Ürün Tanıtım Metni

Kaspersky SIEM

kaspersky GELECEĞİ YAKALAYIN

İçindekiler

Güvenlik Bilgi ve Olay Yönetimi Pazarı

Kuruluşlardaki siber güvenlik liderleri, altyapılarına sızma girişimlerinin sayısının artması, siber güvenlik personelinin yetersizliği ve giderek karmaşıklaşan saldırılar da dahil olmak üzere çok sayıda zorlukla karşı karşıyadır.

Ayrıca kuruluşlar, küresel SIEM pazarını etkileyen veri saklama, denetim ve olay incelemesi ile ilgili yasal gerekliliklere uymak zorundadır.

Kuruluşlar ayrıca, siber saldırı uyarılarını önceliklerine göre ayırma ve büyüme ve artan karmaşıklık nedeniyle bunları daha verimli bir şekilde önceliklendirme baskısı altındadır.

Buna ek olarak, uzaktan çalışma koşulları şirketlerin SaaS uygulamalarını benimsemesine ve çalışanların kendi cihazlarını getirmelerine (BYOD) izin vermesine yol açarak ağ görünürlüğünü geleneksel çevrenin sınırlarının ötesine genişletme ihtiyacını ortaya çıkarmıştır.

Son olarak, bilgi güvenliği alanında nitelikli uzmanlar bulmak günümüz piyasasında büyük bir zorluk teşkil etmektedir. Şirketler kaynaklarını optimize etmenin ve siber güvenlik verimliliğini artırmanın yollarını arıyor. Sonuç olarak, kuruluşlar SOC ekipleri için kolayca erişilebilir ve eyleme geçirilebilir istihbarat verileri istiyor.

Kaspersky Human Factor 360 Raporu'na göre

%77 oranında şirket en az bir siber güvenlik ihlali yaşadı ve birçoğu bu dönemde altıya kadar ihlal yaşadı

%41 %51 oranında şirket siber güvenlik altyapılarında eksiklikler olduğunu düşünüyor ve ileriye dönük olarak bu alandaki yatırımlarını artırmayı planlıyor

Daha fazla bilgi

Kaspersky SIEM ve mimarisi hakkında

Kaspersky Unified Monitoring and Analysis Platform, güvenlik verilerini ve olaylarını yönetmek için entegre bir yeni nesil SIEM çözümüdür. Güvenlik bilgileri olaylarını alma, işleme ve depolama ve gelen verileri analiz etme ve ilişkilendirme konusunda mükemmeldir. Platform ayrıca bir arama özelliğine sahiptir, potansiyel tehditler tespit edildiğinde uyarılar oluşturur ve oluşturulan uyarılara otomatik yanıtları ve tehdit avcılığını destekler.

Yüksek performanslı modüler mimari, her örnekte saniyede yüz binlerce olayın (EPS) işlenmesine ve sistem gereksinimlerini optimize ederek toplam sahip olma maliyetinin (TCO) azaltılmasına olanak tanır.

Üçüncü taraf ve Kaspersky ürünlerini merkezi bir bilgi güvenliği sistemine dahil eden Kaspersky SIEM, kurumsal ve endüstriyel ortamların güvenliğini sağlamanın yanı sıra BT'de başlayıp OT sistemlerine geçiş yapan siber saldırıları tespit edebilen kapsamlı bir savunma stratejisinin önemli bir parçasıdır.

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

Çözüm, Kaspersky ürünleri, işletim sistemleri, üçüncü taraf uygulamalar, güvenlik araçları ve çeşitli veritabanları dahil olmak üzere çeşitli kaynaklardan güvenlik olaylarını alır ve olayları birbiriyle ilişkilendirir ve kurumsal ağ altyapılarındaki şüpheli etkinlikleri belirlemek ve güvenlik olaylarının zamanında bildirilmesini sağlamak için bunları tehdit istihbaratı beslemelerinden gelen verilerle zenginleştirir.

Kaspersky SIEM, tüm güvenlik kontrollerinden günlükleri toplayarak ve verileri gerçek zamanlı olarak ilişkilendirerek olay inceleme ve müdahale için gereken tüm bilgileri bir araya getirir ve sağlar.

Ayrıca Kaspersky SIEM, operatörlerin geçmiş verileri analiz edip ilişkilendirmesine ve anormallikleri belirlemek için istatistiksel temeller oluşturmasına olanak tanıyarak tehdit avcılarının daha önce bilinmeyen tehditleri keşfetmesini sağlar.

Kaspersky Unified Monitoring and Analysis Platform aşağıdaki bileşenleri içerir

Sistem bileşen ayarlarını kontrol etmek ve izlemek için merkezi bir grafik kullanıcı arayüzüne sahip bir **Çekirdek**. Platforma API kullanılarak üçüncü taraf çözümlerden erişilebilir.

