CyberFortress

ÜRÜN TEKNİK DOKÜMANI

Mail Gateway

E-Mailleriniz için APT ve Zero Day koruması

E-posta hâlâ bir kuruma girmenin en güvenilir yolu – ve oradan gelen saldırılar artık saldırıya benzemiyor. Mail Gateway mail trafiği baştan sona analiz eder; böylece tehditler sistemlerinize ulaşmadan önce çözülür.

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

PLATFORM

Tek başına duran bir ağ geçidi değil

Mail Gateway, diğer her modülle aynı çekirdeği paylaşır. E-posta akışında yakalanan zararlı bir ek, anında Threat Hunter'ın, Cloud Hunter'ın ve SIEM'inizin üzerine aksiyon aldığı bir göstergeye dönüşür – o ekin kopyasını çoktan almış olan uç nokta da aynı hareketle bulunur. Merkezî politika, karantina ve raporlama MA 360° içinde yaşar; davranışsal değerlendirme CyberFortress AI'dan gelir. Tek konsol, tek karar, tek denetim izi.

MA 360° — platform çekirdeği

Her güvenlik katmanından telemetri toplar, gerçek zamanlı olarak ilişkilendirir ve müdahaleyi orkestre eder. Mail Gateway ürettiği her kararı ona teslim eder ve diğer tüm modüllerin yazdığı ortak istihbaratı geri okur.

DÖRT GÜVENLİK MODÜLÜ

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.

Malware Analyzer 360

Dinamik sandbox'ta kontrollü çalıştırma, statik kod incelemesi, canlı URL kararları ve İçerik Zararsızlaştırma & Yeniden Oluşturma – e-posta akışındaki her ek ve bağlantının teslim edildiği motor.

Threat Hunter

Merkezî analizle desteklenen hafif bir uç nokta ajanı. Silahlandırılmış bir ek bulunduğunda, kopyasını çoktan almış olan uç noktalar aynı hareketle belirlenir.

Cloud Hunter

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

CyberFortress TI ile Veri Katmanı

Göndericiler, alan adları ve bağlantılar platformun geri kalanının kullandığı aynı canlı istihbarata karşı denetlenir – günde terabaytlar, gerçek zamanlı ilişkilendirilir.

CyberFortress AI

Kimliğe bürünmeyi, BEC'i ve hedefli kimlik avını içerikten çok davranıştan tespit eder; kurumunuzda normal yazışmanın neye benzediğini öğrenir.

NEDEN MAIL GATEWAY

Saldırganların hâlâ çaldığı kapı

E-posta güvenliğinin çoğu yanlış bir varsayımla başlar: içinde bilinen zararlı bir şey bulunmadıkça mesaj temizdir. Sıfır güven bunu tersine çevirir. Hiçbir mesaj meşru görünmesi sayesinde teslim edilmez – her gönderici, her ek ve her bağlantı bunu hak etmek zorundadır.

Bu ayrım önemlidir, çünkü başarıya ulaşan saldırılar tam da meşru görünmek üzere kurgulanmış olanlardır. Bir İş E-postası Ele Geçirme mesajında ek de bağlantı da yoktur. Hedefli bir kimlik avı kampanyası tek bir şirket, bazen tek bir kişi için yazılır ve başka hiçbir yerde görülmemiştir. Silahlandırılmış bir doküman, makro çalışana kadar gerçek bir dokümandır.

Mail Gateway, çevre güvenliğinde bir kez değil sürekli doğrulama yapar. Ekler sandbox'ta kontrollü olarak çalıştırılır, bağlantılar tıklandığı anda yeniden değerlendirilir ve gönderici davranışı kurumunuzdaki normal yazışmanın gerçekte neye benzediğine karşı tartılır. Onu, geldikleri gün hiçbir imza taşımayan sıfır gün saldırılarına karşı etkili kılan da budur.

DÖRT SALDIRI, TEK KANAL

Kimlik avı
İnandırıcı marka görünümü ve kısaltılmış bağlantıların ardındaki kimlik bilgisi toplama sayfaları.

