CyberFortress

ÜRÜN TEKNİK DOKÜMANI

Cloud Hunter

Bulut iş yükleri, bulut native analiz gerektirir

Genel amaçlı güvenlik denetimleri bulutun sınırında durur. Cloud Hunter bulutun içine girer – yayına aldığınız konteyner imajlarını, veriyi sakladığınız bucket'ları ve iş yüklerinizin paylaştığı dosya sistemlerini hibrit yöntem ile çok bulutlu ortamlar boyunca inceler.

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

PLATFORM

Tek olay, iki değil

Hibrit ya da çok bulutlu olsun, bulgular diğer her modülle aynı çekirdeğe düşer – böylece bir depolama bucket'ındaki zararlı dosya ile onu yükleyen uç nokta iki olay değil, tek bir olaydır. Konteyner çalışma zamanı davranışı CyberFortress AI tarafından bağlam içinde okunur, şüpheli nesneler Malware Analyzer 360 tarafından kontrollü olarak çalıştırılır ve her şey, platformun geri kalanının kullandığı aynı açık arabirimler üzerinden SIEM'inize ulaşır.

MA 360° — platform çekirdeği

Bulut bulgularını uç nokta ve e-posta etkinliğiyle ilişkilendirir, ortak tehdit istihbaratıyla zenginleştirir ve müdahaleyi orkestre eder — böylece bir konteyner anomalisi izole olarak değil, platformun gördüğü her şeye karşı okunur.

DÖRT GÜVENLİK MODÜLÜ

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.

Malware Analyzer 360

Dinamik sandbox'ta kontrollü çalıştırma, statik kod incelemesi ve CDR — bucket'larda ve paylaşımlarda bulunan şüpheli dosyaların yalnızca itibara göre değerlendirilmek yerine çalıştırıldığı yer.

Threat Hunter

Merkezî analizle desteklenen hafif bir uç nokta ajanı. Zararlı bir nesneyi yükleyen iş istasyonu, nesnenin kendisiyle aynı hareketle belirlenir.

Mail Gateway

Kimlik avı, BEC, fidye yazılımı ve e-posta kaynaklı APT'lere karşı çok katmanlı savunma; ürettiği her kararı platformun geri kalanıyla paylaşır.

CyberFortress TI ile Veri Katmanı

Konteyner ve bucket etkinliği içeri akar; canlı CVE verisi ve tehdit bağlamı geri döner – böylece geçen ay temiz olan bir imaj, bugün yayımlananlara karşı yeniden değerlendirilir.

CyberFortress AI

Konteyner çalışma zamanı davranışını bağlam içinde okur; sıradan sapmayı gerçek bir ihlalden ayıran da budur.

NEDEN CLOUD HUNTER

Saldırı yüzeyi tedarik zincirinin kendisi

Modern bir iş yükü yazılmaz, birleştirilir. Temel imajlar, paket depoları, derleme hatları ve üçüncü taraf katmanların hepsi üretimde çalıştırdığınız şeyin parçası olur – ve her biri, saldırganın ağınıza hiç dokunmadan size ulaşabileceği bir yerdir.

Konteyner taramasının çoğu tek bir platforma bağlıdır: tek bir bulutun imaj deposu, tek bir üreticinin kümesi. Bu da bir geliştirici dizüstü bilgisayarında derlenen, özel bir depoda saklanan ya da geçen yıl satın aldığınız ortamda çalışan imajları tamamen değerlendirilmemiş bırakır. Cloud Hunter konteynerleri bunların hepsinde değerlendirir ve bulguları tek yerde raporlar; böylece hibrit ve çok bulutlu ortamlar dört kısmi yanıt yerine tek bir yanıt alır.

Ve gerçekten yayına giden şeyi inceler. Zafiyetli bir bağımlılık, bir katmana gömülmüş bir sır ya da çalışma zamanında derleme anındakinden farklı davranan bir konteyner – hepsi platformun, olaya dönüşmeden önce öne çıkardığı bulgulardır.

KONTEYNER NEREDEYSE

Yerel & derleme anı
Bir imaj hiç gönderilmeden önce geliştirici makineleri ve CI koşucuları.

İmaj depoları
Genel ve özel depolar; gönderimde ve planlı olarak taranır.

Yerinde kümeler
Kendi veri merkezinizde çalışan Docker ve Kubernetes.

Her genel bulut
Yönetilen Kubernetes ve konteyner hizmetleri; hibrit ve çok bulutlu.