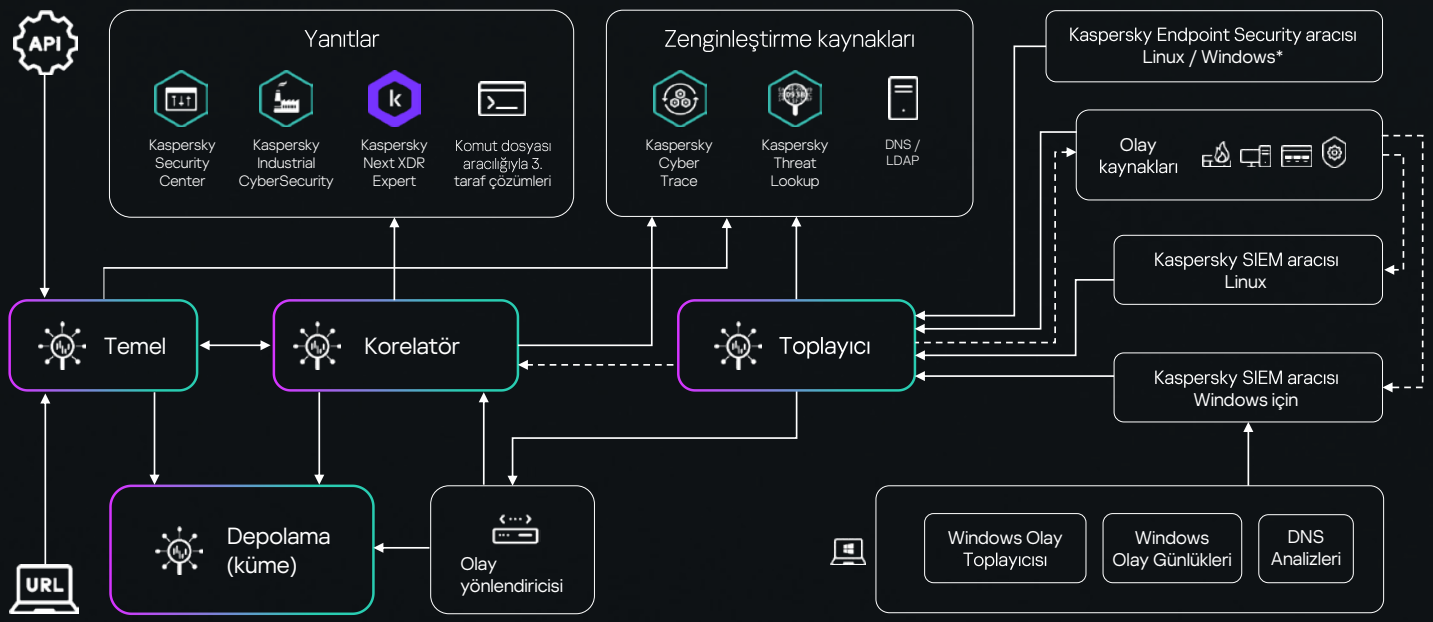
İlişkilendirme kuralları, işlenen olayların belirli dizilerini tespit etmek ve tanıma işleminden sonra ilişkilendirme olayları/uyarıları oluşturmak veya aktif bir listeyle etkileşime geçmek gibi belirli eylemleri gerçekleştirmek için kullanılır. **Korelatör**, toplayıcılardan alınan normalleştirilmiş olayları analiz ettikten sonra gerekli eylemleri gerçekleştirmek için aktif listeleri kullanır ve ilişkilendirme kriterlerine göre uyarılar oluşturur.

Bir veya daha fazla **Toplayıcı** harici kaynaklardan olayları alır ve bunları ön işleme tabi tutar: sözlükleri, DNS hizmetine yapılan çağrıları ve diğer araçları kullanarak bunları normalleştirir (tek bir biçime dönüştürür), filtreler, toplar ve harici kaynaklardan gelen verilerle zenginleştirir.

Depolama, normalleştirilmiş olayları saklamak için kullanılır, böylece analitik verileri çıkarmak için SIEM'den hızlı ve sürekli olarak erişilebilirler.

Aracılar, iş istasyonları ve sunuculardaki işlenmemiş olayları SIEM toplayıcılarına iletir. Windows günlük olaylarını doğrudan toplayıcıya göndermek artık Kaspersky Endpoint Security for Windows 12.6 veya Linux 12.2'de mümkün. Bu, olay kaynaklarını Kaspersky SIEM sistemiyle entegre etmek için gereken iş miktarını önemli ölçüde azaltır.

Olay yönlendiricileri, toplayıcılar düşük bant genişliğine sahip uzak ofislere veya zaten meşgul olan veri bağlantılarına kurulduğunda olayları gecikme olmaksızın düzenli bir şekilde alarak bağlantılardaki yükü ve güvenlik duvarlarında açılan bağlantı noktası sayısını azaltır.



Kaspersky SIEM işlevselliği

Düzenli güncellemeler ve iyileştirmelerle Kaspersky ve üçüncü taraf satıcılardan yüzlerce kaynağa yerleşik ve özel bağlayıcılar.

Kaspersky Profesyonel Hizmetler ekibi tarafından ücretsiz ek bağlayıcılar oluşturularak harici olay kaynaklarının entegrasyonu.

Hızlı arama sorguları ve güvenlik olaylarına ilişkin hazır raporlar.

Mevzuata uygunluk ve olay incelemesi için günlüklerin yerel olarak güvenli bir şekilde depolanması.

Kaspersky SIEM, operatörlerin dağıtılmış depolama kümelerindeki ilgili olayları daha hızlı ve daha kolay bulmasına yardımcı olmak için birden fazla depoda olay aramalarını destekler.

Güvenlik olayları hakkındaki bilgileri izleyin, işleyin ve saklayın

Kaspersky Unified Monitoring and Analysis Platform, günlüklerden olayları alır ve farklı olay kaynaklarından gelen verileri normalleştirerek tutarlı hale getirir. Bu bilgi güvenliği olayları oturum açma girişimlerini, veritabanı etkileşimlerini veya sensör bilgi yayınlarını içerebilir ve şirketin korunan BT altyapısının tamamından toplanır. Tek bir olay önemli görünmeyebilir, ancak bir bütün olarak ele alındığında, birden fazla tekil olay, güvenlik sorunlarını tespit etmek için kullanılabilecek daha büyük bir kötü niyetli faaliyet resmi çizer.

Merkezi yerel havuzumuz olan veri gölü, güvenlik çözümleri (EPP, FW, IAM, vb.), işletim sistemleri, iş uygulamaları (İK sistemleri, ofis araçları), fiziksel güvenlik sistemleri (otomatik erişim kontrol sistemleri) ve diğer cihazlar dahil olmak üzere çeşitli kaynaklardan günlükleri toplamak, dizine eklemek ve analiz etmek için bir platform sağlar.

Olaylar, filtrelendikten ve toplandıktan sonra analiz edilmek ve saklanmak üzere korelatöre iletilir. Uyarıları tanımlamak için, toplayıcı kaynaklardan olayları alır, işler ve bunları depolama, korelatör ve/veya üçüncü taraf hizmetlerine yönlendirir. İşlenmemiş olaylar iş istasyonları ve sunuculardan SIEM toplayıcılarına (bazı durumlarda aracılar tarafından) iletilir ve ek analiz için diğer sistemlere gönderilebilir.

İlişkilendirme olayları, belirli bir olayın veya ilgili olaylar dizisinin tanınması üzerine çözüm tarafından üretilir ve ayrıca analiz edilir ve saklanır. Bir olay veya olaylar dizisi potansiyel bir güvenlik tehdidine işaret ediyorsa Kaspersky SIEM, tehditle ilgili bilgileri ve güvenlik uzmanlarının dikkate alması gereken diğer ilgili bilgileri içeren bir uyarı oluşturur.

Olayları bileşenler arasında aktarmak için isteğe bağlı şifrelemeye sahip güvenilir aktarım protokolleri kullanılır. İzole segmentlerden veri toplamak için sistem tarafından bir veri diyotu kullanılabilir.

Kaspersky SIEM, sunucular, iş istasyonları ve ağ cihazlarının geniş bir envanterini sağlayarak merkezi varlık yönetimine olanak tanır. Platform, güvenlik açığı tarayıcıları gibi kaynaklardan varlık güvenlik açıkları hakkında veri toplayabilir ve tehditleri belirlemek için bunları varlık kategorisi verileriyle ilişkilendirebilir. Bu, güvenlik ekiplerine tüm varlık ortamına ilişkin görünürlük sağlar.

Analistleri desteklemek amacıyla, güvenlik düzeyini daha iyi değerlendirmek için MITRE ATT&CK matrisinin kurallara göre kapsamı görüntülenir.

Kaspersky sunucuları tarafından MITRE eşleme ve yanıt önerileriyle düzenli olarak güncellenen saldırı senaryolarını tespit etmek için 650'den fazla önceden yapılandırılmış ilişkilendirme kuralı.

Kaspersky Threat Intelligence Portal'dan (Kaspersky Threat Lookup ve Kaspersky CyberTrace kullanılarak) toplanan analitik verilerle zenginleştirilerek veri alaka düzeyi artırıldı.

Varlıklar ve altyapı hakkındaki veriler Kaspersky Security Center'dan ve üçüncü taraf kaynaklardan toplanır.

Kullanıcılar, ClickHouse veri madenciliği işlevini kullanarak bir olayı belirli bir zaman dilimi için gruplanmış, toplanmış, ortalama, maksimum ve minimum değerlerle karşılaştırabilir. Bu, çok sayıda hizmet kuralının oluşturulmasını gerektirmeden algılama mantığının yeteneklerini önemli ölçüde genişletir.

İçerik oluşturma ve düzenlemeyi kolaylaştırmak için, kullanıcıların filtre kriterlerinde herhangi bir değişiklik yapmadan önce amaçlanan değişikliğin hangi ilişkilendirme kurallarına uygulanacağını önceden öğrenmelerine olanak tanıyoruz.

Güvenlik olaylarının gerçek zamanlı ve geçmişe dönük ilişkilendirilmesi

Kaspersky SIEM, saldırıları ve tehditleri tanımlamak için özel kurallar ve sektördeki en başarılı ve deneyimli aktif tehdit avlama ekiplerinden biri olan Kaspersky SOC tarafından geliştirilen yüzlerce önceden tanımlanmış kural ile neredeyse gerçek zamanlı çapraz ilişkilendirme gerçekleştirir. Kaspersky SOC uzmanları, yüksek uzmanlık ve bilgi düzeylerini onaylayan çok sayıda sertifikaya sahiptir.

Olayların **korelasyonu gerçek zamanlı olarak gerçekleştirilir**. Korelatör normalleştirilmiş olayları analiz eder, ilişkilendirme kurallarına uygun olarak uyarılar oluşturur ve tüm aktif liste işlemlerini gerçekleştirir.

Korelatörün çalışma prensibi olay imza analizine dayanır, yani her olay kullanıcı tarafından belirlenen ilişkilendirme kurallarına uygun olarak ele alınır. Yazılım bir ilişkilendirme olayı oluşturur ve ilişkilendirme kuralının gerekliliklerini karşılayan bir dizi olay bulduğunda bunu depoya gönderir. Kullanıcı, ilişkilendirme olayını ek analiz için korelatöre göndererek ilişkilendirme kurallarını önceki bir analizin sonuçları tarafından tetiklenecek şekilde uyarlayabilir. İlişkilendirme kuralı çıktıları diğer ilişkilendirme kuralları tarafından kullanılabilir. Örneğin, birkaç küçük uyarı daha büyük bir uyarı oluşturabilir (toplu bir deneme yanılma saldırısı olayını ortaya çıkarmak için birkaç deneme yanılma saldırısı girişimi analiz edilebilir).

Platform, eğilimleri tespit etmek, daha önce tanımlanmamış tehditleri bulmak ve belirli güvenlik unsurları tarafından gözden kaçırılan saldırıları belirlemek için geçmiş verileri kullanır ve tüm bunlar genel tehdit tespitini iyileştirir.

Üçüncü taraf çözümler veya **Kaspersky EndpointDetection and Response** gibi entegre ürünler sensör tarafında algılama gerçekleştirir. Kullanıcılar ürün ayarlarını değiştirerek bu süreci kontrol edebilir ve bu ürünlerin kendi algılama mantıkları aracılığıyla zaten işledikleri olayları ve telemetriyi elde edebilirler.

Çözümün ilişkilendirme motoru platform tarafında tespit özelliğine sahiptir. Platformun güçlü ilişkilendirme motoru sayesinde kullanıcılar uyarlanabilir ilişkilendirme kuralları oluşturabilir. Sürekli olarak genişletilen ve güncellenen ticari olarak erişilebilir üçüncü taraf ürünlerini desteklemek için hazır kurallar ve normalleştirici paketleri de mevcuttur.

Korelatörün çalışma prensibi olay imza analizine dayanır, yani her olay kullanıcı tarafından belirlenen ilişkilendirme kurallarına uygun olarak ele alınır. Yazılım bir ilişkilendirme olayı oluşturur ve ilişkilendirme kuralının gerekliliklerini karşılayan bir dizi olay bulduğunda bunu depoya gönderir.

Operatörlerin güçlü bir sütun odaklı veritabanı kullanarak geçmiş verileri analiz etmesine ve ilişkilendirmesine olanak tanıyarak önceden bilinmeyen tehditleri keşfetmek için tehdit avcılığı.

Kullanıcılar, etiket tabanlı arama işlevini kullanarak tek bir etiketle birleştirilmiş filtreleri, sözlükleri ve kuralları kolayca bulabilirler. Arama sorgusu geçmişinin saklanması, kullanıcının önceki sorgulara kolaylıkla erişmesini sağlar.

Platform, ClickHouse ve Hadoop Dağıtılmış Dosya Sistemi (HDFS) veya yerel diskleri kullanan sıcak ve soğuk depolama seçenekleri sayesinde pahalı depolama donanımları için bütçe aşımı yapmadan verileri uzun süre depolayabilir.

Yöneticiler esnek ayarları kullanarak disk alt sistemindeki alan sorunlarını önleyebilir: olay depolama derinliği, günlere ek olarak disk alanının yüzdesi olarak gigabayt cinsinden ayarlanabilir.

Güvenlik olayı veri depolama

Kaspersky SIEM'in depolama bileşeni, **Kaspersky Unified Monitoring and Analysis Platform'dan** analitik verilere hızlı ve sürekli olarak erişmek amacıyla normalleştirilmiş olayları depolamak için kullanılır.

ClickHouse sürekliliği ve erişim hızını garanti eder. Depolama, bir ClickHouse kümesi aracılığıyla Kaspersky SIEM depolama hizmetine bağlanır. ClickHouse kümelerine soğuk depolama diskleri de eklenebilir.

Kullanıcılar, depolanan olayları belirli bir niteliğe göre gruplandırmak için depolara alan ekleyebilir. Bu, yöneticilerin belirli özelliklerine göre olaylar için farklı depolama süreleri ayarlamasına olanak tanır.

Kaspersky Unified Monitoring and Analysis Platform, veri alımından ödün vermeden disk alanı kullanımını önemli ölçüde azaltmak için veri sıkıştırma işlemini de gerçekleştirir. Kaspersky çözümü tarafından iki alan desteklenir: biri hızlı veri alımı, diğeri ise büyük miktarda verilerin depolanması için.

Platformun iki ayrı bölümü vardır: biri Hadoop Dağıtılmış Dosya Sistemi veya yerel diskler üzerinde gerçekleştirilebilen soğuk depolama için, diğeri ise ClickHouse kullanan operasyonel depolama için. Bu bölümler kullanıcılar için şeffaftır.

Operatörler arşivler arasında gezinmek zorunda kalmadan tek bir arayüzde arama sorguları oluşturabilir ve tüm çabalarını soruşturmaya yoğunlaştırabilirler. Bu, bir yandan mükemmel kullanıcı deneyimini korurken diğer yandan **sistemin sahip olma maliyetini düşürür**. Platform, operatörlerin dağıtılmış depolama kümelerindeki ilgili olayları daha hızlı ve daha kolay bulmasına yardımcı olmak için birden fazla depoda olay aramalarını destekler.

Kuruluşlar, çeşitli kaynaklardan günlükleri güvenli bir şekilde toplayıp depolayarak veri saklama, denetim ve olay incelemesi için yasal gerekliliklerle uyumlu kalabilirler. Ayrıca, merkezi ve yapılandırılmış depolama, şirketlerin gerektiğinde günlükleri alıp analiz etmesini kolaylaştırır.

Kaspersky Next XDR Expert

Kaspersky Next XDR Expert ile oynatma kitapları aracılığıyla daha geniş kapsamlı yanıt yetenekleri mevcuttur.

Daha fazla bilgi

Entegre yanıt yetenekleri

Kaspersky ürünlerini kullanan yerleşik yanıt işlevi, güvenlik verimliliğini artırır. Örneğin, uç nokta müdahale yeteneklerini genişletmek için Kaspersky SIEM, varlıkların ağ izolasyonunu ve önleme kurallarını yönetmek veya uygulamaları ve komut dosyalarını yürütmek için Kaspersky Endpoint Detection and Response ile birleştirilebilir. Bu yanıt eylemleri, Kaspersky Endpoint Security aracısı ile varlıklar üzerinde manuel veya otomatik olarak gerçekleştirilebilir.

Otomatik envanter bilgisi toplama (kurulu yazılım, güvenlik açıkları, ekipman, varlık sahipleri vb.) bilgi güvenliği olaylarını bağlamsallaştırmaya ve olay incelemelerine yardımcı olabilir.

Kaspersky SIEM, düzinelerce kullanıma hazır tehdit verisi akışını (ticari ve genel) destekleyen tam özellikli bir tehdit istihbaratı platformu olan Kaspersky CyberTrace'ten yararlanarak olay zenginleştirmeyi, uzlaşma göstergeleri hakkında bağlamsal bilgilerle gerçek zamanlı olarak otomatik olarak yayınlar.

Kaspersky SIEM'in yapay zeka bileşenleri, altyapıdaki şüpheli etkinliklerin hızlı bir şekilde tespit edilmesini sağlar

Yapay zeka ve makine öğrenimi araçları

Kaspersky, ürünlerimizin tehditleri daha hızlı tespit etme ve tespitleri doğru bir şekilde önceliklendirme konusundaki etkinliğini artırmak için tahmine dayalı algoritmalar, kümeleme teknikleri, sinir ağları, istatistiksel modelleme teknikleri ve uzman algoritmalar kullanır.

İzleme ve müdahale ekipleri, büyük veri ve yapay zeka sistemleri tarafından doğrulanan uyarıları önceliklendirebilir ve potansiyel hasarı önlemeye odaklanabilir. Yapay zeka modülü, geçmiş verileri analiz ederek, gelen uyarıları önceliklendirerek ve varlıklar için yapay zeka tabanlı risk puanları sağlayarak triyaja yardımcı olur. Bu yaklaşım, proaktif aramalar için kullanılabilecek değerli hipotezler üretilmesine yardımcı olur.

Platform, olayları gerçek zamanlı olarak birbirine bağlamak için kullanıcı tanımlı ilişkilendirme kurallarını kullanır. İlişkilendirme modülü, ani trafik artışları veya potansiyel bir olaya işaret eden çoklu hizmet erişimleri gibi anormal etkinlikleri tespit etmek için yapay zeka algoritmaları uygular ve hasar oluşmadan önce erken tespit sağlar.

Kaspersky SIEM, yapay zeka ve büyük veri teknolojileri kullanılarak oluşturulan Kaspersky Threat Intelligence verilerini de içerir. Veritabanı, manuel APT analizi sonuçları, Darknet operasyonel verileri, Kaspersky Security Network'ten alınan bilgiler ve düzenli yeni kötü amaçlı yazılım analizlerinden elde edilen içgörülerle sürekli olarak zenginleştirilmektedir.

Tüm bu teknolojiler, kullanıcıların siber olayların neden olduğu potansiyel zararı en aza indirmelerine ve MTTR ile MTTD'yi artırmalarına yardımcı olur.

Panolar ve raporlarla olağanüstü görselleştirme, eğilimleri, kalıpları ve anormal olayları belirlemek için verileri en kullanışlı biçimlerde sunar.

Göstergelerin kolayca görselleştirilmesi ve görüntülenmesi için özelleştirilebilir widget'lar sayesinde analistler olay önceliklerini belirleyebilir, temel nedenleri tespit edebilir ve tehditlere daha verimli bir şekilde yanıt verebilirken, kuruluşlar da güvenlik operasyonlarının etkinliğini takip edebilir, eğilimleri belirleyebilir ve güvenlik sistemlerinin genel sağlığını değerlendirebilir.

Kullanıcılar olay alanı verilerini sözlüklerin, tabloların, varlıkların ve hesap özniteliklerinin içerikleriyle zenginleştirebilir ve bu verileri arama ve görselleştirme için kullanabilir. Bu, daha bağlamsal veriler içeren panolar ve raporlar oluşturulmasına yardımcı olur.

Bu çözüm, kullanıcıların ayarlanabilen kendi widget'larının yanı sıra **çeşitli widget gruplarına sahip düzenler oluşturmalarına yardımcı olur:**

Temel uyarı ölçütleri

(önem derecesi, öncelik ve durum)

- Etkilenen varlıklar
- Son bildirimler
- En çok uyarı alan veri kaynakları
- Belirli operatörlere atanan uyarılar
- Etkilenen kullanıcılar ve/veya cihazlar
- İlkeye göre uyarılar

Kilit olay göstergeleri

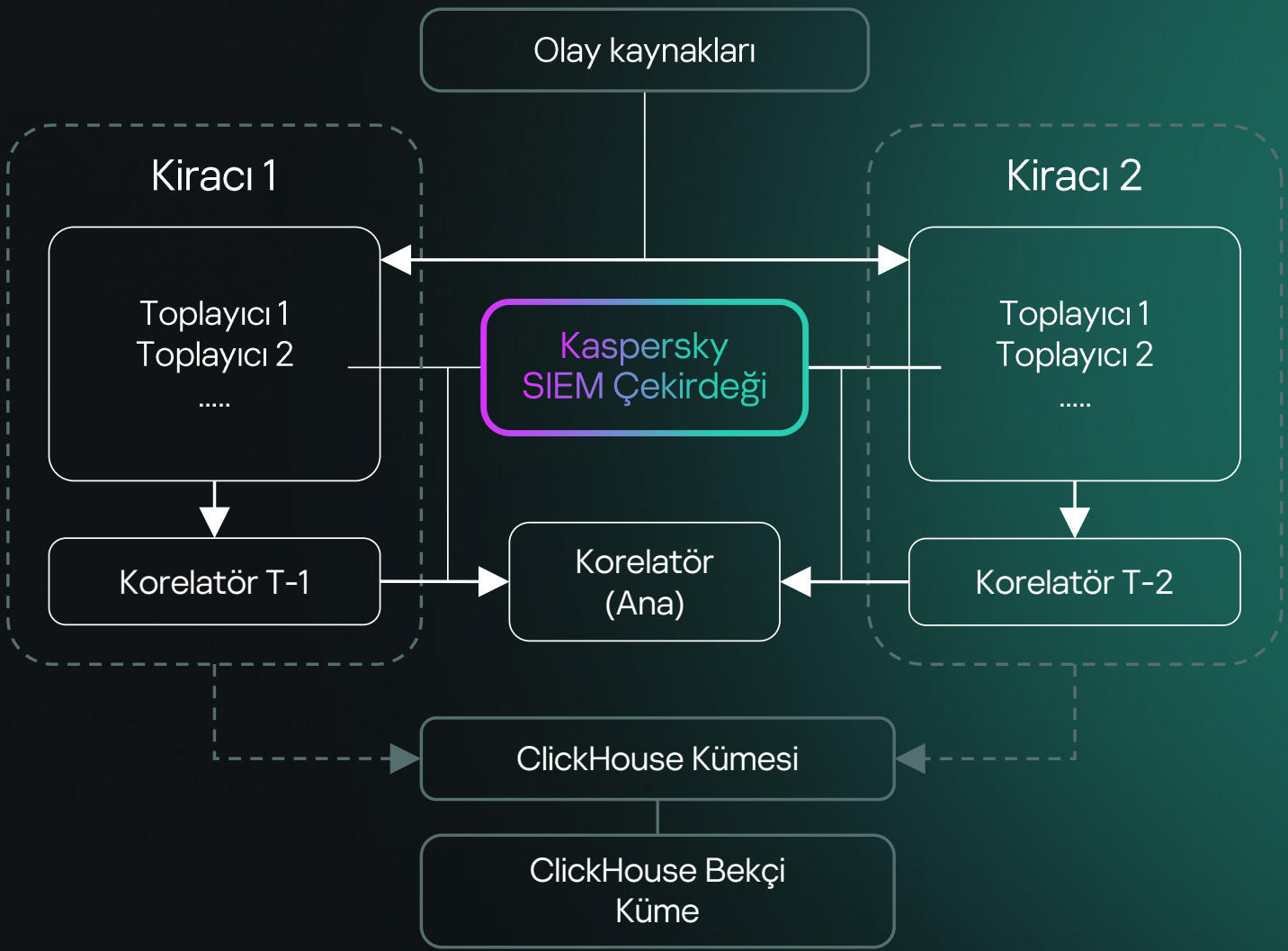
(önem derecesi ve atama)

- Etkilenen cihazlar
- NetFlow trafik hacmine (BytesIn) göre en iyi dahili ve harici IP'ler
- Uzaktan yönetim için üst düğümler (3389, 22 numaralı portlar)
- Dahili portlar için toplam NetFlow baytları
- Etkinlik, kategori, varlık ve kullanıcı sayısına göre en iyi kaynaklar

Çoklu kullanım mimarisi

Kaspersky SIEM tam çoklu kiracılık desteği sunar, yani bir kiracıdaki kullanıcılar başka bir kiracının verilerini (olaylar, uyarılar, vakalar vb.) göremez. Çoklu kullanım modunda, ana kuruluşta dağıtılan Kaspersky SIEM uygulamasının tek bir örneği, şubelerin izole edilmesini sağlar, böylece kendi olaylarını alır ve işlerler.

Sistem ana arayüz üzerinden merkezi olarak yönetilir ve kiracılar yalnızca kendi kaynaklarına, hizmetlerine ve ayarlarına erişimle bağımsız olarak çalışır. Kiracı ile ilgili olaylar ayrı olarak saklanır. Kullanıcılar aynı anda çok sayıda kiracıya erişebilir. Genel yönetici, web arayüzünün farklı bölümlerinde hangi kiracı verilerinin görüntüleneceğini de belirleyebilir.



Platform, etkinlikleri alanlara dağıtmak için filtre tabanlı bir sistem sunuyor. Olaylara kullanıcı erişimi artık alan düzeyinde ayarlanmaktadır. Bu, tek bir kiracı içindeki olaylara erişimin granüler kontrolünü sağlar.

