FORENSOFT

SİBER TEHDİT KALKANI

YERLİ ve MİLLİ

Yapay zekâ tabanlı, kötü amaçlı dosya ve uygulamalarla gerçekletrilen siber saldırılara karşı savunma sistemi

YAPAY ZEKÂ

Machine Learning System siber güvenlik sistemi

TÜRKİYE'DE BİR İLK !

DÖKÜMAN KORUMA KALKANI

Tehdit Yok ! Veri Kaybı Yok !

SIFIRINCI GÜN ATAKLARI'na karşı etkin koruma

zero-day attack protection

- Kurumsal ağ denetimi ve güvenliği
- Web trafiği tehdit engelleme
- E-Posta tehditlerine karşı koruma
- Zararlı uygulama ve dosya tespiti

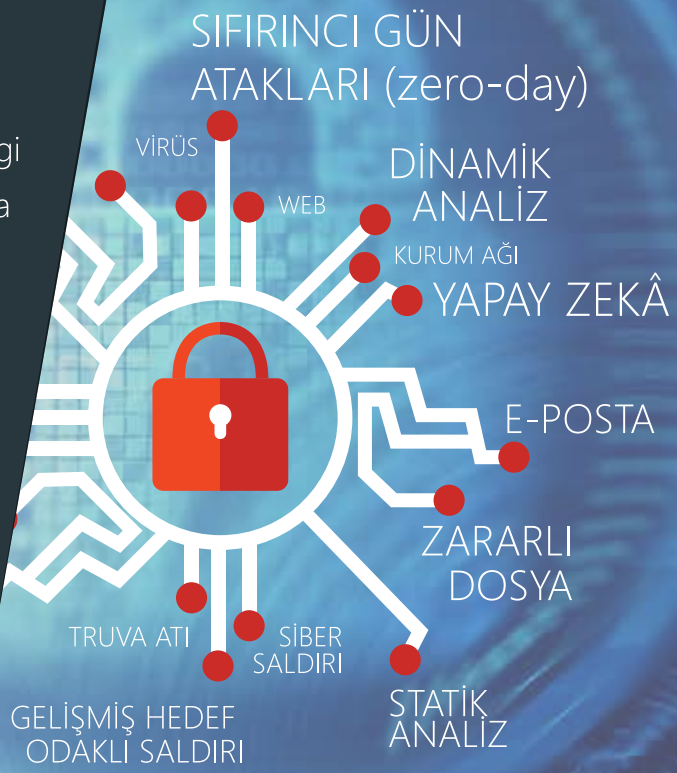
YERLİ ÜRETİM

TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ üyesidir.

SİBER TEHDİT NEDİR ?

Kamu ve özel kurumların bilgi teknolojileri altyapısı büyük oranda **web, e-posta** ve web üzerinden **dosya** alışverişine bağımlıdır.

Dünyadaki siber saldırıların **%90**'ından fazlası, bu haberleşme kanallarını, kurumlara sızmak, değerli verilerine ulaşmak veya zarar vermek için kullanmaktadırlar.



Ülkemizde kurumsal olarak kullanılan Antivirüs yazılımlarının neredeyse tamamı yabancı menşeilidir.

Bu ürün antivirüs yazılımlarından çok daha etkin bir koruma sağlamaktadır.

YAPAY ZEKÂ

Siber Tehdit Kalkanı, web, e-posta, dosya transferi gibi işlemler esnasında yazılımların veya dosyaların davranışlarını kurum ağından tamamen izole edilmiş sanal makineler üzerinde yapay zeka teknolojisini kullanarak inceler ve tehdit unsurunu sisteme henüz erişmeden engeller.

Antivirüs programları sadece, zaten bilinen ve daha önce başka sistemlere zarar verdikten sonra kötü amaçlı olduğu anlaşılmış dosyaları tespit edebilirler.

Yapay Zekâlı Statik ve Dinamik Analiz Motoru

Siber Tehdit Kalkanı ise, kurumsal ağ ortamlarına web ve e-posta yolu ile sızmak isteyen ve imza tabanlı anti-virüsler tarafından tespit edilemeyen zararlı yazılımları kurum ağına girmeden önce yapay zekalı statik ve dinamik analiz yöntemiyle tespit eder ve sisteme erişimini engeller.

