Extended Detection and Response (XDR) platformu ile endüstriyel işletmelerin kapsamlı güvenliğini sağlayın

Kaspersky Industrial CyberSecurity

kaspersky geleceği yakalayın

Kötü amaçlı yazılım saldırısına uğrayanlar

2024 yılının ilk çeyreğinde, toplam 30 siber güvenlik olayı, etkilenen kuruluşlar veya sorumlu yetkililer tarafından kamuya açık bir şekilde teyit edilmiştir ve bu olayların %64,5'ini imalat sektöründe meydana gelmiştir.

Kaspersky ICS-CERT, Haziran 2022

Daha fazla bilgi edinin

Endüstriyel tehdit ortamı

Endüstriyel altyapıların sahipleri ve operatörleri için yeni gerçeklik, siber aktivistlerin otomasyon sistemlerine artan ilgisi, yüksek yasal gereklilikler, BT-OT yakınsaması ve endüstriyel sektörde siber saldırı çeşitliliğinin artması gibi faktörlerle şekilleniyor (2024'ün ilk çeyreğinde Kaspersky'nin çözümleri endüstriyel otomasyon sistemlerinde 10.865 farklı aileden kötü amaçlı yazılımı engelledi).

Genellikle olumlu olarak değerlendirilen dijital teknolojilerin sayısının artması, BT ve OT ortamları arasındaki boşluğu ortadan kaldırarak OT ortamlarını siber suçlulara karşı daha savunmasız hale getiriyor. ICS ortamına getirilen tek bir flash sürücü bir şirketin temel işini etkileyebilir, yüksek motivasyona sahip bir korsan grubu OT ağlarına girerek büyük hasara yol açabilir ve/veya değerli bilgileri çalabilir. Otomasyon standartlarının genel önerilerden yasal düzenleme gereksinimlerine doğru evrimleşmesi ve en iyi uygulamaları paylaşma ve riskleri yönetme ihtiyacının artması göz önünde bulundurulduğunda, endüstriyel işletmelerin siber güvenliğinin sağlanmasının büyük bir zorluk olduğu görülüyor.

Kaspersky ICS CERT, aşağıdaki sektörler işletmelerinin artan sıklıkla siber saldırılarla karşılaşacağını öngörüyor:

Petrol, Gaz ve Kimya

Bu şirketler için kilit bir rekabet faktörü olan arama, çıkarma, taşıma ve rafinajın dijitalleştirilmesi; IIoT, Dronlar ve Robotların entegre edilmesi, 5G, blok zinciri ve VR çözümlerinin kullanılması anlamına geliyor ve bu da kötü niyetli eylemler için alanı oldukça genişletiyor.

Kritik üretim

Maliyet etkinliğini artırma arayışında olan bu kuruluşlar, en son teknolojileri kullanıyor, bağlanabilirliği artırıyor, buluttan yararlanıyor ve BT-OT yakınsama senaryolarını keşfediyor; tüm bunlar da yepyeni ve sürekli değişen tehditlere maruz kalmayı artırıyor.

Mineraller, Metal ve Maden

Kritik ve ulusal öneme sahip üretim için bir mihenk taşı olan sektör, otomasyon ve dijital teknolojileri devreye sokarken giderleri dengelemek zorundadır. Hem siber aktivistler hem de yüksek potansiyelli saldırganlar çekici bir alan olduğundan, siber güvenlikten ödün vermek mümkün değildir.

Güç, Şebekeler ve Kamu Hizmetleri

Dijital ve gelişmekte olan teknolojiler, halen çoğu enerji tesisinin bel kemiği olan eski altyapı korunurken enerji dönüşümünü sağlamak için hayati önem taşımaktadır. Yine de, ekstra siber güvenlik çabaları gerektiren en büyük riski oluştururlar.

Başta ICS ve SCADA olmak üzere endüstriyel sistemlere yönelik saldırılar yükselişte. Bu arada, günümüzde endüstriyel ortamları hedef alan siber tehditler geleneksel çözümlere karşı dirençli görünmektedir. Bu çerçevede Kaspersky, bu sektörler için kapsamlı bir yaklaşım sunuyor. Web sitemizdeki müşteri başarı hikayelerimizi, tehdit ortamı içgörülerimizi ve senaryoya özel tekliflerimizi keşfedin.