Sistem ana arayüz üzerinden merkezi olarak yönetilirken, kiracılar birbirlerinden bağımsız olarak çalışır ve yalnızca kendi kaynaklarına, hizmetlerine ve ayarlarına erişebilirler. Kiracıların etkinlikleri ayrı olarak saklanır.

Çok çeşitli kullanıma hazır entegrasyonlar

Kaspersky Unified Monitoring and Analysis Platform, ürünlerin gelişmiş verimlilikle koordineli kullanımı için Kaspersky çözümleri ve teknolojileriyle tam olarak entegre edilmiştir. Üçüncü taraf satıcılar, Tehdit İstihbaratı entegrasyonu için tek bir arayüz, uç nokta sensörlerimizi SIEM aracıları olarak kullanma kapasitesi ve çok daha fazlasını içeren kendi ürünlerimizle sorunsuz entegrasyon düzeyimizle rekabet edemez.

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response *

Kaspersky Security Center

Kaspersky Secure Mail Gateway

Kaspersky Web Traffic Security

Kaspersky Threat Lookup

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Automated Security Awareness Platform

ve daha fazlası

Kaspersky Threat Intelligence hizmetlerinin zengin portföyü ile entegrasyon, tehditlerin belirlenmesine ve önceliklendirilmesine yardımcı olur ve yeni saldırılar, tehlike göstergeleri ve saldırgan taktikleri ve teknikleri hakkında bağlamsal bilgilere hızlı erişim sağlar.

* Kaspersky Endpoint Detection and Response Expert, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Next EDR Foundations, Kaspersky Next EDR Optimum, Kaspersky Next EDR Expert ile olası entegrasyonları içerir

Kaspersky SIEM, diğer sistemlerden ve cihazlardan veri (günlük) alma konusunda mükemmeldir. Kaynak ayrıştırma kurallarını ayarlama masrafı olmadan hızlı uygulamayı kolaylaştırmak için platform, Kaspersky ürünleri ve üçüncü taraf ürünleri için çok çeşitli kullanıma hazır entegrasyonlarla birlikte gelir:

Güvenlik alanına göre

- Uç Nokta Koruması (EPP ve EDR çözümleri)
- E-posta ve web trafiği koruması (e-posta koruması, NDR, FW/ NGFW, UTM, IDS)
- Güvenlik Farkındalığı
- Bulut iş yükü (CASB, CWPP)
- Tehdit İstihbaratı (CTI)
- Kimlik Güvenliği (IAM, PAM)
- OT / IoT Güvenliği
- Veri Kaybı Önleme (DLP)

Veri türüne göre

- XML
- Syslog
- CSV
- JSON
- SQL
- CEF
- Öne Çıkan Yönler
- RegExp
- NetFlow v5
- NetFlow v9
- IPFIX

Aktarım türüne göre

- TCP
- UDP
- NetFlow
- sFlow
- NATS JetStream
- Kafka
- HTTP
- SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse, Elasticsearch)
- Dosya
- Diode
- FTP
- NFS
- WMI
- WEC
- ETW (DNS analizleri)
- SNMP
- SNMP Traps
- VMware API
- MS Office 365

Kaspersky Professional Services ekibi veya iş ortakları tarafından, bağlanabilir ürünlerin API'lerini kullanmak da dahil olmak üzere ek entegrasyonlar geliştirilebilir. Desteklenen etkinlik kaynaklarının tam listesini görüntüleyin.

Tam liste

Tedarikçiye göre

- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilon
- Ayehu
- Barracuda Networks
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- Check Point
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- Deep Instinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- F5 BIG-IP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion soft
- Intralinks
- Juniper Networks
- Kemp Technologies
- Kerio
- Lieberman Software
- MariaDB
- Microsoft
- MikroTik
- Minerva Labs
- NetIQ
- NETSCOUT
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto Networks
- Penta Security
- Proofpoint
- Radware
- Recorded Future
- ReversingLabs
- SailPoint
- SentinelOne
- SonicWall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro Trustwave
- VMWare
- Vormetric
- WatchGuard
- Windchill FRACAS
- Zettaset
- Zscaler
- vb.

Kaspersky Premium Support

Kaspersky SIEM için Premium Destek

Kaspersky SIEM için Kaspersky Premium Destek, hem Premium hem de Premium Plus lisanslarla birlikte gelir ve Kaspersky SIEM'inizin sorunsuz çalışmasını sağlamak için her türlü soruna hızlı yanıt ve yüksek kaliteli yardım sağlar

İletişim	Standart destek	Premium lisans	Premium Plus lisansı
Şirket Hesabı (web portalı)	●	●	●
Telefon		●	●
E-posta		●	●

Hizmet			
Kaspersky SIEM için özel ayrıştırıcılar		5	10
Sorunların teşhisi için uzaktan yardım		●	●
Destek taleplerinin öncelikli olarak iletilmesi		Yüksek	En yüksek
Özel yamalama			●
Özel Teknik Hesap Yöneticisi (TAM)			●
TAM durum raporları			Üç aylık rapor

Yanıt süreleri			
Kritik konular	SLA yok	2 saat (7/24)	30 dakika (7/24)
Yüksek düzey sorunlar	SLA yok	6 saat (5/8)	4 saat (7/24)
Orta düzey sorunlar	SLA yok	8 saat (5/8)	6 saat (5/8)
Düşük düzey sorunlar	SLA yok	10 saat (5/8)	8 saat (5/8)

