Endüstriyel Kurumların sürdürülebilirliği ve dijital dönüşümü için güvenlik platformu

Kaspersky Endüstriyel Siber Güvenlik Platformu

kaspersky GELECEĞİ YAKALAYIN

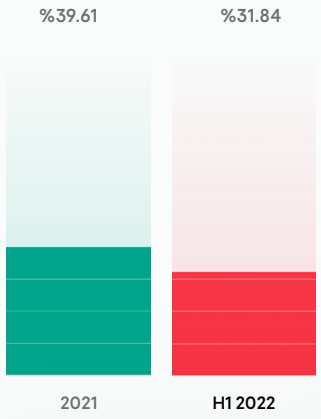
Kötü amaçlı yazılım saldırısına uğrayanlar

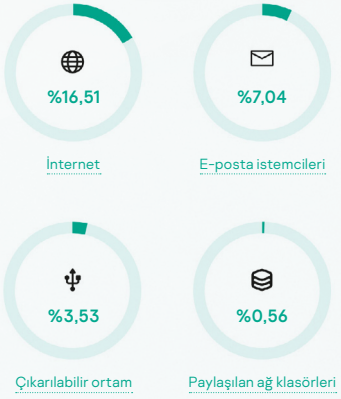
2022 yılının başından itibaren ICS ile ilgili bilgisayarların neredeyse %30'una yakını kötü amaçlı yazılım saldırısına uğradı; bu önceki yıla göre %10 daha az seviyede

Kaspersky ICS-CERT, Haziran 2022

Daha fazla bilgi edinin

2022 yılının başından itibaren ICS bilgisayarlarında engellenen kötü amaçlı nesne yüzdesi





Endüstriyel kurumlar BT ve OT (operasyonel teknoloji) altyapılarının siber güvenliğine farklı şekilde yaklaşır. Birçok şirketin kurumsal ağlarında zaten olgunlaşmış Algılama ve Yanıt önlemleri bulunuyor; ancak iş operasyonel teknolojiye (OT) geldiğinde bunlar genellikle modası geçmiş ayrı ortamlar yaklaşımına güveniyorlar. Endüstriyel şirketler giderek artan şekilde "dijital" hale geliyor, akıllı teknolojilere, yeni otomasyon sistemlerine ve dijital dönüşümün benimsenmesine giderek daha fazla yatırım yapıyor. Bu aslında BT ve OT ortamları arasında siber tehditlerin endüstriyel otomasyon ve kontrol sistemlerine erişebilmelerini önlemek için kullanılan geleneksel boşluğu ortadan kaldırıyor.

Hedef olabilirsiniz ama kurban olmayın

Kazara meydana gelen ayrı ortamların ihlali ya da kötü amaçlı yazılım bulaşmasının kurbanı olmak için bir hedef olmanız gerekmez. Tek bir flaş sürücü, cep telefonu, kimlik avı e-posta mesajı ya da ICS ortamına getirilmiş bir fidye yazılımı bir şirketin temel işleyişini ciddi şekilde etkileyebilir. Aynı zamanda, motive olmuş bir bilgisayar korsanı grubu operasyonel teknoloji (OT) ağlarına girebilir ve ekipmanlarda, işlemlerde, üründe, güvenlik ve kalitede ciddi hasara neden olabilir veya değerli bilgileri çalabilir.

Operasyonel Teknoloji (OT) için temel siber güvenlik

Bağımsız ve bağlı sistemler için

uç nokta koruması. Güvenli ve test edilmiş bir çözüm güvenlik politikalarını zorunlu kılmaya, uyumluluğu desteklemeye, güvenlik denetimleri gerçekleştirmeye, envanteri yönetmeye, yamalama görevleri gerçekleştirmeye ve uç nokta sensörü olarak hassas netlikte telemetri bilgilerini toplamaya yardımcı olabilir

İletişim görünürlüğü,

tehdit algılama ve varlık yönetimi için ağ koruması. Ağ Trafik Analizi ve İzinsiz Giriş Algılama güvenlik duvarı ayarlarının, ağ segmentasyonunun ve ağ kullanım uyumluluğunun etkinliğini kontrol eder ve güvenli manüel yanıt sağlanmasına yardımcı olur

Kazaları azaltmak ve insan faktörünü (insan hatası)

en aza indirmek için eğitim programları

Altyapıyı araştırmak,

uzman analizleri gerçekleştirmek veya bir olayın etkisini en aza indirmek için uzman hizmetleri

