WEB SERVER

SAFEGUARD

Kesintisiz Web Hizmeti & Bilgi Güvenliği

- ✓ Kötü Amaçlı Yazılım Saldırıları
- ✓ Fidye Yazılımı Saldırıları
- ✓ Apt Saldırıları

Anında Tespit ve Savunma Eylemleri ile Kapsamlı

Web Tabanlı Bilgi Güvenliği

İÇERİK

1. **Web Saldırıları**

- Saldırı İstatistikleri ve Örnekleri
- Web Shell Kullanılan Saldırılar
- Gelişmiş Web Shell Tehditleri
- Ağ Güvenliğindeki Sınırlar

2. Web Saldırılarına Karşı Önlemler

- Neden WSS?
- Web Shell Savunma İşlevleri
- WSS Temel Özellikleri
- WSS Cloud
- WSS Tespit Yönetimi
- UMV Teknolojisi ve Rekabetçiliği
- WSS Sistem Yapılandırma Şeması

3. Referanslar

SIK GÖRÜLEN WEB KORSANLIKLARI

Atak Türleri

1. İç ve dış çalışanlardan kaynaklanan güvenlik açıkları

2. Ağ güvenliği çözümü güvenlik açıklarını hedefleyen saldırılar

- Ağ güvenlik sistem açıkları (kalıp halinde analiz edilir)
- Virüs programları tarafından oluşturulan kötü amaçlı kod saldırıları
- Ağ bypas tekniği ve penetrasyondaki artış

3. İşletim sistemi Web Sunucusu/ WAS Zero Day Saldırıları

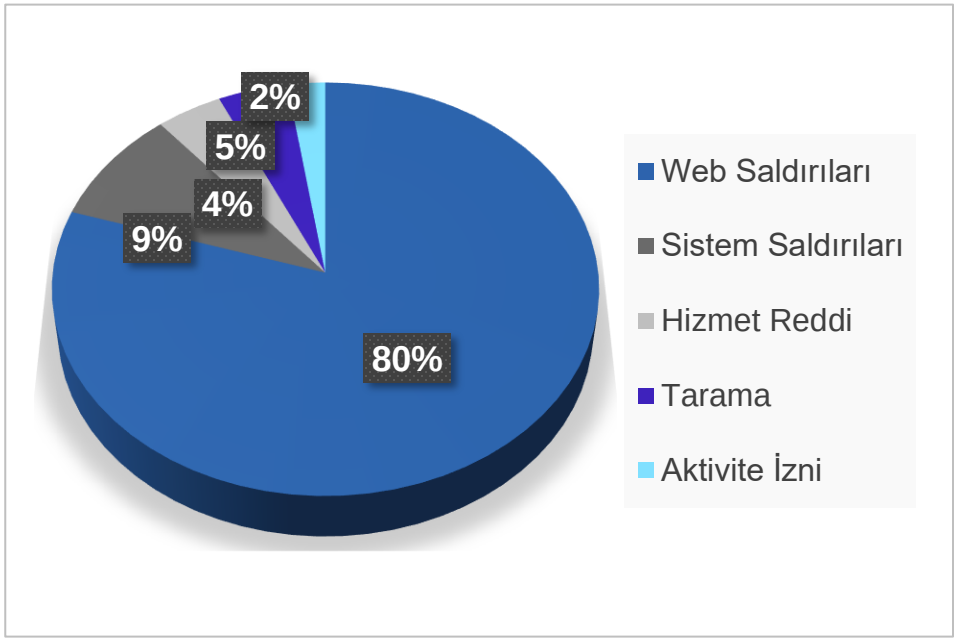
4. Bildirim panosu yükleme saldırıları kaynak kod güvenlik açıklarını hedefleyen saldırı yüklemeleri

- Yanlış uzantı güvenlik açıkları
- Görüntü dosyası kılık değiştirmiş saldırılar

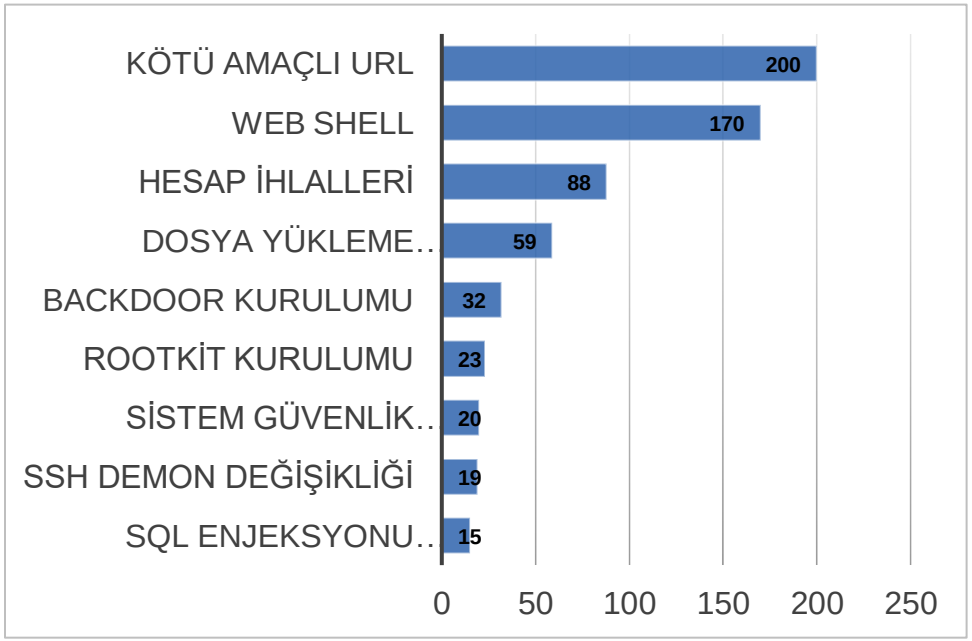
SİBER SALDIRI İSTATİSTİKLERİ

KISA İnternet İhlali Müdahale Merkezi tarafından yapılan araştırmalarda siber saldırıların çoğunluğu web zafiyetlerinden geçen kötü amaçlı kodlar ve Web Shell kullanarak yapılmaktadır. Web Shell, yani web kabuğu son zamanlarda sıklıkla kullanılmakta olan neredeyse web üzerinden yapılan bütün saldırıların sebebi olarak bilinen kötü amaçlı komut dosyalarıdır. Web kabukları kötü amaçlı yazılım yüklemek, saldırı yüzeyi oluşturmak ve ek saldırılar başlatmak için kullanılır. Ağ güvenlik açıklarından geçtikten sonra bir web sunucusuna yüklenir ve veri hırsızlığı yapmak, yeni güvenlik açıkları oluşturmak, hedeflenen web uygulamalarına veya sisteme arka kapı kullanarak sızmak ve daha fazlası için kullanılır.