Endüstriyel ve kurumsal siber güvenlik arasındaki örtüşmeler hakkında derin bilgilere ve en yeni güvenlik teknolojilerini sağlayacak kapasiteye sahip, güvenebileceğiniz bir iş ortağı seçmek her zamankinden daha büyük öneme sahiptir.

APT saldırılarının birincil hedefleri aşağıdakileri içerecek:

Kritik altyapı sahipleri ve operatörleri

Petrol ve Gaz, Kimya, Enerji ve Kamu Hizmetleri sektörlerinden stratejik öneme sahip kuruluşlar, operasyonel müdahalelerden kaynaklanan çok daha büyük potansiyel sonuçlarla karşı karşıyadır

Kritik üretim

Tek bir tesisten ülke çapında veya uluslararası ölçeğe kadar, Metal ve Madencilik, Tarım ve küresel imalat sektörlerinden olanlar da dahil olmak üzere bu şirketler, önemli olay maliyetlerinin söz konusu olduğu yüksek riskli faaliyetlerde bulunmaktadır

2024'ün başlarında sanayi kuruluşlarına yönelik APT ve finansal saldırılar hakkında daha fazla bilgi edinin

Daha fazla bilgi edinin

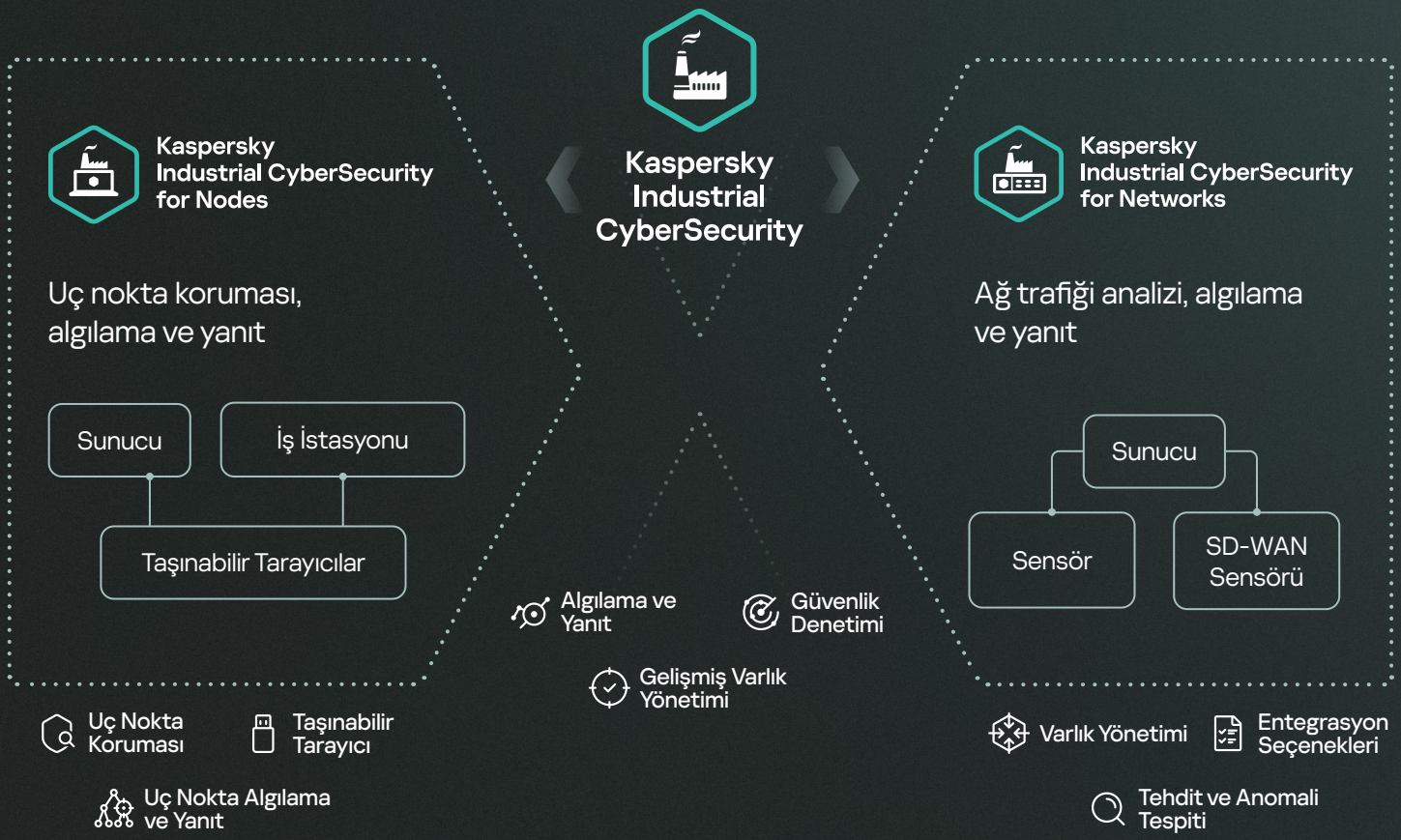
Gelişmiş ICS güvenliği teknolojileri

BT ve OT ortamları arasında, OT'yi siber suçlulardan korumak için kullanılan boşluk giderek daralmaya devam ediyor, bu nedenle kritik altyapıyı korumak için kapsamlı bir kurumsal sınıf tek satıcılı güvenlik çözümü artık Siber-Fiziksel sistemlerin sahipleri ve operatörleri için bir zorunluluk haline geldi. **Kaspersky Industrial CyberSecurity (KICS)**, KICS for Networks ve KICS for Nodes bileşenlerinden oluşan yerel XDR platformu, endüstriyel otomasyon sistemlerini ve ağlarını korur.

KICS for Networks, endüstriyel ağ izleme, saldırı tespiti ve risk yönetimi sağlayan, aynı zamanda güvenlik açıkları ve endüstri standartlarına uygunluk açısından endüstriyel ağ düğümlerinin merkezi denetimini gerçekleştiren bir trafik analizi, algılama ve yanıt ürünüdür. **KICS for Nodes**, OVAL* tabanlı uyumluluk denetimi ile endüstriyel düzeyde uç nokta koruması, algılama ve yanıt sunar. Bu modüler, düşük etkili çözüm Linux, Windows, eski, bağımsız sistemler ve PLC'lerle uyumludur. Taşınabilir Tarayıcı versiyonu, bağımsız makineleri ve yüklenici cihazlarını kurulum gerektirmeden korur.