Global tanınırlık

Frost and Sullivan şirketi Global Endüstriyel (OT/ICS) Siber Güvenlik pazarı analizini esas alarak Kaspersky şirketini 2020 Yılın Global Şirketi Ödülü ile ödüllendirdi

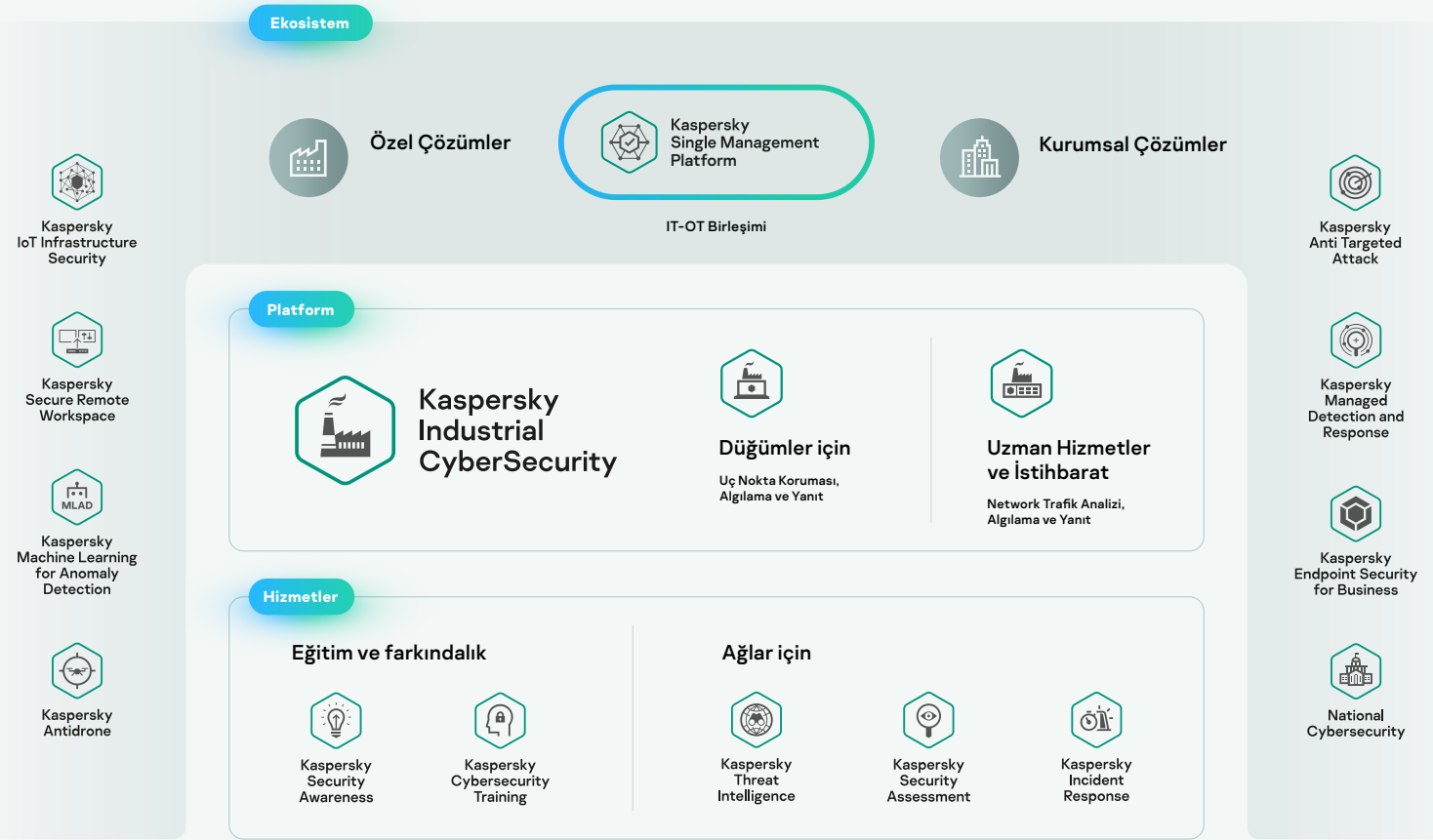
VDC'nin yıllık global araştırmasında endüstriyel otomasyon topluluğundaki 250'den fazla nitelikli profesyonelin genel derecelendirmelerine göre Kaspersky endüstriyel siber güvenlik kategorisinde en iyi tedarikçiydi.

Kaspersky'nin sağladıkları

Kaspersky Industrial CyberSecurity (KICS) Platformu yerel entegre teknolojiler ve uzman eğitim ve hizmet portföyüyle birlikte endüstriyel kurumların ve kritik öneme sahip altyapı operatörlerinin tüm siber güvenlik ihtiyaçlarını karşılar.

Platform, aşağıdakileri içeren endüstriyel kurumlar için benzersiz bir ekosistemde önemli bir temel unsurdur:

- **Kaspersky'nin gerçek IT-OT birleştirmesini ve tek tedarikçi yaklaşımının çok sayıda faydasını sunan, sınıfının en iyisi Kurumsal Çözümleri**
- **Siber fiziksel güvenlik, endüstriyel nesnelerin interneti (IOT) güvenliği, makine öğrenimi, güvenli uzaktan çalışma alanı ve daha fazlası için çeşitli Özel Çözümler sınırsız çevik ölçeklenebilirlik sunar**



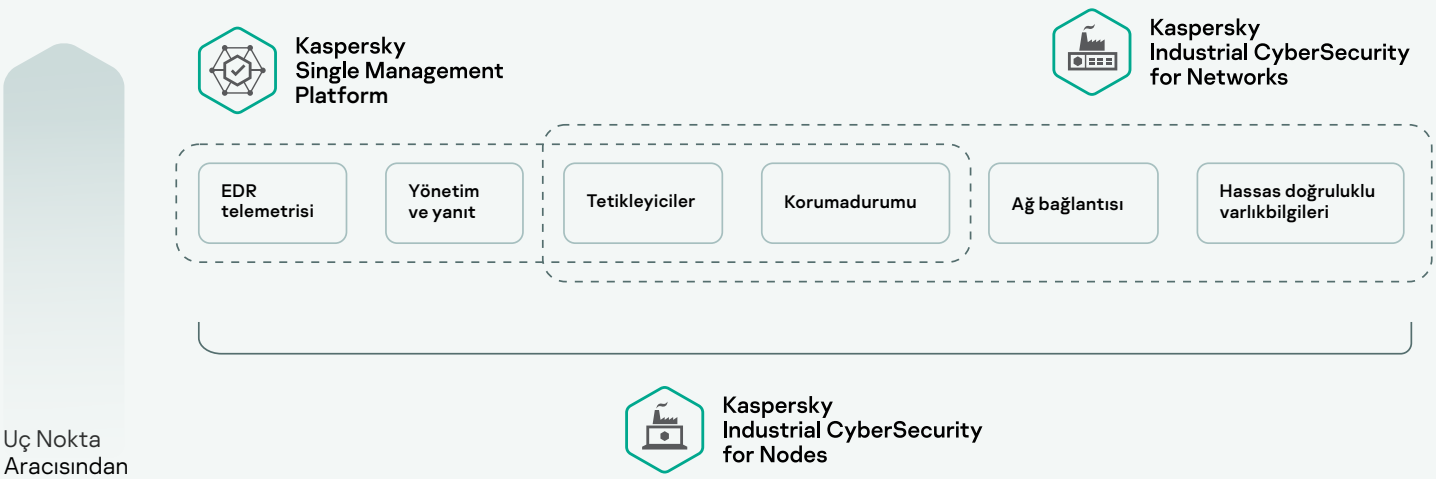
Kaspersky Industrial CyberSecurity Platformu aşağıdaki kategorilerde liderdir:

- OT Uç Nokta Güvenliği
- OT Ağ İzleme ve Görünürlük
- Anormallik Algılama, Olay Yanıt ve Bildirme
- OT Güvenlik Hizmetleri

Birlikte kullanıldıklarında kullanıcı daha büyük resmi ve daha geniş bağlamı görür: 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.

Ürünler

KICS, temel Endüstriyel Otomasyon ve Kontrol Sistemi bileşenlerinin her seviyede kapsamlı şekilde korunması için tasarlanmış bir OT siber güvenlik platformudur. 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.



KICS for Nodes uyumluluk denetim ve uç nokta sensör işlevselliğine sahip uç nokta koruma, algılama ve yanıt yazılımıdır.

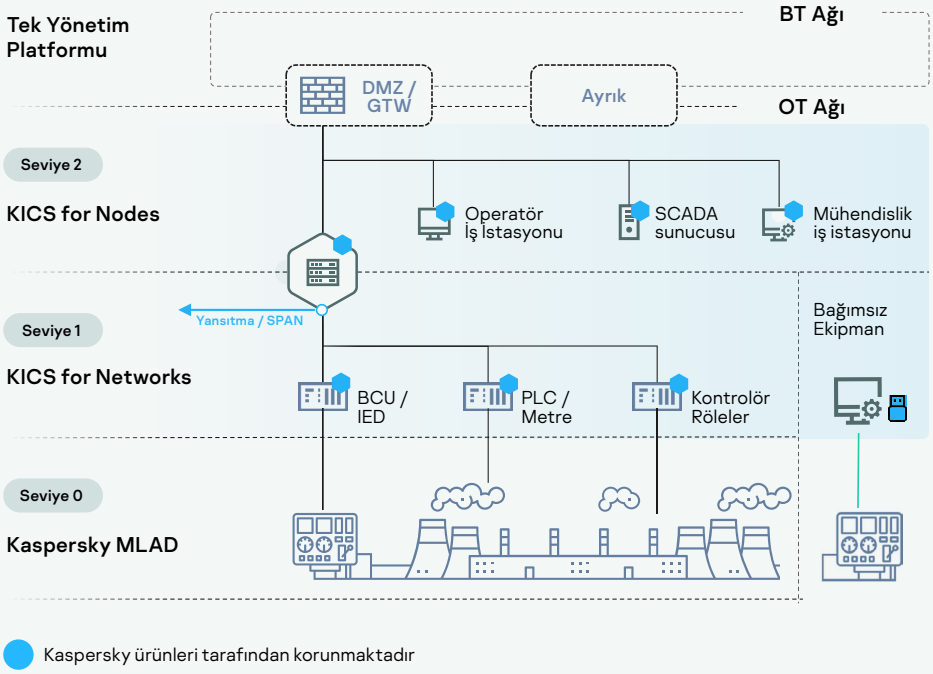
KICS for Networks ürünü OT ağ trafik analizi, algılaması ve yanıtı için tasarlanmıştır.

Tek Yönetim Platformu gelişmiş EDR arabirimi ile hızlı ölçeklenebilirliği çok sayıda yere götürür.

Ek işlevler

Bu çözüm çok sayıda ek işlev sağlar. Ağ **Etkin Toplama** teknolojisi ağ topolojisinin ve varlıklar ayarlarının hızlı ve hassas netlikte toplanabilmesini sağlar. **Uç Nokta Denetimi** işlevi geçerli ayarların güvenliği ve kontrol güvenlik açıkları da dahil olmak üzere, güvenlik politikası uyumluluğunu sağlamaya yardımcı olur. KICS for Nodes ürününün **Taşınabilir Tarayıcı** sunum yöntemi bağımsız, ayrı ekipman güvenliği denetimlerinde en iyi uygulalamarı oluşturmaya yardımcı olur. **Anormallik Algılama Makine Öğrenimi** teknolojik işlem derinliğinde erken anormallik algılama sistemidir.

Çözüm Mimarisi



Kaspersky ürünleri tarafından korunmaktadır

Özellikler

Varlık keşfi
Pasif OT varlık tespiti ve envanteri

Derin paket incelemesi
Teknik işlem telemetrisinin gerçek zamanlıya yakın analizi

Ağ bütünlük kontrolü
İzinsiz ağ ana makineleri ve akışları algılar

İzinsiz giriş algılama sistemi
Kötü amaçlı ağ faaliyetleri hakkında uyarılar gönderir

Komuta kontrol
Endüstriyel protokoller üzerindeki komutları teftiş eder

Harici entegrasyon
Esnek API entegrasyonu algılama ve önleme özellikleri ekler

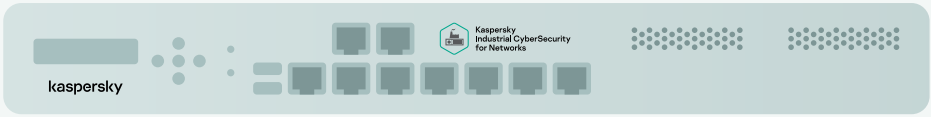
Anormallik algılama için makine öğrenimi (MLAD)
Gerçek zamanlı telemetri ve tarihsel veri madenciliği (tekrar ortaya çıkan sinir ağı) ile geçmiş veri madenciliği üzerinden siber ve fiziksel anormallikleri bulur

