



Otomotiv sektöründe siber güvenliğe hız verin

Her virajda güveni tesis
etmek için yol gösterici
rehberiniz

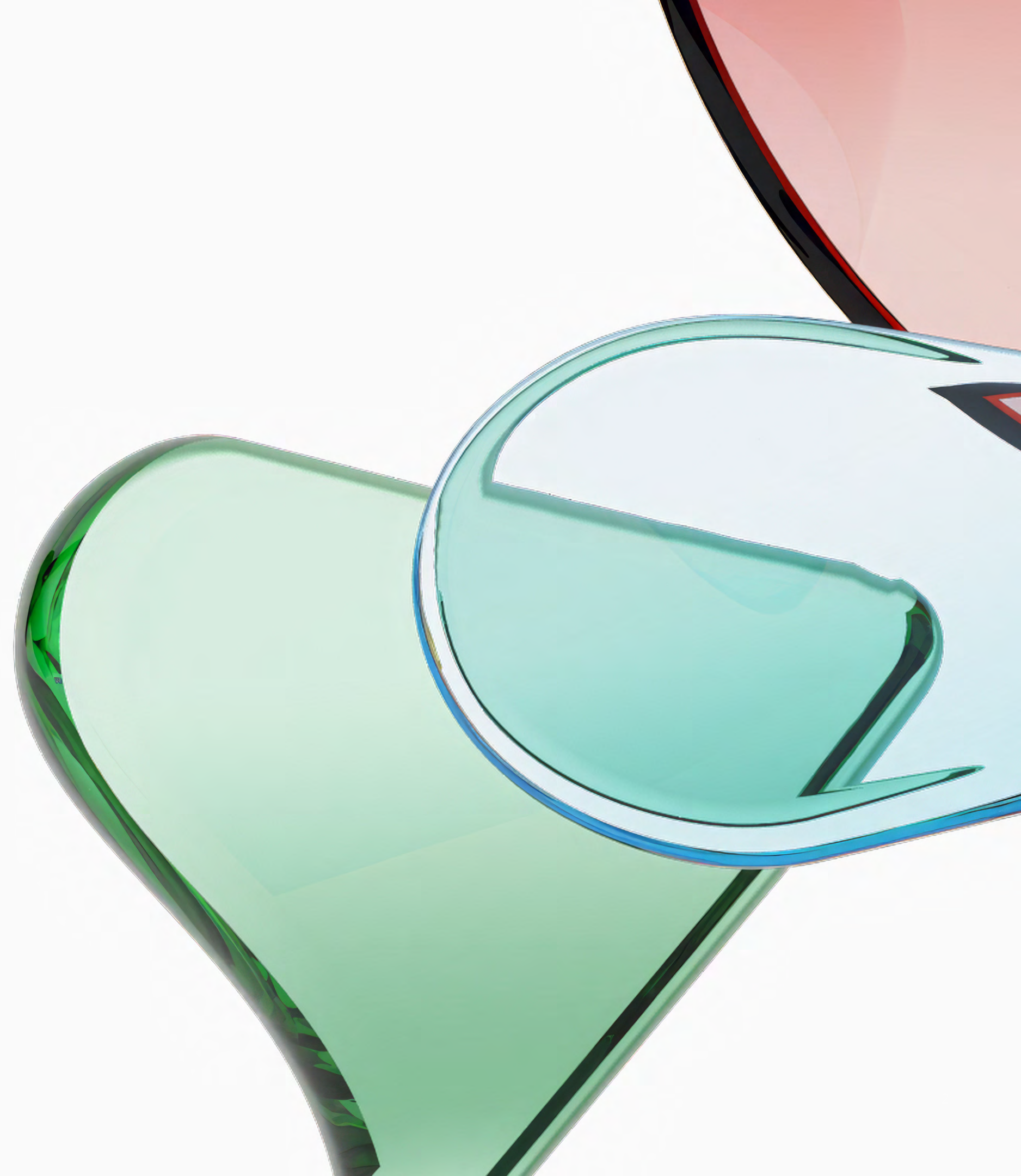


İçindekiler

- 1 Otomotiv sektöründe siber güvenliğe hız vermek
- 2 Uyumluluk ve güvenliği sağlamak için yol gösterici rehberiniz
- 3 Otomotiv sektöründe siber güvenlik planlamasına ilişkin dört temel ilke
- 4 Güven ve uyumluluğu tesis etmeye yönelik beş temel araç
- 5 Sağlam bir siber güvenlik ekosistemi oluşturmak
- 6 Güvenli bir dijital geleceğe adım atmak



Otomotiv sektöründe siber güvenliğe hız verin:
Her virajda güveni tesis etmek için yol gösterici rehberin



Otomotiv sektöründe siber güvenliğe hız vermek

Bağlantılı ve otonom sürüş teknolojilerinin yükselişi hem üreticiler hem de tüketiciler açısından önemli yeni fırsatların kapısını aralıyor. Üreticilerin bu teknolojilerin potansiyelini hayata geçirebilmek için taşıtlara yönelik elektrik sistemlerinde ve elektronik (E/E) sistemlerde siber güvenliğe ilişkin gün geçtikçe artan talepleri karşılayabilmeleri gerekmektedir.

