CyberFortress

ÜRÜN TEKNİK DOKÜMANI

Threat Hunter

Kapsamlı zararlı analizi, lightweight ajan

Uç nokta, kullanıcıların işini gerçekten yaptığı – ve sızmaların çoğunun gerçeğe dönüştüğü – yerdir. Threat Hunter kurumsal cihazları, onları analiz iş istasyonuna çevirmeden korur: ajan lightweight kalır, bütün iş platform çekirdeğinde yapılır.

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

PLATFORM

Ajan küçük, çünkü çekirdek değil

Cihazda toplanan olaylar, gerçek zamanlı tespiti yürüten MA 360° tarafından merkezî olarak işlenir. Bu ayrım tasarımın tamamıdır: uç nokta performansını ve yönetilebilirliğini korur; gelişmiş tehdit analizi – sandbox'ta kontrollü çalıştırma, statik inceleme, davranışsal sınıflandırma – ait olduğu yerde, platform çekirdeğinde gerçekleşir.

MA 360° — platform çekirdeği

Her güvenlik katmanından telemetri toplar, gerçek zamanlı olarak ilişkilendirir ve müdahaleyi orkestre eder. Uç nokta tespitleri; önem derecesine göre sıralanmış, tehdit istihbaratıyla zenginleştirilmiş ve e-posta akışı ile bulut ortamının gördükleriyle ilişkilendirilmiş hâlde gelir.

DÖRT GÜVENLİK MODÜLÜ

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.

Malware Analyzer 360

Dinamik sandbox'ta kontrollü çalıştırma, statik kod incelemesi, canlı URL kararları ve CDR – ajanın topladığı her şüpheli artefaktın, itibar sorgusu değil gerçek bir karar için gönderildiği yer.

Mail Gateway

Kimlik avı, BEC, fidye yazılımı ve e-posta kaynaklı APT'lere karşı çok katmanlı savunma. E-posta akışında yakalanan silahlandırılmış bir ek, aynı hareketle tüm uç nokta ortamında taranır.

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

Cihaz telemetrisi içeri akar; taze IoC'ler ve YARA kuralları geri döner. Ortam, kurulum anında donmuş bir kural setine değil yeni istihbarata karşı denetlenir.

CyberFortress AI

Uç nokta tespitlerini önem derecesine göre sıralar ve düz bir uyarı listesinin gömeceği sessiz, uzun süreli etkinliği öne çıkarır.

NEDEN THREAT HUNTER

Tespit bekler. Avcılık aramaya gider.

Tespit, bir şeyin kurala takılmasını bekler. Avcılık ise bir hipotezle başlar – haberlerdeki yeni bir kampanya, tuhaf bir kimlik doğrulama örüntüsü, bir ISAC'tan gelen ihbar – ve bunun içeride olup olmadığını denetlemeye gider.

İkisinin de uç noktadan aynı şeye ihtiyacı vardır: gerçekten sorgulayabileceğiniz bir ortam. Threat Hunter, bağlı her cihazı kendi kurallarınızla tarayabileceğiniz, artefakt toplayabileceğiniz ve bulduğunuzu platformun geri kalanını çalıştıran aynı motorda kontrollü biçimde çalıştırabileceğiniz bir şeye dönüştürür.

Ajanın kendisi bilinçli olarak küçük kalır. Zararlı yazılımın gerçekten kullandığı yolları – USB cihazları, dosya paylaşımları, indirmeler, Outlook ve tarayıcı – izler, bir sızmayı erken durduran denetimleri uygular ve geri kalan her şeyi çekirdeğe devreder. Kurcalamaya karşı koruma, saldırgan onu kapatmaya çalıştığında çalışmayı sürdürmesini sağlar; ki bu, bir sızmanın yaptığı ilk işlerden biridir.

İŞ NEREDE YAPILIYOR

Uç noktada
Toplama, uygulama, USB ve paylaşım denetimi, filigran, kurcalamaya karşı koruma.

MA 360° içinde
Gerçek zamanlı tespit, sandbox'ta çalıştırma, korelasyon ve önem derecesi sıralaması.

