Kaspersky OT CyberSecurity

Endüstriyel işletmeler için siber-fiziksel güvenlik ekosistemi

kaspersky GELECEĞİ YAKALAYIN

Kaspersky
OT CyberSecurity

Birleştirilmiş Endüstriyel Güvenlik Kavramı

Teknolojiler
Test edilmiş, uyumlu ve onaylı endüstriyel güvenlik çözümlerinden oluşan sağlan bir seçki

Bilgi
Güvenilir tehdit analizi ve kapsamlı endüstriyel siber güvenlik eğitimi

Uzmanlık
Kapsamlı endüstriyel siber güvenlik için eksiksiz profesyonel hizmetler

BT-OT Birleştirme

Kaspersky Extended Detection and Response (XDR)

Teknolojiler

Özel Çözümler
- **Kaspersky Antidrone**
- **Kaspersky Anomali Algılaması için Makine Öğrenimi** (MLAD)
- **Kaspersky SD-WAN**

Kaspersky Endüstriyel Siber Güvenlik

KICS XDR

for Nodes
Endpoint protection, detection and response

for Networks
Ağ trafiği analizi, algılama ve yanıt

Kaspersky İşletim Sistemi Çözümleri
- **Kaspersky IoT Secure Gateway**
- **Kaspersky Secure Remote Workspace**
- **Kaspersky Automotive Secure Gateway**

Bilgi

Siber Hijyen	Tehdit İstihbaratı	Eğitim
Kaspersky Güvenlik Farkındalığı Eğitimleri	Kaspersky ICS Tehdit İstihbaratı	Kaspersky ICS CERT Uzman Eğitimleri

Uzmanlık

Bulma	Yönetilen Hizmet	Yanıt
Kaspersky ICS Güvenlik Değerlendirmesi	Kaspersky Incident Response	Kaspersky Managed Detection and Response

Kaspersky OT CyberSecurity

BT-OT Birleştirme

Kaspersky Extended Detection and Response

Kaspersky IoT Secure Gateway

Kaspersky SD-WAN

Kaspersky Endüstriyel Siber Güvenlik

KICS XDR

for Nodes
Endpoint protection, detection and response

for Networks
Ağ trafiği analizi, algılama ve yanıt

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Secure Remote Workspace

Kaspersky Antidrone

Kaspersky Automotive Secure Gateway

4 Industry 4.0 & IIoT

3 IT systems

2 Monitoring & Control

1 Automation & Protection

0 Technological process

Uzmanlık

Bulma
Kaspersky ICS Güvenlik Değerlendirmesi

Yönetilen Hizmet
Kaspersky Incident Response

Yanıt
Kaspersky Managed Detection and Response

Bilgi

Siber Hijyen
Kaspersky Güvenlik Farkındalığı Eğitimleri

Tehdit İstihbaratı
Kaspersky ICS Tehdit İstihbaratı

Eğitim
Kaspersky ICS CERT Uzman Eğitimleri

Siteyi ziyaret et

Kaspersky Endüstriyel Siber Güvenlik

XDR

TEKNOLOJİ

Otomasyon sistemlerini korumak için yerel XDR platformu

- Gizli tehditleri, anomalileri, güvenlik açıklarını ve izinsiz giriş denemelerini operasyonlarınız için tehlikeli hale gelmeden önce açığa çıkarır
- Otomasyon satıcıları ve düzenleyicileri tarafından sertifikalıdır
- Teknolojik işlemler üzerinde olumsuz etkisi yoktur. Kabul edilemez hasarı önler
- Karmaşık, dağıtılmış otomasyon altyapısı ve olay yanıtının yönetilmesini kolaylaştırır
- Riskleri azaltmaya yardımcı olur ve ihlallerin kaydını tutar

XDR platformunun avantajları

Endüstriyel Otomasyon ve Kontrol Sistemleri (IACS) için uçtan uca kapsam. Linux, Windows, yalıtılmış veya üçüncü taraf bilgisayarlar için koruma ve ağ anomalileri ile tehditlerini algılama.

Uç noktaların ve ağların aktif ve/veya pasif güvenlik denetimi. Tüm IACS düzeylerinde merkezileştirilmiş risk, güvenlik ilkesi ve varlık yönetimi.

Olağanüstü sistemler ve ağ görünürlüğü. Tüm yok etme zincirinin araştırılması ve yeniden oluşturulması. Endüstriyel ağlar ve farklı düğümler arasında olay ilerlemesine yönelik görünürlük.

İş ortağından satın al Bir demo talep edin Veri Sayfası

ics.kaspersky.com

Siteyi ziyaret et

XDR

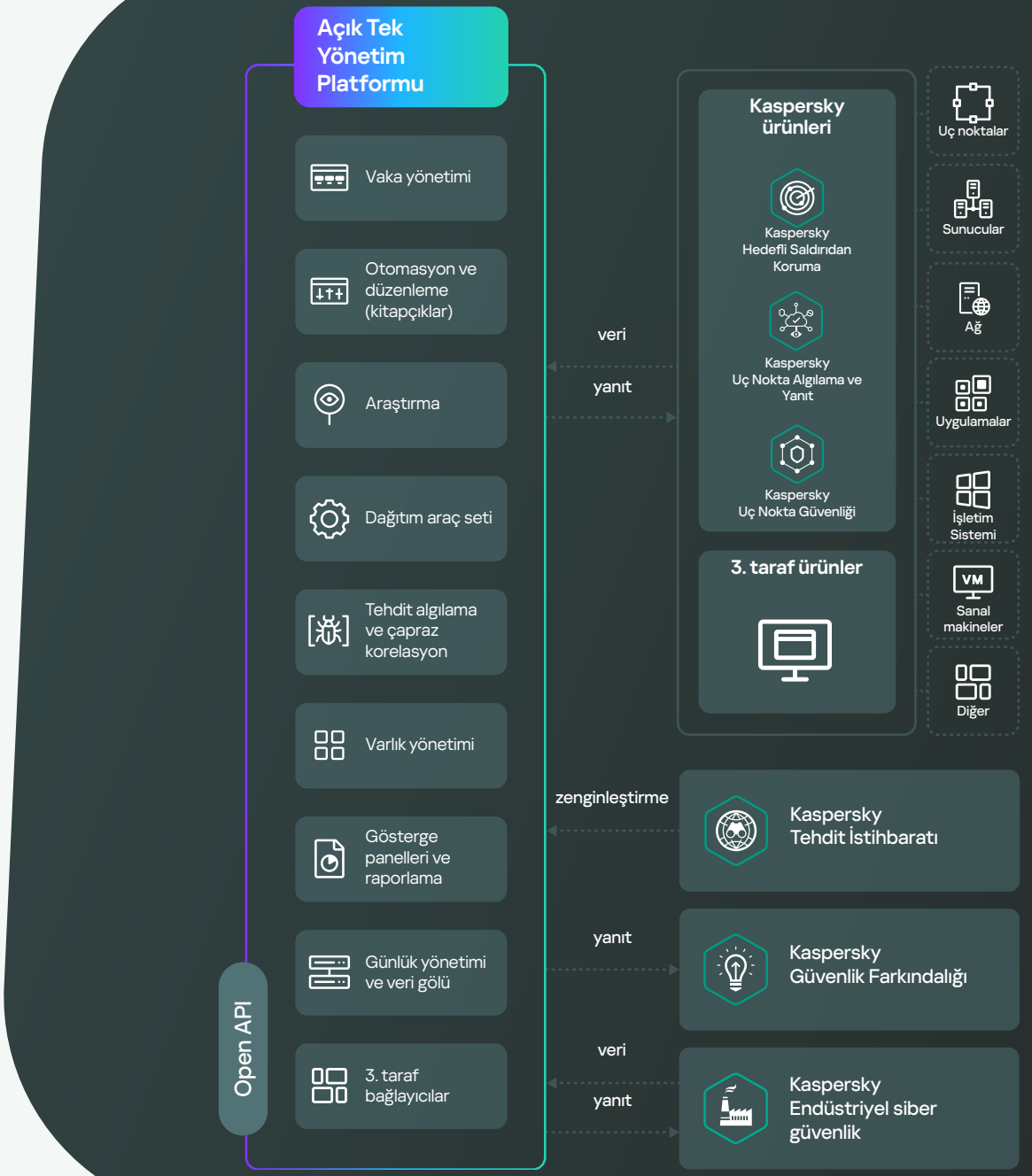
Kaspersky Extended Detection and Response

