CyberFortress

ÜRÜN TEKNİK DOKÜMANI

Malware Analyzer 360

Gelişmiş zararlı yazılım ve URL analizi

İmza tabanlı araçlar yalnızca birinin daha önce adını koyduğu tehditleri yakalar. Malware Analyzer 360 dosyaları, bağlantıları ve davranışları gerçekte ne yaptıklarına göre değerlendirir – böylece sıfır gün ve APT etkinliği yerleşmeden önce ortaya çıkar.

cyber-fortress.com | info@cyber-fortress.com

PLATFORM

Tek çekirdek. Her katman onu besler.

CyberFortress, birbirinden bağımsız araçların kataloğu değildir. Her modül telemetrisini tek bir çekirdeğe akıtır, ortak tehdit istihbaratıyla zenginleştirilir ve tek bir istihbarat katmanı tarafından okunur – böylece e-posta akışında yakalanan zararlı bir dosya ile o dosyanın kopyasını çoktan almış olan uç nokta iki olay değil, tek bir olaydır.

MA 360° — platform çekirdeği

Her güvenlik katmanından telemetri toplar, gerçek zamanlı olarak ilişkilendirir ve müdahaleyi orkestre eder. Tespit, sınıflandırma ve kontrol altına alma kararları saniyeler içinde üretilir; analiz motoru bir L1/L2 ekibinin aksi hâlde taşıyacağı manuel triyaj yükünün %80'ine kadarını üstlenir.

DÖRT GÜVENLİK MODÜLÜ

Malware Analyzer 360

Dinamik sandbox'ta kontrollü çalıştırma, statik kod incelemesi, canlı URL kararları ve İçerik Zararsızlaştırma & Yeniden Oluşturma (CDR). Her karar, çıkarılan IoC'ler ve otomatik MITRE ATT&CK eşlemesiyle birlikte gelir.

Mail Gateway

Kimlik avı, BEC, fidye yazılımı ve e-posta kaynaklı APT'lere karşı çok katmanlı savunma. Yapay zekâ destekli kimlik avı önleme, eklerin sandbox analizi, tıklama anında URL yeniden yazma, inline ve BCC konumlandırma, ayrıca Outlook eklentisi.

Threat Hunter

Merkezî analizle desteklenen hafif bir uç nokta ajanı – USB, paylaşım ve indirme denetimi, otomatik triyaj, YARA taramaları, ekran filigranı, kurcalamaya karşı koruma ve air-gap kiosk ile köprü modları.

Cloud Hunter

CVE tabanlı taramayla konteyner ve imaj analizi, bucket açıklık denetimi, bulut dosya sistemi koruması ve hibrit ile çok bulutlu ortamlarda gerçek zamanlı izleme.

CyberFortress TI ile Veri Katmanı

Çok kaynaklı tehdit istihbaratı ve günde terabaytlar ölçeğinde gerçek zamanlı korelasyon – her modülün okuduğu ve geri yazdığı omurga.

CyberFortress AI

Tüm platformu saran davranışsal analitik ve milisaniyelik sınıflandırma; her olaydan öğrenir ve ilerledikçe yanlış pozitifleri azaltır.

NEDEN MALWARE ANALYZER 360

Adına göre değil, davranışına göre

Gelişmiş bir saldırı, hâlihazırda sahip olduğunuz kontrolleri atlatmak için tasarlanır. Adı konmamış hâlde gelir, yükünü saklar, sanal makinede çalışıp çalışmadığını kontrol eder ve bekler. İmza eşleştirme, henüz kimsenin yayımlamadığı bir şeyi tanımlayamaz.

Malware Analyzer 360 başka bir soruyu yanıtlar: *bu dosyayı daha önce gördük mü* değil, *bu süreç meşru bir sürecin asla yapmayacağı bir şey mi yapıyor*. Örnek, sıkılaştırılmış ve tamamen izole bir ortamda kontrollü biçimde çalıştırılır; her sistem çağrısı, kayıt defteri değişikliği, bellek hareketi, ağ bağlantısı ve başlatılan süreç gerçekleştiği anda kaydedilir — statik geçiş ise dosyayı hiç çalıştırmadan kod düzeyinde okuyup imzaları, şüpheli API çağrılarını, paketleme ve şaşırtma tekniklerini çıkarır.

İki yöntem birlikte, her birinin tek başına açık bıraktığı boşluğu kapatır: bilinen ailelerde *ve* sıfır gün örneklerinde güçlü kapsama. Atlatma işe yaramaz. Uyuyan, saklanan veya sandbox'ı parmak izinden tanımaya çalışan zararlı yazılım eninde sonunda harekete geçmek zorundadır; geçtiğinde davranış izi onu ele verir.

SANAL MAKİNELERDE KARANTİNA

Kontrollü çalıştır
Özelleştirilmiş, tamamen izole bir sanal makinede çalıştırılır.

İzle
Binlerce örüntü kontrolü ve yerleştirilmiş sensörler her eylemi kaydeder.

Analiz et
Yapay zekâ destekli çok akışlı analiz, saldırının tüm bağlamını ortaya koyar.

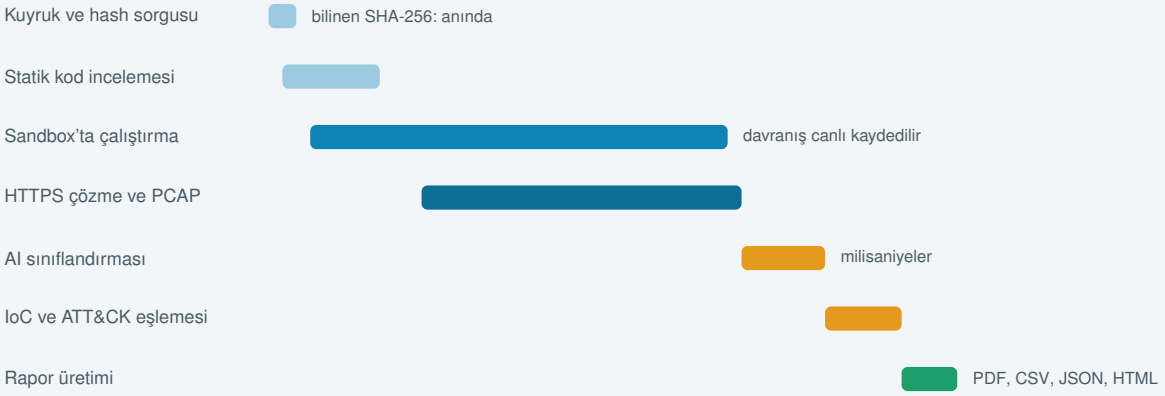
%99,7
Bilinen ve daha önce görülmemiş örneklerde tespit oranı

~2 dk
APT örneği için statik ve dinamik tam triyaj raporu

18
Her saldırının profillendiği ayrı karakteristik

ATT&CK
Bulgular taktik, teknik ve prosedürlere eşlenir

Gönderimden rapora – iki dakika nereye gidiyor



APT sınıfı bir Windows örneği için gösterge niteliğinde süreler. Geçişler eşzamanlı yürür; kontrollü çalıştırma hâlâ kayıt alırken statik okuma çoktan tamamlanmıştır.

MOTORUN İÇİNDE

Dört analiz katmanı, tek karar

Analizöre giren bir dosya ya da bağlantı, aynı anda her açıdan incelenir. Davranış izolasyonda izlenir, kod hiç çalıştırılmadan okunur, hedefler canlı olarak çözümlenir ve kullanıcıya ulaşacak her şey varmadan önce temiz biçimde yeniden oluşturulabilir.

Dinamik analiz

Örnek, sıkılaştırılmış ve izole bir ortamda çalıştırılır; her sistem çağrısı, kayıt defteri değişikliği, bellek hareketi, ağ bağlantısı ve başlatılan süreç gerçek zamanlı kaydedilir. Free-Run teknolojisi, analistin zararlı etkinliği olurken izlemesine olanak tanır.

Statik analiz

Dosya çalıştırılmadan okunur: imza çıkarımı, şüpheli API ve fonksiyon çağrıları, paketleme ve şaşırtma teknikleri, gömülü kaynaklar ve bilinen zararlı kod örüntüleri.

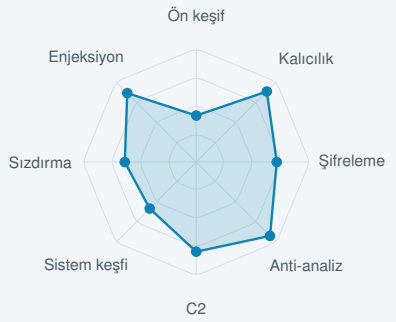
URL analizi

Bağlantılar çözümlenir ve yönlendirmeler boyunca gerçek hedefine kadar takip edilir – kimlik avı ve kimlik bilgisi toplama sayfaları, komuta kontrol (C2) noktaları ve drive-by indirme zincirleri – tek bir üretim makinesini bile riske atmadan.

İçerik Zararsızlaştırma & Yeniden Oluşturma

CDR aktif içeriği – makrolar, gömülü betikler, bozuk yapılar – söker ve dokümanı temiz, kullanılabilir bir dosya olarak yeniden oluşturur; böylece iş akışı, bekleyemeyeceği bir kararı beklemek zorunda kalmaz.

Davranışsal sınıflandırma



Bir bankacılık truva atı örneği için temsilî profil. Her saldırı tek bir karara indirgenmek yerine 18 karakteristiğe karşı olasılıksal olarak puanlanır.

İki geçiş neden birlikte çalışır

Adlandırılmış aileleri daha önce görülmemiş örneklerle harmanlayan bir iç korpustaki kapsama. Hiçbir yöntem tek başına birleşik değere ulaşamaz; birleşik motor ise atlatmanın bilinçli olduğu yerlerde de ayakta kalır.

ANALİSTE NE DÖNÜYOR

Saldırı Haritası

Örneğin ürettiği her süreç, dosya ve sistem değişikliğini gösteren, dal dal gezilebilen tamamen dinamik bir yürütme zinciri haritası.

Sınıflandırma

18 karakteristikten oluşan yelpazede yapay zekâ destekli olasılıksal puanlama; radar grafiği olarak sunulur, böylece aile ve niyet bir bakışta görülür.

Ağ Trafiği

HTTPS trafiği çözüldükten sonra bağlantı kurulan alan adları ve portlar coğrafi olarak gösterilir – C2 altyapısı ve verinin nereye gittiği açığa çıkar.

Tam Rapor

Tüm bulguları, göstergeleri ve ATT&CK eşlemelerini içeren kapsamlı rapor.

IoC Listesi

Analizden çıkarılan ihlal göstergelerinin (IoC) kapsamlı listesi.

AÇIK MİMARİ

Kullandığınız yapının üzerine oturur

Amaç tek güvenlik tedarikçiniz olmak değil – zaten parasını ödediğiniz araçları daha çok çalıştırmak. Hafif ajanlar uç noktalardan en düşük ayak iziyle veri toplar; RESTful API ise motoru 40'tan fazla güvenlik aracına iki yönlü veri ve aksiyon akışıyla bağlar.

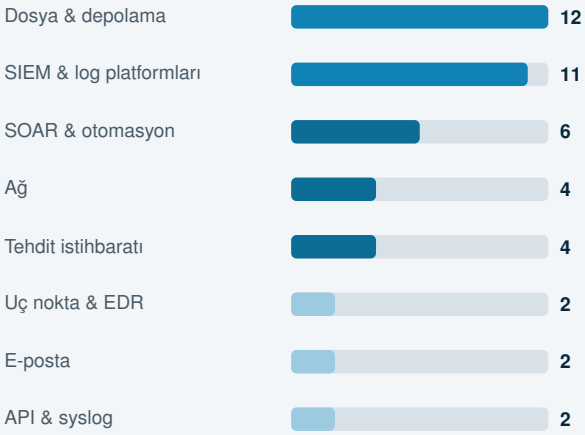
43
Sekiz kategoride bugün kullanıma hazır entegrasyon

16
Hiç kod gerektirmeyen dahili konnektör

2 yönlü
Yalnızca dışa aktarım değil; iki yönlü veri *ve* aksiyon akışı

REST
Listede olmayan her şey için tam API

43 entegrasyon nerede duruyor



On altısı dahili konnektör olarak gelir; gerisi RESTful API veya syslog üzerinden bağlanır. Listede olmayan her şey doğrudan bağlanabilir.

İki giriş yolu

Ajan tabanlı toplama. Hafif ajanlar uç noktalardan veriyi otomatik toplar; makineye en düşük yükü bindirerek en yüksek görünürlüğü sağlar. Uç nokta ve e-posta güvenlik modülleriyle doğal biçimde birlikte çalışır.

RESTful API. Açık API, motoru 40'tan fazla güvenlik aracına iki yönlü akışla bağlar ve kurum içinde geliştirdiğiniz her şey için de aynı ölçüde kullanılabilir – dosya ve URL gönderin, kararları sorgulayın ya da alın, tam raporları ve IoC'leri çekin, platform aksiyonlarını tetikleyin.

Tek alarm, tek orkestre edilmiş müdahale

01 Alarm
SIEM, anormal dışa doğru trafik için alarm üretir.

02 Playbook
SOAR playbook'u analist devreye girmeden otomatik çalışır.

03 İzole et
MA 360° uç noktayı izole eder ve şüpheli dosyayı gönderir.

04 Analiz
Sandbox, IoC'ler ve ATT&CK eşlemesiyle bir karar döndürür.

05 Uygula
IoC'ler otomatik olarak EDR'ye ve güvenlik duvarına iletilir.

06 Kayıt
Talep kaydı kendini günceller, denetim izi kapanır.

Kayıtları sistemler arasında taşımak işin kolay yarısı – değer, bağlantının veriyle birlikte aksiyonu da taşımasıyla ortaya çıkar. Eskiden bir dizi insan devrinden oluşan süreç tek bir akışa dönüşür.

PRATİKTE

Ekipler nerede kullanıyor

Analizör, platformun geri kalanının arkasında bir hizmet olarak çalışır — ve API üzerinden doğrudan sizin araçlarınıza yanıt verir.

E-posta ekleri

Mail Gateway üzerinden gelen her ek kontrollü olarak çalıştırılır ve politika gerektiriyorsa teslimden önce CDR ile temiz biçimde yeniden oluşturulur.

Kullanıcıların yüklediği dosyalar

Portallar, talep yönetim sistemleri, SharePoint, OneDrive ve dosya paylaşımları; dosya hiç saklanmadan veya açılmadan önce karar için gönderim yapar.

Şüpheli URL'ler

Analistler ve otomatik playbook'lar, tek bir üretim makinesini bile maruz bırakmadan bir bağlantının gerçek hedefini ve amacını çözer.

Uç noktalarda APT avı

Threat Hunter'ın topladığı şüpheli artefaktlar analizöre geri gönderilir; sessiz bir anomali, adı konmuş ve eşlenmiş bir sızmaya dönüşür.

Adli inceleme ve olay müdahale

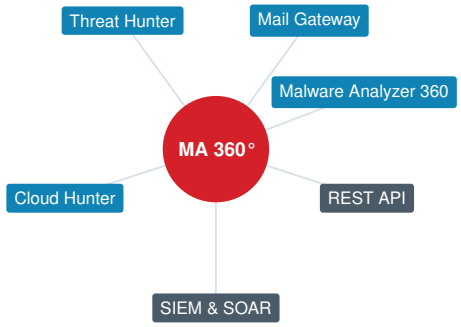
Toplu gönderim, saklanan kayıtlar, ekran görüntüleri ve süreç zaman çizelgeleri; olay müdahale ekiplerine bir vakanın gerçek-ten üretmesi gereken delil zincirini verir.

SOC eskalasyonu

L1 analistinin kapatamadığı vaka, zincirin üstüne devredilen belirsiz bir karar yerine kesin bir yanıtla geri döner.

Tek gönderim, birçok hedef

Karar, sürecin sonu değildir. Çıkarılan göstergeler doğrudan onları uygulayan araçlara iletilir ve olay kaydı kendini günceller.



Karar	zararlı ya da temiz
IoC'ler	hash'ler ve altyapı
ATT&CK eşlemesi	taktikler ve teknikler
Rapor	PDF, CSV, JSON, HTML

Sizi atlatan örneği bize gönderin.

Kendi ortamınızda 30 günlük bir PoC çalışması yürütün ya da başka bir yerde belirsiz dönen dosyayı bize getirin.

cyber-fortress.com
info@cyber-fortress.com

TEKNİK ÖZELLİKLER

Özellikler ve yetenekler

TESPİT & ANALİZ MOTORLARI

- Sıkılaştırılmış, izole sandbox içinde dinamik davranış analizi
- Örneği hiç çalıştırmadan statik kod incelemesi
- Tüm yönlendirme zincirini çözen canlı URL analizi
- Doküman ve arşivler için İçerik Zararsızlaştırma & Yeniden Oluşturma
- *Zararlı* ve *Temiz* için yapay zekâ destekli olasılıksal sonuç
- Saldırılar 18 ayrı karakteristik üzerinden profillenir
- Paketli, şaşırtılmış ve polimorfik örnekler davranıştan yakalanır
- Çok aşamalı saldırı zincirleri her aşamada takip edilir
- Uyku, sanal makine kontrolü ve diğer sandbox atlatma teknikleri etkisiz
- Snort ve Suricata imza eşleştirmesi
- Gönderimlere ve saklanan artefaktlara YARA kuralı eşleştirmesi
- Yüksek hacim altında ayakta kalan paralel eşzamanlı analiz
- Bellek, süreç, kayıt defteri, dosya sistemi ve ağ sensörleri
- Her çalıştırmada binlerce davranışsal örüntü kontrolü

KAPSAMA

- İç içe ve parola korumalı arşivler dâhil tüm dosya türleri
- Office dokümanları, PDF'ler, betikler, kurulum dosyaları ve çalıştırılabilirler
- Windows, Linux, Android ve konteyner yükleri
- Tamamen özelleştirilebilir sanal makine imajları ve kurulu yazılımlar
- Özel çalıştırma süreleri, bölge ayarları ve ağ profilleri
- Dosya, URL, toplu gönderim veya API üzerinden gönderim

ANALİZ & RAPORLAMA

- Saldırı topografyasında gezinmek için tamamen dinamik Saldırı Haritası
- Detaya inilebilen etkileşimli artefakt ve ağ haritaları
- Free-Run teknolojisiyle zararlı etkinliği sanal makinede canlı izleme
- Radar grafiği olarak sunulan olasılıksal sınıflandırma
- HTTPS trafiğini çözer, etkinliğin kaynak ve hedeflerini haritalar
- Bağlantı kurulan alan adları ve portlar coğrafi olarak gösterilir
- İlişkili zafiyet eşleşmelerini içeren işlem kayıtları
- Bellek dökümleri, diske bırakılan dosyalar, çıkarılan yükler ve PCAP'ler indirilebilir
- Her gönderim için saklanan ekran görüntüleri ve süreç zaman çizelgeleri
- Otomatik IoC çıkarımı – hash'ler, alan adları, IP'ler, mutex'ler ve bırakılan dosya yolları
- Otomatik MITRE ATT&CK taktik ve teknik eşlemesi
- VirusTotal, YARA ve MITRE ATT&CK entegrasyonu
- Daha önce analiz edilmiş dosyalar için SHA-256 doğrulamalı anlık rapor
- PDF, CSV, JSON ve HTML rapor üretimi
- Adli inceleme ve uyumluluk için delil niteliğinde saklama
- Yapay zekâ asistanı bulguları sade bir dille yorumlar

OTOMATİK TRİYAJ

- Önem derecesi puanlaması gönderim kuyruğunu otomatik sıralar
- Bilinen temiz ve bilinen zararlı, kuyruktan anında düşer
- L1/L2 ekibinin manuel işinin %80'ine kadarını üstlenir
- Sessiz ve uzun süreli zararlı etkinlik gömülmek yerine öne çıkarılır

BİLDİRİMLER

- Özelleştirilebilir kayıtları syslog sunucunuza gönderir
- Analiz sonuçlarını istenen her biçimde e-postayla iletir
- Dinamik, anlaşılır raporları üçüncü taraflara dağıtır
- Karar tamamlandığında webhook geri çağrıları

SİSTEMLER & ENTEGRASYONLAR

- Sekiz kategoride 43 entegrasyon – 16 dahili konnektör
- İki yönlü veri ve aksiyon akışlı RESTful API
- SIEM: Splunk, Sentinel, QRadar, Elastic, LogRhythm, ArcSight, Chronicle, Graylog, Wazuh, Sumo Logic, Rapid7 InsightIDR
- SOAR: Cortex XSOAR, Splunk SOAR, Forti-SOAR, Tines, Swimlane, Torq
- EDR/EPP: CrowdStrike Falcon ve Microsoft Defender
- Tehdit istihbaratı: MISP, OpenCTI, ThreatQ, Anomali ThreatStream
- IMAP ve SMTP entegrasyonu; Postfix e-posta akışı
- Bulut depolama – SharePoint, OneDrive, Drive, Box, Dropbox, S3, Azure Blob, Nextcloud
- Yerel dosya paylaşım sistemi ve FTP/SFTP entegrasyonu
- ICAP proxy ve ağ TAP arabirimi entegrasyonu
- Yukarı akış besleyici olarak Broadcom CAS ve OPSWAT MetaDefender
- Özel Outlook eklentisi
- Geri kalan her şey için syslog akışı

KONUMLANDIRMA

- Yerinde (on-premise), bulut veya hibrit konumlandırma
- Kiosk ve köprü modlarıyla air-gap konumlandırma
- Tek düğümden ulusal ölçekli ortamlara kadar ölçeklenir

KURAL SETLERİ & GÜNCELLEME DÖNGÜSÜ

- Gece çalışan botlar algoritmalarımızı küresel zararlı yazılım veri tabanlarına karşı doğrular
- Bir eksiklik gözlendiğinde yapay zekâ yeniden eğitilir
- İçerik ekibi canlı saldırı araştırmasından her gün yeni kural yazar
- Bizimkilerin yanında özel YARA, Snort, Sigma ve IoC içeriği
- Tek tıkla sorunsuz ürün güncellemesi

YÖNETİCİ İŞLEVLERİ

- Rol tabanlı kullanıcı yönetimi
- Analiz sonuçlarını kimin okuyabileceğine dair rol kısıtlaması
- Verilerinizi yedekleyin ve geri yükleyin
- Her motor için sağlık izleme
- Gerçek zamanlı disk kapasitesi izleme
- Gönderimlerin ve yönetici işlemlerinin tam denetim izi

CyberFortress

Çünkü tespit edilemeyeni tespit ediyoruz.

Malware Analyzer 360, tek bir çekirdek üzerindeki dört modülden biridir. Tek başına konumlandırın ya da çevresindeki katmanları devreye alın; tek bir karar tüm ortamı yönetsin.

PLATFORMA GENEL BAKIŞ

MA 360°
Çekirdek — toplama, korelasyon ve orkestrasyon.

Malware Analyzer 360
Sandbox, statik analiz, URL kararları ve CDR.

CyberFortress TI
Kapsamlı tehdit istihbaratı ve analitiği.

Mail Gateway
Kimlik avı, BEC, fidye yazılımı ve e-posta kaynaklı APT'ler.

Threat Hunter
Hafif ajan, YARA taramaları ve air-gap modları.

Cloud Hunter
Konteyner, bucket ve bulut dosya sistemi koruması.

CyberFortress AI
Her modülü saran davranışsal analitik.

cyber-fortress.com

info@cyber-fortress.com