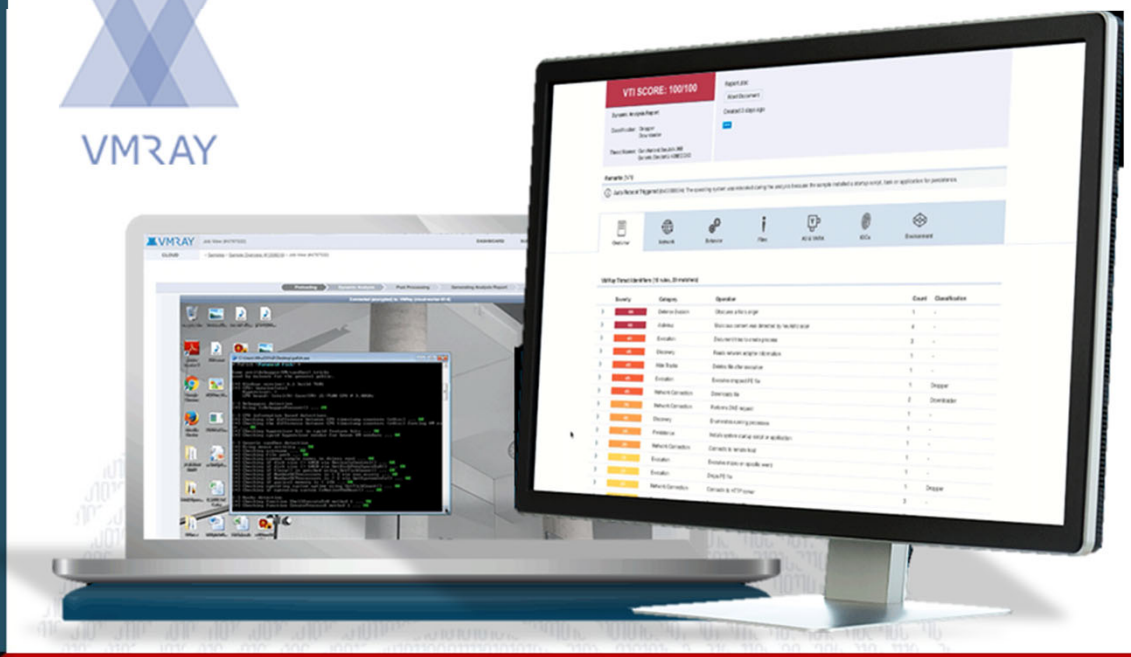
DIFOSE

VMRAY



VMRAY ANALYZER

ÜRÜN AÇIKLAMASI

VMRay Analyzer, yazılım analistlerinin ve olay müdahale ekiplerinin kötü amaçlı yazılımlara karşı gizlilik içinde tehditleri izlemesine, analiz etmesine ve tehlike göstergelerini tanımlamasına olanak tanıyan otomatik, kötü amaçlı yazılım analizi ve algılama çözümüdür.

Geleneksel sandbox çözümlerinden farklı olarak, VMRay Analyzer yalnızca hiper yönetici katmanında çalışır ve analiz ortamında tek bir biti değiştirmeye gerek yoktur. VMRay Analyzer kötü amaçlı yazılımlara karşı tamamen gizlilik içinde kötü amaçlı yazılım ile sistem arasındaki etkileşimin izlenmesini sağlar.

Günümüzde kötü amaçlı yazılımlar, bir analiz ortamını algılayacak şekilde tasarlanmıştır. En gizlenebilir kötü amaçlı yazılım bile VMRay Analyzer'da ortaya çıkacaktır.

VMRAY ANALYZER RAPORUNUN SAĞLADIKLARI:

- Üst düzeyde tespit (Kötü Amaçlı, Şüpheli veya Kötü Amaçlı Değil)
- Tehdit Göstergeleri
- Analiz sırasında alınan ekran görüntüleri
- Ağ Davranışı
- IOC'ler
- İndirilebilir İşlev Günlüğü
- Ve daha fazlası

KULLANIM

VMRay Analyzer 'Şimdi *(Now)*, Yakın *(Near)*, Derin *(Deep)*' mimarisi kullanır - dosyalar önce ultra hızlı motor tarafından önceliklendirilir. ('Şimdi'), etkin ve potansiyel olan kötü amaçlı bileşenler için statik olarak analiz edilir ('Yakın') ve tam dinamik sandbox analizi yapılır ('Derin'). Sandbox analizi, piyasadaki en hızlı ve en ölçeklenebilir olanıdır ve uygun maliyetli bir sanallaştırılmış ortamda bare-metal performansı sunar.