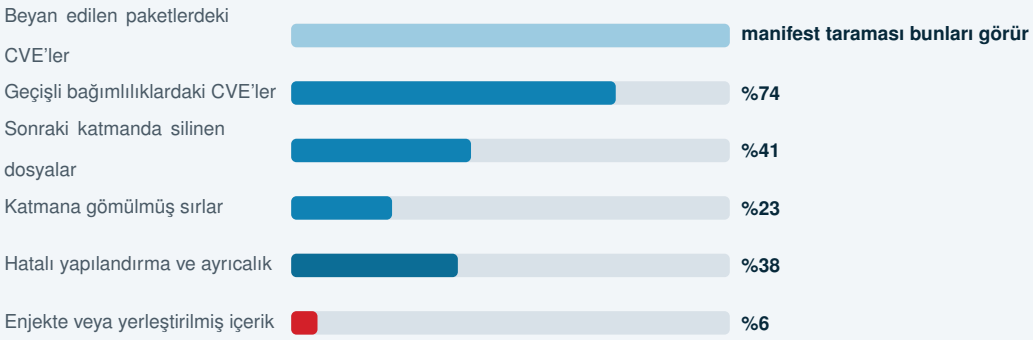
CVE
Konteyner zafiyetleri canlı CVE verisine karşı taranır

Çoklu
Tek konsoldan hibrit ve çok bulutlu kapsama

Anlık
Bulut kaynak etkinliğinin sürekli izlenmesi

K8s
Docker ve Kubernetes imajları, yapılandırma ve davranış

Katman derinliğinde değerlendirme, manifest taramasının bulamadığını nasıl buluyor



Üretim imajlarından oluşan bir iç korpusta bulguların gösterge niteliğindeki dağılımı. Yalnızca manifest okuyan bir tarama beyan edilen bağımlılık listesini görür; altındaki her şey ancak imaj katman katman açıldığında görünür.

CLOUD HUNTER'IN İÇİNDE

Dört katmanlı bulut kapsaması

Her biri, geleneksel araçların incelenmemiş bırakmaya eğilimli olduğu bulut saldırı yüzeyinin bir parçasını ele alır.

Konteyner analizi

Docker ve Kubernetes genelinde imajlar, yapılandırmalar ve çalışma zamanı davranışı derinlemesine incelenir. Enjekte edilmiş zararlı kod, hatalı yapılandırmalar, zafiyetli bağımlılıklar ve tedarik zinciri riskleri otomatik tespit edilir; konteyner zafiyetleri CVE temelinde taranır ve kritik bulgular ortaya çıktığı anda raporlanır.

Bucket taraması

S3, Blob ve benzeri nesne depoları hatalı izinler, herkese açık hâle gelmiş bucket'lar, zararlı içerik ve şüpheli dosya etkinliği için sürekli taranır — hem veri sızma yolları hem zararlı yüklemeler erkenden engellenir.

Dosya sistemi koruması

Bulutun içindeki dosya hareketleri gerçek zamanlı analiz edilir. Zararlı içerik, betik tabanlı saldırılar, şüpheli çalıştırılabilirler ve anormal değişiklikler anında yakalanır – birden fazla iş yükünün okuduğu paylaşımlı depolama için kritik bir savunma.

Gerçek zamanlı izleme

Bulut kaynakları genelindeki etkinlik sürekli izlenir; operasyonel görünürlük yükselirken tehditler ölçülecek bir etki doğurmadan yakalanır.

Her imajda altı denetim

CVE zafiyet taraması

Her paket ve bağımlılık güncel CVE verisiyle eşleştirilir; kritik bulgular bir sonraki planlı incelemede değil, göründüğü anda öne çıkarılır.

Katman katman inceleme

Sonraki bir katmanda silinen şey imajda hâlâ durur ve yalnızca manifest okuyan bir tarama onu asla görmez.

Hatalı yapılandırma denetimi

Ayrıcalıklı bayraklar, açık portlar, yazılabilir dosya sistemleri, root kullanıcıları ve gevşek bağlamalar – izole bir iş yükünü dayanağa çeviren hatalar.

Zararlı içerik

Enjekte edilmiş kod, arka kapılar, kripto madencileri ve silahlandırılmış ikili dosyalar yalnızca itibara göre değerlendirilmek yerine sandbox'ta çalıştırılır.

Tedarik zinciri riski

Temel imajlar, çekilen paketler ve derleme anı bağımlılıkları ne olduklarıyla değerlendirilir: sizin ayrıcalıklarınızla çalışan, başkasına ait kod.

Çalışma zamanı sapması

Üretimde testtekinden farklı davranan bir konteyner anomali olarak işaretlenir; hiçbir ön konumlandırma taramasının öngöremeyeceği ihlal yakalanır.

YAŞAM DÖNGÜSÜ BOYUNCA

En ucuzu erken, en dürüstü geç

Değerlendirme hattın iki ucunda da çalışır. Geçit denetimi sorunu yayına gitmeden yakalar; imaj deposu taramaları ve çalışma zamanı izleme ise ancak yayına gittikten sonra soruna dönüşen şeyi yakalar.

