Kapsamlı endüstriyel kurumsal güvenlik için bir XDR platformu

# Kaspersky Endüstriyel Siber Güvenlik

kaspersky GELECEĞİ YAKALAYIN

## Kötü amaçlı yazılım saldırısına uğrayanlar

2023 yılının başından itibaren ICS ile ilgili bilgisayarların yaklaşık %35'i kötü amaçlı yazılım saldırısına uğradı; bu önceki yıla göre %5 daha az seviyede.

Kaspersky ICS CERT, Ekim 2023

Daha fazla bilgi edinin

# ICS ve endüstriyel kuruluşların karşılaştığı siber tehditler

Endüstriyel altyapı sahipleri ve operatörleri için yeni gerçeklik, hacktivistlerin otomasyon sistemleri, yüksek düzenleme gereksinimleri, BT-OT birleşmesi ve endüstriyel sektördeki siber saldırı çeşitliliğindeki artış (Kaspersky ICS CERT istatistiklerine göre H2 2022'ye kıyasla H1 2023'te neredeyse %50 artış görüldü) tarafından şekillendiriliyor.

Genellikle olumlu olarak değerlendirilen dijital teknolojilerin yaygınlaşması, 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 Kimyasal

Bu kuruluşların kontrol ettiği veri ve sistemlerin yüksek değeri, operasyonları kesintiye uğratmak veya fiyatlar üzerinde ayarlama yapmak isteyen fidye yazılımları ve kötü amaçlı aktörler için bu kuruluşları çekici bir hedef haline getirir.

### Yüksek Profilli Endüstriyel Üretim

Bu kuruluşlar kritik toplumsal roller oynar ve finansal kazanç için kötüye kullanılarak büyük ekonomik hasara ve itibar kaybına neden olabilecek değerli verilere sahiptir.

### Mineraller, Metal ve Maden

Mineraller, metal ve maden endüstrisi değerli kaynakları, finansal etkisi ve birbirine bağlı tedarik zincirleri nedeniyle hedeflenir.

### Güç, Şebekeler ve Kamu Hizmetleri

Güç, şebekeler ve kamu hizmetlerinin günlük hayatımızdaki temel önemi, kaos oluşturmayı veya bunları kendi etkisi altına almayı hedefleyen saldırıların başlıca nedenidir.

## APT saldırılarının birincil hedefleri aşağıdakileri içerecek:

### Kritik altyapı sahipleri ve operatörleri

Stratejik öneme sahip kamu veya genel işletmeler operasyonel arabirimden önemli ölçüde büyük olası sonuçlarla karşılaşıyor

### Yüksek profilli endüstri oyuncuları

Tek bir tesisten ulusal veya uluslararası ölçeğe kadar, bu şirketler önemli olay maliyetlerine sahip yüksek riskli operasyonlara sahiptir

Üretim ve iş süreci kararlılığı ve değerli varlıkların korunması, endüstriyel kuruluşların ve kritik altyapı tesislerinin sürdürülebilir gelişimiyle doğrudan ilişkilidir. Başta ICS ve SCADA olmak üzere endüstriyel sistemlere yönelik saldırılar yükselişte. Bununla birlikte, endüstriyel ortamları hedefleyen modern siber saldırılar geleneksel çözümlerden etkilenmiyor gibi görünüyor.

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.

Endüstriyel kuruluşlara karşı saldırıların genel TTP'leri hakkında daha fazla bilgi edinin

Daha fazla bilgi edinin

KICS XDR Platformu kullanıcıların daha büyük resmi ve daha geniş bağlamı görmesini sağlar: ağ ve uç nokta seviyesindeki olaylar zinciri, hassas netlikte varlık parametreleri, trafik yansıtmalarının henüz kullanılamadığı segmentlerle bile ağ iletişimi ve topoloji haritaları ve daha fazlası.