Hızlı yanıt

Daha hızlı ve güvenilir sorun çözümü için talepler katı SLA'lar ile önceliklendirilir

Özel ayrıştırıcılar

Özel ayrıştırıcılar, SIEM'in belirli veri kaynaklarınızdan gelen benzersiz günlük formatlarını işlemesini sağlar

Özel TAM

Premium Plus lisansı ile bir TAM, tüm sorunları yüksek hesap verebilirlikle yönetir

Özel yamalar

Premium Plus lisansı ile belirli sorunlar için tasarlanmış özel düzeltmeler ve yamalar edinin

Neden bizi seçmelisiniz?

Maliyet verimliliği açısından eski SIEM satıcılarından sürekli olarak daha iyi performans gösteren ve her örnekte yüz binlerce EPS'yi işleyebilen yüksek performanslı modüler bir çözümle donanım veya sanallaştırma kurulum gereksinimlerinden %50'ye kadar tasarruf edin ve sahip olma maliyetini azaltın.

Lisanslama seçeneklerimizle esnek kalın. Taşmaları sınırlamak için toplama ve filtrelemeden sonra günlük ortalama EPS akışını izliyoruz ve gerçekleşmeleri durumunda Kaspersky SIEM'e erişimi kısıtlamıyoruz.

Yerleşik yanıt seçenekleriyle hem Kaspersky hem de üçüncü taraf entegrasyonlarının geniş bir yelpazesinden yararlanın. Diğer satıcılar, Tehdit İstihbaratı entegrasyonu için tek bir arayüz, uç nokta sensörlerimizi SIEM aracıları olarak kullanma kapasitesi ve çok daha fazlasını içeren kendi ürünlerimizle sorunsuz entegrasyon düzeyimizle rekabet edemez.

ClickHouse ve Hadoop Dağıtılmış Dosya Sistemi (HDFS) veya yerel diskleri kullanarak sıcak ve soğuk depolama seçenekleriyle uzun bir süre bütçenizi aşmadan düşük maliyetli, tavizsiz bir şekilde yerel olarak veri depolayın ve aynı anda her iki alanda da hızlı bir şekilde arama yapın.

Dünya lideri araştırmacı ve analist ekibimiz tarafından Kaspersky Threat Intelligence Portal üzerinden sağlanan taktiksel, operasyonel ve stratejik Tehdit İstihbaratı ile zenginleştirme sayesinde veri alaka düzeyini artırın, saptama ve önceliklendirmeyi hızlandırın.

Kuruluşların ana altyapısında tek bir SIEM kurulumunun kendi olaylarını alan ve işleyen kullanıcılar için izole SIEM oluşturulmasını sağladığı yerel çoklu kullanım desteği sunan bir MSSP ve büyük kuruluşlara hazır çözümle yerleşik çoklu kullanımdan yararlanın.

Dünya çapındaki kurumlar, siber güvenlik verimliliğini artıran kapsamlı bilgi güvenliği süreçleri geliştirmek için Kaspersky Birleşik İzleme ve Analiz Platformu'na güveniyor.

Daha fazla bilgi

Kaspersky, iOS cihazlarını hedef alan daha önce bilinmeyen kötü amaçlı yazılımları ortaya çıkarmak için kendi SIEM'ini kullandı

Kaspersky Birleşik İzleme ve Analiz Platformunu kullanarak mobil cihazlara ayrılmış kendi kurumsal Wi-Fi ağımızın ağ trafiğini izlerken, birden fazla iOS tabanlı telefondan kaynaklanan şüpheli etkinlik tespit ettik.

Modern iOS cihazlarını içeriden incelemek mümkün olmadığından, söz konusu cihazların çevrimdışı yedeklerini oluşturduk, bunları Mobile Verification Toolkit'in mvt-ios programını kullanarak inceledik ve ele geçirme izlerini keşfettik.

Apple, Kaspersky araştırmacıları tarafından tespit edilen dört sıfırıncı gün güvenlik açığını gidermek için güvenlik güncellemeleri yayınlayarak yanıt verdi:

CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, CVE-2023-41990

Bu güvenlik açıkları iPhone'lar, iPod'lar, iPad'ler, macOS aygıtları, Apple TV'ler ve Apple Watch'lar dahil olmak üzere çok çeşitli Apple ürünlerini etkilemektedir. Kaspersky ayrıca Apple'ı, şirketin daha sonra hafiflettiği bir donanım özelliğinin istismarı hakkında bilgilendirdi.

Neden Kaspersky?

Kaspersky SIEM, 5 Uzmanlık Merkezinin yıllara dayanan bilgi birikimini ve rafine becerilerini bir araya getirir.

Daha fazla bilgi

27

27 yılı aşkın süredir en çok test edilen, en çok ödül alan teknolojilerimizle sizi güvende tutmak için araçlar geliştiriyor ve hizmetler sunuyoruz.

Daha fazla bilgi

Dünya çapında binlerce müşterisi ve iş ortağı olan, **şeffaflık ve bağımsızlık** ilkelerine bağlı küresel bir özel siber güvenlik şirketiyiz.

Daha fazla bilgi

Kaspersky Unified Monitoring and Analysis Platform

Daha fazla bilgi

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın