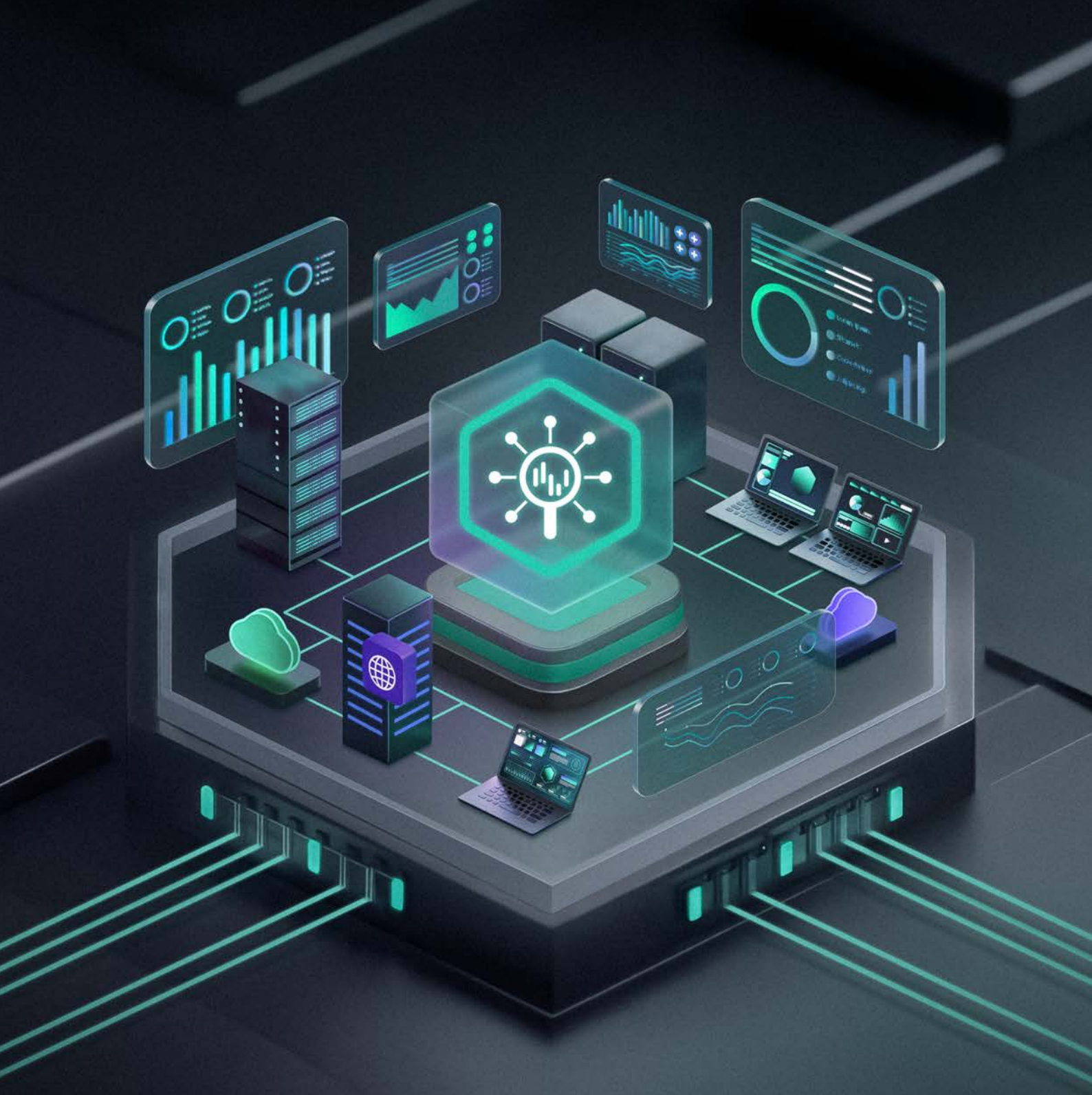


Veri Sayfası

Kaspersky SIEM

Yapay zeka ile desteklenen ve dünya standartlarında Tehdit İstihbaratı ile geliştirilmiş yeni nesil çözümümüzle güvenlik operasyonlarınızı dönüştürün.

kaspersky geleceği yakalayın

Kaspersky SIEM, karmaşık BT altyapıları, yüksek veri hacimleri ve katı yasal gereklilikleri olan kuruluşlar içindir. Ürün, yerleşik çoklu kiracılık desteği ile MSSP uyumluluğu sunar.

Bu kuruluşlar, etkili güvenliğin yalnızca önlemeyle değil, aynı zamanda çeşitli sistemlerdeki tehditleri gerçek zamanlı olarak tespit etme, analiz etme ve bunlara yanıt verme becerisine de bağlı olduğunu kabul etmektedir.

Güvenlik operasyonlarınızın etkisini en üst düzeye çıkarın

Büyük kuruluşlar, giderek artan sayıda Gelişmiş Kalıcı Tehdit (APT) ile karşı karşıya kalmaktadır. 2024 yılında, dört işletmeden birinde APT'ler tespit edildi ve tüm yüksek öneme sahip olayların %43'ünü oluşturdu[1]. Sonuçları, iş kesintilerinden mali kayıplara ve uzun vadeli itibar kaybına kadar uzanan maliyetli sonuçlar doğurur.

Güvenlik ekipleri benzeri görülmemiş bir baskı altında. Koruma sistemleri büyük miktarda veri üretir, bu da depolama maliyetlerini artırır ve SIEM dağıtımlarını pahalı hale getirir. Nitelikli uzmanlar az sayıda bulunurken, var olan ekipler aşırı yüklenmiş durumda. Güvenlik Operasyon Merkezlerinin (SOC) %70'i, art arda gelen uyarılarla başa çıkmakta zorlanıyor[2]. Bunun üzerine, SIEM sistemlerinin yönetiminin karmaşıklığı, zaten sınırlı olan kaynakları daha da zorlamaktadır.

En deneyimli Güvenlik Operasyon Merkezleri bile, gürültüyü ortadan kaldırıp en önemli konulara odaklanmalarına yardımcı olacak günümüzün yapay zeka destekli araçları olmadan verimlilik ve etki kaybı riskiyle karşı karşıyadır.

Ekibinizi, dünya çapında bir tehdit istihbaratı ile desteklenen, yapay zeka destekli bir SIEM ile donatın.

Kaspersky SIEM, güvenlik ekibinizin gelen güvenlik verilerini yönetmesine ve analiz etmesine yardımcı olmak için tasarlanmış yeni nesil bir çözümdür. Şu konularda mükemmeldir:

Kaspersky ürünleri, işletim sistemleri, üçüncü taraf uygulamalar, güvenlik araçları ve veritabanları dahil olmak üzere çeşitli kaynaklardan olayları toplama, işleme ve depolama.

Gelen verileri gerçek zamanlı olarak analiz edip ilişkilendirerek, şüpheli etkinlikleri tespit etmek için sektör lideri Tehdit İstihbaratı ile zenginleştirir.

Hızlı olay araştırması ve müdahalesi için zamanında uyarılar sağlama.

Kesintisiz eşzamanlı arama işlevine sahip sıcak ve soğuk depolama seçenekleri sayesinde, pahalı depolama donanımı için bütçenizi aşmadan verileri uzun süre depolayın.

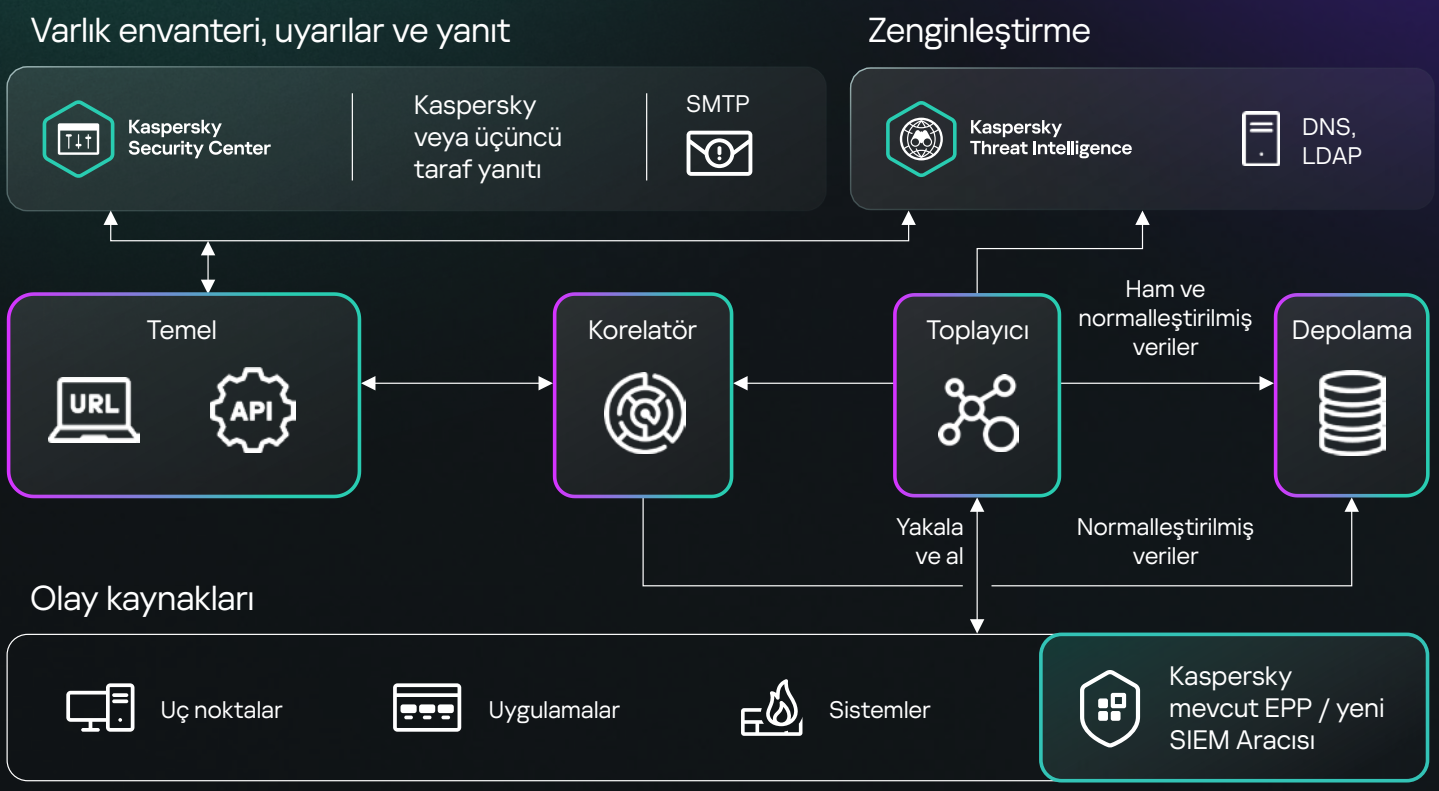
Güvenlik kaynaklarından gelen günlükleri birleştirerek ve bunları gerçek zamanlı olarak ilişkilendirerek, Kaspersky SIEM analistlerinize verimli bir şekilde yanıt vermek için gereken tam görünürlük ve bağlamı sağlar.

Tehdit avcılarınızın daha önce bilinmeyen tehditleri ortaya çıkarmasını sağlayan gelişmiş arama ve analiz özellikleri sunar. UEBA algılama kuralları seti ile tarihsel veri analizi ve istatistiksel temel belirleme, ekibinizin anomalileri tespit etmesine ve sofistike saldırıları durdurmasına yardımcı olur.

Kaspersky SIEM ile SOC'niz, çok büyük miktarda veriyi eyleme geçirilebilir güvenlik bilgilerine dönüştürmek için ihtiyaç duyduğu görünürlük, zeka ve verimliliği elde eder. Çözüm, internet bağlantısı olmadan da çalışabilir ve tam veri egemenliği sağlar.

1 Kaspersky Managed Detection and Response analist raporu, 2024
2 Kaspersky Raporu: Modern bilgi güvenliği profesyonelinin portresi, 2024

Nasıl çalışır?



Çözümün mikro hizmet mimarisi sayesinde, yöneticileriniz Kaspersky SIEM'i tam donanımlı bir SIEM aracı veya günlük yönetim sistemi olarak kullanmak için ihtiyaç duydukları mikro hizmetleri oluşturabilir ve yapılandırabilir.

Kaspersky SIEM, Kaspersky ve üçüncü taraf ürünlerini merkezi bir güvenlik sistemine entegre eden Open Single Management Platform[3] üzerine kurulmuştur. Kapsamlı bir savunma stratejisinin önemli bir parçasını oluşturur, kurumsal ve endüstriyel ortamları korur ve BT sistemlerinden OT sistemlerine geçen siber saldırıları tespit eder.

Kaspersky SIEM'i öne çıkaran özellikler

Performansı en üst düzeye çıkarır, maliyetleri en aza indirir

Eski çözümlerden daha üstün performans gösteren ve her bir örnekte yüz binlerce EPS'yi işleyen yüksek performanslı, modüler SIEM ile donanım ve sanallaştırma maliyetlerini %50'ye kadar azaltın ve TCO'yu düşürün.

Birleşik tek Kaspersky ekosistemi

Yerleşik yanıt seçenekleriyle 200'den fazla önceden yapılandırılmış Kaspersky ve üçüncü taraf entegrasyonlarından yararlanın. Kesintisiz ekosistemimiz, Tehdit İstihbaratı için tek bir arabirim sunar, uç nokta sensörlerini SIEM ajanları olarak kullanır ve diğer satıcıların sunamadığı entegrasyon yetenekleri sağlar.

Dâhili SOC uzmanlığı

700'den fazla önceden yapılandırılmış algılama kuralına erişin. Bu kurallar, sektörün en deneyimli tehdit avcılarından biri olan Kaspersky SOC tarafından geliştirilmiş olup, MITRE eşlemesi ve yanıt kılavuzuyla üç ayda bir güncellenmektedir.

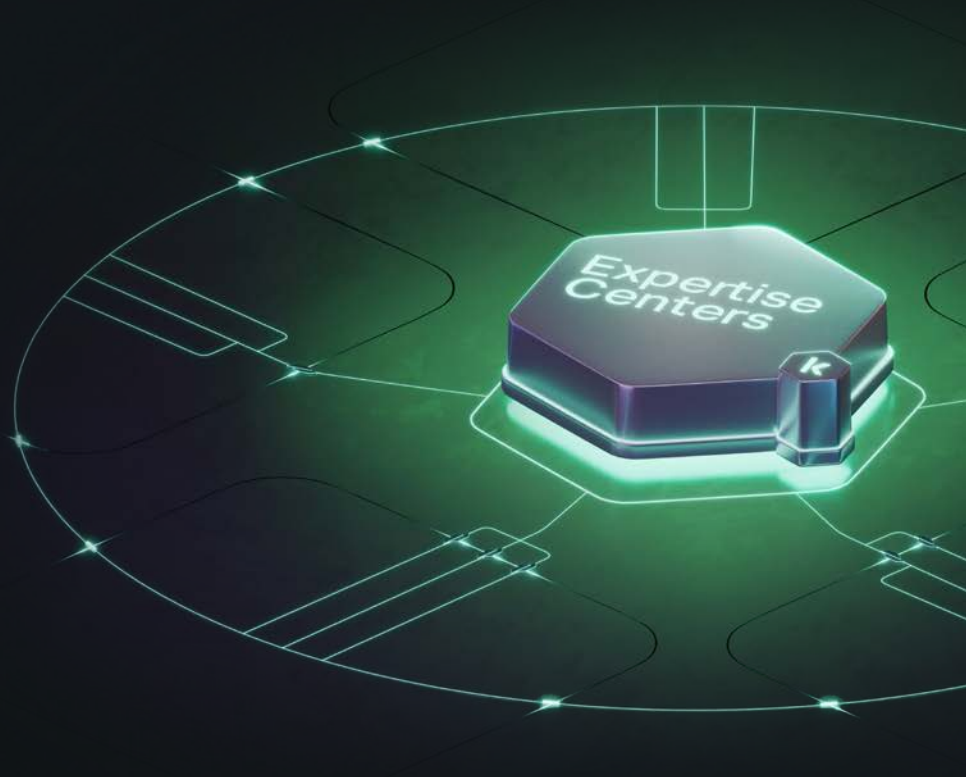
Yapay Zekâ Destekli Tehdit Tespiti

Yapay zeka ile geliştirilmiş bileşenler, DLL yönlendirme saldırısı yapay zeka algılama, varlıkların AI tabanlı risk puanlaması ve daha fazlası ile altyapınızda şüpheli etkinlikleri hızla tespit eder. Bu özellikler algılama doğruluğunu artırır, hatalı pozitifleri azaltır ve siber olayların etkisini en aza indirerek MTTD ve MTTR'nizi iyileştirmeye yardımcı olur.

3 Bu platform tarafından desteklenen Kaspersky Next XDR Expert, gelişmiş tehdit avcılığı, otomatikleştirilmiş kitapçıklar ve kolaylaştırılmış vaka yönetimi ile yeteneklerini genişletir.

Kaspersky SIEM, siber güvenliği geliştirmeye adanmış beş uzmanlaşmış, birleşik merkez olan Kaspersky Expertise Centers'ın yıllara dayanan bilgi birikiminden ve rafine becerilerinden yararlanır.

Daha fazla bilgi



Kaspersky SIEM, Kaspersky Profesyonel Hizmetleri veya güvenilir iş ortakları tarafından sunulan ve bağlı ürünlerin API özelliklerinden yararlanan özel entegrasyonlar da dahil olmak üzere 7/24 Premium Destek ve Hizmetler ile birlikte gelir.

SIEM dağıtımınızdan maksimum değer elde etmenizi sağlamak için anahtar teslimi uygulama, sorunsuz geçiş desteği ve sürekli uzmanlık sağlıyoruz.

Kaspersky SIEM

www.kaspersky.com.tr

Daha fazla bilgi

#kaspersky
#geleceğiyakalayın