Güvenlik açığı yönetimi
Kaspersky ICS CERT tarafından sağlanan, endüstriyel ekipmandaki güvenlik açıkları güncellenebilir veritabanı

Kaspersky Industrial CyberSecurity for Networks

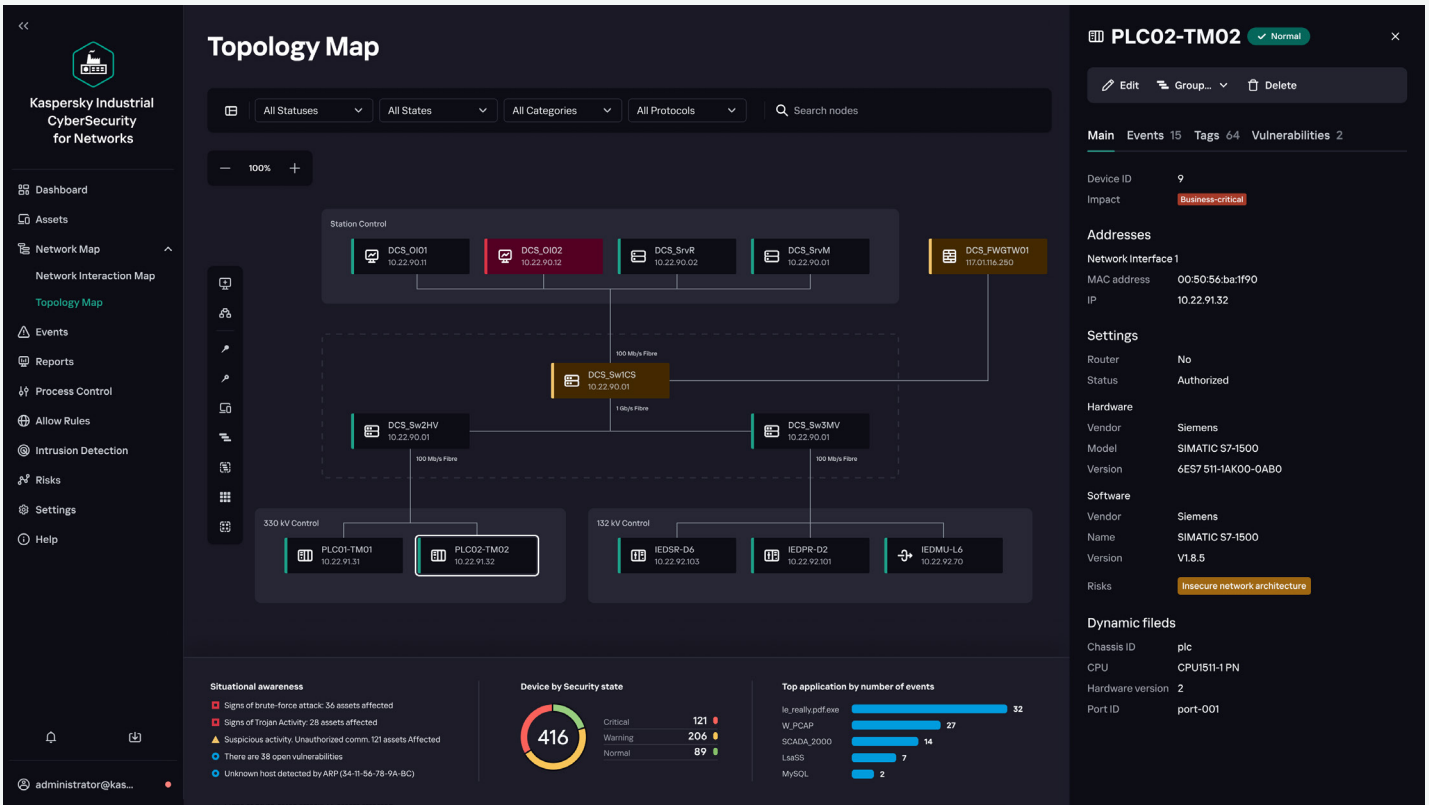
QT Ağ, Trafik Analizi, Algılama ve Yanıt Pasif trafik izleme, etkin toplama ve uç nokta sensörleriyle net risk görünürlüğü.

ICS ağlarındaki anormal durumları ve izinsiz girişleri erken aşamalarında algılar ve endüstriyel süreçlerde olumsuz etki oluşmasını önlemek için gerekli önlemlerin alınmasını sağlar.