Hızlı evrim

Otomotiv sektörü hızlı bir evrim sürecinden geçmektedir. İddialı inovasyonlara imza atılıyor olması, gelişmiş teknolojiler geliştiriliyor olması ve tüketicilerin bağlantılı araçlara daha fazla ilgi duyar hale gelmesi, tedarikçiler, üreticiler, yolcular ve kullanıcılar açısından daha fazla fırsat ve seçenek anlamına gelmektedir.

Bağlanabilirlik ve otomasyon

Taşıtların dinamik trafik ortamlarında dahi güvenli bir şekilde ilerlemesini mümkün kılan yapay zeka (artificial intelligence, AI) ve makine öğrenimi (machine learning, ML) destekli taşıt otomasyonu bu hızlı evrimi en iyi yansıtan sonuçların başında gelmektedir. Tüketiciler ayrıca mobil uygulamalar üzerinden araçlarına bağlanarak taşıtlarının durumunu ve işlevlerini kontrol edebilmektedir.

Genişleyip büyüyen bir tehdit ortamı

Bu ilerlemeye paralel olarak sürekli değişim gösteren bir tehdit ortamı da söz konusu. Kuruluşlar, bu tehdit ortamının yarattığı riskleri önleyebilmek için sağlam, iyi düşünülmüş ve tutarlı siber güvenlik stratejilerine ihtiyaç duyar.



Rob Brown, BSI Global Otomotiv Sektörü Başkanı

"Günümüzün bağlantılı taşıtlar çağında güveni tesis edebilmek için otomotiv sektöründe siber güvenliğe yönelik tüm yaşam döngüsünü kapsayan bir yaklaşıma ihtiyaç duyulmaktadır. Bu kılavuz ve ortaklığımız yoluyla, müşterileriniz, ortaklarınız ve paydaşlarınız nezdinde kalıcı güveni tesis etmek için standartlara dayalı uyumluluk konusunda size destek olacağız."



Otomotiv sektöründe siber güvenliğe hız verin:
Her virajda güveni tesis etmek için yol gösterici rehberiniz

Uyumluluk ve güvenlięi saęlamak için yol gösterici rehberiniz

Baęlantılı araçlar güvenlik, konfor ve zenginleştirilmiş seyahat deneyimleri sunmaktadır. Ancak tasarım aşamasından kullanımdan kaldırılma aşamasına kadar tüm yaşam döngüleri boyunca siber tehditlere karşı savunmasızdırlar. Kişiyi Tanımlamak için Kullanılabilen Bilgiler (PII), ödeme bilgileri, seyahat geçmişi ve konum verilerinin tümü hack'lenebilir, kötüye kullanılabilir veya manipüle edilebilir. Bu sonucunda bir kullanıcının taşıta veya taşıtının sistemlerine erişimi engellenebilir.

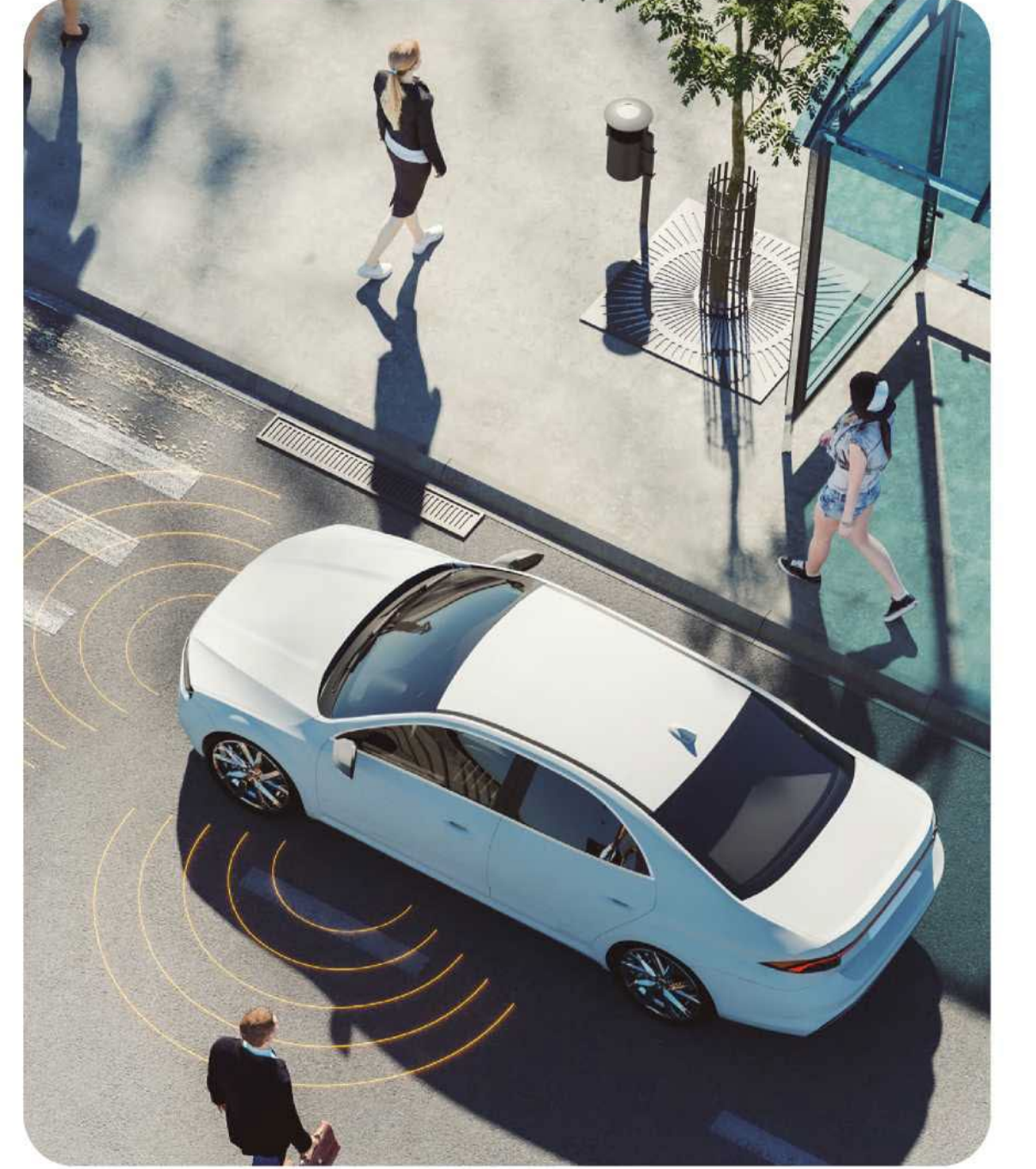
Standart olarak güvenlik

Bu nedenle, siber güvenlięe yönelik olarak ürün yaşam döngüsünün tamamında standart odaklı bir yaklaşımın benimsenmesi büyük önem taşımaktadır. Bu yaklaşım geleceęe hazır, güvenli ve sorumlu bir baęlantılı otomotiv sektörünün temel yapı taşıdır.

Size sağlayacağımız önerileri izleyerek:

- otomotiv eko sistemindeki dijital riskleri etkin şekilde azaltabilirsiniz;
- taşıt yaşam döngüsü boyunca güveni tesis edebilirsiniz;
- tedarik zinciri güvenliğini ve iş birliğini güçlendirebilirsiniz;
- küresel düzenlemelere uyma konusundaki kararlılığınızı gösterebilirsiniz.

2030 yılına gelindiğinde dünya genelinde satılan yeni taşıtların %95'i baęlantılı olacak, bununla birlikte kullanımdaki taşıt sayısı 2023'teki 192 milyon seviyesinden 2027'ye kadar 367 milyona çıkacak.¹



Artan otomasyon ile birlikte daha güçlü siber güvenlik çözümlerine ihtiyaç duyuluyor

Otomotiv Mühendisleri Birliği (SAE) Otomasyon Seviyeleri

SAE'nin farklı sürüş otomasyonu seviyelerini ifade eden Seviye 0 (sürüş otomasyonu yok) ile Seviye 5 (tam sürüş otomasyonu) arasındaki SAE Levels of Driving Automation™, otomotiv sektöründe siber güvenliğinin artırılmasına ilişkin bağlamı göstermektedir.



SAE J3016™ LEVELS OF DRIVING AUTOMATION™

Daha fazla bilgi için bkz.: [sae.org/standards/content/j3016_202104](https://www.sae.org/standards/content/j3016_202104)

Telif Hakkı © 2021 SAE International. Özet tablo, SAE International'ın içerik kaynağı olarak gösterilmesi koşuluyla "OLDUĞU GİBİ" serbestçe kopyalanabilir ve dağıtılabilir.

