

Kaspersky OT CyberSecurity

Siber-fiziksel sistemlerin dayanıklılığı için
özel olarak tasarlanmış entegre çözüm





Kaspersky OT CyberSecurity

Deneyimin dayanıklılık
sağladığı yer



Endüstriyel teknolojiler

Güçlü endüstriyel güvenlik çözümleri –
test edilmiş, standartlara uygun
ve onaylanmış



Uygulamaya yönelik bilgi

Güvenilir tehdit analizi ve kapsamlı
endüstriyel siber güvenlik eğitimleri



Sahada kanıtlanmış uzmanlık

Sağlam ve bütünsel bir yaklaşım
için eksiksiz profesyonel hizmet
yelpazesi siber güvenlik



Kaspersky Next
XDR Expert

BT - OT Yakınsaması

IT XDR

Teknolojiler

Özel
Çözümler



Kaspersky
Antidrone



Kaspersky
Machine Learning
for Anomaly Detection



Kaspersky
SD-WAN



Kaspersky
Industrial
CyberSecurity

Native OT XDR



for Nodes

Endpoint protection,
detection and
response



for Networks

Network traffic
analysis, detection
and response

Kaspersky İşletim
Sistemi Çözümleri



Kaspersky
Thin Client



Kaspersky
Automotive
Secure Gateway

Bilgi

Siber
Hijyen



Kaspersky
Security
Awareness

Tehdit
İstihbaratı



Kaspersky
ICS Threat
Intelligence

Eğitim



Kaspersky
ICS CERT
Training

Uzmanlık

Bulma



Kaspersky
ICS Security
Assessment

Yanıt



Kaspersky
Incident
Response

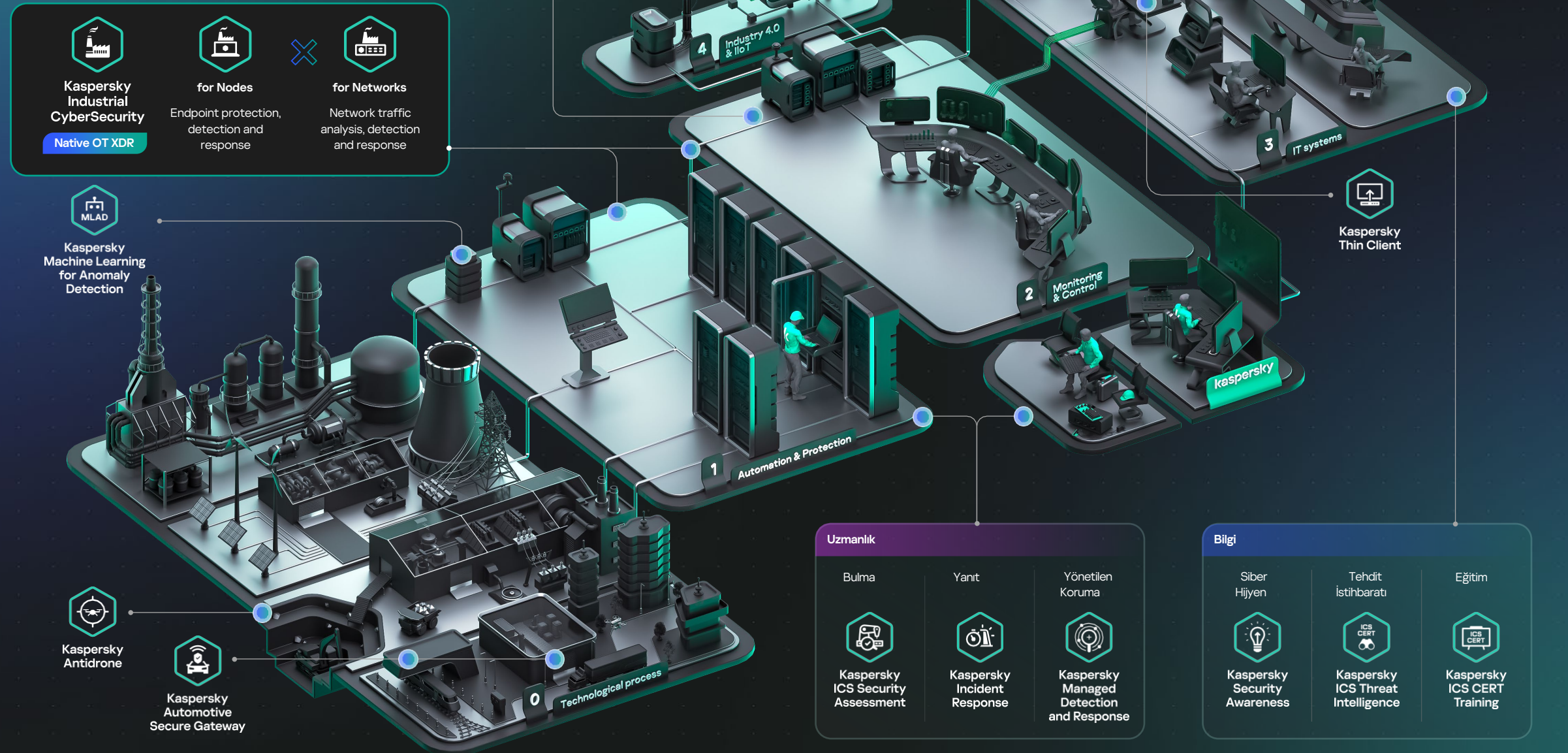
Yönetilen
Koruma



Kaspersky
Managed
Detection
and Response

Kritik öneme sahip sistemler için eksiksiz koruma

Kritik öneme sahip sistemler için eksiksiz koruma





Kaspersky
Industrial
CyberSecurity

360° durum farkındalığı ve risk maruziyetinin kontrolü

- **Varlık envanteri ve ağ görünürlüğü.** Bağlı tüm cihazları ve yapılandırmalarını takip edin. Bir ağ grafiği oluşturun ve veri akışlarını analiz edin.
- **Tehdit ortadan kaldırma.** Ana bilgisayarlar ve ağlar genelinde tehditleri tespit edin ve azaltın, bunun için temel nedenlere ilişkin bilgiler ve güvenli müdahale önlemlerinden yararlanın.
- **Risk değerlendirme.** Güvenlik açıklarını değerlendirin ve ana bilgisayarların, ağ cihazlarının ve kontrolcülerinin güvenlik ayarlarını izleyin

Önemli avantajlar



200'den fazla endüstriyel otomasyon sistemi ve cihazıyla test edilmiş ve kanıtlanmış uyumluluk



Kritik altyapılar için özel olarak tasarlanmış, çok sayıda sorunu çözen ve sorunsuz bir şekilde entegre edilmiş OT XDR platformu



Sistem performansını veya işlem sürekliliğini etkilemeyen, az yer kaplayan bir çözüm



KICS ve temel teknolojileri,
sektörün önde gelen denetimlerine tabidir



ISA/IEC 62443-4-1



SOC 2 Type 2



ISO/IEC 27001



GB 42250-2022



Kaspersky Next XDR Expert

İřletmenizin endüstriyel ve kurumsal bölümlerinde uçtan uca koruma

Kaspersky Next XDR Expert ile yakın entegrasyon sayesinde, Kaspersky Industrial CyberSecurity platformu, üçüncü taraf çözümlerle etkileřimlerin yanı sıra gelişmiş araştırma ve müdahale yeteneklerini de içeren yeni senaryolar sunar. Bu entegrasyon, endüstriyel ve kurumsal ortamların kesiřtięi noktalarda iřletmenizi korumaya yardımcı olur.

Güvenlik ekipleri, bir olayın seyrine ilişkin bütünsel bir bakış açısı elde eder ve gelecekte benzer olayların yaşanmasını önlemek için olayın temel nedenlerini belirler.

Önemli avantajlar

-  Birleřtirilmiş, varlık yoğun BT/OT/IoT altyapıları için güvenlik ve veri egemenlięi
-  Kaspersky ürün yelpazesi genelinde yerel uyumluluk, kusursuz ve benzersiz bir entegrasyon sağlar

Veri kaynakları

Kaspersky çözümleri

Üçüncü taraf

xFlows

Etkinlikler

Entegrasyonları



Kaspersky Anti Targeted Attack
NDR Enhanced



Kaspersky Threat Intelligence



Kaspersky Managed Detection and Response

ve talep üzerine daha fazla Kaspersky veya üçüncü taraf entegrasyonu

Kaspersky Next XDR Expert

Açık Tek Yönetim Platformu

Endpoint Detection and Response

Araştırma grafik

Tehdit algılama ve çapraz korelasyon

Günlük yönetimi ve veri gölü

Panolar ve raporlama

Kitapçıklar

Vaka yönetimi

Merkezi varlık yönetimi

Üçüncü taraf

Dağıtım araç seti

Veri Yanıt

Sandbox, e-posta ve hibrit güvenlik ile EDR

Güvenlik Farkındalıęı, Sanal Ortam, E-posta ve hibrit bulut güvenlięi



Kaspersky Automated Security Awareness Platform



Kaspersky Security for Mail Server



Kaspersky Hybrid Cloud Security



Kaspersky Sandbox



Kaspersky Machine Learning for Anomaly Detection

Anomalilerin erken tespiti ve öngörüsöl analiz

- Ekipman arızalarını ve insan hatalarını kritik duruma ulaşmadan önce algılayarak hataları ve kazaları önlemeye yardımcı olur
- Özel bir saldırı veya sabotajı işaret edebilecek olağandışı çalışan davranışlarını veya ekipman kullanımlarını tespit eder.
- Siber-fiziksel sistemlerin çalışmasında, çok sayıda işlem parametresindeki küçük sapmaların yol açtığı, tespit edilmesi zor anormallikleri belirler.

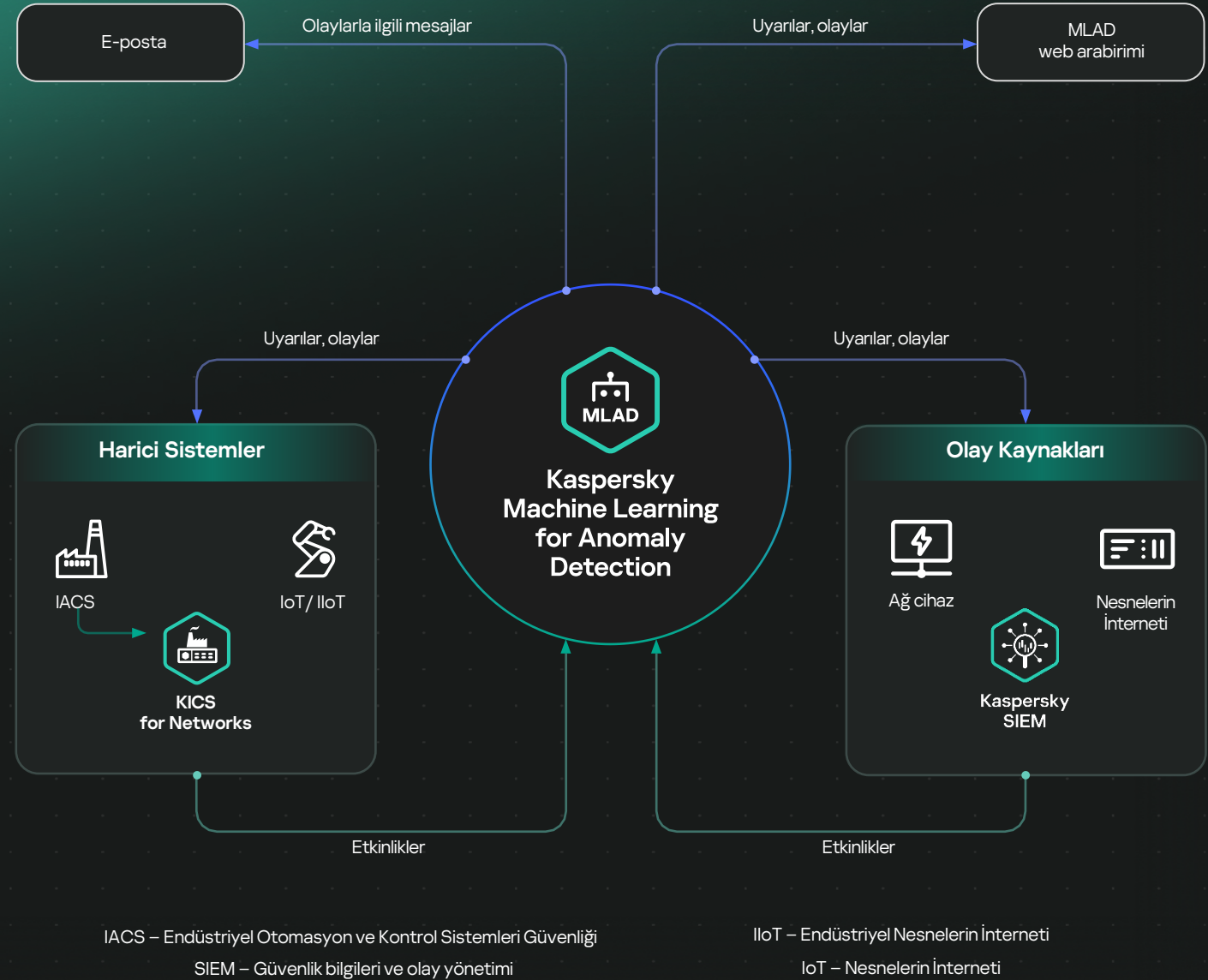
Dış sistemlerle entegrasyon



Kaspersky MLAD, KICS for Networks'ten ağlar, endüstriyel otomasyon sistemleri ve IoT/IIoT cihazlarına ilişkin işlem telemetri verilerini alır



MLAD olay işleyicisi, SIEM sistemleri, IIoT ve ağ cihazları gibi harici kaynaklarla CEF mesajları alışverişinde bulunur





Kaspersky Industrial CyberSecurity, endüstriyel trafiği toplamak, merkezi izleme sağlamak ve dağıtık endüstriyel nesneleri ve sistemleri korumak için SD-WAN altyapısının kullanımını destekler.

Önemli avantajlar



Kolay ölçeklenebilirlik



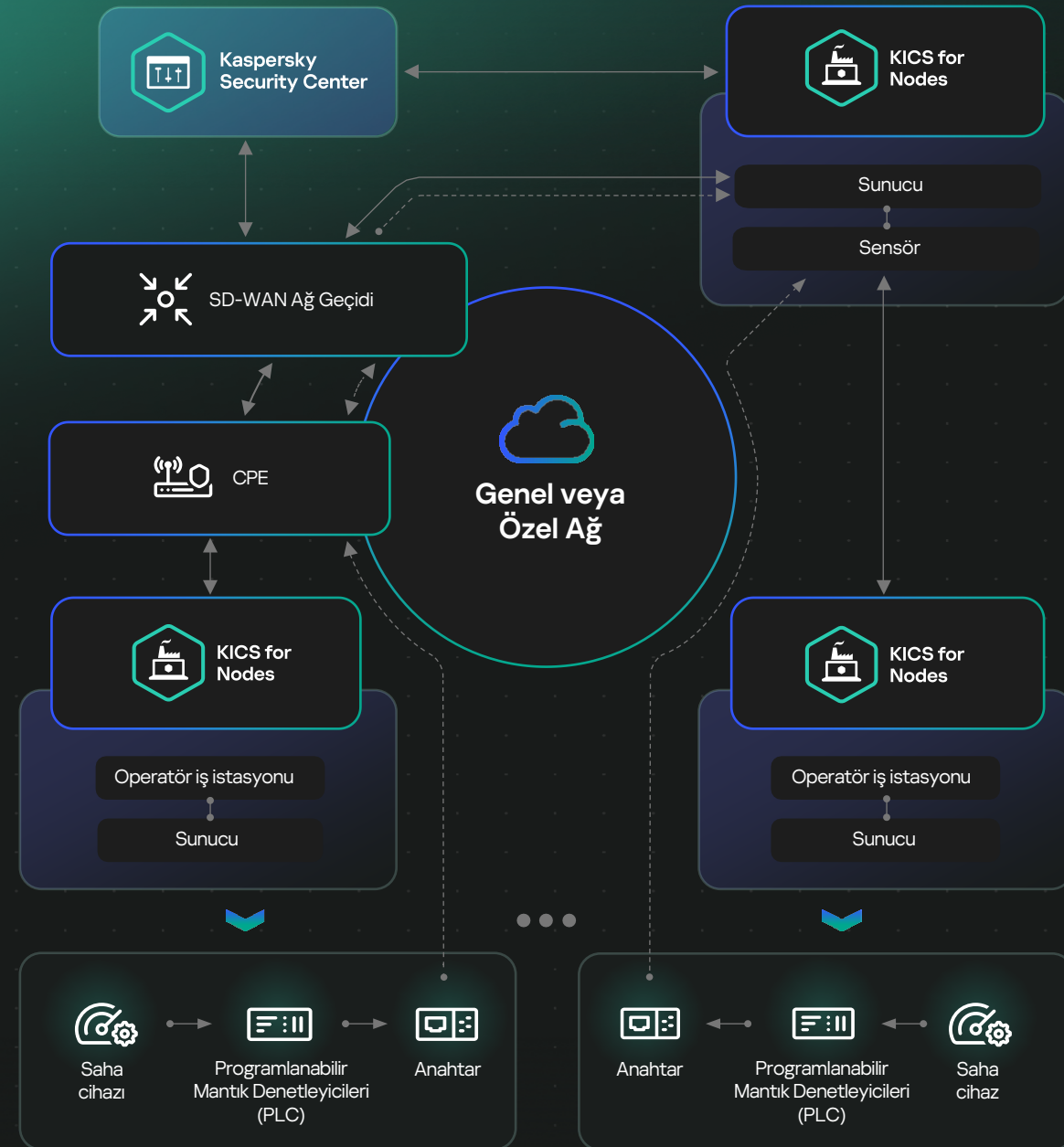
Maliyet optimizasyonu



Kolay yönetim



Merkezi güvenlik



---> SPAN → Ağ trafiği; Düğüm telemetri; Kontrol

**Kaspersky
Antidrone**

Drone izleme ve savunması

Kaspersky Antidrone, yetkisiz drone'ların tesis alanına girmesini engelleyerek endüstriyel işletmelerde üretim kesintisi riskini azaltmaya yardımcı olur. Sistem hava sahasını otomatik olarak tarayarak drone'ları algılar ve sınıflandırır. Gerçekleşen olaylar hakkında bilgiler web arabiriminde görüntülenir. Bir olay durumunda ve izin verilen yerlerde, operatörler drone'u etkisiz hale getirebilir.

Kaspersky Antidrone, her büyüklükteki endüstriyel tesiste kurulabilen modüler bir çözümdür. Ayrıca, "dost ya da düşman" modunu da destekleyerek, kuruluşların kendi drone'larını müdahaleye maruz kalmadan kullanmalarına olanak tanırken, yetkisiz drone'ların bölgeye girmesini önler.

Önemli avantajlar



Kaspersky Antidrone, farklı üreticilere ait radar, RF tarayıcıları, kameralar ve sinyal bozucuların tek bir entegre sistemde bir araya getirilip koordine edilmesini sağlar.



Çoklu sensör füzyonu, karmaşık, gürültülü veya görüşün kısıtlı olduğu koşullarda algılama güvenilirliğini önemli ölçüde artırır.



Donanım sensörleri



Radar



Video



RF



Etki azaltma

Diğer türdeki tespit ve önleme cihazları

Yazılım

**Kaspersky
Antidrone**

Web arabirimi



Kaspersky
Thin Client

Güvenli uzaktan ve sanal masaüstü altyapısı

Risk

Kullanıcı iş istasyonları siber saldırılar için en yaygın hedefler arasındadır

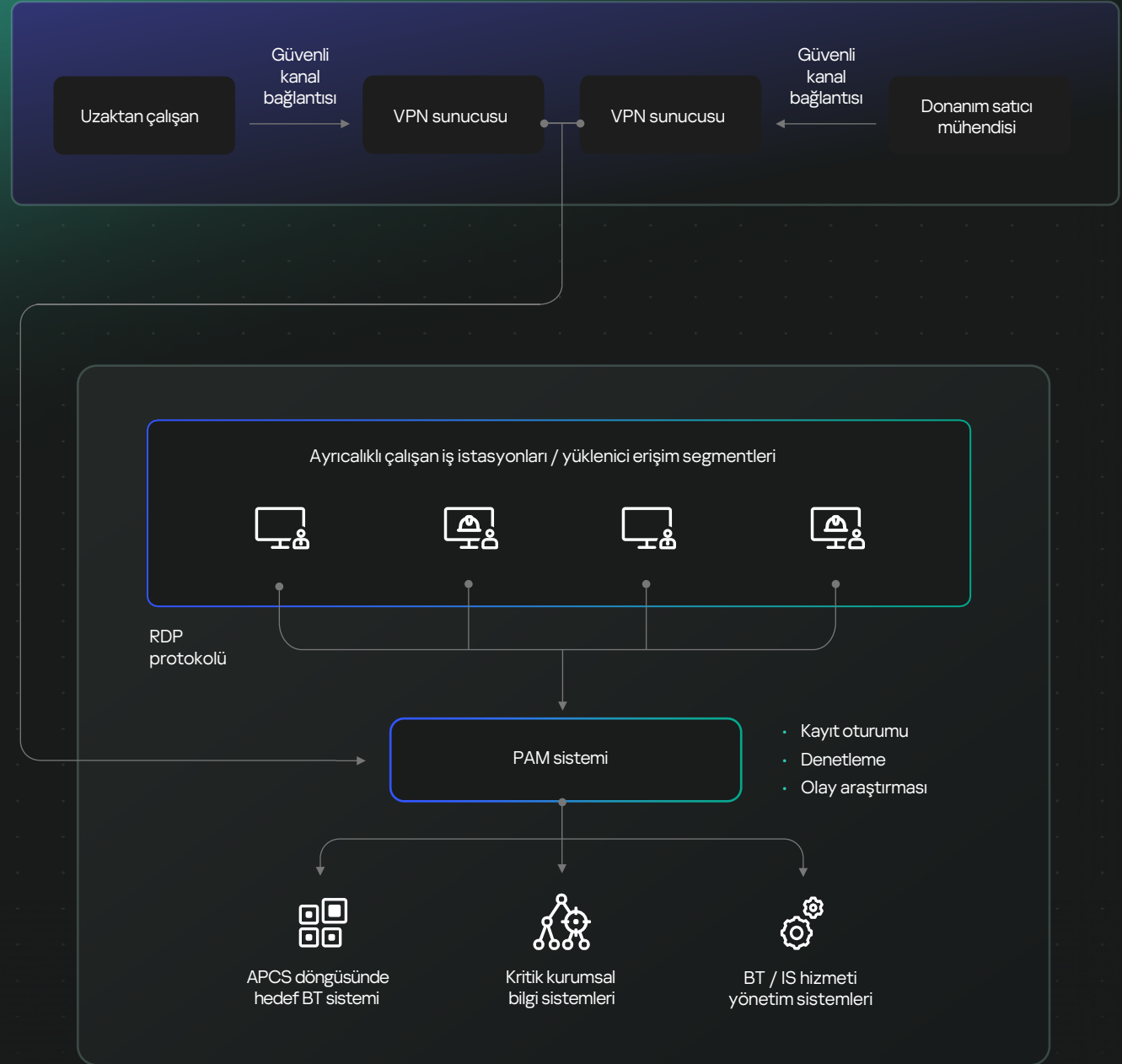
Çözüm

Kaspersky Thin Client, Kaspersky'nin kendi mikro çekirdekli KasperskyOS işletim sistemini temel alan, yönetilebilir ve işlevsel bir ince istemci altyapısı kurmaya yönelik bir çözümdür.

Aktif soğutma sistemi veya hareketli parçalar içermeyen ince istemciler, üretim ortamlarında son derece güvenilir bir performans sunar.

Önemli avantajlar

- Tasarımda Güvenli
- IS ve BT için tek bir yönetim platformu
- Sadece iki dakikada altyapı entegrasyonu





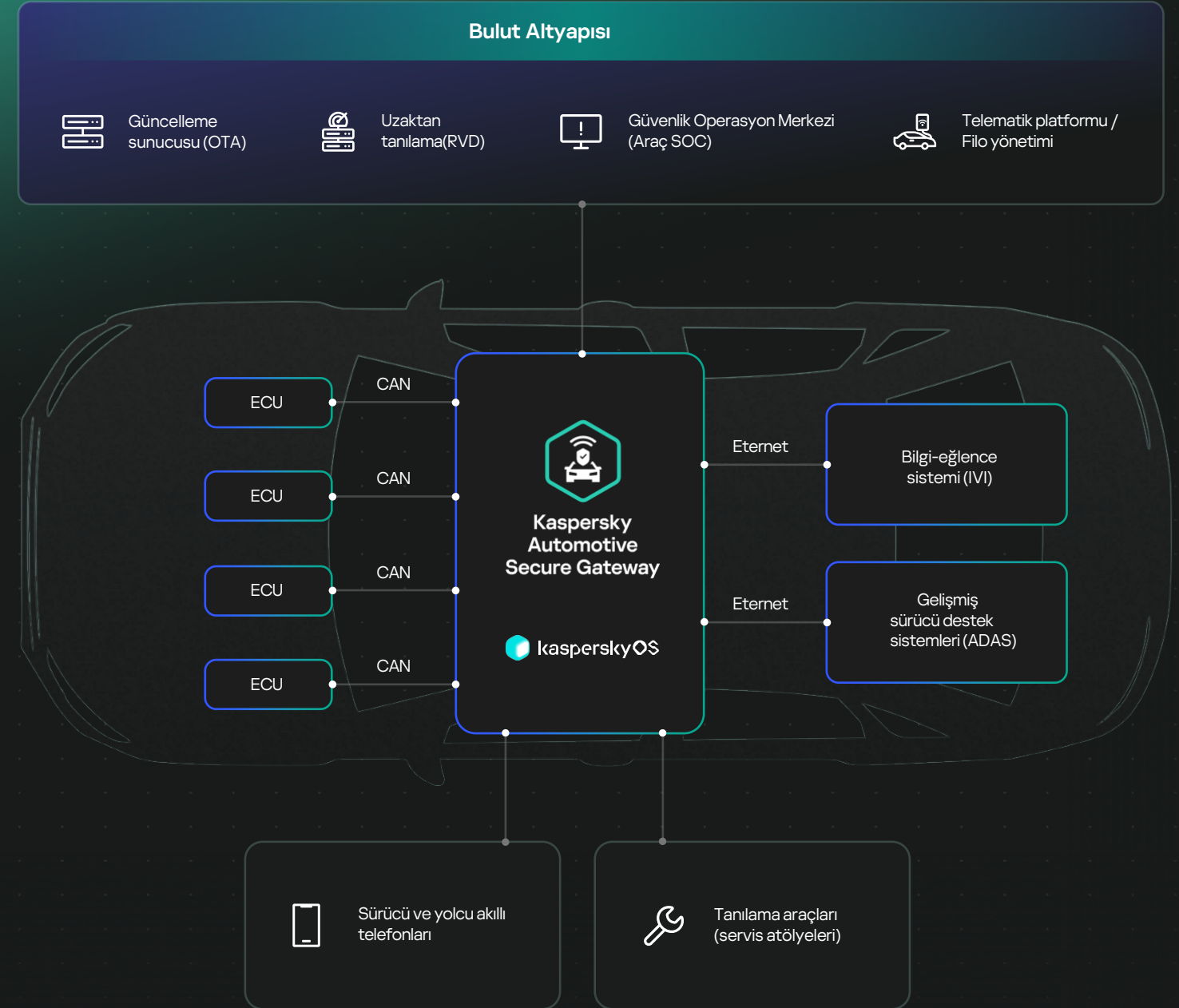
Kaspersky Automotive Secure Gateway

Baęlantılı araçlar için güvenilir BT sistemleri oluşturmak

- Baęlantılı araçlar için güvenli yazılım aę geçidi; aynı zamanda telematik kontrol ünitesi (TCU) işlevlerini de yerine getirir
- İşletim sistemi düzeyinde güvenlik
- Araçların siber güvenlięi ve emniyetini sağlamak için en güncel gerekliliklere uygunluk (ISO 26262, ISO/SAE 21434, UN R155, UN R156, Uptane)
- E/E mimarisinin elektronik birimleri arasında ve bu birimler ile baęlı araç bulutu ve arıza teşhis cihazları arasında güvenli ve güvenilir iletişim
- Uzaktan arıza teşhisi, güvenli kablosuz ECU güncellemeleri ve dięer telematik hizmetlerin uygulanması

Önemli avantajlar

- Yüksek bilgi güvenlięi gereksinimleri olan sektörler için benzersiz güvenlik ve siber baęışıklık
- Güvenli bir aę geçidi ile telematik kontrol ünitesinin tek bir çözümde birleştirilmesi, maliyetlerin düşürülmesine yardımcı olur
- Özel iletişim kuralları, hücresel trafik maliyetlerinin en aza indirilmesine yardımcı olur





Kaspersky ICS Threat Intelligence



Endüstriyel siber güvenlik tehditleri ve güvenlik açıklarına ilişkin derinlemesine içgörü, etkili risk değerlendirmesi, saldırı tespiti, olay soruşturması ve müdahaleyi desteklemek amacıyla.

Endüstriyel siber güvenlik alanında kurulan ilk özel CERT olan Kaspersky ICS CERT'in eşsiz uzmanlığı ve deneyimi ile desteklenmektedir.

Önemli avantajlar



Hızlı tehdit tespiti ve kapsamlı analiz imkanları sunar



Araştırmalarda daha fazla etkinlik ve proaktif Tehdit Avcılığı



Bilgiye dayalı kararlar almak için kapsamlı tehdit ve güvenlik açığı bilgileri

Kaspersky Threat Intelligence ürünleri ve hizmetleri

Makine tarafından okunabilir Tehdit İstihbaratı

Kaspersky
Threat Data Feeds ● ○ ICS

Kaspersky
CyberTrace ● ●

Tehdit İstihbaratı Uzman Desteği

Kaspersky
Takedown Hizmeti ●

Kaspersky
Analiste Sorun ● ● ● ICS

● Taktiksel ● Operasyonel ● Stratejik
○ Kaspersky Threat Intelligence Portal üzerinden erişilebilir

İnsan tarafından okunabilir Tehdit İstihbaratı

Kaspersky
Threat Lookup ● ● ○

Kaspersky Dijital Ayak
İzi İstihbaratı ● ● ○

Kaspersky
Threat Analysis ● ○

Sandbox | İlişkilendirme | Benzerlik

Kaspersky Threat
Intelligence Reporting ● ● ● ○

APT | Suç amaçlı yazılım | ICS

Kaspersky Tehdit
Altyapı Takibi ● ● ○

Uzmanlık merkezleri



Kaspersky Küresel
Araştırma ve
Analiz Ekibi



Kaspersky
AI Technology
Araştırma



Kaspersky
ICS CERT



Kaspersky
Tehdit
Araştırması



Kaspersky
Güvenlik
Hizmetleri



● Tehdit Araştırması ● Olay Araştırması



Kaspersky Threat Data Feeds



Kaspersky Threat Data Feeds hizmeti, endüstriyel kuruluşların ağılarını ve sistemlerini siber tehditlere karşı korumalarına yardımcı olmak üzere neredeyse gerçek zamanlı tehdit istihbaratı sağlar. ICS veri akışları, endüstriyel kontrol sistemlerinde istismar edilebilirliği kanıtlanmış, bilinen zararlı dosyalar ve en son bilinen güvenlik açıkları hakkında bilgiler içerir. Bu veriler, bağlam içinde değerlendirildiğinde genel durumu ortaya koymaya yardımcı olur ve “kim, ne, nerede, ne zaman” sorularına yanıt vererek düşmanları tespit etmeyi, daha hızlı kararlar almayı ve etkili bir şekilde müdahale etmeyi sağlar.

Önemli avantajlar



Geliştirilmiş ve hızlandırılmış olay müdahale ve adli inceleme yetenekleri



Güçlendirilmiş güvenlik çözümleri



Hassas verilerin ve fikri mülkiyetin dışarı sızmasını önler

Elde edeceğiniz:

Kaspersky ICS Hashes Veri Akışı

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

No önleme

No algılama

No Araştırma

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

No önleme

No algılama

No Araştırma

OVAL formatta ICS Güvenlik Açığı Veri Akışı

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

No algılama



Kaspersky ICS Intelligence Reporting



Kaspersky ICS Tehdit İstihbaratı Raporlaması, endüstriyel kuruluşları hedef alan kötü amaçlı saldırılar hakkında derinlikli istihbarat ve daha fazla farkındalığın yanı sıra, en yaygın kullanılan endüstriyel denetim 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** üzerinden sunulur ve API aracılığıyla da erişilebilir.

Önemli avantajlar



Kritik varlıkları korumak ve teknolojik süreçlerin güvenliğini ve sürekliliğini sağlamak için bildirilen tehditleri tespit edin ve önleyin



Tespit edilen kötü amaçlı veya şüpheli faaliyetleri Kaspersky arařtırmalarıyla ilişkilendirerek olayları belirli saldırı kampanyalarına bağlayın ve tehditleri tespit edin

Elde edeceğiniz:



APT raporları

Endüstriyel kuruluşları hedef alan yeni APT ve yüksek hacimli saldırılar hakkında raporlar ve aktif tehditlere ilişkin 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



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 açığı analizi ve riski azaltma

Bilgilendirmelerimiz tehditleri belirlemeye ve azaltmaya yardımcı olmak için Kaspersky uzmanlarından eyleme geçirilebilir tavsiyeler sunar.



Kaspersky Ask the Analyst

Kaspersky Ask the Analyst, Kaspersky Threat Intelligence portföyünü tamamlar. Bu hizmet sayesinde, karşılařtığınız veya ilgilendiğiniz belirli güvenlik açıkları ve tehditler hakkında destek ve faydalı bilgiler için uzmanlarla iletişime geçebilirsiniz. Bu bilgileri kullanarak hem bir bütün olarak řirketinizi hem de endüstriyel altyapınızı hedef alan tehditlere karşı savunmanızı güçlendirebilirsiniz.

Önemli avantajlar



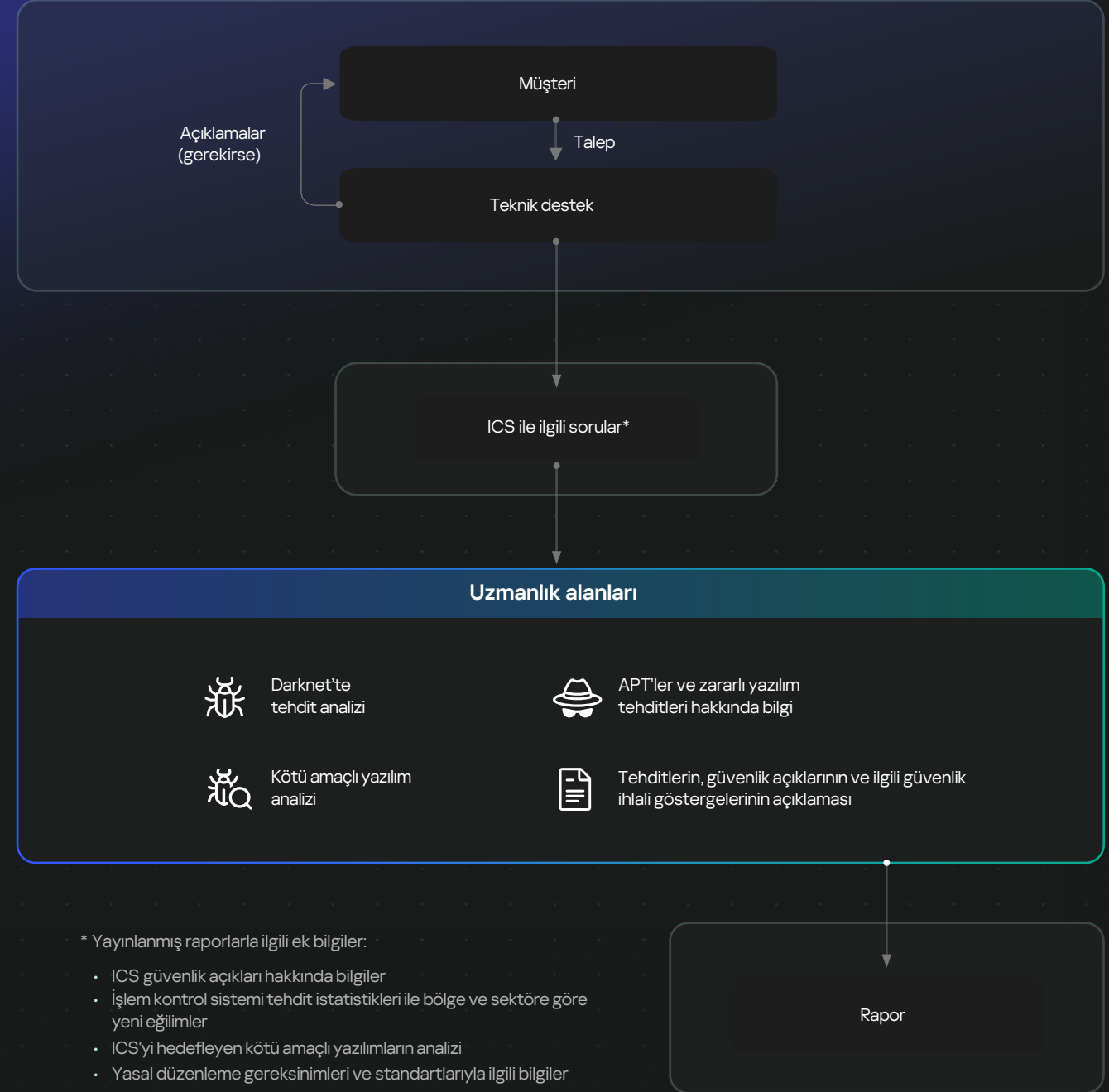
Kaspersky ICS CERT'teki endüstriyel güvenlik uzmanları da dahil önde gelen tehdit istihbaratı uzmanlarına ulaşma imkanı



Etkin soruřtırmalar için kişiselleřtirilmiş ve ayrıntılı bağlamsal bilgiler



Tehditlere ve güvenlik açıklarına hızlı ve etkili bir şekilde nasıl müdahale edileceğine dair uzmanlarımızdan ayrıntılı talimatlar





Kaspersky Security Awareness

Çalıřanları bir insan güvenlik duvarına dönüřtürün

Kaspersky Security Awareness portföyü, kuruluşunuzun her kademesinde güçlü bir siber güvenlik kültürünün oluřturulmasına yardımcı olur:

- **Kaspersky Etkileřimli Koruma Simülasyonu (KIPS)** – endüstriyel senaryolara (enerji üretimi, petrol ve gaz, petrokimya vb.) özel olarak tasarlanmış oyun tabanlı simülasyon. Bu çalıřma, siber güvenliğin iř performansını nasıl etkilediğini ortaya koyarak, yöneticilerin stratejik kararların etkisini somut olarak görmelerini sağlar.
- **Kaspersky Automated Security Awareness Platform (ASAP)** – etkileřimli eğitimler ve simüle edilmiş kimlik avı saldırıları yoluyla tüm çalıřanlar arasında güvenli davranıřlar geliřtirir ve çalıřanlara sektöre özgü siber güvenlik konusunda temel bilgi ve beceriler kazandırır.
- **Kaspersky Yönetici Eğitimi** – karar vericilere ve birim yöneticilerine siber güvenlik ortamını net bir řekilde kavratran pratik bir kurs.

Kapsanan başlıca konular



E-posta



Web siteleri ve internet



Parolalar ve hesaplar



Sosyal medya ve mesajlařma uygulamaları



Endüstriyel siber güvenlik



Bilgisayar Güvenlięi



Mobil cihazlar



Gizli veriler



GDPR



Fiziksel veri güvenlięi



Banka kartı güvenlięi ve PCI DSS



Yapay zeka ve sinir aęları



Kiřisel veriler



Kaspersky ICS CERT Training

Uygulamalı öğrenme

ICS eğitim programımız, BT, OT ve bilgi güvenlięi uzmanlarının yanı sıra yöneticiler ve dięer çalıřanların endüstriyel siber güvenlik konusundaki bilgilerini geniřletmelerine ve bu alanda özel uygulamalı beceriler geliřtirmelerine yardımcı olmak üzere tasarlanmıştır.

Kaspersky uzmanlarından pratik beceriler



Dijital adli delil toplama ve olay müdahalesi



OT/IoT cihazlarında ve endüstriyel yazılımlarda güvenlik açıklarını keřfetme



BT, OT ve IS uzmanları için iřlevler arası eğitim programları





Kaspersky
ICS Security
Assessment

OT ortamlarında siber dayanıklılığın sağlanması

Risk

Siber suçluların bütün bir endüstriyel sistemi ele geçirmeleri için tek bir güvenlik açığı yeterlidir

Çözüm

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

Önemli avantajlar

- Operatörleri, mühendisleri ve diğer personeli korumak için güvenlik önlemlerini güçlendirin
- Hackerların üretim hatlarını, üretim ekipmanlarını veya robotik sistemleri aksatmak için istismar edebileceği güvenlik açıklarını tespit edin
- Üretim tasarımlarını, projelerini ve programlarını hırsızlığa karşı koruyun
- Ürün kalitesini veya güvenliğini tehlikeye atabilecek ihlalleri önleyin

Kaspersky'nin Endüstriyel Güvenlik Değerlendirmesine Yaklaşımı



Dış sızma testi
Kara kutu veya gri kutu

İnternet

Endüstriyel (OT) altyapı

- Ağ mimarisi ve ekipmanları
- Endüstriyel çözümler, iş istasyonları ve sunucular
- Cihazlar ve bileşenler

Cihazlar ve
bileşenler



OT güvenlik analizi

- Beyaz kutu testi
- Saldırı simülasyonu
- Değerlendirme

Kurumsal LAN, MES



İç sızma testi
Kara kutu veya gri kutu

Test ortamı



Donanım ve yazılım bileşenlerinin
güvenlik analizi

- Beyaz kutu testi
- Sıfır günü güvenlik açıkları
- Sertleştirme kılavuzları



Kaspersky Managed Detection and Response

Yapay zeka destekli. İnsanlar tarafından mükemmelleştirildi

- Endüstriyel kuruluşunuzu hedefleyen tehditlerin sürekli olarak araştırılması, algılanması ve yok edilmesi
- Yeni siber güvenlik uzmanlarını işe alma ihtiyacını ortadan kaldırarak güvenlik maliyetlerini azaltma
- Kendi bünyenizde bir SOC kurmanıza gerek kalmadan, bir SOC'nin tüm temel avantajlarından yararlanın

Müşterilerimizin %22'si sanayi sektöründendir

Daha fazla bilgi için [MDR analist raporuna](#) göz atın

Önemli avantajlar



Proaktif tehdit algılama: Patentli saldırı göstergeleri, kontrol sistemi içindeki gizli tehditlerin tespit edilmesine yardımcı olur



Otomatikleştirilmiş ve yönlendirilmiş 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

Telemetri

MDR Cloud

Telemetri

Toplama

İşleme

Depolama

- Büyük Veri
- Yapay Zeka
- Analiz

Kaspersky SOC

İzleme

Tehdit avlama

Önceliklendirme, bağıntı ve zenginleştirme

Olay Müdahalesi Platformu

SOC analistleri tarafından soruşturma

Yanıt

Kaspersky
MDR web
console

Öneriler
ve yönlendirilmiş
müdahale

Erişim

Yanıt

Müşterilerin endüstriyel ve kurumsal altyapısı



Kaspersky
Industrial CyberSecurity
for Nodes

Sunucu

Gömülü sistemler

İş İstasyonu

Gateway



Kaspersky'nin BT altyapısı
için koruma çözümleri

Sunucu

Bilgisayar

Ağ

Sanal makine

Dizüstü bilgisayar



Kaspersky Incident Response

Bir güvenlik ihlalinin ardından ortaya çıkan durumun yönetimi

Risk

Kritik altyapıyı etkileyen olaylar, endüstriyel tesislerde müdahale çalışmalarının yürütülmesi için uygun uzmanlık gerektirir. Yanlış ve zamanında yapılmayan müdahaleler, bir saldırının yol açtığı hasarı önemli ölçüde artırabilir.

Çözüm

- Kaspersky Küresel Acil Durum Müdahale Ekibi tarafından olay sonuçlarının hızla ortadan kaldırılması
- Tüm olay araştırma ve müdahale süreci boyunca destek
- Kendi yenilikçi araçlarımıza dayalı istihbarat, veri toplama ve düzeltme
- Ekiplerinizle anında uzmanlık desteği ve bilgi paylaşımı

Hizmet bileşenleri



Olay yanıtı: Tehditlerin araştırılması ve yok edilmesi



Dijital adli delil toplama
Dijital delillerin analizi



Kötü amaçlı yazılım analizi
Bir saldırıda kullanılan dosyalar hakkında detaylı bilgi edinin

Kaspersky Security Services'in
[küresel raporuyla](#) siber dünyanın yapısını keşfedin



Güvenebileceğiniz bir iş ortağı



30 yıllık birinci sınıf
deneyim ve petabaytlarca
tehdit verisi



ICS CERT - kendi uluslararası
OT/IoT güvenlik
araştırma bölümümüz



BT/OT güvenliği sektöründe
çeşitli ödüller ve başarılarla
kanıtlanmış uzmanlık



Otomasyon tedarikçilerinin
çözümleriyle 200'den fazla
uyumluluk sertifikası



Kanıtlanmış teknolojik etkinlik ve
sektör standartları ile gerekliliklerine
uygunluk



OT ekosistemi
hakkında daha
fazla bilgi

BT ekosistemi
hakkında daha
fazla bilgi

Bize Ulaşın