Müşterilerimizin yerleşik kurulu kaynak kullanımına, entegrasyonuna ve garanti uygulamalarına hızlıca ve optimum şekilde entegre olabilen cihazdan bağımsız çözüm.

Arabirim



KICS for Nodes dağıtılmış otomasyon sistemlerinin zorlu gereksinimleri için özellikle tasarlanmıştı: karışık ve karmaşık ortamlar, çalışmada uzatılmış süreler, bağımsız ve bağlı kullanım vakaları, katılımlı ve bakım gerektirmeyen kurulumlar ve tüm maliyetlerde kontrol önceliği kullanımı

Kaspersky Industrial CyberSecurity 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.

Endüstriyel Uç Nokta Koruma, Algılama ve Yanıt

Modern, dijital, yönetimli ve dağıtımlı otomasyon sistemlerinin her bir uç noktasını korur. Kök neden analiz işleminde olay görünürlüğünün yeni seviyelerini açığa çıkarır. Aracı, bir olayın iş istasyonlarında, sunucularda, ağ geçitlerinde ve diğer uç noktalarındaki ilerlemesinin net ve ayrıntılı görsel temsilini oluşturarak uç nokta telemetri bilgilerini toplar, böylece bir olayla tam olarak ilgilenildiğine ve tekrar olmayacağına dair otomasyon sistem yöneticilerine güvence verir.

Avantajlar

Düşük etki
En iyi sistem performansı için korunan cihazda düşük etki

Uyumluluk
Eski nesil düşük performanslı bilgisayarlarla ve Windows XP SP2 ve Windows Server 2003 SP1 ve üzeri sistemlerle uyumluluk

Uzatılmış yaşam ömrü
5 yıla kadar lisanslama ve genişletilmiş destekle uzatılmış yaşam ömrü

Tüm MS Desktop,
Server ve Embedded Windows OS için tam işlevsellik

Modüler kurulum
Esnek seçenekler ve güvenli müdahaleci olmayan ayarlar

Karışık altyapıları kapsar
Windows, Linux ve Taşınabilir varyantlar

KICS for Nodes Taşınabilir Tarayıcı
Güvenlik yazılımının yüklenemeyeceği bağımsız makine, otomasyon sistemleri ya da ekipmanlarda siber güvenlik politikasını zorunlu kılar. Bağımsız bir altyapıda bile üstün durumsal farkındalık ve OT görünürlüğü.

Kurulum gerektirmeyen çözüm
KICS for Nodes birden fazla ek Taşınabilir Tarayıcı flaş sürücüsünde etkinleştirilebilir. Bu özellik uç nokta verilerini toplamak ve kullanışlı bir özet raporda bunları organize etmek üzere bakım işlemleri sırasında birden fazla makinede eş zamanlı isteğe bağlı taramalar gerçekleştirilmesine yardımcı olur.

Mevzuat ve iç politika uyumluluğu
KICS for Nodes Taşınabilir Tarayıcı, üçüncü taraf yüklenici bilgisayarları da dahil olmak üzere, bir OT yerine erişen ekipmanda kötü niyetli yazılımla mücadele uyumluluk kontrolleri gerçekleştirir. Düşük operasyonel ayak izi olup, mevcut güvenlik çözümlerine müdahale etmez.

Avantajlar

Durumsal farkındalık

Sistemler / politika yönetimi

Ölüm zinciri ve yanıt

Raporlama ve bildirim

SIEM entegrasyonu

HMI / MES entegrasyonu

Kaspersky Single Management Platform

Tek Yönetim Platformu olaylar, olay analitikleri ve daha fazlasıyla zenginleştirilmiş tüm coğrafi olarak dağıtılmış varlıkların bir haritasıyla birlikte, bütün OT altyapısının güvenlik düzenlemesi için merkezi bir güvenlik yönetim çözümüdür. OT ve BT güvenlik ekipleri karışımının verimliliğini artırır. Tüm güvenlik kontrollerinizin ahenk içinde çalışarak hızlı ve hassas netlikte yanıt imkanı sağlayan bir yerdir.

Altyapıyı araştırmak,

Hizmetlerimizden oluşan paketimiz KICS portföyünün önemli bir parçasını oluşturur. Endüstriyel siber güvenlik değerlendirmelerinden olay yanıtına kadar tam güvenlik hizmetleri döngüsü sağlıyoruz.

> Diğer tedarikçilere kıyasla Endüstriyel Kontrol Sistemi (ICS) siber güvenlik alanındaki deneyimleri, profesyonellikleri ve çözümlerinin giriftliği bize büyük bir değer kattı ve şirketimizin güvenlik stratejisi için daha parlak bir gelecek sağladı.
>
> Ondřej Sýkora,
> C&A Yöneticisi, Plzeňský Prazdroj

Endüstriyel Siber Güvenlik Değerlendirmesi

Endüstriyel Siber Güvenlik Değerlendirmesi: Kaspersky, dış ve iç sızma testleri, OT güvenlik değerlendirmesi ve otomasyon çözümü güvenlik değerlendirmesi de dahil olmak üzere minimum müdahaleci endüstriyel güvenlik değerlendirmesi sağlar. Kaspersky uzmanları bir şirketin altyapısına ilişkin derinlemesine bilgiler ve ICS siber güvenlik duruşunun nasıl güçlendirilebileceğine ilişkin öneriler sunar.

> Alıştırmaları gerçekleştirerek ve Kaspersky ekibinin bilgisinden faydalanarak siber güvenlik tehditlerine karşı korumamızı artırdık.
>
> Yu Tat Ming,
> CEO, PacificLight

Tehdit İstihbaratı

Kaspersky uzmanları tarafından toplanan güncel analitik bilgiler hedeflenen endüstriyel siber saldırılara karşı müşterinin korumasının iyileştirilmesine yardımcı olur. TI akışları ya da özel raporlar şeklinde sunularak, bölgesel, endüstri ve ICS yazılım parametrelerine göre özel müşteri ihtiyaçlarını karşılarlar.

Olay müdahalesi

Bir olay durumunda Kaspersky uzmanları verileri ve kötü amaçlı yazılımı toplar ve analiz eder, olay zaman çizelgesini yeniden oluşturur, olası kaynakları ve motivasyonu kararlaştırır ve ayrıntılı bir düzeltme planı geliştirir. Plan, kötü amaçlı yazılımın müşterinin sistemlerinden silinmesine ve kötü amaçlı işlemlerinin geri alınmasına ilişkin öneriler içerir.

Eğitim ve farkındalık

> Kaspersky, ICS grubumuz için profesyonel endüstriyel siber güvenlik becerileri eğitimi verebilecek mümkün olan en iyi şirketti.
>
> Søren Egede Knudsen,
> Sorumlu Teknik Başkan

Endüstriyel siber güvenlik farkındalık eğitimi

Endüstriyel bilgisayarlı sistemlerle çalışanlar ve onların yöneticileri için yerinde ve çevrimiçi etkileşimli eğitim ve siber güvenlik oyunları. Katılımcılar özellikle endüstriyel ortamları hedefleyen mevcut tehdit ortamı ve saldırı vektörleri hakkında derin bilgiler kazanır, uygulamalı senaryoları keşfeder ve siber güvenli beceriler edinirler.

Uzman eğitim programları

ICS Sızma Testi ve ICS Dijital Adli Delil Toplama eğitim kursları siber güvenlik profesyonellerine yöneliktir. Katılımcılar endüstriyel ortamlarda kapsamlı sızma testleri ya da dijital adli delil toplama işlemleri gerçekleştirebilmek için gereken tüm ileri düzey becerileri kazanır.

Özel çözümler ekosistemi

Kaspersky IoT Infrastructure Security

Kaspersky'nin Siber Bağışıklık yaklaşımını esas alarak Eşyaların İnterneti'ni ağ geçidi düzeyinde korur

Daha fazla bilgi edinin

Kaspersky Antidrone

Herhangi bir boyuttaki tesiste hava sahasını drone'lara karşı korur

Daha fazla bilgi edinin

Kaspersky Secure Remote Workspace

Siber Bağışıklığa sahip işlevsel ince istemci altyapısı

Daha fazla bilgi edinin

Kaspersky Security CAD

Tasarım ve operasyon aşamaları için bilgi güvenlik sistemlerinin dijital modellemesi

Daha fazla bilgi edinin

Kaspersky Machine Learning for Anomaly Detection

Endüstriyel teknoloji süreçlerinde erken anormallik algılama sistemi

Daha fazla bilgi edinin

www.kaspersky.com.tr

Kaspersky Industrial CyberSecurity

Daha fazla bilgi edinin