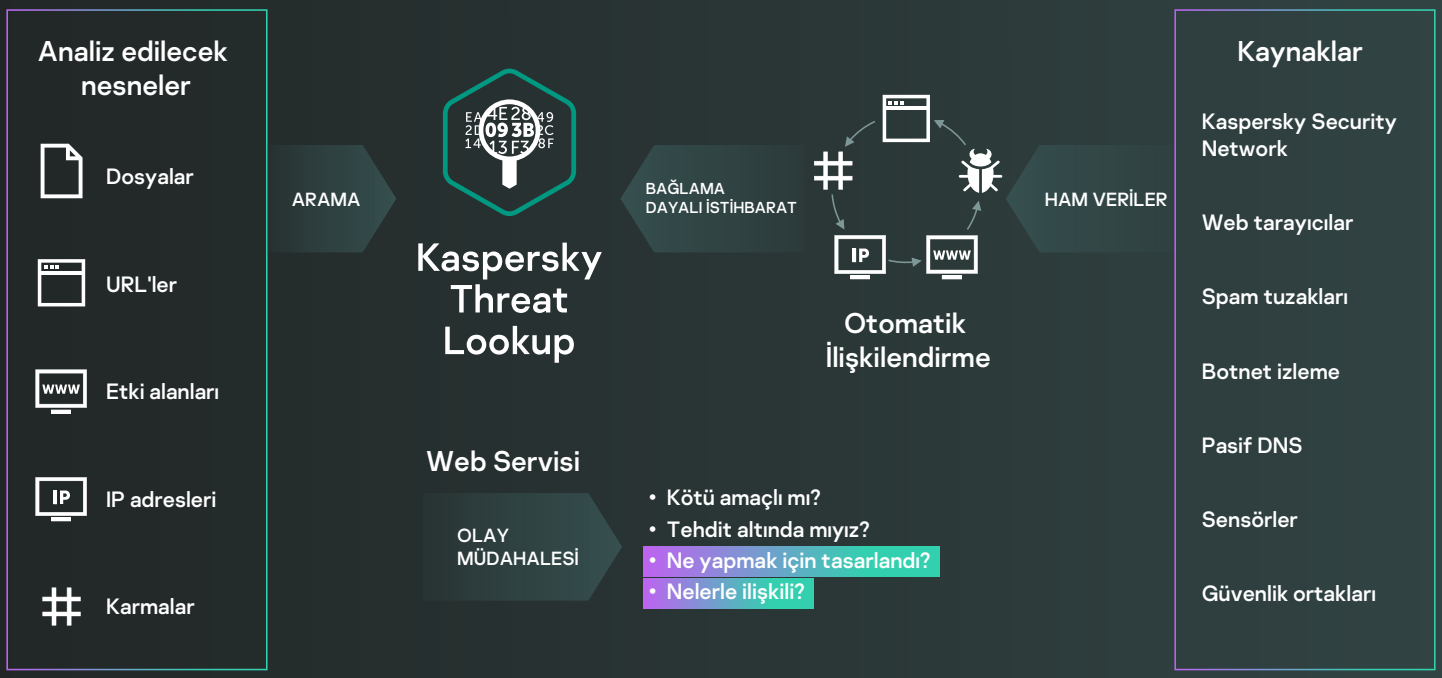
Kaspersky Threat Lookup

kaspersky GELECEĞİ YAKALAYIN

Kaspersky Threat Lookup

Siber suçlar sınır tanımamaktadır ve teknik kapasiteleri hızla gelişmektedir; siber suçlular hedeflerini tehdit etmek için dark web kaynaklarını kullanırken saldırıların giderek ne kadar gelişmiş hale geldiği görülmektedir. Savunmanızı tehlikeye atmak için yeni girişimler ortaya çıktıkça siber tehditlerin sıklığı, karmaşıklığı ve gizlenme taktikleri de sürekli artmaktadır. Saldırganlar, işletmenizin işleyişini aksatmak, varlıklarınızı çalmak veya müşterilerinize zarar vermek için karmaşık ölüm zincirleri ve özelleştirilmiş Taktikler, Teknikler ve Prosedürler (TTP'ler) kullanmaktadır.

Kaspersky Tehdit Arama, Kaspersky'nin siber tehditler ve bunların ilişkileri konusunda elde ettiği bilgi birikiminin tamamını tek ve güçlü bir web hizmetinde sunar. Amaç, güvenlik ekiplerinize mümkün olduğunca fazla veri sağlayarak siber saldırıları kuruluşunuzu etkilemeden önce önlemektir. Platform; URL'ler, etki alanları, IP adresleri, dosya karmaları, tehdit adları, istatistiksel/davranışsal veriler, WHOIS/DNS verileri, dosya özellikleri, coğrafi konum verileri, indirme zincirleri, zaman damgaları vb. hakkında en güncel ve ayrıntılı tehdit istihbaratını alır. Sonuç olarak, yeni ve büyümekte olan tehditler küresel çapta görünür hale gelir; bu da kuruluşunuzun güvenliğini sağlamanıza yardımcı olur ve olaylara müdahaleyi destekler.



Öne Çıkan Noktalar

Güvenilir İstihbarat: Kaspersky Tehdit Arama'nın önemli bir özelliği, eyleme geçirilebilir bağlamla zenginleştirilmiş tehdit istihbaratı verilerimizin güvenilirliğidir. Kaspersky, kötü amaçlı yazılım testlerinde[1] alanında lider konumundadır ve sıfıra yakın hatalı pozitif sonuçla en yüksek algılama oranlarını elde ederek güvenlik istihbaratımızın benzersiz kalitesini gösterir

Tehdit avlama: Etkilerini ve sıklıklarını en aza indirmek için saldırıları önlemede, saptamada ve yanıtlamada proaktif olun. Saldırıları takip ederek en kısa zamanda etkili bir şekilde ortadan kaldırın. Bir tehdidi ne kadar erken fark ederseniz o kadar az hasara neden olur, onarımlar o kadar hızlı yapılır ve ağ operasyonları o kadar erken normale döner

Olay araştırmaları: Bir Araştırma Grafiği, Tehdit Aramada depolanan verileri ve algılanan tehditleri görsel olarak incelemenize olanak tanıyarak olay araştırmalarını destekler. Bir olayın tam kapsamını daha iyi anlayabilmeniz ve temel nedenini belirleyebilmeniz için URL'ler, etki alanları, IP'ler, dosyalar ve diğer bağlamlar arasındaki ilişkinin grafik bir görselleştirmesini sunar

Ana arama: Tek ve güçlü bir arabirimde tüm aktif tehdit istihbaratı ürünlerinde ve harici kaynaklarda (OSINT IoCs, Dark Web ve Surface Web dahil) bilgi arayın

Kullanımı kolay Web arabirimi veya RESTful API: Tercihinize bağlı olarak bir web arabirimi yoluyla (bir web tarayıcısı üzerinden) hizmeti manuel modda kullanın veya basit bir RESTful API üzerinden hizmete erişim sağlayın

Çok çeşitli dışa aktarma biçimleri: Tehdit istihbaratının tüm avantajlarından faydalanmak, operasyon iş akışını otomatikleştirmek veya SIEM'ler gibi güvenlik kontrollerini entegre etmek için IOC'leri (Güvenlik İhlal Göstergeleri) veya eyleme geçirilebilir bağlamı STIX, OpenIOC, JSON, Yara, Snort ve hatta CSV gibi yaygın olarak kullanılan ve daha düzenli, makine tarafından okunabilen paylaşım biçimleri olarak dışa aktarın

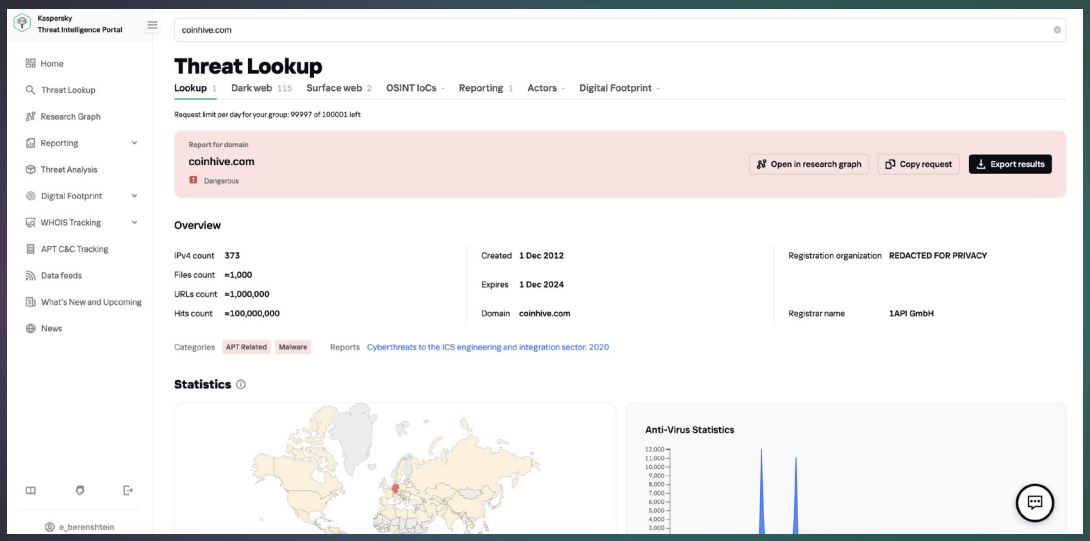
Avantajlar

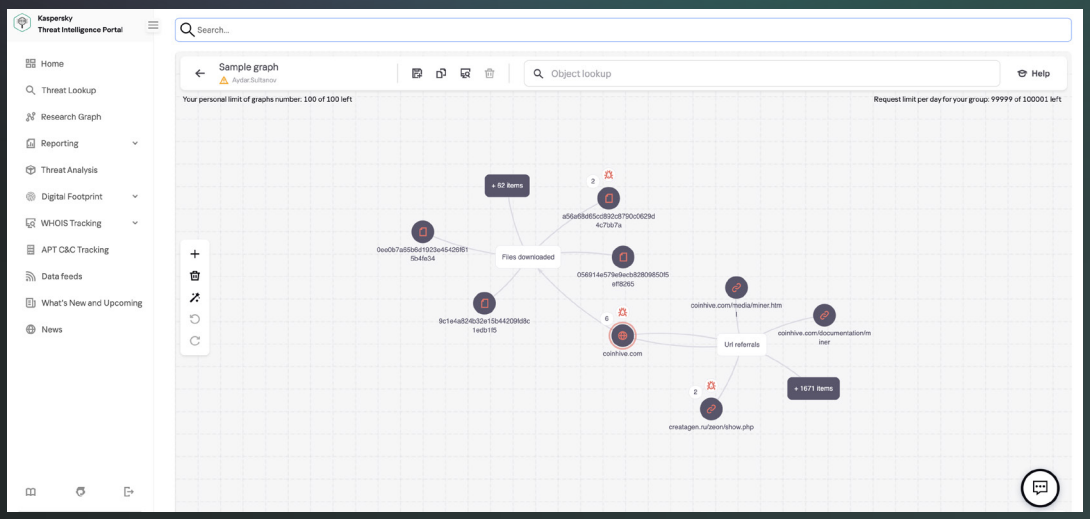
Saldırıları önceliklendirmenize ve işletmeniz için en çok risk teşkil eden tehditleri en aza indirmeye odaklanmanıza olanak tanıyan yüksek düzeyde doğrulanmış tehdit bağlamı ile tehdit göstergeleriyle ilgili ayrıntılı aramalar yapın

Ana bilgisayarlar ve ağ üzerindeki güvenlik olaylarını daha verimli ve etkili bir şekilde tanılayıp analiz edin ve bilinmeyen tehditlere karşı dahili sistemlerden gelen sinyalleri önceliklendirin

Kritik sistemler ve veriler tehlikeye girmeden ölüm zincirini bozmak için olay müdahalesi ve tehdit avlama kabiliyetlerinizi geliştirin

[1] kaspersky.com/top3





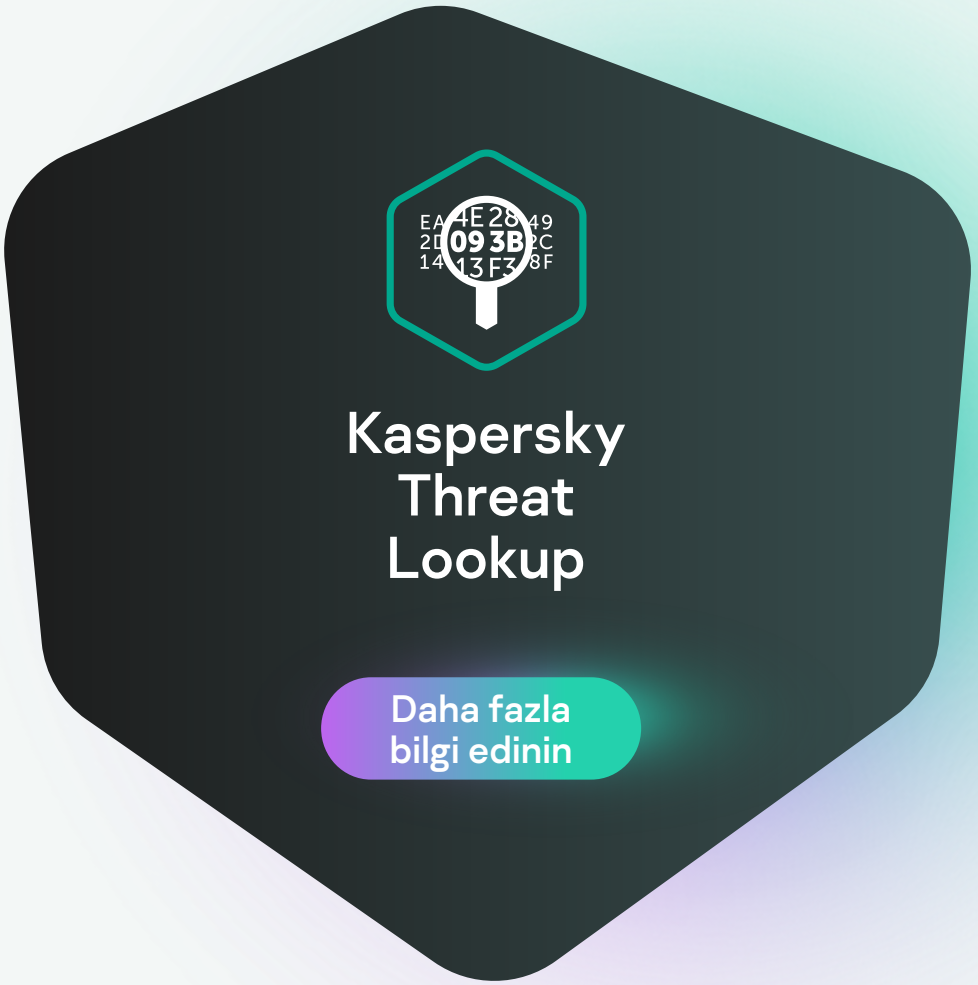
Artık;

Web tabanlı bir arabirimden veya RESTful API aracılığıyla tehdit göstergelerini arayabileceksiniz

Yeni şüpheli nesneleri bulmak için sertifikalar, sık kullanılan adlar, dosya yolları veya ilgili URL'ler dahil olmak üzere gelişmiş ayrıntıları inceleyebileceksiniz

Bulduğunuz nesnenin yaygın mı yoksa benzersiz mi olduğunu kontrol edebileceksiniz

Bir nesnenin neden kötü amaçlı olarak değerlendirilmesi gerektiğini anlayabileceksiniz



www.kaspersky.com.tr