Değerlendirme hattın neresinde çalışıyor

01 — Derleme
Bir imaj gönderilmeden önce geliştirici makineleri ve CI koşucuları.

02 — İmaj deposu
Genel ve özel depolar, gönderimde ve planlı olarak taranır.

03 — Geçit
Zafiyetli ya da kurcalanmış katman terfi etmez, hattı düşürür.

04 — Yayına alma
Küme yapılandırması ve kabul durumu değerlendirilir.

05 — Çalışma zamanı
Davranış yalnızca öncesinde değil, sonrasında da izlenir.

06 — Yeniden değerlendir
Saklanan imajlar yeni CVE'ler yayımlandıkça yeniden denetlenir.

Her aşamada aynı motor ve aynı bulgular – böylece üretimde bulunan bir zafiyet, onu getiren derlemeye kadar geriye izlenebilir.

CI/CD imaj geçidi

İmajlar terfiden önce değerlendirilir; böylece zafiyetli ya da kurcalanmış bir katman üretime ulaşmak yerine hattı düşürür.

İmaj deposu taramaları

Hâlihazırda saklanan her şey yeni CVE'ler yayımlandıkça yeniden değerlendirilir – geçen ay temiz olan bir imaj bugün temiz olmayabilir.

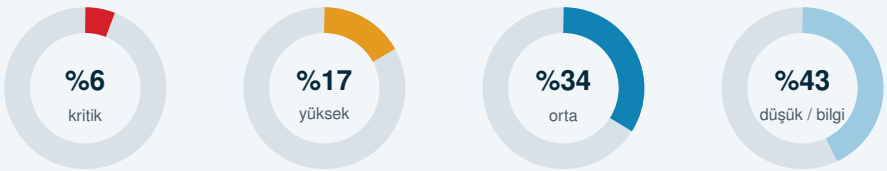
Denetim & uyumluluk

Bulgular, önem dereceleri ve giderme durumu; ne çalıştırdığınızı ve nesinin yanlış olduğunu soran bir denetçiyi tatmin edecek biçimde raporlanır.

Olay müdahalesi

Bir şey ters gittiğinde değerlendirme geçmişi, kusuru hangi imajların taşıdığını ve nerelere konumlandırıldığını gösterir.

İlk değerlendirmede bulguların önem dağılımı



Bir üretim ad alanında tipik ilk çalıştırma dağılımı. İlk değerlendirmenin döndürdüğünün çoğu acil değildir – değer, acil olan azınlığı ayırmakta.

PRATİKTE

Ekipler nerede kullanıyor

Hibrit ve çok bulutlu ortamlardaki yaygın konumlandırmalar – genellikle tek bir ad alanı ya da depolama hesabıyla başlar.

CI/CD imaj geçidi

İmajlar terfiden önce taranır; böylece zafiyetli ya da kurcalanmış bir katman üretime ulaşmak yerine hattı düşürür.

Herkese açıklık taramaları

Sürekli denetimler, yanlışlıkla herkese açık hâle getirilmiş bir bucket'ı yakalar – bulut veri sızıntısının en yaygın tek nedeni.

Paylaşımlı depolama hijyeni

Paylaşımlı bulut depolamasına düşen dosyalar, başka bir iş yükü ya da kullanıcı onları almadan önce zararlı içeriğe karşı denetlenir.

Çalışma zamanı sapma tespiti

Üretimde testtekinden farklı davranan bir konteyner, gürültü sayılıp geçilmek yerine anomali olarak işaretlenir.

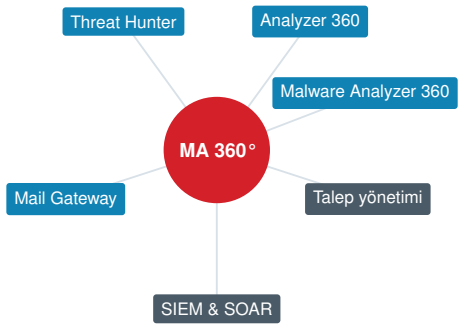
Satın alınan ve devralınan ortamlar

Geçen yıl satın aldığınız ortam, kendi kurduğunuzla aynı motor tarafından değerlendirilir; böylece iki kısmi yanıt yerine tek bir yanıt olur.

Düzenlemeye tabi iş yükleri

Değerlendirme geçmişi, önem dereceleri ve giderme durumu; bir düzenleyicinin ya da denetçinin istediği belgeli kanıt zincirini sağlar.

Bir bulut bulgusuna ne oluyor



Bulgu	CVE, açıklık ya da zararlı içerik
Önem	sıralanmış, düz liste değil
Korelasyon	hangi uç nokta ya da kutu dokundu
Aksiyon	hat geçidi, talep kaydı, SIEM olayı

İlk kümenizi bu hafta tarayın.