Bu bileşenler bir araya geldiğinde, merkezi varlık envanteri, risk yönetimi ve denetim sunan KICS XDR platformunu oluşturuyor ve kapsamlı bir olay grafiği, analizler ve daha fazlasına sahip tek bir platform aracılığıyla çeşitli, dağıtılmış altyapılarda güvenlik ölçeklenebilirliği sağlıyor.

KICS XDR platformu, kullanıcıların daha büyük resmi ve daha geniş bağlamı görmesini sağlar: ağ ve uç nokta seviyelerindeki olaylar zinciri, hassas varlık parametreleri, trafik yansıtmanın henüz mevcut olmadığı segmentlerden bile ağ iletişimi ve topoloji haritaları ve daha fazlası.



* Open Vulnerability and Assessment Language (OVAL)

Platform Uygulama Noktaları

OT ve BT ortamlarının birleştirilmesi

DMZ / GTW

BT ortamı

OT ortamı

Kaspersky Industrial CyberSecurity for Nodes

- Operatör iş istasyonu
- SCADA sunucusu
- Mühendislik İş İstasyonu
- ICS Ağ Geçidi

Ağ ekipmanı

SPAN

Kaspersky Industrial CyberSecurity for Networks

- Bölme Kontrol Birimi (BCU)
- Akıllı Elektronik Cihaz (IED)
- Programlanabilir Mantık Denetleyicileri (PLC)
- Aktarma koruması ve güvenlik önlemli sistem (SIS)
- Yalıtılmış Düğümler (KICS Taşınabilir Tarayıcı ile manuel denetleme)

Erken anomali algılama ve tahmine dayalı analiz

Kaspersky Anomali Algılama için Makine Öğrenimi (Kaspersky MLAD), geniş kapsamlı telemetri verilerini aynı anda izlemek için bir sinir ağı kullanan yenilikçi bir sistemdir. Ekipman arızalarını ve insan hatalarını algılayarak hata ve kazaları önlemeye yardımcı olur, tipik olmayan çalışan eylemlerini veya ekipman işlemlerini özelleştirilmiş bir saldırı veya sabotaj işareti olarak belirler ve anomali algılama ile ekipman koşulu ve yaşam döngüsünün tahmine dayalı analizini birleştirir.