SİBER OLAYLAR



WEB SALDIRILARI



WEB SALDIRI ÖRNEKLERİ

Web üzerinden yapılan saldırılar ve web kabukları kullanılan siber saldırı olayları;

***Microsoft Exchange*:** Mart 2021 Microsoft Exchange sunucusundaki dört sıfırıncı gün güvenlik açığından yararlanarak erişim sağlandıktan sonra, Hafnium sunucu üzerinde uzaktan kontrol sağlamak için bir web kabuğu kullandı. Bu uzak bağlantı, verileri sızdırmak için kullanılır. Özellikle, web kabuğu saldırıları 2021'de ikiye katlandı. Bu siber saldırının yaklaşık 30.000 ABD kuruluşunu etkilediği düşünülüyor.
Kaynak: https://www.savunmatr.com/siber-guvenlik/microsoft-web-shell-saldirilari-hizla-yayiliyor-h8375.html

Shell Petrol: FTA'daki dört güvenlik açığından (CVE-2021-27101 , CVE-2021-27102 , CVE-2021-27103 CVE-2021-27104) yararlanır. Ardından DEWMODE web kabuğunu yükler ve dosyaları çalmak için kullanır. Bunlar kurbanların şifresiz cihazlarında saklanır.
Kaynak: https://siberbasin.net/gaz-ve-petrol-sirketi-shell-hacklendi/

Dışişleri Bakanlıkları: Hacker grubu güvenlik açıklarından yararlanarak ilk erişim için China Chopper adlı web kabuğunu keşif amaçlı kullanarak arka kapı adlı yazılımı kuruyor. Web kabuğu, saldırıya uğrayan sistemlerde tanıtılan kötü amaçlı bir komut dosyası olarak tanımlanıyor.
Kaynak: https://qha.com.tr/haberler/disisleri-bakanliklarini-hedef-alan-yeni-bir-siber-casusluk-grubu-tespit-edildi/327272/

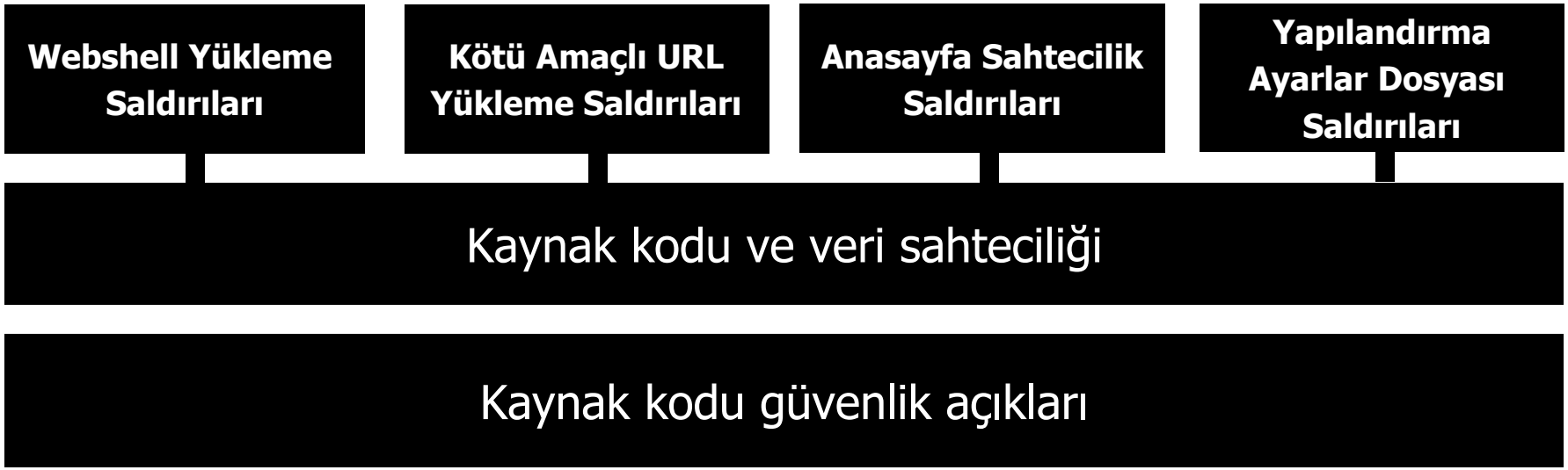
Yemek Sepeti: web uygulama sunucusu üzerinde bir açıklık bulunduğu, bu açıklıktan yararlanılarak, uygulama kurulduğu(web kabuğu) ve komut çalıştırılmak suretiyle sunucuya erişilebildiği ifade edilmiştir."
Kaynak: https://siberbulten.com/siber-saldirilar-2/yemek-sepeti-saldirisi-hakkinda-bilmeniz-gereken-5-sey/

Ayrıca, **MNG Kargo ve Sinoz Kozmetik** vb. gibi birçok firma web servisleri üzerinden siber saldırıya uğramıştır.

WEB KORSANLIKLARI

Web Sunucusu Hackleme Yöntemleri

Çoğu web tabanlı saldırı, web kaynak kodundaki en zayıf güvenlik açıklarını hedef alır ve veri korsanlığı yoluyla ilerler. Web shelleri, kötü amaçlı URL'leri, ana sayfa sahteciliğini ve web sunucusu yapılandırma ayar dosyalarının değiştirilmesinde kullanan saldırı yöntemlerine yol açar.



WEBSHELL NEDİR?

Webshell yani web kabuğu, hackerların bir saldırı yöntemi olarak kullandığı kötü amaçlı script dosyasıdır. Güvenlik açıklarını aşarak sunucuya ulaşan webshell dosyası çalıştırıldığında yönetici yetkilerini ele geçirir ve bilgi hırsızlığı, dosya değişikliği, web sayfası tahrifatı, kötü amaçlı URL/kod yayma, yeni bir güvenlik açığı oluşturmak veya bir sonraki saldırısına alt yapı hazırlamak için sıklıkla kullanılan tehlikeli bir **saldırı tekniğidir**.

1. Atak
Web sunucusunu ele geçirme

Hacker Bilgisayarı

Güvenlik açığı analizi → Web Shell yükleme → Sistem ele geçirme →

- Ayarlar dosyasını değiştirip yeni güvenlik açıkları yükleme
- Kötü amaçlı kod/URL yükleme
- Ana sayfa sahteciliği saldırısı