Cloud Hunter'ı tek bir ad alanına ya da depolama hesabına yöneltin; CVE tabanlı bir taramanın ve bir bucket taramasının neler çıkardığını görün.

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

TEKNİK ÖZELLİKLER

Özellikler ve yetenekler

KONTEYNER ANALİZİ

- Docker ve Kubernetes imajları, yapılandırması ve çalışma zamanı davranışı
- Canlı CVE verisine karşı CVE tabanlı zafiyet taraması
- Manifest okuması değil, katman katman inceleme
- Sonraki bir katmanda silinen içerik de bulunur
- Geçişli ve derleme anı bağımlılıkları değerlendirilir
- Enjekte edilmiş zararlı kod, arka kapılar ve kripto madencileri tespiti
- Şüpheli ikili dosyalar sandbox'ta kontrollü çalıştırılır
- Katmana gömülmüş sırlar ve kimlik bilgileri öne çıkarılır
- Kritik bulgular göründüğü anda raporlanır

YAPILANDIRMA & GÜVENLİK DURUŞU

- Ayrıcalıklı bayrak ve root kullanıcı tespiti
- Açık portlar ve gevşek ağ politikası
- Yazılabilir dosya sistemleri ve gevşek bağlamalar
- Küme ve kabul yapılandırması değerlendirilir
- Hatalı yapılandırma yalnızca varlığına göre değil, istismar edilebilirliğine göre sıralanır
- Giderme durumu yeniden değerlendirmeler boyunca izlenir

BUCKET & NESNE DEPOLAMA

- S3, Azure Blob ve benzeri nesne depoları
- Hatalı izinler için sürekli tarama
- Herkese açık bucket tespiti
- Saklanan nesnelerde zararlı içerik
- Şüpheli dosya etkinliği ve erişim örüntüleri
- Zararlı yüklemeler, alt akıştaki iş yükleri okumadan engellenir
- Nesneler yalnızca planlı değil, geldikleri anda taranır

DOSYA SİSTEMİ KORUMASI

- Bulut içindeki dosya hareketlerinin gerçek zamanlı analizi
- Zararlı içerik ve betik tabanlı saldırılar anında yakalanır
- Şüpheli çalıştırılabilirler çalışmadan önce belirlenir
- Paylaşımlı depolamada anormal değişiklik tespiti
- Politika gerektirdiğinde CDR dokümanları temiz olarak yeniden oluşturur

ÇALIŞMA ZAMANI & İZLEME

- Bulut kaynak etkinliğinin sürekli izlenmesi
- Çalışma zamanı davranışı derleme anı beklentisiyle karşılaştırılır
- Sapma, gürültü sayılıp geçilmek yerine anomali olarak işaretlenir
- Davranışsal bağlam CyberFortress AI tarafından sağlanır
- Tehditler ölçülecek bir etki doğurmadan yakalanır

KAPSAMA

- Derleme anında geliştirici makineleri ve CI koşucuları
- Genel ve özel imaj depoları; gönderimde ve planlı olarak
- Yerinde Docker ve Kubernetes kümeleri
- Herhangi bir genel bulutta yönetilen Kubernetes ve konteyner hizmetleri
- Tek konsoldan hibrit ve çok bulutlu ortamlar
- Satın alınan ve devralınan ortamlar aynı motorla değerlendirilir

HAT & YAŞAM DÖNGÜSÜ

- CI/CD geçit denetimi – kötü bir katman hattı düşürür
- Yeni CVE'ler yayımlandıkça imaj deposunun yeniden değerlendirilmesi
- Yayına alma anında yapılandırma değerlendirmesi
- Yayın sonrası çalışma zamanı izleme
- Olay müdahalesi ve denetim için değerlendirme geçmişi

RAPORLAMA & YÖNETİM

- Bulgular, önem dereceleri ve giderme durumu tek raporda
- PDF, CSV, JSON ve HTML rapor üretimi
- Syslog sunucunuza akıtılan özelleştirilebilir kayıtlar
- Rol tabanlı kullanıcı yönetimi ve erişim kısıtlaması
- Her motor için sağlık izleme
- Değerlendirmelerin 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
- Bulut depolama: Amazon S3, Azure Blob, Google Drive, Box, Dropbox
- Tehdit istihbaratı: MISP, OpenCTI, ThreatQ, Anomali ThreatStream
- Talep yönetim sistemleri bulguları otomatik açar, günceller ve kapatır
- Geri kalan her şey için syslog akışı

CyberFortress

İmajlarınızın içinde gerçekte ne olduğunu bilin.

Cloud 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