SIFIRINCI GÜN ATAKLARI

Zero-Day Attacks

Siber Güvenlik Kalkanı ZYDK Sistemi, başka birçok sistemin aksine dokümanlarda yer alan bilinen zararlı yazılımları bulmak yerine dokümanlarda yer alabilecek ve zararlı yazılımların çalıştırılmasına neden olabilecek genel mekanizmaları ortadan kaldırıp etkisiz hale getirerek imza tabanlı anti-virüslerle tespitinin imkansız olduğu ispatlanmış ve kum sandığı tabanlı dinamik analiz ile dahi bulması çok zor sıfırıncı gün ataklarını engelleyebilmektedir.

Siber Güvenlik Kalkanı ZYDK Sistemi Microsoft Ofis ve Adobe PDF dokümanları ile harekete geçerek yayılan sıfırıncı gün zararlı yazılım tehditlerini ortadan kaldırarak nötralize etmek için kullanılabilecek ilk ve tek yerli yazılımdır.

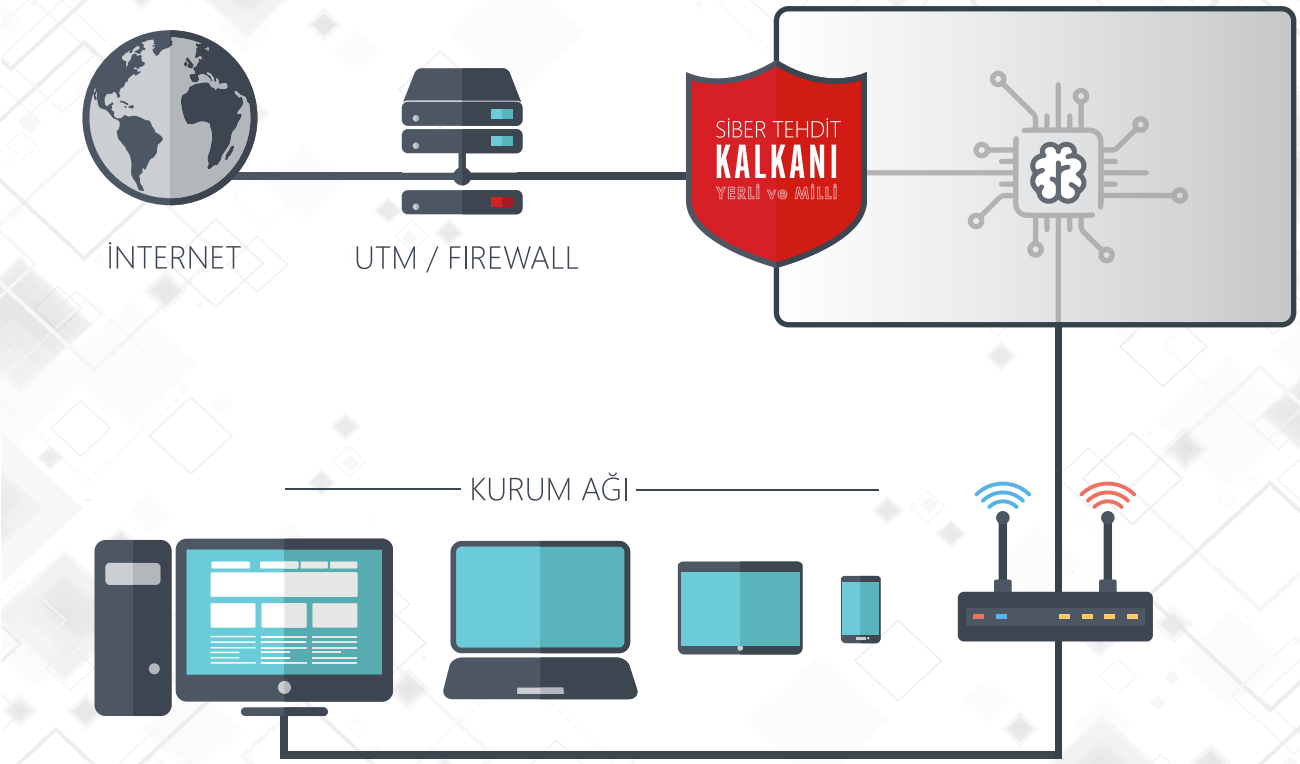
Siber Güvenlik Kalkanı ZYDK Sistemi, başka birçok sistemin aksine dokümanlarda yer alan bilinen zararlı yazılımları bulmak yerine dokümanlarda yer alabilecek ve zararlı yazılımların çalıştırılmasına neden olabilecek genel mekanizmaları ortadan kaldırıp etkisiz hale getirerek imza tabanlı anti-virüslerle tespitinin imkansız olduğu ispatlanmış ve kum sandığı tabanlı dinamik analiz ile dahi bulması çok zor sıfırıncı gün ataklarını engelleyebilmektedir.

Kurumsal ağ ortamlarına web ve e-posta yolu ile sızmak isteyen zararlı yazılımlar, internet ortamından kurum içi ağa girmeden önce ağ geçidinde **Statik Analiz** yöntemi ile analiz edilir.

Şüpheli bir yazılım olduğuna karar verildiği takdirde kurum içi ağa girişi engellenir.

Şüpheli yazılım veya dosyanın sistemden izole edilmiş sanal makinelerde dinamik analizi yapılarak, etki ve aktiviteleri belirlenir. Yapay zeka kullanılarak yazılımın veya dosyanın zararlı olup olmadığı çok daha etkin bir şekilde tespit edilir.

Dinamik Analizi yapılan yazılımın veya dosyanın analiz sonucuna göre beyaz veya kara listeye eklenir. Bu sayede benzer yazılım veya dosyalarla karşılaşıldığında daha da hızlı şekilde engellenmesi sağlanır.



KURULUM

Şeffaf modda kurularak son kullanıcıların bilgisayar sistemlerinde herhangi bir ayar gerektirmeden tüm ağlara kolayca entegre olur.

ENTEGRASYON

Mevcut güvenlik sisteminizde var olan Firewall ve UTM gibi cihazlarınızla ICAP protokolü kullanarak entegre şekilde çalışır.

DÜŞÜK MALİYET

Kurumlarda yer alan sunuculara ve iş istasyonlarına kolayca kurulumu yapılabilir böylece ek bir donanım yatırımı yapılmasına gerek kalmaz.

TEKNİK DESTEK

Sisteminizin güvenliği için konusunda uzman teknik personelimiz size her zaman destek verecektir.

SİBER TEHDİT KALKANI İLE
GÜVENDESİNİZ

Siber Tehdit Kalkanı, kurum ağınıza giren web trafiğini sürekli olarak kontrol altında tutar.

Bütün web trafiği siber tehdit kalkanı üzerinden geçer ve tehditler anında tespit edilebilir.

Kurumdaki bilgisayarlar web sitelerine, sisteme ait vekil sunucular aracığılıyla bağlanırlar, direkt olarak erişemezler.

Bu sayede web sitelerinden kaynaklanan ve indirilen dosyalardan dolayı oluşabilecek tehditler kullanılan bilgisayara ulaşamadan tespit edilir ve engellenir.

Herhangi bir web sitesinden bir dosya indirmek istediğinizde, dosyanın güvenli olup olmadığını, sistemden soyutlanmış sanal makineler üzerinde analiz eder. Herhangi bir zararlı yazılım veya tehdit tespit edilmesi durumunda, ilgili dosya henüz sisteme erişmeden engellenir.

Gelen ve giden bütün mail trafiğinizi kontrol altında tutar. Maillere eklenen dosyaların tehdit içerip içermediğini, kurum ağından soyutlanmış vekil mail sunucuları üzerinde analiz eder. yapılan statik ve dimanik analizler sonucunda, mail ekiyle gelen dosyanın tehdit içermesi durumunda, sisteme erişmeden engellenmesi sağlanır.

Günlük hayatta, iş yaşamınızda sıklıkla kullandığınız veya paylaştığınız PDF, WORD, EXCEL, POWERPOINT gibi gibi zararsız görünen dosyalar **çok tehlikeli virüsler içeriyor olabilirler.**

Siber tehdit kalkanı çalıştırabilir olan her türlü dosyayı, siz indirmeden önce, sistemden izole edilmiş sanal makineler üzerinde çalıştırır ve davranışlarını analiz eder. Tehdit içeren her türlü dosyanın kurum ağına ve bilgisayarlara erişmesini engeller.

Siber tehdit kalkanı, bir sonraki sürümünde, taşınabilir disklerden kaynaklanabilecek tehditleri de önleyecek ve sisteminizin güvenliğini en üst düzeye çıkaracaktır.

TÜRKİYE'de BİR İLK !

TEHDİT YOK !
VERİ KAYBI YOK !

DÖKÜMAN KORUMA KALKANI

Siber Tehdit Kalkanı, analizi yapıldıktan sonra zararlı olduğu tespit edilen PDF ve Office dosyalarının sisteme zarar vermesini engeller. Fakat bunun yanısıra dosyanın içeriğini de görüntüleyebilmenizi sağlar. Bu sayede siber saldırılardan korunmanın yanısıra **veri kayıpları da yaşamazsınız.**

Bu özellik şu an Dünya'daki çoğu siber güvenlik yazılımında bulunmamaktadır !

PDF ve Office dosyaları gün geçtikçe daha çeşitli türden (Görüntü, ses, metin vb.) veriyi depolamak ve paylaşmak amacıyla kullanılmaktadır. Günlük ofis yaşamında herkes tarafından sıkça kullanılan PDF ve Microsoft Office dosyalarındaki açıklar zararlı yazılımların sisteme erişmesi bakımından oldukça tehlikeli olabilmektedirler.

%100 Çözüm

Zararlı uygulama içeren PDF ve Office dosyalarının sisteme zarar vermesini önleme başarımız %99 'un üzerinde olarak raporlanmıştır.

GENEL ÖZELLİKLER

Web tabanlı sistem yönetim ara yüzü
İş yönetim ve kontrol motoru
Ağ yapılandırması
Güvenlik duvarı (firewall) yapılandırması
Web ve e-posta vekil sunucuları
Statik analiz motoru
Dinamik analiz motoru
Loglama ve raporlama

SİBER TEHDİT
KALKANI
YERLİ ve MİLLİ

YENİLİKLER

HTTP/HTTPS trafiği yakalar ve istenirse Virustotal'den sorgulama yapabilir.

Analiz sonucu şüpheli görülen dosyaların yerel ağa girmesine izin vermez.

Yerel ağa entegre olarak Ağ Geçidi ve Şeffaf (transparent) farklı 2 modda çalışabilir.

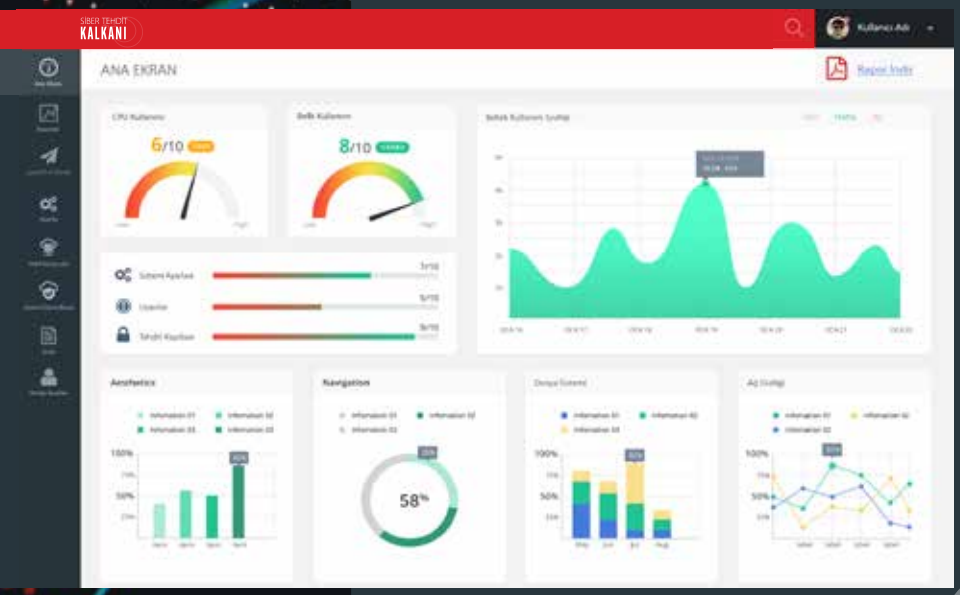
UTM cihazlarının desteklediği ICAP protokolünü desteleyerek bu cihazlarla bütünleşik çalışabilir.

İnternette gezinirken hiçbir zaman web sitelerinin sunucularıyla direkt bağlantı kurulmaz. Vekil sunucular üzerinde gerekli kontroller yapıldıktan sonra, web sitesi herhangi bir tehdit içermiyorsa erişimine izin verilir ve bütün bu işlemler siber tehdit kalkanı yazılımı sayesinde anlık olarak gerçekleştirilir.

YÖNETİM ARAYÜZÜ

Siber Tehdit Kalkanı güvenli (HTTPS bağlantısı) ile ve sadece sistemde tanımlı kullanıcıların bağlanabileceği ve REST (Representational State Transfer) mimarisinde bir web tabanlı sistem yönetim ara yüzüne sahiptir

Sistem yöneticisine aşağıda belirtilen ve normalde komut satırından çok karmaşık ve çok sayıda komut gerektiren işlemleri kolayca yapabilmesine olanak sağlamaktadır.



KULLANICI DOSTU

WEB TABANLI

MOBİL UYUMLU

- Sistemin ağ konfigürasyonu
- Firewall konfigürasyonu
- İp tabanlı politika oluşturma (hangi ip'lerin zararlı yazılım taramasına girip girmeyeceğini içeren politikalar vb.)
- Zararlı yazılım analizi konfigürasyonu (zararlı yazılım analizi yapılacak maksimum dosya boyutu, maksimum arşiv boyutu, dosya türleri, Url beyaz listesi vb.)
- Sanal makinelerin yönetimi ve durumu

STATİK ANALİZ MOTORU

Statik analiz motorumuz, yazılımın sistem üzerinde çalıştırılmadan önce veya herhangi bir dosya açılmadan önce, zararlı özellik içermediğinin tespiti için kullanılmaktadır.

Statik analiz motorumuz tarafından zararlı özellikler içerdiği tespit edilen yazılımlara, erişim engellenebilir veya dinamik analiz motorumuza gönderilebilir.

DİNAMİK ANALİZ MOTORU

Dinamik analiz motorumuz, sanal makine yönetim yapısı ve zararlı yazılım davranış analiz motoru olmak üzere iki kısımdan oluşmaktadır.

Her bir zararlı yazılım analizi, izole edilmiş ve ilk kurulum anına dönülebildiği bir sanal makinede başlatılmaktadır Sanal makine sayısı, kullanılan donanımın kapasitesine göre ayarlanabilmektedir

LOGLAMA VE RAPORLAMA

Loglama ve raporlama modülü ile sistem yöneticisine web trafiğinde tespit edilen zararlı yazılımlar hakkında kapsamlı raporlar sunulabilmektedir.

Ayrıca ICAP, web, e posta ve ftp trafiği logları da tutulmaktadır ve web arayüzünden ip, url, md5, alan adı, id vb. bazlı sorgular yapilabilmektedir.

- Kurumsal ağ denetimi ve güvenliği
- Web trafiği tehdit engelleme
- E-Posta tehditlerine karşı koruma
- Zararlı uygulama ve dosya tespiti

FARKI NEDİR ?

SİBER TEHDİT KALKANI

YERLİ ve MİLLİ

Siber Tehdit Kalkanı ;

- Gelişmiş, hedef odaklı siber tehditlere (APT) karşı savunma kalkanı oluşturur.
- Güçlü yabancı ülkeler, istihbarat örgütleri ve yasadışı örgütler tarafından gerçekleştitilebilen saldırılara karşı güvenlik sağlar.
- Ülkemizdeki çözümlerin %97'si yabancı olup %55'i İsrail, %35'i ise ABD kökenlidir.
- Tamamen yerli kaynaklarla, Türk yazılımcılar tarafından geliştirilmiştir.
- Bu ürün Türkiye'nin tek, yapay zekâ tabanlı siber güvenlik yazılımıdır.
- Yabancı rakiplerine göre çok daha düşük maliyetlidir.

SİBER TEHDİT
KALKANI
YERLİ ve MİLLİ

Ankara Teknoloji Geliştirme Bölgesi
Bilkent Cyberpark
iletisim@forensoft.com

www.sibertehditkalkani.com
www.forensoft.com

FORENSOFT