2. Atak
Hedefdeki / çalışan bilgisayarını ele geçirme

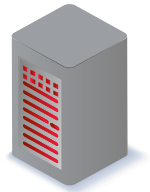
Kullanıcı Bilgisayarı

Kötü amaçlı URL aracılığıyla kötü amaçlı kod bulaştırmak →

Ransomware Infection
↓
Zombie PC →

Dahili yönetim sunucusu kimlik/PW hırsızlığı → Dahili sunucu istilası

3. Atak
Dahili sunucu ele geçirme

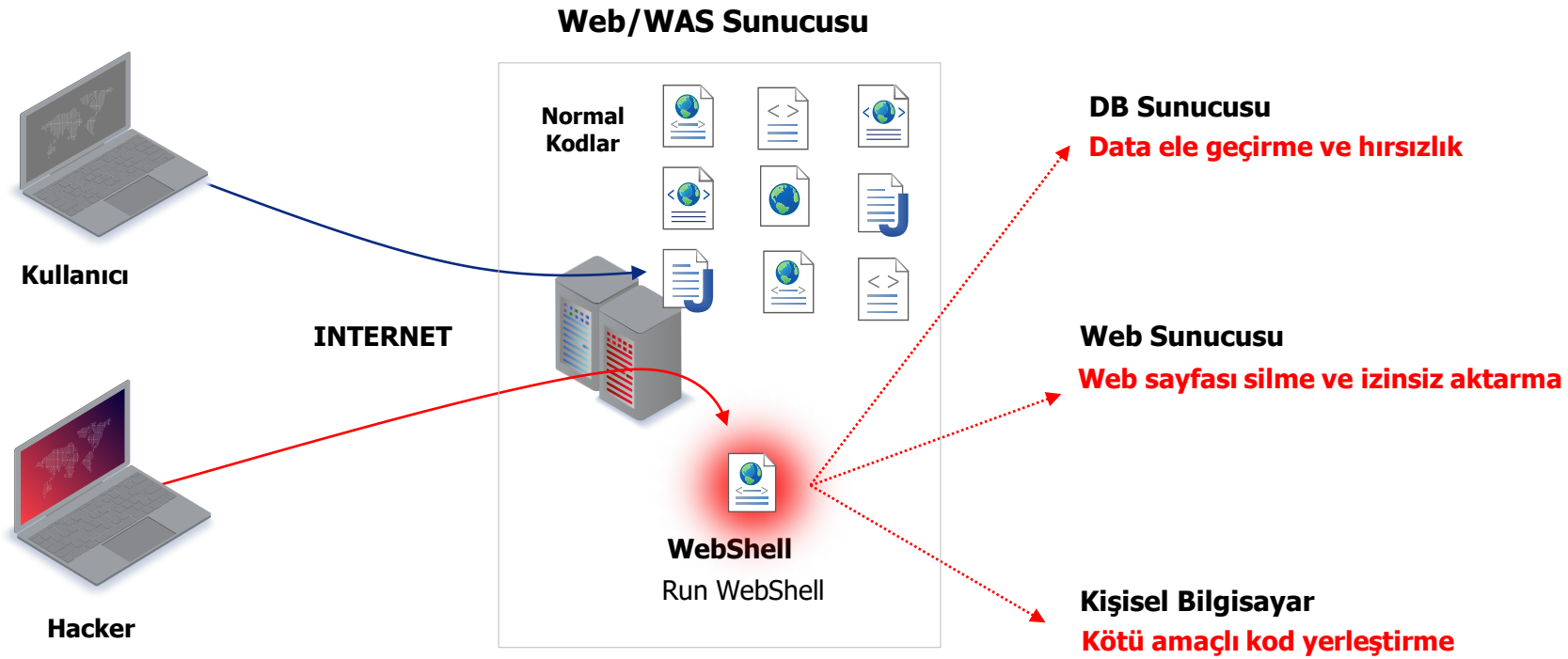


Dahili Sunucu

Dahili sunucu istilası → Data Kaçırma → Sistem çökertme

WEBSHELL NEDİR?

Web hizmetleri için evrensel 80 port arka kapı görevi görerek, sınıflandırılmış verileri çalmak, web sayfalarını tahrif etmek, sayfalara yetkisiz erişimi sağlamak ve kötü amaçlı kod yaymak gibi ciddi bilgisayar korsanlığı saldırılarına yol açar.



WEB SHELL TANIMI VE TEHLİKELERİ

- Web Shell yani web kabukları, web uygulaması komut dosyaları (ASP, JSP, PHP, CGI, vb.) biçiminde erişim olmaksızın doğrudan komutları yürütmek için bir geçiş noktası sunar.
- Web Kabukları uzaktan inşa edilir, savunmasız yerlere yerleştirilir ve herhangi bir zamanda etkinleştirilir. İstediği zaman istediği yerde kendilerini imha edebilir ve sunucularda saklanarak sürekli bilgi hırsızlığında bulunur.
- Web Kabukları başarılı bir şekilde yüklendikten sonra, uzaktan komut verebilir. Bu komutlar, dosya eklemek, silmek, yürütmek, başka yürütülebilir dosyalar veya komut dosyaları için kullanılabilir.
- Web Kabukları, casus yazılımlardan ve diğer bilinen bilgisayar korsanlığı yöntemlerinden daha tehlikeli olduğu bildirilmiştir.
- APT saldırılarında sıklıkla kullanıldığı görülen web kabukları önemli siber olaylarına yol açmaktadır.
- Çok çeşitli güvenlik açıklarını kullanarak ağdaki diğer sistemlere virüs bulaştırdıktan sonra SQL ekleme saldırısı ve siteler arası komut dosyası çalıştırma (XSS) sahteciliği saldırında da web kabuklarını kullanılabilir.
- Web Kabukları dosyaları değiştirerek veya ekleyerek web sitelerini tahrif etmek için sıklıkla kullanılır.

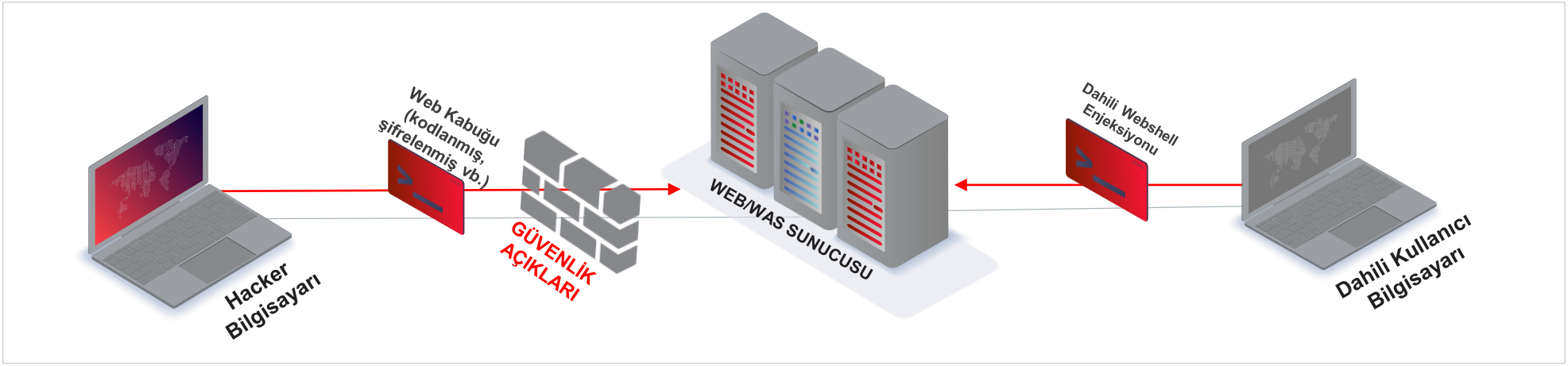
GELİŞMİŞ WEB SHELL TEHDİTLERİ

Web kabukları, komut konsolunu kullanarak web sunucularının kontrolünü tamamen ele geçirebilir