### Uç nokta sensörü

- Koruma Durumu
- Güvenlik Denetimi
- Ağ İletişimleri
- Ana Bilgisayar Telemetri Gönderimi
- Ekipman İzleme
- Olay Müdahalesi

# Gelişmiş ICS güvenliği teknolojileri

Kaspersky Industrial CyberSecurity (KICS) endüstriyel kuruluşlar için kritik OT ekipmanı, varlıkları ve ağlarını siber ortamda başlatılan tehditlerden korumak için özel olarak tasarlanmış ve sertifikalı bir yerel Genişletilmiş Algılama ve Müdahale (XDR) Platformudur. Platform, her düzeyde temel Endüstriyel Otomasyon ve Kontrol Sistemi bileşenlerinin güvenliğini sağlayan tümleştirilmiş teknolojilerden oluşur. KICS for Nodes uyumluluk denetim ve uç nokta sensör işlevselliğine sahip uç nokta koruma, algılama ve yanıt yazılımıdır. KICS for Networks ürünü OT ağ trafik analizi, algılaması ve yanıtı için tasarlanmıştır. OT Güvenlik Operasyonlarını yüksek hacimli büyük, çeşitli ve coğrafi olarak dağıtılmış endüstriyel altyapılara ölçeklendirmek için gerekli olan site düzeyi merkezileştirilmiş yönetim işlevi platformla tümleşiktir.

Platform bileşenleri arasındaki sorunsuz entegrasyon birden fazla coğrafi alana dağılmış OT ağlarının ve otomasyon sistemlerinin tam görünürlüğünü sağlayarak, iyileştirilmiş müşteri deneyimi, durumsal farkındalık ve kurulum esnekliği sunar. Genişletilmiş Algılama ve Yanıt ile KICS Platformu BT-OT birleştirmesi sağlar ve çeşitli tek satıcı avantajları sunar.

**Kaspersky Industrial CyberSecurity for Nodes**

EDR ile geliştirilmiş
Uç Nokta Koruması

- Sunucu
- İş İstasyonu
- Taşınabilir Tarayıcılar

**Kaspersky Endüstriyel Siber Güvenlik**

- Birleştirilmiş Konsol
- Yerel Tümleştirme
- Ürünler Arası Senaryolar
- Genel Saldırı Yapısı
- Risk ve Varlık Yönetimi

**Kaspersky Industrial CyberSecurity for Networks**

Endüstriyel Cihazları
Ağ Tehditlerinden Koruma

- Sunucu
- Sensör

Yanıt Önlemleri

- Ana bilgisayar izolasyonu
- Yürütme Önleme
- Karantina

# Platform Uygulama Noktaları

## OT ve BT ortamlarının birleştirilmesi

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

BT ortamı

OT ortamı

DMZ / GTW

Operatör iş istasyonu

SCADA sunucusu

Mühendislik İş İstasyonu

ICS Ağ Geçidi

Ağ ekipmanı

SPAN

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 İçin 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.

## Fiziksel Düzey

Daha fazla bilgi edinin

Kaspersky ürünleri tarafından korunmaktadır

Kaspersky Industrial CyberSecurity for Networks

# KICS for Networks

Yazılım veya sanal cihaz olarak gönderilen özel protokol düzeyi endüstriyel ağ izleme ve trafik analizi çözümü.

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.

Çözüm, olayları önlemek için riskleri algılamaya ve güvenlik açıkları ve ağ bağlantılarından veriler ve çeşitli varlıkların rolü ile riskeri derecelendirmeye yardımcı olur.

## Yararları

### Varlık Envanteri

Pasif ve aktif veri toplama yöntemlerini kullanan otomatik varlık envanteri ve veri toplama

### Ağ Envanteri ve Görselleştirme

- Ağ iletişimi haritası
- Ağ topolojisi diyagramı

### Güvenlik Açığı ve Risk Değerlendirmesi

- OT'ye özgü güvenlik açığı ve risk yönetimi
- Otomatik puanlama ve önceliklendirme
- Risk düzeltme önerileri

### Ağ Anomali Algılama

Taban çizgisi sapma izleme ile kötü amaçlı ve şüpheli ağ etkinliği algılama sayesinde ağ bütünlük kontrolü

### OT İşlem Kontrolü ve Derinlemesine Paket İncelemesi (DPI)

- Endüstriyel yük veri ayıklama
- Gerçek zamanlı işlem kontrolü
- Endüstriyel komut kontrolü
- Kaspersky MLAD tarafından gelişmiş OT işlem izleme

### Tümleştirme ve Veri Değişimi

- Merkezileştirilmiş bilgiler
- Kaspersky ve üçüncü taraf veya Müşteri sistemlerinde tümleştirme (IEC 104, OPC, CEF, Syslog, API tabanlı konnektörler)

## Merkezileştirilmiş uyumluluk endüstriyel ağ düğümlerinin denetlenmesi

KICS for Networks ağ donanımı ve uç noktalarının zayıf noktalar ve OVAL* ve XCCDF** endüstri standartlarıyla uyumluluk için aracı tabanlı (KICS for Nodes aracılığıyla) ve aracısız denetimi dahil merkezileştirilmiş endüstriyel ağ düğümü denetimi sunar.

- Windows, Linux düğümleri, ağ cihazları için otomatik merkezileştirilmiş güvenlik denetimi
- Uyumluluk denetimi. Uyumluluk denetimleri ve parametreler için tam olarak işlevsel düzenleyici
- Tüm raporlar ve varlık verileri tek bir yerden kullanılabilir – KICS for Networks varlık tabanı
- Düğüm kimlik bilgileri için korumalı kasa
- Tüm üçüncü taraf veya özel OVAL veritabanları desteklenir
- ICS CERT tarafından yerleşik SCADA güvenlik açıkları veritabanı

* Open Vulnerability and Assessment Language (OVAL)
** Extensible Configuration Checklist Description Format (XCCDF)

# Kaspersky Industrial CyberSecurity for Nodes

# KICS for Nodes

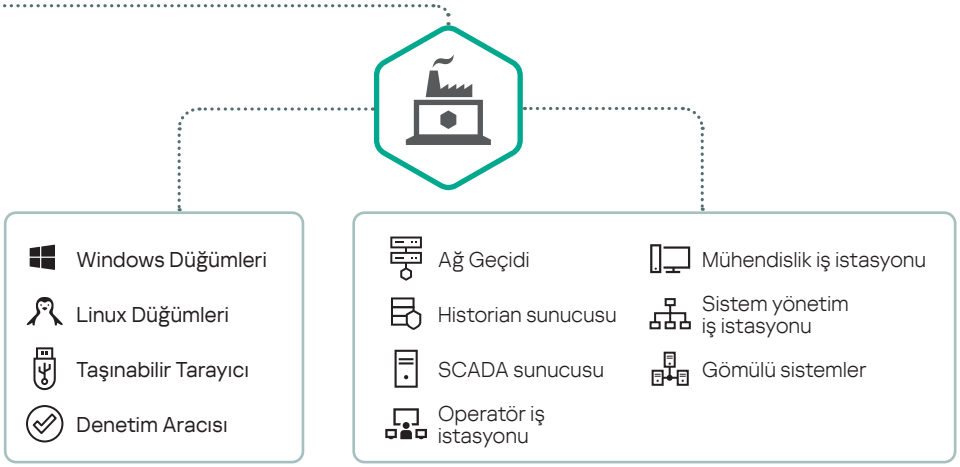
Endüstri seviyesi, test edilmiş ve belgelenmiş Uç Nokta Koruma, Algılama ve Yanıt Linux, Windows ve bağımsız sistemler için düşük etkili, uyumlu ve kararlı çözüm.

KICS for Nodes modern, 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.

**KICS for Nodes Portable Scanner** güvenlik yazılımının yüklenemeyeceği bağımsız makine, otomasyon sistemleri ya da ekipmanlarda siber güvenlik politikasını zorunlu kılar. Düşük operasyonel ayak izi sayesinde mevcut güvenlik çözümlerinin çalışmasını engellemez.

- Tek başına altyapı için bile en iyi durumsal farkındalığı ve OT görünürlüğünü sağlayan yükleme gerektirmeyen çözüm.
- Bakım pencerelerinde birden fazla makinede aynı anda isteğe bağlı taramalar yapmanıza olanak tanır ve kolay anlaşılan raporlar sağlar.
- Üçüncü taraf yüklenicilerin bilgisayarları dahil bir OT sitesine erişen ekipman üzerinde kötü amaçlı yazılım koruması uyumluluk denetimleri gerçekleştirir.

