Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ ● AYDA BİR YAYINLANIR

AĞUSTOS 2026 **SAYI: 157**

FOKUS:
HAVALİMANI GÜVENLİĞİ

KAPAK:
VERİ YEDEKLEME VE DEPOLAMA

ÖGF
ÖZEL GÜVENLİK FEDERASYONU YAYINIDIR

Securitas Technology

securitastechnology.com.tr

Geleceği göremeyiz ama çözümlerimiz ile geleceği koruyabiliriz

İhtiyaçlar değişse de esnek ve adaptif teknolojilerimiz ile her duruma hızlıca uyum sağlıyoruz.

Sunduğumuz teknolojilerle geleceğin güvenliğini şekillendiriyor, dünyanızın daha güvenli hale gelmesine yardımcı oluyoruz.

Farklı bir dünya görüyoruz

GÜVENLİKTEDARİK.com

Son teknolojiye uygun, ürün ve çözümlerden HABERİNİZ VAR MI?

• Elektrik proje taahhüt firmaları • Bayi odaklı çalışan firmalar
• Havalimanları ilgili birimleri • Bankalar ilgili birimleri • İnşaat firmaları
• Oteller ilgili birimleri • Hastaneler ilgili birimleri • AVM'ler ilgili birimleri
• TÜRKLİM Üyeleri • Belediyeler ilgili birimleri • Emniyet Genel Müdürlüğü ilgili birimleri • Zincir mağazalar • Üniversiteler • Mimarlık ofisleri
• Sektör profesyonelleri AĞIMIZA KATILIN

TÜM TÜRKİYE'DE SESİNİZ OLALIM!

✔ CCTV ve video kontrol sistemleri,
✔ Yangın algılama ve ihbar sistemleri,
✔ Yangın söndürme sistemleri,
✔ Geçiş kontrol sistemleri,
✔ Hırsız alarm sistemleri,
✔ Alarm izleme merkezleri,
✔ Apartman konuşma sistemleri,
✔ Mobil takip sistemleri,
✔ Drone teknolojileri

Çok sayıda köklü firmanın çözüm ortağı olmuş ve geleceği tasarlamayı ilke edinmiş bir hizmet ajansı olan ARKHE TANITIM HİZMETLERİ tarafından hazırlanmaktadır. Bünyesinde GÜVENLİK YÖNETİMİ, PERPA GÜNDEM, TECHNEWS ve KURUMSAL YATIRIMCI dergilerini barındıran ARKHE TANITIM HİZMETLERİ; grafik tasarım, kurumsal kimlik çalışmaları, web ve her türlü promosyon ihtiyaçlarınıza fark yaratan tasarım, hız ve müşteriyi koruyan fiyat politikasıyla çözümler sunmaktadır.

Güvenlik Yönetimi
ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ

arkhe tanıtım hizmetleri

www.guvenlikyonetimi.com

OKiSAN®
Güvenlik Teknolojileri San.ve Tic.A.Ş

28 YILIMIZ

Güven Duyduğunuz Her Yerde **BİZ** varız !

alhua
TÜRKİYE DİSTRİBÜTÖRÜ

"Okisan , Güçlü, Güvenli Ürünler Sunar.."
Projelerinize Uygun Çözüm Önerileri

- Covid-19 Ürünleri
- CCTV Çözümleri
- TERMAL Çözümleri
- YANGIN Çözümleri
- MOBİL Çözümleri

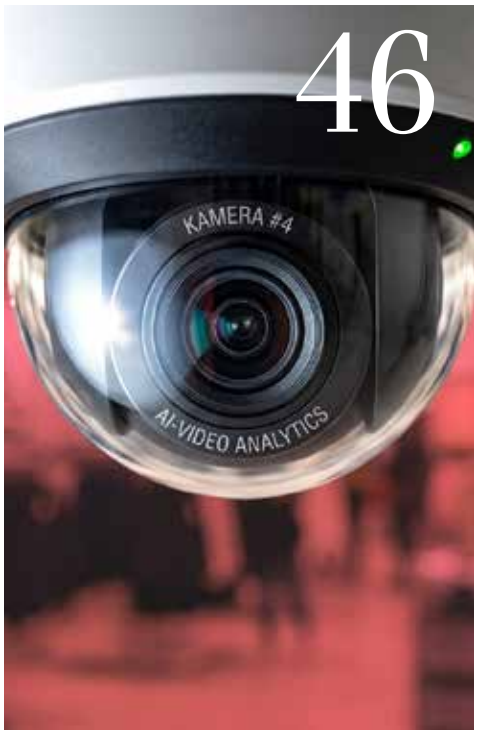
OKiSAN® Güvenlik Teknolojileri San.ve Tic.A.Ş

Okisan Plaza, Mahmut Şevket Paşa mah.
Odesa Bulvarı, Ersan Sok. No:24 Okmeydanı / İST

Merkez 444 1 309
Ankara Bölge 0312 482 40 00
İzmir Bölge 0232 449 15 16

Bizi Sosyal Medya Hesaplarımızdan Takip Edin !

içindekiler



4 BAŞKAN

6 EDİTÖR

8 GÜNCEL
Sektör ile ilgili kısa haberler

18 KÖŞE
Hayata Bakış

SEKTÖRDEN

20 İlgiyle Yönetilen Yaşam Alanlarında Güven ve Konfor: 360° Profesyonel Tesis Yönetimi

KAPAK
VERİ YEDEKLEME VE DEPOLAMA

24 Veri Merkezlerinde Uçtan Uca Erişim Güvenliği

28 Veri Tutan Değil, Karar Veren Sistemler

32 Türkiye'nin veri merkezi kapasitesini 1 GW'a çıkarma hedefi gündemde

FOKUS
HAVALİMANI GÜVENLİĞİ

36 Havalimanı Güvenliğinde Yeni Dönem Akıllı Video Teknolojileri Operasyonların Merkezinde

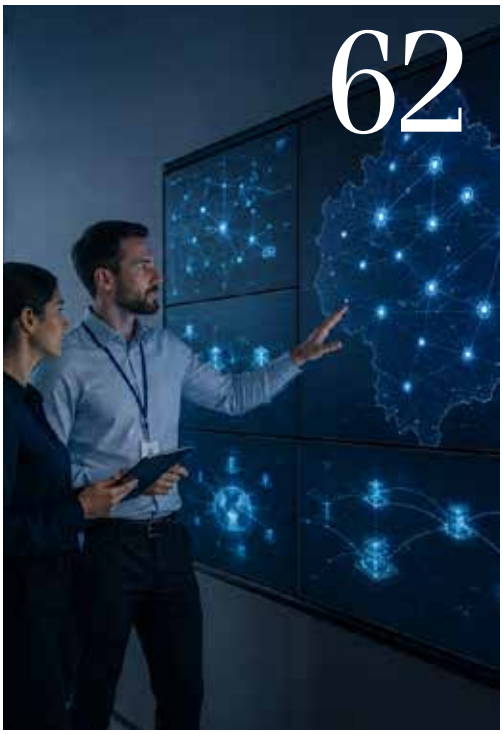
38 Havalimanlarında Güvenlik Fiziki Korumadan Yapay Zekâ Destekli Güvenliğe

Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ

AYDA BİR YAYINLANIR

AĞUSTOS 2026



ELEKTRONİK GÜVENLİK

46 Mağazalar Artık Düşünebiliyor: Tepe Kurumsal'dan Yapay Zeka Destekli Operasyonel Yönetim

46 AI-Powered video güvenliği ile daha güvenli bir ziyaretçi deneyimi

50 AI-Powered video güvenliği ile daha güvenli bir ziyaretçi deneyimi

YANGIN GÜVENLİĞİ

54 Okul kapıları güvenli tahliye için yeterli mi?

57 Elektrikli Araçlarda Yangın Güvenliği Önlemleri

BİLGİ GÜVENLİĞİ

60 Kesintisiz Koruma için Ölçeklenebilir Güvenlik Modülleri

62 Egemen Bulut İçin Verinin Yanı Sıra Kontrol de Yerelleşmeli

64 Tanımadığınız Kişilerden Gelen Hediye Tuzağına Karşı 6 Kritik Önlem

66 QR kodlu kimlik avı saldırıları kurumları hedef alıyor

74 EDITORYAL TAKVIM

75 REKLAM İNDEKSİ

Özel Güvenlik Federasyonu adına imtiyaz sahibi
O. Oryal ÜNVER

Yürütme Kurulu
O. Oryal ÜNVER
İsmail UZELLİ
Murat Kösereisoğlu
Levent GÜLER
Alp SAUL

Genel Yayın Yönetmeni
Devrim BOZKURT
devrim@guvenlikyonetimi.com

Yazı İşleri
info@guvenlikyonetimi.com

Danışma Kurulu
Alp SAUL
Prof. Dr. Gazi UÇKUN
Deniz GÜRKAN
Engin ŞAHİN
Faruk DOĞAN
Hakan ÖZALP
İsmail UZELLİ
Murat Kösereisoğlu
O. Oryal ÜNVER
Yusuf Ziya ÖNCEL

Görsel Yönetmen
Derya BOZKURT
derya@guvenlikyonetimi.com

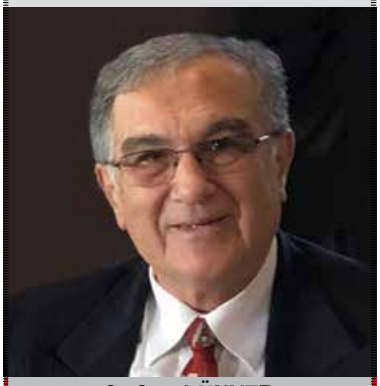
Reklam Müdürü
Nazlı ÇATAK
info@guvenlikyonetimi.com

Yayın Türü
Yerel Süreli Yayın.
Ayda bir yayınlanır.

Yönetim Adresi
Arkhe Tanıtım Hizmetleri
Eyüpsultan - İstanbul
Tel: 0542 250 72 49
0533 413 78 08

Fuarlar fırsat alanlarıdır

Değerli okurlarımız;



O. Oryal ÜNVER
ÖGF (Özel Güvenlik Federasyonu)
Yönetim Kurulu Başkanı

Fuarlar, günlük sosyal ilişkilerin bir parçası olarak fuarlar, birçok olanaklarla doludur.

İlk fuarın nerede ve ne zaman yapıldığı bilinmemekle birlikte, kanıtlar, M.Ö. 500 kadar erken dönemlerde fuarların varlığına işaret etmektedir. Hezekiel kitabında yer alan kutsal yazılar: "Tarshish, tüccarların çeşitliliğinin çokluğu nedeniyle tüccardı. gümüş, demir, teneke ve kurşun, fuarlarda işlem gördüler. " Ezekiel'in, M.Ö. 588 yılında yazıldığı iddia edilen Tire'nin yıkımını açıklaması, Tire'yi önemli bir pazar ve fuar merkezi olarak tanımlamaktadır.

Dini faaliyetin ticarete eşlik ettiği aynı derecede açıktır. Kutsal gün anlamına gelen Latin dünyası "feria", "adil" kelimesinin mantıksal kökü gibi görünür. Dinin ve ticaretin karıştığı bu evrim zamanla devam etti ve Batı Avrupa'ya taşındı. Periyodik toplantılar, takas, takas ve nihayetinde doğrudan satış amacıyla her türlü malın üreticilerini bir araya getirdi. Bu pazara eğlence ve diğer etkinlik biçimleri eklenmiş, böylece bu ilkel pazar bugün bildiğimiz üzere fuarların boyutunu değişirmiştir. Fuarlarda, sergilenen tiyatro grupları, müzisyenler, egzotik hayvanlar ve diğer meraklıların sergilendiği fuarın önemli bir parçasıdır.

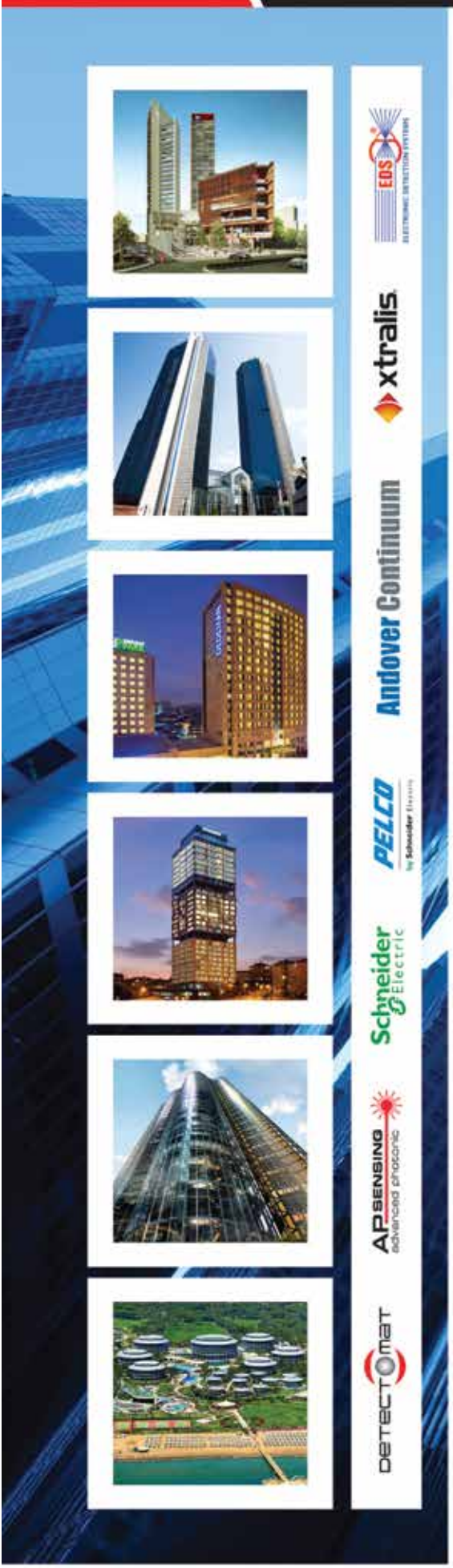
Fuarlar gençlik geliştirme programları gibi eğitim faaliyet alanlarıdır, günümüzde fuarlar artık kariyer fuarları şekline dönüşmüştür. Kariyer fuarları hem iş arayanlar hem de işverenler için eşit fırsat yaratmaktadır. Kariyer fuarları genellikle sizi gitmek istediğiniz yere ulaştıracak kişilere yönlendirir, seçtikleri alanda çalışan potansiyel kişilerle ve başarılı olmak isteyen kişiler için, mükemmel iletişim ağı kurma fırsatıdır.Kariyer fuarlarındaki şirket temsilcileri, iş fırsatları ve işe alım süreçleri hakkında sizi bilgilendirecektir. İşverenlerle ağ oluşturmanın yanı sıra, lisansüstü çalışmalar ve katılım fırsatları hakkında daha fazla bilgi edinebilirsiniz.

Kariyer fuarları seçtiğiniz sektör hakkında genel bilgi edinme şansı sunar. İlgili endüstrideki farklı meslekleri öğrenmek veya hangi sektöre girmek istediğinize karar vermek anlamına gelebilir. İş fırsatları sunan büyük şirketlere kadar çeşitli işletmeleri keşfetmek, doğrudan bağlantı kurmak ve hizmetlerinizi onlara tanıtmak için fırsat alanlarıdır.

Sonuç olarak; gençlerimizin fuarlara vakit ayırmalarını ve mesleki gelişimlerini sağlayabilecekleri ortamdır. Bu ay içinde gerçekleşecek olan, ISAF 2018 Güvenlik Fuarı, güvenlik sektörüne ilgi duyan ve çalışan gençler için güzel bir olanaktır. Dergimizin özel sayısı da bu fuarda sizlerle beraber olacaktır.

İyi şanslar, görüşmek dileğiyle! Aydınlık günler sizin olsun…

"Fuarlar, çeşitli işletmeleri keşfetmek, doğrudan bağlantı kurmak ve hizmetlerinizi onlara tanıtmak için fırsat alanlarıdır."



EOS
xtralis
Andover Continuum
PELCO
Schneider Electric
APSENSING advanced photonic
DETECTOMAT

Akıllı binalar için kalıcı çözümler...

Yangın ve CO Alarm Sistemleri
IP CCTV Sistemleri
Kartlı Giriş Kontrol Sistemleri
Acil Anons Sistemleri
HVAC Mekanik Otomasyon Sistemleri
Enerji Otomasyon Sistemleri
KNX Aydınlatma Otomasyon Sistemleri

Sistemler Arası Entegrasyon

SmartStruxure

Powered by
StruxureWare™ Building Operation

matriks
BİNA KONTROL SİSTEMLERİ

www.matrikstr.com

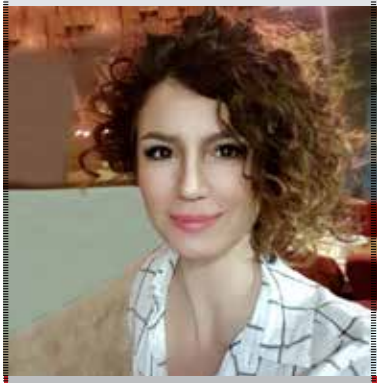
Ataşehir Atatürk Mah. Ekincioğlu Sok. No:21 34758 Ataşehir-Istanbul / Türkiye **Tel:** +90 216 574 91 91 Pbx **Fax:** +90 216 574 95 90 **info@matrikstr.com**

Ağustos 2026 sayımızdan...

Ağustos 2026 sayımızdan merhaba,
Kapak bölümümüzde **VERİ YEDEKLEME VE DEPOLAMA** konusunu işledik. "Dijital dünyada artan veri trafiği, veri merkezlerinin önemini giderek artırıyor. Milyonlarca verinin depolandığı ve işlendiği bu tesislerde, verilerin güvenli bir ortamda saklanması ve altyapının olası tehditlere karşı korunması kritik önem taşıyor." haberimizin devamını sayfalardan okuyabilirsiniz.

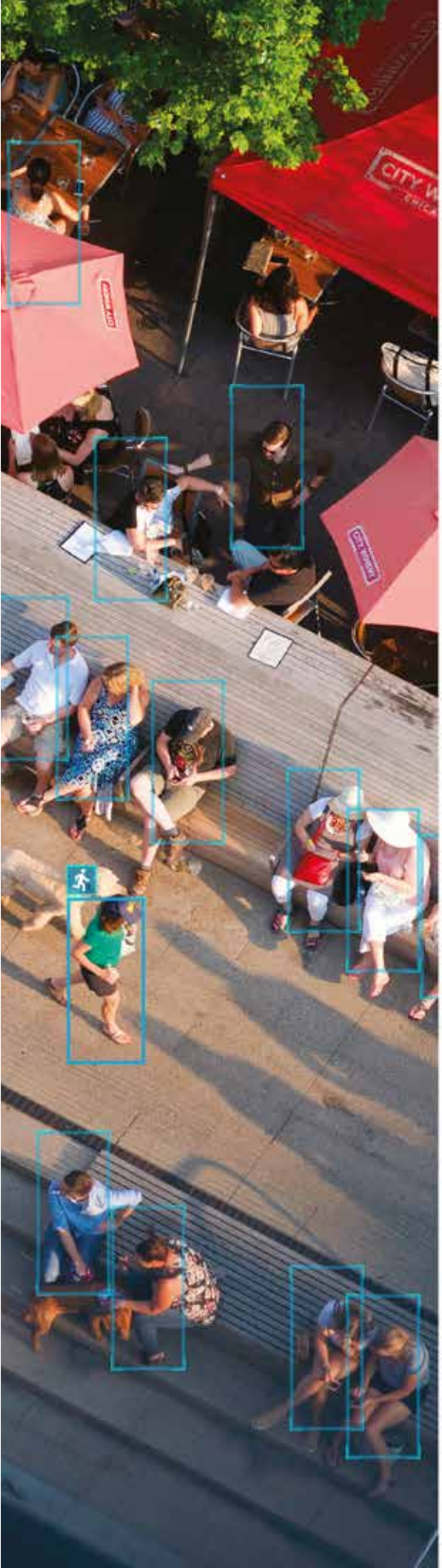
Fokus bölümümüzün konusu ise **HAVALİMANI GÜVENLİĞİ**. Milyonlarca yolcunun, çalışanların, bagajların, kargoların ve operasyonel süreçlerin aynı anda hareket ettiği havalimanlarında güvenlik, tek bir kontrol noktasından ibaret değil. Fiziki çevre güvenliğinden geçiş kontrol sistemlerine, CCTV ve video analitikten X-Ray ve CT tarama teknolojilerine, yangın algılama ve ARFF hizmetlerinden acil durum yönetimine kadar uzanan çok katmanlı güvenlik mimarisi, yapay zekâ ve veri analitiğinin de etkisiyle yeniden şekilleniyor. Havalimanlarının güvenliğini sağlayan bu bütünleşik yapı, tehditleri yalnızca olay gerçekleştikten sonra tespit etmeyi değil, riskleri mümkün olduğunca erken fark ederek önlemeyi hedefliyor.

Keyifli okumalar…



Derya BOZKURT

> “Mutluluk dediğimiz şey, yoğun bir şekilde bastırılmış ve engellenmiş olan ihtiyaçların kısa süreliğine tatmin edilmesinden başka bir şey değildir.”
>
> Freud



Y3K

Gördüğünüze inanın, göremediğinizi ona bırakın

Stadyum, şehir meydanı, deniz ve hava limanı gibi büyük ve kalabalık alanlarda yüksek çözünürlüğe sahip **Avigilon H5 Pro** ile üst düzey izleme ve kayıt yapılabiliyor. Sahip olduğu ileri seviye çözünürlük sayesinde her detayın incelenebilmesine olanak veriyor.

- 61 MP'ye kadar çözünürlük
- Video analiz yeteneği
- Gece görüşü

Detaylı bilgi için bizimle iletişime geçin:
www.y3k.com.tr

Securitas

Pronet'in müşteri odaklı hizmet dönüşümüne 3 Stevie Ödülü!

Pronet, uluslararası iş dünyasının en saygın organizasyonlarından Stevie Ödülleri'nde üç ayrı kategoride dereceye girerek 2 Altın ve 1 Gümüş Stevie Ödülü'nün sahibi oldu. İnteraktif güvenlik sektörünün öncü markası Pronet, müşteri deneyimi ve hizmet kalitesindeki dönüşüm odaklı yaklaşımını uluslararası arenada kazandığı prestijli ödüllerle taçlandırmaya devam ediyor. Marka, iş dünyasının en saygın ödül programları arasında gösterilen, her yıl 60'tan fazla ülkeden binlerce projenin yarıştığı Uluslararası İş Ödülleri (International Business Awards - Stevie® Awards) 2026'dan 2 Altın, 1 Gümüş ödülle döndü.

Pronet'e uluslararası alanda büyük prestij kazandıran "İlk 100 Günü Sahiplenmek: Proaktif İlişkilerle Müşteri Bağlılığı Oluşturmak" projesi, müşteri yolculuğunun en kritik evresine odaklanıyor. Müşteri ilişkilerinin ilk 100 gününe proaktif iletişim ve yüksek memnuniyet anlayışıyla yön veren Pronet, bu yenilikçi modeliyle küresel jüriden tam not aldı. Şirket, "Yeni Ürün & Ürün Yönetimi" kategorisinin "Müşteri Hizmetleri Çözümü" dalında Altın Stevie Ödülü'ne layık görülürken, "Müşteri Hizmetleri" kategorisinde hayata geçirdiği bütüncül vizyon sayesinde "Yılın Müşteri Hizmetleri Dönüşümü" dalında bir diğer Altın Stevie Ödülü'nün sahibi oldu. Pronet ayrıca, kullanıcı odaklı hizmet yaklaşımını "Başarı" kategorisindeki "Müşteri Memnuniyetinde Başarı" dalında kazandığı Gümüş Stevie Ödülü ile tescilledi.

Uluslararası Stevie Ödülleri, 2002 yılından bu yana dünya çapındaki kurum ve kuruluşların en başarılı uygulamalarını, inovasyonlarını ve müşteri hizmetleri dönüşümlerini ödüllendiren en prestijli platformlardan biri olarak kabul ediliyor. Bu küresel organizasyonda elde edilen 2 Altın ve 1 Gümüş derece, Pronet'in sadece Türkiye'de değil, uluslararası standartlarda da müşteri memnuniyetini şekillendiren öncü konumunu kanıtlıyor. Süreçlerin şeffaflığı, kesintisiz teknik destek altyapısı ve proaktif iletişim modelleriyle sektördeki standartları yükseltmeye devam eden marka, kullanıcılarına sunduğu güven odaklı hizmet ekosistemini geliştirmeyi sürdürüyor.

Para ve değerli eşyalarınızın güvenliğine odaklanırken
maliyetinizi azaltıyor,
risklerinizi devralıyor,
zaman kaybınızı önlüyoruz.
0212 603 03 70

LOOMIS

Managing **cash** in society.

Kesintisiz işleyişin anahtarı güçlü siber güvenlik

Günümüzde siber güvenlik ister büyük ister küçük ölçekli olsun her şirketin en stratejik adımları arasında yer alıyor. Siber saldırılar, şirketlere yol açtıkları mali zararların yanı sıra kurumlara itibar kayıpları da yaşatabiliyor. Siber güvenlikte küresel bir lider olan ESET, şirketlerin görünmeyen stratejik gücü olan siber güvenliği mercek altına aldı.

Küresel ekonomik belirsizlikler, jeopolitik gerilimler ve dijital dönüşüm baskısı altında işletmelerin karşılaştığı tehditler giderek artıyor. Siber güvenlik eskiye göre daha iyi anlaşılıyor olmasına karşın doğru adımlar zamanında atılmıyor.

Siber tehditler şirketlerin gündeminde daha fazla yer alıyor

ESET uzmanları siber güvenlik yatırımları ile şirketlerin fikri mülkiyetin ve rekabet avantajının korunmasında, yeni pazarlara açılma ve regülasyonlara uyum alanında; dijital dönüşüm projelerinin güvence altına alınmasında ve güvenli ürünlerle müşteri sadakati ve kârlılığın artırılmasında değer yaratabileceklerinin altını çiziyor.

Siber güvenlik, başarısının genellikle göze çarpmadığı birkaç iş fonksiyonundan biri konumunda. Teknik olayların iş krizlerine dönüşmesini önlemek için tasarlanan, görünüşte sıradan bir dizi süreç ve kontrolü yansıtıyor. Çalıştığında yüzeyde çok az değişiklik olur. Kuruluştaki herkes işini yapar. Yokluğunu ya da sorunları herkes fark ediyor çünkü maliyetler hızla artıyor. Kesintileri önlemek hayati önem taşır ancak bunu yapmanın maliyetini diğer iş öncelikleriyle karşılaştırmak her zaman kolay değil.

Kısıtlı bir güvenlik bütçesiyle idare eden şirketteki yöneticiler, şimdiye kadarki harcamalarının yeterli olduğunu söyleyen deneyimlere sahip olabilir ancak işinizin birkaç yıl boyunca zarar görmemesi, size gelecek yıl hakkında çok az

şey söyler. Güvenlik genellikle istatistikçilerin "şişman kuyruk riski" olarak adlandırdığı şeyi içerir; her şey birdenbire ters gitmeye başlayana kadar her şeyin yolunda olduğu ancak o zaman zararın varoluşsal boyuta ulaşabileceği türden bir risk. Birçok tehdidin gelişmesi ve yasal gerekliliklerin sıkılaşmasıyla zaman içinde olasılıklar iyileşmez; aksine, daha da kötüleşir.Rakiplerin yapamadığı güvenli olmayan bir ortamda güvenli bir şekilde çalışmaya devam etme yeteneği, nadiren ölçülen veya tartışılan bir rekabet avantajıdır.

Tepe Güvenlik'ten Alarm Doğrulama Çalıştayı

Tepe Güvenlik tarafından Antalya'da düzenlenen çalıştayda, alarm izleme hizmetlerinde teknoloji odaklı dönüşüm ve alarm doğrulama sistemleri ele alındı. Kamera, ses analizi ve farklı dedektörlerle desteklenen sistemlerin, gerçek risklerin tespit edilerek ilgili kolluk kuvvetlerine iletilmesindeki rolü değerlendirildi. Güvenlik hizmetlerinde dijitalleşmenin yaygınlaşması, yalnızca özel sektör açısından değil, kamu kaynaklarının daha etkin ve verimli kullanılması açısından da önem taşıyor. Teknoloji destekli alarm izleme ve doğrulama çözümlerinin yaygınlaşmasıyla birlikte, güvenlik operasyonlarında zaman ve kaynak kayıplarının azaltılması ve müdahale süreçlerinin daha etkin hale getirilmesi amaçlanıyor.

Çalıştayda ayrıca 112 entegrasyonu ve asılsız ihbarların azaltılmasına yönelik çözüm önerileri görüşüldü. Teknoloji destekli alarm doğrulama uygulamalarının, güvenlik hizmetlerinde müdahale süreçlerinin daha etkin yürütülmesine ve kamu kaynaklarının daha verimli kullanılmasına katkı sağladığı vurgulandı.


PRONET+
PRONET+
TÜM GÜVENLİK SİSTEMİNİ
TEK UYGULAMADAN YÖNETTİĞİN
EVİNE GÜVEN
PRONET+
Sistem
444 1 911
pronet.com.tr

Securitas Türkiye, Enerji ve Maden Segmenti Liderliği'ne Semih Yağcı Getirildi...

Güvenlik sektörünün önemli oyuncusu Securitas Türkiye'nin Enerji ve Maden Segmenti Liderliği görevine Semih Yağcı getirildi. Enerji sektöründe farklı görevlerde edindiği deneyimle Yağcı, Securitas'ın enerji ve maden sektörüne yönelik güvenlik çözümlerinin geliştirilmesi ve koordinasyonundan sorumlu olacak.

Osmangazi Üniversitesi Makine Mühendisliği Bölümü mezunu olan Semih Yağcı, kariyerine Aksa Jeneratör'de başladı. Sırasıyla Borusan Holding, FG Wilson Türkiye, Aydem Holding gibi enerji şirketleri bünyesinde edindiği 22 yıllık tecrübenin 15 yılı aşkın kısmında tüm Türkiye satış organizasyonu yönetimini üstlendi.

2026 yılının ikinci yarısında Securitas Türkiye ailesine katılan Semih Yağcı, Enerji ve Maden Segmenti Lideri olarak görevine başladı. Yağcı, yeni görevinde enerji ve maden sektörlerinin ihtiyaç ve risklerine yönelik güvenlik çözümlerinin geliştirilmesi, uygulanması ve koordinasyonunu yürütecek.

NETSYS, Opinnate MSSP Programı'na Launch Partner olarak katılan ilk iş ortağı oldu

Opinnate MSSP Programı; bayiler, MSP'ler ve MSSP'lerin firewall güvenlik politikalarını yalnızca işletmekle kalmayıp risk azaltma, sürekli görünürlük, uyumluluk, optimizasyon ve kontrollü otomasyon ekseninde yönetilen servislere dönüştürmesini hedefliyor. Launch, Growth ve Strategic Partner seviyelerinden oluşan yapı, iş ortaklarına müşteri portföyleriyle birlikte büyüyebilecek aşamalı ve sürdürülebilir bir gelişim yolu sunuyor.

Program kapsamında NETSYS, seçilen servis ve ürün kapsamına bağlı olarak firewall politika analizi ve yönetişimi, uyumluluk değerlendirmeleri, optimizasyon, politika yaşam döngüsü yönetimi, otomasyon ve yönetici raporlaması gibi yetkinlikleri paketlenebilir hizmetlere dönüştürebilecek. Merkezi yönetim yaklaşımı ve müşteri ortamlarında konumlandırılabilen Collector bileşenleri, farklı müşteri ortamlarının ayrıştırılarak verimli biçimde yönetilmesini destekleyecek.

Karmaşık firewall politikalarından ölçülebilir güvenlik çıktısına Kuruluşların firewall ortamları büyüdükçe kural hacmi, farklı üretici teknolojileri, değişiklik talepleri ve uyumluluk yükümlülükleri de karmaşıklaşıyor. Bu iş birliğiyle NETSYS müşterileri, seçilen hizmet kapsamına göre aşağıdaki çıktılardan yararlanabilecek:

Sürekli görünürlük: Firewall kurallarının kullanımı, risk durumu ve politika yapısının merkezi biçimde izlenmesi.

Risk azaltma ve yönetişim: Gereksiz, gölgelenmiş, süresi dolmuş, aşırı izinli veya kurum politikalarıyla uyumsuz kuralların belirlenmesi.

Denetlenebilirlik: Uyumluluk kontrolleri, planlı raporlar, değişiklik takibi ve yönetici görünürlüğüyle denetim hazırlığının güçlendirilmesi.

Operasyonel verimlilik: Optimizasyon ve kontrollü otomasyonla manuel iş yükünün, tekrar eden operasyonların ve hata riskinin azaltılması.

Ölçeklenebilir hizmet modeli: Farklı müşteri büyüklükleri ve olgunluk seviyeleri için analizden otomasyona uzanan servis paketlerinin oluşturulması.

securitas.com.tr

Huzurlu bir yaşam arıyorsan...

Daha fazla
bilgi için
QR kodu okutun.

Biz buradayız.

Securitas

Hanwha Vision 16 mK Altı NETD'ye Sahip Ultra Hassas VGA AI Termal Kamera Serisini Piyasaya Sürüyor

Hanwha Vision, yeni VGA AI Tele lens Termal Kamera serisini piyasaya sürdü ve hem kara hem de deniz ortamlarında son derece doğru AI tabanlı algılama sağlamak üzere tasarlanmış yeni nesil bir termal gözetim çözümünü tanıttı. Ultra hassas termal görüntüleme, gelişmiş AI analitiği, görev kritik siber güvenlik ve sağlam dayanıklılığı birleştiren yeni seri, en zorlu koşullarda kritik altyapı, çevre koruma, kıyı izleme ve sınır güvenliği operasyonlarını desteklemek üzere tasarlanmıştır.

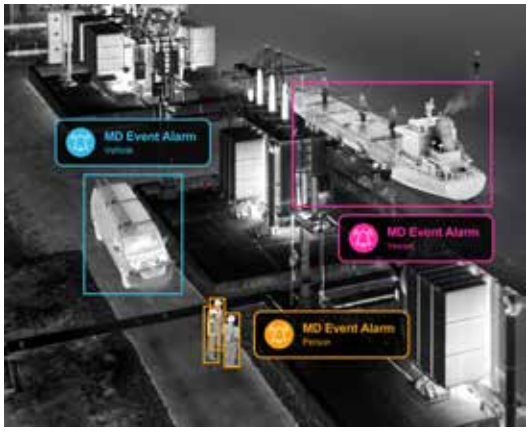
Yeni serinin kalbinde, 16mK'nın altında NETD ile endüstri lideri termal hassasiyet yer alıyor ve kameraların düşük görünürlük ortamlarında bile son derece rafine termal verileri yakalamasını sağlıyor. Bu gelişmiş termal hassasiyet, AI motorunun kısmen gizlenmiş olabilecek insanlar ve araçlar dahil olmak üzere nesneleri daha büyük bir doğrulukla sınıflandırmasına olanak tanır ve çömelmiş veya yere yatmış olabilecek bireyleri de kapsar. Sadece hareket algılamaktan ziyade, kameralar, yüksek riskli ortamlarda yanlış alarmları azaltmak ve durumsal farkındalığı artırmak için gereken termal netlik seviyesini sağlamak üzere tasarlanmıştır.

Geleneksel çevre gözetiminin ötesine geçerek, VGA AI Termal Kamera serisi, deniz ortamları için optimize edilmiş AI-Powered Gemi Algılama yeteneklerini de içerir. Teknoloji, operatörlerin karada insanlar ve araçlar için uygulanan aynı akıllı analitiği kullanarak gemileri doğru bir şekilde algılamasını ve sınıflandırmasını sağlar. Kıyı koruma, liman güvenliği ve deniz sınır kontrolü için tasarlanan sistem, termal görüntüleme teknolojisi kullanarak sis, yağmur, kar ve tam karanlıkta güvenilir performans sağlar. Bu, kuruluşların hava veya aydınlatma koşullarından bağımsız olarak kıyı şeritleri, su yolları ve açık deniz ortamlarında sürekli farkındalık sağlamasına olanak tanır.

Geniş bir operasyonel gereksinim yelpazesini desteklemek için, yeni seri dört lens seçeneği ile sunulmaktadır — 13mm, 19mm, 35mm ve 60mm — dağıtım ihtiyaçlarına göre algılama aralığı ve görüş alanında esneklik sağlar. Ayrıca, her model 30fps yüksek kare hızında veya 8fps versiyonunda sunulmaktadır, bu da müşterilerin bölgesel düzenlemeler ve tedarik gereksinimleri ile uyumlu yapılandırmaları seçmelerine olanak tanır.

Siber güvenlik de yeni platformun temel odak noktası olmaya devam ediyor. VGA AI Termal Kamera serisi, yetkisiz erişim ve siber tehditlere karşı sistemleri korumak için tasarlanmış donanım kökenli şifreleme sağlayan FIPS 140-3 Seviye 3 sertifikalı Güvenli Eleman içerir. SD kart bölme şifrelemesi ile birleştirildiğinde, kameralar hassas gözetim görüntülerini kurcalamaya karşı korumaya yardımcı olur ve kritik kanıtların bütünlüğünü ve güvenilirliğini sağlar.

Zorlu dış mekan kurulumları için tasarlanan seri, IP66/67, NEMA 4X ve IK10 derecelendirmeleri dahil olmak üzere kapsamlı çevresel koruma ile inşa edilmiştir ve MIL-STD-810H uyumluluğu yağmur, nem, titreşim ve tuz



maruziyetine karşı direnci kapsar. Gelişmiş geçici koruma, elektrik dalgalanmalarına ve kararsız güç koşullarına karşı güvenilirliği daha da artırır ve görev kritik ortamlarda kesintisiz çalışmayı destekler.

VGA AI Termal Kamera serisinin lansmanı ile Hanwha Vision, hem kara hem de deniz güvenliği uygulamalarında doğru algılama, akıllı analitik ve güvenilir performans sağlayabilen gelişmiş termal görüntüleme çözümleri sunarak AI odaklı gözetim portföyünü genişletmeye devam ediyor.

Bir bakışta (sadece web sitesi haber merkezi içeriği için)

- Sub-16mK termal hassasiyet ile gelişmiş bir AI motoru, düşük görünürlük koşullarında yanlış alarmları önemli ölçüde azaltmak için insanları ve araçları doğru bir şekilde sınıflandırır.
- Yeni AI-Powered gemi algılama, kıyı şeritleri ve su yollarında tam karanlık veya şiddetli hava koşullarında kıyı ve liman güvenliğine güvenilir izleme getiriyor.
- FIPS 140-3 Seviye 3 şifreleme ve MIL-STD-810H sağlam derecelendirmeler, hassas verileri korur ve en zorlu ortamlarda kesintisiz çalışmayı sağlar.

GÜVENLİK,
DETAYLARI GÖRME SANATIDIR!

Detaylar için
QR kodu okutunuz.

Üretim Alanlarındaki Çalışan Performansı ile Doğal Aydınlatmanın İlişkisi

Fabrikalar, depolar ve lojistik yapılar, alan verimliliği ve iklimlendirme maliyetleri gözetilerek tasarlandığı için çoğu zaman pencere veya çatı ışıklığı bulunmadan inşa ediliyor. Üretim sahalarında gerçekleştirilen hakemli bir araştırma, bu koşulların çalışanlar üzerindeki etkisini sayısal verilerle ortaya koyuyor. Tamamen yapay aydınlatmaya dayalı bölümlerde çalışanların yüzde 68,7'si dikkat kaybı bildirirken, doğal aydınlatmanın ağırlıklı olduğu bölümlerde bu oran yüzde 25,2'de kalıyor. Göz yorgunluğu bildiren çalışanların oranı ise aynı bölümlerde sırasıyla yüzde 60 ve yüzde 35 olarak ölçülüyor.
Form Endüstri Tesisleri, farklı yapı tiplerine uygun doğal aydınlatma sistemleriyle gün ışığının büyük hacimli yapılara daha dengeli yayılmasına destek sağlıyor.
Araştırma, aydınlatma koşullarının operasyonel güvenlik açısından da önem taşıdığını gösteriyor. Tamamen yapay aydınlatmaya dayalı bölümlerde çalışanların yarısı, mevcut aydınlatmanın çalışma sırasında hataya yol açabileceğini belirtiyor. Aydınlatmanın kazaya neden olabileceğini ifade eden çalışanların oranı bu bölümlerde yüzde 41,7'ye ulaşırken, doğal aydınlatmanın ağırlıklı olduğu bölümlerde yüzde 28,3'te kalıyor. Baş ağrısı bildiren çalışanların oranı da yüzde 61,6'ya karşı yüzde 39,4 olarak ölçülüyor. Bulgular, doğal ışığın hassas montaj, kalite kontrol ve makine kullanımı gibi görsel dikkat gerektiren süreçlerde çalışan performansını etkileyebildiğine işaret ediyor.
Gün ışığının yalnızca cephelerden alınması, derin planlı üretim yapılarının iç bölümlerine yeterli düzeyde ulaşmasını zorlaştırıyor. Form Endüstri Tesisleri'nin doğal aydınlatma sistemleri, gün ışığının üst kotlardan iç mekana alınmasını ve alan geneline dengeli biçimde yayılmasını sağlıyor. Sistemde kullanılan yüksek performanslı reflektif kanallar, gün ışığını derin iç hacimlere minimum kayıpla taşıyor. Elektrik enerjisi tüketmeden çalışan sistem, gündüz saatlerindeki yapay aydınlatma ihtiyacını azaltarak enerji tasarrufuna da katkı sağlıyor. Form Endüstri Tesisleri, doğal aydınlatma alanındaki ürün yetkinliği ve uygulama deneyimiyle çalışan konforunu ve yapı performansını birlikte destekleyen çözümler sunuyor.

TEPE
GÜVENLİK

TEPE'DE YENİ DÖNEM

TEPE
KURUMSAL

444 15 98
tepekurumsal.com.tr

"Tenkitlere dikkat"

Oğuz GÜLAY

Çocukların yetenekleri ne kadar erken yaşta fark edilebilir ve desteklenirse şüphesiz o kadar iyi olur. İstemediğimiz durumlarda onların yeteneklerinin önüne set çekmek, çatışmaya girmek yerine olumlu yerlere yönlendirmeye çalışmak daha akılcı ve faydalı olur. Çocuklarımızı sevmedikleri, yapı ve yeteneklerine uygun olmayan şeylere zorlamak çocuklarımıza da bize de fayda sağlamaz.

Çocuğumuzun kusurunu görünce gerektiğinde ikaz ettiğimiz gibi düzelttiğinde de ya da güzel bir şey yaptığında da takdir etmeyi bilmeliyiz ki bize olan güveni artsın ve ikazlarımız etkili olsun.

Yalnız takdirlerimizin gerçekçi olmasına dikkat edelim. Aksi halde çocuğun size olan güveni sarsılır sözlerinizi ciddi bulmaz; kendine olan güveni de kaybolur. Öyleyse övgüde de aşırıya kaçmamak lazım. Sözleriniz doğru olsun. Aşırı övgüler çocuğun ayaklarını yerden kesip sonrasında büyük hayal kırıklıklarına yol açabilir. Tenkitlerde ise meseleyi gerektiğinden fazla büyütür ve hakkı teslim etmezseniz inandırıcılığınızı ve etkinizi kaybedersiniz.

Çocuklar bırakın başkalarıyla; kendi kardeşleriyle bile kıyaslamamalıdır. Çünkü aşağılanan çocukların kendine güvenleri gelişmez. Çocukları birbirleri ile yarış havasına değil birbirlerini destekleyerek birbirleriyle yardımlaşarak hedefe doğru koşu havasına sokun.

Hatalarını mümkün olduğu kadar doğrudan değil dolaylı yollardan belirtmeye çalışın mesela isim vermeden ve kimseyi de zan altında bırakmadan genel konuşabilirsiniz.

Çocuğun anne - baba tarafından devamlı tenkit edilmesi; aşırı sert tepkiler, başkalarının önünde azarlanmalar çocukta aşağılık duygusuna yol açar. Çocuğun kişiliğini değil davranışlarını eleştirin. Ona "sen şöylesin" demektense "yaptığın hareket şöyle" demek daha doğru olur. Bu sayede çocuk hareketleri ve kişiliği arasındaki farkı ayırt etmeyi öğrenir.

"Sen kıskançsın, inatçısın" demekten kaçınıp kıskançlık ve inatçılık üzerinde birlikte düşünmek, çocuğun özgüvenini geliştirmesini doğrudan sağlar. Bu arada çocukların yeteneklerinin toplum içinde; kusurlarının ise yalnızken söylenmesi gerektiğini unutmamalıyız.

Çocuğa "su getir" diye bağırmak ve argo kelimelerle hitap etmek başka, " bana bir su getir" demek başka " bana bir su getirir misin?" demek daha başka, " bana bir su getirir misin yavrucuğum" demek ise çok daha başkadır.

Bunların her biri çocuğun ruhunda ayrı ayrı hisler uyandırır. Belli ya da belirsiz ayrı ayrı tepkilere yol açar. Çocuğun yapılanmasında; şekillenmesinde ayrı bir tuğla ya da harç olur ve maalesef siz bunun belki hiç farkında bile olmazsınız.

Farkında olunabilmesi dileğimle…

"Çocuğun anne - baba tarafından devamlı tenkit edilmesi; aşırı sert tepkiler, başkalarının önünde azarlanmalar çocukta aşağılık duygusuna yol açar. Çocuğun kişiliğini değil davranışlarını eleştirin."

Değişimi birlikte yakalayalım...

Creative Çözümler

Logo Amblem Tasarım

Kurumsal Kimlik Tasarımı

Katalog, Broşür Tasarımı

Ambalaj Tasarımı

Basın İlanı Tasarımı

Broşür ve İnsert

Baskı Çözümleri

Güvenlik Yönetimi
ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ

Gündem

ARKHE TANITIM HİZMETLERİ
Perpa Ticaret Merkezi B Blok
Kat:6 No:672
Okmeydanı / Şişli / İstanbul
Tel : (212) 210 54 45
www.guvenlikyonetimi.com

arkhe
tanıtım hizmetleri

İlgiyle Yönetilen Yaşam Alanlarında Güven ve Konfor: **360° Profesyonel Tesis Yönetimi**

Profesyonel tesis yönetimi; yaşam ve çalışma alanlarındaki operasyonel, teknik, idari ve hukuki süreçleri 7/24 destek, şeffaf iletişim ve sürdürülebilir planlamayla yöneten bütünleşik bir hizmet disiplinidir.

İLGİ GÜVENLİK

Tesis yönetimi artık günlük işlerin ötesinde

Site, rezidans, toplu konut, iş merkezi ve karma yaşam alanlarında yönetim, uzun yıllar boyunca günlük işlerin yürütülmesi ve ortaya çıkan sorunların çözülmesi üzerinden değerlendirildi. Oysa modern yaşam alanlarında küçük görünen bir aksaklık; güvenlikten teknik altyapıya, ortak alan kullanımından bütçe düzenine kadar birçok süreci aynı anda etkileyebilir. Zamanında yapılmayan bir kontrol yaşam konforunu azaltabilir, yeterince açıklanmayan bir karar yönetim güvenini zedeleyebilir. Bu nedenle profesyonel tesis yönetimi, yalnızca görev dağıtan bir hizmet olmaktan çıkarak yaşam alanının düzenini, değerini ve sürekliliğini koruyan stratejik bir yönetim işlevine dönüşür. İLGİ Grup'un yaklaşımı da ilanda vurgulanan "İlgiyle Yönetilen Yaşam Alanları" fikrini sahadaki gerçek ihtiyaçlarla birlikte ele alır.

360° profesyonel tesis yönetimi neyi ifade eder?

"360° Profesyonel Tesis Yönetimi" yaklaşımı, yaşam alanındaki tüm temas noktalarının ortak bir yönetim modeli içinde görünür, ölçülebilir ve takip edilebilir hale gelmesini ifade eder. Bu bütünlük, her işi tek bir ekibin yapması değil; güvenlik, temizlik, teknik bakım, idari işler, mali süreçler ve tedarikçi yönetiminin aynı planın tamamlayıcı parçaları olarak çalışmasıdır. Hangi talebin kim tarafından karşılanacağı, hangi kontrolün ne sıklıkla yapılacağı, hangi hizmetin nasıl raporlanacağı ve hangi durumda yönetime bilgi verileceği netleştiğinde günlük işleyiş kişilere bağlı olmaktan çıkar. Böylece yönetim, yalnızca sorunlara müdahale eden bir yapı değil; ihtiyaçları önceden gören, kaynakları doğru yönlendiren ve hizmet kalitesini sürekli geliştiren bir sisteme dönüşür.

Güven ve konfor aynı yönetim planında buluşmalı

Bir yaşam alanında güven ve konfor birbirinden bağımsız değildir. Kontrollü giriş-çıkış, çalışan teknik

sistemler, temiz ve düzenli ortak alanlar, doğru aydınlatma, erişilebilir yönetim ve zamanında bilgilendirme aynı yaşam deneyiminin parçalarıdır. Güvenlik önlemleri güçlü olsa da teknik aksaklıkların tekrarladığı, taleplerin cevapsız kaldığı veya ortak alanların düzenli yönetilmediği bir yapıda kullanıcı memnuniyeti sürdürülemez. Aynı şekilde yalnızca estetik ve konfora odaklanan, riskleri ve operasyonel sürekliliği göz ardı eden bir yönetim de kalıcı değer üretemez. Profesyonel tesis yönetimi, günlük yaşamı gereksiz prosedürlerle zorlaştırmadan güvenliğin, düzenin ve konforun birlikte korunmasını sağlar; sakinlerin, yatırımcıların ve işyeri sahiplerinin beklentilerini ortak bir yönetim zemini üzerinde buluşturur.

Operasyonel süreçlerin görünmeyen düzeni

Tesis yaşamının kesintisiz ilerlemesini sağlayan çok sayıda günlük operasyon bulunur. Görevli vardiyalarından ziyaretçi ve tedarikçi girişlerine, teslimat düzeninden otopark akışına, temizlik planından ortak alan kullanımına kadar her adım belirli bir koordinasyon gerektirir. Operasyonel yönetim, yalnızca yapılacak işleri sıralamak değil; hizmet standardını tanımlamak, görevleri kontrol etmek, aksaklıkları kayıt altına almak ve tekrar eden problemlerin nedenlerini belirlemektir. Doğru kurgulanmış bir işleyişte tesis sakinleri hangi konuda kime ulaşacağını bilir, ekipler sorumluluk sınırlarını görür ve tedarikçiler belirlenmiş kurallara göre hareket eder. Belirsizliğin azaldığı alanlarda hem hizmet kalitesi yükselir hem de yönetimin günlük akışı daha hızlı ve tutarlı hale gelir.

Teknik yönetim: Arıza sonrasında değil, süreklilik için önlem

Elektrik ve mekanik sistemler, asansörler, su ve enerji altyapıları, yangın güvenliği ekipmanları, aydınlatma ve ortak alan sistemleri modern yaşam alanlarının görünmeyen omurgasını oluşturur. Bu sistemlerden birindeki aksama yalnızca teknik bir problem değildir; güvenliği, konforu, maliyetleri ve kullanıcı memnuniyetini doğrudan etkiler. Profesyonel teknik yönetim bu nedenle arıza sonrasında müdahaleden önce koruyucu ve önleyici bakım anlayışına dayanır. Bakım takvimlerinin oluşturulması, periyodik kontrollerin izlenmesi, kritik ekipman geçmişinin tutulması ve hizmet alınan firmaların performansının değerlendirilmesi gerekir. Hangi sistemin ne zaman kontrol edildiği, hangi sorunun tekrar ettiği ve hangi müdahalenin kalıcı çözüm ürettiği düzenli kayıtlarla görülebildiğinde teknik yönetim, günlük operasyonun sürdürülebilirliğini güvence altına alır.

Şeffaf idari ve mali yönetim

Tesis yönetiminde güvenin en hassas başlıklarından biri idari ve mali süreçlerdir. Bütçenin hazırlanması, aidat ve gider takibi, hizmet alımlarının planlanması, sözleşmeler, tedarikçi ödemeleri ve dönemsel yatırımlar yalnızca muhasebe işlemleri olarak ele alınamaz. Şeffaflık, rakamların paylaşılmasının ötesinde; harcamanın hangi ihtiyaca cevap verdiğinin, hangi alternatiflerin değerlendirildiğinin ve sonucun nasıl takip edildiğinin anlaşılır biçimde açıklanmasıdır. Belge düzeni, onay adımları, görev ve yetki sınırları ile raporlama periyotları standart hale geldiğinde karar alma süreçleri hızlanır ve hata

> “Elektrik ve mekanik sistemler, asansörler, su ve enerji altyapıları, yangın güvenliği ekipmanları, aydınlatma ve ortak alan sistemleri modern yaşam alanlarının görünmeyen omurgasını oluşturur.

riski azalır. Böylece tesis sakinleri ve yatırımcılar yönetim kaynaklarının nasıl kullanıldığını izleyebilir; yönetim kurulları ise geleceğe yönelik kararlarını daha sağlıklı veriyle alabilir.

Hukuki süreçlerde uyum ve sorumluluk

Profesyonel site ve tesis yönetimi; ortak yaşam kuralları, hizmet sözleşmeleri, iş sağlığı ve güvenliği, kişisel verilerin korunması, acil durum yükümlülükleri ve tedarikçi ilişkileri gibi çok sayıda hukuki ve idari sorumluluk içerir. Bu başlıkların yalnızca bir uyuşmazlık ortaya çıktığında ele alınması, yönetim açısından gereksiz risk oluşturur. Kararların uygun yöntemlerle alınması, sözleşmelerde sorumlulukların açıkça tanımlanması, gerekli kayıtların düzenli tutulması ve bildirimlerin zamanında yapılması önleyici yönetimin parçasıdır. Kuralların kişilere göre değişmediği, uygulamaların gerekçelerinin açıklanabildiği ve uyuşmazlıkların belirli bir yöntemle ele alındığı yapılarda yönetim daha adil, öngörülebilir ve güvenilir hale gelir.

7/24 destek: Erişilebilir ve takip edilebilir yönetim

Yaşam alanlarındaki ihtiyaçlar yalnızca mesai saatlerinde ortaya çıkmaz. Teknik bir arıza, güvenlik bildirimi veya acil koordinasyon gerektiren bir durum günün herhangi bir anında yaşanabilir. Bu nedenle 7/24 destek, yalnızca sürekli açık bir iletişim hattı değil; bildirimin alınması, önem seviyesinin belirlenmesi, doğru sorumluya aktarılması ve çözüm sürecinin takip edilmesidir. Kritik durumlarla rutin talepler birbirinden ayrıldığında ekipler kaynaklarını doğru kullanır ve gerçekten acil konulara daha hızlı müdahale eder. Talebin hangi aşamada olduğu, kimin sorumluluğunda bulunduğu ve ne zaman sonuçlandığı kayıt altına alındığında ise hizmet kalitesi ölçülebilir hale gelir. Erişilebilir ve izlenebilir yönetim, sakinlerin yalnızca sesini duyurmasını değil, çözüm sürecine güvenmesini de sağlar.

İnsan kaynağı, güvenlik ve hizmet ekiplerinin aynı dili konuşması

Güçlü tesis yönetimi yalnızca yazılım, cihaz veya prosedürlerle kurulmaz. Güvenlik görevlileri, teknik ekipler, temizlik personeli, idari çalışanlar ve dış hizmet sağlayıcıların aynı operasyon dilini kullanması gerekir. Bir güvenlik bildiriminin teknik ekibe zamanında aktarılması, ortak alandaki bir aksaklığın doğru sorumluya yönlendirilmesi veya tedarikçi çalışmasının saha düzeniyle uyumlu yürütülmesi ancak etkili koordinasyonla mümkündür. Teknoloji bu koordinasyonu desteklediği ölçüde değerlidir; yanlış tanımlanmış bir iş akışı ya da takip edilmeyen kayıt sistemi beklenen yönetim değerini üretmez. Bu nedenle görev tanımları, kontrol listeleri, raporlama alışkanlıkları ve eskalasyon adımları yaşam alanının gerçek ihtiyaçlarına göre tasarlanmalıdır. Eğitimli insan kaynağı, düzenli kayıt ve doğru teknoloji bir araya geldiğinde güvenlik ve hizmet kalitesi sürdürülebilir hale gelir.

İLGİ Grup ile her detay kontrol altında

Tesis yönetimi bir kez planlanıp değişmeden uygulanacak sabit bir yapı değildir. Kullanıcı profili, teknik altyapı, bütçe öncelikleri ve risk haritası zaman içinde değişir. Bu nedenle profesyonel yönetim; düzenli gözden geçirme, saha geri bildirimi, raporlama ve iyileştirme döngüsüyle ele alınmalıdır. İLGİ Grup, operasyonel, teknik, idari ve hukuki süreçleri 360° profesyonel tesis yönetimi yaklaşımının tamamlayıcı parçaları olarak değerlendirir. Güvenlik alanındaki deneyimini 7/24 destek, şeffaf yönetim ve sürdürülebilir planlamayla birleştirerek güvenli, düzenli ve konforlu yaşam alanları oluşturur. Çünkü ilgiyle yönetilen yaşam alanlarında her detay, İLGİ Grup ile kontrol altındadır.

İLGİ GRUP

360° Profesyonel tesis yönetimi hizmeti nereden alabilirim?

Güven ve Konforlu Bir Hayat,
İlgiyle Yönetilen Yaşam Alanlarında!

7/24 Destek ve Şeffaf Yönetim

Profesyonel tesis ve site yönetimi hizmetimizle yaşam ve çalışma alanlarınızdaki tüm operasyonel, teknik, idari ve hukuki süreçleri şeffaf, sürdürülebilir ve profesyonel bir anlayışla yönetiyoruz.

İlgi Grup olarak; site sakinlerinin, yatırımcıların ve işyeri sahiplerinin güvenli, düzenli ve konforlu bir ortamda yaşamlarını sürdürebilmeleri için tüm yönetim süreçlerini titizlikle üstleniyoruz.

Her Detay İlgi ile Kontrol Altında!

ilgigrup.com

Güvenlik ve danışmanlık çözümleri **İLGİ** gerektirir

@ilgigrup

Veri Merkezlerinde Uçtan Uca Erişim Güvenliği

Dijital dünyada artan veri trafiği, veri merkezlerinin önemini giderek artırıyor. Milyonlarca verinin depolandığı ve işlendiği bu tesislerde, verilerin güvenli bir ortamda saklanması ve altyapının olası tehditlere karşı korunması kritik önem taşıyor.

ÖZCAN GÜRLER / DİJİTAL ERİŞİM ÇÖZÜMLERİ SATIŞ MÜDÜRÜ
ASSA ABLOY

Veri merkezlerinde erişimin güvenli ve kontrollü şekilde yönetilmesi için farklı ihtiyaçlara yönelik çözümler sunan ASSA ABLOY, erişim kontrolünden biyometrik doğrulamaya, kabinet güvenliğinden anahtar ve varlık yönetimine kadar uzanan çözümleriyle veri merkezlerinin güvenlik altyapısını destekliyor.

Dijitalleşmenin hızlanmasıyla birlikte veri merkezlerinin önemi her geçen gün artıyor. Kritik verilerin saklandığı ve dijital altyapının yönetildiği bu tesislerde fizikselgüvenlik, bilgi güvenliğinin sağlanmasında önemli bir rol oynuyor. Fiziksel altyapının ve erişim noktalarının güvence altına alınması, yetkisiz erişimlerin önlenmesi ve kritik alanların kontrollü şekilde yönetilmesi, veri merkezlerinde güvenlik yaklaşımının temel unsurlarını oluşturuyor.

Geçiş çözümleri alanında dünyanın lider şirketlerinden ASSA ABLOY, veri merkezlerinin farklı güvenlik ihtiyaçlarına yönelik erişim kontrolü, biyometrik doğrulama, elektro-mekanik kilitleme, kabinet güvenliği, anahtar ve varlık yönetimi çözümleri sunuyor.

Veri merkezlerinde güvenli erişim için kapsamlı çözümler

Veri merkezlerinde farklı güvenlik seviyelerine sahip alanların bulunması, erişim yetkilerinin doğru şekilde tanımlanmasını ve yalnızca yetkili kişilerin ilgili bölümlere ulaşabilmesini

ÖZCAN GÜRLER

gerektiriyor. Bu kapsamda ASSA ABLOY, veri merkezlerinin farklı erişim noktalarına yönelik çözümler sunuyor. Kartlı geçiş sistemleri ve okuyucular, yetkili kişilerin giriş ve çıkışlarının kontrol edilmesini sağlarken, elektro-mekanik, manyetik ve elektrikli kilit çözümleri kapı güvenliğini destekliyor. ASSA ABLOY'un ToC ve standart biyometrik çözümleri ise erişim güvenliğinde kimlik doğrulama seviyesini güçlendiriyor.

Beyaz alan ve kabinet güvenliği

Veri merkezlerinin en kritik bölümlerinden biri olan beyaz alanlarda, yalnızca alan girişlerinin değil, kabinet ekipmanlarının da korunması gerekiyor. ASSA ABLOY'un elektronik ve kablosuz kabinet kilitleri, bu ihtiyaca yönelik farklı çözümler sunuyor. KS200, KS210 ve KS-EM elektronik kabinet kilitleri ile Aperio C100 kablosuz elektronik kilit, kabinetlere erişimin kontrol edilmesine olanak sağlıyor.

> "Kartlı geçiş sistemleri ve okuyucular, yetkili kişilerin giriş ve çıkışlarının kontrol edilmesini sağlarken, elektro-mekanik, manyetik ve elektrikli kilit çözümleri kapı güvenliğini destekliyor.

Erişim yönetimine dijital boyut

Veri merkezlerinde kabinetlerin yanı sıra anahtarların ve kritik ekipmanlara erişim yetkilerinin de kontrollü şekilde yönetilmesi önem taşıyor. Anahtarsız mobil kilit çözümü ABLOY CUMULUS,

fiziksel anahtar ihtiyacını ortadan kaldırarak erişim yönetimine dijital bir boyut kazandırıyor. PROTEC2 CLIQ ise mekanik ve elektronik güvenliği bir araya getirerek anahtarların yetkilendirilmesine ve erişim haklarının yönetilmesine yardımcı oluyor.

Akıllı anahtar ve varlık yönetimi

Veri merkezlerinde güvenlik yalnızca kapı ve kilitlerle sınırlı kalmıyor. Kritik ekipmanlara ve fiziksel varlıklara erişimin kim tarafından, ne zaman ve hangi yetkiyle gerçekleştirildiğinin takip edilebilmesi de operasyonel güvenliğin önemli unsurları arasında yer alıyor. ASSA ABLOY'un Trakaçözümleri, akıllı anahtar ve varlık yönetimi yaklaşımıyla bu ihtiyaca cevap veriyor. Traka L-Touch, S-Touch ve M-Touch key cabinet system çözümleri, anahtarların ve kritik varlıkların kontrollü şekilde saklanmasına, yetkilendirilmesine ve takip edilmesine yardımcı oluyor.

Acil durumlarda güvenli tahliye

Veri merkezlerinde güvenlik kadar acil durumlarda hızlı ve güvenli tahliye de kritik önem taşıyor. ASSA ABLOY, yangın çıkış alanları ve acil çıkış noktalarındagüvenli tahliyeyi destekleyecek geçiş çözümleriyle tesislerin güvenlik altyapısının tamamlayıcı bir parçasını oluşturuyor.

ASSA ABLOY Dijital Erişim Çözümleri Satış Müdürü Özcan Gürler, veri merkezlerinde güvenliğin çok katmanlı bir yaklaşımla ele alınması gerektiğini belirterek şunları söyledi:

"Veri merkezlerinde güvenli erişim, kritik verilerin ve altyapının korunmasının temel unsurlarından biri. Bu nedenle farklı erişim noktalarının ihtiyaca uygun çözümlerle güvence altına alınması gerekiyor. Personel ve ziyaretçi erişimlerinden kritik alanlara, beyaz alanlardan kabinetlere, anahtar ve varlık yönetiminden acil durum çıkışlarına kadar tüm süreçlerin birbiriyle entegre şekilde ele alınması önem taşıyor. ASSA ABLOY olarak, veri merkezlerinde erişimin güvenli ve kontrollü şekilde yönetilmesi için farklı ihtiyaçlara yönelik çözümler sunuyoruz.

> "Amacımız, veri merkezlerinin güvenlik altyapısına uçtan uca katkı sağlama

Amacımız, fiziksel erişim güvenliğini dijital yönetim kabiliyetiyle birleştirerek veri merkezlerinin güvenlik altyapısına uçtan uca katkı sağlamak."

ASSA ABLOY, 7-10 Ekim'de İSAF Datacenter'da

ASSA ABLOY, veri merkezlerine yönelik erişim ve güvenlik çözümlerini 7-10 Ekim tarihleri arasında İstanbul Fuar Merkezi'nde düzenlenecek İSAF Datacenter Fuarı'ndasektör profesyonelleriyle buluşturacak. Fuarda; kartlı geçiş, biyometrik doğrulama, elektro-mekanik kilitleme, kabinet güvenliği, anahtar ve varlık yönetimi ile acil çıkışlara yönelik çözümler tanıtılacak.

VİYA; Yapay Zeka Destekli 7/24 Akıllı Hasta Bakıcı Sistemi

- **360° Kesintisiz Takip** – Her açıdan tam kontrol, eksiksiz hasta gözetimi
- **GDPR Uyumlu Gizlilik** – Güvenli ve etik veri koruma standartları
- **Gelişmiş İzleme Lisansı** – Profesyonel ve yüksek hassasiyetli izleme teknolojisi
- **Kolay Entegrasyon** – Mevcut sistemlerle zahmetsiz uyum
- **Yüksek Güvenlik & Erken Müdahale** – Riskleri önceden tespit eden akıllı analizler
- **Bakım Personeline Destek** – İş yükünü azaltan verimli asistan
- **Maksimum Esneklik** – Farklı bakım ortamlarına kolay uyum
- **Dayanıklılık & Maliyet Verimliliği** – Uzun ömürlü, ekonomik çözüm

VİYA ile geleceğin hasta bakımını bugünden deneyimleyin!

Uluslararası Kabul Edilmiş Sertifikalar

MOBOTIX
Gold Partner 2025

Alev oluşmadan önce yangınları tesbit edin.

VdS EN 54-10 Certified CNPP PBST

VİYA AKADEMİ ACADEMY

Hocapaşa Mah. Nöbethane Cad.
No:19 Fatih - İstanbul
Tel: +90 532 767 0444
90 532 211 3038
E-mail: info@viyagroup.net
haterettin@viyagroup.net

Veri Tutan Değil, **Karar Veren Sistemler**

Türkiye'de CRM kullanımı yüzde 12'de kalırken yapay zekâ, müşteri yönetimini kayıt sisteminden karar mekanizmasına taşıyor

İSA DEMİRCİ / KURUCU
EKSENIUM

Türkiye'de şirketlerin yüzde 28,3'ü kurumsal kaynak planlama (ERP) yazılımı kullanırken müşteri ilişkileri yönetimi (CRM) kullananların oranı yüzde 12'de kalıyor. TÜİK'in 2025 Girişimlerde Bilişim Teknolojileri Kullanım Araştırması, şirketlerin kaynak planlamasında dijitalleşirken müşteri süreçlerinin sistemleştirilmesinde aynı hızın yakalanamadığını gösteriyor. Yapay zekâ, otomasyon ve low-code teknolojilerindeki gelişmeler ise CRM'in rolünü veri kaydeden bir sistemden, şirket geçmişini analiz ederek karar ve aksiyon üreten bir yapıya doğru taşıyor.

TÜİK verilerine göre ücretli bulut bilişim hizmeti kullanan girişimlerin oranı yüzde 20,4'e, sosyal medya kullananların oranı yüzde 55,2'ye ulaşırken CRM kullanımı özellikle küçük ve orta ölçekli işletmelerde daha düşük seyrediyor. 10-49 çalışanlı girişimlerde CRM kullanım oranı yüzde 9,9'a kadar geriliyor. Buna karşılık birçok şirkette müşteri süreçleri hâlâ Excel tabloları, e-posta, mesajlaşma uygulamaları, muhasebe programları ve farklı yazılımlar arasında yürütülüyor.

Bu parçalı yapı yalnızca veri dağınıklığı yaratmıyor. Aynı müşterinin farklı sistemlerde tekrar tutulmasına, takiplerin kişilere bağımlı kalmasına, fırsatların hangi aşamada kaybedildiğinin görülememesine ve yönetimin satış sürecinin tamamını tek noktadan izleyememesine neden olabiliyor. İsa Demirci,

İSA DEMİRCİ

bu tablonun zamanla normalleştiğine dikkat çekerek, "Ortaya düzensizliğin kendisinin düzen hâline geldiği bir yapı çıkıyor. Şirket bir süre sonra bu dağınıklığa alışıyor ve onu bir eksiklik olarak değil, çalışma biçimi olarak kabul ediyor," dedi. Eksenium Kurucusu İsa Demirci, CRM'in yapay zekâyla birlikte yeni bir evreye girdiğini belirterek, "Bugün birçok şirkette CRM hâlâ verinin girildiği, saklandığı ve raporlandığı bir sistem olarak görülüyor. Bundan sonraki aşamada şirketin kendi geçmişini okuyarak hangi satışın risk altında olduğunu, hangi müşterinin takip edilmesi gerektiğini ve bir sonraki aksiyonun ne olması gerektiğini önerecek. Asıl değişim, CRM'in kayıt tutulan yerden işin yürütüldüğü ve karar üretildiği yere dönüşmesi olacak. Şirketlerin rekabeti yalnızca hangi yapay zekâ modelini kullandıklarıyla değil, kendi verilerini ne kadar doğru ve anlamlı kullanabildikleriyle şekillenecek," dedi.

"Asıl değişim, CRM'in kayıt tutulan yerden işin yürütüldüğü ve karar üretildiği yere dönüşmesi olacak. Şirketlerin rekabeti yalnızca hangi yapay zekâ modelini kullandıklarıyla değil, kendi verilerini ne kadar doğru ve anlamlı kullanabildikleriyle şekillenecek

CRM projelerinde kritik konu teknoloji değil, süreç tasarımı

CRM sistemleri devreye girdiğinde müşteri takibinin nerede aksadığı, fırsatların hangi aşamada kaybedildiği ve ekiplerin performansı ölçülebilir hâle geliyor. Bu nedenle projelerin başarısını yalnızca yazılım seçimi değil; süreçlerin nasıl tasarlandığı, verinin hangi yapıda toplandığı ve çalışanların sistemi günlük iş akışına ne ölçüde dahil ettiği belirliyor.

İsa Demirci, "CRM'in zor tarafı yazılımdan çok getirdiği şeffaflık ve çalışma biçimindeki değişim.

> CRM'i hazır bir yazılımın şirket içine kurulmasından ziyade, kurumun çalışma biçimine göre genişletilebilen bir teknoloji altyapısı olarak konumlandırıyor. Böylece standart platformun karşılamadığı sektörel veya şirkete özel süreçler, aynı ekosistem içinde geliştirilen yeni teknoloji katmanlarıyla yönetilebiliyor.

Sistem devreye girdiğinde şirketin görünmeyen tarafları görünür oluyor; takiplerin nerede aksadığı, fırsatların neden kaybedildiği ve performansın nasıl dağıldığı ölçülebiliyor. Yapay zekâ bu ihtiyacı azaltmayacak; tam tersine doğru kurulmuş süreçleri ve temiz veriyi daha kritik hâle getirecek. Sistem yanlış veya eksik veriyle besleniyorsa yapay zekânın üreteceği öneri de aynı ölçüde sorunlu olacaktır. Bu nedenle başarılı bir CRM projesi teknik kurulumdan önce doğru süreç tasarımı, sonrasında ise gerçek kullanıcı adaptasyonu gerektiriyor," ifadelerini kullandı.

Eksenium, bu yaklaşım doğrultusunda canlıya geçiş sonrasında altı ay boyunca birebir destek vererek yalnızca sistemin teknik çalışmasını değil, ekiplerin kullanım alışkanlıklarını ve süreç adaptasyonunu da takip ediyor.

Sağlık turizminde CRM hasta takibinden operasyon yönetimine geçiyor

Bu dönüşümün belirgin biçimde görüldüğü alanlardan biri sağlık turizmi. Çok dilli, çok kanallı ve çoğu zaman haftalar ya da aylar süren hasta yolculuğunun ilk temastan tedavi sonrasına kadar tek yapı altında yönetilmesi, CRM'i basit bir hasta listesinin ötesine taşıyor.

Eksenium, iki ülkede faaliyet gösteren bir diş kliniği için küresel bulut tabanlı iş yazılımları platformu Zoho'nun CRM altyapısı üzerinde geliştirdiği sistemde diş şeması üzerinden tedavi planlamasını, kliniğin kendi fiyat kataloğunu ve hastanın kendi dilinde tedavi planı oluşturulmasını aynı yapıda birleştirdi. Projede 34 iş akışı ve 15 özel fonksiyon ile manuel takip ve raporlama süreçleri otomasyona taşındı.

Farklı ülkelerde yedi şubeyle faaliyet gösteren başka bir klinik grubunda ise gelen talepler, teklifler, tahsilatlar, çalışan performansı ve şube sonuçları tek CRM hesabında toplandı. Farklı para birimlerindeki sonuçların ortak yapıda karşılaştırılabildiği sistem yaklaşık iki buçuk yıldır aktif olarak kullanılıyor. Yurt dışındaki satış ekibi için CRM eğitimi ekibin kendi dilinde hazırlanarak sistemin şube genelinde benimsenmesi sağlandı.

Eksenium, Zoho'nun üzerine kendi teknoloji katmanlarını geliştiriyor

Eksenium'un çalışmaları standart CRM kurulumu ve konfigürasyonuyla sınırlı kalmıyor. Şirket, Zoho altyapısı üzerinde kurumlara özel fonksiyonlar, CRM ekranının içinde çalışan arayüzler ve sunucusuz uygulamalar geliştirirken; kurulumların sağlık kontrolü, iş akışlarının yönetimi ve geliştirilen kodların izlenmesi gibi ihtiyaçlar için kendi araçlarını da oluşturuyor.

Bu yaklaşım, CRM'i hazır bir yazılımın şirket içine kurulmasından ziyade, kurumun çalışma biçimine göre genişletilebilen bir teknoloji altyapısı olarak konumlandırıyor. Böylece standart platformun karşılamadığı sektörel veya şirkete özel süreçler, aynı ekosistem içinde geliştirilen yeni teknoloji katmanlarıyla yönetilebiliyor.

İsa Demirci'nin Zoho ekosistemindeki yaklaşık 10 yıllık deneyimi üzerine konumlanan ve 2023'ten bu yana Zoho Authorized Partner olarak faaliyet gösteren Eksenium, bugüne kadar Türkiye, Hollanda, Sırbistan, Bosna Hersek ve Polonya'da 30'un üzerinde proje gerçekleştirdi. Şirketin 14 Zoho uygulamasında yetkinliği bulunurken müşteri projeleri ve kendi geliştirdiği araçlarla birlikte 13 özel çözüm ve entegrasyon hayata geçirildi. Eksenium, kurulumlarında standart olarak canlıya geçiş sonrası altı ay birebir destek veriyor.

Yapay zekâ, doğru CRM kurulumunu daha kritik hâle getiriyor

Yeni nesil kurumsal yapay zekâ uygulamalarında asıl değer, şirketlerin yıllar içinde oluşturduğu satış, teklif, müşteri ve operasyon verisinin anlamlandırılabilmesinden doğuyor. Üç yıllık satış geçmişinin hangi müşterilerin neden kaybedildiğini, hangi satış süreçlerinin yavaşladığını veya hangi fırsatların önceliklendirilmesi gerektiğini gösterebilmesi, CRM'i raporlama aracından karar destek sistemine taşıyor.

Ancak bunun için verinin ilk günden itibaren doğru yapıda toplanması gerekiyor. Eksik, dağınık veya yanlış sınıflandırılmış veri yalnızca mevcut raporlamayı değil, gelecekte bu veri üzerinden çalışacak yapay zekâ sistemlerinin üreteceği sonuçları da doğrudan etkiliyor.

Eksenium önümüzdeki dönemde Türkiye'de tekrar eden sektörel ihtiyaçlar ve yerel iş akışları için geliştirdiği çözümleri yeniden kullanılabilir ürünlere dönüştürmeyi; Zoho Marketplace'e yönelik eklentilerini ve Zoho Catalyst tabanlı uygulama geliştirme çalışmalarını genişletmeyi hedefliyor.

Türkiye'nin veri merkezi kapasitesini 1 GW'a çıkarma hedefi gündemde

Türkiye, verilerin ülke içinde saklanmasını ve yönetilmesini sağlayan bulut çözümlerine, yüksek performanslı bilgi işleme ve yeni nesil veri merkezlerine yönelik yatırımlarını hızlandırıyor. GITEX Ai Türkiye ise dünyadan ve Türkiye'den teknoloji liderlerini İstanbul'da buluşturuyor.

GITEX AI TÜRKİYE

Türkiye, yapay zekâyı kurumların iş süreçlerinde yaygınlaştırmak amacıyla veri merkezlerine, bulut platformlarına, yüksek performanslı bilgi işleme ve akıllı altyapılara yönelik yatırımlarına hız veriyor. Yapay zekâda yeni bir dönemin önünü açacak bu altyapı yatırımları, gelecek hafta düzenlenecek GITEX Ai Türkiye'de gündemin odağında olacak.
Türkiye, 2026–2030 Yapay Zekâ Vizyonu ve Eylem Planı kapsamında, yapay zekâ altyapısı, bulut bilişim ve veri merkezleri alanlarında en az 10 milyar ABD doları tutarında özel sektör yatırımı yapılmasını hedefliyor. Plan doğrultusunda, 2030 yılına kadar veri merkezlerinin kurulu kapasitesinin en az 1 GW'a çıkarılması amaçlanıyor.
Dünyanın dört bir yanından katılımcıları ağırlayacak teknoloji ve yapay zekâ etkinliği GITEX Ai Türkiye, 9–10 Eylül 2026 tarihlerinde İstanbul Fuar Merkezi'nde düzenlenecek. Etkinlikte 350'nin üzerinde şirket ve girişim ürün ve çözümlerini sergileyecek; yatırımcılar, politika yapıcılar, uzman konuşmacılar ve teknoloji yöneticileri bir araya gelecek.
Katılımcılar arasında altyapı, bulut ve bilgi işlem teknolojilerine yön veren Google Cloud, HPE & NVIDIA, AWS, Schneider Electric, Huawei, ASUS, Dell Technologies, SAP ve TrendAI gibi küresel teknoloji devleri yer alıyor. Etkinliğin Veri Merkezi ve Akıllı Altyapı bölümü, Türkiye'nin yapay zekâ hedeflerini hayata geçirmek ve bu teknolojinin yaygın kullanımını sağlamak için ihtiyaç duyduğu güvenli, ihtiyaca göre büyüyebilen ve kesintilere karşı dayanıklı altyapıların nasıl kurulabileceğine odaklanacak.

ERSİN BÜYÜKYILMAZ
TREOMIND CEO

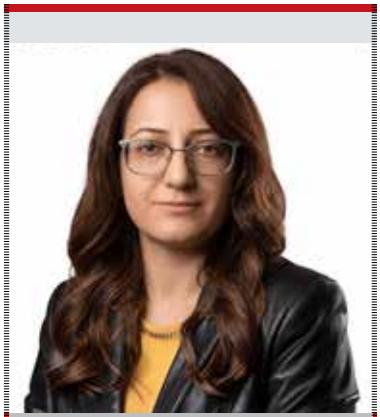
> "Asıl mesele yalnızca ne kadar işlem gücü sağlayabildiğimiz değil, bu kapasiteyi güvenli, ölçeklenebilir ve iş süreçlerinde doğrudan kullanılabilecek yapay zekâ sistemlerine ne kadar etkili biçimde dönüştürebildiğimiz.

Yapay zekâda kapasite kadar etkin kullanım da önemli

Kurumlar yapay zekâyı iş süreçlerinde kullanmaya başladıkça, yalnızca işlem kapasitesini artırmanın yeterli olmadığı da görülüyor. Kullanılan altyapının, yapay zekâ uygulamalarını kurum genelinde güvenli ve verimli biçimde çalıştırabilmesi gerekiyor.
GITEX Ai Türkiye katılımcılarından Türkiye merkezli yapay zekâ ve teknoloji altyapısı şirketi Treomind, işlem kapasitesinin etkin kullanımının önemine dikkat çekiyor.

Treomind CEO'su Ersin Büyükyılmaz, "Asıl mesele yalnızca ne kadar işlem gücü sağlayabildiğimiz değil, bu kapasiteyi güvenli, ölçeklenebilir ve iş süreçlerinde doğrudan kullanılabilecek yapay zekâ sistemlerine ne kadar etkili biçimde dönüştürebildiğimiz" diyor.
Büyükyılmaz, kurumların yapay zekâyı etkin kullanabilmesi için verilerini doğru yönetmesi ve bilgi işlem kaynaklarını, bulut altyapısını ve güvenlik çözümlerini iş stratejileriyle uyumlu biçimde planlaması gerektiğini belirtiyor. "Her yapay zekâ yatırımı, açıkça tanımlanmış bir iş ihtiyacına yanıt vermeli ve ölçülebilir sonuçlar üretmeli" diye ekliyor.
Yapay zekâya yönelik talebin hızla artması, verilerin nerede tutulduğu ve kim tarafından kontrol edildiği konusunu da

YILMAZ BARÇIN
FİXCLOUD KURUCU ORTAĞI VE CEO'SU



NESLİHAN KURT
OPENZEKA CEO

gündemin ön sıralarına taşıyor. Verilerin ülke sınırları içinde saklanmasını ve yönetilmesini sağlayan bulut çözümleri ile yapay zekâ altyapısı konusunda uzmanlaşan Türk bulut teknolojileri sağlayıcısı FixCloud, şirketlerin kendi verileri üzerindeki kontrolünü koruyarak yüksek performanslı bilgi işlem kaynaklarından yararlanmasına yardımcı olmayı amaçlıyor.

FixCloud Kurucu Ortağı ve CEO'su Yılmaz Barçın, "Kurumların, başlangıçta büyük yatırımlar yapmadan, yüksek performanslı grafik işlemci (GPU) kaynaklarını ihtiyaçları ölçüsünde kullanabilecekleri hizmet modellerine yönelmesi gerekiyor" diyor.
Barçın, yasal düzenlemelerin getirdiği yükümlülükler arttıkça hassas verilerin Türkiye sınırları içinde tutulmasının da daha fazla önem kazandığını vurguluyor. Kamu, şirketler ve altyapı sağlayıcıları arasında güçlendirilecek iş birliklerinin, Türkiye'nin Avrasya için bölgesel bir bulut, veri ve yapay zekâ altyapısı merkezi hâline gelmesini destekleyebileceğini belirtiyor.
FixCloud, GITEX Ai Türkiye'de verilerin Türkiye'de saklanmasını ve yönetilmesini sağlayan bulut platformunu, ihtiyaca göre artırılıp azaltılabilen yapay zekâ işlem kapasitesini ve kritik yapay zekâ verileri ile modellerini korumaya yönelik çözümlerini tanıtacak.

Her yapay zekâ uygulaması için doğru altyapı

Yapay zekânın günlük iş süreçlerindeki kullanımı yaygınlaştıkça, şirketlerin bu uygulamaları hangi altyapıda çalıştıracağı daha fazla önem kazanıyor: Hangi işlemler bulutta, hangileri veri merkezinde, hangileri ise verinin üretildiği noktaya daha yakın bir ortamda yürütülmeli? Verinin kaynağına yakın noktalarda işlenmesini sağlayan uç bilişim, robotik ve kurumsal yapay zekâ alanlarında faaliyet gösteren yapay zekâ altyapısı şirketi OpenZeka, altyapı kararlarının her işletmenin kendine özgü ihtiyaçlarına göre şekillenmesi gerektiğini savunuyor.

OpenZeka CEO'su Neslihan Kurt, "Şirketler yatırımlarını faaliyet gösterdikleri sektöre, yürütecekleri işlemlere, veri gereksinimlerine ve bütçelerine göre planlamalı. Rekabet avantajı, yalnızca uç bilişim, bulut veya veri merkezi altyapısından birini seçerek elde edilmeyecek. Asıl farkı, her uygulamayı ihtiyacına en uygun ortamda çalıştırabilen şirketler yaratacak" diyor.
OpenZeka, GITEX Ai Türkiye'de NVIDIA destekli altyapıların robotik uygulamalarda, kullanıcıya veya cihaza yakın noktalarda çalışan yapay zekâ sistemlerinde ve büyük ölçekli kurumsal işlemlerde nasıl kullanılabileceğini gösterecek.
Kurt, yapay zekânın Türkiye genelinde yaygınlaşması için donanım ve yazılım şirketlerinin, girişimlerin, üniversitelerin, işletmelerin ve kamu kurumlarının iş birliği yapması gerektiğini belirtiyor. Bu paydaşların her birinin, Türkiye'nin gelişen yapay zekâ ekosistemine kendi uzmanlığıyla katkı sunduğunu ifade ediyor.
Yapay zekâ ekosistemindeki gelişim, altyapı talebine de yansıyor. Sunucu ve bilgi işlem altyapısı sağlayan ASUS Altyapı Çözümleri İş Grubu, Türkiye'deki bulut operatörlerinin, verileri ve sistemleri ülke içinden yönetmeye olanak tanıyan yapay zekâ altyapıları kurduğunu gözlemliyor. Aynı zamanda, yönetimi Türkiye'de olan bilgi

KEVIN LI
ASUS ALTYAPI ÇÖZ. İŞ GRUBU EEMEA BÖLGESİ GEN. MÜD.

WASEEM HAMBROUC
CLOUD ETEL İŞ GELİŞTİRME MÜDÜRÜ

> Bilgi işlem altyapıları büyüdükçe, yapay zekâyı destekleyen bulut altyapıları da gelişiyor.

işlem altyapılarına talep artarken, üretim ve finansal hizmetlerde yapay zekâyla yürütülen işlemlerin hacmi büyüyor.

ASUS Altyapı Çözümleri İş Grubu EEMEA Bölgesi Genel Müdürü Kevin Li, "ASUS olarak 30 yılı aşkın süredir Türkiye'de faaliyet gösteriyoruz. Bugün çok belirgin bir dönüşüme tanıklık ediyoruz. Türkiye'deki bulut operatörleri ve şirketler, verileri ve sistemleri Türkiye'den yönetebilecekleri büyük ölçekli yapay zekâ altyapıları kuruyor" diyor. ASUS, etkinlikte yapay zekâ uygulamalarının geliştirilmesinden büyük ölçekte kullanılmasına kadar tüm aşamaları destekleyen en yeni bilgi işlem, veri merkezi, uç bilişim ve depolama çözümlerini sergileyecek.

Bulut altyapıları daha akıllı ve dayanıklı hâle geliyor

Bilgi işlem altyapıları büyüdükçe, yapay zekâyı destekleyen bulut altyapıları da gelişiyor. Bölgesel bulut ve dijital altyapı sağlayıcısı Cloud ETEL, kurumların maliyetlerini gözetirken güvenliği ve hizmet sürekliliğini de sağlayan, birbiriyle bağlantılı bulut ortamları oluşturmasına odaklanıyor.

Cloud ETEL İş Geliştirme Müdürü Waseem Hambrouch, yeni nesil bulut platformlarının 'daha akıllı, otonom ve dayanıklı' hâle geldiğini; yapay zekâ, otomasyon, siber güvenlik ve yüksek performanslı bilgi işlem teknolojilerini bir araya getirdiğini belirtiyor. Şirket, GITEX Ai Türkiye'de işletmelerin giderek karmaşıklaşan dijital sistemlerini yönetmelerine yardımcı olacak bulut, bağlantı ve yapay zekâ çözümlerini tanıtacak. Altyapı yatırımları, konferans programının da temel gündem maddelerinden biri olacak. İlk gün düzenlenecek "1 GW'a Geri Sayım: Türkiye'nin Yapay Zekâda Önümüzdeki On Yılını Şekillendirecek Altyapı Yatırımları" başlıklı oturumda, ulusal yapay zekâ planında öngörülen bilgi işlem altyapısının nasıl hayata geçirileceği ele alınacak.

Oturumda **Equinix Türkiye Genel Müdürü Ersel Oymak**, Schneider Electric Türkiye ve Orta Asya Güvenli Güç ve Veri Merkezlerinden Sorumlu Başkan Yardımcısı Bihter Gönenli ve HPE EMEA ve LATAM Bölgeleri Yüksek Performanslı Bilgi İşlem ve Yapay Zekâ İş Birimi Başkan Yardımcısı ve Genel Müdürü Damien Declat yer alacak.
Türkiye Cumhuriyeti Cumhurbaşkanlığı Yatırım ve Finans Ofisi (Invest in Türkiye) ev sahipliğinde, Sanayi ve Teknoloji Bakanlığı'nın stratejik ortaklığında gerçekleştirilen GITEX Ai Türkiye, Dubai Dünya Ticaret Merkezi ile Informa'nın ortak girişimi inD tarafından düzenleniyor. Dünya genelindeki GITEX etkinliklerinin organizasyonunu da inD üstleniyor. Etkinlik, Trendyol, Andevos ve Halkbank gibi Türkiye'nin önde gelen kuruluşlarının yanı sıra Antalya Teknokent, İTÜ ARI Teknokent ve Giresun Teknopark'ın da aralarında bulunduğu teknoparkları bir araya getirecek.

Havalimanı Güvenliğinde Yeni Dönem
Akıllı Video Teknolojileri Operasyonların Merkezinde

Türkiye, verilerin ülke içinde saklanmasını ve yönetilmesini sağlayan bulut çözümlerine, yüksek performanslı bilgi işleme ve yeni nesil veri merkezlerine yönelik yatırımlarını hızlandırıyor. GITEX Ai Türkiye ise dünyadan ve Türkiye'den teknoloji liderlerini İstanbul'da buluşturuyor.

AXIS COMMUNICATIONS

Artan yolcu hacmi, genişleyen altyapılar ve değişen tehdit dinamikleri, havalimanlarını her zamankinden daha karmaşık operasyon merkezlerine dönüştürüyor. Bu dönüşüm, güvenlikten operasyonel verimliliğe kadar tüm süreçlerin daha akıllı ve entegre teknolojilerle yeniden ele alınmasını zorunlu kılıyor.
Axis Communications, havalimanı güvenliğine yönelik yaklaşımın artık sadece gözetimle sınırlı olmadığını; operasyonel zekâ, veri analitiği ve uçtan uca entegrasyonla şekillendiğini vurguluyor.

Güvenlikten Operasyonel Zekâya Geçiş

Geleneksel güvenlik sistemleri yerini; gerçek zamanlı veri sağlayan, olayları analiz eden ve karar süreçlerini hızlandıran akıllı video çözümlerine bırakıyor. Yapay zekâ destekli video analitiği sayesinde yolcu akışı izlenebiliyor, yoğunluklar tespit edilebiliyor ve potansiyel riskler daha oluşmadan önlenebiliyor.

Katmanlı Güvenlik ve 7/24 İzleme

Modern havalimanlarında güvenlik artık tek bir sistemle değil, katmanlı bir yapı ile sağlanıyor. Perimetre güvenliğinden terminal içi izlemeye kadar uzanan bu yapı; termal kameralar, video analitikler ve radar teknolojileri ile destekleniyor.

Bu sistemler sayesinde:

- Yetkisiz girişler gerçek zamanlı tespit ediliyor
- Yanlış alarmlar minimize ediliyor
- Şüpheli hareketler otomatik olarak izlenip raporlanıyor

Ayrıca entegre ses sistemleri ile anlık uyarılar yapılabiliyor ve potansiyel tehditler henüz büyümeden engellenebiliyor.

Yolcu ve Çalışan Güvenliği Öncelikte

Akıllı video çözümleri yalnızca güvenliği artırmakla kalmıyor; aynı zamanda yolcu deneyimini de iyileştiriyor. Bagaj akışının izlenmesi, yetkisiz erişimlerin tespiti ve anlık uyarı mekanizmaları sayesinde operasyonel aksaklıklar minimuma indiriliyor.

Entegre ve Veri Odaklı Havalimanı Operasyonları

Axis'in havacılık çözümleri, havalimanlarının tüm operasyonlarını kapsayan entegre bir platform sunuyor. Otoparktan piste, terminalden bagaj alanına kadar tüm süreçler tek bir sistem üzerinden yönetilebiliyor.

Bu sayede:

- Yolcu akışı ve yoğunluk gerçek zamanlı analiz ediliyor
- Bagaj ve lojistik süreçleri optimize ediliyor
- Personel ve saha operasyonları daha verimli hale getiriliyor

Axis Communications Özel Müşteriler Müdürü Çiğdem Gülgün Tunçer konuyla ilgili şunları söylüyor:

"Günümüzde havalimanlarında güvenlik artık yalnızca izlemekle sınırlı değil. Asıl değer, veriyi anlamlandırarak operasyonel içgörüye dönüştürebilmekte yatıyor. Akıllı video analitiği sayesinde sadece riskleri daha erken tespit etmekle kalmıyor, aynı

zamanda yolcu akışını optimize ederek operasyonel verimliliği de artırıyoruz. Entegre ve siber güvenliği yüksek sistemler, havalimanlarının hem bugününü hem de geleceğini güvence altına alıyor."

Her Koşulda Güvenilir Performans

Havalimanları gibi kritik ortamlarda sistemlerin kesintisiz çalışması büyük önem taşıyor. Axis çözümleri; düşük ışık, kötü hava koşulları ve geniş alanlarda dahi yüksek performans sunarak 7/24 güvenilir izleme sağlıyor. Aynı zamanda açık platform yapısı sayesinde farklı sistemlerle kolay entegrasyon imkânı sunarak uzun vadeli yatırım koruması sağlıyor.

Geleceğin Havalimanları: Daha Akıllı, Daha Güvenli

Günümüzde havalimanı operatörleri için öncelik artık sadece tehditleri tespit etmek değil; tüm operasyonu daha akıllı, sürdürülebilir ve yolcu odaklı hale getirmek.
Akıllı video teknolojileri ve gelişmiş analitik çözümler, havalimanlarını daha güvenli hale getirirken aynı zamanda operasyonel mükemmeliyetin de temelini oluşturuyor.

Havalimanlarında Güvenlik
Fiziki Korumadan Yapay Zekâ Destekli Güvenliğe

DERLEME: DERYA BOZKURT

Milyonlarca yolcunun, çalışanların, bagajların, kargoların ve operasyonel süreçlerin aynı anda hareket ettiği havalimanlarında güvenlik, tek bir kontrol noktasından ibaret değil. Fiziki çevre güvenliğinden geçiş kontrol sistemlerine, CCTV ve video analitikten X-Ray ve CT tarama teknolojilerine, yangın algılama ve ARFF hizmetlerinden acil durum yönetimine kadar uzanan çok katmanlı güvenlik mimarisi, yapay zekâ ve veri analitiğinin de etkisiyle yeniden şekilleniyor.

Havalimanları, milyonlarca yolcunun, binlerce çalışanın, yüzlerce aracın, tonlarca bagaj ve kargonun aynı anda hareket ettiği, son derece karmaşık ve birbirine bağlı yapılardır.
Bu nedenle havalimanı güvenliği yalnızca terminal girişinde yolcuların ve bagajların kontrol edilmesinden ibaret değildir. Güvenli bir havalimanı; çevre güvenliği, erişim kontrolü, yolcu ve bagaj taraması, kamera sistemleri, alarm ve ihbar altyapıları, yangın güvenliği, acil durum yönetimi, kargo güvenliği, personel güvenliği ve giderek daha fazla önem kazanan siber güvenliğin birlikte çalıştığı çok katmanlı bir sistemdir.
Uluslararası sivil havacılığın güvenlik çerçevesinin temel belgelerinden biri olan ICAO Annex 17, havacılığın yasa dışı müdahale eylemlerine karşı korunmasını esas alır. ICAO'ya göre havacılık güvenliği; yolcuların, mürettebatın, yer personelinin ve toplumun yasa dışı müdahale eylemlerine karşı korunmasını hedefleyen teknik ve idari önlemler bütünüdür. Annex 17 aynı zamanda güvenliğin yalnızca havalimanı işletmesinin değil, devletlerin, havayollarının ve ilgili diğer aktörlerin ortak sorumluluğu olduğunu ortaya koymaktadır.
Günümüzde bu yaklaşım daha da genişlemiştir. Çünkü modern havalimanlarında güvenlik sistemleri artık yalnızca fiziksel tehditleri algılayan cihazlardan oluşmamaktadır. Kameralardan elde edilen görüntüler, erişim kontrol kayıtları, X-ray ve bilgisayarlı tomografi görüntüleri, alarm verileri ve operasyonel bilgiler giderek daha fazla veri analitiği ve yapay zekâ sistemleriyle birlikte değerlendirilmektedir. 2026 yılında yayımlanan kapsamlı bir çalışma, havalimanlarında yapay zekâ uygulamalarının risk tanımlama, risk değerlendirme ve risk azaltma süreçlerine giderek daha fazla dahil edildiğini, ancak uygulamaların hâlen çoğunlukla tekil teknolojiler üzerine yoğunlaştığını ortaya koymaktadır.
Bu nedenle havalimanı güvenliğinin geleceği, tek bir güvenlik cihazının daha gelişmiş hale gelmesinden çok, farklı güvenlik katmanlarının birbiriyle entegre çalışmasına bağlı olacaktır.

Havalimanı Güvenliğinin Temelini Fiziki Güvenlik Oluşturuyor

Havalimanının güvenlik mimarisinin ilk katmanı fiziksel çevredir. Terminal binaları, apronlar, pist ve taksi yolları, yakıt tesisleri, kargo alanları, bakım hangarları, otoparklar ve teknik tesisler farklı güvenlik seviyelerine ihtiyaç duyar.
Havalimanlarının geniş yüzölçümü, fiziksel güvenliği diğer birçok kritik tesisten farklılaştırmaktadır. Bir fabrikanın veya ofis binasının birkaç giriş kapısı bulunabilirken, büyük bir havalimanının kilometrelerce uzunlukta çevre hattı, çok sayıda araç ve personel giriş noktası ve birbirinden farklı güvenlik gereksinimleri olan çok sayıda operasyonel alanı vardır.
Bu nedenle çevre güvenliğinde çit sistemleri, kontrollü kapılar, güvenlik noktaları, aydınlatma, devriye sistemleri ve elektronik algılama teknolojileri birlikte kullanılmaktadır. FAA'nın havalimanı tasarımına ilişkin materyallerinde de çevre çitleri ve yetkili personel ile araçların girişini sağlayan kontrollü kapılar, havalimanı güvenlik mimarisinin temel unsurları arasında ele alın-

maktadır.
Ancak modern yaklaşımda çitin kendisi güvenliğin tamamı değildir. Çit, fiziksel bir geciktirme ve sınır oluşturma mekanizmasıdır. Asıl amaç, yetkisiz giriş girişimini mümkün olduğunca erken tespit etmek, alarmı doğrulamak ve olayın ilgili güvenlik ekiplerine aktarılmasını sağlamaktır.
Bu noktada çevre güvenlik sistemleri devreye girer.

Çevre Güvenliğinde Elektronik Algılama Sistemleri

Havalimanlarının geniş çevrelerinin yalnızca insan gücüyle sürekli izlenmesi mümkün değildir. Bu nedenle çevre güvenliğinde farklı elektronik algılama teknolojileri kullanılmaktadır.
Kamera tabanlı video analiz sistemleri, kızılötesi ve termal kameralar, mikrodalga algılama, fiber optik algılama, lazer tabanlı sistemler ve çeşitli çevre ihlal algılama teknolojileri farklı koşullarda kullanılabilir.
Akademik literatürde çevre ihlal tespit sistemlerinin önemli bir bölümünün yanlış alarm oranını azaltmaya odaklandığı görülmektedir. Özellikle hava koşulları, hayvan hareketleri, bitki örtüsü, gölgeler ve çevresel titreşimler elektronik güvenlik sistemlerinde yanlış alarm oluştura-

> Video analitiği sayesinde belirli hareket biçimleri, olağan dışı davranışlar, belirli bölgelerde uzun süre kalma, ters yönde hareket veya belirlenmiş güvenlik bölgelerine girme gibi durumlar otomatik olarak işaretlenebilir.

bilmektedir. Havalimanı çevresine yönelik lazer tabanlı bir araştırmada da farklı ihlal türlerinin algılanması ve alarm eşiklerinin belirlenmesi üzerinde durulmuştur.

Video tabanlı çevre güvenliğinde ise yapay zekâ ve bilgisayarlı görü sistemleri önem kazanmaktadır. Literatürde hareket algılama, nesne takibi, insan tespiti ve anomali tespiti gibi yöntemlerin çevre güvenliğinde kullanılabildiği gösterilmektedir. Bununla birlikte araştırmacılar, gerçek dünyadaki çevresel değişkenlerin ve farklı kamera koşullarının sistem performansını etkileyebildiğine dikkat çekmektedir.

Burada temel hedef yalnızca "bir hareket var" bilgisini üretmek değildir. Güvenlik sistemi mümkün olduğunca "ne hareket ediyor, nerede hareket ediyor, hareket normal mi ve güvenlik personelinin müdahalesini gerektiriyor mu?" sorularına yanıt verebilmelidir.

Kamera Sistemleri: İzlemeden Akıllı Analize

CCTV sistemleri uzun yıllardır havalimanı güvenliğinin temel araçlarından biridir. Terminal girişleri, güvenlik noktaları, bagaj alanları, otoparklar, kritik tesisler ve operasyonel bölgeler kameralarla izlenmektedir.

Ancak kamera sayısının artırılması tek başına güvenliği artırmaz. Çok sayıda kameranın aynı anda insan operatörler tarafından izlenmesi mümkün değildir. Bu nedenle modern güvenlik yaklaşımı "kamera izleme"den "video analitiği"ne doğru ilerlemektedir.

Video analitiği sayesinde belirli hareket biçimleri, olağan dışı davranışlar, belirli bölgelerde uzun süre kalma, ters yönde hareket veya belirlenmiş güvenlik bölgelerine girme gibi durumlar otomatik olarak işaretlenebilir.

Burada yapay zekânın rolü insan güvenlik görevlisinin tamamen ortadan kaldırılması değil, insan operatörün dikkatini gerektiren olayların önceliklendirilmesidir.

Bu ayrım önemlidir. Çünkü güvenlik sistemlerinin ürettiği her alarm gerçek bir tehdit değildir. Çok fazla yanlış alarm, güvenlik personelinin gerçek olaylara verdiği tepkiyi geciktirebilir. Bu nedenle modern sistemlerde alarm doğrulama ve insan-makine iş birliği önemli bir tasarım kriteridir.

Geçiş Kontrolü: "Kim, Nereye, Ne Zaman Girebilir?"

Havalimanı güvenliğinin en kritik alanlarından biri geçiş kontrolüdür. Çünkü havalimanında herkesin her bölgeye erişmesi mümkün değildir. Yolcuların kullandığı alanlar ile operasyonel alanlar, personel bölgeleri, apron, bagaj işleme alanları, teknik odalar, kargo tesisleri ve kritik altyapı birbirinden ayrılmalıdır.

Bu nedenle erişim kontrol sistemlerinin temel mantığı basittir: Bir kişinin kim olduğu, hangi alana erişim yetkisine sahip olduğu ve bu erişimin hangi zaman diliminde gerçekleşebileceği doğrulanmalıdır. Kartlı geçiş sistemleri bu yapının temel araçlarından biridir. Bunun yanında biyometrik doğrulama, parmak izi, yüz tanıma ve diğer kimlik doğrulama yöntemleri de giderek daha fazla araştırılmaktadır.

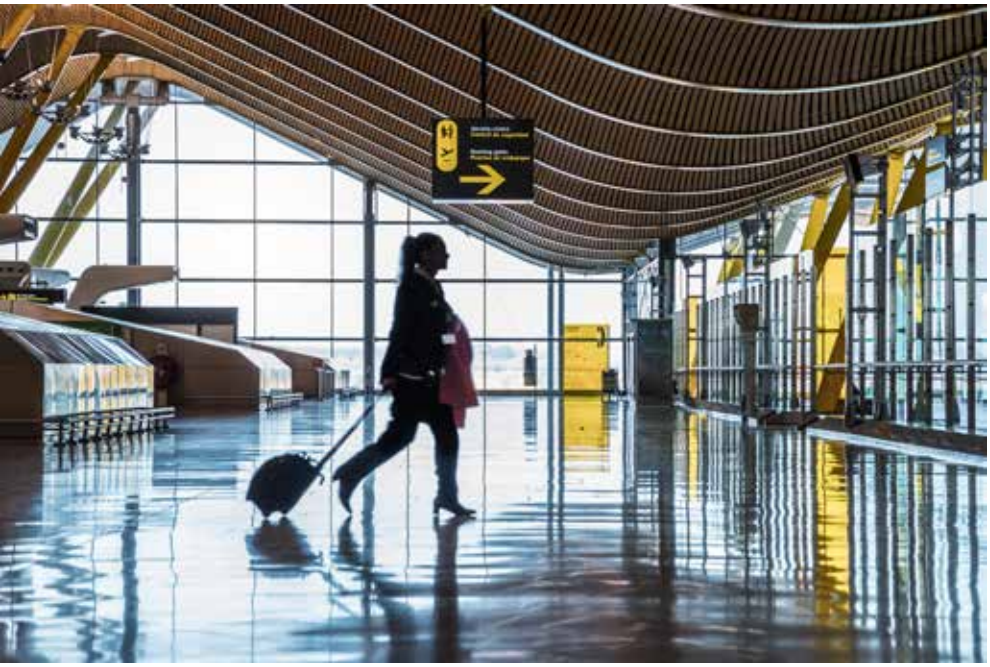
Ancak biyometrik teknolojilerin kullanımı yalnızca teknik bir konu değildir. Kimlik bilgilerinin korunması, kişisel verilerin işlenmesi, sistemlerin hata oranları ve farklı kullanıcı gruplarında ortaya çıkabilecek performans farklılıkları da değerlendirilmelidir.

ICAO'nun güvenlik yaklaşımında erişim kontrolü kritik güvenlik alanlarından biri olarak değerlendirilmektedir. ICAO'nun güvenlik denetim çerçevesinde yolcu ve bagajların korunmasının yanında, havalimanlarının kısıtlı ve güvenlik açısından kritik bölgelerine yetkisiz müdahalenin önlenmesi de temel güvenlik kontrolleri arasında sayılmaktadır.

Elektronik Güvenlik Sistemlerinin Birbirine Entegrasyonu

Modern havalimanında asıl dönüşüm, tek tek cihazlardan ziyade bu cihazların birbiriyle konuşabilmesidir.

Örneğin bir erişim kontrol sistemi yetkisiz bir kapı açılması tespit ettiğinde, yalnızca kapı üzerindeki alarmın çalışması yeterli değildir. Olayın güvenlik yönetim merkezine



iletilmesi, ilgili kameranın otomatik olarak olay bölgesine yönelmesi, olayın kayıt altına alınması ve gerekli personelin bilgilendirilmesi güvenlik zincirinin bir parçasıdır.
Bu nedenle güvenlik yönetim yazılımları, video yönetim sistemleri, erişim kontrol sistemleri, yangın alarm sistemleri ve diğer elektronik güvenlik çözümlerinin entegre çalışması önem kazanmaktadır.
Bu yaklaşım, havalimanının tek tek cihazlardan oluşan bir yapı olmaktan çıkıp "entegre güvenlik ekosistemi" haline gelmesini sağlar.

Yolcu ve El Bagajı Güvenliği

Yolcu güvenlik kontrol noktaları havalimanı güvenliğinin kamuoyu tarafından en fazla görülen bölümüdür. Ancak burada da teknolojik dönüşüm hızlı biçimde devam etmektedir.
Geleneksel X-ray sistemlerinde bagajların iki boyutlu görüntüleri incelenirken, bilgisayarlı tomografi yani CT teknolojileri bagajın üç boyutlu görüntüsünün oluşturulmasına olanak sağlamaktadır.
Bilimsel araştırmalar, CT teknolojisinin tehdit tespitinin otomatikleştirilmesi açısından önemli avantajlar sunduğunu ortaya koymaktadır.
Bununla birlikte görüntü kalitesi, işlem hızı, yanlış alarm oranı ve görüntülerin insan operatör tarafından değerlendirilmesi gibi unsurlar hâlen kritik önem taşımaktadır.
2026 yılında yayımlanan güncel bir derleme ise X-ray ve CT teknolojilerindeki gelişmelerin yapay zekâ destekli tehdit analizleriyle birleştiğini ortaya koymaktadır. Çalışmaya göre yolcu kontrol noktaları, uçak altı bagajı ve kargo güvenliği farklı operasyonel gereksinimlere sahip olduğundan, teknolojilerin uygulanması da aynı şekilde değerlendirilmelidir.

Yapay Zekâ Destekli X-Ray ve CT Analizi

Güvenlik taramasında yapay zekânın temel amacı insan operatörün yerine geçmekten çok, görüntülerde dikkat gerektiren nesnelerin belirlenmesine yardımcı olmaktır.
Derin öğrenme tabanlı sistemler; nesne sınıflandırma, nesne tespiti, görüntü bölütleme ve anomali tespiti gibi görevlerde araştırılmaktadır.
2022 tarihli kapsamlı bir akademik derleme, derin öğrenmenin X-ray güvenlik görüntülerindeki otomatik tehdit tespitinde giderek daha önemli bir araştırma alanı haline geldiğini göstermektedir.
Bununla birlikte havalimanı güvenliği açısından yapay zekânın önünde önemli bir problem vardır: gerçek tehditler normal bagajlara kıyasla çok daha az görülür.
Bu nedenle sistemin eğitiminde tehdit içeren görüntülerin azlığı, farklı havalimanlarındaki cihazların farklı görüntü üretmesi, bagajların birbirine karışmış görüntüleri ve yanlış alarm oranları önemli sorunlar yaratmaktadır.
2026 yılında IEEE'de yayımlanan bir çalışmada da sınıf dengesizliği, farklı havalimanları ve tarayıcılar arasında ortaya çıkabilecek veri farklılıkları, işlem süresi ve yanlış alarm oranı gibi konuların gerçek dünyadaki AI destekli bagaj taramasının önemli sorunları olduğu vurgulanmaktadır.
Dolayısıyla geleceğin güvenlik taraması yalnızca "AI tehdit buluyor" şeklinde düşünülmemelidir. Asıl hedef, AI'ın tespit ettiği şüpheli görüntüyü güvenlik görevlisinin hızlı ve doğru biçimde değerlendirebilmesini sağlayan insan-makine iş birliğidir.

Kayıtlı Bagaj ve Kargo Güvenliği

Havalimanı güvenliğinin önemli bir

bölümü yolcunun yanında taşıdığı bagajın dışında gerçekleşir.
Kayıtlı bagajın güvenlik kontrolü, bagajın kabulünden uçağa yüklenmesine kadar devam eden çok aşamalı bir süreçtir. Benzer şekilde kargo güvenliği de yalnızca terminalde yapılan bir kontrolden ibaret değildir. Kargonun kaynağı, tedarik zincirindeki güvenlik uygulamaları, tarama süreçleri ve uçağa yüklenmeden önceki kontroller bir bütün olarak değerlendirilir.
ICAO Annex 17, uçaklara yüklenmeden önce kargo ve postaya uygun güvenlik kontrollerinin uygulanmasını öngörmektedir. Bu kontroller fiziksel tarama yoluyla gerçekleştirilebildiği gibi güvenli tedarik zinciri mekanizmalarıyla da desteklenebilir.
Bu yaklaşım, havalimanı güvenliğinin terminal kapısında başlamadığını açık biçimde göstermektedir.

Personel ve İç Tehdit Riski

Güvenlik sistemleri çoğu zaman dışarıdan gelebilecek tehditlere odaklanırken, havalimanlarında yetkili erişime sahip kişilerin oluşturabileceği risk de ayrı olarak ele alınmalıdır.
Çünkü havalimanı çalışanları, yükleniciler, bakım ekipleri, temizlik personeli, teknik personel ve diğer çalışanlar operasyonel olarak yolculardan çok daha geniş alanlara erişebilir.
Bu nedenle personel kimlik doğrulaması, yetki seviyelerinin belirlenmesi, erişim kayıtlarının tutulması ve gerektiğinde erişim yetkilerinin hızlı biçimde iptal edilebilmesi önemlidir.
ICAO'nun güncel güvenlik yaklaşımı da iç tehdit konusunu özellikle vurgulamaktadır. Annex 17 kapsamında gerçekleştirilen güncellemeler

arasında iç tehditlerin daha iyi ele alınması ve havacılık güvenliği kültürünün güçlendirilmesine yönelik çalışmalar bulunmaktadır.

Yangın Güvenliği: Havalimanında İkinci Bir Güvenlik Katmanı

Havalimanlarında güvenlik kavramı yalnızca yasa dışı müdahalelerin önlenmesi anlamına gelmez.
Yangın, uçak kazası, yakıt kaynaklı olaylar, teknik arızalar ve diğer acil durumlar da havalimanı güvenliğinin önemli bileşenleridir.
ICAO Annex 14, aerodromların tasarım ve işletme standartları içerisinde kurtarma ve yangınla mücadele hizmetlerine özel önem vermektedir. ICAO'nun Airport Services Manual dokümanı ise kurtarma ve yangınla mücadele hizmetlerinde koruma düzeyi, kritik alan yaklaşımı, söndürücü maddeler, araçlar, itfaiye istasyonlarının konumu ve operasyonel prosedürler gibi konuları kapsamaktadır.
Havalimanı yangın güvenliğini terminal binası ile sınırlamak da doğru değildir.
Terminal binalarında yangın algılama ve alarm sistemleri, sprinkler sistemleri, yangın pompaları, acil aydınlatma, duman kontrolü, yangın kapıları ve tahliye sistemleri önemliyken; uçak park alanları, hangarlar, yakıt depolama ve ikmal alanları gibi bölgelerin kendine özgü riskleri vardır.
Özellikle uçak yakıtı ve büyük miktarda yanıcı maddenin bulunduğu operasyonel bölgelerde yangının erken tespiti ve hızlı müdahale kritik önem taşır.

Aircraft Rescue and Fire Fighting: Uçak Kurtarma ve Yangınla Mücadele

Havalimanı yangın güvenliğinin en özel alanlarından biri Aircraft Rescue and Fire Fighting, yani ARFF hizmetleridir.
Bu sistemin temel amacı yalnızca uçağın yanmasını önlemek değildir.

> Eğitimli personel, doğru prosedürler, güvenlik kültürü, düzenli tatbikatlar ve teknolojiyle insanın doğru şekilde bir araya getirilmesi aynı derecede önemlidir.

Esas amaç, bir uçak kazası veya olayında insanların hayatta kalabileceği koşulları oluşturmak, tahliye yollarını desteklemek ve kurtarılması gereken kişilere mümkün olan en kısa sürede ulaşmaktır.
ICAO, etkili kurtarma ve yangınla mücadelede eğitim, ekipmanın etkinliği ve personel ile araçların olay yerine ulaşma hızını temel faktörler arasında değerlendirmektedir.
ABD Federal Havacılık İdaresi de sertifikalı havalimanlarında ARFF hizmetlerine ilişkin eğitim, araçlar ve operasyonel gereklilikleri düzenlemektedir.
Dolayısıyla havalimanı yangın güvenliğinde "yangın söndürme" ile "kurtarma" birbirinden ayrı düşünülemez.

Acil Durum Yönetimi ve Koordinasyon

Havalimanlarında güvenlik olayları çoğu zaman tek bir kurumun müdahalesiyle çözülemez.
Bir acil durumda havalimanı işletmesi, itfaiye, sağlık ekipleri, güvenlik birimleri, havayolu şirketleri, hava trafik hizmetleri ve gerektiğinde kolluk kuvvetleri koordineli biçimde hareket etmek zorundadır.
Bu nedenle acil durum planlarının hazırlanması kadar düzenli olarak test edilmesi de önemlidir.
ICAO standartlarında acil durumlara yönelik planların hazırlanması ve belirli aralıklarla test edilmesi özellikle vurgulanmaktadır.
Bu noktada güvenlik teknolojileri operasyonel koordinasyonun önemli bir parçasıdır. Yangın alarmı, kamera görüntüsü, erişim kontrol bilgisi ve olay kayıtlarının aynı operasyon merkezinde bir araya getirilmesi, müdahale ekiplerinin olay hakkında daha hızlı bilgi edinmesine yardımcı olabilir.

Güvenlikte Siber Alanın Yükselen Önemi

Havalimanlarının dijitalleşmesi yeni bir güvenlik alanını da beraberinde getirmektedir: siber güvenlik.
Modern havalimanlarında check-in sistemlerinden bagaj yönetimine, erişim kontrolünden kamera sistemlerine, uçuş bilgi ekranlarından operasyonel haberleşmeye kadar çok sayıda sistem dijital altyapıya bağlıdır.
Bu nedenle fiziksel güvenlik ile siber güvenlik artık birbirinden tamamen ayrı düşünülemez.
Bir güvenlik kamerasının fiziksel olarak sağlam olması yeterli değildir; görüntünün güvenilir biçimde aktarılması ve yetkisiz kişilerin sisteme erişememesi de gerekir. Aynı şekilde bir erişim kontrol kapısının fiziksel olarak sağlam olması kadar, erişim yetkilerini yöneten dijital altyapının korunması da önemlidir.
ICAO, havacılık güvenliği kapsamında siber güvenliği de gelişen tehdit alanlarından biri olarak ele almakta ve havacılık siber güvenliği ile güvenlik mimarisinin geliştirilmesine yönelik çalışmalar yürütmektedir.

Güvenlikte En Zayıf Halka: İnsan Faktörü

En gelişmiş güvenlik teknolojileri bile insan faktöründen bağımsız değildir.
X-ray operatörünün dikkat düzeyi, güvenlik görevlisinin alarmı değerlendirme biçimi, bakım personelinin prosedürlere uyumu veya bir çalışanın şüpheli durumu bildirmesi sistemin genel performansını etkileyebilir.
Bilimsel araştırmalar da X-ray görüntülerinin değerlendirilmesinde insan faktörlerinin önemini vurgulamaktadır. Özellikle yoğun çalışma koşulları, dikkat ve deneyim gibi faktörler tarama performansını etkileyebilmektedir.
Bu nedenle geleceğin havalimanı güvenliği sadece daha fazla kamera, daha güçlü X-ray cihazı veya daha gelişmiş yapay zekâ anlamına gelmeyecektir.
Eğitimli personel, doğru prosedürler, güvenlik kültürü, düzenli tatbikatlar ve teknolojiyle insanın doğru şekilde bir araya getirilmesi aynı derecede önemlidir.

Geleceğin Havalimanı Güvenliği: Entegre ve Veri Odaklı Model

Havalimanı güvenliği giderek "tek cihaz" mantığından uzaklaşmaktadır.
Geleceğin güvenlik mimarisinde kamera sistemleri, çevre güvenliği, geçiş kontrolü, X-ray ve CT taraması, yangın algılama, alarm yönetimi, personel kimlik doğrulama, bagaj sistemleri ve siber güvenlik altyapısının aynı güvenlik ekosistemi içerisinde değerlendirilmesi beklenmektedir.
Bu dönüşümde yapay zekâ önemli

> Havalimanı güvenliğinin başarısı, bir olay meydana geldikten sonra ne kadar hızlı müdahale edildiği kadar, olay gerçekleşmeden önce riskin ne kadar erken fark edildiğiyle de ölçülecektir.

bir rol oynayacaktır. Ancak yapay zekânın güvenlik sistemlerinde kullanılmasında açıklanabilirlik, veri kalitesi, yanlış alarm oranı, farklı havalimanlarında genellenebilirlik ve insan denetimi gibi konular önemini koruyacaktır.

2026 yılında yayımlanan sistematik bir inceleme, havalimanlarında yapay zekâ çalışmalarının hızla arttığını ancak araştırmaların hâlen önemli ölçüde tekil uygulamalara odaklandığını ortaya koymaktadır. Çalışmaya göre özellikle güvenlik, insan faktörleri ve sistem düzeyindeki risk yönetiminin daha bütünleşik biçimde ele alınmasına ihtiyaç bulunmaktadır.

Bu sonuç, havalimanı güvenliğinin geleceği açısından önemli bir noktaya işaret etmektedir: Güvenlik, tek bir teknoloji projesi değil, bütün havalimanını kapsayan bir sistem mühendisliği yaklaşımıdır.

Sonuç

Havalimanı güvenliği, günümüzde fiziksel güvenlikten elektronik güvenliğe, yolcu taramasından yangınla mücadeleye, erişim kontrolünden kargo güvenliğine ve siber güvenlikten insan faktörlerine kadar genişleyen çok katmanlı bir yapı haline gelmiştir.

Çevre çitleri ve güvenlik kapıları fiziksel sınırı oluştururken; kameralar ve çevre algılama sistemleri bu sınırın izlenmesini sağlar. Geçiş kontrol sistemleri insanların ve araçların hangi alanlara erişebileceğini belirler. X-ray ve CT teknolojileri bagaj ve kargoların taranmasında önemli rol oynarken, yapay zekâ bu görüntülerin analizinde güvenlik personeline yardımcı olmaya başlamıştır.

Yangın güvenliği ise ayrı bir katman olarak değil, havalimanının genel acil durum ve yaşam güvenliği mimarisinin parçası olarak değerlendirilmelidir. ICAO'nun Annex 14 ve kurtarma-yangınla mücadele yaklaşımı, olay sonrasında yalnızca yangının söndürülmesine değil, insanların kurtarılmasına ve hayatta kalma koşullarının oluşturulmasına odaklanmaktadır.

Önümüzdeki dönemde güvenlik teknolojilerindeki en önemli değişim, cihazların daha akıllı hale gelmesinden çok, farklı sistemlerin ortak bir güvenlik anlayışı içerisinde birbirleriyle iletişim kurabilmesi olacaktır.

Çünkü modern havalimanında güvenlik; bir kamera, bir X-ray cihazı, bir güvenlik görevlisi veya bir erişim kontrol kapısından oluşmaz. Güvenlik, bütün bu katmanların birlikte çalışmasıdır.

GÜVENLİKTEDARİK.com

Son teknolojiye uygun, ürün ve çözümlerden HABERİNİZ VAR MI?

• Elektrik proje taahhüt firmaları • Bayi odaklı çalışan firmalar
• Havalimanları ilgili birimleri • Bankalar ilgili birimleri • İnşaat firmaları
• Oteller ilgili birimleri • Hastaneler ilgili birimleri • AVM'ler ilgili birimleri
• TÜRKLİM Üyeleri • Belediyeler ilgili birimleri • Emniyet Genel Müdürlüğü ilgili birimleri • Zincir mağazalar • Üniversiteler • Mimarlık ofisleri
• Sektör profesyonelleri AĞIMIZA KATILIN

TÜM TÜRKİYE'DE SESİNİZ OLALIM!

✔ CCTV ve video kontrol sistemleri,
✔ Yangın algılama ve ihbar sistemleri,
✔ Yangın söndürme sistemleri,
✔ Geçiş kontrol sistemleri,
✔ Hırsız alarm sistemleri,
✔ Alarm izleme merkezleri,
✔ Apartman konuşma sistemleri,
✔ Mobil takip sistemleri,
✔ Drone teknolojileri

Çok sayıda köklü firmanın çözüm ortağı olmuş ve geleceği tasarlamayı ilke edinmiş bir hizmet ajansı olan **ARKHE TANITIM HİZMETLERİ** tarafından hazırlanmaktadır. Bünyesinde GÜVENLİK YÖNETİMİ, PERPA GÜNDEM, TECHNEWS ve KURUMSAL YATIRIMCI dergilerini barındıran ARKHE TANITIM HİZMETLERİ; grafik tasarım, kurumsal kimlik çalışmaları, web ve her türlü promosyon ihtiyaçlarınıza fark yaratan tasarım, hız ve müşteriyi koruyan fiyat politikasıyla çözümler sunmaktadır.

Güvenlik Yönetimi

arkhe tanıtım hizmetleri

www.guvenlikyonetimi.com

Mağazalar Artık Düşünebiliyor: **Tepe Kurumsal'dan Yapay Zeka Destekli Operasyonel Yönetim**

Türkiye'nin entegre tesis yönetimi ve kurumsal hizmetler alanındaki lider markası Tepe Kurumsal, perakende sektöründe uzun yıllardır başarıyla sürdürdüğü entegre hizmet anlayışıyla sektörün dönüşümüne yön vermeye devam ediyor. Tepe Kurumsal sunduğu bütünsel hizmet yapısı sayesinde, mağaza içindeki tüm fiziki ve dijital altyapı görünmez bir koruma ve yönetim kalkanı olarak çalışırken, operasyonel riskler daha gerçekleşmeden engelleniyor.

ERCAN DEMİRAL / EGÇ GENEL MÜDÜR YARDIMCISI
TEPE GÜVENLİK

Perakende sektörü, dijital dönüşümün en radikal virajını dönüyor. Bugüne kadar sadece kayıp önleme ve ciro takibi üzerine kurulan geleneksel mağaza yönetim modelleri, yerini yapay zeka odaklı "Operasyonel Zekâ" kavramına bırakıyor. Güvenlikten operasyona, veri analizinden saha yönetimine kadar tüm süreçleri tek bir çatı altında birleştiren Tepe Kurumsal, uzun yıllardır başarıyla sürdürdüğü bu bütünsel iş modeliyle perakende dünyasındaki değişime liderlik etmeye devam ediyor.

ERCAN DEMİRAL

Yapay zeka destekli video analitiği: Kameralar artık sadece izlemiyor, düşünüyor!

Sektörün dinamiklerini uzun süredir bu vizyonla şekillendiren Tepe Kurumsal, işletmelere sıradan bir güvenlik veya operasyon hizmetinin çok ötesinde, yaşayan bir dijital sinir sistemi sunuyor. Şirketin güçlü altyapısıyla entegre çalışan RFID sistemleri, video analitik çözümleri, POS entegrasyonları, erişim kontrol mekanizmaları ve Alarm İzleme Merkezi sahada kusursuz bir senkronizasyonla işliyor. Tepe Kurumsal'ın sunduğu çözümlerin odağında yer alan yapay zeka destekli video analitik platformları, geleneksel CCTV sistemlerini sadece görüntü kaydeden pasif cihazlar olmaktan çıkararak proaktif birer karar mekanizmasına dönüştürüyor. Uçta analitik (Edge Analytics) ve yapay zeka algoritmalarıyla çalışan bu sistem; belirli bir reyon çevresindeki olağan dışı bekleme-leri anında yakalıyor, personel harici kişilerin yasaklı bölgelere veya dijital sınır çizgilerine girdiği an alarm üretiyor. Müşteri veya çalışanların düşme vakalarını saliseler içinde operasyon merkezine raporlayan teknoloji; değerli bir ürünün yerinden alınması ya da şüpheli bir paketin bırakılması gibi durumlarda da gerçek zamanlı risk sınıflandırması yaparak ekipleri hızla harekete geçiriyor.

"Sadece tesis hizmeti vermiyor, işletmelerin operasyonel zekasını yönetiyoruz"

Perakende sektörünün mevcut durumunu ve geleceğini değerlendiren Tepe Güvenlik EGÇ Genel Müdür Yardımcısı Ercan Demiral, geleneksel yöntemlerin artık günümüz hızına yetişemediğini belirterek şunları söyledi: "Geleceğin başarılı perakendecileri yalnızca gün sonu satış rakamlarını inceleyenler olmayacak. Gerçek liderler; riskleri daha doğmadan öngörebilen,

> "Geleceğin başarılı perakendecileri yalnızca gün sonu satış rakamlarını inceleyenler olmayacak. Gerçek liderler; riskleri daha doğmadan öngörebilen, müşteri davranışını milimetrik olarak okuyan ve operasyonlarını veriyle optimize eden kurumlar olacak.

müşteri davranışını milimetrik olarak okuyan ve operasyonlarını veriyle optimize eden kurumlar olacak. Çünkü artık mesele bir kriz anını yönetmek değil; o krizin hiç yaşanmamasını sağlayacak proaktif refleksi devreye almaktır. Tepe Kurumsal olarak biz sadece fiziksel güvenlik veya temizlik ve yönetim hizmeti vermiyoruz; yapay zekayı ve teknolojiyi arkamıza alarak işletmelerin operasyonel zekasını yönetiyoruz. Mağazalara sadece teknoloji kurmuyor, onlara yaşayan bir dijital sinir sistemi kazandırıyoruz" dedi.

Riskler gerçekleşmeden müdahale eden Tepe refleksi

Tepe Kurumsal'ın sahada fark yaratan en büyük gücü, yapay zeka destekli uzaktan izleme ve analiz yeteneklerini operasyonel tecrübesiyle birleştirmesi oluyor. Mağazalardaki kameraları sadece birer kayıt cihazı olmaktan çıkaran bu entegre hizmet yapısı; şüpheli davranışları, yetkisiz alan ihlallerini ve dijital sınır ihlallerini anında tespit ederek Tepe'nin uzman saha ekiplerini harekete geçiriyor. İş sağlığı ve güvenliği kapsamında müşteri veya çalışanların düşme vakalarını saliseler içinde operasyon merkezine bildiren sistem, değerli bir nesnenin yerinden oynatılması ya da şüpheli bir paketin bırakılması gibi durumlarda da anında risk sınıflandırması yapıyor. Tepe Kurumsal ekipleri, bu gerçek zamanlı veri akışı sayesinde olaylar henüz büyümeden, proaktif bir yaklaşımla duruma müdahale ediyor.

> "Tepe Kurumsal'ın sahada fark yaratan en büyük gücü, yapay zeka destekli uzaktan izleme ve analiz yeteneklerini operasyonel tecrübesiyle birleştirmesi oluyor.

Mimari varsayımlar yerini Tepe Kurumsal verilerine bırakıyor

Tepe Kurumsal, sunduğu yoğunluk haritalama (Heat Mapping) ve kişi sayım (People Counting) odaklı analiz hizmetleriyle perakendecilerin stratejik ve ticari kararlarına da doğrudan katkı sağlıyor. Mağaza içi müşteri hareketlerini anlık olarak ölçen bu sistemler, ziyaretçilerin satışa dönme oranlarını hesaplarken, hangi reyonların ilgi gördüğünü, hangi alanlarda yığılmalar yaşandığını ve hangi saatlerde yoğunluğun arttığını net bir biçimde raporluyor. Tepe Kurumsal'ın sağladığı bu operasyonel veri akışı sayesinde perakendeciler; personel planlamasını gerçek yoğunluğa göre yapıyor, kategori yönetimini güçlendiriyor ve promosyon alanlarını tamamen müşteri reflekslerine göre yeniden şekillendiriyor.

Tüm güvenlik sektörünü kapsayan **www.guvenliktedarik.com**; güvenlik sektörüne ürün ve hizmet sunan firmalarla nihai kullanıcının buluştuğu bir online alışveriş ve tanıtım sitesidir. Güvenliğin ihtiyaca uygun şekilde tesis edilmesi adına tüm ilgililerin ürün / hizmet alımı ve satımını hedefleyen **www.guvenliktedarik.com**; en son teknolojiye uygun ürün ve çözümlerden herkesi haberdar eden online platformdur.

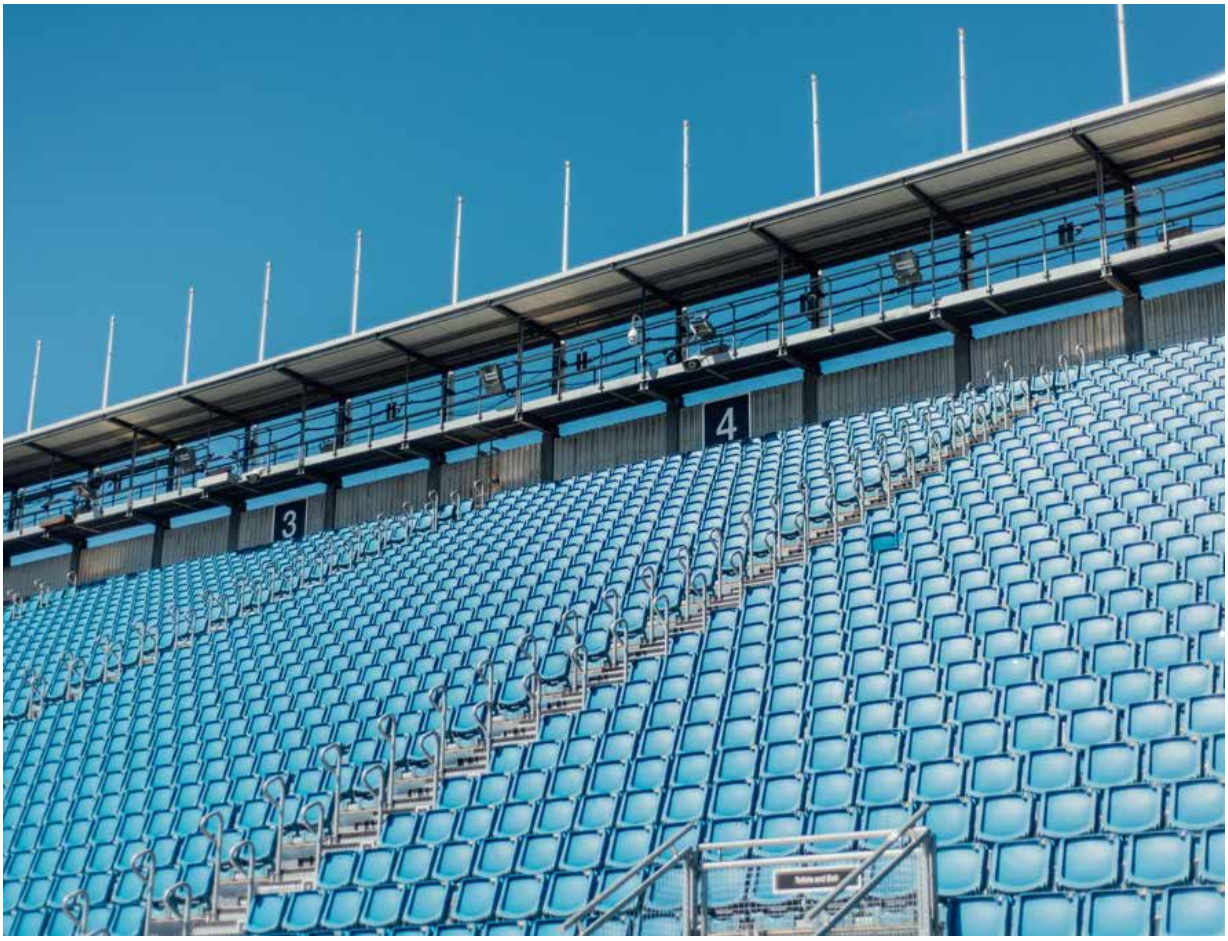
GÜVENLİKTEDARİK.com

- CCTV ve video kontrol sistemleri,
- Yangın algılama ve ihbar sistemleri,
- Yangın söndürme sistemleri,
- Geçiş kontrol sistemleri,
- Hırsız alarm sistemleri,
- Mobil takip sistemleri,
- Alarm izleme merkezleri,
- Apartman konuşma sistemleri,
- Drone teknolojisi

AI-Powered video güvenliği ile daha güvenli bir ziyaretçi deneyimi

"Stadyumlar ve arenalar artık sadece etkinlik günlerinde hayat bulan yerler değil. Giderek daha fazla, konserler, konferanslar, konaklama, perakende ve topluluk etkinlikleri için yıl boyunca merkezler haline geliyorlar. "

JOHN LUTZ BOORMAN / ÜRÜN VE PAZARLAMA MÜDÜRÜ,
HANWHA VİSİON AVRUPA



Stadyumlar ve arenalar artık sadece etkinlik günlerinde hayat bulan yerler değil. Giderek daha fazla, konserler, konferanslar, konaklama, perakende ve topluluk etkinlikleri için yıl boyunca merkezler haline geliyorlar. Tottenham Hotspur Stadyumu, futbol maçlarının ötesinde ek gelir ve izleyici kitlesi üreten bir mekan örneğidir. 2025 ticari geliri, dört National Football League (NFL) franchise'ına, yüksek profilli boks etkinliklerine ve Beyoncé yaz konser serisine ev sahipliği yapması nedeniyle 255,2 milyon £'dan 277,1 milyon £'a yükselmiştir.

Çok amaçlı mekanlar proaktif güvenliğe ihtiyaç duyar.

Ancak, bu mekanlar daha karmaşık ve çok yönlü hale geldikçe, yıl boyunca ziyaretçileri ve personeli güvende tutma zorluğu da artıyor. Güvenlik artık sadece olaylara yanıt vermekle ilgili değil; bunun yerine, stadyum liderliğinin güvenliği farklı etkinlik türlerine ve risk seviyelerine göre uyarlamasını, sağlık ve güvenlik ile bakımın üstesinden gelmesini ve pazarlama, satış, operasyonlar ve daha fazlasına değer katmasını sağlayan stratejik bir işlev haline geldi.

Daha da önemlisi, mekan işletmecileri yakında 2025 Terörizm (Tesislerin Korunması) Yasası'na, daha iyi bilinen adıyla Martyn Yasası'na uymak zorunda kalacaklar. Bu yasa,

JOHN LUTZ BOORMAN

Nisan 2025'te Kraliyet Onayı aldı ve 2027 baharında yürürlüğe girmesi bekleniyor. Uygulamanın beklenmesinden bir yıldan az bir süre kala, büyük halka açık mekanlardan sorumlu kuruluşlar, hazırlıklarını güçlendirirken olumlu bir ziyaretçi deneyimini nasıl sürdürebileceklerini giderek daha fazla değerlendiriyorlar.

2017'deki Manchester Arena saldırısının kurbanı Martyn Hett'in anısına adlandırılan bu yasa, mekan işletmecilerine terörizm riskini değerlendirme ve bir terör saldırısı meydana gelirse önlemeye, yanıt vermeye ve etkisini azaltmaya yardımcı olacak uygun önlemleri alma sorumluluğu getiriyor.

Özellikle, 800'den fazla katılımcıya sahip mekanlar için video gözetimi, araç erişim kontrolü, yer güvenliği gibi fiziksel koruma düzenli olarak değerlendirilmelidir. AI-Powered video çözümleri, Martyn Yasası kapsamındaki yükümlülüklerini yerine getirmelerine yardımcı olabilir.

Geleneksel video gözetiminden uzaklaşmak

Geleneksel video gözetim sistemleri her zaman mekan güvenliğinde kritik bir rol oynamıştır, ancak etkinlikleri genellikle onlarca, hatta yüzlerce video akışını aynı anda izleyen insan operatörlere bağlı olmuştur. Yoğun ortamlarda, özellikle güvenlik ekipleri büyük kalabalıkları, birden fazla giriş noktasını ve hızlı hareket eden durumları yönetirken, kritik detaylar gözden kaçabilir.

AI-Powered kameralar ve video yönetim sistemleri (VMS) ile operatörlerin artık birden fazla video, sohbet ve sensör veri akışını sürekli izlemeleri gerekmiyor. Bunun yerine, AI izleme yaparak şüpheli faaliyetleri, yetkisiz nesneleri (insanlar ve araçlar), kalabalık sıkışıklığını vb. işaretler ve operatörlerin gerektiğinde yanıt vermesini sağlar. Operatörler diğer faaliyetlere odaklanmakta serbest kalırken, sistem müdahale gerektiren olayları hızla bildirir ve olaylara hızlı yanıt vererek durumların tırmanmasını önlemeye yardımcı olur. Yer ekipleri ayrıca, bir kişi veya ilgi çekici bir aracı izlemelerine ve bulmalarına yardımcı olabilecek, giysi rengi, seyahat yönü ve potansiyel olarak silah taşıyıp taşımadıkları gibi bağlamsal, AI-Powered içgörülerden faydalanır.

Martyn Yasası'nı desteklemek Güvenlik ekiplerinin durumları daha ciddi bir hale gelmeden değerlendirmelerini ve yanıt vermelerini sağlayarak,

mekanlar Martyn Yasası'nın temelini oluşturan bazı hedefler için daha iyi hazırlanmış olur. Yasalar, kuruluşların tahliye, kilitlenme prosedürleri ve etkili iletişim gibi önlemlerle olaylara nasıl yanıt vereceklerini düşünmelerini gerektirerek hazırlığa özel bir vurgu yapar. Durumsal farkındalık, tüm bu dört unsur için temeldir.

Modern kameralar, operatörlere ilgi çekici bir olay veya nesnenin yüksek çözünürlüklü görüntülerini sağlar. Piyasada bulunan çoğu kamera 1080p çözünürlükten başlar ve 4MP, 6MP, 8MP veya 4K çözünürlük seçenekleri sunar. Kamera form faktörleri de gelişmiştir; kubbe, düz göz, mermi, balık gözü, pan-tilt-zoom (PTZ), termal ve çok yönlü modeller, mekanlara her boyutta alan ve gözetim ihtiyacına uygun bir dizi seçenek sunar.

Kapsamlı gözetim için gerçek zamanlı zeka650

Video gözetiminden elde edilen gerçek zamanlı istihbarat, operatörlere bir mekan ve çevresindeki ortamda neler olduğunu daha net bir şekilde anlamalarını sağlar. Hayati olarak, AI-Powered video analitiği ve AI nesne algılama, operatörlerin dikkat ve eylem gerektiren olayları kaçırmalarını önlemeye yardımcı olur.

Acil bir durumda, güvenlik ekipleri kalabalık hareketlerini izleyebilir, potansiyel darboğazları belirleyebilir, potansiyel bir saldırganın bilinen son konumuna doğru hareket edebilir ve halkı tehlikeli alanlardan uzaklaştırabilir. Bir saldırganın konumu, fiziksel görünümü ve seyahat yönü ile mekân içinde saklanan yaralılar veya kişiler hakkında bilgi, sahadaki personel ve acil servislerle paylaşılabilir, bu da daha hızlı ve daha etkili bir yanıtın koordine edilmesine yardımcı olur.

Operatör yanıt sürelerini ve verimliliğini daha da iyileştirmek için, bir kişi bir çizgiyi geçtiğinde ve belirli bir süre boyunca önceden tanımlanmış bir alanda kaldığında, örneğin, birden fazla analitik tetikleyiciye dayalı olarak uyarılar ayarlanabilir.

> Operatörler yalnızca bir mekânın içindeki etkinlikleri değil, aynı zamanda etkinliklerden önce ve sonra büyük kalabalıkların toplandığı çevredeki kamusal alanlardaki etkinlikleri de anlamaktan sorumludur.

Etkinlik sonrası verimli soruşturmalar

Etkinlik sonrası soruşturmalar için, operatörler videoda depolanan meta verileri kullanarak görüntüleri hızlıca arayabilir. Örneğin, gri bir üst giyen tüm kişilerin görüntülerini veya bunu daha da filtrelemek için gri bir üst giyen bir çocuğun görüntülerini çıkarabilirler. Bu, soruşturmaların yürütülme verimliliğini ve hızını artırır. Ayrıca, bir video analitik aracı bunu destekliyorsa, operatörler, aradıkları şeyi bir ifade veya cümle olarak girmelerine olanak tanıyan AI-Powered bir arama özelliğini kullanabilirler ve sistem onlara tüm ilgili sonuçları gösterir. Anlamsal arama olarak bilinen bu özellik, bir üretken AI aracını bir sonuca yönlendirmeye benzer şekilde daha doğal bir arama yoludur. Operatörler ayrıca belirli bir ilgi alanını seçerek o alanla ilgili tüm görüntüleri görebilir, bu da o alandaki hareketi hızlıca bulmalarını sağlar. Tüm kaydedilen video görüntülerinde o bölümdeki tüm hareketi görebilirler, örneğin, bir odada şüpheli bir paketi kimin bıraktığını görmek için. Bazı video analitik sistemleri, birden fazla kamera üzerinden benzer nesnelerin görüntülerini de çekebilir, bu da yoğun ve büyük bir etkinlik alanında hareket ederken bir araç veya ilgi çekici bir kişinin yönünü takip etmeye yardımcı olabilir.

Çevre ötesinde koruma

Modern mekân güvenliği giderek çevre çiti veya turnikeden öteye uzanıyor. Birçok yeni stadyum gelişimi, daha geniş eğlence bölgeleri, perakende destinasyonları ve karma kullanımlı topluluklar içinde yer alıyor. Sonuç olarak, operatörler yalnızca bir mekânın içindeki etkinlikleri değil, aynı zamanda etkinliklerden önce ve sonra büyük kalabalıkların toplandığı çevredeki kamusal alanlardaki etkinlikleri de anlamaktan sorumludur.

AI özellikli video, operatörlerin büyük alanları verimli bir şekilde izlemelerine, birden fazla konum ve karma kullanımlı tesisler (arena, perakende, ulaşım bağlantıları, depolama ve arka alanlar vb.) genelinde durumsal farkındalığı sürdürmelerine yardımcı olur. Operatörler, potansiyel riskleri kapsamlı bir şekilde anlayarak sorunlar büyümeden önce daha güçlü bir yanıt verme yeteneği kazanır.

Ek değer sağlama

Pazarlama, satış, bakım, personel ve temizlik gibi diğer departmanlara da katma değerli faydalar vardır. Yoğun dönemleri ve kalabalık akış desenlerini anlamak ve tahmin etmek, uzun kuyruk uzunluklarına uyarı vermek, tıkanıklık noktalarını belirlemek ve araç hareketlerini ve park yerlerini izlemek, ziyaretçi deneyimini iyileştirmeye ve etkinlik operasyonlarını kolaylaştırmaya yardımcı olur. Bu, bir gün bir futbol maçının, ertesi gün bir kurumsal etkinliğin ve sonraki gün bir konserin düzenlendiği, her seferinde farklı stadyum alanlarının kullanıldığı çok amaçlı mekânlar için özellikle faydalıdır.

Operatörlerin, insanların alanlarında nasıl hareket ettiğini ve kaynakların en iyi nerede konuşlandırılacağını görmeleri gerekir. AI-Powered video analitikleri, bu zekayı gerçek zamanlı olarak sağlayabilir.

Şimdi hazırlık zamanı

Mekân liderlerinin, Martyn Yasası yürürlüğe girmeden önce güvenlik stratejilerini güçlendirmek için kısa bir fırsat penceresi var. AI-Powered video güvenliğine yatırım yapmak, güvenliği proaktif, değer üreten bir işlev haline getirir ve günümüzün çok amaçlı etkinlik alanlarının ihtiyaçlarını karşılar, katılımcıların alışık olduğu ziyaretçi deneyimini sunmaya yardımcı olur.

Okul kapıları **güvenli tahliye** için yeterli mi?

14 Eylül'de milyonlarca öğrenci için yeni eğitim öğretim yılı başlarken, okullarda yangın güvenliği yeniden gündemde. MKS'ye göre güvenli tahliye yalnızca acil çıkış kapılarının bulunmasına değil; yangın ve dumanın yayılımını sınırlayan pasif güvenlik sistemlerinin, kaçış yollarının ve düzenli tatbikatların birlikte çalışmasına bağlı.

MKS METAL

Yaz tatilinin ardından okul koridorlarında ziller yeniden çalmaya hazırlanıyor. Millî Eğitim Bakanlığı'nın açıkladığı 2026-2027 eğitim öğretim yılı takvimine göre okullarda birinci dönem 14 Eylül 2026 Pazartesi günü başlayacak. Yeni dönemde milyonlarca öğrenci ve eğitim çalışanı yeniden okul binalarında bir araya gelirken, yapıların yangın güvenliği de yeniden önem kazanıyor. Türkiye'de yaklaşık 18 milyon öğrenci ve 1,2 milyon öğretmenin eğitim aldığı düşünüldüğünde, okullarda yangın anında hızlı ve güvenli tahliye büyük önem taşıyor. MKS'ye göre bu güvenlik yalnızca yangın söndürme cihazları veya acil çıkış kapılarının bulunmasıyla sağlanamıyor. Kaçış yollarının açık tutulması, yangın ve dumanın yayılımının sınırlandırılması, kapıların doğru özelliklerde olması ve tahliye planlarının düzenli olarak uygulanması gerekiyor.

Kapının bulunması yeterli değil

Yangın kapıları ve teknik metal kapı sistemleri üreticisi MKS, okullarda güvenli tahliyenin "kaçış kapısı var mı?" sorusundan daha kapsamlı değerlendirilmesi gerektiğine dikkat çekiyor. Yangın anında öğrencilerin güvenli biçimde binadan uzaklaşabilmesi için kaçış yollarının erişilebilir olması, kapıların

YUSUF ADNAN BOTANLIOĞLU

doğru özelliklerde seçilmesi ve yangın ile dumanın diğer bölümlere yayılmasının geciktirilmesi gerekiyor.

MKS Genel Müdürü Yusuf Adnan Botanlıoğlu, okul yangınlarında tahliye için kazanılan her sürenin kritik olduğunu belirterek şu değerlendirmede bulundu: "14 Eylül'de okullarda yeniden ziller çalacak ve milyonlarca öğrenci sınıflarına dönecek. Bu nedenle yangın güvenliğini yalnızca eğitim yılı başında kontrol edilen bir başlık olarak değil, sürekli yönetilmesi gereken bir güvenlik sistemi olarak görmek gerekiyor. Yangın kapısı, ancak doğru ürün, doğru mühendislik, doğru montaj ve düzenli bakımla görevini yerine getirebilir. Yangın anında kazanılacak birkaç dakika bile tahliyenin güvenliğini doğrudan etkileyebilir."

Türkiye'de yangın riski sürüyor

İstanbul Büyükşehir Belediyesi İtfaiye Dairesi Başkanlığı verilerine göre 2025 yılında İstanbul'da 27 bin 820 yangın ve 64 bin 628 diğer itfaiye olayı olmak üzere toplam 92 bin 448 olaya müdahale edildi. Yangınların 6 bin 545'i konutlarda, 323'ü fabrikalarda, 3 bin 677'si ise diğer binalarda meydana geldi.

Bu tablo, yangın güvenliğinin yalnızca yangının çıkış nedenine odaklanılarak ele alınamayacağını gösteriyor. MKS'nin değerlendirmesine göre yangının başlamasını önlemek kadar, başladıktan sonra bina içerisinde yayılmasını geciktirmek ve insanların güvenli şekilde tahliye edilmesine zaman kazandırmak da kritik önem taşıyor.

Okullarda denetimler sürüyor

Eğitim yapılarındaki yangın güvenliği konusunda denetimler de devam ediyor. 2026 yılında yayımlanan bir MEB açıklamasında okul, pansiyon, özel yurt ve özel kurslarda gerçekleştirilen denetimlerde elektrik tesisatı, bina mimarisi ve yangından korunma donanımlarının incelendiği belirtildi.

MEB'in okul güvenliği talimatlarında ise her kat için tahliye ve acil çıkış planlarının görünür noktalara asılması, acil çıkış kapılarının kilitli olmaması, yangın söndürme cihazlarının periyodik kontrollerinin yapılması ve yangın ikaz sistemlerinin çalışır durumda tutulması isteniyor.

MKS'ye göre bu uygulamaların tamamı aynı güvenlik zincirinin parçaları. Tahliye planının bulunması kadar, planda gösterilen çıkışların gerçekten kullanılabilir durumda olması da önem taşıyor.

Yangın kapıları tahliye süresini koruyor

AFAD, kapalı alan yangınlarında yangının yayılmasını önlemek amacıyla kapı ve pencerelerin kapalı tutulmasına dikkat çekiyor. Kurumun yangın güvenliği bilgilendirmesinde, başka bir odadan duman veya yanık kokusu gelmesi halinde kapının açılmaması gerektiği de belirtiliyor.

Bu yaklaşım, kapıların yangın sırasında yalnızca bir geçiş noktası olmadığını; yangın ve dumanın yayılımını sınırlamada önemli bir güvenlik unsuru olduğunu ortaya koyuyor.

MKS'ye göre yangın kapıları, yangın kompartımanları arasındaki geçişleri koruyarak alev ve dumanın yayılımını geciktirebiliyor. Bu nedenle özellikle öğrencilerin yoğun olarak bulunduğu eğitim yapılarında kapıların sertifikasyonu, yangına dayanım performansı, montajı ve kullanım koşulları birlikte değerlendirilmelidir.

Pasif ve aktif sistemler birlikte çalışmalı

Yangın güvenliği yalnızca yangın kapılarından da oluşmuyor. Sprinkler sistemleri, yangın alarm ve algılama sistemleri, acil aydınlatmalar ve söndürme ekipmanları aktif güvenlik sistemlerinin önemli parçalarını oluştururken; yangın kapıları, yangın kompartımanları ve benzeri yapısal çözümler pasif yangın güvenliğinin temel unsur-

ları arasında yer alıyor.
Uluslararası veriler de eğitim yapılarında çok katmanlı yangın güvenliğinin önemine işaret ediyor. ABD Ulusal Yangından Korunma Birliği'nin (NFPA) 2020-2024 dönemini kapsayan güncel verilerine göre, ABD'de itfaiye teşkilatları okul mülklerinde yılda ortalama yaklaşık 3 bin 230 yangına müdahale etti. Veriler, eğitim yapılarında yangın riskinin devam ettiğini gösterirken; yangının algılanması, yayılmasının sınırlandırılması ve öğrencilerin güvenli şekilde tahliye edilmesi için aktif ve pasif yangın güvenliği sistemlerinin birlikte çalışmasının önemini ortaya koyuyor.
MKS'ye göre bu veriler Türkiye'deki okullara doğrudan uyarlanabilecek bir yangın istatistiği değil; ancak eğitim yapılarında yangın güvenliğinin çok katmanlı biçimde ele alınmasının önemini gösteren uluslararası bir referans niteliğinde.

Tatbikatlar gerçek tahliyeye hazırlanıyor

Fiziksel güvenlik sistemlerinin yanı sıra öğrencilerin ve eğitim çalışanlarının yangın anındaki davranışlara hazırlıklı olması da önem taşıyor. MEB, 2025 yılında "Afetler ve Dayanıklılık Ayı" kapsamında ülke genelindeki okullarda eş zamanlı tatbikatlar gerçekleştirdi. Tatbikatlarda öğrencilerin okul binalarını güvenli şekilde tahliye etmeleri sağlanırken, yangın sırasında yapılması gerekenler de uygulamalı olarak anlatıldı.
MKS'ye göre düzenli tatbikatlar, acil çıkışların ve tahliye planlarının yalnızca kâğıt üzerinde kalmasını önlüyor. Özellikle küçük yaş gruplarının bulunduğu okullarda öğretmenlerin ve öğrencilerin tahliye rotalarını önceden bilmesi, acil durum sırasında yaşanabilecek panik ve karmaşanın azaltılmasına katkı sağlıyor.

"Yangın kapısı sürekli açık tutulmamalı"

Yangın kapılarının performansını belirleyen unsurlardan biri de kullanım sırasında doğru şekilde çalıştırılması. MKS, yangın kapılarının sürekli açık tutulması, önlerinin çeşitli eşyalarla kapatılması veya kapatma mekanizmalarının devre dışı bırakılması gibi uygulamaların yangın anındaki işlevi olumsuz etkileyebileceğine dikkat çekiyor.

MKS Genel Müdürü Yusuf Adnan Botanlıoğlu, bakım ve kontrolün önemini şöyle ifade etti:
"Bir yangın kapısının sertifikalı olması tek başına yeterli değil. Menteşeler, kapatıcı mekanizmalar, fitiller ve kilit sistemleri zaman içerisinde yıpranabiliyor. Kapının sürekli açık tutulması veya önüne eşya konulması da performansı etkileyebiliyor. Bu nedenle okullar açılmadan önce yapılacak kontrollerin yanı sıra eğitim yılı boyunca da düzenli bakım ve kontrollerin sürdürülmesi gerekiyor."

Yeni eğitim yılı öncesinde kontrol zamanı

14 Eylül'de başlayacak yeni eğitim öğretim yılı öncesinde okullarda yalnızca sınıfların ve dersliklerin değil, yangın güvenliği sistemlerinin de yeniden kontrol edilmesi gerektiğini belirten MKS; yangın kapıları, acil çıkışlar, alarm sistemleri, söndürme ekipmanları, tahliye planları ve tatbikatların birlikte değerlendirilmesini öneriyor.

Mühendislik odaklı üretim yaklaşımı

2007 yılından bu yana yangın kapıları ve teknik metal kapı sistemleri alanında faaliyet gösteren MKS, İstanbul Kartal'daki 9 bin metrekarelik üretim tesisinde; yangın kapıları, acil çıkış kapıları, metal kapılar, camlı kapılar, akustik kapılar, şaft kapıları, menfezli kapılar ve paslanmaz çelik kapılar başta olmak üzere geniş ürün gamıyla hizmet veriyor. Proje bazlı çalışan şirket; mühendislik desteğinden üretime, montajdan satış sonrası hizmetlere kadar tüm süreci tek çatı altında yönetiyor.
MKS, yeni eğitim öğretim yılı öncesinde okul yöneticilerine yangın güvenliğini yalnızca yasal bir gereklilik olarak değil, doğrudan insan hayatını ilgilendiren bütünsel bir güvenlik sistemi olarak ele alma çağrısında bulunuyor. Şirket, güvenli yapıların ancak doğru mühendislik, standartlara uygun ürün, doğru uygulama, düzenli bakım ve etkin tahliye planlarının bir arada uygulanmasıyla mümkün olabileceğinin altını çiziyor.

Elektrikli Araçlarda **Yangın Güvenliği Önlemleri**

Lityum bataryalarda meydana gelebilecek termal, mekanik ve elektriksel istismarların yanı sıra, yangın durumunda doğru müdahale yöntemleri ve yangının yayılmasını önlemeye yönelik yangın güvenliği önlemleri büyük önem taşımaktadır. Özellikle kapalı alanlarda bulunan elektrikli araç şarj istasyonlarında; pasif ve aktif yangın güvenliği tedbirlerinin, izleme sistemlerinin ve uygun mühendislik çözümlerinin birlikte değerlendirilmesi gerekmektedir.

MUSTAFA SALİH KORKMAZ / MÜHENDİSLİK VE KONTROL MÜDÜRÜ
EFECTİS ERA AVRASYA

Elektrikli araçların kullanımı, kişisel mobilite araçları ve binek otomobiller ile başlayarak kamyon, tır ve iş makineleri gibi uygulamalarla günden güne artarken; bu araçların yangın güvenliği önemli bir konu başlığı haline gelmiştir. Elektrikli araç yangınlarının temel sebebi pil paketlerindeki arızalardır.

Elektrikli araçlarda Lityum piller kullanılmaktadır. Lityum pilleri günlük hayatımızla iç içe olan pek çok cihazda kullanmaktayız. Cep telefonu, bilgisayar ve elektrikli araçların yanı sıra; sensörler, radyo iletişim cihazları, tıbbi cihazlar (kalp pilleri gibi) gibi uygulamalarda da tercih edilmektedir.

Lityum Pillerin Avantajları

- Diğer pil türlerine göre çok daha hızlı şarj ve deşarj (gerektiğinde yüksek güç çıkışı) olabilmekte; şarj kesintilerinden etkilenmemektedir,
- Çok daha yüksek kullanım ömrü bulunmaktadır,
- Hızlı sıcaklık değişimlerinden çok az etkilenmekte ve pil seviyesinden bağımsız stabil güç çıkışı sağlayabilmektedir,

Diğer pil türleriyle aynı şarj kapasitesini, genellikle yarısından daha az boyutlarda sağlayabilmektedir.

MUSTAFA SALİH KORKMAZ

Lityum Pillerin Dezavantajları

- Diğer pil türlerine göre daha pahalıdır,
- Bakım ve tamir işlemleri çok daha zahmetlidir,
- Hasar durumunda yangın ve patlama riski bulunmaktadır.

Batarya Yangınlarının Temel Sebepleri

- **Termal İstismar:** Dış ısı yahut alev kaynakları vasıtasıyla batarya hücresinin tutuşmasıdır.

Elektrikli araçlarda termal istismardan korunabilmek amacıyla batarya paketleri zırhlı bir dış çeper içerisinde bulunur ve özel soğutma sistemleri ile korunurlar. Bu sistemlerin düzgün çalıştığı durumlarda, iç sebeplerden termal istismar sebepli elektrikli araç yangını çıkma ihtimali çok düşüktür.

- **Mekanik İstismar:** Batarya hücresinin düşürme, ezilme ve delinme gibi fiziksel etmenler sebebiyle hasara uğrayarak tutuşmasıdır.

Mekanik istismardan korunabilmek amacıyla batarya paketinin tamamı fiziksel darbelere karşı zırhlarla korunmakta, ayrıca iç ünitelerde de ezilme ve delinme etkilerine karşı önlemler alınmaktadır. Tüm bu önlemlere rağmen ağır hasarlı kazalarda batarya paketi zarar görerek yangın çıkabilmektedir.

- **Elektriksel İstismar:** Bataryanın şarj esnasında; kapasitesi üstünde şarj edilmesi, yüksek gerilime maruz kalması, çok hızlı şarj yahut deşarj edilmesi gibi etmenler sebebiyle tutuşmasıdır.

Elektriksel istismar, elektrikli araçlarda en sık karşılaşılan yangın sebebidir.

Pil paketlerinde üretim kaynaklı kusurlar,

- Mekanik istismar sonucu oluşan mikro hasarlar,
- Pil şarj istasyonundaki üretim kaynaklı kusurlar, hatalı montaj ve/veya hatalı güç beslemesi, en önemli elektriksel istismar sebepleridir.

Termal Kaçak Nedir?

Lityum pillerin üretiminde, yanıcı ve patlayıcı özelliğe sahip Lityum tuzları kullanılmaktadır. Piller üzerinde meydana gelebilecek istismar faktörlerinden herhangi biri, pilin içeriğindeki yapıyı dengesizleştirerek, kimyasal reaksiyon ile ısı üretmeye başlamasına neden olabilir. Bu durumda kontrolsüz bir reaksiyon olan “termal kaçak” meydana gelebilir. Bu belirli bir seviyeye ulaşırsa, daha fazla ısı ve basınç üreten kimyasal reaksiyonları tetikleyerek pozitif geri besleme döngüsüne neden olur. Bu durum, pil ünitesi tamamen kendini yakıp tüketene kadar devam eder.

Yangın Durumunda Müdahale Nasıl Olmalıdır?

Pil yangınları, kapalı muhafaza içerisinde kimyasal kaynaklı yangınlar olduğu ve yüksek akım ile beslendikleri için günümüz imkan ve kabiliyetleriyle güvenilir bir şekilde söndürülememektedir. Batarya paketi ta-

mamen kendini tüketene kadar yanmaya devam etmektedir. Yangın durumunda alınabilecek en etkili önlem, yanan aracın çevresini tahliye etmek ve soğutma faaliyetleriyle yangının yayılmasını önlemektir.
İç mekanlarda çıkabilecek elektrikli araç yangınlarına karşı alınacak yangın mühendisliği önlemleri büyük önem arz etmektedir.

Elektrikli Araç Şarj İstasyonu Yangınlarını Önlemek İçin Neler Yapılabilir?

1. Şarj İstasyonlarının Elektriksel Güvenlik Önlemleri: Elektriksel istismar kaynaklı yangınları önleyebilmenin en önemli adımı, şarj istasyonlarının CE ve diğer ulusal ve uluslararası sertifikalara uygun modellerden seçilmesi; üretim kaynaklı kusurlara karşı kalite kontrol önlemlerini almış güvenilir bir markanın ürünlerinin tercih edilmesi, montaj ve güç beslemesi unsurlarının üretici firmanın yönergeleri ve Elektrik İç Tesisat Yönetmeliği'ne uygun olarak yapılmasıdır.

2. Pasif Yangın Güvenliği Önlemlerinin Alınması: Yangın durumunda can kaybını önleyebilmek için öncelikle mimari yangın güvenliği unsurları olan pasif yangın güvenliği önlemleri tam olarak uygulanmış olmalıdır. Bunlar:

- Acil durum tahliye planlaması; kaçış mesafeleri ve çıkışların uygunluk kontrolleri,
- Tahliye sırasında kullanılacak acil durum aydınlatma ve yönlendirme sistemlerinin doğru tasarım ve uygulamaları,
- Çıkan yangının ve/veya patlamanın yayılmasını durduran yangın kompartımanı ihtiyaçlarının belirlenmesi ve doğru şekilde uygulandığının teyit edilmesidir. Yangın kompartımantasyonu sağlanabilmesi için mahalin tüm duvarları, tabanı ve tavanı yönetmeliğin belirttiği yangına dayanım seviyesinde olmalı ve mahalden geçen tüm açıklıklar uygun yangına dayanımlı cihaz ve ürünlerle izole edilmelidir. (Yangın kapıları, damperler, pasif yalıtım uygulamaları gibi).

3. Aktif Yangın Güvenliği Önlemlerinin Alınması:

- Şarj istasyonu mahaline uygun söndürme sistemlerinin seçilmesi: Depo tavan yüksekliği, depolama tipi ve depolanan bataryaların kimyasal muhteviyatları göz önüne alınarak uygun söndürme sistemlerinin kullanılmasıdır. Batarya yangınlarında, ürün kendi kendini tüketene kadar tam olarak söndürme sağlanamasa bile, baskılama yapılarak yangının kontrol altına alınıp yayılmasının önüne geçilebilmektedir.
- Pil paketleri doğru akım (DC) kaynaklarıdır. Sulu soğutma ve müdahale sırasında elektrik şoku riskini önleyebilmek için birden fazla güvenlik önlemi alınması önerilmektedir.

4. İzleme ve Takip Önlemlerinin Alınması:

- Şarj esnasında akülerin hidrojen gazı çıkarması, yetersiz havalandırma durumlarında patlama riski oluşturmaktadır.

> "Bu seviyede yangın güvenliğinin sağlanabilmesi için, ulusal yangın yönetmeliğimizde olduğu kadar, güncel çalışmalar ve uluslararası yönetmelikler üzerinde de derin bir bilgi sahibi olmak gerekmektedir.

Uygun havalandırma, erken teşhis sistemleri ve acil müdahale planları, meydana gelirse termal kaçağın sonuçlarının hafifletilmesine de yardımcı olabilir,

- Termal görüntüleme, pil hücrelerinin sıcaklığını izlemek ve termal kaçağı önlemek için yararlı bir araç olabilir,
- İstasyonların izole alanlarda kurulması, şarj esnasında araçlar arasında ek mesafe bırakılması, yeterli manevra alanı sağlanması ve enerjiyi kesecek acil stop düğmelerinin bulunması da önemli güvenlik tedbirleri arasındadır,
- Şarj mahalinin amacı dışında kullanılması önlenmelidir.

Bu seviyede yangın güvenliğinin sağlanabilmesi için, ulusal yangın yönetmeliğimizde olduğu kadar, güncel çalışmalar ve uluslararası yönetmelikler üzerinde de derin bir bilgi sahibi olmak gerekmektedir.

Kesintisiz Koruma için **Ölçeklenebilir Güvenlik Modülleri**

Yeni güncelleme, küçük ve orta ölçekli işletmelerin mevcut teknoloji altyapılarını yeniden tasarlamaya gerek kalmadan, ihtiyaçlarına özel Güvenlik Modülleri ekleyerek korumalarını güçlendirmesine olanak tanıyor. Güvenlik Farkındalığı, E-posta Güvenliği, İş Yükü Güvenliği, Tehdit Arama ve Analizi ile Güvenlik Açığı Yönetimi modülleri, mevcut güvenlik altyapısının koruma kapsamını genişletiyor.

KASPERSKY

Küçük ve orta ölçekli işletmeler (KOBİ'ler) büyüdükçe, giderek daha çeşitli siber tehditlerle karşı karşıya kalıyor. Kaspersky'nin kurum içi araştırma merkezi tarafından gerçekleştirilen yakın tarihli bir araştırmaya göre, son bir yıl içinde KOBİ'leri etkileyen en yaygın dış tehditlerin başında kimlik avı (%20) ve yazılım güvenlik açıklarının istismar edilmesi (%17) geliyor. Öte yandan, bu kuruluşların siber güvenlik çözümü sağlayıcılarını değiştirmesinin başlıca nedenleri kurum içi sorunlardan kaynaklanıyor. Katılımcıların %26'sı mevcut çözümlerle uyumluluk ve entegrasyon sorunlarını, %23'ü ise birden fazla ürünü tek bir platformda birleştirme ihtiyacını temel nedenler arasında gösteriyor.
Bu veriler, e-posta, çalışanlar, iş yükleri ve güvenlik açıkları gibi alanlarda ortaya çıkan yeni güvenlik ihtiyaçları, KOBİ'leri süreçleri kolaylaştıran ve gereksiz karmaşıklığı ortadan kaldıran basit ve bütünleşik siber güvenlik çözümlerine yönelttiğini gösteriyor. Kaspersky Next Optimum için sunulan yeni Güvenlik Modülleri, müşterilerin ihtiyaçlarını adım adım karşılamasına, kendileri için en önemli özellikleri seçerek mevcut altyapılarına eklemesine ve güvenlik süreçlerini yönetilebilir tutmasına olanak tanıyor.

Kaspersky Next Optimum için yeni Güvenlik Modülleri

Kaspersky Next Optimum, Kaspersky Next ürün ailesinin KOBİ'lere yönelik çözümü olarak öne çıkıyor. Müşteriler, mevcut ihtiyaçları ve sahip oldukları kaynaklar doğrultusunda EDR, XDR ve MXDR yetenekleri arasından seçim yapabiliyor. İhtiyaçlar ve mevcut kaynaklar değiştikçe müşteriler bu yetenekler arasında sorunsuz şekilde geçiş yapabiliyor. Kaspersky Next Optimum artık KOBİ'lerin mevcut teknoloji altyapılarını değiştirmeden veya gereksiz bir karmaşıklık yaratmadan en kritik risk alanlarındaki korumalarını güçlendirmelerini sağlayan bir Güvenlik Modülleri seti de sunuyor.
Uç nokta, güvenliğin temelini oluşturmaya devam ederken, modüller korumayı cihazın ötesine taşıyarak saldırı zincirinin daha erken aşamalarında tehditlerin durdurulmasına yardımcı olan ek güvenlik katmanları sunuyor. Her bir modül, operasyonel kısıtlar, mevcut tehdit ortamı ve işletmelerin özel büyüme hedefleri dikkate alınarak gerçek dünyadaki iş ihtiyaçları doğrultusunda tasarlandı. Böylece KOBİ'ler, gereksiz operasyonel yük oluşturmadan, kendileri için kritik önem taşıyan senaryolara yönelik ihtiyaç duydukları araçlara sahip oluyor.

Yeni Güvenlik Modülleri şunları içeriyor:

- **Güvenlik Farkındalığı –** Özellikle siber güvenlik kültürünün henüz yeterince gelişmediği büyüyen ekiplerde kimlik avı, sosyal mühendislik ve kullanıcı hatalarından kaynaklanan riskleri azaltıyor.
- **E-posta Güvenliği** – E-posta kaynaklı tehditleri kullanıcılara ulaşmadan önce engelliyor, e-posta

altyapısı genelinde görünürlüğü artırıyor ve hassas iletişimlerin korunmasına yardımcı oluyor.

- **İş Yükü Güvenliği** – Hibrit bulut ortamlarını temel güvenlik kontrolleriyle koruyor. Buluta geçiş yapan veya dijital altyapısını hızla ölçeklendiren kuruluşlar için ideal bir çözüm sunuyor.
- **Tehdit Arama ve Analizi** – Şüpheli dosyaların derinlemesine analiz edilmesini sağlayarak olaylara müdahale süreçlerini hızlandırıyor, tehdit avcılığı sırasında uzman görüşü sağlıyor.
- **Güvenlik Açığı Yönetimi** Tüm BT varlıkları genelindeki güvenlik açıklarının tespit edilmesini ve giderilmesini kolaylaştırıyor. Özellikle hızla büyüyen veya dağınık BT ortamındaki güvenlik açıklarının tamamının tespit edilmesini ve giderilmesini kolaylaştırıyor.

Şirketler, bu amaca yönelik modülleri Kaspersky Next Optimum'un temel uç nokta, EDR, XDR ve MXDR yetenekleriyle bir araya getirerek esnek ve ölçeklenebilir bir güvenlik yaklaşımına sahip oluyor. Böylece koruma uç noktanın ötesine taşınırken tehditlerin cihaza ulaşmadan, güvenlik açıklarından yararlanmadan veya hesapları ele geçirmeden önce ele alınmasına yardımcı olunuyor ve en kritik alanlara odaklı koruma sağlanıyor.

Simüle Edilmiş Kimlik Avı Kampanyaları ve Ele Geçirilmiş Kimlik Bilgilerine İlişkin İçgörüler

Bunun yanı sıra Kaspersky Next Optimum, yerleşik simüle edilmiş kimlik avı kampanyaları ve ele geçirilmiş kimlik bilgilerine ilişkin içgörüler ile koruma yeteneklerini genişletiyor. Daha önce yalnızca Kaspersky Next XDR Optimum ve Kaspersky Next MXDR Optimum gibi en gelişmiş çözümlerde sunulan simüle edilmiş kimlik avı kampanyaları işlevi, müşterilerden gelen yoğun talep doğrultusunda Kaspersky Next EDR Foundations'a da dahil edildi. Önceden yapılandırılmış kimlik avı şablonları sayesinde çözümü kullanan yöneticiler gerçekçi kimlik avı simülasyonları gerçekleştirebiliyor, kullanıcıların hazırlık düzeyini test edebiliyor, bilgi eksikliklerini ortaya çıkarabiliyor ve güvenlik açısından risk taşıyan süreçleri belirleyebiliyor. Otomatik raporlama özelliği ise eğitim ihtiyaçlarının ve farkındalık düzeyindeki gelişimin zaman içinde takip edilmesini sağlıyor.

Bununla birlikte, Kaspersky Next MXDR Optimum, Kaspersky Digital Footprint Intelligence tarafından desteklenen uzman destekli tehdit avcılığı özelliğini sunuyor. Çözüm, sızdırılmış kimlik bilgilerini uyarılar ve şüpheli kimlik doğrulama girişimleriyle ilişkilendirerek olası hesap ele geçirme vakalarını daha erken tespit ediyor, olayların önceliklendirilmesini iyileştiriyor ve hesaplarla ilişkili risklere ilişkin kapsamlı görünürlük sağlıyor. Müşteri geri bildirimleri doğrultusunda yönetilen koruma deneyimi de müşteri geri bildirimleri doğrultusunda geliştirildi. Temel yönetim yetenekleri artık mobil cihazlar ve tabletler için optimize edilirken, Telegram üzerinden gönderilen olay bildirimlerinde olayın önceliği, etkilenen varlıklar, öneriler ve ilgili olaya doğrudan yönlendiren bir bağlantı yer alıyor.

Son olarak şirketler artık altyapılarını optimize edilmiş ve zaman kazandıran Pro View Console üzerinden yönetmeye başlayabiliyor ve güvenlik yaklaşımlarını baştan tasarlamak zorunda kalmadan daha ayrıntılı yönetim imkânı sunan Expert View Console'a sorunsuz şekilde geçiş yapabiliyor. Böylece kuruluşlar temel ihtiyaçlarla başlayıp işletmeleri hazır olduğunda yönetim yeteneklerini genişletebiliyor.

Kaspersky Birleşik Platform Ürün Grubu Başkanı Ilya Markelov konuya ilişkin değerlendirmesinde şu ifadeleri kullanıyor: "Günümüzün hızla büyüyen KOBİ dünyasında saldırı yüzeyi, siber güvenlik bütçelerinden ve mevcut kaynaklardan çok daha hızlı genişliyor. Kaspersky Next Optimum'un Güvenlik Modülleri; kurumların mevcut teknoloji altyapılarını yeniden tasarlamadan veya günlük iş akışlarını sekteye uğratmalarına gerek kalmadan ister kimlik avı farkındalığı ister e-posta güvenliği olsun, tam olarak kritik risk alanlarını güçlendirmelerini sağlıyor. Bu esneklik, küçük ve orta ölçekli işletmelerin güvenilir bir korumaya ulaşması önündeki geleneksel maliyet ve karmaşıklık bariyerlerini ortadan kaldırıyor."

Egemen Bulut İçin Verinin Yanı Sıra Kontrol de Yerelleşmeli

Yerel bulut alanları gecikmeyi düşürür ve veriyi yakına taşır; ancak egemenliği tek başına sağlamaz. DT Cloud Kurucu CEO'su Tolga Dinçer'e göre asıl soru, sunucunun nerede olduğu değil, platform üzerindeki karar ve müdahale yetkisinin nerede kaldığıdır.

TOLGA DİNÇER / KURUCU CEO
DT CLOUD

Verinin hangi ülkede tutulduğu, bulut hizmeti seçiminde kritik bir ölçüt. Özellikle kamu kurumları ile finans, enerji, sağlık ve savunma gibi sıkı düzenlemelere tabi alanlarda verinin ülke sınırları içinde kalması; uyum, güvenlik ve risk yönetimi açısından vazgeçilmez. Ancak dijital egemenlik, veri merkezinin posta adresinden daha geniş bir konu. Platform üzerindeki karar ve müdahale yetkisinin kimde olduğu, operasyonun nereden yürütüldüğü, kriptografik anahtarların nerede yönetildiği ve sağlayıcının hangi ülkenin hukukuna tabi olduğu da aynı ölçüde belirleyici. Avrupa Komisyonu'nun 1 Haziran 2026'da açıkladığı Egemen Bulut Çerçevesi de bu ayrımı somutlaştırıyor. Çerçeve, bulut hizmetlerini 48 kriter ve sekiz kategori üzerinden değerlendiriyor: stratejik egemenlik; hukuk ve yargı yetkisi; veri ve yapay zekâ; operasyon; tedarik zinciri; teknoloji; güvenlik ve uyum; çevresel sürdürülebilirlik. Verinin fiziksel konumu bu değerlendirmenin önemli, fakat tek başına yeterli olmayan unsurlarından biri.

Bu ayrım, Türkiye'de gündeme gelen yerel bulut alanları (local zones) açısından da önemli. Local zone; bilgi işlem, depolama, ağ ve belirli platform servislerini kullanıcıya veya verinin üretildiği noktaya yaklaştırarak düşük gecikme, gerçek zamanlı veri işleme, yapay zekâ çıkarımı ve veri yerleşimi gibi senaryolarda ciddi değer sağlar. Ancak birçok modelde bu alan, kendi başına egemen bir bulut bölgesi değil; başka bir ülkedeki ana bulut bölgesinin coğrafi uzantısıdır.

Bu, teorik bir ayrım değil. Önde gelen global sağlayıcıların resmî teknik dokümantasyonlarında, Local Zone kontrol düzlemi işlemlerinin en az bir bölümünün ana bölgede yürütüldüğü; benzer şekilde bazı Extended Zone modellerinde kontrol düzleminin ana bölgede kaldığı açıkça belirtiliyor. İş yükü ve uygulama verisi Türkiye'de bulunsa bile kimlik ve erişim, kaynak yaşam döngüsü, politika, anahtar yönetimi, izleme veya yönetim API'leri yurt dışındaki ana bölgeye

TOLGA DİNÇER

bağlı olabilir. Böyle bir mimaride veri düzlemi yerelleşir; kontrol düzlemi ise yerelleşmeyebilir. DT Cloud Kurucu CEO'su Tolga Dinçer, bu nedenle yer seçiminin tek başına egemenlik göstergesi olarak görülmemesi gerektiğini vurguladı: "Bulut bir lokasyon değil, bir kontrol topolojisidir. Sunucu Türkiye'de olabilir; fakat kaynak oluşturma, kimlik yönetimi, güvenlik politikası, şifreleme anahtarı, izleme ve ölçekleme kararları yurt dışındaki ana bölgeye gidiyorsa yalnızca veri düzlemi yerelleşmiş olur. Egemenlik, ihtiyaç anında karar ve müdahale yetkisinin ülke içinde kalmasıdır."

Local Zone'un Gerçek Testi: Ana Bölge Bağlantısı Kesildiğinde Ne Olur?

Egemenlik açısından en somut test, ana bölgeyle bağlantı kesildiğinde kurumun platform üzerindeki yönetim ve müdahale kabiliyetini sürdürüp sürdüremediğidir. Kurum böyle bir durumda yeni kaynak oluşturabiliyor mu? Uygulama devreye alabiliyor, kapasiteyi ölçekleyebiliyor, kullanıcı yetkilerini ve güvenlik politikalarını değiştirebiliyor, arızalı bileşenleri yeniden devreye alabiliyor mu? Mevcut sanal makinelerin çalışmaya devam etmesi tek başına yeterli değildir. Kritik yönetim işlemleri ana bölgedeki servislere bağlıysa operasyonel kontrol sınırlandırılmıştır.

Bu nedenle egemen bulut değerlendirmesi dört temel soruya net cevap vermeli: Verinin, yedeklerin, günlüklerin, meta verinin ve şifreleme anahtarlarının tamamı nerede? Kontrol düzlemini kim işletiyor ve ayrıcalıklı müdahaleler nereden yapılıyor? Hizmet sağlayıcısı ve alt yüklenicileri hangi hukuk düzenlerinin yetkisine tabi? Kurum API, veri formatı ve yönetim servisleri bakımından ne kadar bağımsız; iş yüklerini başka bir ortama taşıyacak gerçekçi bir çıkış planına sahip mi?

DT Cloud'un Yaklaşımı: Yerel Kaynak, Egemen Kontrol, Dağıtık Operasyon

DT Cloud, local zone yaklaşımını yabancı bir ana bölgenin Türkiye'deki uzantısını kurmak olarak görmüyor. Mimariyi; altyapı, egemen kontrol ve dağıtık operasyonu birbirini tamamlayan üç katmanda ele alıyor:

Foundation: Türkiye'deki çok bölgeli bilgi işlem, depolama ve ağ kaynaklarını; farklı üretici ve teknolojileri destekleyen, açık ve taşınabilir bir altyapı temeli üzerinde sunuyor. Böylece donanım veya tek bir teknoloji üreticisine bağımlılık azaltılıyor.

Cloud Management Platform (CMP): DT Cloud'un yerli ve egemen kontrol düzlemi olarak kaynak yaşam döngüsünü, kimlik ve politikaları, yerleşim kararlarını, kapasiteyi ve gözlemlenebilirliği ortak bir yönetim katmanında birleştiriyor. CMP yalnızca bir portal değil; farklı altyapılar üzerinde politika ve operasyon egemenliği sağlayan federatif kontrol katmanı olarak çalışıyor.

Continuum: Aynı yönetim modelini core ve bölgesel alanlardan endüstriyel ve taktik edge'e kadar genişletiyor. Edge Orchestrator merkezi politika, yerleşim ve yaşam döngüsünü yönetirken; Edge Manager yerelde operasyonel özerklik, politika uygulama ve bağlantı kesintilerinde çalışmaya devam etme kabiliyeti sağlıyor.

Bu mimari; Türkiye içindeki operasyon ekibi, yerel anahtar ve yetki yönetimi, BTK yetkilendirmeleri ve TCMB Topluluk Bulutu hizmet modelinin gerekliliklerini karşılayan kontrol çerçevesiyle tamamlanıyor. Böylece veri yerleşimi, operasyon, hukuk ve teknoloji boyutları aynı egemen bulut yaklaşımında bir araya geliyor.

Dinçer, DT Cloud'un yaklaşımını şöyle özetledi: "Bizim local zone yaklaşımımız, yurt dışındaki bir ana bölgenin Türkiye'deki uzantısını kurmak değil; aynı egemen kontrol düzlemi altında farklı lokasyonlarda yer alan çekirdek bulutlar ile yerel kaynak ve yerel hareket kabiliyeti oluşturmaktır. Normal zamanda tek platform olarak yönetilen, bağlantı kesildiğinde ise kritik operasyonlarını yerelde sürdürebilen bir yapı kuruyoruz. Egemenlik iddiası yalnızca SLA ile değil; API hâkimiyeti, anahtar yönetimi, ayrıcalıklı erişim, kriz anındaki müdahale kabiliyeti ve gerçek bir çıkış planıyla ölçülmelidir."

Tanımadığınız Kişilerden Gelen Hediye Tuzağına Karşı **6 Kritik Önlem**

Global siber güvenlik lideri Bitdefender, dünyanın en büyük oyun platformlarından Steam'de tanınmayan kullanıcılardan gelen hediye tekliflerinin ciddi bir dolandırıcılık aracına dönüştüğüne dikkat çekiyor.

ALEV AKKOYUNLU / BİTDEFENDER TÜRKİYE DİSTRİBÜTÖRÜ LAYKON BİLİŞİM OPERASYON DİREKTÖRÜ

Steam, kullanıcıların birbirine hediye olarak oyun göndermesine olanak tanıyan pratik bir özelliğe sahip. Ancak saldırganlar bu özelliği bir dolandırıcılık aracına dönüştürmüş durumda. Steam'in geliştiricisi Valve'ın da açıkça uyardığı üzere, tanınmayan bir kullanıcıdan gelen hediye çoğu zaman masum bir jest olmaktan uzak kalıyor. Bu tür teklifler; çalıntı bir kartla satın alınmış bir oyunun aklanması, nadir oyun içi eşyaların ele geçirilmesi ya da sahte bir bağlantı üzerinden hesap bilgilerinin çalınması gibi farklı amaçlara hizmet edebiliyor. Beklenmedik bir hediye çoğu zaman bir sohbet başlatmak, karşı tarafta bir zorunluluk hissi yaratmak veya tanınmayan bir hesabı güvenilir göstermek için kullanılıyor. Bu noktada Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, oyuncuların tanımadıkları kişilerden gelen hediyeleri kabul etmemesi gerektiğini vurguluyor.

"Tanımadığınız Birinden Gelen Hediye Çoğu Zaman Karşılığında Bir Şey Bekler"

Bu tür tekliflerin oyuncuları güven ve zorunluluk hissiyle hareket etmeye ittiğini belirten Bitdefender Türkiye Distribütörü Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, "Steam üzerindeki hediye dolandırıcılıklarının çoğu, oyuncuda bir minnet veya zorunluluk duygusu oluşturmayı amaçlıyor. Saldırgan çalıntı bir kartla aldığı

ALEV AKKOYUNLU

oyunu gönderiyor, ardından karşılığında oyun içi eşya, cüzdan kodu veya para talep ediyor. Bu takas, dolandırıcının çalıntı bir alışverişi temiz bir değere dönüştürmesini sağlarken, ödeme iptal edildiğinde oyuncuyu şüpheli bir işlemin ortasında bırakabiliyor. Özellikle genç oyuncular, bu tür bedava oyun ve eşya vaatlerine yetişkinlere göre daha kolay kanabiliyor ve çoğu zaman hesabı çalındıktan veya bir takasa ikna edildikten sonra durumun farkına varıyor. Bu nedenle ebeveynlerin, oyun oynayan çocuklarını tanımadıkları kişilerden gelen hediyeler konusunda önceden bilinçlendirmesi büyük önem taşıyor. Burada en etkili korunma yöntemi çok basit: Tanımadığınız birinden gelen hediyeyi kabul etmeyin ve karşılığında hiçbir şey göndermeyin." dedi.

Alev Akkoyunlu, Steam hediye dolandırıcılığına karşı alınması gereken 6 önlemi paylaşıyor:

1. Tanımadığınız kişilerden gelen hediyeleri reddedin. Teklif ne kadar cazip görünürse görünsün, tanımadığınız bir kullanıcıdan gelen hediyeyi kabul etmeyin. Bu, hem güvenliğinizi korumanın hem de hesabınızın olası kısıtlamalardan etkilenmemesinin en etkili yoludur. Valve da çalıntı hediyelerin kabul edilmesinin hesap kısıtlamalarına yol açabileceğini açıkça belirtiyor.

2. "Yanlışlıkla gönderdim" bahanesine kanmayın. Bazı saldırganlar önce küçük bir hediye göndererek güven kazanır, ardından pahalı bir şeyi yanlışlıkla gönderdiğini iddia ederek karşılığında nadir oyun içi eşyalar talep eder. Suçlama, hesabı şikayet etme tehdidi veya uydurma bir son tarih gibi baskı yöntemlerine karşı sakin kalın ve hiçbir şey göndermeyin.

3. Hesap doğrulaması isteyen bağlantılara asla tıklamayın. Bir hediyeyi "kabul etmek", yaş doğrulaması yapmak veya gönderenin profilini görüntülemek için giriş yapmanızı isteyen bağlantılar, hesabınızı çalmak için hazırlanmış sahte Steam kopyaları olabilir. Kullanıcı adı, şifre, Steam Guard kodu veya QR onayı isteyen hiçbir bağlantıyı kullanmayın.

4. Sizi Steam dışına yönlendiren tekliflere karşı dikkatli olun. Saldırganlar çoğu zaman konuşmayı Discord, Telegram gibi platformlara taşımaya çalışır. Ayrıca kendini Valve veya Steam Destek çalışanı olarak tanıtıp eşyalarınızı "doğrulamanızı" isteyen kişilere de güvenmeyin. Valve, çalışanlarının hesap sorunlarını asla sohbet uygulamaları üzerinden görüşmediğini belirtiyor.

> "Tanımadığınız birinden gelen hediyeyi kabul etmeyin ve karşılığında hiçbir şey göndermeyin

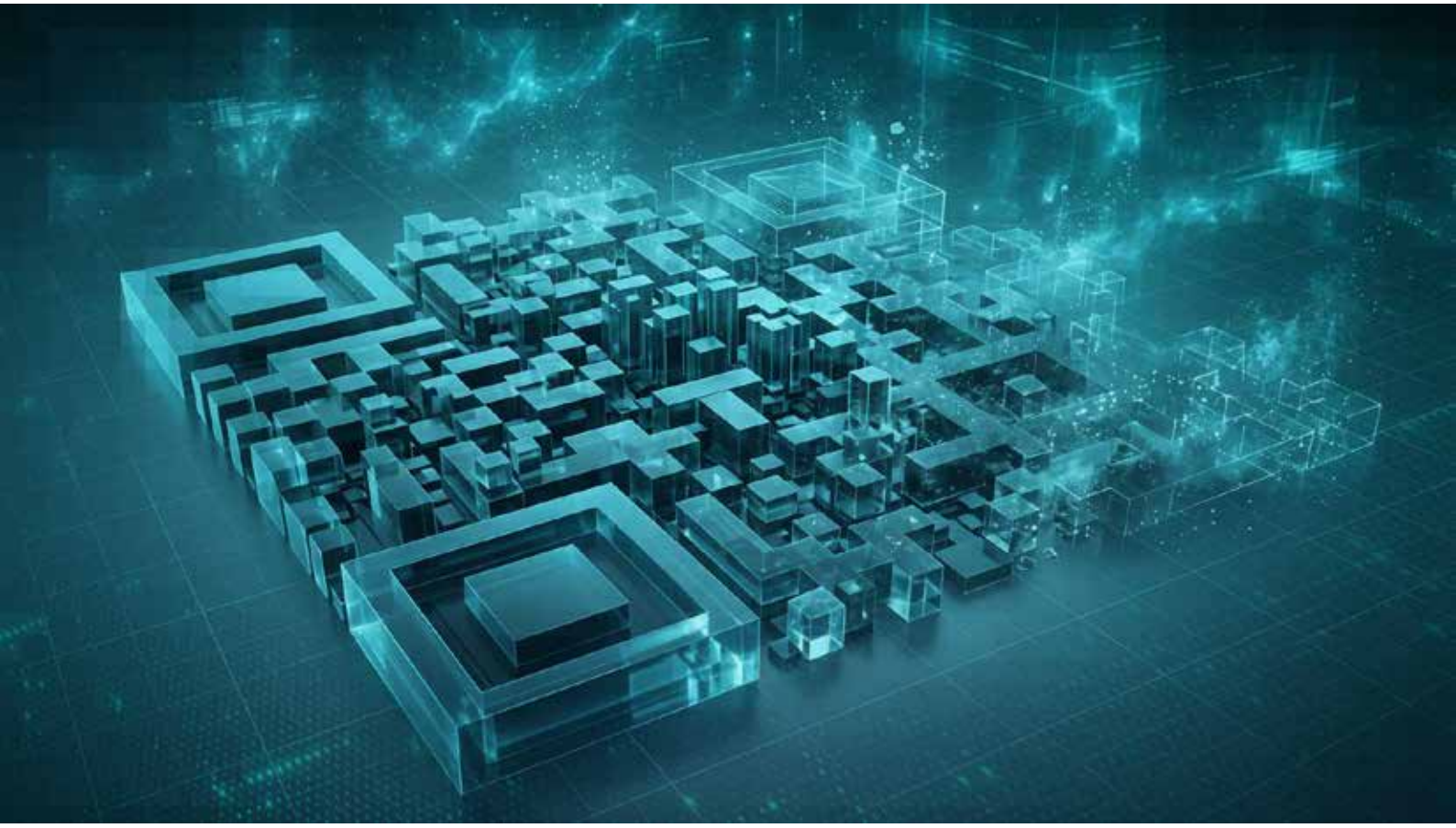
5. Oyun oynayan çocuklarınızı bu tuzaklara karşı bilinçlendirin. Bedava oyun ve nadir eşya vaatleri en çok genç oyuncuları hedef alır. Çocuğunuza, tanımadığı kişilerden gelen hediyeleri kabul etmemesi, karşılığında eşya veya bilgi göndermemesi ve şüpheli bir durumda mutlaka size danışması gerektiğini anlatın. Ayrıca bir arkadaşınızın hesabı da ele geçirilmiş olabileceğinden, tanıdığınız birinden gelen beklenmedik hediyeleri farklı bir iletişim yöntemiyle teyit edin.

6. Hesabınızı güçlü bir doğrulama ve güvenlik çözümüyle koruyun. Steam Guard'ı etkinleştirin ve hesabınız için benzersiz, güçlü bir şifre kullanın. İki adımlı doğrulama, şifreniz ele geçirilse bile saldırganın hesabınıza girmesini zorlaştırır. Bitdefender gibi güncel bir güvenlik çözümü ise sahte sayfaları ve zararlı bağlantıları tespit ederek ek bir koruma katmanı sağlar.

QR kodlu kimlik avı saldırıları kurumları hedef alıyor

Menülerde, sokak lambalarında, park alanlarında sıkça görülen; son yıllarda e-postalarda da giderek daha fazla yer alan QR kodlar siber saldırganların ilgi alanı olmaya devam ediyor. Bunun temel sebebi QR kodların kötü amaçlı bağlantıları gizlemek, bazı geleneksel kurumsal güvenlik filtrelerini atlatmak ve etkileşimi kurumsal bir bilgisayardan güvenlik kontrolleri daha az olan kişisel bir telefona aktarmak için siber suçlulara fırsatlar sunmasından kaynaklanıyor.

ESET



Çalışanları tuzağa düşürmek için yeni "quishing" yani QR kodlu kimlik avı teknikleri de ortaya çıkıyor. Siber güvenlik alanında küresel bir lider olan ESET, kurumların QR kod ile gelen tehditlerden korunabilmesi için bilinmesi gerekenleri paylaştı.

Quishing neden bu kadar tehlikelidir?

"Quick Response" (Hızlı Yanıt) kelimesinin kısaltması olan QR kodu, URL'leri, ödeme ayrıntılarını, iletişim bilgilerini ve diğer verileri kodlayabilen iki boyutlu bir barkod. Kullanıcıların A noktasından B noktasına hızlıca ulaşmasına yardımcı olur. Bu durumda hedef genellikle bir web sitesi veya uygulamadır. QR kodları, çeşitli nedenlerle siber tehdit aktörlerinin ilgisini çekiyor. Pandemi sırasında temassız etkileşimlere olan talebin de etkisiyle yaygınlaşan kullanımları, bu kodları taramayı günlük yaşamın sıradan bir parçası hâline getirmişti. Bu da birkaç yıl öncesine kıyasla bugün telefonlarımızı çıkarıp QR kodlarını tarama olasılığımızın daha yüksek olduğu anlamına geliyor. QR kodları kimlik avı iş akışlarına da mükemmel bir şekilde uyum sağlar; tek yapmanız gereken, kötü amaçlı bağlantıyı veya eki bir QR koduyla değiştirmektir. Aslında birçok kimlik avı kiti, özel bir QR kodu oluşturucuya sahiptir. En önemlisi, kurbanı nispeten iyi korunan bir kurumsal ortamdan potansiyel olarak yönetilmeyen bir mobil cihaza yönlendirerek kurumsal düzeyde güvenliği atlatırlar. Saldırgan için önemli bir avantaj da gizliliktir. Hedef, okunabilir metin olarak değil görsel bir desende kodlanmıştır; bu da arkasındaki kötü amaçlı URL'leri gizler ve bazı geleneksel e-posta filtrelerinin bunları ayıklayıp incelemesini engeller. Bazen PDF veya JPEG eklerine gömülerek daha da gizlenirler. Bu da çalışanların gelen kutularına ulaşma olasılıklarının daha yüksek olduğu anlamına gelir. Bu gerçekleştiğinde, çalışan gerçek bir mesajı kötü niyetli olandan ayırt etmekte zorlanabilir. Genellikle yazım hataları veya dil bilgisi hataları açısından analiz edilecek fazla metin yoktur. Ayrıca bağlantı, görsel bir desene etkili bir şekilde kodlandığından insan gözüyle görülemez. Güvenilir bir markayla birlikte kullanıldığında – örneğin, bir DocuSign e-postası veya Microsoft'tan gelen bir güncelleme – "quishing" saldırısı, klasik phishing mesajlarıyla benzer sosyal mühendislik taktiklerinden yararlanır. Güvenilir marka imajı, kurbanın bağlantıya tıklayabileceğine dair güven verir. Ayrıca genellikle bir bahaneyle aciliyet hissi yaratılır. Kötü amaçlı QR kodları, kullanıcıları hesaplarını güvence altına almaya veya bilgilerini doğrulamak için kimlik doğrulaması yapmaya teşvik eden uyarılara sıklıkla gömülür.

ESET 2026 Yılı İlk Yarı Tehdit Raporu'na göre, 2026 yılının ilk yarısında tüm phishing e-postalarının en az yüzde 11'inde kötü amaçlı QR kodları yer aldı. "ESET, 'QRCode/Phishing' algılama adı altında quishing e-postalarını adresinde takip etmektedir. Bu algılama, dosya türlerinin büyük çoğunluğundaki QR kodlarını tanımlamak ve içlerindeki URL'leri çözmek üzere tasarlanmış, ESET e-posta tarayıcısının özel bir katmanı aracılığıyla çalışır. Çıkarılan URL'ler, ESET'in kimlik avı önleme, kötü amaçlı yazılım önleme ve spam önleme motorları kullanılarak taranır;

zararlı URL'ler engellenir ve ilgili e-postalar işaretlenir veya silinir".

Tehdit aktörleri yenilik yapmaya devam ediyor

Herhangi bir tehdit ortamı eğiliminde olduğu gibi, kötü niyetli aktörler de maksimum etki elde etmek için çabalarını geliştirmeye devam ediyor. Quishing saldırıları, yalnızca kötü amaçlı yazılım yüklemek ve kimlik bilgilerini çalmak için değil, aynı zamanda MFA jetonlarını toplamak için de kullanılıyor. Güvenlik araştırmacıları, bu saldırıların farklı amaçlarla tasarlandığını da gözlemlemiştir:

- Kötü amaçlı yazılımın meşru uygulamalar gibi gösterildiği doğrudan uygulama indirmeleri yoluyla uygulama mağazası güvenliğini atlatmak.
- Kullanıcıyı kötü amaçlı veya oltalama web sitesine yönlendirmek yerine, doğrudan meşru bir sosyal medya, ödeme veya başka bir uygulamaya bağlamak. Bu, çeşitli senaryolarda kullanılabilir: Hesap ele geçirme: Kurban, kendi hesabında saldırganı doğrulamaya yönlendirilir. Kurban, alıcı bilgileri önceden doldurulmuş bir ödeme uygulamasına yönlendirildiği finansal dolandırıcılıkla karşı karşıya kalabilir.
- Kişi veya takvim zehirlemesi: Kötü amaçlı toplantı bağlantıları veya yeni kişi bilgileri yardımcı uygulamalara gömülür ve tıklandığında kullanıcıları kimlik avı sitelerine yönlendirir. Uzun, kötü amaçlı web adreslerini küçük bağlantılara dönüştüren ve bunları QR kodlarına gömen QR kodu kısaltıcılarını kullanarak güvenlik araçlarını gizlemek.

İşletmenizi Quishing saldırılarından koruyun

Neyse ki insan, süreç ve teknoloji ayarlamalarının doğru bir şekilde harmanlanması, kuruluşların maruz kaldığı quishing riskini büyük ölçüde azaltmaya yardımcı olabilir.

- Kullanıcı farkındalık eğitimlerine ve simülasyon tatbikatlarına "quishing" konusunu dâhil edin. Çalışanları, istenmeyen e-postalardaki QR kodlarını taramaktan kaçınmaya ve şüpheli her şeyi bildirmeleri konusunda teşvik edin. E-postanın güvenilir bir kaynaktan geldiğine inanıyorlarsa e-postadan ayrı olarak elde ettikleri iletişim bilgilerini kullanarak gönderenle tekrar teyit etmeleri gerekir.
- Saygın bir güvenlik sağlayıcısının sunduğu çözümün bir parçası olarak e-posta güvenliğini de içeren teknik kontrolleri değerlendirerek, quishing e-postalarının kullanıcıların gelen kutularına ulaşma riskini en aza indirin.
- Çalışanların cihazlarına bir mobil güvenlik çözümü ekleyerek kötü amaçlı sitelere ve diğer tehditlere erişimi engelleyin.
- Tüm hassas hesaplarda phishing'e karşı dayanıklı çok faktörlü kimlik doğrulama (MFA) uygulamasını zorunlu kılın; böylece kullanıcılar kandırılsa bile saldırganlar kurumsal sistemlere sızamayacaktır. Mobil cihaz yönetimi (MDM) araçları, tüm cihazların kurumsal politikaya uygun şekilde korunmasını sağlamanıza yardımcı olabilir.
- Saldırı yüzeyini azaltın, en az ayrıcalık ve tam zamanında erişim ilkelerini uygulayın.
- Güvenlik araçlarınız da dâhil olmak üzere tüm mobil işletim sistemlerini ve kurumsal yazılımları güncel tutun.
- Şüpheli etkinlikler için sürekli izleme yapın. En kötü senaryo durumunda olay müdahale planlarını uygulayın.

Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ

Özel Güvenlik Federasyonu'nun imtiyaz sahipliğini üstlendiği **Güvenlik Yönetimi Dergisi** havalimanları, Kamu Hastaneleri Birliği Genel Sekreterlikleri, AVM'ler, oteller, banka müdürlükleri, elektrik proje / taahhüt firmaları, inşaat şirketleri, TÜRKLİM (Türk Liman İşletmeleri) üyeleri, Emniyet Genel Müdürlükleri, Özel Güvenlik Daire Başkanlığı ve Özel Güvenlik Şube Müdürlükleri, bayi odaklı çalışan firmalara ve sektör profesyonellerine ulaşmaktadır. Gerek içeriği ve gerekse özel dağıtım ağıyla, sektörün nabzını tutan dergimiz, GÜSOD, GESİDER, ASIS ve ÖGF ile aynı platformda yer almaktadır.

Kapak, Fokus ve Özel Dosya konularımız başta olmak üzere, dergimizde sizin de projelerinize, teknik yazı ya da makalelerinize, ürün/sistem anlatımlarınıza ve reklamlarınıza yer vermek istiyoruz.

Turkcell Dergilik

www.guvenlikyonetimi.com

TurkTelecom E-dergi

Güvenlik Yönetimi

ÖZEL GÜVENLİK SEKTÖRÜNÜN SESİ

Editöryel Takvim

	KAPAK KONUSU	FOKUS KONUSU	ÖZEL DOSYA KONUSU
OCAK	Biyometrik Sistemler	Otel Güvenliği	Bina Otomasyon sistemleri
ŞUBAT	Para ve Kıymetli Eşya Taşıma	Spor Güvenliği	Drone Teknolojileri
MART	Yangın Algılama Sistemleri	AVM Güvenliği	VIP Koruma
NİSAN	Geçiş Kontrol Sistemleri	Endüstriyel Tesis Güvenliği	Toplumsal Davranış Psikolojisi ve Özel Güvenlik
MAYIS	CCTV ve Çevre Birimleri	Tarihi Varlıklar ve Müze Güvenliği	Acil Anos ve Seslendirme Sistemleri
HAZİRAN	Ulaşım Güvenliği	Tünel Uygulamaları	Hemşire Çağrı Sistemleri
TEMMUZ	Şehir izleme Sistemleri	Deniz ve Liman Güvenliği	Alarm İzleme Merkezleri
AĞUSTOS	Veri Yedekleme ve Depolama	Havalimanı Güvenliği	Dünyada ve Türkiye'de Özel Güvenlik
EYLÜL	Yangın Söndürme Sistemleri	Okul Öğrenci ve Kampüs Güvenliği	Duman Kontrol ve Tahliye Sistemleri
EKİM	Bilgi Güvenliği	Hastane Güvenliği	Güvenlikte Kablo
KASIM	Araç Takip Sistemleri	Kritik Tesis Güvenliği	Çevre Güvenliği
ARALIK	Sektöre Yön Verenler	Mağaza Güvenliği	Afet ve Tahliye Güvenliği

REKLAM INDEKS

19

65

15

23

9

5

11

13

AK

17

45

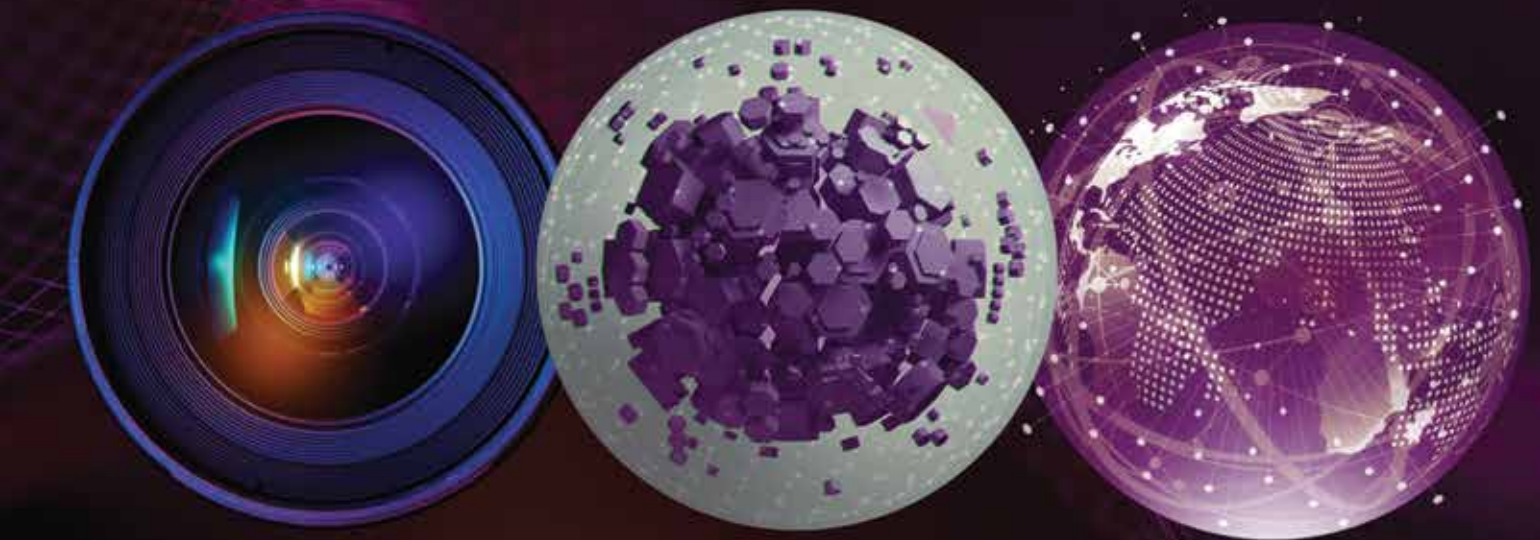
70

9

Western Digital.

GÜVENLİK GÖZETİMİNDEN

ÖTE



YAKALAYIN **DEPOLAYIN** **ANALİZ EDİN**