Sistem Komutları	• Sistemi okuma ve kapatma • Hedef programlarını değiştirme, silme, durdurma/kaldırma
Ağ Komutları	• Güvenliği ihlal edilmiş/zayıf bağlantı noktalarının tespiti için bağlantı noktası tarama • TELNET, SSH, FTP üzerinden hedef sunucu penetrasyonu (dahili ağ erişimi)
Veritabanı Erişimi	• Veri sızıntıları, ele geçirme, değiştirme ve silme
Sistem Dosyası Erişimi	• Gelişmiş bilgisayar korsanlığı aracı yükleme (Anahtar log, arka kapı) • Dosya değişikliği (kötü amaçlı kod ekleme) • Dosya değiştirme, silme • Tüm sistem dizinini okuma
Kullanıcı Bilgisayarı	• Kötü amaçlı kod bulaştırma • Veri sızıntıları, yönetici bilgilerine erişme • DDoS saldırılarını tetikleme

AĞ GÜVENLİK ÖNLEMLERİNDEKİ SINIRLAR

IPS, IDS, Güvenlik Duvarı, WAF, L3swich, anti-ddos, vb. gibi güvenlik uygulamaları.



KURUM DIŞI SALDIRILAR

- **Tespit ve savunmadaki** sınırlamalar
- Sisteme **önceden eklenmiş** web kabuğunu algılamada güçlük
- **Çeşitli** ve **karmaşık** web kabuğu yükleme yöntemleri;

  - **kodlanmış/şifrelenmiş** web kabuğu,

  - **gizlenmiş** web kabuğu,

  - **bilinmeyen** web kabuğu,

  - **parçalara bölünmüş** web kabuğu (daha sonra sistemde birleştirilir),

  - dönüştürme işlevi(conversion) kullanılan web kabukları,

vb. gibi **filtreleme, kalıp eşleştirmedeki zorluk** ağ güvenlik önlemlerinde sınırlar içerir.

KURUM İÇİ RİSKLER

Dahili sistemden yüklenen web kabuklarını tespit etmesi zor ve engellenemez olması büyük tehlike oluşturmaktadır.

- İş ortakları
- Web hizmeti üzerinden kurumsal müşteriler
- Dahili PC kullanıcıları, dahili çalışanlar

vb. gibi dahili sistemden yapılan web kabuğu yüklemesi sıklıkla görülmektedir.

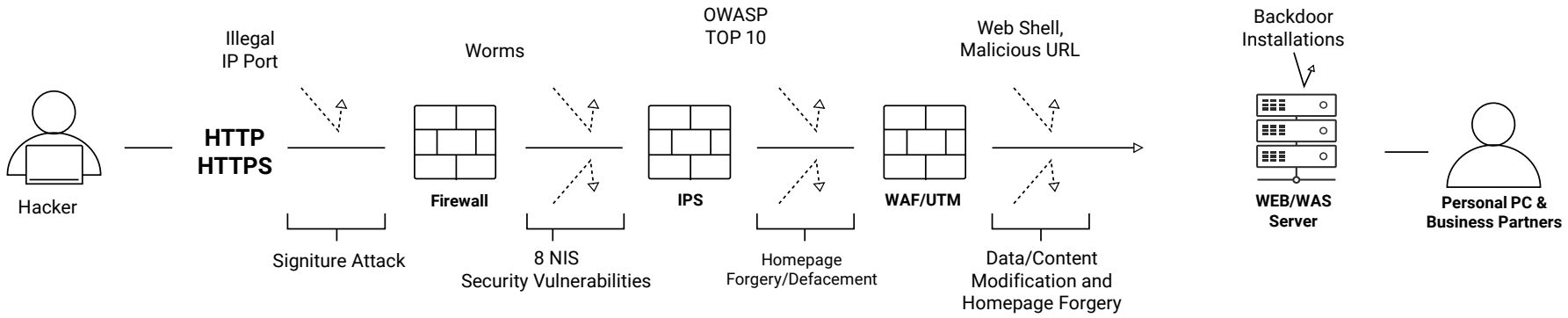
WEB SALDIRILARA KARŞI ÖNLEM

Siber saldırılar kaçınılmaz!

Çeşitli güvenlik açıkları, ağ güvenliği cihazlarındaki güvenlik sınırlamaları, bypass teknikleri, iş ortakları, istisnalar vb. gibi riskler nedeniyle saldırılar kaçınılmazdır. Bu riskler, gelişmiş web saldırılarının farkındalığı ve yaklaşan saldırılara karşı sıkı hazırlık gerektirmektedir.

Herşeyden sonra hasardan kim sorumludur?

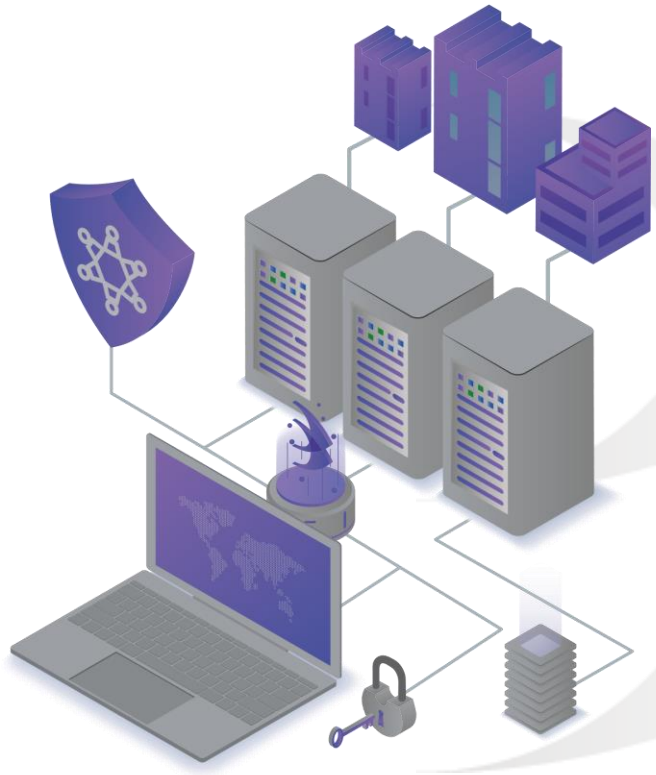
Entegre güvenlik artırıcı çözüm olan WSS, ağ zayıf noktalarından geçen ve saldırı zemini oluşturmaya hazırlanan web kabuklarını ve kötü amaçlı URL'leri sisteminizde yakalayarak, daha hiçbir değişiklik veya veri hırsızlığı gerçekleşmeden önlem almanızı sağlar. Böylelikle güvenlik önlemlerinizi tam olarak kapsayarak, saldırı anında dahi web sunucularınızı ve web tabanlı verilerinizi korurken web hizmetlerinizi kesintiye uğratmaz.



İÇERİK

WSS NEDİR?

WSS (Web Server Safeguard), web sunucularını web kabukları kullanılarak yapılan veri hırsızlığı, fidye yazılımı, APT vb. gibi çok çeşitli web tabanlı saldırılara karşı etkili bir şekilde koruma sağlamak için tespit, karantina ve restorasyon çözümü sunmaktadır. WSS, web hizmetlerini gerçek zamanlı olarak izleyerek, WEB/WAS'a eklenen kötü amaçlı script dosyaları, URL/kodları ve dosya değişikliklerini tespit eder, karantinaya alır ve tespit detaylarını incelemenizi sağlar.



WSS Real-Time İzleme ve Savunma Eylemleri

✓ **Kötü Amaçlı Dosya Yükleme Saldırısı**

Malicious script (web shell), malicious kod/url yükleme saldırılarına karşı, tespit, karantina, istisna işleme, yetkili bilgilendirme, siyahbeyaz/gri liste olarak yönetme ve istatistik rapor sağlama

✓ **PII (Personal Idenrifiable Information) Tespiti**

Web sunucularında tutulması tehlikeli olan veri güvenliğine ilişkin yükümlülüklere karşı kişisel bilgileri dosya, belge, veritabanı içerisinde tespit ve bilgilendirme

✓ **Dosya Bütünlüğü (File Integrity)**

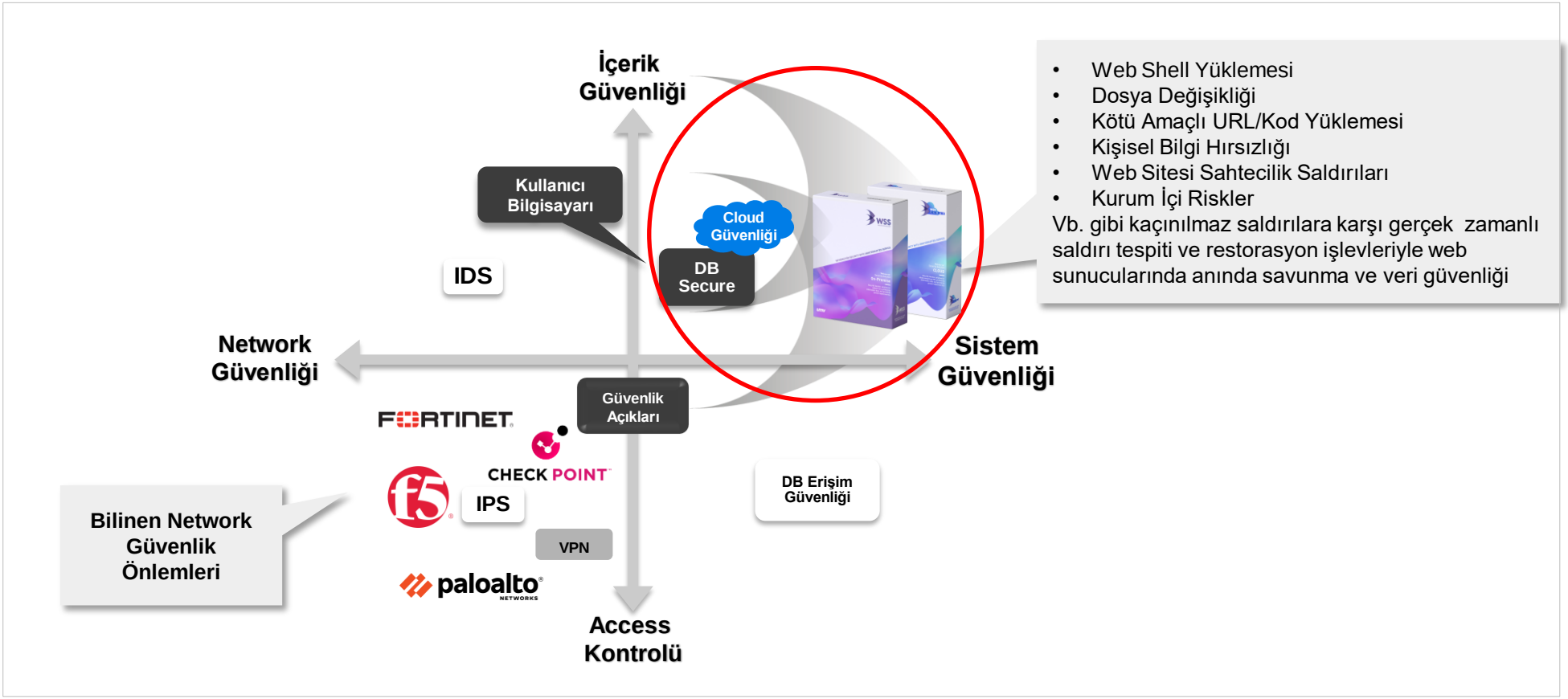
Kaynak dosyası, yapılandırma ayarları, önemli dosyalarda yapılan değişiklikleri tespit eder veya otomatik geri yükleme yaparak saldırıyı engelleme ve IP tespiti yaparak yetkiliye bilgilendirme

✓ **Kaynak Kodu Anında Restorasyon**

Web sitesi dosya değişikliklerinde kaynak kodunu orijinaline geri döndürme

WEB SALDIRILARINDA SİSTEM GÜVENLİĞİ ÖNEMİ

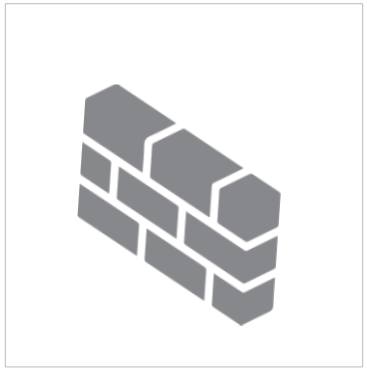
Kaçınılmaz olan web güvenlik açıklarından yararlanan saldırılarda sadece ağ güvenliği yetersiz kalabilir, bu gibi ağ güvenlik önlemlerini atlayabilen saldırılarda hasara uğramadan gerçek zamanlı tespiti ve hızlı yanıt önemlidir.



TAM KAPSAMLI WEB GÜVENLİĞİ

Web saldırıları tekniklerinin çoğunluğunda web kabuğu kullanıldığı bilinmektedir. Web üzerinden yapılan saldırıları önlemek için kapsamlı güvenlik çözümü kullanımı esastır. Farklı biçimler ve yöntemlerle güvenlik açıklarından yararlanarak sisteme erişebilen web kabuklarının kullanıldığı saldırı tekniklerine karşı sistem içerisinde de tam kapsamlı güvenlik için WSS kullanımı önerilmektedir.

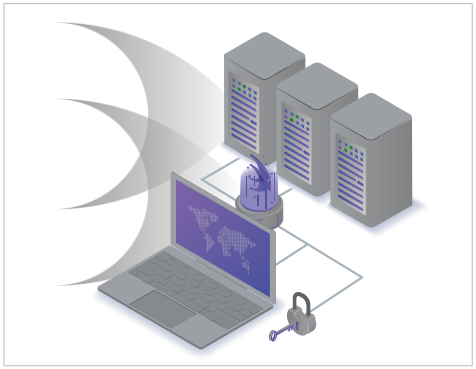
EDR – NDR GİBİ BİLİNEN GÜVENLİK ÖNLEMLERİ



Web Güvenlik Duvarı

IPS - IDS - VPN - V3 vb.

WSS İLE TAM KAPSAMLI GÜVENLİK

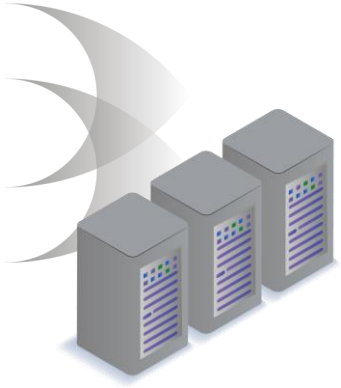


Kodlanan, gizlenen, bilinmeyen ve bypass teknikleri kullanarak yüklenen tespiti zor web kabuklarını bilinen güvenlik önlemleriyle tespit etmek zordur. Bu gibi sürekli gelişen web saldırılarına karşı tam kapsamlı güvenlik önlemleri alınmadığı takdirde güvenlik zafiyetlerini aşarak sunuculara ulaşabilen web kabuklarıyla güvenlik olayları sıklıkla yaşanmaktadır.

WSS, web üzerinden yüklenen web kabukları, kod/url yükleme saldırı teknikleri, dosya değişiklikleri ve web sitesi tahrif saldırılarını gerçek zamanlı olarak izleme, tespit ve savunma eylemleriyle tam kapsamlı güvenlik sağlar

WSS ÇÖZÜM YAPISI

Bilgi depolamak için kullanılan WSS yönetim sunucusu S/W, tespit işlevi sağlayan aracı ve yönetici bilgisayar programından oluşur. Her bir WEB/WAS sunucularınıza aracı kurulumuyla işlev sağlar.



WSS TESPİT ARACISI	WSS SUNUCUSU	WSS YÖNETİCİSİ
• Web kabuğu tespiti ve kötü amaçlı URL tespiti • Kişisel bilgi tespiti • Web kabuğu tespiti ve filtreleme sonuçlarını sunucuya iletme vb. • JDK 1.5 tarafından desteklenen tüm işletim sistemleriyle uyumluluk	• Web kabuğu algılama bilgileri/geçmiş depolama • Uzaktan yönetim kontrolü • Web kabuğu kalıp güncellemesi ve aracı dağıtımı vb. işlevleri gerçekleştirme • VM veya PC'ye yüklenerek çalışan sunucu yazılımı	• Tespit işlevini çalıştırma • İzleme, uzaktan eylem, ortam ayarı işlevleri • İdari otorite yönetimi, istatistik ve raporlama • Güvenlik kontrol ve işletim bilgisayarı üzerine kurulum

WSS TESPİT YÖNTEMİ

Algılama performansını iyileştirmek için,

bilinmeyen kötü amaçlı kodlar toplanır ve

WSS tarafından üretilen **salt kod analiz**

motoru – SCR Ayrıştırıcı aracılığıyla tespit edilir

WSS, tespit etme performansını artırmak için kötü amaçlı kodları toplar;

- ✓ 30.000'den fazla birime uygulanan tespit aracısı (agent)
- ✓ Kalıp uygulaması ve özel durum desteği
- ✓ Yanlış pozitifleri en aza indirir

Kalıp Tespiti

DB'de depolanan kalıpları izinsiz giriş yapan dosyalardaki kalıplarla karşılaştırarak tespit

Algoritma Tespiti

JAVA komut dosyası gibi algılanması zor olan kalıpların kodlanmış (encoded) gizlenmiş (obfuscated) web kabuklarını dahili kod aracılığı ile tespit

Hash Değer Tespiti

Sistemi yavaşlatan sonsuz kalıp dosyalarının tespitinde daha verimli bir performans için dosyalara hash değeri oluşturarak kalıp karşılaştırmasıyla tam tespit ve gerçek zamanlı tespit performansı

Signature (İmza) Tespit

Bilinen web kabuklarını algılamak için web kabuğu imzaları oluşturur ve tespit eder

WSS KOLAY YÖNETİM ÖZELLİKLERİ

Güvenlik

- Ayarlar sunucusunun kaynak kullanımı ayarlanabilirliği (Minimum CPU/Bellek kullanımı)
- Yedekleme desteği (Etkin/Etkin)
- Saldırganın IP kimlik tespiti

Tespit ve Güncelleme Kolaylığı

- Otomatik kalıp tespit aracı(aracı) güncellemesi
- En son yapılan tespitleri yönetim sunucusuna otomatik yedeklenme
- Yetkisiz uzantı filtresi

Otomatik Karantina ve Rapor

- Tek tıklamayla otomatik karantina ve rapor
- Hedef dizini otomatik algılama
- İşlem sırasında yeni hedef dizinlerin otomatik algılanması

Hiyerarşi Yönetimi

- Yönetici ayrıntılı yetki yönetimi (yönetici/kontrol çalışanı/operasyon çalışanı)

Uyumluluk

- Java 1.5 veya üstü
- Tüm işletim sistemleriyle uyumluluk (Windows, Linux, Unix)

Entegrasyon

- Harici sistemlere bağlanabilme
- SYSLOG, SMTP, API, etc.
- ESM, SIEM, yapılandırma yönetimi, SMS, EMAIL, vb.

WSS ÖZELLİK LİSTESİ

ARACI (AGENT)

- Aracı Yönetim Özellikleri
- Aracı kaynak kullanım ayarları
- Aracı kaynak kullanımı aşıldığında bildirim
- Aracı ayarlarını toplu olarak değiştirme
- Tespit ilkelerini toplu uygulama
- Aracının otomatik/manuel/toplu güncelleme işlevi
- Çevrimdışı tehşis ve sonuç yönetimi
- Aracı otomatik yeniden başlatma

RAPORLAMA

- Grup ve bireysel rapor oluşturma
- Periyodik (günlük, haftalık, aylık) rapor oluşturma
- Algılama ilkesi durumunun indirilmesini sağlar
- Algılama listesinin durumunu varlığa veya gruba göre dosya halinde indirme