Tek konsolda
Tüm ortam için politika, tarama sonuçları ve raporlama.

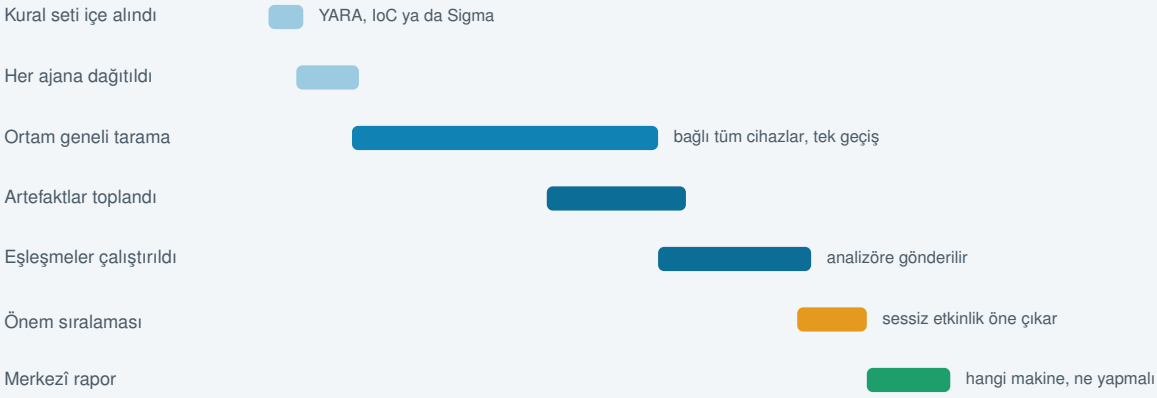
Merkezî
Tespit uç noktada değil, MA 360° içinde çalışır

YARA
Bağlı her cihazda taranan özel kural setleri

Air-gap
İzole ağlar için kiosk ve köprü modları

Sürekli
Kurcalamaya karşı koruma ajanın kapatılmasını engeller

İhlal değerlendirmesi: tek tarama, tek yanıt



Taze bir kampanya raporuyla tetiklenen ortam genelinde YARA taramasının gösterge niteliğindeki akışı. Ajan toplar; çekirdek analiz eder; yanıt bir eşleşme yığını değil sıralanmış bir liste olarak gelir.

UÇ NOKTADA

Koruma, görünürlük ve denetim

Altı yetenek cihaz üzerinde çalışır – her makineye tam bir analiz motorunun ağırlığını bindirmeden.

Gerçek kanallarda APT denetimi

USB cihazları, dosya paylaşımları ve indirmeler zararlı yazılımın gerçek yollarıdır. Bu yollarla gelen dosyalar çalışmadan önce MA 360°'ın gerçek zamanlı analizine karşı denetlenir.

Otomatik triyaj

Tespitler cihazın kendi üzerinde önem derecesine göre sıralanır; böylece güvenlik ekibi kritik vakaları önce görür ve sessiz, uzun süreli zararlı etkinlik gömülmek yerine yine de öne çıkar.

Ekran filigranı

Oturuma özgü dinamik filigran, fotoğraf veya ekran görüntüsüyle veri sızdırmayı caydırır ve içeriden gelen etkinliği kullanıcı ile oturum düzeyinde izlenebilir kılar – aksi hâlde kayıt bırakmayan tek sızma yolu.

Kurcalamaya karşı koruma

Saldırganlar bir sızmanın erken aşamasında güvenlik yazılımını devre dışı bırakır. Kurcalamaya karşı koruma, ajanı durdurma veya kaldırma girişimlerini engelleyerek kapsamayı kesintisiz etkin tutar.

Outlook & tarayıcı entegrasyonu

Ek inceleme, kullanıcıların gününü geçirdiği iki uygulamanın içine iner; zararlı ekler ve bağlantılar iş olup bittikten sonra değil etkileşim noktasında yakalanır.