Daha fazla bilgi edinin

Fiziksel Düzey

Kaspersky ürünleri tarafından korunmaktadır

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Endüstriyel ağ izleme ve trafik analizi çözümü. Tescilli endüstriyel protokollerin Derin Paket İncelemesini (DPI) etkinleştirir. Yazılım veya sanal cihaz olarak gönderilir.

KICS for Networks ICS'deki anomalileri ve izinsiz girişleri erken aşamada belirler, saldırının ağ üzerinde ve düğümlerde nasıl geliştiğini gösterir (EDR ölüm zinciri ve telemetri) ve endüstriyel işlemler üzerindeki olumsuz etkileri önlemek için gerekli eylemlerin gerçekleştirilmesini sağlar.

Varlık yönetimi

Varlık keşfi
Güvenlik açığı veritabanı, risk önceliklendirme ve güvenli aktif yoklama ile varlıklarınız hakkında bilgi edinin

Ağ görünürlüğü
En üst düzeyde görünürlük için trafiği izleyin, topoloji haritaları oluşturun ve zaman içinde ağ duruşunu izleyin

Trafik analiz araç seti
Ağ oturumlarını takip ve analiz ederek ayrıntılı trafik verilerinin dışa aktarılmasını ve depolanmasını sağlar

Avantajları

- Endüstriyel uygulamalar ve protokoller için uzmanlaştırılmıştır. Çok çeşitli OT protokolleri, cihazları ve ağ saldırıları için kullanıma hazır destek + harici projelerden içe aktarmaya izin verir
- Güvenlik denetimi yapılandırması için önceden ayarlanmış kurallar
- Kullanıcı dostu arayüz ve özelleştirilebilir raporlar
- Dağıtılmış altyapı genelinde eksiksiz risk farkındalığı
- Birden fazla kaynaktan gelen trafik örneklerini alır: kendi ağ sensörleri, SD-WAN sensörleri, uç nokta sensörleri ve taşınabilir problar

Ekosistem ve entegrasyonlar

Ekosistem
Aşağıdaki çözümlerle entegrasyon ve birleşik çapraz ürün siber güvenlik yaklaşımımız sayesinde Kaspersky ekosisteminin kapsamlı özelliklerinden yararlanın:

- Kaspersky Next XDR Expert
Daha fazla bilgi alın

- Kaspersky IoT Secure Gateway (KISG)
Daha fazla bilgi alın

- Kaspersky Machine Learning for Anomaly Detection (MLAD)
Daha fazla bilgi alın

- Kaspersky Software-Defined Wide Area Network (SD-WAN)
Daha fazla bilgi alın

Ekosistemin tüm unsurlarını tek bir konsol üzerinden yönetin

Üçüncü taraf entegrasyonları
Çok sayıda harici güvenlik aracı ve platformu ile sorunsuz uyumluluğun keyfini çıkarın

Tehdit ve anomali tespiti

Saldırı tespiti
İmza tabanlı tespit ve kaba kuvvet veya tarama girişimlerini tespit eden istatistiksel bir motor

Ağ bütünlüğü kontrolü
Sistem normal ağ etkileşimlerini öğrenir ve her sapmada alarm verir

Anomali tespiti
Temel paket ve protokol seviyesi anormalliklerini tespit eder. MLAD ile geliştirilebilir

Endüstriyel protokollerin DPI'sı
Süreç ve komuta kontrolünü destekler ve telemetri verilerini verimli bir şekilde izler

Olay korelasyonu
Güvenlik olaylarını MITRE sınıflandırması ve tek bir ölüm zinciri ile ilişkilendirir

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

Endüstri seviyesi, test edilmiş ve belgelenmiş Uç Nokta Koruma, Algılama ve Yanıt Linux, Windows ve bağımsız sistemler için düşük etkili, uyumlu ve kararlı çözüm.

KICS for Nodes günümüzün, dijital, yönetimli ve dağıtımlı otomasyon sistemlerindeki her bir uç noktayı korur. Çözüm, bir olayın iş istasyonlarında, sunucularda, ağ geçitlerinde ve diğer uç noktalarındaki ilerlemesinin net ve ayrıntılı görsel temsilini oluşturarak telemetri bilgilerini toplar, böylece bir olayla tam olarak ilgilenildiğine ve tekrar olmayacağına dair otomasyon sistem yöneticilerine güvence verir.

Uç nokta koruması

Gerçek zamanlı tehdit önleme
Saldırıları önlemek ve dosyaları korumak için çıkarılabilir sürücüler ve kritik alanlar için özel ve isteğe bağlı taramalar

Yerel etkinlik kontrolü
Cihaz ve Wi-Fi kontrol özellikleri. Tam yerel faaliyet farkındalığı için PLC proje bütünlüğünün sağlanması

Ağ etkinliği kontrolü
Ana bilgisayar güvenlik duvarlarını yönetin ve ağ oturumlarını engelleyerek ağ tehditlerine karşı koruma sağlayın

Sistem izleme
İşletim sisteminin güvenliğini sağlamak için dosya bütünlüğünü doğrulayın, kayıt defteri erişimini izleyin, sistem günlüklerindeki tehditleri tespit edin

EDR (Uç nokta algılama ve müdahale)

Algılama
Tehlike Göstergeleri (IoC'ler) için taramalar, kapsamlı izleme ve raporlama özellikleri

Yanıt
Yürütmeyi önleme, dosyaları karantinaya alma/silme, işlemleri başlatma/sonlandırma, ağları izole etme ve daha fazlası

Windows Düğümleri
Taşınabilir Tarayıcı
Linux Düğümleri
Denetim Aracısı

Taşınabilir tarayıcı

Kötü amaçlı yazılım tarayıcısı
Bağımsız ekipmanların ve endüstriyel alana getirilen tüm bilgisayarların kötü amaçlı yazılımdan koruma taramaları

OVAL taraması
Manuel güvenlik açığı ve uyumluluk taramaları ile bağımsız makinelerde siber güvenlik politikasını uygulayın

Paket yakalama
İzole edilmiş altyapılarda bile üstün farkındalığın kilidini açmak için ağ trafiğini yakalayın ve analiz edin

Temel varlık envanteri
Sıfır ayak izi çözümünü kullanarak donanım ve yazılım hakkında kapsamlı veri toplayın

Avantajları

- Korunan cihazlar üzerinde düşük etki, ayarlanabilir kaynak tüketimi
- Eski işletim sistemi ve endüstriyel otomasyon satıcıları ile uyumluluk
- Temel güvenlik yapılandırmasının yanı sıra ana bilgisayarlarınızı her türlü tehditten korumak için gelişmiş seçenekler
- Modüler dağıtım ve müdahaleci olmayan ayarlar
- PLC desteği: Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4; Schneider Electric Modicon M340, M580; CODESYS V3 cihazları; Fastwel CPM723-01
- Esnek lisanslama seçenekleri, 1 aydan 5 yıla kadar
- En popüler ICS için doğrulanmış ve verimli yapılandırma ön ayarları

Ağ Geçidi
Historian sunucusu
SCADA sunucusu
Operatör iş istasyonu
Gömülü sistemler
Sistem yönetimi iş istasyonu
Mühendislik iş istasyonu

KICS Platformu ve ötesi

Kuruluşunuzun endüstriyel ve kurumsal segmentleri arasında birleştirilmiş siber güvenlik

Native OT XDR

Kaspersky Industrial Cybersecurity, KICS for Networks ve KICS for Nodes'un temel bileşenleri, ekosistemimiz içinde sorunsuz bir şekilde birlikte çalışarak bütünleşik ve uyumlu bir deneyim sağlamak üzere özel olarak tasarlanmıştır. Birlikte satın alındıklarında, ek değerli çapraz ürün işlevselliği sunan yerel bir XDR Platformunu meydana getirirler.

