CyberFortress

PLATFORM TEKNİK DOKÜMANI

MA 360°

Her savunma katmanına güç veren çekirdek

MA 360° yığındaki bir ürün daha değildir. Platformun merkezinde duran işleme, analiz ve orkestrasyon motorudur – her güvenlik katmanından gelen telemetrinin toplandığı, ilişkilendirildiği ve bir karara dönüştürüldüğü yerdir.

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

PLATFORM

Tek çekirdek. Tek veri modeli. Tek konsol.

Saldırı hangi vektörden gelirse gelsin aynı motora düşer ve en ince ayrıntısına kadar analiz edilir. Bir platformu ürün paketinden ayıran şey budur: bir e-posta ekinde görülen dosya, onu açan uç nokta ve ulaştığı bulut bucket'ı üç uyarı 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 milisaniyeler içinde üretilir; analiz motoru bir L1/L2 ekibinin aksi hâlde taşıyacağı manuel triyaj yükünün %80'ine kadarını üstlenir.

ÇEKİRDEĞİN SÜRDÜĞÜ MODÜLLER

Malware Analyzer 360

Bilinmeyen ve hedefli saldırılar için dinamik sandbox, statik analiz, URL kararları ve 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 koruma; tıklama anında URL yeniden yazma ve inline ya da BCC konumlandırma ile.

Threat Hunter

Hafif ajan, otomatik triyaj, YARA taramaları, ekran filigranı, kurcalamaya karşı koruma ve air-gap kiosk ile köprü desteği.

Cloud Hunter

Hibrit ve çok bulutlu ortamlarda konteyner ve imaj analizi, bucket taraması ve gerçek zamanlı bulut dosya sistemi koruması.

CyberFortress TI ile Veri Katmanı

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

Arayüz, API, Ajan & 3. Taraf

Açık mimari – hâlihazırda sahip olduğunuzu değiştirmeden platformu genişleten 43 hazır entegrasyon.

ÇEKİRDEK NEDEN ÖNEMLİ

Her şeyin dayandığı altı görev

Her güvenlik ürünü uyarı üretir. Çok azı karar üretir. Aradaki fark, bir değerlendirmenin yapılması gerektiği anda ortamda resmin bütününü tutan bir şeyin olup olmamasıdır – ki bu, çekirdeğin görevidir.

Ajanlar, API'ler ve üçüncü taraf konnektörler; kayıtları, sandbox kararlarını, uç nokta telemetrisini, e-posta akışını ve bulut etkinliğini tek bir normalleştirilmiş modele besler; böylece hâlihazırda sahip olduğunuz araçlar değiştirilmek yerine değerini korur. Veri Katmanı tehdit istihbaratını, geçmiş bağlamı ve davranışsal referans değerlerini ekler. CyberFortress AI davranışı sınıflandırır ve riski puanlar.

Sonra çekirdek harekete geçer. Tek karar, çok aksiyon: uç noktayı izole et, mesajı karantinaya al, SIEM'e bir IoC gönder ve talep kaydını aç – hem platformun kendi modüllerini hem mevcut SOAR playbook'larınızı aynı karardan, dakikalar değil milisaniyeler içinde sürerek. Yavaş ve sessiz APT kampanyalarına karşı bu fark oyunun tamamıdır.

ÇEKİRDEK GERÇEKTE NE YAPIYOR

Birleşik veri toplama
Her kaynak tek bir ortak modele normalleştirilir.

Gerçek zamanlı işleme
Dakikalar değil, milisaniyeler içinde karar.

Derin korelasyon
Üç uyarı, tanımlanmış tek bir olaya dönüşür.

Orkestrasyon
Tek karar her modülü ve SOAR'ınızı sürer.

360°
Uç nokta, e-posta, bulut ve ağ telemetrisi tek ekranda

< 1 sn
Tespit, sınıflandırma ve müdahale kararları

%80
Güvenlik analistleriniz için daha az manuel triyaj işi

Milyonlar
Her saniye işlenen olay ve zararlı etkinlik

Korelasyon ve zenginleştirme neyi değiştiriyor

Platformu önceki araçlarıyla karşılaştıran ekiplerin bildirdiği değerler. Kazanç daha uzun bir uyarı listesinden değil bağlamdan gelir – ham olayların yerini zenginleştirilmiş olaylar alır.

NASIL ÇALIŞIR

Sinyalden aksiyona

Platforma giren her olay, hangi modül üretmiş olursa olsun aynı dört adımı izler. Yeni bir modülü devreye alındığı gün kullanışlı kılan da bu tutarlılıktır.

Her olayın izlediği dört adım

01
Topla
Uç nokta ajanları, e-posta ağ geçidi kancaları, bulut konnektörleri ve API çağrıları ham telemetriyi sürekli akıtır.

02
Zenginleştir
Veri Katmanı tehdit istihbaratını, geçmiş bağlamı ve davranışsal referans değerlerini ekler.

03
Karar ver
CyberFortress AI davranışı sınıflandırır, riski puanlar ve MITRE ATT&CK'e eşler.

04
Harekete geç
Kontrol altına alma ilgili modüllerde ve SIEM, SOAR, EDR ile talep sistemlerinde tetiklenir.

Toplama süreklidir, zenginleştirme otomatiktir ve karar aksiyonları da beraberinde taşır. Politika aksini söylemedikçe hiçbir adım bir insanı beklemez.

Altı sorumluluk

Birleşik veri toplama
Ajanlar, API'ler ve üçüncü taraf konnektörler; kayıtları, sandbox kararlarını, uç nokta telemetrisini, e-posta akışını ve bulut etkinliğini tek bir normalleştirilmiş modele besler.

Gerçek zamanlı işleme
Tespit, sınıflandırma ve müdahale milisaniyeler içinde üretilir – saldırı, ölçülecek bir etki doğurmadan durdurulur.

Derin korelasyon
Çekirdek, modüller, zaman ve varlıklar arasındaki ilişkili olayları birleştirir, zenginleştirir ve parçaları değil zincirin bütününü sunar.

Orkestrasyon
Tek karar, çok aksiyon: izole et, karantinaya al, IoC gönder, talep kaydını aç — platformun modüllerinde ve kendi playbook'larınızda.

Analist kazancı
Analiz motoru, bir L1/L2 ekibinin aksi hâlde taşıyacağı manuel işin %80'ine kadarını kaldırır; böylece analistler saatlerini insan gerektiren vakalara ayırır.

Ayakta kalan ölçek
Saniyede milyonlarca olayı sürdürmek üzere kurulmuş yüksek performanslı bir mimari – aynı motor hem orta ölçekli bir kurumu hem ulusal ölçekli bir ortamı çalıştırır.

Altta duran katmanlar

CyberFortress AI — davranışsal istihbarat

Dört güvenlik modülü — analiz ve uygulama

MA 360° — toplama ve orkestrasyon

CF TI ile Veri Katmanı — korelasyon ve bağlam

Veri Katmanını besleyenler

CyberFortress Tehdit İstihbaratı – her gün ölçekte analiz ettiğimiz zararlı yazılımlardan beslenen kendi operasyonumuz.

Platform içi telemetri – kayıtlar, sandbox kararları, URL sonuçları, uç nokta telemetrisi, konteyner davranışı ve bulut etkinliği.

Üçüncü taraf istihbarat – dış ticari ve topluluk beslemeleri; böylece tek bir üreticinin görüşüyle sınırlı kalmazsınız.

Makine öğrenmesi referansları – modeller normal davranışı kendi verinizden öğrenir ve anomalileri otomatik işaretler.

AÇIK MİMARİ

Yığınınızı değiştirmeden genişletin

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.

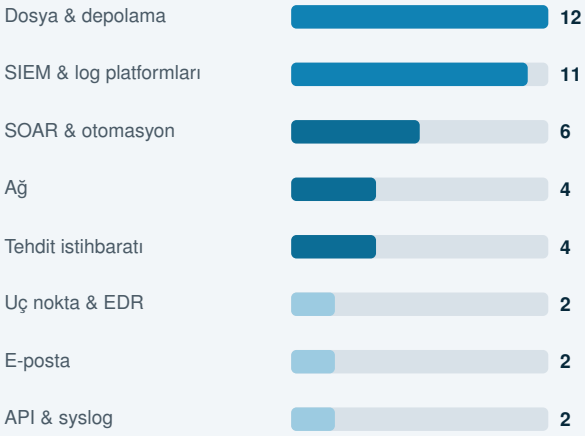
43
Sekiz kategoride bugün kullanıma hazır entegrasyon

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

Çekirdek günlük işte neyi değiştiriyor

Çekirdek bir kez konumlandırılır ve sonrasında devreye alınan her modül onun sayesinde keskinleşir. Ekiplerin ilk bildirdiği farklar bunlar.

Üç uyarı yerine tek olay

Bir e-posta ekinde görülen dosya, onu açan uç nokta ve ulaştığı bulut bucket'ı; üç konsolda üç talep kaydı yerine, zincirin bütünü görünür hâlde tek bir anlatıda birleşir.

Kendini sıralayan bir kuyruk

Otomatik önem derecesi sıralaması, değerlendirme gerektiren vakaları en üste taşır. Bilinen temiz ve bilinen zararlı anında düşer.

Mevcut araçlar değerini korur

SIEM, SOAR, EDR ve talep sistemleri yerlerinde kalır ve daha iyi veri alır. Güvenlik veri gölü yetkili kaynak olmayı sürdürür; ekibinizin zaten izlediği panolar çalışmaya devam eder.

Devretmeden kontrol altına alma

Bir uç noktayı izole etmek, bir mesajı karantinaya almak ve bir IoC göndermek; hepsi aynı karardan, aynı saniye içinde, bir insan sistemler arasında haber taşımadan yürür.

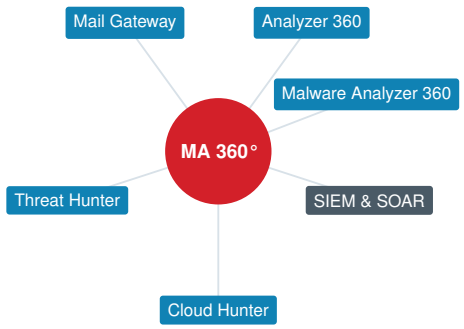
Yeniden tasarım olmadan ölçek

Aynı motor, yoğun tehdit trafiği altında hem orta ölçekli bir kurumu hem ulusal ölçekli bir ortamı çalıştırır – yüksek performanslı bir mimaride saniyede milyonlarca olay.

Analistler kendilerini gerektiren işte

L1/L2 triyajının %80'ine kadarı motor tarafından üstlenilir ve gelen uyarılar açmaya değecek kadar zenginleştirilmiş olur.

Tek karar nereye ulaşıyor



Karar	sınıflandırılmış ve puanlanmış
Kontrol altına alma	izole et, karantina, engelle
Dağıtım	SIEM, EDR, güvenlik duvarına IoC
Kayıt	talep kaydı ve denetim izi

Çekirdeği kendi verinizle çalışırken görün.

Kendi ortamınızda 30 günlük bir PoC çalışması başlatın ya da güvenlik ekibinizle teknik bir mimari oturumu planlayın.

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

TEKNİK ÖZELLİKLER

Özellikler ve yetenekler

VERİ TOPLAMA

- Uç nokta ajanları, e-posta ağ geçidi kancaları ve bulut konnektörleri
- Hâlihazırda kullandığınız her araçtan RESTful API ile gönderim
- Mevcut güvenlik ürünleri için üçüncü taraf konnektörler
- Kayıtlar, olay kayıtları ve sandbox kararları birlikte alınır
- Her şey tek bir ortak veri modeline normalleştirilir
- Yüksek performanslı motorlarla günde terabaytlar sürdürülür
- Mevcut araç yatırımları değerini korur

İŞLEME & KORELASYON

- Bir saniyenin altında tespit, sınıflandırma ve müdahale
- Saniyede milyonlarca olay sürdürülür
- Modüller, zaman ve varlıklar arasında gerçek zamanlı korelasyon
- İlişkili olaylar tek bir olay anlatısında birleştirilir
- CyberFortress Tehdit İstihbaratı ile zenginleştirme
- Geçmiş bağlam ve davranışsal referans değerleri eklenir
- Zenginleştirmeyle tehdit görünürlüğünde %95'e kadar artış
- Yanlış pozitiflerde %95'e kadar azalma

KARAR & SINIFLANDIRMA

- CyberFortress AI ile milisaniyeler içinde davranışsal sınıflandırma
- LLM ve makine öğrenmesiyle tehdit yorumlama
- Yalın bir karar değil, risk puanlaması
- Otomatik MITRE ATT&CK taktik ve teknik eşlemesi
- Her olaydan uyarlanabilir öğrenme
- Kendi referans değerlerinize karşı anomali tespiti
- Ortalama tespit süresinde %90'a kadar iyileşme

ORKESTRASYON & MÜDAHALE

- Tek karar her modülü eşzamanlı sürer
- Karar anında uç nokta izolasyonu
- Mesaj karantinası ve geriye dönük kaldırma
- SIEM, EDR ve güvenlik duvarına IoC gönderimi
- Talep kaydı oluşturma, güncelleme ve kapatma
- Mevcut SOAR playbook'ları aynı karardan sürülür
- Playbook'lar analiz için çekirdeğe geri çağrı yapabilir

ANALİST DENEYİMİ

- Uç nokta, e-posta, bulut ve ağ telemetrisi tek ekranda
- Kuyruğun otomatik triyajı ve önem derecesi sıralaması
- Manuel L1/L2 işinin %80'ine kadarı üstlenilir
- Gerçek olaylarda 10 kat daha hızlı analist aksiyonu
- Sade dille bulgular ve giderme adımları
- Yapay zekâ asistanı sonuçları L1 ve L2 analistleri için yorumlar
- Düz bir uyarı listesi değil, gezilebilir tam olay zinciri

SÜRÜLEN MODÜLLER

- Malware Analyzer 360 – sandbox, statik analiz, URL ve CDR
- Mail Gateway – kimlik avı, BEC, fidye yazılımı ve e-posta APT'leri
- Threat Hunter – uç nokta ajanı, YARA taramaları ve air-gap modları
- Cloud Hunter – konteyner, bucket ve bulut dosya sistemi
- Her biri tek başına konumlandırılabilir, diğerleriyle daha keskin

ENTEGRASYONLAR

- Sekiz kategoride 43 entegrasyon – 16'sı dahili
- 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, FortiSOAR, Tines, Swimlane, Torq
- EDR/EPP: CrowdStrike Falcon ve Microsoft Defender
- Tehdit istihbaratı: MISP, OpenCTI, ThreatQ, Anomali ThreatStream
- Bulut depolama: SharePoint, OneDrive, Drive, Box, Dropbox, S3, Azure Blob, Nextcloud
- Ağ: ICAP proxy, TAP arabirimi, Broadcom CAS, OPSWAT MetaDefender
- E-posta: IMAP ve Postfix e-posta akışı
- Geri kalan her şey için syslog akışı

KONUMLANDIRMA & ÖLÇEK

- Yerinde (on-premise), bulut veya hibrit konumlandırma
- Kiosk ve köprü modlarıyla air-gap konumlandırma
- Tek düğümden ulusal ölçekli ortamlara kadar ölçeklenir
- Yoğun tehdit trafiği altında yüksek performanslı mimari
- Tek tıkla sorunsuz ürün güncellemesi

YÖNETİM

- Rol tabanlı kullanıcı yönetimi
- Analiz sonuçlarını kimin okuyabileceğine dair rol kısıtlaması
- Merkezî politika, karantina ve raporlama
- Verilerinizi yedekleyin ve geri yükleyin
- Her motor için sağlık izleme
- Gerçek zamanlı disk kapasitesi izleme
- PDF, CSV, JSON ve HTML rapor üretimi
- Kararların ve yönetici işlemlerinin tam denetim izi

CyberFortress

Tek çekirdek. Her katman onu besler.

MA 360°, dört güvenlik modülünün üzerinde çalıştığı motordur. Tek bir modülle ya da hepsiyle başlayın – bir ürün yığınıyla bir güvenlik sistemi arasındaki farkı yaratan şey çekirdektir.

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