TEKNOLOJİ

Kuruluşunuzun endüstriyel ve kurumsal segmentleri arasında birleştirilmiş siber güvenlik

Kaspersky Genişletilmiş Algılama ve Yanıt ile yakın tümleştirme aracılığıyla, Kaspersky Endüstriyel Siber Güvenlik platformu gelişmiş araştırma ve yanıt özelliklerine sahip üçüncü taraf çözümlerle etkileşimleri içeren yeni senaryoları etkinleştirir. Platform ayrıca işletmenizi yalnızca endüstriyel ortamlarda değil aynı zamanda endüstriyel ve kurumsal ortamların örtüştüğü yerlerde de korur. Bu, Kaspersky'nin sınıfında en iyi BT siber güvenlik portföyüyle yakından uyum sayesinde gerçekleştirilir.

Bu şekilde, güvenlik ekipleri bir olayın gelişiminin bütünsel bir görünümüne sahip olur ve gelecekte benzer olayların ortaya çıkmasını önlemek için olayın kök nedenini belirler.



KICS ile yanıt örnekleri:

- ✔ AV taraması ve AV veritabanı güncellemesi
- ✔ Görevleri başlatma
- ✔ Değişiklik düğümü yetkilendirmesi
- ✔ Düğüm ve işlem yalıtımı

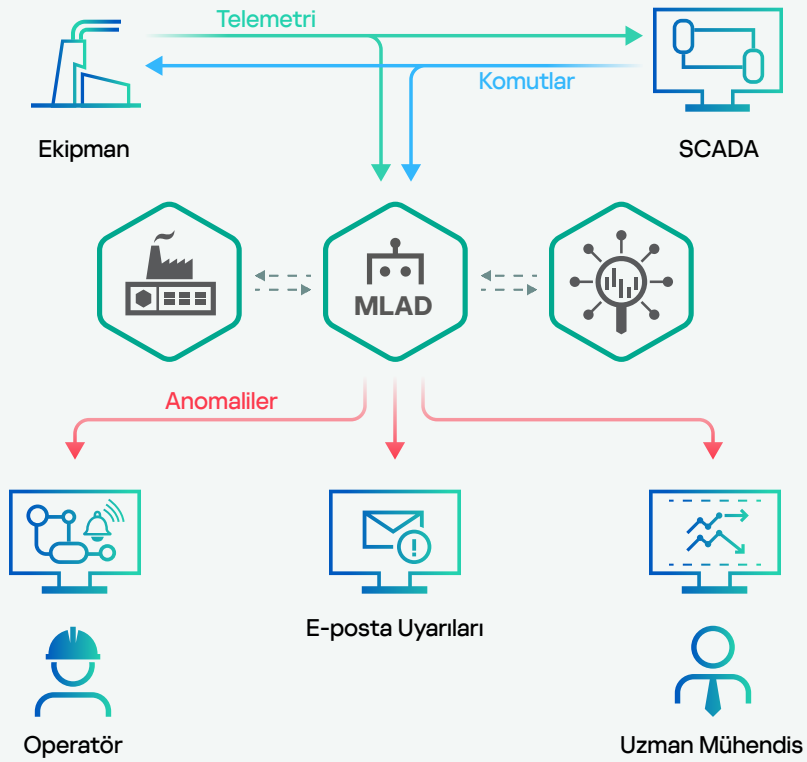
Bize Ulaşın Veri Sayfası

Siteyi ziyaret et

MLAD

Kaspersky Machine learning for Anomaly Detection

TEKNOLOJİ



Erken anomali algılama ve tahmine dayalı analiz

- Ekipman arızalarını ve insan hatalarını kritik duruma ulaşmadan önce algılayarak hata ve kazaları önlemeye yardımcı olur
- Tipik olmayan çalışan eylemlerini veya ekipman işlemlerini özelleştirilmiş bir saldırı veya sabotaj işareti olarak belirler
- Anomali algılama ile ekipman koşulu ve yaşam döngüsünün tahmine dayalı analizini birleştirir

Ekosistem ve yapay zeka

KICS for Networks ve KUMA ile tümleştirme: bu sistemlerden telemetri ve olayları alır ve algılanan anomaliler hakkında uyarıları geri gönderir

Tanılama kurallarını sorunun önceden tanımlanmış belirtilerine uygulayarak makine öğreniminin normal ekipman davranışından sapmaları algılamasını sağlar

Çalışan eylemleriyle ilgili telemetri ve olayları analiz etmek ve işlemek için yapay zeka kullanır

Siteyi ziyaret et

SD-WAN

Kaspersky SD-WAN

TEKNOLOJİ

Kaspersky SD-WAN özellikleri:

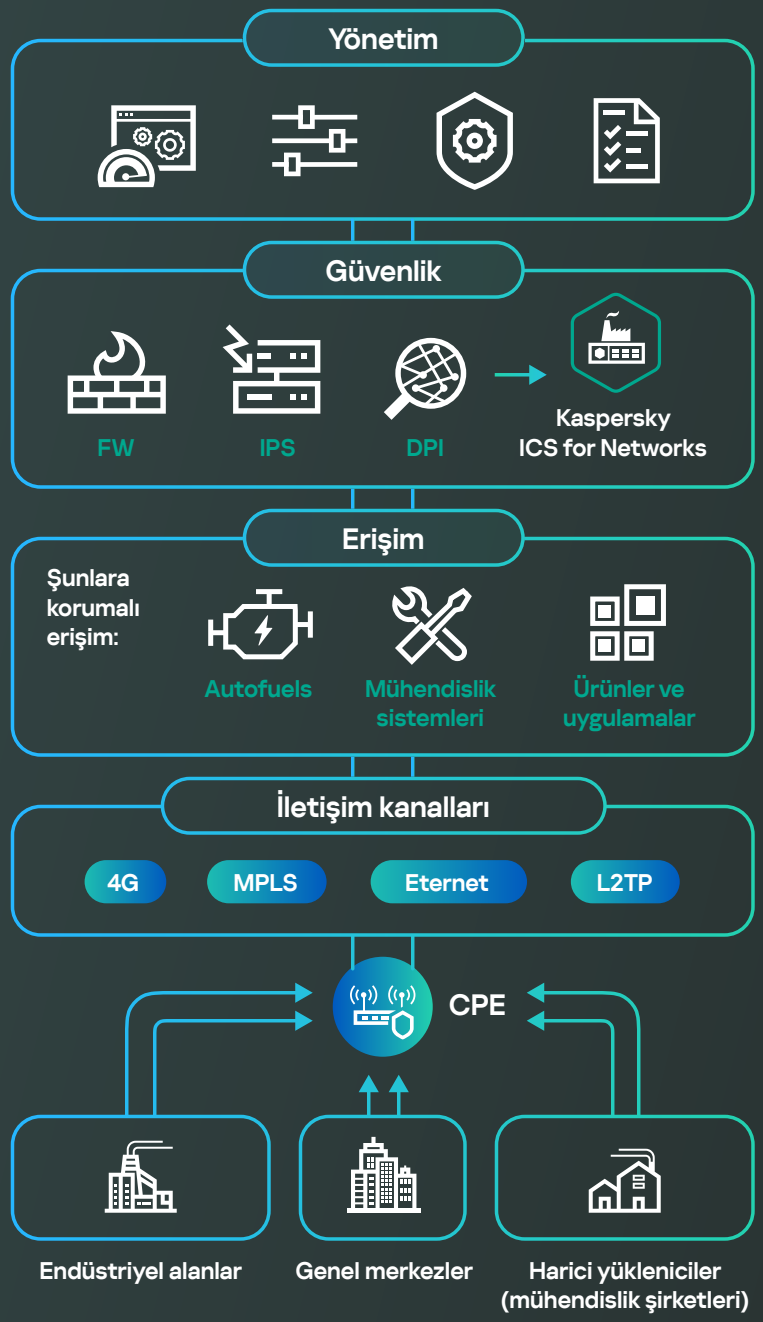
- Kolay ölçeklenebilirlik
- Kolay yönetim
- Maliyet optimizasyonu
- Merkezi güvenlik

Güvenilir endüstriyel ağlar için tek bir çözüm

Kaspersky SD-WAN kuruluşların üretim süreçlerinin devamlılığını sağlarken merkezi yönetime sahip hataya dayanıklı, coğrafi olarak dağıtılmış bir ağ oluşturmasına olanak sağlar. Kaspersky SD-WAN mimarisi, Sanal Ağ İşlevleri (VNF'ler) yöneticisi aracılığıyla Kaspersky ve üçüncü taraf güvenlik araçlarını kolayca tümleştirmenize olanak sağlar.

Kaspersky ICS for Networks ile SD-WAN altyapısını kullanarak, çeşitli dağıtılmış endüstriyel siteler için merkezileştirilmiş bir izleme ve koruma sistemini düzenleyebilirsiniz.

Bize Ulaşın



Siteyi ziyaret et

Kaspersky Antidrone

TEKNOLOJİ

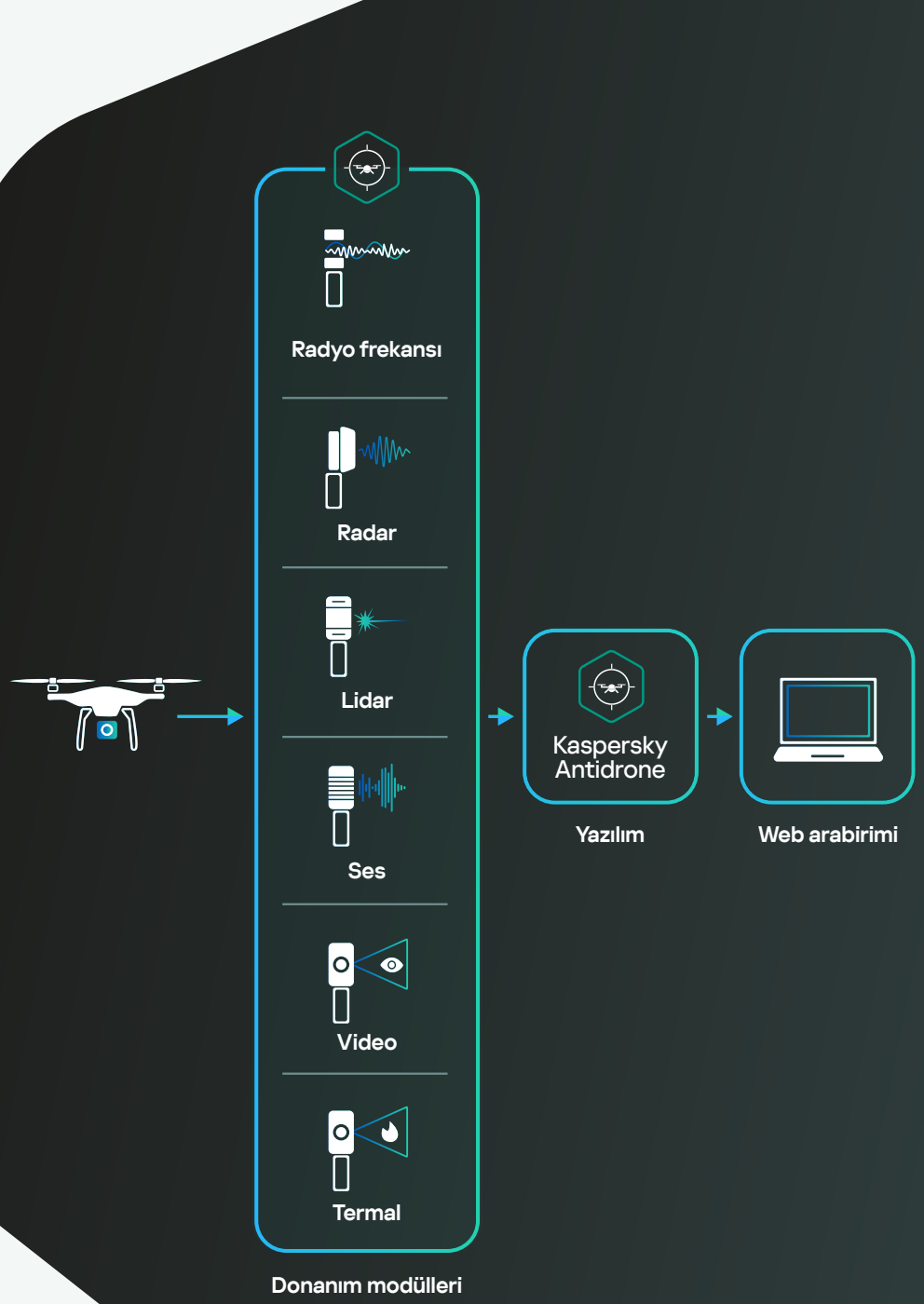
Temel Özellikler

- Drone algılama ve izleme
- Sinir ağlarını kullanarak drone sınıflandırma
- Tek yönlü ve çok yönlü jamming

