ISSN:1305-3698

CAD CAM CAE DÜNYASI

www.cadcamcaedunyasi.com.tr

Nisan Mayıs Haziran 2024 Sayı: 74 Yıl: 20 Fiyatı: 125 ₺

CadCamCae Dünyası

Prestij Yayıncılık

PLM Teknolojileri ve Hizmetleri
3D Printer Sistemleri Dergisi

PLM Technology and Services
3D Printer Systems Magazine

DELL TECHNOLOGİES
Dell Technologies'den
Yapay Zekâ Araştırması

ESET
Verilerimizi Neden
Korumamız Gerekir?

KASPERSKY
Kötü Amaçlı Mobil
Bankacılık Yazılımları
2023'te Küresel Çapta
%32 Büyüdü

CADCAMCAE Dünyası Dergisi

PRESTİJ YAYINCILIK BASIM HİZMETLERİ SAN. ve TİC. LTD. ŞTİ.
Adına İmtiyaz Sahibi / *Publisher*
Kenan ANIL

Sorumlu Yazı İşleri Müdürü / *Editor in Chief*
Kenan ANIL (yazi@prestijyayincilik.com.tr)

Yazı İşleri / Editor
yazi@prestijyayincilik.com.tr

Kurumsal İletişim Direktörü /
Corporate Communications Director
Hayriye ANIL

Reklam ve Halkla İlişkiler Yetkilisi
Advertising and Public Relations Officer

Grafik Tasarım / *Graphic Design*
Durmuş ÖZELÇİ

Kapak Tasarımı / *Cover Design*
Durmuş ÖZELÇİ

Web Sorumlusu / *Web Responsible*
Durmuş ÖZELÇİ

Video Kurgu / Montaj / *Video Editing*

Abone Sorumlusu / *Subscription*
Hayriye ANIL

Hukuk Danışmanı / *Law Adviser*
Av. Yakup Lütfi KÜÇÜK

Mali Danışman / *Financial Responsibility*
Mali Müşavir Mustafa Macır

YAYIN KURULU / *Editorial Board*
(yazi@prestijyayincilik.com.tr)

YAYIN KURULU
Prof. Dr. Ali ORAL (Balıkesir Üni.),
Doç. Dr. H. Alpay ER (Özyeğin Üni.),
Prof. Dr. Bilgin KAFTANOĞLU (Atılım Üni.),
Doç.Dr. Fehmi ERZİNCANLI (Düzce Üni.),
Prof.Dr. M. Cemal ÇAKIR (Uludağ Üni.),
Prof. Dr. Mustafa KURT (Mar. Üni),
Doç. Dr. M. Emre İLAL (İzmir Yük. Tek.),
Öğr.Gör. Jülide EDİRNE (Haliç Üni.),
Doç. Dr. İbrahim SAKLAKOĞLU (Ege Üni.)

DANIŞMANLAR KURULU
Tonay Abay (ÜÇGEN YAZILIM),
Cem Şirolu (YENASOFT),
Burak S. Pekcan (info(+)TRON),
Aydın Çıkın (GRUPOTOMASYON),
Tayfun Erkeskin (TET BİLGİSAYAR),
Ayhan Bebitoğlu (PLASTOSEL),
Salih Bozkurt (DEFNE MÜHENDİSLİK),
Dr. Erdal Gamsız (SES 3000),
Ferhat Teker (BAŞKENTCADCAM),
Emre Öztürk (ANOVA),
Orkun Nuras (ORSA),
Mustafa Erten (TEKYAZ)
Tolgahan KÖROĞLU (DESİTA YAZILIM)
Yönetim Merkezi / Management Centre

PRESTİJ YAYINCILIK BASIM HİZMETLERİ
SAN. ve TİC. LTD. ŞTİ.
Talatpaşa Mah. Gülbaşak Sk. No: 2/B 34400
Kağıthane - İstanbul
Tel: 0 212 320 36 90 (pbx)
Fax: 0 212 320 36 91

İnternet: www.cadcamcaedunyasi.com.tr
e-mail: info@prestijyayincilik.com.tr
Nisan Mayıs Haziran 2024 Yıl: 20 Sayı: 74
Dergi Üç Ayda Bir Yayınlanır.
Basın Kanununa Göre Yerel-Süreli Yayındır."
Dergimiz Dijital Ortamda Yayınlanıp Basılı Hali Yoktur.

Yayın Tarihi: Haziran 2024

editörden

kenananil@prestijyayincilik.com.tr

Değerli Okuyucu Dostlarımız,


Kenan ANIL

Dolu dolu bir mayıs ayı geçirdik. BHTS 2. Uluslararası Boğaziçilsıl işlem sempozyumu ve sergisi Haliç kongre merkezinde gerçekleşti. Yoğun bir ziyaretçinin olduğu sempozyum çok güzel gerçekleşti. Firmaların gerçekleştirdikleri etkinlikler ve fuarlar. Her günü dolu geçen bir mayıs.

Bu sayımızda EFRS Demir Çelik sempozyumu ve Win fuarı ve arkasından Kurban bayramı. İslam aleminin Kurban Bayramını kutlar. Bu vesileyle insan katliamı yapan İsrail'in bir an önce vahşi savaşı bitirmesini diliyorum.

Bizler müşteri memnuniyetini artırmak amacıyla 2012 yılından beri dijital ortamda dergilerimizi yayınlayarak ve sosyal medyada güncelliği korumak amacıyla hizmetlerimizi sürdürmekteyiz.
Basılı yayınlarımızı kargo yolu ile iletirken dijital ortamda sizlere ulaşılmasının rakamlarla raporlanmasını gerçekleştirebiliyoruz.

Yaptığımız bu hizmetlerle çağın yapay zekası ile sizlere değer katmaya devam ediyoruz. Bundan dolayı sektörün haber akışını sağlamak için bizleri desteklemenizi bekliyoruz. Bu zamana kadar destekleyenlere teşekkürlerimizi bir borç biliyoruz.

Bu süreç için de üretimde ki yenilikleri ve sektör haberlerini bizlere olan güvenizle sizlere her kanaldan ulaştırmaya çalışıyoruz.

Bizi izlemeye devam edin. Sizlerin verdiği güçle çalışmaya devam ediyoruz.

Güçlü ve sağlıklı yarınlar için. Gelecek nesillere güzel günler bırakmanın bilinciyle sağlıkla kalın.

bitis yazılım dayanışma ve korunma birlikteliği

Sektörel Yayıncılar Derneği Üyesidir.
www.sevad.org

içindekiler

içindekiler...

*Kapakta kullanılan görsel **Dell Technologies Haberine** aittir.*

Reklam İndeksi

DELL POWEREDGE SUNUCULAR, VERİ MERKEZİNDEN UÇ NOKTAYA İŞ YÜKLERİNİ DESTEKLİYOR

Dell Technologies'in genişletilmiş yeni sunucu portföyü, Dell'in büyük müşterilerine, bulut hizmeti sağlayıcılarına (CSP'ler) ve küçük işletmelere çeşitli iş yüklerinin üstesinden gelebilecek bilgi işlem gücü sunuyor.

Dell Technologies, Dell PowerEdge'in kullanıldığı her ortam için performans ve verimlilik yükseltmeleriyle sektörün en çok satan sunucu portföyünü genişletiyor. Bu sunucular, Dell'in her büyüklükteki müşterisine hizmet veren en yeni nesil sunucu inovasyonunu temsil ediyor.

Çok yönlülük ön planda tutularak tasarlanan bu yeni Dell PowerEdge sunucuları, her ölçekteki CSP'ler, küçük işletmeler ve uçta faaliyet gösterenler de dâhil olmak üzere kuruluşlar için işlemleri basitleştirmeyi amaçlayan verimli yapılandırmalar sunuyor. Yeni sunucularda elde edilen performans iyileştirmeleriyle müşteriler, çeşitli iş yüklerinin üstesinden gelebilecek bilgi işlem gücüne sahip oluyor.

Dell Technologies Altyapı Çözümleri Grubu Ürün Yönetimi Kıdemli Başkan Yardımcısı Travis Vigil, konuyla ilgili olarak, "Müşterilerimiz bir yandan güç ve emisyon yönetimine odaklanırken bir yandan da daha yoğun bilgi işlem iş yüklerini yönetmek için en yeni sunucularımıza yöneliyor. Bu, Dell PowerEdge'in BT altyapısının belkemiğini oluşturduğu, müşterilerin değişen iş taleplerine uyum sağlamasına yardımcı olduğu ve uç, veri merkezleri ve buluttaki iş yüklerini desteklediği otuz yıllık deneyimimize dayanıyor" dedi.

BULUT HİZMETİ SAĞLAYICILARI İÇİN GELİŞMİŞ PERFORMANS VE VERİMLİLİK

Yeni Dell PowerEdge R670 CSP Edition ve R770 CSP Edition sunucuları, bulut servis sağlayıcılarına sanallaştırma ve veri analizi gibi yüksek yoğunluklu ve ölçeklenebilir bulut iş yükleri dâhil olmak üzere yüksek performanslı bilgi işlem için optimum performans sunuyor. Ayrıca Dell Erken Erişim Programı sayesinde müşteriler, bu yeni sunucu tasarımlarını değerlendirebiliyor, böylece CSP'ler kullanıma sunulduğu ilk günden itibaren üretimi ölçeklendirebiliyor.

Akıllı Soğutma teknolojisiyle tasarlanan bu sunucular, enerji verimliliğine sahip olup değişen çevresel koşullara dinamik olarak uyum sağlıyor. Bunun yanında müşterilerin önceki nesle kıyasla raf başına 2,3 kata kadar daha fazla performans elde etmeleri öngörülüyor. Sunucularda, büyük, heterojen ortamlar için açık bir ekosistemde yönetimi kolaylaştırmak adına OpenBMC ™ üzerine kurulu Dell Open Server Manager da bulunuyor.

Yeni CSP Edition sunucular, Dell PowerEdge portföyüne ilk kez Veri Merkezi - Modüler Donanım Sistemi (DC-MHS) mimarisini getiriyor. Bu DC-MHS spesifikasyonu, sunucuları standartlaştırarak, tasarımı geliştirerek ve müşteriler için daha fazla seçenek sunarak mevcut altyapıya daha kolay sunucu entegrasyonunu destekliyor. Open Compute Project'in bir parçası olan DC-MHS; veri merkezi, uç ve kurumsal altyapı genelinde birlikte çalışabilirliği artırmak için donanım teknolojisini yeniden tasarlamayı amaçlayan, Dell Technologies ve Intel'in de dâhil olduğu altı şirketin ortak bir çalışması olarak karşımıza çıkıyor.

Intel Corporation Intel® Xeon® Verimli Çekirdekli Ürünler Başkan Yardımcısı ve Genel Müdürü Ryan Tabrah, konuyla ilgili "Intel olarak, Dell Technologies'in, çeşitli sektörlerdeki müşterilerin geleceğin yapay zekâ veri merkezleri için yüksek yoğunluklu, verimli bilgi işlem vaadini hızlı ve sorunsuz bir şekilde yerine getirmelerini sağlayan en yeni nesil Intel® Xeon® 6 işlemci geliştirmemizde ön saflarda yer almasından heyecan duyuyoruz" diye konuştu.

DAHA KÜÇÜK AYAK İZİ, İKİ KAT PERFORMANS

Dell PowerEdge T160 ve R260 sunucuları, güçlü ve yoğun konfigürasyonlar arayan küçük işletmelere ve uzak ofislere kompakt bilgi işlem gücü sağlıyor. Fiziksel ayak izi neredeyse yarıya inen (yüzde 42) T160, boyanmamış metal şasi de dâhil olmak üzere sürdürülebilir malzemelerin daha fazla kullanılmasıyla daha düşük bir karbon ayak izi sunuyor. Sunucu, önceki nesle kıyasla yüzde 23'e kadar daha fazla güç tasarrufu sağlıyor. R260 sunucu ise yüzde 24 oranında düşürülmüş fiziksel ayak izi ve artırılmış çok yönlülüğüyle öne çıkıyor.

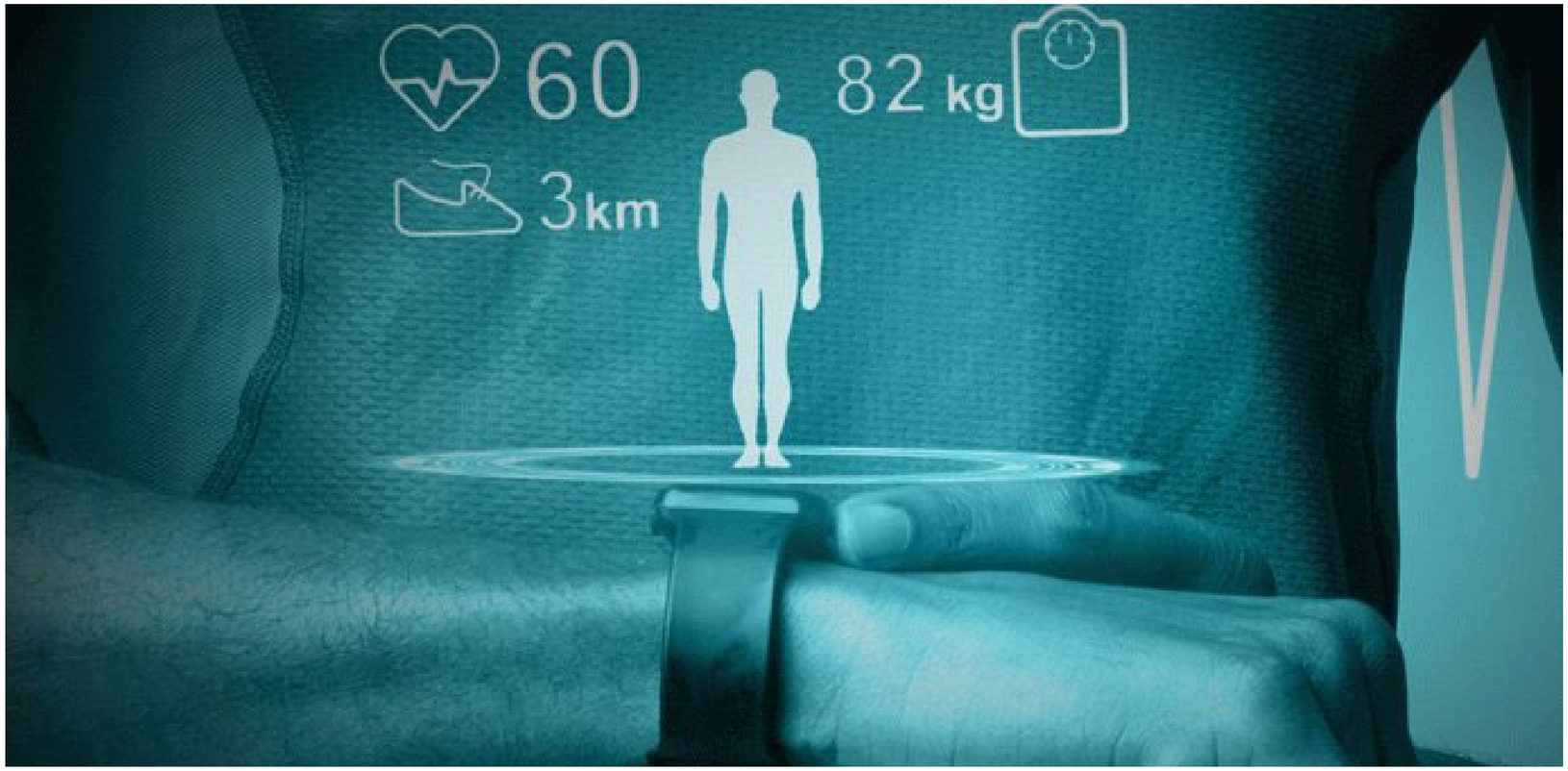
Her iki sunucuda da Intel® Xeon® E-2400 işlemciler bulunuyor ve önceki nesle kıyasla iki kat daha fazla performans sunuluyor. T160, uç noktalara yakın kurulumlarda gerçek zamanlı veri işlemeye ihtiyaç duyan kuruluşlar için tasarlanmış bir sunucu olarak karşımıza çıkıyor. Uç noktalara yakın sanallaştırma dağıtımları için optimize edilmiş R260 ise gecikme süresini yüzde 50'ye kadar azaltıyor.

Zorlu ortamlar için tasarlanan T160 ve R260, toz ve yağ parçacıklarından koruyan, daha iyi performans ve akustik için engelsiz hava akışı sağlamaya yardımcı olan filtre çerçevelerine sahip iç donanımıyla da dikkat çekiyor.

IDC Kurumsal Altyapı Uygulaması Araştırma Başkan Yardımcısı Kuba Stolarski, Dell'in portföyüyle ilgili olarak "Performanstan ödün vermeden enerji verimliliğini ve altyapı yoğunluğunu en üst düzeye çıkaran teknoloji, modern sürdürülebilir veri merkezi operasyonları için kritik öneme sahip. Dell'in portföyü, her ölçekten kuruluşa sürdürülebilirlik hedeflerini karşılayacak yenilikçi sunucu çözümleri sunarken, yönetimi basitleştiriyor ve son teknolojiyle performansı yükseltiyor" dedi.

SATIŞ TARİHİ

- Dell PowerEdge R670 CSP Edition ve R770 CSP Edition, Temmuz ayında yetkili Bulut Servis Sağlayıcıları için küresel olarak satışa sunulacak ve genel kullanım için çok yakında piyasaya sürülecek.
- Dell PowerEdge T160, Mayıs ayında global olarak satışa sunulacak.
- Dell PowerEdge R260 Mayıs ayında tüm dünyada satışa sunulacak.



GİYİLEBİLİR CİHAZLAR GİZLİLİK RİSKİ TAŞIYOR MU?

Akıllı saatler, fitness takip cihazları ve diğer giyilebilir cihazlar cep telefonlarımız ve tabletlerimiz kadar olağan hale geldi. Bu bağlantılı cihazlar saati söylemekten çok daha fazlasını yapıyor. Sağlığımızı takip ediyor, e-postalarımızı görüntülüyor, akıllı evlerimizi kontrol ediyor ve hatta mağazalarda ödeme yapmak için bile kullanılabiliyorlar.

iyilebilir cihazlar günlük hayatımıza her zamankinden daha fazla girerken aynı zamanda daha fazla veri topluyor ve giderek artan sayıda başka akıllı sistemlere bağlanıyor. Bu potansiyel güvenlik ve gizlilik risklerini önceden anlamakta fayda var. Tehdit aktörlerinin akıllı giyilebilir cihazlara ve ilgili uygulama ve yazılım ekosistemine yönelik saldırılardan para kazanmalarının birçok yolu bulunuyor. Verileri ve şifreleri ele geçirip manipüle edebilir ve kayıp ya da çalıntı cihazların kilidini açabilirler. Kişisel verilerin üçüncü taraflarla gizlice paylaşılmasıyla ilgili potansiyel gizlilik endişeleri de var.

GİYİLEBİLİR CİHAZLARIN EKOSİSTEMLERİ NEREDE YETERSİZ KALIYOR?

Taktığınız cihaz resmin yalnızca bir parçası. Aslında cihazın yazılımından uygulamasına bağlantı için kullandığı protokollere ve arka uç bulut sunucularına kadar birden fazla unsur vardır. Güvenlik ve gizlilik üretici tarafından gerektiği gibi dikkate alınmadıysa hepsi saldırıya açıktır. İşte bunlardan birkaçı:

Bluetooth: Bluetooth Düşük Enerji genellikle giyilebilir cihazları akıllı telefonunuzla eşleştirmek için kullanılır. Ancak yıllar içinde protokolde çok sayıda güvenlik açığı keşfedildi. Bu açıklar, yakın mesafedeki saldırganların cihazları çökertmesine, bilgileri gözetlemesine veya verileri manipüle etmesine olanak sağlayabilir.

Cihazlar: Genellikle cihaz üzerindeki yazılım, kötü programlama nedeniyle harici saldırılara karşı savunmasızdır. En iyi tasarlanmış saat bile nihayetinde insanlar tarafından üretilmiştir ve bu nedenle kodlama hataları içerebilir. Bunlar da gizlilik sızıntılarına, veri kaybına ve daha fazlasına yol açabilir. Ayrıca cihazlardaki zayıf kimlik doğrulama/şifreleme, cihazların ele geçirilme ve gizli dinlemeye maruz kalması anlamına gelebilir. Kullanıcılar, giyilebilir cihazlarındaki hassas mesajları/verileri halka açık yerlerde görüntülerken omuz sörfçülerinin de farkında olmalıdır.

Uygulamalar: Giyilebilir cihazlarla bağlantılı akıllı telefon uygulamaları bir başka saldırı yoludur. Kötü yazılmış ve güvenlik açıklarıyla dolu olabilirler ve kullanıcı verilerine ve cihazlarına erişimi açığa çıkarabilirler. Uygulamaların ve hatta kullanıcıların veriler konusunda dikkatsiz davranması da ayrı bir risktir. Meşru uygulamalar gibi görünmek üzere tasarlanmış sahte uygulamaları yanlışlıkla indirebilir ve kişisel bilgilerinizi bunlara girebilirsiniz.

Arkadaki sunucular: Belirtildiği gibi sağlayıcıların bulut tabanlı sistemleri, konum verileri ve diğer ayrıntılar dahil olmak üzere cihaz bilgilerini depolayabilir. Bu, saldırganlar için cazip bir hedef teşkil eder. Güvenlik konusunda iyi bir geçmişe sahip saygın bir sağlayıcı seçmek dışında bu konuda yapabileceğiniz pek bir şey yoktur.

GİYİLEBİLİR CİHAZLARI GÜVENDE TUTMAK İÇİN İPUÇLARI

- Saygın giyilebilir cihaz sağlayıcılarını seçmeye özen gösterin.
- Doğru yapılandırıldıklarından emin olmak için gizlilik ve güvenlik ayarlarını yakından inceleyin.
- Yetkisiz eşleştirmeyi önlemek için ayarları değiştirin.
- İki faktörlü kimlik doğrulamayı açın.
- Kilit ekranlarını parola ile koruyun.

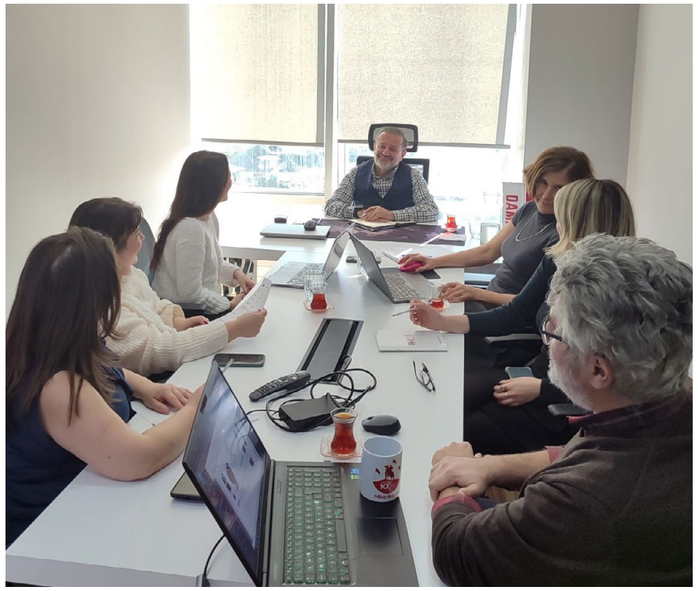
AKILLI TELEFONUNUZU KORUYUN:

- Yalnızca yasal uygulama mağazalarını kullanın
- Tüm yazılımları güncel tutun
- Cihazları asla jailbreak/root etmeyin
- Uygulama izinlerini sınırlayın
- Cihaza saygın bir güvenlik yazılımı yükleyin

AKILLI EVİNİZİ KORUYUN:

- Giyilebilir cihazları ön kapınızla senkronize etmeyin
- Cihazları misafir Wi-Fi ağında tutmaya özen gösterin
- Tüm cihazları en son aygıt yazılımına güncelleyin
- Tüm cihaz şifrelerinin fabrika varsayılan ayarlarından değiştirildiğinden emin olun

SAVUNMA, HAVACILIK VE UZAY SEKTÖRLERİNİN DİJİTAL PLATFORMU DAMISE, İHRACATA KATKI SAĞLIYOR



Savunma havacılık, uzay ve denizcilik sektörlerinde faaliyet gösteren firmalara yönelik hayata geçirilen "DAMISE" hem dijital bir pazaryeri hem arama motoru hem de dijital ihracat süreçlerinin yönetimini sağlayan bir yapı olarak faaliyet gösteriyor. Kullanıcıları arasında NATO "Türk Endüstri Günü" etkinliğinde DAMISE platformu üzerinden dijital ürün/hizmet tanıtımları gerçekleştirilmiş olan ASELSAN, HAVELSAN, ASPİLSAN gibi ana yüklenici firmaların da olduğu platformun asıl hayata geçirilme amacı ise ihracatı artırmak... Firmaların ihracat için küresel tedarik zinciri giriş süreçlerine hakim olması ve tasarımdan itibaren atılacak adımları bunlara göre izlemesi gerektiğini söyleyen DAMISE Genel Müdürü ve Kurucu Ortağı Yasemin Ok, "Firmaların dijital ortamda sektörel gelişmelere ve firmalara tek tıkla erişebildiği bir platform oluşturduk. DAMISE; Ekosistem, Akademi, Dijital Vitrin ve Tedarikçi Yönetim Sistemi çözümleriyle faaliyet gösteren yeni nesil dijital bir platformdur" dedi.

NATO "Türk Endüstri Günü" etkinliğinde ürün/hizmet tanıtımları yapan ASELSAN, HAVELSAN, ASPİLSAN gibi ana yüklenici kullanıcıları var

"Platform; savunma havacılık, uzay, denizcilik ve 52 alt sektörde SAHA İstanbul üye firmaları ile ilgili yapılan analizler ve pazar araştırmaları sonucu ortaya çıkan ihtiyaçları karşılamak adına hayata geçirdiğimiz dijital bir platformdur. Ana yükleniciler, kurumsal KOBİ ve ölçekli firmalar, tedarikçi ve tedarikçi olmayı isteyenler, çatı kuruluşlar, hizmet sağlayıcılar ve kamu kuruluşları kullanıcılarımız arasında yer almaktadır" diyen Yasemin Ok, aralarında ASELSAN, HAVELSAN, ASPİLSAN gibi ana yüklenici firmaların da bulunduğunu ancak ana hedeflerinin uluslararası bir platform olması sayesinde global markalar olan Airbus, Boeing gibi firmalara da ulaşmak olduğunu ifade etti.

"SEKTÖRDE KÜRESEL TEDARİK ZİNCİRİ KONUSUNDA BÜYÜK BİR BİLGİ AÇIĞI VARDI"

Sistemi bir örnekle açıklayan Ok, "Örneğin ana yükleniciler, KOBİ ve diğer firmalarla çalışmak istiyor ancak sektörle ilgili çok ciddi sertifikasyon, akreditasyon, uluslararası anlaşmalar ile kritik ve stratejik bilgiler gibi engeller söz konusu... Dolayısıyla sadece ürünü geliştirmek bu sektörde satışı getirmemektedir. Firmaların küresel tedarik zinciri giriş süreçlerini bilmesi ve tasarımdan itibaren bu bilgiler çerçevesinde süreci yönetmesi de beklenmektedir. Ancak sektörde bunların çok bilinmediğini, hatta eksik ya da yanlış bilindiğini ve yönlendirmeye ihtiyaç olduğunu gördük. Özellikle KOBİ'lerimizin çok başarılı teknik kabiliyetleri olmasına rağmen küresel tedarik zincirine giriş süreçleri hakkında doğru bilgiye sahip olmadıklarını fark ettik. Diğer tarafta ana üreticiler de uluslararası sertifikasyon, akreditasyon ve uluslararası anlaşmalar gereği olan küresel tedarik zincirindeki süreçlerde uygun firmalarla çalışmak zorundalar. Bu iki durum başarıyla gerçekleştiği zaman iş satışa dönüşmekte ve ihracat gerçekleşebilmektedir. Biz de gördüğümüz bu ihtiyaçları dijitalde karşılamak adına 2017'de yola çıktık" diye konuştu.

SEKTÖRÜN TÜM İHTİYAÇLARINA TEK TUŞLA ULAŞABİLME İMKANI SUNUYOR

Firmaların dijital ortamda sektörel gelişmelere ve firmalara tek tıkla erişebildiği bir platform olduğunu vurgulayan Ok, "Bu platformda firmalara; ürün ve hizmet sergileyebilme, sektörel arama motoruna ulaşabilme, ulusal ve uluslararası görünürlük sağlayabilme, firma potansiyellerini ortaya koyabilme, sektörde iş birlikleri oluşturabilme, deneyim ve bilgi paylaşabilme, analiz ve detaylı rapor alabilme ve küresel tedarik zincirine dahil olabilme süreçleriyle ilgili konularda hizmet alabilmektedir. DAMISE; Ekosistem, Akademi, Dijital Vitrin ve Tedarikçi Yönetim Sistemi çözümleriyle faaliyet gösteren yeni nesil dijital bir platformdur" dedi.

ANA YÜKLENİCİLER TEDARİKÇİ FİRMA ARAYIŞI İÇİN ÇAĞRIYA ÇIKABİLİYOR

Ok, sözlerini şöyle sürdürdü: "Firmaların ürün ve hizmetleri gerek uluslararası ürün kodlarına göre gerek kabiliyetlerine ya da ürünün teknik özelliklerine göre arayabilecekleri, platform içerisinde kurum hafızası oluşturmak için favorilere ekleyebilecekleri, kendisini favorilere ekleyenleri görebilecekleri ve platform üzerinden mesajlaşabilecekleri teknik imkanlar sunmaktayız. Bunlara ek olarak, ürün/hizmetlerini ulusal ve uluslararası pazarda hangi firmaların incelediğini görebilecekleri bir ortam da sunmaktayız. Bunlar ciddi istatistiki veri analizi gerektirmektedir. Diğer taraftan sektörel kuruluşlara nasıl tedarikçi olunabileceğini, yeterli özelliklere sahip olup olmadıklarını değerlendirebilecekleri bir özellik de (Tedarikçi Yönetim Sistemi) bulunmaktadır. Örneğin bir ana yüklenici firma kendine özel bir uyumluluk listesi de sunabilir. KOBİ veya diğer firmalar bu listeden kendi yeterliliklerini kontrol edebilirler. Ana yüklenici bu liste üzerinden çağrıya çıkıp tedarikçi arayışına girebilir. Listedeki kabiliyetleri sağlayan firmalar bunlara başvurabilir veya eksiklikleri olanlar da eksikliklerini gidermek üzere farklı çözümlerimizden (Akademi) faydalanabilmektedir."

"TÜRK ÜRÜN VE HİZMETLERİNİN DÜNYADA BOY GÖSTERMESİNİ HEDEFLİYORUZ"

Temel amaçlarının ihracat olduğunu vurgulayan Ok, sözlerini şöyle noktaladı: "Türk ürünlerinin ve hizmetlerinin küresel pazarda yerini almasını, markalaşarak dünyada boy göstermesini ve küresel tedarik zinciri süreçlerinde yer almasını hedefliyoruz. Dijital Vitrin hizmet modülümüz ise; fiziksel, online veya hibrit etkinliklerin senkron veya asenkron olarak dijitalde yer almasını, firma, ürün veya hizmet lansmanlarının Dijital Vitrin üzerinden tüm dünyada sergilenmesini sağlamaktadır. Özetle savunma havacılık, uzay, denizcilik ve 52 alt sektör için DAMISE; dijital bir pazaryeri, dijital bir arama motoru, dijital bir iletişim alanı ve ihracat süreçlerinin dijital yönetimini sağlayan yeni nesil dijital bir platformdur. Bir yandan da platformumuza yeni nesil teknolojiler dahil etmeye devam etmekteyiz. Örneğin atıl stok, atıl kapasite gibi konular ülkemizde en çok ihtiyaç duyulan alanlar... Bu konuların hızlı ve pratik çözümüne yönelik çalışmalarımız devam etmektedir."

MERCEDES-BENZ TÜRK, DİJİTALLEŞME YOLUNDA SCADA İLE VİTES ARTIRIYOR

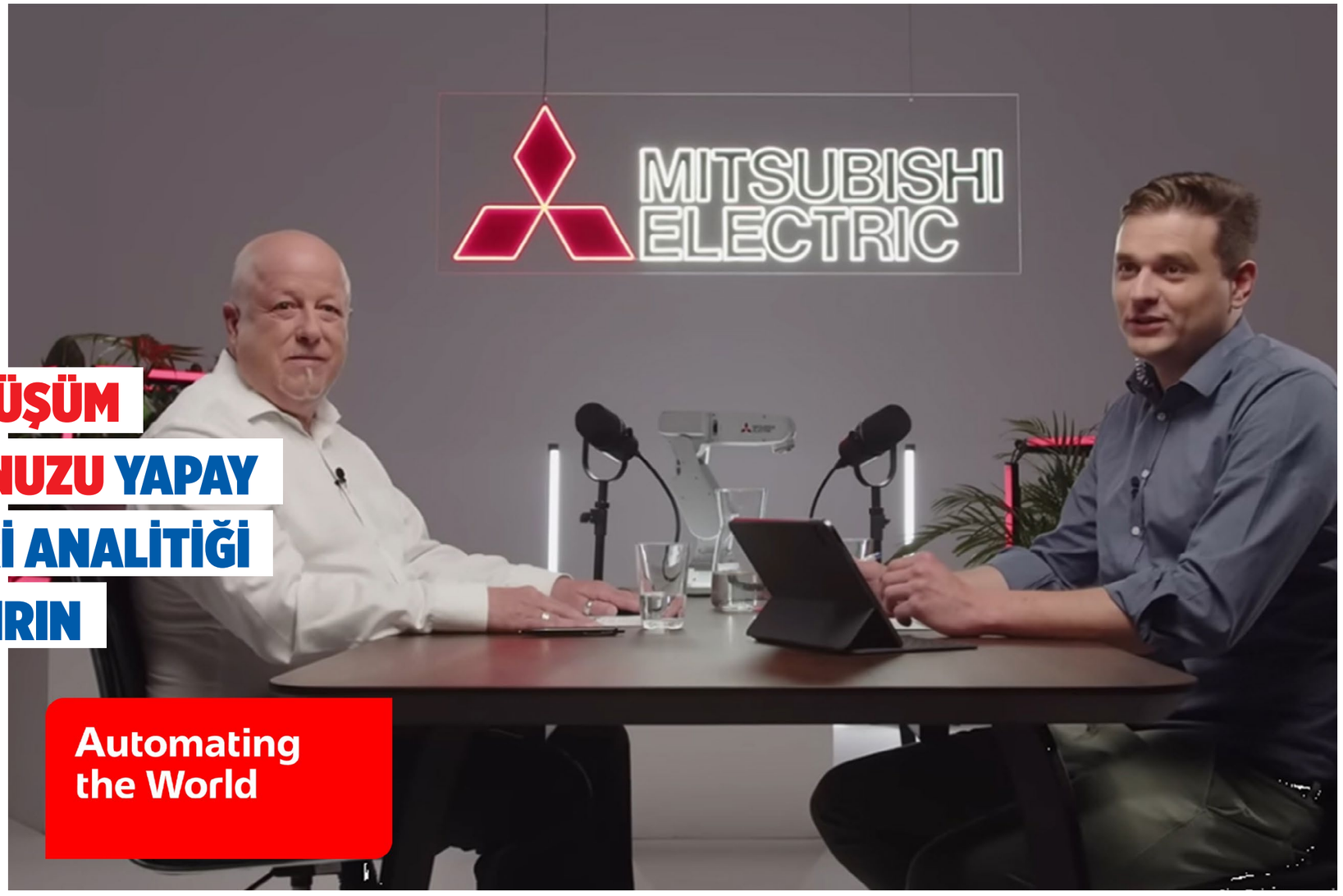
Mercedes-Benz Türk, yenilikçi teknolojileri üretim süreçlerine entegre ederek üretim kalitesini ve verimliliğini artırmaya devam ediyor. Bu kapsamda Mercedes-Benz Türk, Aksaray Kamyon Fabrikası'nda tesis performansını izleyerek süreçleri optimize eden ve hızlı müdahale imkanı sunan SCADA Projesi'ni başlattı. İlk aşamada 15 istasyonda hizmet verecek olan sistem, ilerleyen süreçte 25 istasyona genişleyecek. Ekipmanların bakım faaliyetlerinde verimliliğin artmasını sağlayan SCADA projesi, potansiyel arızaları belirleyerek planlı bakım yapılmasını da mümkün kılacak.

Dijital dönüşüm ve teknolojik inovasyon alanlarında sektörüne öncülük eden Mercedes-Benz Türk, endüstriyel dönüşüm vizyonu çerçevesinde, Aksaray Kamyon Fabrikası'nda SCADA (Supervisory Control and Data Acquisition) Projesi'ni hayata geçirdi.

Tesislerin performansını izleme, süreçleri optimize etme, arıza ve hata durumlarında hızlı müdahale etme gibi önemli yetenekler sağlayan SCADA sistemi, ilk aşamada montaj hattındaki 15 istasyonda hizmet verecek. İlerleyen süreçte ise diğer hollerdeki istasyonların da dahil edilmesiyle, toplam 25 istasyonda hizmet sunacak şekilde genişletilecek. Böylece bütün makineler tek bir platformda toplanacak ve montaj hattındaki makinelerde olası bir sorun yaşadığında, bu durumun hızla tespit edilmesi ve buna uygun bir şekilde müdahale edilmesi sağlanacak. SCADA sistemi, montaj hattındaki makinelerden gelen verileri sürekli olarak izleyerek, herhangi bir arıza veya performans düşüklüğü tespit ettiğinde, bu durumu hızla operatörlere bildirecek ve sorunların hızlıca çözülmesine olanak tanıyacak. Bu sayede üretim sürekliliği ve verimlilik artarken, aksamaların da minimum düzeye indirilmesi sağlanacak.

SCADA sistemi sürekli olarak sensörlerden gelen verileri izleyerek, analiz ettiği için ekipmanların performansı hakkında bilgiler sağlayarak, potansiyel arızaların belirlenmesine de yardımcı olacak. Bu doğrultuda arızaları önceden tahmin etmek ve planlı bakım işlemlerini gerçekleştirmek mümkün olacak. Bu da makinelerin beklenmedik duruşlarını önleyerek üretim sürekliliğine katkı sağlayacak.

www.cadcamcaedunyasi.com.tr



DİJİTAL DÖNÜŞÜM YOLCULUĞUNUZU YAPAY ZEKÂ VE VERİ ANALİTİĞİ İLE HIZLANDIRIN

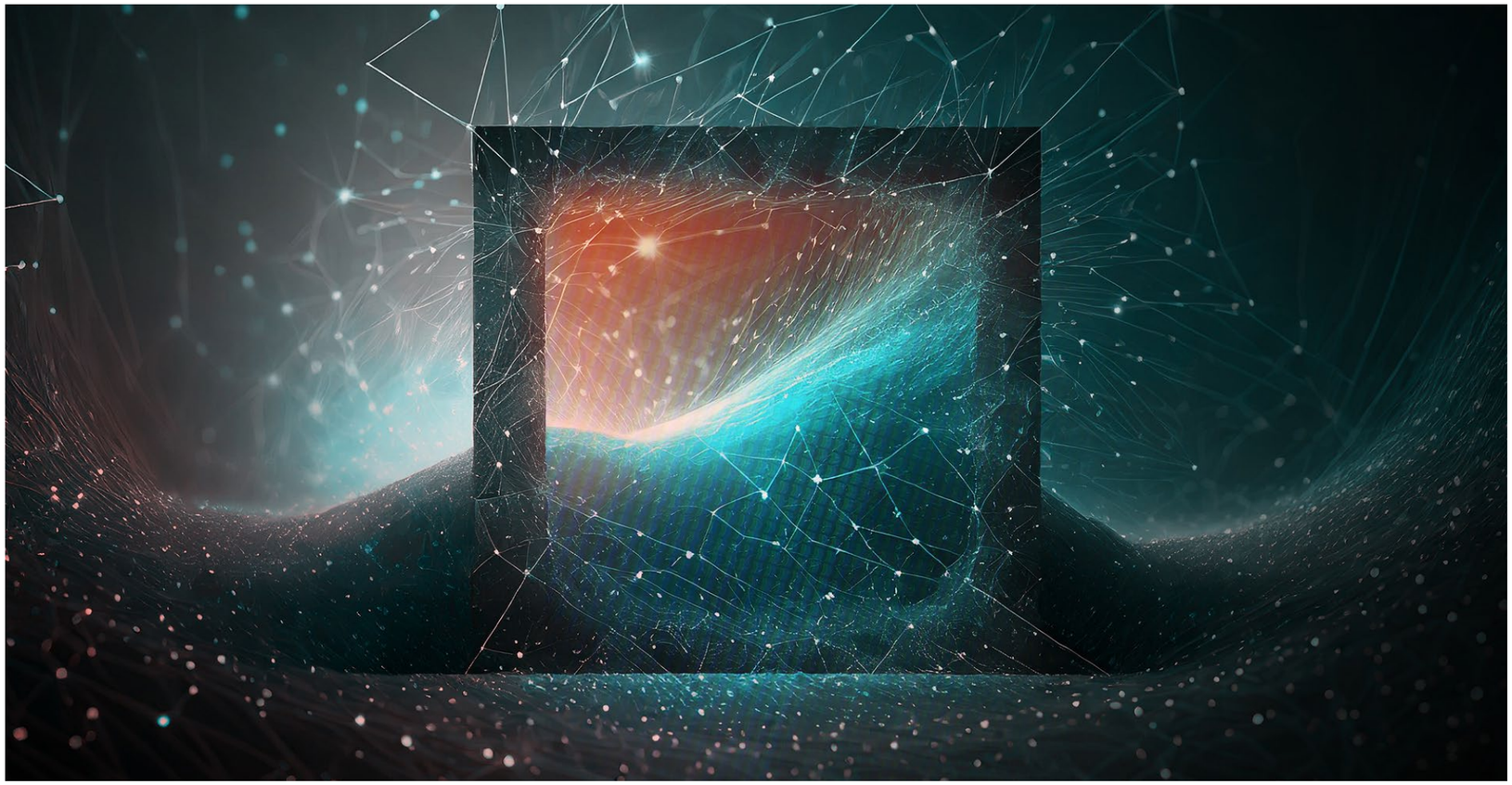
Yapay zekâ ve veri analitiği üretim sektöründe sadece süreçleri iyileştirmekle kalmıyor, kalite sorunlarının temel nedenlerinin belirlenmesinde, şirketlerin verimlilik hedeflerine ulaşmalarında da önemli rol oynuyor. Mitsubishi Electric Fabrika Otomasyon Sistemleri EMEA Başkanı Hartmut Pütz, yeni dijital endüstri ortamında öne çıkabilmek ve pazarın sürekli değişen ihtiyaçlarına hızla uyum sağlayabilmek isteyen üreticilere yapay zekâ ve veri analitiğinden etkin biçimde yararlanmaları önerisinde bulunuyor.

Her alanda hayatımızı dönüştüren yapay zekâ üretim sektörünü de yeniden şekillendiriyor. Karmaşık durumları çözme, karar alma süreçlerini kolaylaştırma ve üretim süreçlerine dair eksiksiz bir genel bakış sunma gücüne sahip yapay zekâ destekli araçlar, hızlı veri artışıyla birlikte her geçen gün daha gerekli hale geliyor. Tahmin yöntemlerini daha güvenilir hale getirerek şirketlerin talepteki hızlı değişimlerle başa çıkmalarına yardımcı olan veri odaklı teknolojiler sayesinde üreticiler verimli, fazla özelleştirilmiş ve kişiselleştirilmiş üretim yapabiliyor. Mitsubishi Electric Fabrika Otomasyon Sistemleri EMEA Başkanı Hartmut Pütz, yapay zekâ ve 'daha akıllı' operasyonların, daha verimli ve uygun maliyetli fabrika operasyonlarına olanak tanıdığını vurguluyor.

Bir fabrikadaki unsurları 'akıllı' hale getirmenin ve darboğaz uygulamalarına odaklanmanın üretkenliği ve verimliliği büyük ölçüde artırabildiğini kaydeden Pütz, yapay zekânın kestirimci bakımdaki önemli rolü ile üreticilerin operasyonel maliyetlerde de önemli tasarruf elde etmelerine yardımcı olduğunu anlatıyor. Örneğin yapay zekâ; maliyetli, beklenmedik ekipman arızalarını ve acil durum kapanmalarını önleyerek fabrikaların karşılaşılabilecekleri olası büyük riskleri bertaraf etmelerine yardımcı oluyor.

Fabrika otomasyonunun verinin gücüyle gelecekte daha da gelişeceğini kaydeden Pütz, dijitalleşen endüstriyel ortamda üreticilerin öne çıkabilmek ve pazarın sürekli değişen ihtiyaçlarına hızla uyum sağlayabilmek için veri kullanımını ve yönetimini optimize etmeleri ve yapay zekâyı benimsemeleri gerektiğini ifade ediyor. Üretim sektörünün geleceğini veriye dayalı operasyonlar şekillendirecek olsa da, çoğu veri hâlâ yeterince etkili bir şekilde kullanılmıyor. Hartmut Pütz, bu sorunu çözmek için de fabrikalara verilerin daha iyi kullanılması gerekliliğine dayanan ve üretimin iyileştirilmesi için Kaizen yöntemi gibi küçük adımları kullanan "Kaizen Düzeyinde Akıllı Üretim" (SMKL) modelini öneriyor.

Mitsubishi Electric Fabrika Otomasyon Sistemleri EMEA Başkanı Hartmut Pütz'ün "Dijital üretimde trendler ve zorluklar", "Robotlarda yapay zekâ, işbirlikçi robotlar ve yazılım tabanlı inovasyon dahil ölçülebilir çözümler", "Basit değişikliklerin uygulanması ve üretim süreçlerinin optimize edilmesi" ve "Üretimdeki kaçınılmaz değişikliklere uyum sağlamak" gibi konularda görüşlerini paylaştığı video röportajını https://www.youtube.com/watch?v=UcGwFmAPJrY linkinden izleyebilirsiniz.



FOTOĞRAFLARA SAKLANAN ZARARLI YAZILIMLAR

Bazı fotoğraflarda göründüğünden fazlası vardır; ilk bakışta masum olan görseller, içinde zararlı yazılımlar barındırabilirler. Dijital güvenlik şirketi ESET güncelleme ve yamaların her zaman yapılması gerektiğine vurgu yaptı.

Bir siber güvenlik yazılımı çoğu kötü amaçlı dosyayı tespit edebilir. Bu nedenle, tehdit aktörleri tespit edilmemek için sürekli olarak farklı yollar ararlar. Bu teknikler arasında görüntülere veya fotoğraflara gizlenmiş kötü amaçlı yazılımlar kullanmak da vardır. Zararlı yazılımlar, tespit edilmekten kaçınmak için bir dosya içinde veri gizleme tekniği olan steganografi sayesinde çeşitli formatlardaki görüntülerin içine yerleştirilebilirler. ESET Research, bu tekniğin Worok siber casusluk grubu tarafından kullanıldığını tespit etti. Bu grup, görüntü dosyalarına kötü amaçlı kod gizliyor ve çalıştırmak üzere bir yük çıkarmak için yalnızca belirli piksel bilgilerini alıyordu.

Çoğu zaman, kötü amaçlı görüntüler web sitelerinde kullanıma sunulur veya belgelerin içine yerleştirilir. Görüntüdeki kod tek başına çalıştırılamaz, yürütülemez veya gömülü haldeyken kendi kendine çıkarılamaz. Kötü amaçlı kodun çıkarılması ve çalıştırılmasıyla ilgilenen başka bir kötü amaçlı yazılım parçasının teslim edilmesi gerekir. Burada gereken kullanıcı etkileşimi düzeyi farklıdır ve bir kişinin kötü niyetli faaliyeti fark etme olasılığı, görüntünün kendisinden ziyade ayıklama işlemine dahil olan koda bağlı görünmektedir.

SOSYAL MEDYADAKİ FOTOĞRAFLAR TEHLİKELİ KOD BARINDIRIR MI?

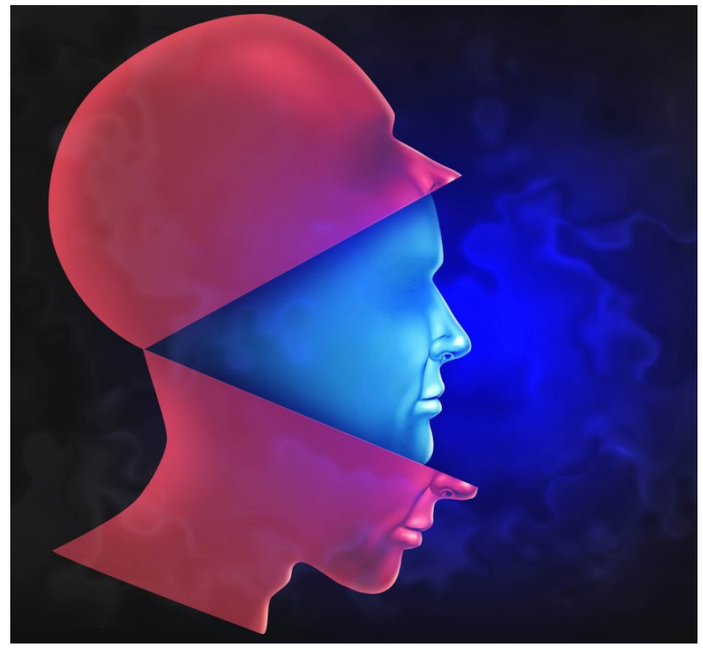
Sosyal medya web sitelerine yüklenen görsellerin genellikle yoğun bir şekilde sıkıştırıldığını ve değiştirildiğini göz önünde bulundurun, bu nedenle saldırganın çalışan zararlı kodu içlerinde gizlemesi çok zor olacaktır. Bu durum, bir fotoğrafın Instagram'a yüklenmeden önce ve yüklendikten sonra nasıl göründüğünü karşılaştırdığınızda açıkça görülebilir. Genellikle belirgin kalite farklılıkları vardır. RGB piksel gizleme ve diğer steganografik yöntemler yalnızca gizli veriler kötü amaçlı kodu çıkarabilecek ve sistemde çalıştırabilecek bir program tarafından okunduğunda tehlike oluşturabilir. Görüntüler genellikle komuta ve kontrol (C&C) sunucularından indirilen kötü amaçlı yazılımları gizlemek ve siber güvenlik yazılımları tarafından tespit edilmelerini önlemek için kullanılır.

SİSTEMLERİNİZİ HER ZAMAN GÜNCEL TUTUN

Görüntülerden çıkarılan herhangi bir istismar kodu, başarılı bir istismar için güvenlik açıklarının mevcut olmasına bağlıdır. Sistemleriniz zaten yamalıysa, istismarın çalışma şansı yoktur; bu nedenle, dijital güvenlik yazılımınızı, uygulamalarınızı ve işletim sistemlerinizi her zaman güncel tutmanız iyi bir fikirdir. Yazılımlarınızın tüm yamalarını uygulayarak ve güvenilir, güncellenmiş bir güvenlik çözümü kullanarak istismar kitleri tarafından zarar görmekten kaçınılabilirsiniz.

Detaylı bilgi;

https://antivirus.com.tr/zararli-yazilimlar-fotograflarda-mi-sakla-niyor-hem-de-dusundugunuz-den-daha-fazla/



DASSAULT SYSTÈMES FIRST® ROBOTİCS COMPETİTİON'I DESTEKLEYEREK TÜRKİYE'DE STEM EĞİTİMİNİ TEŞVİK EDİYOR

Sürdürülebilir inovasyon için sanal ikiz deneyimlerini çok sayıda sektörle buluşturan teknoloji firması Dassault Systèmes, Türkiye'deki FIRST Robotics Competition'a sponsor olduğunu duyurdu. Fikret Yüksel Vakfı tarafından düzenlenen yarışma, 22-24 Mart 2024 tarihleri arasında Volkswagen Arena'da gerçekleştirilecek.

Marmara Bölge Turu'nun "Teknoloji Lideri" sponsoru olarak Dassault Systèmes, bilim, teknoloji, mühendislik ve matematik (STEM) alanlarında eğitimi teşvik etme taahhüdünün altını çiziyor. Bu yıl CRESCENDO temasına odaklanan yarışma, sanatın (A) geleneksel STEM çerçevesine entegrasyonunu vurguluyor. Öğrencileri problem çözme ve inovasyona yönelik disiplinler arası yaklaşımları keşfetmeye teşvik ediyor. Bu kapsamda, öğrenciler projeleri için Dassault Systèmes'in 3DEXPERIENCE platformunu ve SOLIDWORKS uygulamalarını kullanabilecekler.

Dassault Systèmes Türkiye Ülke Müdürü Hakan Kul, etkinlik kapsamında 23 Mart Cumartesi günü bir açılış konuşması yapacak. Hakan Kul, geleceğin iş gücünü şekillendirmede iş birliği, kapsayıcılık ve yaratıcılığın önemini, Dassault Systèmes'in eğitimde eşitlik, çeşitlilik ve kapsayıcılık girişimlerini destekleme taahhüdünü ve teknoloji ile inovasyonun dönüştürücü gücüne olan inancını vurgulayacak.

FIRST® Robotics Competition, Türkiye genelinde 18 şehirden 130'dan fazla yerel takımı ve 25 uluslararası takımı bir araya getiriyor. Bu sponsorluk aracılığıyla Dassault Systèmes, eğitimin önemini ve yarının iş gücü için gerekli becerilerin geliştirilmesini vurgulayarak yeni nesil inovatörlere ilham vermeyi ve onları güçlendirmeyi amaçlıyor.

GELECEĞİN MÜHENDİSLERİNE YATIRIM:

MİKROİŞLEMCİLER VE IoT LABORATUVARI

Özdisan Elektronik, sanayi- üniversite iş birlikleri doğrultusunda Doğuş Üniversitesi ile yeni bir çalışmaya imza attı. Elektronik sektöründeki tecrübelerini eğitim alanına taşıyan şirket, özellikle mikroişlemciler ve IoT alanlarındaki uzmanlığını son teknoloji ekipmanlarla donatılmış "Geleceğe Yolculuk - Özdisan & DOÜ Maker Laboratuvarı" aracılığıyla öğrencilere aktaracak.

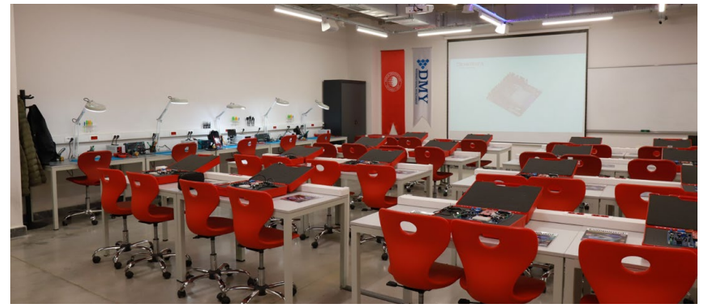
Özdisan Elektronik Genel Müdürü Mustafa Yurttaş: "Kurduğumuz bu modern laboratuvar ile Özdisan Elektronik, geleceğin mühendislerinin yetişmesinde önemli bir rol alıyor. Eğitim kurumuyla Türkiye genelindeki iş birliklerimizi artırarak bu programları genişleteceğiz" dedi.

Türkiye'nin önde gelen elektronik komponent distribütörü Özdisan Elektronik, sanayi- üniversite iş birlikleri doğrultusunda Doğuş Üniversitesi ile yeni bir çalışmaya imza attı. Özdisan Elektronik, mikroişlemciler ve IoT alanlarında uzmanlığını paylaşmak için son teknoloji ekipmanların bulunduğu "Geleceğe Yolculuk - Özdisan & DOÜ Maker Laboratuvarı" ile öğrencilere bilgi ve pratik uygulama fırsatları sunuyor.

Özdisan Elektronik tarafından sağlanan bu modern laboratuvar ortamında öğrenciler, mikroişlemci ve çevrebilimleri konularında öğrendikleri bilgileri uygulamalı bir şekilde geliştirebilecek. Laboratuvar, öğrencilere mikroişlemci ve IoT alanlarında derinlemesine eğitimler sunacak şekilde tasarlanmış olup, bir elektronik mühendisinin ihtiyaç duyabileceği her türlü modern ekipmanla donatıldı. Öğrenciler, Özdisan Elektronik tarafından alanında uzman kişilerden elektroniğin temel prensiplerini, elektronik baskı devre tasarımını, mikroişlemci programlama ve IoT üzerine öğrenme ve pratik deneyim kazanma fırsatına sahip olacak.

Özdisan Elektronik'in bu girişimi, meslek liseleri ve diğer üniversitelerle iş birliklerini de içerecek şekilde genişleyecek. Şirket, önümüzdeki yıllarda Türkiye genelinde daha fazla eğitim kurumuyla ortaklık kurmayı ve eğitim programlarını daha geniş bir öğrenci kitlesine ulaştırmayı planlıyor. Bu iş birliği sayesinde öğrenciler, sadece akademik başarılarını artırmakla kalmayacak, aynı zamanda staj ve iş olanakları konusunda da kendilerini geliştirerek teknoloji sektörüne hazırlanacaklar.

Özdisan Elektronik Genel Müdürü Mustafa Yurttaş, eğitimin teknoloji sektöründeki önemine değinerek şunları söyledi: "Teknolojinin hızla geliştiği bu dönemde, gençleri erken yaşta bu alana yönlendirerek onların gelecekte sektör liderleri olmalarını sağlamak amacıyla bu programı hayata geçirdik. Doğuş Üniversitesi'nde kurduğumuz "Geleceğe Yolculuk - Özdisan & DOÜ Maker Laboratuvarı" ile sadece eğitimi desteklemekle kalmayıp, aynı zamanda teknoloji sektörüne nitelikli mühendisler kazandırmayı da hedefliyoruz. Özdisan Elektronik olarak, elektronik sektöründeki bilgi ve tecrübelerimizi elimizden geldiği kadarıyla eğitim alanına taşımaya özen gösteriyoruz. Bu iş birliği sayesinde, öğrenciler mikroişlemciler ve IoT alanlarında uzmanlığımızdan faydalanarak, son teknoloji ekipmanlarla donatılmış bir laboratuvarda teorik bilgilerini pratikle pekiştirme fırsatı bulacaklar. Bu tür laboratuvarların sayısını da Türkiye genelindeki meslek liselerinde ve üniversitelerde artırmayı amaçlıyoruz."



DELL TECHNOLOGİES'DEN YAPAY ZEKÂ ARAŞTIRMASI

Dell Technologies Araştırması: Yüksek büyüme gösteren şirketler yapay zekâ ve üreten yapay zekânın sektörleri dönüştürmesini bekliyor. Dell Technologies, aralarında Türkiye'nin de olduğu 40 ülkeden 6.600 kişiyle yaptığı araştırmanın sonuçlarını açıkladı. 'Innovation Catalyst' başlıklı araştırmaya göre katılımcıların yüzde 58'i üretken yapay zekâyı uygulamaya başladıklarını belirtiyor.

Dell Technologies; Kuzey Amerika, Latin Amerika, EMEA (Avrupa, Ortadoğu, Afrika), APJ (Asya Pasific ve Japonya) ve Çin'de 100'den fazla çalışanı olan kuruluşlardan 6.600 katılımcının yer aldığı 'Innovation Catalyst' adlı araştırmanın sonuçlarını açıkladı.

Araştırmaya göre katılımcıların yüzde 81'i üretken yapay zekâ (GenAI) ve yapay zekânın (AI) gelecekte sektörleri önemli ölçüde dönüştüreceğine inanıyor. Bu oran, 2023'te yüksek ciro artışı (+yüzde 25) elde eden kuruluşlar için yüzde 91 olurken, düşük ciro artışı (yüzde1-5), sabit ciro veya ciro düşüşü kaydeden kuruluşlar için yüzde 75'e düşüyor.

Aralarında Türkiye'nin de olduğu 40 ülkeden 6.600 bilgi teknolojileri (BT) öncüleri ve şirket yetkilisinin yanıtlarına dayanan araştırma, AI ve GenAI'ya ilişkin önemli bir iyimserlik ortaya koysa da kuruluşların hızlı değişime hazır bulunuşları önemli ölçüde değişiyor. Katılımcıların yüzde 82'si rekabet açısından iyi konumlandıklarını ve sağlam bir stratejiye sahip olduklarını belirtiyor. Bununla birlikte, neredeyse yarısı (yüzde 48) önümüzdeki üç ila beş yıl içinde sektörlerinin neye benzeyeceğinden emin olmadığını ve neredeyse her on katılımcıdan altısı (yüzde 57) değişime ayak uydurmakta zorlandığını ifade ediyor. Katılımcılar, inovasyonu teşvik etmede karşılaştıkları zorluklar arasında doğru yetenek eksikliği (yüzde 35), veri gizliliği ve siber güvenlikle ilgili endişeler (yüzde 31) ve sınırlı bütçenin (yüzde 29) yer aldığını belirtiyor.

GENAI, UYGULAMAYA HAZIR!

Katılımcılar, GenAI'nin BT güvenlik duruşunu iyileştirme (yüzde 52), üretkenliği artırma (yüzde 52) ve müşteri deneyimini geliştirme (yüzde 51) konularında dönüştürücü veya önemli bir potansiyele sahip olduğunu belirtiyor. Bununla birlikte, üstesinden gelinmesi gereken zorlukların da farkındalar. Örneğin yüzde 68'i GenAI'ın yeni güvenlik ve gizlilik sorunları yaratacağından korkuyor, yüzde 73'ü ise verilerinin ve IP'lerinin üçüncü tarafın erişebileceği bir GenAI aracına yerleştirilemeyecek kadar değerli olduğu konusunda hemfikir.

Genel olarak verilen yanıtlar, kuruluşların fikir aşamasından uygulama aşamasına geçerken GenAI pratikleri üzerinde çalıştıklarını gösteriyor; yüzde 58'i GenAI'yi uygulamaya başladıklarını belirtiyor. Kuruluşlarda kullanım arttıkça, risklerin nerede olduğu ve bunlardan kimin sorumlu olduğunun belirlenmesine odaklanılıyor. Katılımcıların yüzde 77'si, herhangi bir AI arızasından veya istenmeyen davranışlardan makine, kullanıcı veya kamu yerine kuruluşun sorumlu olduğu konusunda hemfikir.

Dell Technologies EMEA Başkanı Adrian McDonald konuyla ilgili yaptığı açıklamada "Birçok kişi GenAI gibi dönüştürücü etkisi olan teknolojilerden faydalanmak için harekete geçiyor; değeri ortaya çıkarmak ve büyümeyi desteklemek için yapay zekâyı verilerine entegre ediyor. Bu fırsatı değerlendirmek, sürdürülebilirlik göz önünde bulundurularak tasarlanmış, inovasyon alanında güvenli ve ölçeklenebilir teknoloji temelleri oluşturmak açısından güvenilir ortaklardan oluşan güçlü bir ekosistem gerektiriyor" ifadelerini kullandı.

KURULUŞLAR, GÜNÜMÜZ TEHDİT ORTAMI ZORLUKLARINA GÖĞÜS GERİYOR

Siber güvenlik, kuruluşlar için önemli bir endişe kaynağı olmaya devam ediyor. Katılımcıların yüzde 83'ü son 12 ay içinde bir güvenlik saldırısına maruz kaldıklarını bildirerek bu endişeleri doğruluyor. Çoğunluk (yüzde 89) 'Sıfır Güven' dağıtım stratejisini benimsiyor, yüzde 78'i ise bir siber saldırı veya veri sızıntısından kurtulmak için bir 'Olay Müdahale Planı'na sahip olduklarını söylüyor.

Belirtilen ilk üç sorun arasında kötü amaçlı yazılım, kimlik avı ve veri ihlalleri yer alıyor. Kimlik avına ilişkin sorunlar, çalışanların tehdit ortamında oynadığı rol olmak üzere raporda vurgulanan daha geniş

bir sorunun altını çiziyor. Örneğin, katılımcıların yüzde 67'si bazı çalışanların verimlilik ve üretkenliği artırmak için BT güvenlik kurallarını ve uygulamalarını atladığına inanıyor, yüzde 65'i ise içeriden gelen tehditlerle ilgili endişelerini dile getiriyor. Bu durum, çalışanlar siber güvenlik tehditlerine karşı ilk savunma hattını temsil ettiğinden eğitime odaklanılması gerektiğine işaret ediyor.

DOĞRU TEKNOLOJİ ALTYAPISI, KURULUŞLARIN BAŞARILI OLMASINA YARDIMCI OLACAK

Araştırma ayrıca, GenAI gibi teknolojiler ivme kazandıkça ve veri hacimleri arttıkça modern veri altyapısının kritik rolünü de ortaya koyuyor. Modern, ölçeklenebilir bir altyapıya yatırım yapmak, işletmelerde inovasyonu hızlandırmak için en önemli iyileştirme alanı olarak gösteriliyor. BT karar vericilerinin çoğu (yüzde 82), GenAI'ın uygulanmasında öngördükleri zorlukların üstesinden gelmek için şirket içi veya hibrit bir modeli tercih ettiklerini söylüyor.

Verilerin işletme genelinde paylaşılabilmesi inovasyon bulmacasının önemli bir parçasıyken, katılımcıların yalnızca üçte biri (yüzde 33), mevcutta inovasyon çalışmalarını desteklemek için verileri gerçek zamanlı içgörülere dönüştürebildiklerini söylüyor. Bununla birlikte verilen yanıtlar, kuruluşların bu zorluk karşısında harekete geçtiğini gösteriyor. Katılımcıların yüzde 82'si, verilerin farklılaştırıcı olduğunu ve GenAI stratejilerinin verilerden yararlanmayı ve verileri korumayı içermesi gerektiğini söylüyor. Ayrıca neredeyse yarısı (yüzde 42), önümüzdeki beş yıl içinde verilerinin büyük bir kısmının uçtan geleceğini tahmin ettiklerini belirtiyor.

DİĞER ARAŞTIRMA BULGULARI ARASINDA ŞUNLAR YER ALIYOR:

Beceriler: Katılımcıların üçte ikisi (yüzde 67) şu anda sektörlerinde inovasyon için gerekli yeteneklerin mevcut olmadığını belirtiyor. Öğrenme çevikliği ve isteği, yapay zekâ akıcılığı, yaratıcılık ve yaratıcı düşünme, önümüzdeki beş yıl için ihtiyaç duyulan en önemli beceri ve yetkinlikler olarak sıralanıyor.

Sürdürebilirlik: Katılımcıların yüzde 42'si 'çevresel açıdan sürdürülebilir inovasyonların teşvik edilmesinin' önemli bir iyileştirme alanı olduğunu düşünüyor. Enerji verimliliği üst sıralarda yer alıyor; yüzde 79'u BT ortamlarını daha verimli yönetmek için hizmet olarak sunulan çözümleri deniyor ve yüzde 73'ü daha enerji verimli hâle gelmek için yapay zekâ çıkarımını aktif olarak uç noktalara taşıyor (örneğin, akıllı binalar).

BT'yi stratejik bir ortak hâline getirmek: Hâlihazırda, şirket karar vericilerinin yüzde 81'i BT karar vericilerini stratejik görüşmelere dâhil etmiyor, ancak her iki taraf da daha güçlü bir ilişkiyi ikinci en önemli iyileştirme alanı olarak sıralıyor.

VERİLERİMİZİ NEDEN KORUMAMIZ GEREKİR?

Ne zaman çevrimiçi olsak, arkamızda bir veri izi bırakıyoruz. Hayatlarımız dijital teknoloji ile giderek daha fazla iç içe geçerken dijital ayak izlerimiz de büyümeye devam ediyor. Sosyal medyada paylaşım yaparken veya çevrimiçi ürün satın alırken oluşturduğumuz bazı veri parçaları, internetin gölgelerinde gizlenen siber suçlular için büyük değer taşıyabilir.

Her birimiz potansiyel olarak finansal dolandırıcılıktan gasp kampanyalarına kadar bir dizi tehditle karşı karşıya olduğumuzdan kişisel bilgilerimizi korumanın önemini kavramış olmamız gerekiyor. Dijital güvenlik şirketi ESET kişisel verilerin öneminin altını çizerek kendimizi korumak için alabileceğimiz önlemleri sıraladı.

DOLANDIRICILAR KİŞİSEL VERİLERİMİZİ NEDEN HEDEF ALIYOR?

1. Finansal dolandırıcılık

Finansal dolandırıcılık dijital çağın en yaygın tehditlerinden biridir. Kişisel veriler finansal varlıklarınıza açılan bir kapı görevi görmektedir ve bu da onları her zaman çok para kazanmayı isteyen siber suçlular için birincil hedef haline getirmektedir. Banka kartı bilgilerini korumak sağduyulu bir davranış olsa da bu dikkati bizi tanımlayan diğer tüm bilgilere de yaymak ve banka hesaplarımıza yetkisiz erişimi önlemek için her türlü kişisel bilgiyi koruma konusunda proaktif olmak da aynı derecede önemlidir.

2. Kimlik hırsızlığı

Kimliğiniz, suçlulara sizin adınız altında dolandırıcılık faaliyetlerinde bulunma olanağı verir; bu da yalnızca mali refahınızı tehlikeye atmakla kalmaz, aynı zamanda itibarınızı, güvenilirliğinizi ve genel refahınızı da zedeler. Çalıntı kimlikleri kullanan siber suçlular, "şüphelenmeyen kurbanlar adına" çok çeşitli dolandırıcılık faaliyetleri gerçekleştirebilir, finansal istikrarlarını ve kişisel bütünlüklerini tehlikeye atabilir.

3. Fidye yazılımları ve gasp

Fidye yazılım tehdidi yıllardır dijital ortamda büyük bir tehdit olarak varlığını sürdürüyor. Özellikle kişisel belgeler, hassas iş verileri ve yeri doldurulamaz anılar söz konusu olduğunda, cihazlarınızın ve verilerinizin aniden kilitlenmesinin psikolojik etkisi çok büyüktür.

4. Karanlık web satışı

Kişisel veriler, hem karanlık web olarak bilinen internetin keyifsiz yeraltı dünyasında hem de Telegram gibi ana akım sosyal medya platformlarının gölgeli girintilerinde kazançlı bir meta haline geldi. Çalınan giriş bilgilerinden, sosyal güvenlik kartı detaylarına ve bebeklerin kişisel verilerine kadar her şey kapanın elinde kalıyor.

5. Hesap hırsızlığı

Hesap hırsızlığı, suçluların sosyal medya siteleri, e-posta hizmetleri ve diğer platformlar da dahil olmak üzere çevrimiçi varlığınızın çeşitli yönlerine sızmaları için doğrudan bir yoldur. İçeri girdikten sonra, dolandırıcılık faaliyetleri gerçekleştirmek, kötü amaçlı yazılım yaymak veya kimliğinizi tehlikeye atmak için bu erişimden yararlanırlar. İster verilerimizi depolayan bir şirket, hesap veya hizmetteki veri ihlali nedeniyle olsun ister çevrimiçi ortamda isteyerek paylaştığımız bilgiler sayesinde olsun, saldırganlar genellikle sadece ad, soyad, doğum tarihi veya elde edilen diğer verilerin kombinasyonlarını kullanarak parolalarımızı kırabilir.

6. Oltalama mesajları

Oltalama, özellikle de spearphishing olarak bilinen hedefli tür, belirli kişi veya kuruluşlara yönelik ikna edici mesajlar oluşturmak için kişisel verilerden yararlanabilir. Siber suçlular hedeflerini titizlikle araştırarak isimleri, iş unvanları, şirket bağlantıları ve hatta kişisel ilgi alanları veya faaliyetleri gibi bilgileri toplayabilir. Saldırganlar ellerindeki bu verilerle, taktiklerini meşru ve ilgili görünecek şekilde uyarlayarak başarı olasılığını artırabilir.

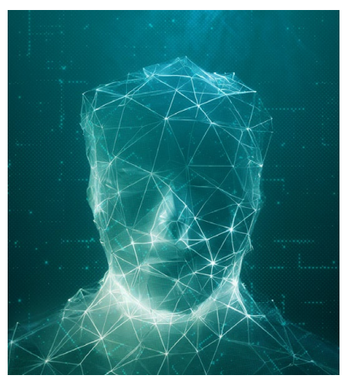
7. Kurumsal casusluk

Kişisel veriler yalnızca "sıradan" siber suçluların ilgisini çekmez; rakip şirketler, hükümetler ve diğer gruplar da bu hassas bilgilerin peşindedir. Kurumsal casusluk alanında, kişisel veriler stratejik avantajlar sağlama ve hedefli saldırıları kolaylaştırma potansiyeli nedeniyle arzulanmaktadır. Çalışanlardan çalınan veriler, sonuçları kişisel gizliliğin çok ötesine geçebilecek hedefli saldırılar için araç haline gelebilir.

KENDİNİZİ KORUMAK İÇİN 7 İPUCU

Verilerinizin siber suçluların hedefine girme riskini büyük ölçüde azaltacak birkaç basit önlem var.

- İstenmeyen e-postalara, mesajlara veya kişisel bilgi taleplerine karşı dikkatli olun ve şüpheli bağlantılara tıklamaktan veya bilmediğiniz kaynaklardan gelen ekleri indirmekten kaçının.
- Çevrimiçi bilgi paylaşımı söz konusu olduğunda ihtiyatlı olun.
- Her bir hesabınız için güçlü ve benzersiz parolalar kullanın.
- İmkan tanıyan her hesapta iki faktörlü kimlik doğrulamayı etkinleştirin.
- Banka hesaplarınızı, kredi raporlarınızı ve diğer finansal hesaplarınızı herhangi bir yetkisiz faaliyete karşı düzenli olarak izleyin. Şüpheli işlemleri veya kimlik hırsızlığı belirtilerini derhal bildirin.
- İhlal edilen parola uyarılarını takip edin ve böyle bir bildirim aldıktan sonra derhal harekete geçin.
- Tüm cihazlarınıza saygın bir güvenlik yazılımı yükleyin.



İTÜ ÇEKİRDEK TECRÜBESİ PARTNER

KULUÇKA AĞI PROJESİ İLE ANADOLU'YA YAYILIYOR

Her yıl 500'den fazla girişimi bir araya getirerek, büyüme yolculuklarını 360 derece destekleyen İTÜ ARI Teknokent'in kuluçka merkezi İTÜ Çekirdek, bir yeniliğe daha imza atarak Anadolu Partner Kuluçka Ağı Projesi'ni hayata geçirdi. Türkiye genelindeki kuluçka merkezleri ve hızlandırma programlarına geçmişte edindiği bilgi, deneyim ve kaynakları sunan İTÜ Çekirdek, bu kapsamda Mayıs ayı içerisinde 14 şehirden 17 kuluçka merkezine kapılarına açarak, katılımcılarla ön kuluçkadan kuluçka sürecine, fon sürecinden pazarlama süreçlerine kadar sahip olduğu bilgeleri paylaştı.

Teknoloji girişimcilerini eğitim, danışmanlık, mentorluk ve geniş bir network ile destekleyerek onların iç ve dış pazardaki başarılarını artırmayı hedefleyen İTÜ ARI Teknokent'in kuluçka merkezi İTÜ Çekirdek, etki alanını daha geniş bir alana yaymak maçıyla Anadolu Partner Kuluçka Ağı Projesi'ni hayata geçirdi. BU sayede Türkiye'nin dört bir yanındaki girişim ekosistemlerini aynı çatı altında buluşturarak sunduğu fırsatlarla Anadolu Kuluçka Merkezleri'ni güçlendirmeyi amaçlayan İTÜ Çekirdek, partner kuluçkalarla birlikte Türkiye ekonomisine katkı sağlamak, teknoloji kümelenmesini güçlendirmek, inovasyonu teşvik etmek ve bilimsel refahı artırmayı hedefliyor. 14 şehirden 17 kuluçka merkezi ile Mayıs ayı içerisinde bir araya gelerek eğitim veren İTÜ Çekirdek yetkilileri, ön kuluçkadan kuluçka sürecine, fon sürecinden pazarlama süreçlerine kadar sahip olduğu know how'ı katılımcılara aktardı.

"İTÜ ARI TEKNOKENT HEP "BİRLİKTE" İLERİYE" DİYOR

Anadolu Partner Kuluçka Ağı'nın İstanbul'dan Türkiye'ye uzanan bir iş birliği programı görevi gördüğünü ifade eden İTÜ ARI Teknokent Genel Müdürü Prof. Dr. Attila Dikbaş, "İTÜ Çekirdek sayesinde bünyemizdeki girişimcilere nasıl ki onları daha ileri taşıyacak imkanlar sunuyorsak programımız sayesinde bunu tüm Türkiye'yi kapsayacak şekilde genişletiyoruz. Birkaç yıl evvel Bilişim Vadisi Fizibilite Raporu'nda sunduğum; Türkiye'deki tüm Teknoparkların ve kuluçka merkezlerinin birbirleriyle entegre olduğu, kontrollü şekilde bölgeler arası giriş-çıkışların yapılabildiği, ortak laboratuvarların kullanabildiği; aslında tüm güçlü kasların birleşerek, daha zayıf veya gelişmekte olan bölgelerin açığını kapattığı 'Anadolu Teknoloji Ağı Projesi'nin ön ayağını İTÜ Çekirdek olarak Anadolu Partner Kuluçka Ağı ile hayata geçiriyoruz. Bu iş birliği kapsamında, İTÜ Çekirdek ve programdaki girişimlerimiz, ülkemizin prestijli girişimcilik etkinliği Big Bang Startup Challenge'da bir araya gelme ve güç birliği oluşturma fırsatını da elde ediyor. Bunun yanında partnerimiz olan kuluçka merkezleriyle fiziksel ve online gerçekleştirilecek olan değerlendirme toplantıları ile soru-cevap günlerinde bir araya gelme, bilgi toplantılarına katılma, sektörel bağlantıların genişletileceği etkinliklere dahil olma imkanını da tanıyoruz. Bu karşılıklı bir ağ; biz bildiklerimizi aktarırken, onlarda da çok şey öğreniyoruz. Herhangi bir sektöre odaklı veya çeşitli sektörlerle iş birliği içerisinde olan, bünyesindeki girişimcilere ve şirketlere destek için belirli ve tanımlı bir süreç sunup bu süreç hakkında bilgi verecek bir web sitesi bulunduran, partnerlik sürecinde başarılı girişimcilerinin, yatırımcılarla tanışma ve inovatif etkinlikleri takip etme amacıyla zaman zaman İstanbul'a seyahat edebilmesine olanak sağlayacak kaynakları sağlamayı hedefleyen tüm kuluçka merkezleri programımıza dahil olabiliyor." dedi.

İTÜ Çekirdek'in kurduğu Anadolu Partner Kuluçka Ağı'na başvurular cekirdek@ariteknokent.com.tr mail adresinden yapılabilir.

KÖTÜ AMAÇLI MOBİL BANKACILIK YAZILIMLARI 2023'TE KÜRESEL ÇAPTA %32 BÜYÜDÜ

Kaspersky, gelişen finansal siber tehdit ortamının ayrıntılı analizini sunan yıllık Finansal Tehditler Raporu'nun 2023 sürümünü yayınladı. Rapor, mobil bankacılığa dair kötü amaçlı yazılımlarda ve kripto para ile ilgili kimlik avında önemli artışlar olduğunu ortaya koyarak, dijital finansal varlıklara yönelik artan tehdidi işaret ediyor.

Geçtiğimiz 12 ay boyunca mobil bankacılık Truva atlarıyla karşılaşan kullanıcı sayısında önemli artış yaşandı ve Android kullanıcılarına yönelik saldırılar 2022'ye kıyasla %32 oranında arttı. En yaygın bankacılık Truva atı, tüm Android saldırılarının %22'sini oluşturan Bian.h oldu. Coğrafi olarak, Afganistan, Türkmenistan ve Tacikistan, bankacılık Truva atlarıyla karşılaşan kullanıcıların en yoğun olduğu yerler olarak kayda geçerken, Türkiye'de bu gibi yazılımlardan etkilenen kullanıcıların neredeyse %3'ü (%2,98) mobil bankacılık kötü amaçlı yazılım saldırılarıyla karşı karşıya geldi.

PC odaklı finansal kötü amaçlı yazılımlarından etkilenen kullanıcı sayısı 2023'te %11 azalırken, Ramnit ve Zbot, etkilenen kullanıcıların %50'sinden fazlasını hedef alan baskın kötü amaçlı yazılım aileleri olarak öne çıktı. Tüketiciler, tüm saldırıların %61,2'sini üzerine çekerek birincil hedef olmaya devam etti.

2023 yılında finansal kimlik avı, kurumsal kullanıcılara yönelik tüm kimlik avı saldırılarının %27,32'sini ve ev kullanıcılarına yönelik saldırıların %30,68'ini oluşturarak önemli bir tehdit olmaya devam etti. E-mağaza markaları, finansal kimlik avı girişimlerinin %41,65'i ile en büyük cazibe merkezi olarak belirlendi. PayPal kimlik avı, elektronik ödeme sistemi kullanıcılarını hedef alan kimlik avı sayfalarının %54,78'ini temsil etti. Raporda ayrıca 2022'deki 5,04 milyon tespit sayısına kıyasla 2023'te 5,84 milyon tespit sayısıyla kripto para kimlik avında bir önceki yıla göre %16'lık artış olduğu vurgulandı.

E- MAĞAZALARA YÖNELİK KİMLİK AVI SALDIRILARI EN YAYGIN ÖRNEK

E-mağazalara yönelik kimlik avı saldırıları, tüm finansal kimlik avı sayfalarının %41,65'ini oluşturarak en yaygın örnek olarak öne çıktı. Amazon kimlik avı girişimlerinin %34'üyle en çok taklit edilen çevrimiçi mağaza olurken, onu %18,66 ile Apple ve %14,71 ile Netflix takip etti. PayPal, saldırıların %54,73'ü ile en çok hedef alınan ödeme sistemi oldu.

Kaspersky'nin kripto para temalı kimlik avı bağlantılarını takip etmeye yönelik 5 milyon 838 bin 499 girişimi engellemesiyle, kripto paraya dair kimlik avı ve dolandırıcılıklar artmaya devam etti. Bu, 2022'ye göre %16'lık artışa karşılık geliyor. Dolandırıcılar ayrıca kripto para borsalarını taklit etti ve Apple gibi büyük şirketler adına coin teklif etti. Kaspersky Güvenlik Uzmanı Igor Golovin, şunları söyledi: "Para her zaman siber suçlular için bir çekim noktası oldu. Kötü amaçlı yazılım saldırılarının önemli bir kısmı finansal olarak motive ediliyor. Geçen yıl mobil kötü amaçlı yazılımlarda görülen artış, siber suçlarda endişe verici bir eğilimin altını çiziyor. Yeni ve agresif kötü amaçlı yazılım türlerinin ortaya çıkmasıyla birlikte saldırganlar taktiklerini mobil cihazları daha agresif bir şekilde hedef alacak şekilde geliştiriyor. Bu durum, bireylerin ve işletmelerin daha dikkatli olmaları, koruyucu önlemleri güncellemeleri ve cihaz güvenliğini uygun şekilde güçlendirmeleri gerektiğinin altını çiziyor."

2023'te finansal tehditlerin durumu hakkında daha fazla bilgi edinmek için Securelist.com adresini ziyaret edebilirsiniz.

Kaspersky, mobil zararlı yazılımlara karşı güvende kalmak için şunları öneriyor:

- Uygulamalarınızı yalnızca Google Play veya Amazon Appstore gibi resmi mağazalardan indirmeyi tercih edin. Bu mağazalardaki uygulamalar %100 güvenli değildir, ancak mağaza temsilcileri tarafından kontrol edilirler ve bazı filtreleme sistemleri vardır. Her uygulama bu mağazalara giremez.
- Kullandığınız uygulamaların izinlerini kontrol edin. Özellikle Erişilebilirlik Hizmetlerini kullanma izni gibi yüksek riskli izinler söz konusu olduğunda bir uygulamaya izin vermeden önce iyi düşünün.
- Güvenilir bir güvenlik çözümü, gizleme tekniklerinden bağımsız olarak kötü amaçlı uygulamaları ve reklam yazılımlarını cihazınızda kötü davranışlar sergilemeye başlamadan önce tespit etmenize yardımcı olabilir.
- İşletim sisteminizi ve önemli uygulamaları güncellemeler mevcut oldukça güncelleyin. Birçok güvenlik sorunu, yazılımların güncellenmiş sürümleri yüklenerek çözülebilir.

SİEMENS VE NVIDIA ENDÜSTRİYEL METAVERSE ALANINDAKİ İŞ BİRLİĞİNİN KAPSAMINI GENİŞLETİYOR

Siemens, endüstriyel metaverse çalışmalarını geliştirmek amacıyla NVIDIA ile sürdürdüğü iş birliğinin kapsamını genişletme kararı aldı. Geliştirilecek yeni ürün, Siemens Xcelerator ile NVIDIA Omniverse Cloud API'larını (uygulama programlama arayüzü) birbirine bağlayarak iş birliğine dayalı, gerçek zamanlı, fiziksel tabana dayanan yapay zeka destekli görselleştirme sunacak. Siemens ve NVIDIA, NVIDIA GTC'de HD Hyundai ile bir araya gelerek entegre görselleştirmenin daha fazla bilgi ve içgörü sağlamaya nasıl yardımcı olduğunu vurguladı.

Siemens, endüstriyel metaverse çalışmalarını geliştirmek amacıyla NVIDIA ile sürdürdüğü iş birliğinin kapsamını genişletme kararı aldı. Siemens ve NVIDIA, NVIDIA GTC Konferansı'nda üreten yapay zekanın karmaşık verilerin görselleştirilmesinde devrim yaratarak fotogerçekçiliği mümkün kılabileceğini gösterdi ve sürdürülebilir gemi üreticisi HD Hyundai'nin yeni ürünler geliştirmek için bu teknolojiyi nasıl kullanabileceğini gösterdi. Siemens, yeni NVIDIA Omniverse Cloud API'larıyla desteklenen etkileşimli görselleştirmeleri Siemens Xcelerator platformuna entegre ederek yapay zeka odaklı dijital ikiz teknolojisinin daha etkin şekilde kullanılmasını sağlayacak.

SİEMENS AG BAŞKANI VE CEO'SU ROLAND BUSCH: "ÜRÜNLERİN VE DENEYİMLERİN TASARLANMA, ÜRETİLME VE SUNULMA ŞEKİLLERİNDE DEVRİM YARATACAĞIZ."

İş birliğine yönelik görüşlerini paylaşan Siemens AG Başkanı ve CEO'su Roland Busch, "Ürünlerin ve deneyimlerin tasarlanma, üretilme ve sunulma şekillerinde devrim yaratacağız. Bu yeni nesil endüstriyel yazılım, endüstriyel metaverse'e giden yolda müşterilerin ürünleri gerçek dünyada olduğu gibi, yani bir bağlam içinde ve çarpıcı bir gerçekçilik seviyesiyle deneyimlemelerini mümkün kılıyor. Gelecekte müşterilerin bu ürünlerle doğal dil girdileri sayesinde etkileşime girmeleri de mümkün olacak. NVIDIA iş birliğimiz sayesinde Siemens Xcelerator portföyüne hızlandırılmış bilgi-işlem, üretken yapay zeka ve Omniverse entegrasyonu kabiliyetleri ekleyeceğiz" ifadelerini kullandı.

NVIDIA CEO'SU JENSEN HUANG: "OMNİVERSE VE ÜRETKEN YAPAY ZEKA, ENDÜSTRİYEL İŞLETMELER İÇİN BÜYÜK BİR DÖNÜŞÜMÜ BERABERİNDE GETİRİYOR."

NVIDIA CEO'su Jensen Huang ise "Omniverse ve üretken yapay zeka, endüstriyel işletmeler için büyük bir dönüşümü beraberinde getiriyor. Siemens, NVIDIA platformlarını müşterileriyle buluşturarak sektör liderlerine her ölçekte yapay zeka destekli dijital ikizlerin yeni neslini oluşturmalarına yönelik fırsatlar sunuyor" dedi.

İki şirket arasındaki iş birliğinin sıradaki aşamasında Siemens, Siemens Xcelerator platformunun bir parçası olan, şirketin sektör lideri bulut tabanlı Ürün Yaşam Döngüsü Yönetimi (PLM) yazılımı Teamcenter® X için bu yılın sonuna doğru yeni bir ürün çıkarmayı planlıyor. NVIDIA Omniverse teknolojileri tarafından desteklenecek sistem, mühendislik ekiplerine iş akışındaki israf ve hataları ortadan kaldıracak yüksek seviyede sezgisel, fotogerçekçi, gerçek zamanlı ve fiziksel tabanlı dijital ikiz oluşturma olanağı sağlayacak.

Üretken yapay zeka kullanımı sayesinde malzeme tanımları ve aydınlatma ortamları gibi ayrıntıların yanı sıra diğer destekleyici ortam unsurlarının fotogerçekçi görsellerle kurulması ve ayarlanması süreci kayda değer oranda hızlandıracak. Mühendislik verilerinin gerçek dünyada görünecekleri şekilde bağlama oturtulması sayesinde daha önce günler süren işler, saatler içinde tamamlanabilecek. Mühendislik ekiplerinin yanı sıra satış ve pazarlama ekiplerinden karar vericilere ve müşterilere kadar diğer paydaşlar da gerçek dünyadaki ürün görünümüne ilişkin daha derinlemesine içgörü ve kavrayış elde ederek daha bilgiye dayalı ve hızlı karar alabilecek.

HD HYUNDAİ BİLGİ İŞLEM MÜDÜRÜ VE DİJİTAL SÜREÇLER BAŞ SORUMLUSU TAEJİN LEE: "BU SÜREÇ HATALARI AZALTACAK, MÜŞTERİ DENEYİMİNİ İYİLEŞTİRECEK, ZAMAN VE MALİYET TASARRUFU SAĞLAYACAK"

Siemens, NVIDIA iş birliğiyle sürdürülebilir gemi üretiminde pazar lideri HD Hyundai'ye gerçek zamanlı ve fotogerçekçi görselleştirmenin oluşturulması sürecini gösterdi. HD Hyundai, yedi milyondan fazla ayrı parça içerebilen oldukça karmaşık sürece sahip amonyak ve hidrojenle çalışan gemiler geliştiriyor. HD Hyundai, Siemens ve NVIDIA'nın yeni ürününü kullanarak devasa büyüklükte mühendislik verisi kümelerini etkileşimli olarak birleştirebilecek ve görselleştirebilecek.

HD Hyundai Bilgi İşlem Müdürü ve Dijital Süreçler Baş Sorumlusu Taejin Lee, "Uzun zamandır ürün yaşam döngüsü yönetimi için güvendiğimiz Siemens Teamcenter'la çalışıyoruz. Bu güven temelinde ve bu yeni iş birliği sayesinde projelerin daha anlaşılır hale gelmesi için yeni nesnelerin ve HDR arka planlarının oluşturulmasında üretken yapay zekayı kullanarak, gemilerin dijital ikizlerini görselleştirebilecek ve bu dijital ikizlerle etkileşimde bulunabileceğiz. Bu süreç hataları azaltacağı, müşteri deneyimini iyileştireceği ve ayrıca zaman ve maliyet tasarrufu sağlayacağı için birçok yönden faydalı olacaktır" dedi.

YAPAY ZEKA İLE PAYLAŞMAMANIZ GEREKEN 7 BİLGİ

Sohbet tabanlı yapay zeka programları, çeşitli konularda yardım almak için son derece popüler ve kullanışlı araçlar haline geldi. Bu programlar, kod yazmaktan sanat eseri oluşturmaya kadar hayal edilebilecek her şeyi oluşturmak için kullanılabiliyor. Ancak her ne kadar gelişmiş olursa olsun, hassas veriler konusunda yapay zeka programlarına güvenilmemesi gerektiğini belirten Bitdefender Antivirüs Türkiye distribütörü Laykon Bilişim'in Operasyon Direktörü Alev Akkoyunlu, sohbet tabanlı yapay zeka programlarıyla paylaşılmaması gereken 7 bilgiyi açıklıyor.

Günlük hayattaki dijital yardımcılar haline gelen sohbet tabanlı yapay zeka programları, yöneltilen soru ve talepleri internetin bilgi havuzunda tarayarak, kullanıcılar için anlamlı dizilimler haline getiriyor. Ancak bu dost canlısı görünen programlar, kullanıcıların kişisel verilerini istismar edebilecek bir prosedürle birlikte çalışıyor. Gerçekleşen konuşmaların tam dökümleri, üretici şirket tarafından toplanıyor ve depolanıyor. Buna tüm sorular, yönlendirmeler, gönderilen mesajlar ve yanıtlar da dahil. Bu sayede şirketler, büyük dil modellerini eğitmek ve programın öğrenmesine yardımcı olmak için bu konuşma verilerini analiz ediyor. Amaç, her ne kadar yapay zekanın dil anlayışını ve diyalog yetenekleri geliştirmek olsa da bu durumun, kullanıcıların kişisel bilgilerini, görüşlerini ve hassas konuşma verilerini tehdit ettiğini belirten Bitdefender Antivirüs Türkiye distribütörü Laykon Bilişim'in Operasyon Direktörü Alev Akkoyunlu, sohbet tabanlı yapay zeka programlarıyla paylaşılmaması gereken 7 bilgiyi açıklıyor.

1. Kişisel tanımlayıcı bilgiler: Tam adınız, ev adresiniz, telefon numaranız, doğum tarihiniz, sosyal güvenlik numaranız veya diğer resmi kimlik numaralarınız gibi önemli kişisel tanımlayıcı bilgileri paylaşmaktan kaçının. Bunlardan herhangi biri sizi taklit etmek için kullanılabilir ve kimlik hırsızlığına, mali dolandırıcılığa veya kişisel bilgilerinizin diğer suç amaçlı kötüye kullanımına yol açabilir.

2. Kullanıcı adları ve şifreler: Parolaları, PIN'leri, kimlik doğrulama kodlarını veya diğer oturum açma kimlik bilgilerini asla yapay zeka sohbet robotlarıyla paylaşmayın. Kimlik bilgileriniz hakkında ipucu vermek bile bilgisayar korsanlarının hesaplarınıza erişmesine yardımcı olabilir.

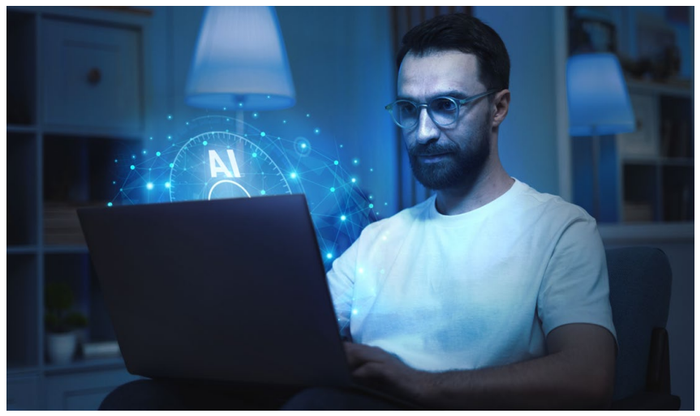
3. Finansal bilgiler: Yapay zeka sohbet robotlarıyla asla finansal hesap bilgilerinizi, kredi kartı numaralarınızı veya gelir detayları paylaşmamalı. Onlardan, genel finans ipuçları ve tavsiyeleri, bütçenize yardımcı olacak genel sorular ve hatta vergi rehberliği isteyebilirsiniz ancak finansal hesaplarınızın ve varlıklarınızın kolayca ele geçirilmesine neden olabileceğinden hassas finansal bilgilerinizi gizli tutun.

4. Özel ve mahrem düşünceler: Yapay zeka sohbet robotları her ne kadar sempatik görünse de herkese açık olarak paylaşmaktan çekineceğiniz derin kişisel düşüncelerinizi, deneyimlerinizi veya fikirlerinizi açıklamaktan kaçınmalısınız. Siyasi veya dini görüşlerden, ilişki sorunlarına veya duygusal mücadelelere kadar her şey, konuşma kayıtlarının ele geçirilmesi veya yanlış kullanılması durumunda açığa çıkabilir.

5. İşle ilgili gizli bilgiler: Özel bilgiler, ticari sırlar, içeriden öğrenilen bilgiler veya herhangi bir türden gizli işyeri verileriyle çalışıyorsanız, bunları herkese açık sohbet programlarıyla tartışmayın. Toplantı tutanaklarını özetlemek veya tekrar eden görevleri otomatikleştirmek için sohbet programlarını kullanmaktan kaçının. Çünkü bu, hassas verileri istemeden ifşa etme veya işvereninizin gizlilik anlaşmalarını ve fikri mülkiyet korumalarını ihlal etme riski taşır.

6. Orijinal yaratıcı çalışmalarınız: Orijinal fikirlerinizi, diğer tüm kullanıcılarla potansiyel olarak paylaşılmasından memnun değilseniz asla sohbet robotlarıyla paylaşmayın.

7. Sağlıkla ilgili bilgiler: Sağlık verilerinizi korumak, potansiyel gizlilik ihlallerine veya hassas tıbbi bilgilerin kötüye kullanılmasına karşı koruma sağlamak anlamına gelir. Bu nedenle, tıbbi durumlarınızı, teşhislerinizi, tedavi ayrıntılarınızı veya ilaç rejimlerinizi asla yapay zeka sohbet programlarına ifşa etmeyin. Bunun yerine, güvenli ve özel bir ortamda nitelikli sağlık uzmanlarıyla görüşün.



YERLİ BATARYA FABRİKASINDA ÜRETİMİ
YERLİ ROBOTLAR YAPACAK

Yenilenebilir enerji ve enerji teknolojileri markası YEO Teknoloji, %100 iştiraki olan Reap Battery bünyesinde planlandığı enerji depolama sistemleri fabrikası makine üretim hattı için Robo Otomasyon ile anlaştı. Anlaşmayla birlikte ileri seviyede otomasyonla enerji depolama sistemleri robotik üretim hattında üretilecek.

İstanbul Tuzla'da inşası devam eden fabrikanın kapasitesi ilk yıl tek vardiyada 1 GWh olacak. Reap Battery, elektrik şebekeleri, yenilenebilir enerji santralleri, endüstriyel, ticari tesisler ve hanelerin enerji dönüşümünü ekonomik ve gelişmiş enerji depolama çözümleri ile garanti altına alacak.

YEO Teknoloji, iştiraki olan Reap Battery'nin inşası süren enerji depolama sistemleri fabrikası için yerli robotik üretim hattı projeleri gerçekleştiren Robo ile anlaştı. Bu imzayla birlikte ileri seviyede otomasyonla Reap Battery fabrikasında enerji depolama sistemleri, robotik üretim hattında üretilecek.

Söz konusu anlaşmayla ilgili imzalar YEO Teknoloji CEO'su Tolunay Yıldız ve Robo Otomasyon CEO'su Haluk Özcan'ın katıldığı törende atıldı. Robo Otomasyon ile YEO arasında ileri seviye otomasyona dayalı robotik üretim hattının tasarımı, geliştirilmesi ve tam kapasite devreye alınması projesi başladı.

Türkiye'nin önde gelen enerji teknolojileri ve mühendislik şirketlerinden YEO Teknoloji, yüzde 100 iştiraki olan Reap Battery ile yerli ve özgün olarak tasarlanan enerji depolama sistemlerini gelişen teknolojiye uyumlu şekilde üretecek. Yüksek kapasiteli, hassas kalite kontrolü ve ileri seviyede otomasyon sistemiyle enerji depolama sistemleri için yerli robotlar çalışacak.

BU YIL SERİ ÜRETİME GEÇİYOR

İnşası devam eden İstanbul Tuzla'da kurulacak fabrikanın kapasitesi ilk yıl tek vardiyada 1 GWh olacak. 2024 yılında tamamlanacak fabrika yatırımıyla birlikte Reap Battery'nin ekonomik ve gelişmiş enerji depolama çözümleri, elektrik şebekeleri, yenilenebilir enerji santralleri, endüstriyel, ticari tesisler ve hanelerin enerji dönüşümünü garanti altına alacak.

Reap Battery, enerji depolama sistemlerinde araştırma ve geliştirme, tasarım ve mühendislik, tedarik ve üretim, işletme ve bakım hizmetlerini tek noktadan sağlayacak. Gelişmiş elektronik ve mekanik tasarım teknikleri, tecrübeli batarya tasarım ekibi ile güvenilir enerji depolama sistemlerini müşteri ihtiyaca yönelik sunacak.

225 MİLYAR DOLARLIK PAZAR

2020 yılı sonunda 10GWh'a ulaşan enerji depolama sistemlerinin dünyadaki kurulu kapasitesinin 2030'da 194GWh'ye çıkması bekleniyor. Enerji ve madencilik sektörlerinde analiz ve danışmanlık hizmeti sunan küresel araştırma

grubu Wood Mackenzie'nin raporuna göre her yıl %35 büyüyeceği tahmin edilen enerji depolama pazar büyüklüğünün 2030'da 225 milyar dolara çıkması bekleniyor.

YEO Teknoloji CEO'su Tolunay Yıldız, bu alandaki hedeflerini şöyle anlatı: "YEO Teknoloji olarak Aralık 2023'te Reap Battery farikası için uzun vadeli kredi anlaşmasını imzalamıştık. Eylül 2023'te çalışmalarına başlanan Reap Batarya'nın giga fabrikası şimdiye kadar öz kaynaklarla finanse edilmişti. Şimdi de yerli enerji depolama sistemleri için Türkiye'nin yerli ve başarılı robotik sistemler üreticisi Robo Otomasyon ile birlikte çalışacağız. Odağımıza 3D yani dijitalizasyon, desentralizasyon, dekarbonizasyonu alarak yenilenebilir enerji kaynaklarından üretilen enerjinin depolanması için de en yeni çözümleri yine Türkiye'de yerli üretim hattımızda üreterek sunacağız."

prestij yayıncılık

DERGİLERİMİZE ABONE OLMAK İSTER MİSİNİZ?

METAL DÜNYASI DERGİSİ
Yıllık / 12 Sayı

2.000₺

KALIP DÜNYASI DERGİSİ
Yıllık / 6 Sayı

2.000₺

CADCAMCAE DÜNYASI E-DERGİSİ
Yıllık / 4 Sayı

500₺

ABONE FORMU / SUBCRIBTION FORM

Abone Bilgileri / Subscriber Informations

Firma / Company Name:

Ad Soyad / Name Surname:

Title / Mr. / Mrs. (tick as applicable)

Departman / Department:

Adres / Adress:

İlçe / County:

İl / City: Posta Kodu / Post Code:

Tel:

Fax:

e-mail:

V. Dairesi / V. No:

☐ **Banka havalesi ile yatırdım**
Payed with bank transfer

☐ **Elden yatırdım**
Direct Payment

Abonelik Başlangıç: ..../..../....
Subscription Begining Date: ..../..../....

Abonelik Bitiş: ..../..../....
Subscription Ending Date: ..../..../....

prestij yayıncılık

BANKA HESAP NUMARALARI - Bank Account Numbers

İş Bankası
1135 Balmumcu Şubesi
Hesap No: 401414
IBAN: TR810006400000111350401414

Akbank
420 Esentepe Şubesi
Hesap No: 37341
IBAN: TR700004600420888000037341

EURO ACCOUNT PRESTIJ YAYINCILIK BAS. HİZ. SAN. TİC. LTD. ŞTİ.
TÜRKİYE İŞ BANKASI - BALMUMCU BRANCH
BICS/SWIFTCODE: 1135 ISBKTRISXXX
IBAN (RATING NUMBER): TR230006400000211353416049
ACCOUNT NO: 3416049

mubitek
Birlikte İdealinize

evok
Software Studio

LOW CODE

FLOW DM

Yüksek boyutlardaki data süreçlerinizi
ister bulutta ister sunucularınızda
yönetin

Merkez Ofis: Altınşehir Mh. Ahmet Taner Kışlalı Cd. 320 Sk. No:3B Güleç Premium Plaza Kat:9 Ofis 35 Nilüfer/ BURSA

AR-GE Ofis: Uludağ Üniversitesi Görükle Kampüsü Üniversite Cd. No:933 / 407 Nilüfer / BURSA

☎ : +90 224 441 30 37

/ mubitek