YARA kural taramaları

Kendi YARA kural setlerinizi bağlı her uç noktada çalıştırın ve merkezî raporlanan ayrıntılı bulgular alın – etkin bir kampanya sırasında "biz etkilendik mi?" sorusunu yanıtlamanın en hızlı yolu.

Diğer tüm denetimlerin açık bıraktığı sızma yolu

Veri nasıl çıkıyor	Kayıt bırakır	Atfedilebilir	Kapsayan
Kopyala ve yapıştır	✓ evet	✓ evet	DLP
E-posta ve ekler	✓ evet	✓ evet	Mail Gateway
USB ve çıkarılabilir medya	✓ evet	✓ evet	Threat Hunter
Yüklemeler ve dosya paylaşımı	✓ evet	✓ evet	Proxy ve analizör
Ekrana tutulan bir kamera	○ hayır	✓ evet	**Ekran Filigranı**
Ekranın görüntüsünün alınması	○ hayır	✓ evet	**Ekran Filigranı**
Zoom/Teams'ten ekran görüntüsü	○ hayır	✓ evet	**Ekran Filigranı**

Kopyalama, e-posta, USB ve yüklemelerin hepsi bir incelemenin üzerinde çalışabileceği kayıt üretir. Ekranın fotoğrafı ise ne süreç, ne dosya, ne de ağ olayı üretir. Bu yolda işleyen denetim filigrandır; çünkü hem gözün hem merceğin gördüğü şey üzerinde çalışır.

Filigran gerçekte ne yapıyor

Oturumu tanımlar

Her oturum kendine özgü bir kod üretir; böylece herhangi bir görüntü kaydı, o andaki makinenin ve oturum açmış kişinin kimliğini taşır.

Kameradan geçer

İşaret, ekranın gösterdiği görüntünün içine çizildiği için telefonla çekilen fotoğrafta da ekran görüntüsünde olduğu gibi bulunur.

Davranışı değiştirir

Değerin çoğu önleyicidir. Kendi kimliğini ekranda gören biri, bir fotoğrafın kendisini işaret ettiğini anlar.

İZOLE AĞLAR

Air-gap ortamların içinde koruma

İzole ağlar çözülmüş bir sorun değil – daha zor bir sorundur. Dosyaların yine de sınırı geçmesi gerekir ve geçtiklerinde genellikle onları izleyen hiçbir şey yoktur. Uç nokta ajanı bu sınırda kiosk veya köprü modunda konumlandırılabilir; böylece dış dünyaya hiç yolu olmayan sistemlerde bile güvenli dosya akışı ve gerçek tehdit analizi mümkün olur.

Kiosk modu

Personelin, çıkarılabilir medyayı güvenli bölgeye girmeden önce taradığı özel bir istasyon. Karar verilmeden hiçbir şey sınırı geçmez.

Köprü modu

İzole ve bağlı segmentler arasında hareket eden dosyaları, her iki yönde de analiz eden denetimli bir aktarım noktası.

Çıkarılabilir medya

USB bellekler öntanımlı olarak güvenilmez kabul edilir ve her takılışta incelenir – uç nokta güvenliğindeki en eski boşluk kapanır.

Tam denetim izi

Her aktarım ve her karar, uyumluluk ve sonraki incelemeler için kaydedilir; bu ortamlarda genellikle bir incelik değil bir zorunluluktur.

Köprü modunda sınırı geçen bir dosya

01 Takma
Medya, kiosk ya da köprü istasyonuna takılır.

02 Envanter
İçerik listelenir ve hash'lenir, arşivler açılır.

03 Analiz
Dosyalar statik ve dinamik analiz için MA 360°a gider.

04 Karar
Temiz, CDR ile yenilenmiş ya da sınırda engellenmiş.

05 Aktarım
Onaylanan içerik güvenli bölgeye bırakılır.

06 Kayıt
Her aktarım ve karar denetim izine yazılır.

Bağlı ortamı koruyan analiz motorunun aynısı air-gap sınırında çalışır. Fiziksel medyayla geldiği için hiçbir şeye güvenilmez.

İzole konumlandırmalar nerede kullanılıyor

OT ve endüstri

Bakım dizüstü bilgisayarının ya da tedarikçi USB belleğinin tek giriş yolu olduğu – ve tarihsel olarak zararlı yazılım için de tek giriş yolu olan — üretim ağları.

Savunma ve kamu

Dış dünyaya erişemeyen ama yine de oradan doküman ve güncelleme kabul etmek zorunda olan gizlilik dereceli segmentler.

Düzenlemeye tabi araştırma

Açığa çıkması hukuki sonuç doğuran veriyi tutan ve her sınır geçişinin belgelenmesi gereken ortamlar.

PRATİKTE

Ekipler nerede kullanıyor

Ajan konumlandırıldıktan sonra uç nokta ekiplerinin en sık başvurduğu senaryolar – ve bir avın gerçekte döndüğü çevrim.

Phish Control

Bir kullanıcı şüpheli mesaj bildirdiğinde Phish Control devreyi oradan devralır: ek kontrollü çalıştırılır, bağlantılar çözülür ve spam incelemesi başlatılır – hiçbir analist dokunmadan. Eskiden kuyrukta bekleyen bildirimler karara dönüşür.

USB ve çıkarılabilir medya denetimi

Kurumsal bir makineye takılan her cihaz güvenilmez kabul edilir ve içeriği çalışamadan önce incelenir.

İhlal değerlendirmesi

Taze bir tehdit raporundan aldığınız YARA kural setini tüm ortama dağıtın ve hangi makinelerin eşleştiğine dair merkezî raporlanan yanıtı tek taramada alın.

İçeriden gelen risk ve veri kaybı

Ekran filigranı ve uç nokta telemetrisi birlikte, verinin ağ üzerinden değil bir kullanıcı üzerinden çıkışını görmeyi, atfetmeyi ve belgelemeyi mümkün kılar.

APT avı

Uç noktada toplanan şüpheli artefaktlar Malware Analyzer 360'a geri gönderilir; sessiz bir anomali, MITRE ATT&CK'e eşlenmiş adı konmuş bir sızmaya dönüşür.

İzole ve düzenlemeye tabi ortamlar

Kiosk ve köprü konumlandırmaları, gerçek zararlı yazılım analizini normalde körlemesine çalışan OT, savunma ve diğer air-gap ortamlara taşır.

Bir av nasıl yürür

01 — Hipotez
Bir kampanya raporundan, taze bir IoC setinden ya da yapay zekânın işaretlediği bir anomaliden başlayın.

02 — Tara
YARA kurallarını ve IoC denetimlerini tek geçişte her uç noktada çalıştırın.

03 — Analiz
Toplanan artefaktlar kontrollü çalıştırılır ve kod düzeyinde okunur.

04 — Operasyona al
Yeni göstergeler SIEM, EDR ve güvenlik duvarına dağıtılır.

Tek seferlik bir iş değil, bir çevrim: sonunda öğrendiğiniz şey, bir sonrakinin başındaki tespit içeriğine dönüşür.

Ajanı tek bir departmanda deneyin.

Tek bir ekibe yayın, makinelerinde bir YARA taraması çalıştırın ve merkezî bir analiz motorunun yerel bir tarayıcının bulamadığı neyi bulduğunu görün.

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

TEKNİK ÖZELLİKLER

Özellikler ve yetenekler

UÇ NOKTA KORUMASI & DENETİMİ

- Her takılışta USB ve çıkarılabilir medya denetimi
- Dosya paylaşımı erişim denetimi ve incelemesi
- Tarayıcıda indirme denetimi
- Dosyalar çalışmadan önce gerçek zamanlı analize karşı denetlenir
- Uygulama ve süreç davranışı izleme
- Ekler ve bağlantılar için Outlook entegrasyonu
- Etkileşim noktasında tarayıcı entegrasyonu
- Ajanı durdurmaya veya kaldırmaya karşı kurcalama koruması
- Cihaz, grup ya da ortam bazında uygulanan politika

ANALİZ & TRİYAJ

- Tespit cihazda değil, merkezî olarak MA 360° içinde çalışır
- Her tespitin otomatik önem derecesi sıralaması
- Sessiz, uzun süreli etkinlik gömülmek yerine öne çıkarılır
- Şüpheli artefaktlar kontrollü çalıştırma için analizöre gönderilir
- İtibar sorgusu değil, statik ve dinamik analiz
- Bulgular otomatik olarak MITRE ATT&CK'e eşlenir
- Analiz edilen her artefakttan IoC çıkarımı
- CyberFortress AI'dan davranışsal anomali tespiti

TEHDİT AVCILIĞI

- Bağlı her uç noktada YARA kural taramaları
- Kendi kurallarınız, bir üreticinin kuralları ya da bu sabah yazılanlar
- IoC ve artefakt arama – hash'ler, alan adları, kayıt defteri anahtarları, mutex'ler, bırakılan dosya yolları
- Geçmiş ve güncel uç nokta etkinliği birlikte aranır
- Tüm ortamda merkezî raporlanan eşleşmeler
- Sıralanmış sonuçlar; yüzlerce eşleşmeli bir tarama da bir yere varır
- Avcılık, kiosk ve köprü modlarıyla izole segmentlere uzanır
- Yeni göstergeler SIEM, EDR ve güvenlik duvarına dağıtılır

İÇERİDEN RİSK & VERİ KORUMASI

- Tüm ekrana döşenen dinamik ekran filigranı
- Her kullanıcı ve her oturum için benzersiz tanımlayıcı
- Ekran görüntüsünde olduğu gibi telefon fotoğrafında da görünür
- İnsanlar normal çalışabilsin diye düşük kontrastla basılır
- Kullanıcı tarafından devre dışı bırakılamaz
- Tek bir uygulamayı değil, tüm masaüstünü kapsar
- Sızdırılan görüntünün makineye ve oturuma atfedilmesi
- Uzak, hibrit ve yüklenici oturumlarında çalışır

AİR-GAP & İZOLE AĞLAR

- Kiosk modu – güvenli sınırda bir tarama istasyonu
- Köprü modu – segmentler arası denetimli aktarım noktası
- Çıkarılabilir medya öntanımlı olarak güvenilmez
- Arşivler bırakılmadan önce açılır ve analiz edilir
- Politika gerektirdiğinde CDR dokümanları temiz olarak yeniden oluşturur
- Her aktarım ve kararın tam denetim izi
- OT, savunma ve düzenlemeye tabi ortamlarda gerçek analiz

AJAN & AYAK İZİ

- Hafif ajan, makinede en düşük yük
- Ağır analiz platform çekirdeğine devredilir
- Kullanıcı etkileşimi gerektirmeyen otomatik toplama
- Sessiz kurulum ve merkezî yükseltme
- Bağlantı kesikken de politikayı uygulamayı sürdürür
- Windows 7 ve üzeri

KONUMLANDIRMA & YÖNETİM

- Yerinde (on-premise), bulut veya hibrit konumlandırma
- Tek departmana ya da tüm ortama yayın
- Merkezî politika, tarama sonuçları ve raporlama tek konsolda
- Rol tabanlı kullanıcı yönetimi
- Analiz sonuçlarını kimin okuyabileceğine dair rol kısıtlaması
- Her motor için sağlık izleme
- Verilerinizi yedekleyin ve geri yükleyin
- Tek tıkla sorunsuz ürün güncellemesi

RAPORLAMA & BİLDİRİMLER

- Syslog sunucunuza akıtılan özelleştirilebilir kayıtlar
- Analiz sonuçları istenen her biçimde e-postayla iletilir
- PDF, CSV, JSON ve HTML rapor üretimi
- Adli inceleme ve uyumluluk için delil niteliğinde saklama
- Gönderimlerin ve yönetici işlemlerinin tam denetim izi

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
- Geri kalan her şey için syslog akışı

CyberFortress

Uyarı düşmeden önce aramaya çıkın.

Threat Hunter, 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