Gelişmiş varlık yönetimi

Uç nokta donanım envanteri
Altyapınızdaki tüm bağlı cihazlara yönelik kapsamlı görünürlük, doğru varlık takibi sağlar ve güvenlik yönetimini geliştirir

Uygulamalar, kullanıcılar ve yamalar envanteri
Ortamınızdaki yazılım dağıtımları, kullanıcı erişimi ve yama durumu hakkında ayrıntılı bilgiler. Doğru yönetim için zenginleştirilmiş veriler ve sayıları azaltılmış potansiyel güvenlik açıkları

Uç nokta trafiği izleme
Olağandışı kalıpları veya potansiyel tehditleri hızlı bir şekilde tespit etmek için her uç noktadaki veri akışlarının sürekli izlenmesi ve şüpheli faaliyetlere anında yanıt verilmesi

Güvenlik denetimi

Güvenlik açığı taramasıGüvenlik zayıflıklarını değerlendirmek, risk farkındalığını artırmak, zamanında müdahale sağlamak ve genel olarak güvenlik pozisyonunuzu güçlendirmek için varlıklarınızı kapsamlı bir şekilde tarayın

Uyumluluk denetimiOVAL ve XCCDF* endüstri standartlarıyla uyumluluk için aracı tabanlı ve aracısız denetim. Tamamen işlevsel bir editör, merkezi rapor veritabanı, düğüm kimlik bilgileri için korumalı kasa ve daha fazlası

Yapılandırma kontrolü Güvenli varlık yapılandırmalarını sağlamak, güvenlik riskleri için değişiklikleri izlemek ve donanım ve yazılım varlıkları için temel bütünlüğü korumak

Algılama ve yanıt

Algılama Tek bir öldürme zinciri görünümü ile ana bilgisayar-ağ olayları korelasyonu yoluyla gelişmiş ve kolaylaştırılmış tehdit tanımlama. Olaylara ilişkin daha derin içgörüler için ağ uyarı verilerinin zenginleştirilmesi

Yanıt Yürütme önleme, ana bilgisayar izolasyonu ve dosya karantinası yoluyla güçlü tehdit azaltma. Sorunsuz güvenlik duvarı entegrasyonları, güvenlik olaylarına hızlı ve etkili bir şekilde yanıt verme yeteneğinizi daha da geliştirir

Open OT XDR

EDR çözümlerinizin işlevselliğini bir korelasyon motoru, otomatik yanıtlar ve üçüncü taraf bağlayıcılarla genişletin - KICS Platformunuzu Kaspersky XDR Core çözümü ile güçlendirerek şunların kilidini açın:

- Bilgi güvenliği olaylarının kapsamlı izlenmesi ve ilişkilendirilmesi (SIEM), çeşitli sistemlerle entegrasyon
- Tehdit İstihbaratı zenginleştirme ve yönetimi

Single IT-OT XDR

Ötesine geçin ve üst düzey BT-OT yakınsamasını kucaklayın. KICS Platformunuzu Kaspersky Next XDR Expert paketimizle birleştirin - Kaspersky'nin sınıfının en iyisi uç nokta koruma işlevinden yararlanın ve aşağıdaki özelliklerin avantajlarından yararlanın:

- Kaspersky Single Management Platform ile tek bir soruşturma grafiği, işlem kılavuzları ve olay yönetimi
- BT altyapısı için kompleks koruma (IT XDR)

XDR Industrial

Kaspersky Industrial CyberSecurity

Daha fazla bilgi edinin

Kaspersky Single Management Platform

XDR Corporate

Kaspersky Next XDR Expert

Daha fazla bilgi edinin

* Extensible Configuration Checklist Description Format (XCCDF)

27 yıllık birinci sınıf deneyim ve petabaytlarca tehdit verisi

ICS CERT

ICS CERT — kendine ait uluslararası OT/IoT güvenlik araştırma bölümü

BT/OT güvenliği sektöründe çeşitli ödüller ve başarılarla kanıtlanmış uzmanlık

Otomasyon sağlayıcılarının çözümleriyle 200'ün üzerinde uyumluluk sertifikası

Kanıtlanmış teknoloji etkinliği, standartlar ve gereksinimlerle uyumluluk

Dünyanın her yerinden müşteriler

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın