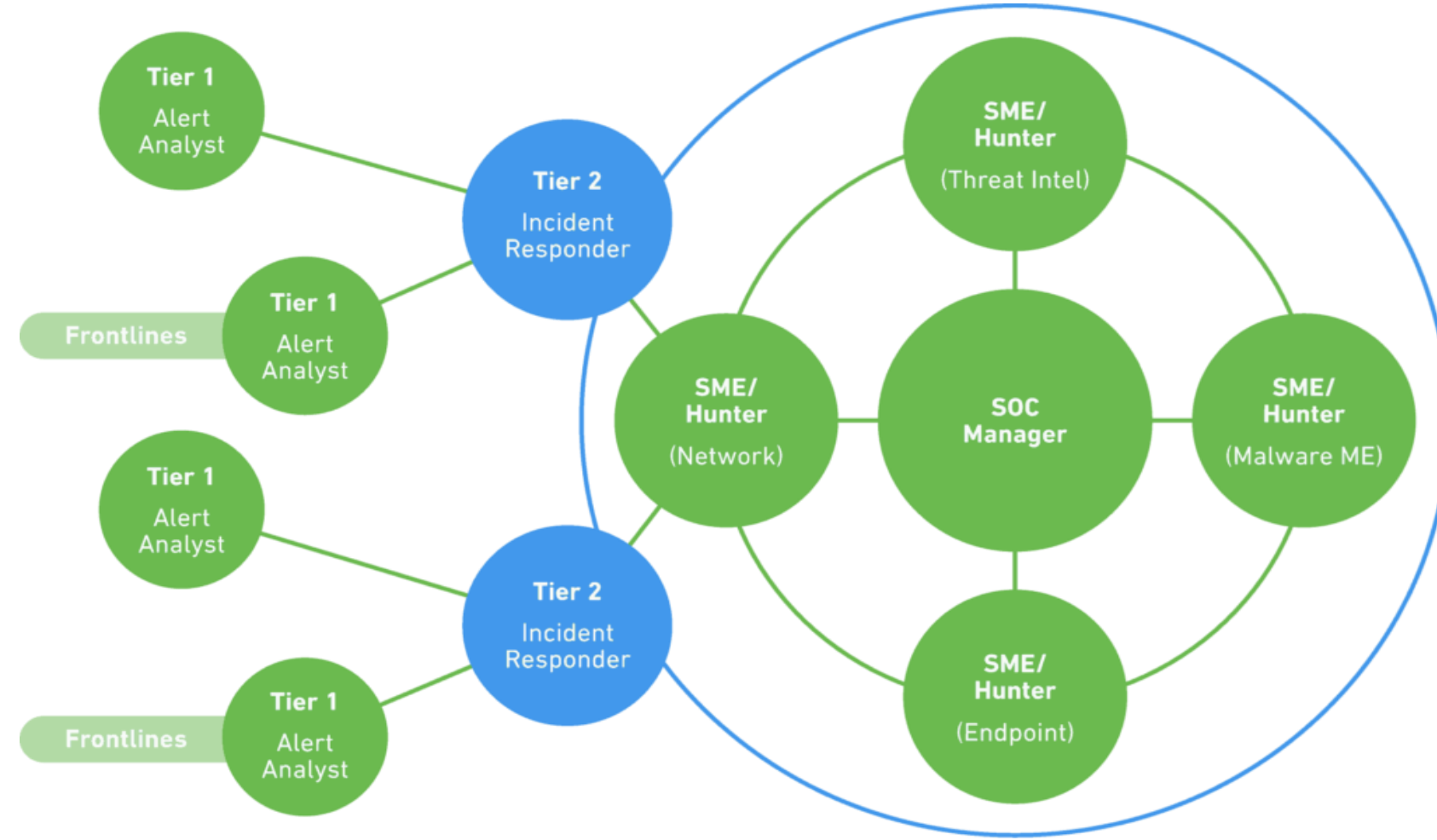
KAYNAK: <https://www.hosting.com.tr/blog/soc/>

SOC ÖRNEKLER

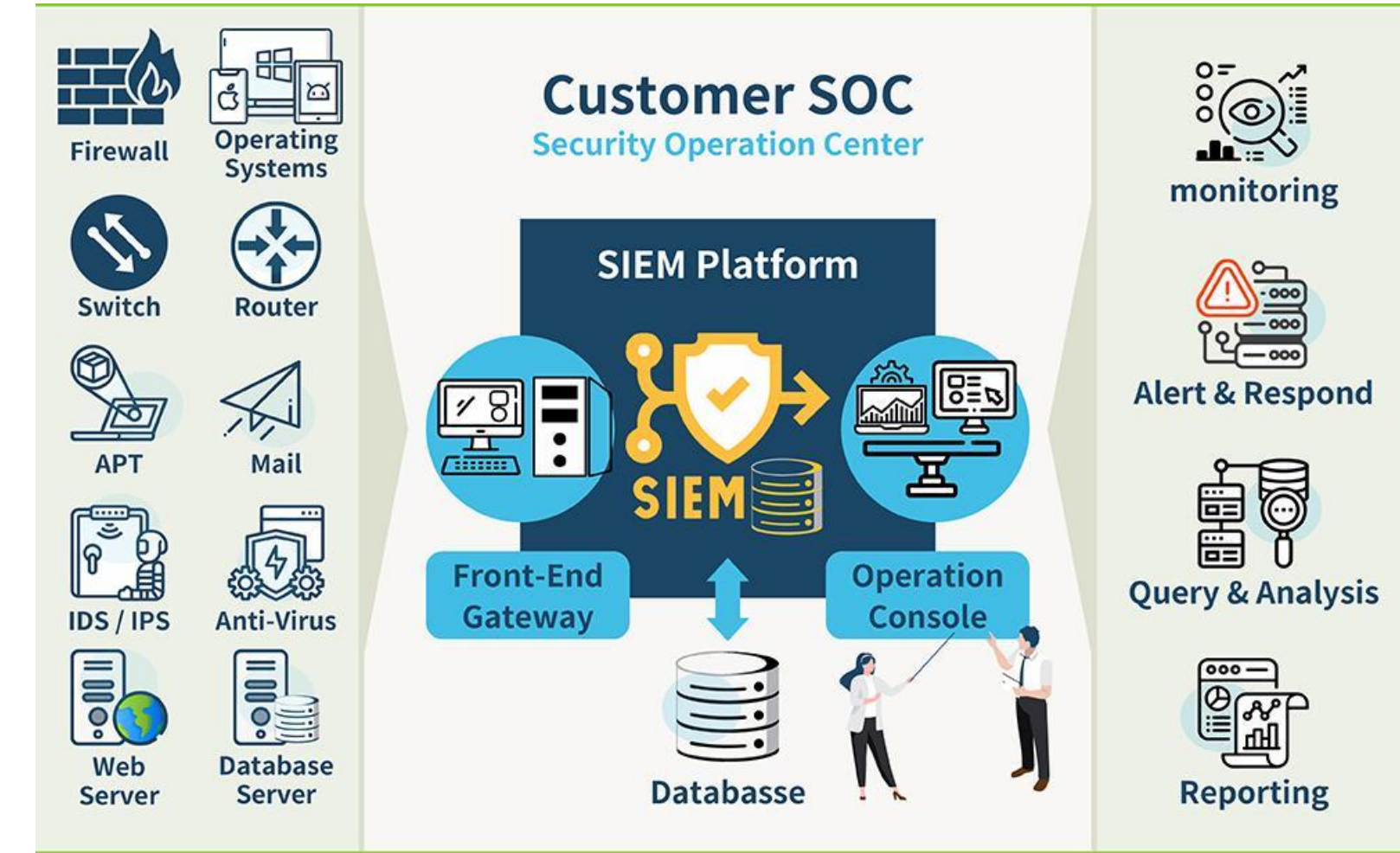
- **Sosyal Mühendislik Saldırısı Tespiti:** Bir çalışan, sahte bir e-posta aldığını bildirir. SOC, bu e-postayı analiz eder, sahte olduğunu teyit eder ve diğer çalışanları uyarır.
- **Siber Tehdit İstihbaratı Kullanımı:** SOC, karanlık web ve siber tehdit istihbarat kaynaklarından gelen bilgileri izler, tehditleri belirler ve buna karşı önlemler alır.
- **Güvenlik Olaylarının İzlenmesi:** SOC, organizasyonun ağlarını ve sistemlerini sürekli olarak izler. Örneğin, bir saldırganın sisteme yetkisiz erişim sağlama girişimini tespit edebilir.



SOC EKİBİNDE ÇALIŞANLAR



KAYNAK: <https://hackernoon.com/complete-guide-on-soc-and-its-implementation-for-your-business-37b063cb9128>



KAYNAK: <https://www.acercsi.com/service.aspx?id=2ca6a42c-36d9-447d-aabf-04430c90c64c>

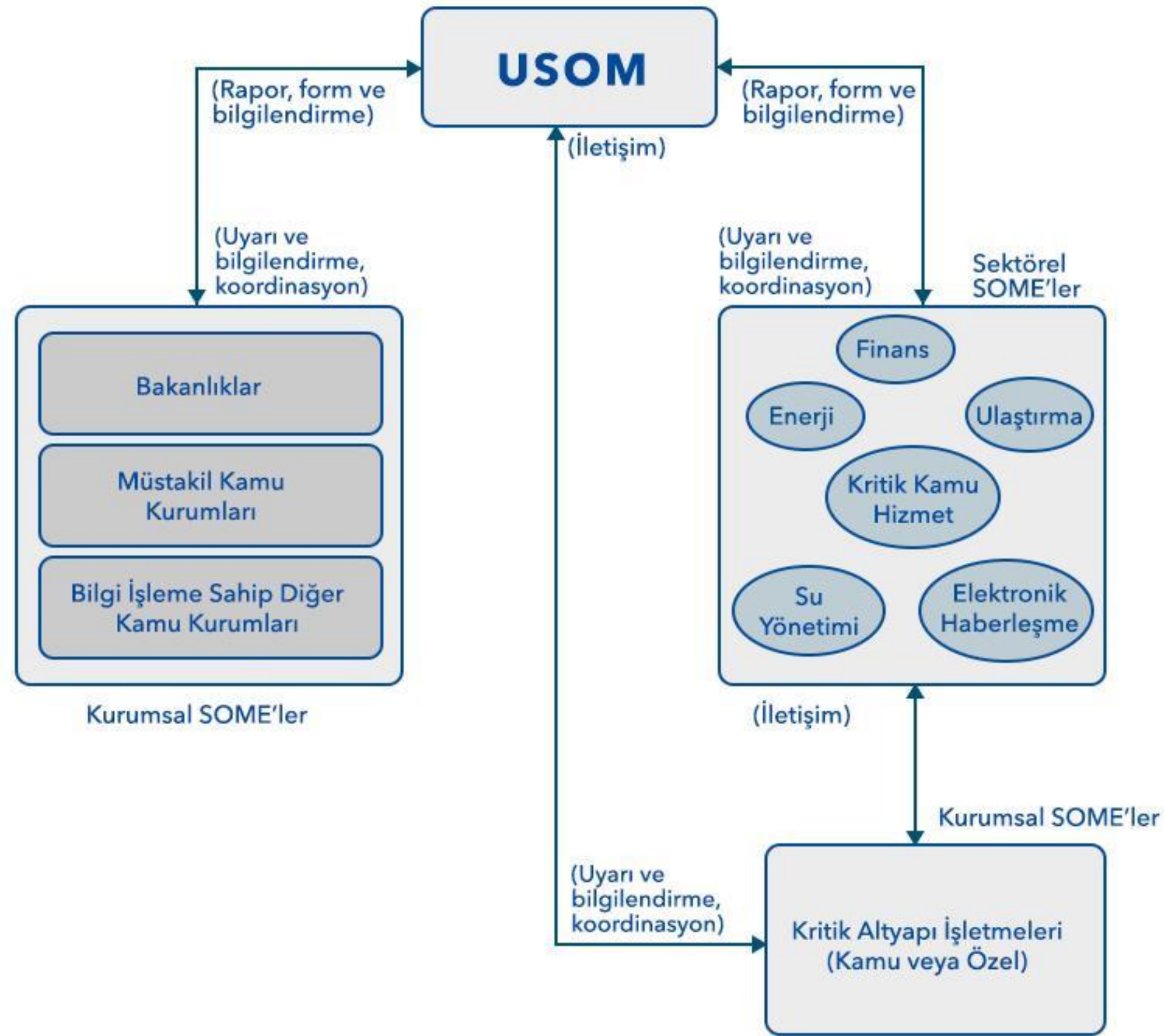
- **Siber Güvenlik Analisti:** Olayları izler, analiz eder ve yanıt planlarını uygular.
- **Siber Tehdit İstihbarat Analisti:** Tehdit istihbaratını izler ve analiz eder.
- **Günlük İzleme Analisti:** Günlük kayıtları inceler ve potansiyel güvenlik olaylarını tespit eder.
- **Kriz Yöneticisi:** Büyük olayların kriz yönetimini sağlar.



Bölüm 22

USOM (ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ)

USOM (ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ)



1. Siber Güvenlik İzleme ve Teşhis
2. Olay Yanıtı ve Müdahale
3. Siber Tehdit İstihbaratı ve Analiz
4. Kamu ve Özel Sektör İşbirliği
5. Siber Güvenlik Bilincinin Artırılması



Şekil 1 : Ulusal Siber Olaylara Müdahale Organizasyonu



GÜNCELLEMELER