ÜRÜN AÇIKLAMASI

VMRay Analyzer Cloud ve VMRay Analyzer On-Premises, aynı temel işlevlere ve kötü amaçlı yazılımları analiz etme ve algılama yeteneğine sahiptir. Cloud ve On-Premises arasındaki temel fark, sunulan özelleştirme düzeyidir.
VMRay Analyzer On-Premises, aşağıdakilerin kapsamlı şekilde özelleştirilmesini destekler:

- Hedef Sanal Makineler: Kuruluşun kendi golden imajı gibi tamamen özelleştirilmiş sanal makine imajındaki dosyaları ve URL'leri analiz edebilir.
- Algılama Kuralları ve Analiz Puanlama Sistemi: Güvenlik ekipleri kendi algılama kurallarını ekleyebilir ve yerleşik analiz puanlama sistemini özelleştirebilir (VMRay Tehdit Tanımlayıcısı veya VTI Puanı ve Yara kuralları)
- Backend Global Ayarları: Bağımsız kullanıcı grupları oluşturma, gelişmiş ağ yapılandırma ayarlarını değiştirme, analiz başına toplam boyut ve bellek dökümü sayısı gibi diğer gelişmiş ayarları değiştirme becerisini içerir.

ANA UNSURLAR

- Platformlar: Windows, macOS
- Kapsam: Tüm dosya türleri ve URL'ler
- Dağıtım: Bulut veya Şirket İçi
- Entegrasyon: Web, e-posta, SOAR, EPP/EDR ve diğer araçlar için 25'ten fazla yerleşik bağlayıcı
- Uyumluluk: KVKK uyumlu, ISO-27001 sertifikalı
- IDA Eklentisi: IDA Pro statik analizini davranış tabanlı verilerle zenginleştirin
- Endüstri Standartları Desteği: MITER ATT & CK ™ Framework, YARA kuralları , STIX ™ ve diğerleri
- Özelleştirilmiş Ortamlar: Hedeflenen kötü amaçlı yazılımların tespitini optimize etmek için golden imaj ve bulut yerelleştirme

İŞLETİM SİSTEMİ

VMRay Analyzer bulut hizmetinde Windows İşletim Sistemlerini (Windows 7'den Windows 10'a kadar) desteklemektedir. Şirket içi için ek Windows sürümleri desteklenir.

ENTEGRASYON

VMRay Analyzer, güvenlik ekosistemindeki üçüncü taraf platformlar için kullanıma hazır destek sağlar - Endpoint Protection, SIEM, SecOps (SOAR) ve Threat Intelligence (TIP). Ayrıca, özel entegrasyonlar için dökümanlanmış bir REST API ve örnek python kütüphaneleri bulunmaktadır.

DESTEK

Avrupa ve ABD çalışma saatlerinde destek verilmektedir. Destek istekleri, e-posta veya Zendesk portalı aracılığıyla veya ücretsiz +1 (888) 958-5801 (Kuzey Amerika) numarası arayarak talep edilebilir.

Daha fazla ayrıntı için www.vmray-legal.com adresindeki lisans sözleşmesine veya İletişim sayfasına bakınız.

YETENEKLER

Office belgeleri, komut dosyaları, arşivler, sürücüler, çalıştırılabilir dosyalar ve URL'ler için tüm ana formatlar desteklenmektedir. Kötü amaçlı yazılım geliştiricileri belirsiz ve güncel olmayan biçimlerden yararlanarak yeni bulaşma vektörleri ararken desteklenen dosya türleri yelpazesi sürekli olarak genişletilmektedir.

Ankara: Ümit Mah. 4281 Sok. Kafkas Sitesi No:6 06810 Ümitköy/ÇANKAYA
İstanbul: Esentepe Mah. Kelebek Sk. No:2 Marmara Kule Kat:10 D:79 34870 KARTAL
+90 (312) 219 56 16
+90 (216) 771 07 97