Drone izleme ve savunma çözümü

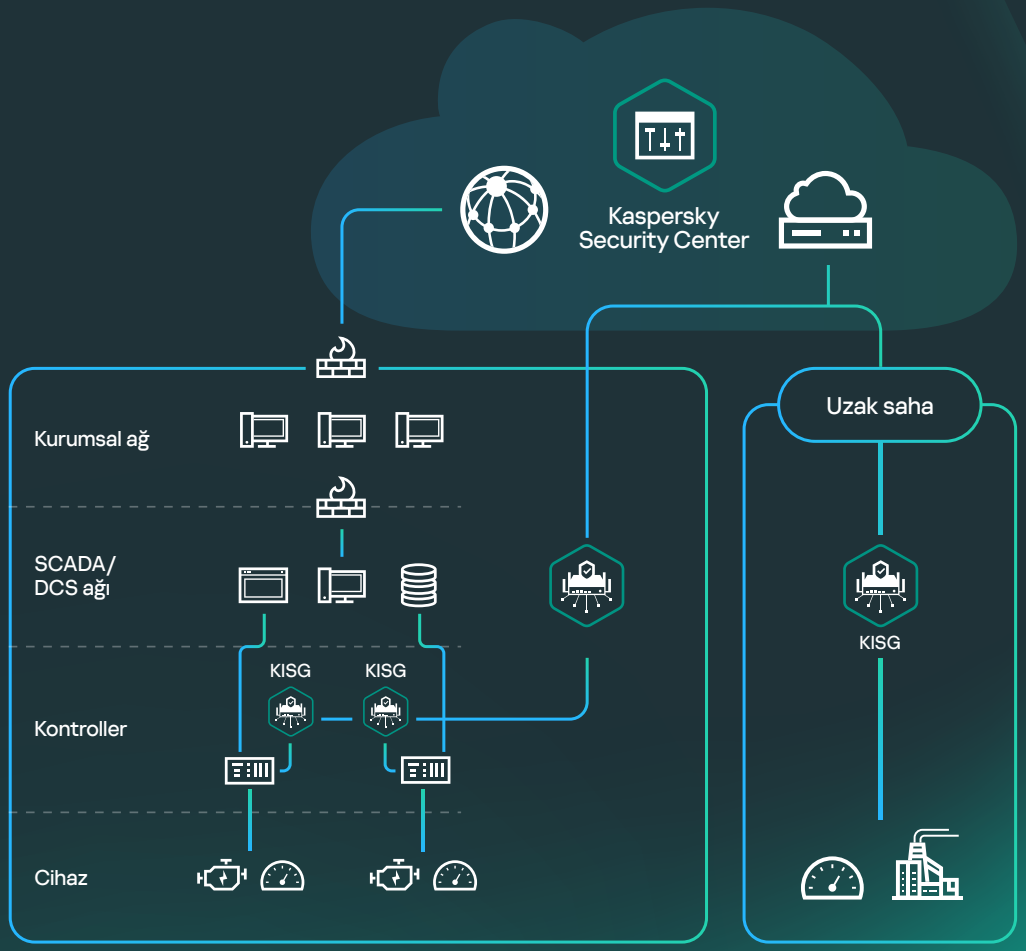
Kaspersky Antidrone yetkisiz drone'ların bölgenize girmesini engelleyerek endüstriyel kuruluşlarda işlemlerin durdurulması olasılığını azaltır. Sistem hava sahasını otomatik olarak tarayarak drone'ları algılar ve sınıflandırır. Gerçekleşen olaylar hakkında bilgiler web arabiriminde görüntülenir. Bir tehdit durumunda, operatör uygun izinlerle drone'u etkisiz hale getirebilir.

Kaspersky Antidrone çözümü modülerdir ve herhangi bir boyuttaki endüstriyel sahaya uygulanabilir. Çözüm ayrıca “dost veya düşman” operasyon modunu destekleyerek müşterilerin kendi drone'larını kullanmasını sağlar ve yasadışı, insansız hava taşıtlarının işlemleri kesintiye uğratmasını önler.



Bir demo talep edin Veri Sayfası

antidrone.kaspersky.com



aprotech

Bu çözümünü teknik ve ticari geliştirmesi Adaptive Production Technologies LLC (Aprotech, bir Kaspersky alt kuruluşu) tarafından gerçekleştirilmektedir

Bize Ulaşın Bir demo talep edin Veri Sayfası

Siteyi ziyaret et

Kaspersky
IoT Secure
Gateway

TEKNOLOJİ

Temel Özellikler

- IoT cihazlarından dijital ve bulut platformlarına güvenli veri toplama ve taşıma
- KasperskyOS'yi temel alan Kaspersky Cyber Immunity, ek güvenlik araçları olmadan çoğu siber saldırı türüne karşı «yerleşik» dayanıklılık sağlar
- Altyapı şeffaflığı, merkezileştirilmiş olay yönetimi ve üretim optimizasyonu

Industry 4.0'te iş geliştirme için güvenilir veriler

Çözüm KasperskyOS'yi temel alan Kaspersky IoT Secure Gateway'den ve Kaspersky Security Center (KSC) yönetim konsolundan oluşur. Ağ geçitleri ekipmandan verileri güvenli bir şekilde toplayıp dijital ve bulut platformlarına aktararak üretimi optimize etmek ve olayları önlemek için yüksek kaliteli iş zekası sunar. Konsol farklı kaynaklardan olayları eşlemeyi ve 100.000'e kadar fiziksel, sanal ve bulut iş istasyonunu yönetmeyi sağlar.

Siteyi ziyaret et

Kaspersky Secure Remote Workspace

TEKNOLOJİ

Ürün Uygulama

Risk

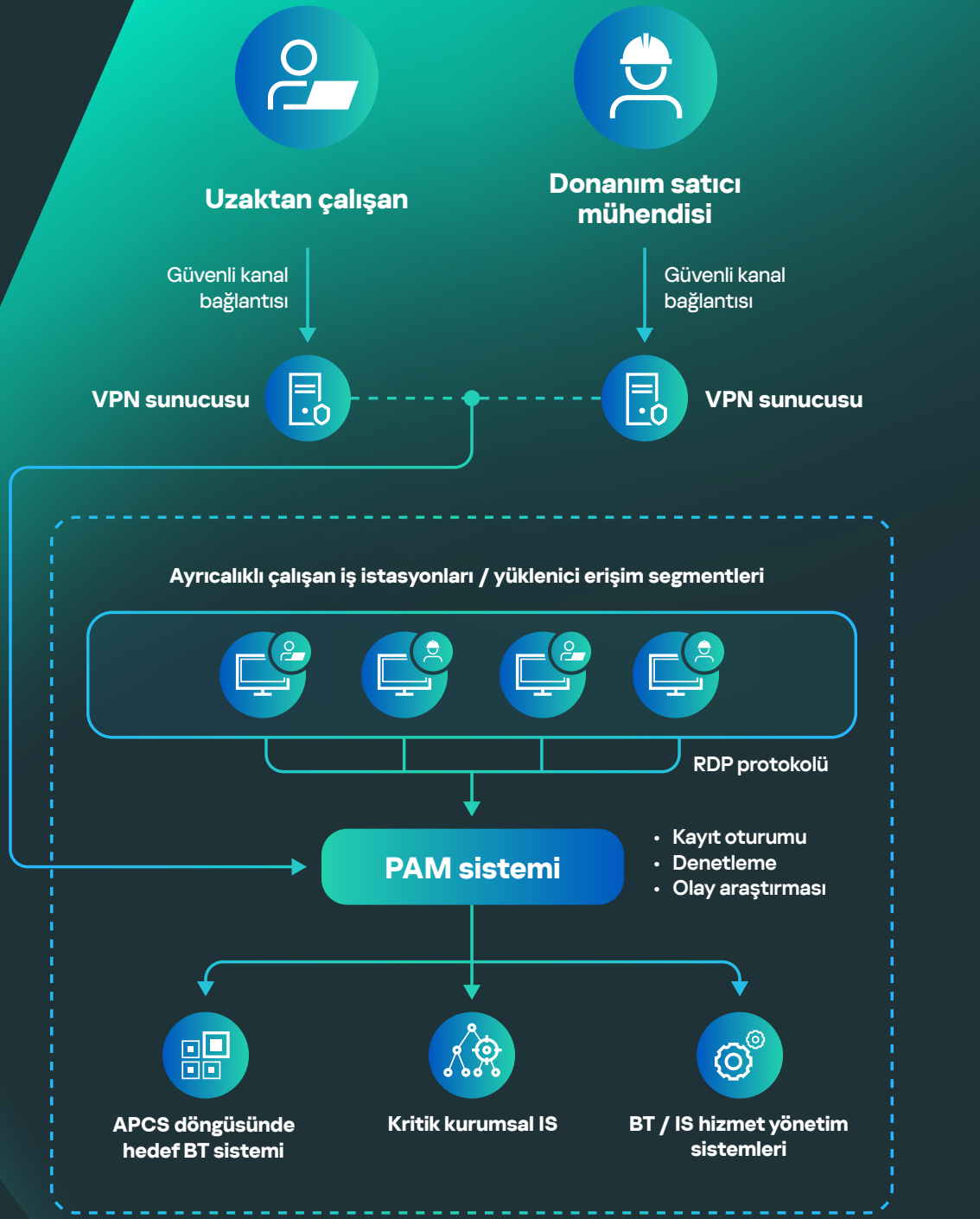
Kullanıcıların iş istasyonları siber saldırılar için en yaygın hedefler arasındadır

Çözüm

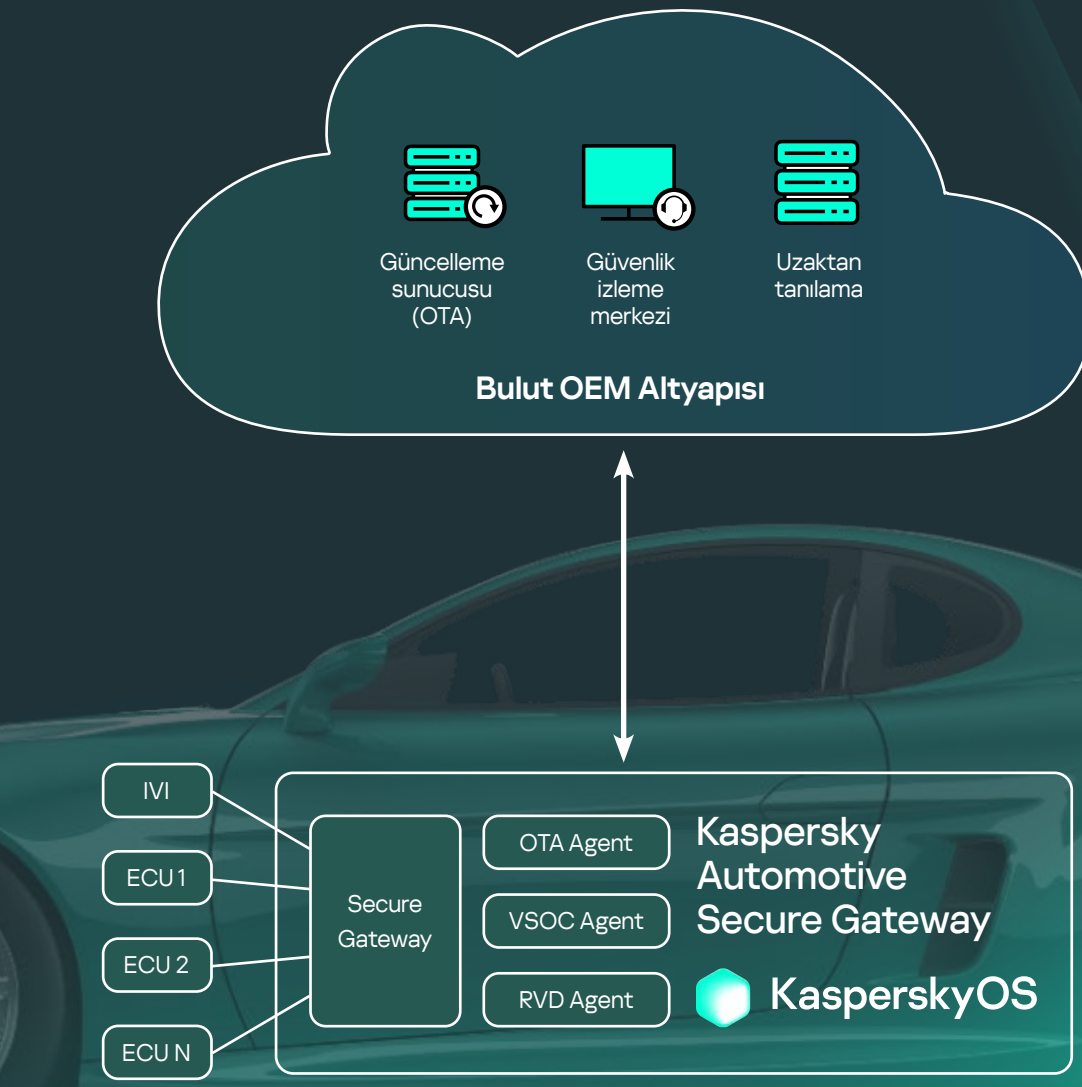
Kaspersky Secure Remote Workspace (KSRW), Kaspersky'nin kendi mikro çekirdek KasperskyOS işletim sistemini temel alan ince istemcilerden oluşan yönetilen ve işlevsel bir altyapı oluşturmaya yönelik bir çözümdür

Siber Saldırılara Dayanıklı İnce İstemci altyapısı

Kaspersky Secure Remote Workspace'in parçası olan Siber Saldırılara Dayanıklı İnce İstemciler, kullanıcıları endüstriyel altyapıya bağlamak için güvenilir bir bölge dahil olmak üzere sanal masaüstlerine güvenli bir bağlantı sağlar.



Çözüme Genel Bakış Bir demo talep edin Veri Sayfası



AUTOSAR

Siteyi ziyaret et

Kaspersky Automotive Secure Gateway

TEKNOLOJİ

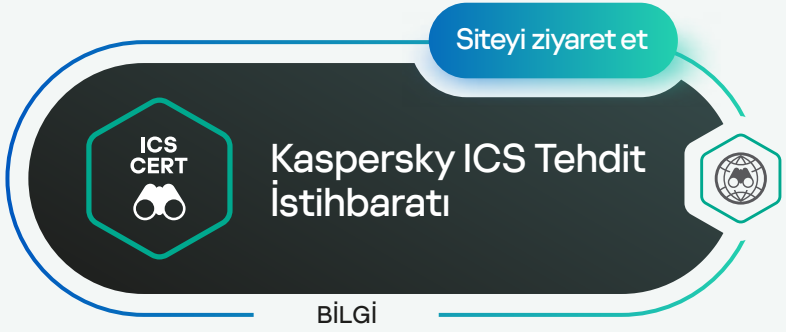
Araç koruması

- Yetkisiz erişim
- ECU hedefli saldırılar
- Araç bilgi-eğlence sistemleri (IVI) aracılığıyla saldırılar
- Kötü amaçlı tanılamalar
- Güncelleme sisteminin güvenliğinin aşılması
- Denetlenmeyen bağlantılar ve veri akışları, iletişim kesintisi

Temel Avantajlar

- Tasarım gereği güvenli çözüm
- Siber güvenlik düzenlemeleriyle uyumlu kalmaya yardımcı olur
- 4'ü 1 arada: Bağlantılı ağ geçitleri, güvenlik ağ geçidi, OTA-ana ve VSOC aracısı
- ISO21434, ISO26262, AUTOSAR Adaptive, Uptane ile uyumluluk

Bize Ulaşın Veri Sayfası



Etkili risk değerlendirmesi, başarılı saldırı tespiti, olay incelemesi ve yanıtı için endüstriyel siber güvenlik tehditleri ve güvenlik açıklarının derin bir şekilde anlaşılmasını sağlar.

Endüstriyel siber güvenlik alanındaki ilk özel CERT olan Kaspersky ICS CERT'in benzersiz uzmanlığı ve deneyimi ile desteklenmektedir.

Temel Özellikler

- Hızlı tehdit tespiti ve kapsamlı analiz imkanları sunar
- İnceleme ve aktif tehdit aramalarının verimliliğini artırır
- Bilgiye dayalı karar almak için kapsamlı tehdit ve güvenlik açığı bilgisi sağlar

Şirketinizi hedef alan siber tehditlere yönelik derinlemesine görünürlük sayesinde düşmanlarınızın bir adım önünde olun

Kaspersky ICS Tehdit Veri Akışları

Düzenli olarak güncellenen tehdit istihbaratı akışı endüstriyel siber güvenliğin özel ihtiyaçlarına uygun olarak uyarlanmıştır

Tehdit İstihbaratı

Otomatik veri akışları

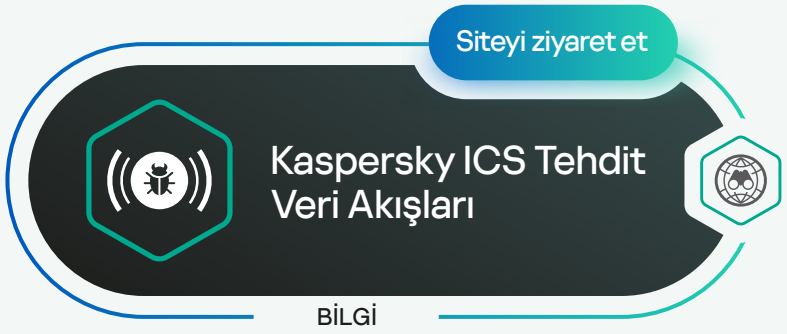
Kaspersky ICS Tehdit İstihbaratı Raporlaması

Endüstriyel kuruluşları hedef alan kötü niyetli kampanyalar hakkında daha fazla farkındalık sağlamanın yanı sıra en popüler endüstriyel kontrol sistemlerinde bulunan zayıf noktalar hakkında bilgi sağlar

Kaspersky Ask the Analyst

Müşterilerin karşılaştıkları veya ilgilendikleri belirli tehditlere yönelik uzman rehberlik ve içgörüler isteyebileceği bir hizmet.

Bir demo talep edin Çözüme genel bakış Bize Ulaşın



Kaspersky Tehdit Veri Akışı hizmeti, endüstriyel işletmelerin ağlarını ve sistemlerini siber tehditlere karşı korumalarına yardımcı olmak için gerçek zamanlı tehdit istihbaratı bilgileri sunar. Veri akışları, bilinen kötü amaçlı yazılımlar, kimlik avı siteleri, en son güvenlik açıkları ve sömürüleri ile diğer siber tehdit türleri hakkında bilgiler içerir. Veriler bağlama yerleştirildiğinde, büyük resmi görmek ve saldırganları belirlemek ve hızlı karar alıp harekete geçmek amacıyla "kim, ne, nerede, ne zaman" sorularını yanıtlamak için daha kolay bir şekilde kullanılabilir.

Elde edecekleriniz:

Kaspersky ICS Hashes Veri Akışı

Zamanında saldırı tespiti ve incelemesini basitleştirmek ve otomatikleştirmek amacıyla ICS (ve OT'de kullanılan diğer sistemler) için tehdit istihbaratı

#önleme

#algılama

#inceleme

Kaspersky ICS Güvenlik Açığı Veri Akışı

ICS sistemleri ve endüstriyel ortamlarda kullanılan diğer sistemlerin yazılım ve donanımlarındaki güvenlik açıklarına ilişkin doğrulanmış ve rafine verilerin bilgisayar tarafından okunabilir bir formatta sağlanması

#önleme

#algılama

#inceleme

OVAL formatında ICS Güvenlik Açığı Veri Akışı

SCADA sistemleri ve diğer endüstriyel yazılımlardaki bilinen güvenlik açıklarının otomatik tespiti için OVAL tanımlarını içeren ve düzenli güncellenen akış

#algılama

Bize Ulaşın Hizmet hakkında detaylı bilgi

Kaspersky ICS Tehdit İstihbaratı Raporlaması endüstriyel kuruluşları hedef alan kötü amaçlı kampanyalar hakkında derinlikli istihbarat ve daha fazla farkındalığın yanı sıra en popüler endüstriyel kontrol sistemlerindeki ve temel teknolojilerdeki güvenlik açıkları hakkında bilgi sağlar. Endüstriyel kuruluşlar için uyarlanmış ayrıntılı bilgiler müşterilerin yazılım ve donanım bileşenleri dahil kritik varlıkları korumasına yardımcı olur ve teknolojik süreçlerin güvenliğini ve sürekliliğini sağlar.

Raporlar **Kaspersky Threat Intelligence Portal** aracılığıyla sunulur veya API aracılığıyla erişilebilir.

Elde edecekleriniz:

APT raporları
Endüstriyel kuruluşları hedef alan yeni APT ve yüksek hacimli saldırı kampanyaları hakkında raporlar ve aktif tehditlere ilişkin raporlar.

Tehdit alanı
Endüstriyel kontrol sistemlerine yönelik tehdit ortamındaki önemli değişiklikler, ICS güvenlik seviyelerini etkileyen yeni keşfedilen kritik faktörler ve ICS'nin maruz kaldığı tehditler hakkında bölgesel, ülke ve sektöre özgü bilgiler de dahil olmak üzere raporlar.

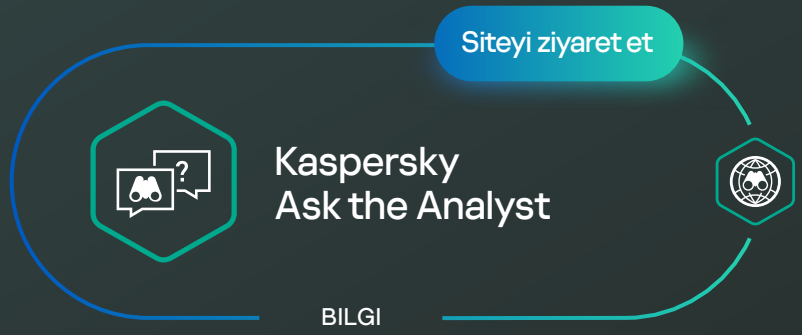
Güvenlik açıklarının bulunması
Endüstriyel kontrol sistemlerinde, endüstriyel nesnelerin internetinde ve çeşitli sektörlerdeki altyapılarda kullanılan en popüler ürünlerde Kaspersky tarafından belirlenen güvenlik açıkları hakkında raporlar.

Güvenlik açığı analizi ve riski azaltma
Bilgilendirmelerimiz tehditleri belirlemeye ve azaltmaya yardımcı olmak için Kaspersky uzmanlarından eyleme geçirilebilir tavsiyeler sunar.

Bize Ulaşın Hizmet hakkında detaylı bilgi

*** Yayınlanmış raporlarla ilgili ek bilgiler:**

- ICS güvenlik açıkları hakkında bilgiler
- İşlem kontrol sistemi tehdit istatistikleri ile bölge ve sektöre göre yeni eğilimler
- ICS'yi hedefleyen kötü amaçlı yazılımların analizi
- Yasal düzenleme gereksinimleri ve standartlarıyla ilgili bilgiler



Elde edecekleriniz:

Kaspersky Analist'e Danış, Kaspersky Tehdit İstihbaratı portföyümüzü tamamlar. Bu hizmet sayesinde, karşılaştığınız veya ilgilendiğiniz belirli güvenlik açıkları ve tehditler hakkında destek ve faydalı bilgiler için uzmanlarla iletişime geçebilirsiniz. Bu bilgileri kullanarak hem bir bütün olarak şirketinizi hem de endüstriyel altyapınızı hedef alan tehditlere karşı savunmanızı güçlendirebilirsiniz.

Temel Avantajlar

Kaspersky ICS CERT'teki endüstriyel güvenlik uzmanları da dahil önde gelen tehdit istihbaratı uzmanlarına ulaşma imkanı

Etkili araştırmalar için kişiselleştirilmiş ve detaylı bağlam bilgisi

Uzmanlarımızdan, tehdit ve güvenlik açıklarına nasıl hızlı müdahale edebileceğinize dair ayrıntılı yönergeler

Bize Ulaşın Hizmet hakkında detaylı bilgi

Siteyi ziyaret et

Kaspersky Güvenlik Farkındalığı

BILGI

Siteyi ziyaret et

Kaspersky ICS CERT Uzman Eğitimleri

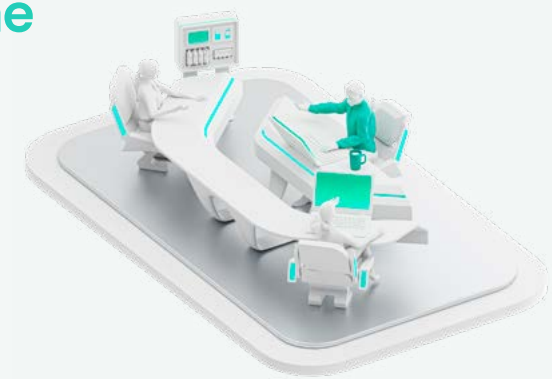
BILGI

Çalışanların siber güvenlik bilgilerini artırma

- Çalışanlarınızı endüstriyel siber güvenliğin en önemli yönleri hakkında gerekli bilgilerle donatarak kuruluşun tüm düzeylerinde farkındalığı artıran eğitim malzemeleri
- Kaspersky Interactive Protection Simulation — farklı sektörler arasında çok sayıda senaryoyu içeren oyun tabanlı iş simülasyonu aracılığıyla eğitim: Termal Güç, Hidroelektrik Güç, Petrol ve Gaz, Petrokimya, Petrol holdingleri vb.
- Kaspersky Automated Security Awareness Platform (ASAP) — siber güvenli davranışları teşvik etmek için tasarlanmış etkileşimli öğrenme modülleri ve kimlik avı saldırısı simülasyonları

Uygulamalı öğrenme

ICS eğitim programımız bilgi teknolojisi (BT), operasyon teknolojisi (OT) ve bilgi güvenliği (IS) profesyonellerinin ve yöneticiler ile diğer çalışanların endüstriyel siber güvenlik hakkında bilgilerini geliştirebilecekleri ve özelleştirilmiş uygulamalı beceriler kazanabilecekleri bir şekilde özel olarak tasarlanmıştır.



Kapsanan başlıca konular

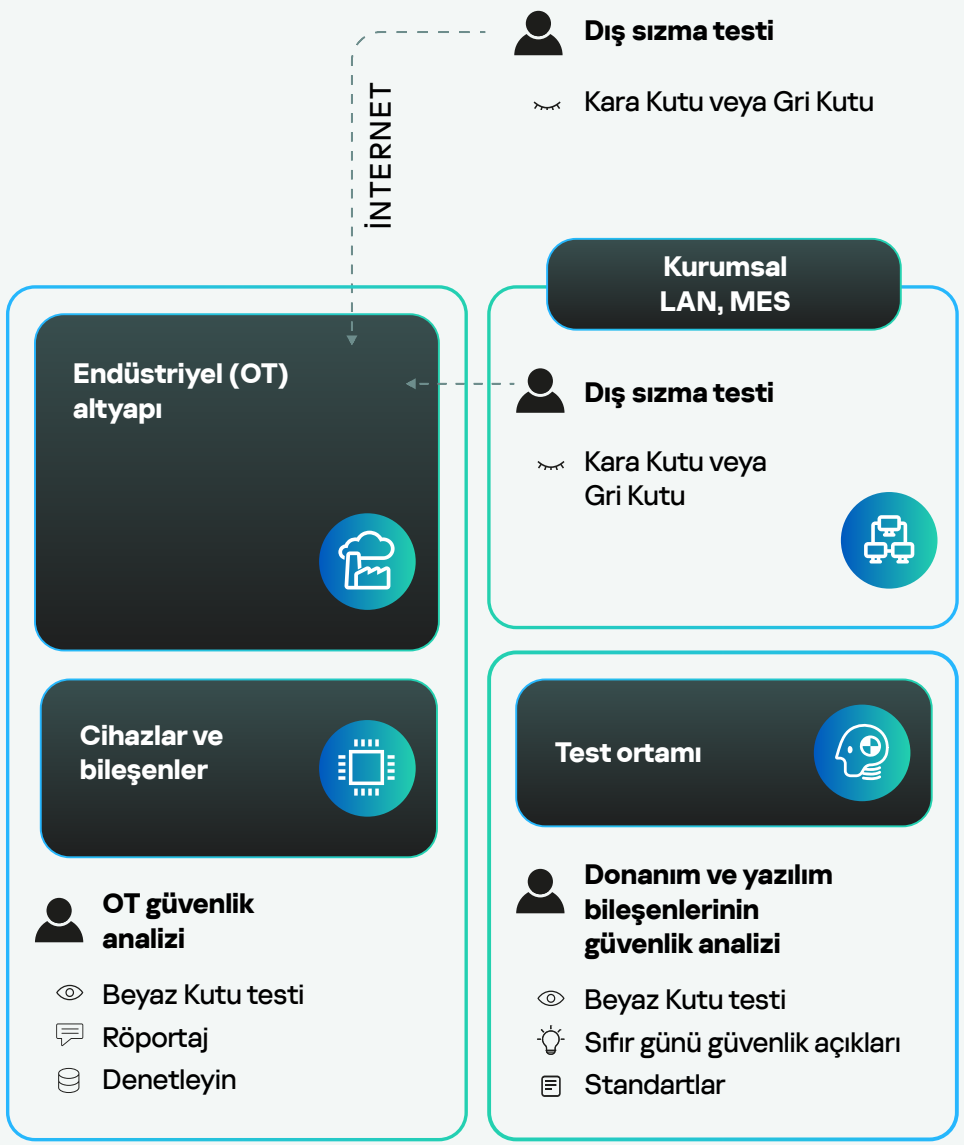
- E-posta
- Web siteleri ve internet
- Parolalar ve hesaplar
- Sosyal medya ve mesajlaşma uygulamaları
- Endüstriyel siber güvenlik
- Bilgisayar Güvenliği
- Mobil cihazlar
- Gizli veriler
- Banka kartı güvenliği ve PCI DSS
- GDPR

Kaspersky uzmanlarından pratik beceriler

- Adli bilişim ve olaya müdahale
- OT/IoT cihazlarında ve endüstriyel yazılımlarda güvenlik açıklarını keşfetme
- BT, OT ve IS uzmanları için işlevler arası eğitim programları

Bize Ulaşın Hemen Deneyin Eğitim Kataloğu

Bize Ulaşın Eğitim Kataloğu



Siteyi ziyaret et

Kaspersky ICS Güvenlik Değerlendirmesi

UZMANLIK

Endüstriyel altyapınızın güvenlik analizi

Aşağıdakiler dahil endüstriyel altyapılardaki güvenlik açıklarını ve zayıf noktaları belirlemeye yönelik kapsamlı bir yaklaşım:

- Saldırı yüzeyi
- Endüstriyel ağ altyapısı, DCS ve endüstriyel cihazların güvenlik düzeyi
- Kritik sistemlerin güvenliğinin aşılmasının riskleri

Kritik bileşenleri kontrol etme

- Endüstriyel protokoller dahil ağ trafiği
- İşlem kontrol bileşenleri: SCADA, PLC, akıllı sayaçlar vb.
- Otomatik işlem kontrol sisteminin fiziksel öğeleri
- ACS ağları dahil ağ altyapısı

Hizmet hakkında detaylı bilgi Bize Ulaşın

Siteyi ziyaret et

Kaspersky Managed Detection and Response

UZMANLIK

Temel Özellikler

- Proaktif tehdit algılama: patentli saldırı göstergeleri kontrol sistemindeki algılanmamış tehditleri izlemeye yardımcı olur
- Otomatik ve kılavuzlu yanıt (isteğe bağlı tam adli delil araştırma ve kötü amaçlı yazılım analizi kullanılabilir)
- ICS siber güvenlik uzmanlığı: sektörün en başarılı ve deneyimli proaktif tehdit algılama ekiplerinden biri tarafından desteklenir

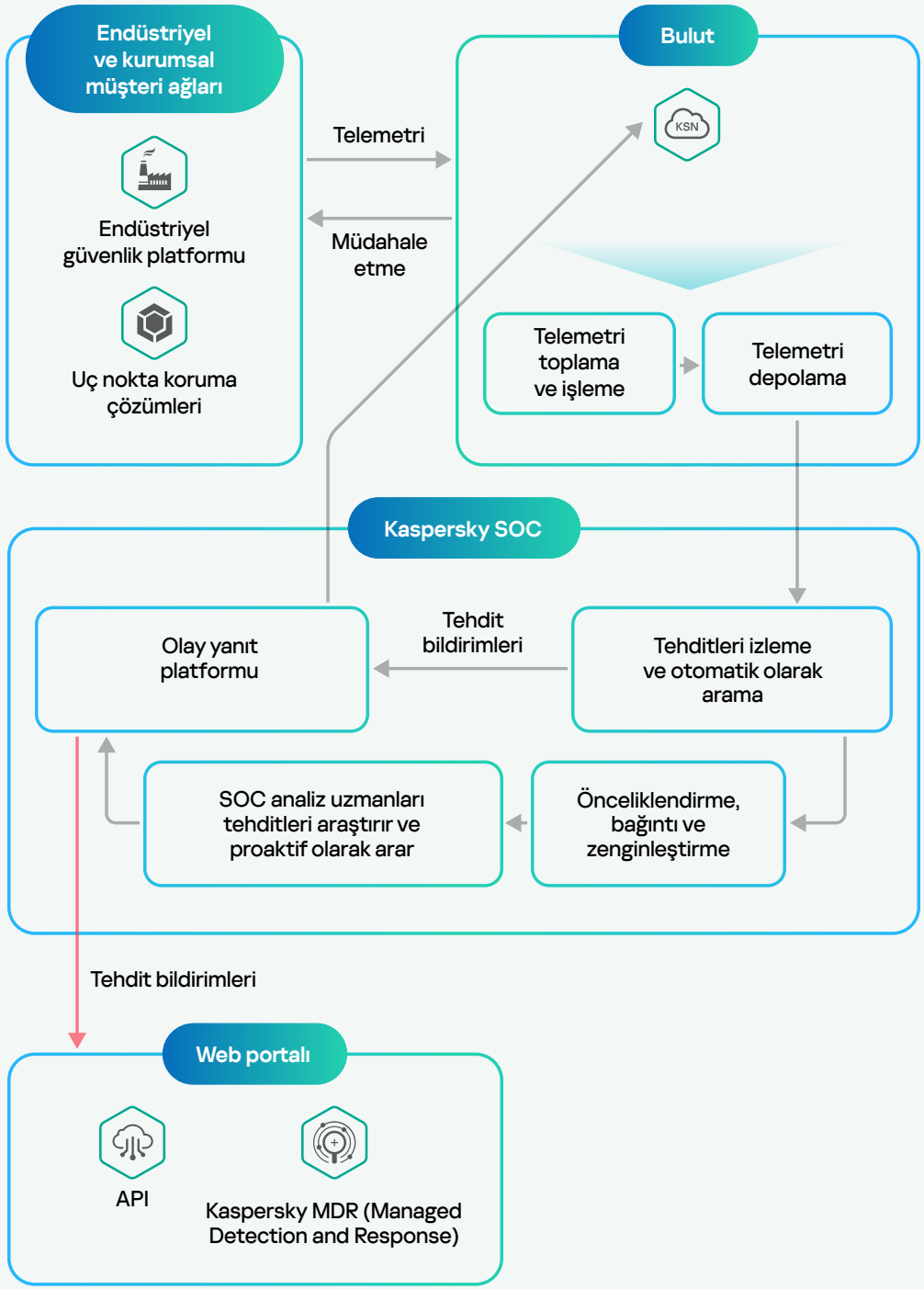
Elde edecekleriniz:

- Endüstriyel kuruluşunuzu hedefleyen tehditlerin sürekli olarak araştırılması, algılanması ve yok edilmesi
- Yeni siber güvenlik uzmanlarını işe alma ihtiyacını ortadan kaldırarak güvenlik maliyetlerini azaltma
- Şirket içinde bulundurmak zorunda kalmadan SOC'nin tüm temel avantajları

Korunan müşterilerimizin %25'i endüstriyel sektörlerdendir

Daha fazla bilgi edinmek için MDR raporuna bakın

Bize Ulaşın Hizmet hakkında detaylı bilgi



Siteyi ziyaret et

Kaspersky Incident Response

UZMANLIK

Olaylara müdahale etme

Risk

Siber suçluların endüstriyel sistemlerin tamamını ele geçirmesi için bir güvenlik açığı yeterlidir

Çözüm

- Kaspersky Küresel Acil Durum Müdahale Ekibi tarafından olay sonuçlarının hızla ortadan kaldırılması
- Olayın nedenlerinin, kaynaklarının ve sonuçlarının analizi
- Kullanılan kötü amaçlı yazılımın ayrıntılı görünümü
- Kaspersky ICS-CERT tarafından ek destek

Hizmet bileşenleri

Olay yanıtı:
Tehditlerin araştırılması ve yok edilmesi

Dijital adli delil:
Dijital kanıtın analizi

Kötü amaçlı yazılım analizi:
Bir saldırıda kullanılan dosyaların ayrıntılı görünümünü alın

Kaspersky ICS-CERT IR Kılavuzu'nu sipariş edin

Daha fazla bilgi edinin

Bize Ulaşın

Kaspersky Küresel Acil Durum Müdahale Ekibi (GERT) araştırmasında IR eğilimlerini keşfedin.

Güvenebileceğiniz bir iş ortağı

- 26 yıllık birinci sınıf deneyim ve petabaytlarca tehdit verisi
- 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

OT ekosistemi hakkında daha fazla bilgi

BT ekosistemi hakkında daha fazla bilgi

İletişim