- Cihaz Kontrolü
- Dosya Bütünlüğü Kontrolü
- PLC Bütünlüğü Kontrolü
- Anti-Cryptor
- Açık Önleme
- Ağ Tehdit Engelleme
- Windows Günlük denetleyicisi
- Wi-Fi Kontrolü
- Güvenlik Duvarı Yönetimi
- Kayıt Defteri İzleyicisi
- Güvenlik Denetimi
- EDR Aracısı
- Uç Nokta Sensörü
  (KICS for Networks ile Tümleştirme)




## Yararları

### Düşük etki

- En iyi sistem performansı için korunan cihazlarda düşük etki
- Yükleme, güncelleme veya yükseltme için yeniden başlatma gerekmez
- Yalnızca algılama modu kullanılabilir
- Ayarlanabilir sistem kaynağı kullanımı

### Uyumluluk

- Windows XP SP2 ve Windows Server 2003 SP1'den itibaren eski işletim sistemi desteği
- Endüstriyel otomasyon sağlayıcılarıyla uyumluluk
- Yükleme gerektirmeyen seçenek olarak Taşınabilir Tarayıcı

### Genişletilmiş koruma

- Kötü amaçlı yazılımlar, fidye yazılımları ve güvenlik açıklarına karşı koruma
- Günlük analizi
- Güvenlik duvarı kontrolü
- Yerleşik ICS EDR teknolojisi
- Hava boşluklu veritabanı güncellemeleri

### Modüler kurulum

- OT için tasarlanmış esnek seçenekler ve güvenli, müdahaleci olmayan ayarlar
- Modüler mimari yalnızca gerekli koruyucu bileşenlerin seçilmesine olanak sağlar

### PLC desteği

- Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4
- Schneider Electric Modicon M340, M580
- CODESYS V3 tabanlı cihazlar
- Fastwel CPM723-01

### Denetleyin

- OVAL açık standart tabanlı kapsamlı güvenlik ve uyumluluk denetimi

## Kaspersky XDR etkililik faktörleri

**Bağlamsal Anlayış** benzersiz özellikler, gereksinimler, özelleştirilmiş sistemler, protokoller ve operasyonel konuları içerir

**ICS ile Tümleştirme** endüstriyel ağ trafiği ve sistem davranışının kapsamlı görünürlüğünü ve analizini sağlar

**OT'ye Özgü Tehdit İstihbaratı** Kaspersky'nin endüstriyel ortam tehdit koruma alanındaki uzmanlığından yararlanır

**Özelleştirme ve yapılandırma** çözümü çeşitli risk toleransı, ağ mimarisi ve yasal düzenleme uyumluluk ihtiyaçlarına göre uyarlamanızı sağlar

Zamanında güncellemeler ve yamalar dahil satıcı desteği ve işbirliğinden en iyi şekilde yararlanmanız için **tek satıcı**

# Kuruluşunuzun endüstriyel ve kurumsal segmentleri arasında birleştirilmiş siber güvenlik

Başta ICS ve SCADA olmak üzere endüstriyel sistemlere yönelik saldırılar yükselişte. Endüstriyel ve kurumsal siber güvenlik arasındaki örtüşmeler hakkında derin bilgilere ve en yeni endüstriyel ve kurumsal siber güvenlik teknolojilerini sağlayacak kapasiteye sahip, güvenebileceğiniz bir iş ortağı seçmek her zamankinden daha büyük öneme sahiptir.

Kaspersky XDR güvenli, tehditlerden arınmış bir çalışma ortamı oluşturmak için mükemmel araçtır. Çeşitli güvenlik protokolleriyle uyumluluğu, güvenli bir siber alan oluşturmayı kolaylaştırarak işletmeniz için endüstriye özgü seçenekler sunar, büyük ve küçük tüm tehditlere karşı korur. Kaspersky XDR'nin tümleştirme seçenekleri tehditlerin birleştirilmiş, geniş kapsamlı bir görünümünü sağlayarak güvenlik ekibinize işletmenizi güncel ve olası tüm tehditlere karşı korumak için ihtiyaç duydukları tüm araçları ve verileri sunar.

Daha fazla bilgi edinin

**BT-OT birleştirme**
Kaspersky Hybrid XDR ile

26 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 satıcılarının çözümleriyle birlikte çalışabilirliğe sahip 100'den fazla sertifika

Kanıtlanmış teknoloji etkinliği, standartlar ve gereksinimlerle uyumluluk

Dünyanın her yeniden müşteriler

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

# Kaspersky Endüstriyel Siber Güvenlik

## Kaspersky Industrial CyberSecurity for Nodes

## Kaspersky Industrial CyberSecurity for Networks

**Daha fazla bilgi edinin**

**www.kaspersky.com.tr**



#kaspersky
#geleceğiyakalayın