İş E-postası Ele Geçirme
Ek yok, bağlantı yok – yalnızca inandırıcı bir ödeme ya da parola talebi.

Fidye yazılımı
Teslimden önce kontrollü çalıştırılan silahlandırılmış dokümanlar ve indiriciler.

Hedefli kimlik avı & APT
Tek bir şirket için kurgulanan, imzayla değil davranışla yakalanan kampanyalar.

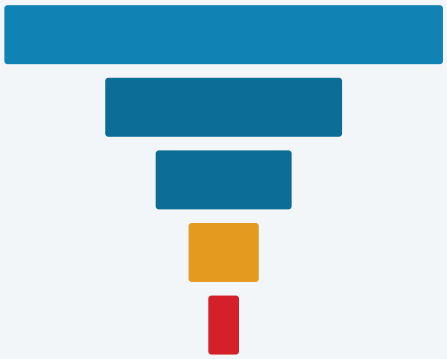
%99,9
Sahte mesajlarda yapay zekâ destekli tespit doğruluğu

Sıfır
Öntanımlı güvenilen mesaj sayısı – her biri doğrulanır

Tıklamada
Bağlantılar yalnızca teslimde değil, tıklamada da doğrulanır

%99,99
Hedeflenen erişilebilirlik; e-posta akışı hiç darboğaz olmaz

Her katmandan geriye ne kalıyor



Gelen mesajlar
trafiğin %100'ü

İtibar ve politika denetimini geçen
~%54

Spam ve toplu filtrelemeyi geçen
~%31

Analize giden ek ve bağlantı
~%9

Engellenen veya CDR ile yenilenen
~%1,4

Kurumsal bir e-posta akışının gösterge niteliğindeki dağılımı. Toplu filtreleme, hedefli saldırıların arasına karışmak için kullandığı gürültüyü temizler; yalnızca geriye kalan, kontrollü çalıştırma maliyetine değer.

AĞ GEÇİDİNİN İÇİNDE

Altı katman, tek e-posta akışı

Dört saldırı türü tek bir teslim kanalını paylaşır – ve aynı motorun farklı katmanları tarafından karşılanır. Her katman öğrendiğini çekirdeğe geri yazar.

Yapay zekâ destekli kimlik avı önleme

Gönderici itibarı, başlık anomalileri, dil örüntüleri, marka taklidi ve görsel benzerlik tek tek denetlenmek yerine birlikte tartılır. Model, kurumunuzda normal yazışmanın neye benzediğine dair bir resim kurar; böylece iyi kurgulanmış bir taklit, hiçbir sabit kuralı ihlal etmese bile sırıtır. **%99,9 tespit doğruluğu.**

Eklerin sandbox analizi

Her ek Malware Analyzer 360'a teslim edilir ve izolasyonda çalıştırılır; böylece bilinen aileler de sıfır gün örnekleri de davranışa göre değerlendirilir. İş akışının karar bekleyemeyeceği yerlerde İçerik Zararsızlaştırma & Yeniden Oluşturma, dokümanın açılması güvenli, yenilenmiş bir sürümünü anında teslim eder.

URL yeniden yazma

Teslim edilen e-postadaki bağlantılar, hedefin yalnızca e-postanın geldiği anda değil kullanıcının tıkladığı anda yeniden değerlendirilmesi için yeniden yazılır. Teslimde zararsız olup saatler sonra zararlı hâle gelen bir sayfa, etkileşim tamamlanmadan karantinaya alınır – ki bu, hedefli kimlik avının standart oyunudur.

Inline & BCC analizi

Inline mod e-postayı aktarım hâlindeyken inceler ve tehditleri yerinde engeller. BCC modu trafiğin bir kopyasını izler ve teslime hiç risk bindirmeden tam görünürlük sağlar. Mimari, hat üzeri taramanın genellikle getirdiği gecikmeyi doğurmadan tespit ve engelleme yapacak şekilde kurulmuştur.

Spam & toplu posta filtreleme

Yüksek hacimli istenmeyen e-posta kullanıcılara ulaşmadan ayrıştırılır; hem insanlar hem analistler için sinyal-gürültü oranı yüksek tutulur. Toplu trafiğin temizlenmesi, hedefli saldırıların kalabalık bir gelen kutusuna karışmak için kullandığı örtüyü de kaldırır.

Outlook eklentisi

Kullanıcılar doğrudan Microsoft Outlook içinden bir eki analize gönderebilir, bir bağlantının gerçek hedefini denetleyebilir ya da şüpheli bir mesaj için spam incelemesi başlatabilir. "Bu tuhaf görünüyor"u gerçek bir gönderime çevirmek tek tık sürer; böylece kullanıcılarınız rapor birikintisi olmak yerine çalışan bir tespit katmanına dönüşür.

İki konumlandırma yolu, tek motor

INLINE MOD – aktarımda inceler, yerinde engeller.

01 **Gelen**
E-posta, hiçbir kutuya düşmeden hat üzerinde ağ geçidine varır.

02 **Analiz**
Gönderici, gövde, bağlantılar ve ekler birlikte çözümlenir.

03 **Teslim**
Temiz teslim, CDR ile yenilenmiş teslim ya da karantina.

BCC MOD – teslime sıfır risk bindirerek tam görünürlük.

01 **Gelen**
E-posta bugün olduğu gibi teslim edilmeye devam eder.

02 **Kopya**
Bir BCC kopyası analiz motoruna akıtılır.

03 **Rapor**
Yalnızca bulgular – e-posta akışına hiç dokunulmaz.

Ortamların çoğu mevcut ağ geçidinin yanında BCC modunda başlar, bulgular anlaşıldıktan sonra hat üzerine geçer. İki mod da aynı analizi yürütür ve aynı konsola raporlar.

PRATİKTE SIFIR GÜVEN

Önemli olduğu anda yeniden doğrulanır

Teslim anındaki taramanın işe yaramamasının nedeni gecikmeli silahlandırmadır. Saldırgan gerçekten zararsız bir sayfanın bağlantısını gönderir, ağ geçidini geçmesini bekler ve içeriği saatler sonra — tüm denetimler çoktan geçtikten sonra – değiştirir.

Gecikmeli silahlandırma kampanyası, saat saat

Teslim anındaki tarama yalnızca ilk saati görür. Geri kalan pencereyi kapatan şey, tıklama anındaki yeniden değerlendirmedir.

Bir mesajın hak etmesi gerekenler

Gönderici

İtibar, başlık anomalileri, kimlik doğrulama kayıtları ve davranış geçmişi birlikte tartılır – kimliğe bürünme ve olağan dışı gönderici örüntüleri, içerik okunmadan önce işaretlenir.

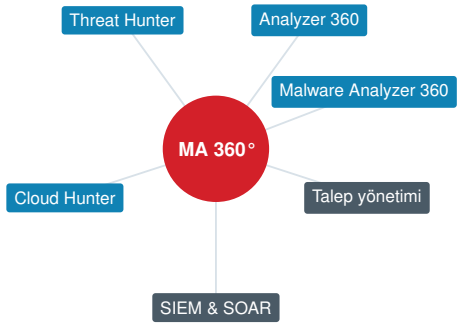
Ek

İzole bir sandbox'ta kontrollü çalıştırılır ve kod düzeyinde okunur. Teslimin bekleyemeyeceği yerde CDR aktif içeriği söküp dokümanı temiz olarak yeniden oluşturur.

Bağlantı

Teslimde tüm yönlendirme zinciri boyunca çözülür, sonra tıklama anında yeniden çözülür – hedef, gerçekte nereye gittiğine göre değerlendirilir.

Karara ne oluyor



Mesaj kararı	teslim, yenile ya da tut
Çıkarılan IoC'ler	gönderici, alan adı, hash
Ortam taraması	başka kim aldı
Denetim izi	tek kayıt, tek konsol

PRATİKTE

Ekipler nerede kullanıyor

Ağ geçidi genellikle ilk devreye alınan modüldür; çünkü ürettiği kanıt anında görülür ve konumlandırma e-posta akışına hiçbir risk bindirmez.

Bugün nelerin geçtiğini ölçmek

Mevcut ağ geçidinin yanında 30 gün BCC modu, mevcut filtrenin tam olarak neyi kaçırdığının raporunu üretir – örnekler, göndericiler ve kararlar ekli hâlde.

Yalnızca teslim anındaki taramayı değiştirmek

Tıklama anında URL yeniden değerlendirmesi, gecikmeli silahlandırmanın dayandığı pencereyi kapatır; eski ağ geçitlerinin çoğunun hâlâ açık bıraktığı boşluk tam da budur.

Kullanıcı bildirimlerini karara çevirmek

Phish Control bildirilen mesajı oradan devralır: ek kontrollü çalıştırılır, bağlantılar çözülür ve spam incelemesi başlatılır – hiçbir analist dokunmadan.

Yönetici ve finans koruması

Davranışsal analiz, içerik taramasının göremediği kimliğe bürünme ve olağan dışı gönderici örüntülerini işaretler – yani taranacak hiçbir şeyin olmadığı BEC senaryosunu.

Düzenlemeye tabi yazışmalar

Her kararın, her serbest bırakmanın ve her yönetici işleminin tam denetim izi; neyin neden teslim edildiğini soran bir düzenleyiciyi tatmin edecek biçimde saklanır.

Ortam genelinde kontrol altına alma

Bir ek teslimden sonra zararlı olarak değerlendirildiğinde, kopyasını çoktan almış olan uç noktalar aynı hareketle belirlenir ve taranır.

Saldırı türüne göre tespit doğruluğu

Bir iç korpustaki gösterge niteliğinde değerler. BEC'te taranacak bir yük bulunmaz; sonucu içerik eşleştirmesi değil davranışsal analizin sürüklemesinin nedeni budur.

Mevcut filtrenizin neyi kaçırdığını görün.

Mevcut ağ geçidinizin yanında 30 gün BCC modunda konumlandırın. E-posta akışında değişiklik yok, teslimde risk yok – yalnızca nelerin geçtiğinin raporu.

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

TEKNİK ÖZELLİKLER

Özellikler ve yetenekler

TEHDİT KAPSAMASI

- Kimlik avı ve kimlik bilgisi toplama kampanyaları
- İş E-postası Ele Geçirme (BEC) ve ödeme dolandırıcılığı
- Fidye yazılımı indiricileri ve silahlandırılmış dokümanlar
- Hedefli kimlik avı ve amaca yönelik APT kampanyaları
- E-posta kaynaklı sıfır gün ve daha önce görülmemiş örnekler
- Marka ve üst yönetim kimliğine bürünme
- Görünen ad ve benzer alan adı sahteciliği
- Zararlı QR kodları ve görsele gömülü yükler
- Yazışma dizisini ele geçirme ve yanıt zinciri istismarı

YAPAY ZEKÂ İLE KİMLİK AVI ÖNLEME

- Sahte mesajlarda %99,9 tespit doğruluğu
- Gönderici itibarı ve davranış geçmişi puanlaması
- Başlık anomalisi ve kimlik doğrulama kaydı analizi
- Dil ve üslup örüntüsü analizi
- Marka taklidi ve görsel benzerlik tespiti
- Kurumunuzun normal yazışma örüntüsünü öğrenir
- Hedefli dolandırıcılık ve kimlik sahteciliğinde proaktif tespit
- Dakikalar değil, milisaniyeler içinde sınıflandırma

EK DOSYA ANALİZİ

- Malware Analyzer 360 sandbox'ında gerçek zamanlı kontrollü çalıştırma
- Dinamik davranışın yanında statik kod incelemesi
- İç içe ve parola korumalı arşivler dâhil tüm dosya türleri
- Office dokümanları, PDF'ler, betikler, kurulum dosyaları ve çalıştırılabilirler
- İçerik Zararsızlaştırma & Yeniden Oluşturma temiz, kullanılabilir dosya üretir
- Makrolar, gömülü betikler ve bozuk yapılar sökülür
- İş akışının bekleyemeyeceği yerde temiz kopya anında teslim edilir
- Kararlar çıkarılan IoC'ler ve MITRE ATT&CK eşlemesiyle gelir

URL KORUMASI

- Tıklama anında yeniden değerlendirme için yeniden yazılan bağlantılar
- Gerçek hedefe kadar çözülen tüm yönlendirme zinciri
- Kısaltıcılar ve yönlendiriciler vardıkları yere göre değerlendirilir
- Teslimden sonra ortaya çıkan gecikmeli silahlandırma yakalanır
- Kimlik avı sayfaları, C2 noktaları ve drive-by zincirleri belirlenir
- Etkileşim, sayfa yüklenmeden önce karantinaya alınır
- Canlı URL kararları platformun geri kalanıyla paylaşılır

SPAM & TOPLU POSTA FİLTRELEME

- Yüksek hacimli istenmeyen e-posta kullanıcılara ulaşmadan ayrılır
- Bülten ve toplu trafik spam'den ayrı sınıflandırılır
- Kullanıcı ve alan adı bazında izin ve engelleme politikası
- Outlook içinden kullanıcı tarafından başlatılan spam incelemesi
- Hedefli saldırıların karıştığı örtüyü temizler

KONUMLANDIRMA & E-POSTA AKIŞI

- Inline mod – aktarımda inceler, yerinde engeller
- BCC modu – teslime sıfır risk bindirerek kopyayı izler
- Hat üzeri tarama gecikmesi olmadan engelleyecek biçimde kurulmuş
- %99,99 hedeflenen erişilebilirlik
- Yerinde (on-premise), bulut veya hibrit konumlandırma
- SMTP, IMAP ve Postfix e-posta akışı entegrasyonu
- Değerlendirme sürecinde mevcut ağ geçidinin yanında çalışır
- Microsoft 365, Google Workspace veya yerinde e-postanın önünde durur

KULLANICI ARAÇLARI

- Özel Microsoft Outlook eklentisi
- Tek tıkla eki analize gönderme
- Açmadan önce bağlantının gerçek hedefini denetleme
- Şüpheli mesaj için spam incelemesi başlatma
- Bildirim yapan kullanıcılar çalışan bir tespit katmanına dönüşür
- Mesajın neden tutulduğuna dair sade dille açıklama

POLİTİKA & KARANTİNA

- Merkezî politika, karantina ve raporlama MA 360° içinde
- Kullanıcı, grup ve alan adı bazında kural setleri
- Tutulan mesajları serbest bırakma, silme veya yeniden analiz etme
- Teslim edilmiş mesajların geriye dönük kaldırılması
- Karantinaya ve analiz sonuçlarına rol tabanlı erişim
- Her kararın ve her yönetici işleminin tam denetim izi

RAPORLAMA & BİLDİRİMLER

- Syslog sunucunuza akıtılan özelleştirilebilir kayıtlar
- Analiz sonuçları istenen her biçimde e-postayla iletilir
- Dinamik, anlaşılır raporlar üçüncü taraflara dağıtılır
- PDF, CSV, JSON ve HTML rapor üretimi
- Her motorun durumunu gösteren sağlık izleme
- Gerçek zamanlı disk kapasitesi izleme

ENTEGRASYONLAR

- İki yönlü veri ve aksiyon akışlı RESTful API
- SIEM: Splunk, Sentinel, QRadar, Elastic, LogRhythm, ArcSight
- SOAR: Cortex XSOAR, Splunk SOAR, FortiSOAR, Tines, Swimlane, Torq
- EDR/EPP: CrowdStrike Falcon ve Microsoft Defender
- Tehdit istihbaratı: MISP, OpenCTI, ThreatQ, Anomali ThreatStream
- Talep yönetim sistemleri olayları otomatik açar, günceller ve kapatır
- Geri kalan her şey için syslog akışı

CyberFortress

Hiçbir mesaj öntanımlı olarak güvenilir değildir.

Mail Gateway, 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