GÜVENLİK

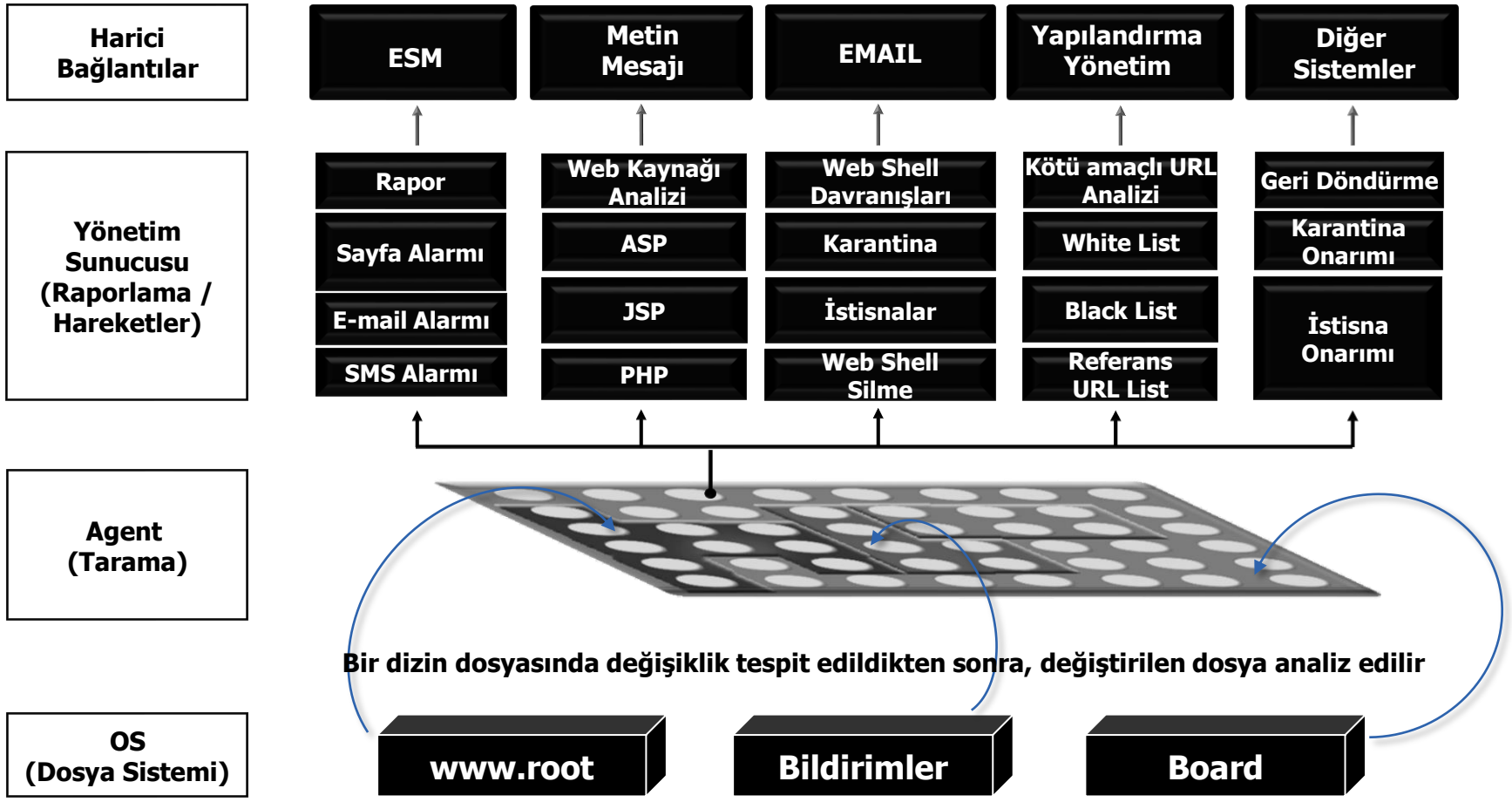
- Tespit edilen dosyaları otomatik engelleme, özel durum işleme
- Tespit edilen Web Shell için analiz isteme
- Tespit edilen dosyalar için toplu istisna/engelleme işleme
- Değiştirilmiş dosyalar için geri yükleme
- Ajanın yönetim sunucusuyla iletişim kesilmesi halinde gerçek zamanlı tespit

YÖNETİM

- Yapılandırma yönetim sistemi ile entegrasyon desteği
- Big data çözümü, entegre log yönetim sistemi ve entegrasyon desteği

WSS YAPISI VE EYLEM YÖNETİMİ

WSS, dosya sistemi izleme yoluyla sahteciliği ve kötü amaçlı kodun oluşumunu tespit eder.



WSS TESPİT ÖZELLİK LİSTESİ

TESPİT YÖNETİMİ

- Ek tespit yöntemi ile engelleme, tespiti ayırarak uygulama
- Algılama türünü nesnelleştirme yoluyla uygulama
- Gerçek zamanlı Web Shell algılama özelliği
- Silinen Web Shell algılama özelliği
- Çeşitli Web Shell algılama özelliği
- Gizlenmiş, kodlanmış web Shell komut dosyalarını algılama ve tespit geçmişi sorgulama
- Eklenti, bypass tespiti özelliği
- Kaynak dosyalarda kötü amaçlı URL algılama özelliği
- Dosya değişikliği tespiti ve değişiklik önleme özelliği
- Dosya değişikliği algılamasında istisna süresi (günlük) ayarlama özelliği
- Yedekleme dosyası oluşturma algılama özelliği
- Yükleme engelleme özelliği
- Kişisel bilgi algılama özelliği
- Kullanıcıya özel istisna kalıplarını ayarlama ve tespit özelliği
- Şifreleme önlemleri özelliği
- Algılama dizin ayarlama özelliği

TESPİT İŞLEME YÖNTEMİ

- Tespit edilen dosyaları otomatik engelleme, özel durum işleme
- Tespit edilen Web Shell için analiz isteme
- Tespit edilen dosyalar için toplu istisna/engelleme işleme
- Değiştirilmiş dosyalar için geri yükleme
- Ajanın yönetim sunucusuyla iletişim kesilmesi halinde aracı gerçek zamanlı tespit

WSS DETAYLI YÖNETİM ÖZELLİKLERİ

- Yönetim ekranı aracılığıyla genel durum izleme
- Gerçek zamanlı CPU yük dengeleme
- Yönetim sunucusu ve aracılarda durum bilgisi izleme
- Kaynak kullanımı izleme
- Kontrol paneli ekranı yönetme
- Genel sistem durumunu denetlemesi için panoları yapılandırma
- Grupları yönetme ve kişileri gruba göre atama
- Tam denetim mevcut (çalışma / uyku) program planlama
- Denetim sırasında ilerleme
- Tespit edilen Web Shell ayrıntılı bilgi analizi
- Orijinal ve değiştirilmiş dosyaların analizi
- İzne göre istisna/engelleme onay süreci
- Kullanıcıya özel geçmiş yönetimi
- Varlık ve gruba göre ilke durumu yönetimi
- Web Shell modellerinin otomatik/manuel/toplu/zamanlanmış dağıtımı
- Algılama sonuçlarının Syslog, SMS ve Messenger vb. gibi etkileşimi ve olay bilgilendirme
- Syslog ayar yönetimi
- Yönetim ekranı erişim kontrolü
- DB yedekleme ayarları

WSS BULUT BİLİŞİM (VM) DESTEĞİ

Scale IN/OUT Ölçeği

- WEB/WAS hizmetinin ölçeği genişletildiğinde algılama hedefinin otomatik olarak kaydedilmesinden sonra otomatik tespit
- WEB/WAS hizmetinin ölçeklendirilirken silinen örneğin tespiti, değiştirilmesi, silinmesinin geçmişini(log) yönetim sunucusuna otomatik kaydetme

Ana Dizini Bulma

- WEB/WAS ana dizinindeki ekleme ve değiştirmeler için tespit planlama
- Ana dizinde değiştirme/ekleme/kontrol etme geçmişi tespiti

Geçmiş Yönetimi

- Java 1.5 veya daha yenisi; tüm işletim sistemleriyle uyumluluk (Windows, Linux, Unix).

Olay Çoğaltma Yönetimi

- Ana dizin NAS alanına dahil edildiğinde, çift yönlü sistemdeki yinelenen tespit olayı önleme

Docker Konteyneri

- Docker Konteyneri VM Güvenlik Desteği

Güvenlik Yönetimi

- Yönetim sunucusuna erişmek için ara sunucu kullanımı (İç güvenlik ilkesi)

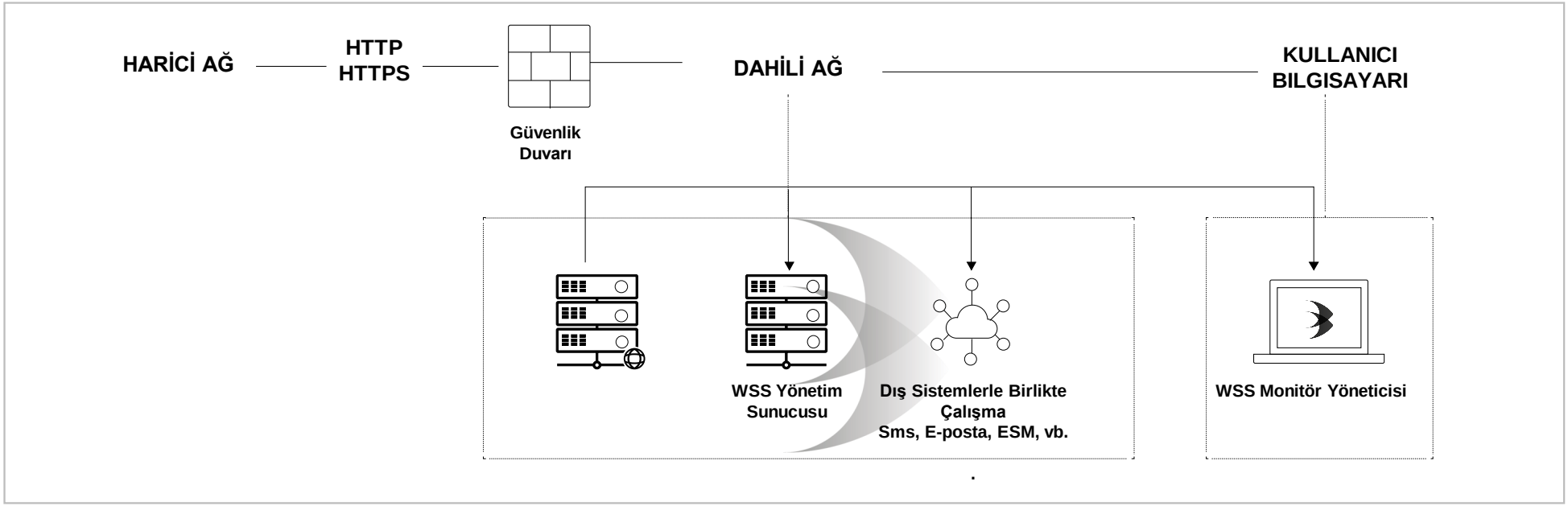
REKABETÇİL ÜSTÜNLÜK

Uzmanlık	UMV, 2008'den beri WSS geliştirme ve özelleştirme ile uğraşmaktadır. Web kabuğu algılama, web sayfası sahteciliğini önleme ve veri/dosya kurtarmaya odaklanmış bir şirket olarak, çoklu güvenlik ürünlerine ve SI işletmelerine odaklanmış rakiplerine kıyasla alanında profesyonellik elde etmiştir - 6 adet web kabuğu ve web güvenliği patenti, CC ve GS sertifikası - Lider güvenlik kontrol şirketleri olan SAMSUNG SDS, GABİA vb. ile ortak çözüm güncelleme
Referans	• İç pazar payında 1 numara • 250 müşterisine kurulmuş ve işletilmekte olan 25.000 den fazla aracı(agent) • Yerli yabancı büyük holdingler, kamu ve finans kurumları olan müşterileri için sürekli özelleştirme, araştırma ve geliştirme • Minimum işletme insan gücü ile maximum verimlilik • Operasyonel destek için çeşitli uygulamalar
İşlev	• Tespit işlevi uzmanlığı - Hash değerleri kullanarak bilinen web kabuklarını algılama/yönetme - Siyah, beyaz ve gri listeleme (kötü amaçlı URL) aracılığıyla aşırı tespit işlevini destekler - Tespit edilen web kabuğu ve kötü amaçlı kalıp risk ve derecelendirme bilgisi sağlar (tespit edilen web kabuğunun hızlı eylemi için yönlendirme) • Entegre web güvenliğine sahip ürünler - Web sunucusu/WAS ayar dosyası değişikliği algılama işlevi (patentli) - Web kabuğu saldırgan IP tespit/izleme işlevi (ikincil ve üçüncül saldırılara karşı hızlı savunma sağlar) - Dosya değişikliği, ortam ayarları değişikliği vb. gibi geliştirilmiş güvenlik aralığı
Güvenilirlik & Ölçeklenebilirlik	• Bulut tabanlı ortamlarda kapsamlı destek • Müşteri sistemleriyle birlikte çalışmayla ilgili çeşitli deneyimler • HA konfigürasyonu (Active/Active) ve kesintisiz hizmet

WSS SİSTEM YAPILANDIRMASI

WSS çözüm yapısı

- WSS yönetim sunucusu S/W,
- WSS aracısı
- WSS yönetici bilgisayar programından (yönetici) oluşur.



İÇERİK

WEBSERVER SAFEGUARD

BİZİ TERCİH EDEN ANA MÜŞTERİLERİMİZ

umv

WEB HİZMETLERİNİZİ WSS İLE KAPSAMLI KORUYUN

Tanıtım Videosuna Git

Bize Ulaşın

+90 (212) 266 21 88

+90 (536) 415 86 96

www.umvwebsecurity.com

sales@umv.co.kr

umv