	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
Sürücü koltuğundaki kişinin ne yapması gerekiyor?	Bu sürücü destek özellikleri etkinleştirildiğinde, ayaklarınız pedallarda olmasa ve direksiyonu çevirmiyor olsanız bile aracı siz kullanıyor sayılırsınız			Bu otomatik sürüş özellikleri etkinleştirildiğinde, "sürücü koltuğunda" oturuyor olsanız bile aracı siz kullanmıyor sayılırsınız		
	Bu destek özelliklerini sürekli olarak denetlemelisiniz ; güvenliği sağlamak için gerektiğinde direksiyonu çevirmeli, fren yapmalı veya hızlanmalısınız			Destek özellikleri istediğinde aracı sizin kullanmanız gerekir	Bu otomatik sürüş özellikleri, sürüşü devralmanızı gerektirmeyecektir	

Telif Hakkı © 2021 SAE International.

	Bunlar sürücü destek özellikleridir			Bunlar otomatik sürüş özellikleridir		
Bu özellikler ne işe yarar?	Bu özellikler uyarılar ve anlık yardım sağlamakla sınırlıdır	Bu özellikler sürücüye direksiyon VEYA frenleme/ hızlanma desteği sağlar	Bu özellikler sürücüye direksiyon VE frenleme/hızlanma desteği sağlar	Bu özellikler, sınırlı koşullar altında araç sürüşü gerçekleştirebilir ve gerekli tüm koşullar karşılanmadıkça çalışmaz.	Bu özellik her türlü koşulda araç sürüşünü gerçekleştirebilir	
Örnek Özellikler	- otomatik acil durum frenlemesi - kör nokta uyarısı - şerit takip uyarısı	şerit ortalama VEYA adaptif hız sabitleme	şerit ortalama VE aynı zamanda adaptif hız sabitleme	sıkışık trafikte şoför görevi görür	- yerel sürücüsüz taksi - pedallar/ direksiyon simidi takılı olabilir veya olmayabilir	Seviye 4 ile aynıdır ancak bu özellik her yerde ve her koşulda araç sürüşü gerçekleştirebilir

²SAE levels of driving automation™ daha net tanımlar içerecek ve uluslararası kitleye hitap edecek şekilde revize edildi

Otomotiv sektöründe siber güvenlik planlamasına ilişkin dört temel ilke

Otomotiv sektöründe siber güvenlik planlamasına dönük bütünsel bir yaklaşım izlenmesi, iş ortaklarınız ve müşterileriniz nezdinde güveni tesis etmenize yardımcı olur. Birbiriyle bağlantılı olarak kabul edilerek dikkate alınması gereken dört temel unsur vardır: taşıt, yaşam döngüsü, tedarik zinciri ve düzenlemeler.

1

Bağlantılı araçlar

Araca yönelik karmaşık siber tehditleri öngörmek

OEM'ler ve tedarikçileri, giderek artan sayıda saldırı yüzeyine yayılmış gelişen siber tehditlere karşı sağlam önlemler aldıklarını göstermelidir. Uygulamalar, Bluetooth, Wi-Fi, telematik ve araç içi tanılama portları gibi giriş noktalarının bulunuyor olması nedeniyle, sistemlerin en iyi uygulama standartlarına uygun şekilde güvence altına alınması gerekmektedir.

3

Ürün yaşam döngüsü

Tüm yaşam döngüsü boyunca siber güvenlik korumasının gösterilmesi

Siber güvenlik sistemlerinin, tasarım, yapım ve işletmeden bakıma (kablosuz (OTA) güncellemeler dahil) ve kullanım ömrü sonundaki veri temizliğine kadar bir aracın ve bağlı mobilite varlıklarının tüm yaşam döngüsünü kapsamaları gerekir. Standartlara dayalı titiz bir planlama, uçtan uca tam güven sağlayacaktır.

2

Tedarik zinciri

Dijital tedarik zinciri riski

Karmaşık tedarik zincirleri, siber güvenlik ihlallerinden malzeme kıtlığına kadar çeşitli aksaklıklara karşı duyarlıdır. Prototiplerden yazılım kodlarına kadar çeşitli hassas verilerin paylaşımında güven esastır. Standartlar ve güvenceler işte bu güvenin sağlanmasına yardımcı olur.

4

Düzenlemeler ve standartlar

Otomotiv sektörüne ilişkin düzenleme ve standartların güncel olarak takip edilmesi

OEM'ler ve tedarikçiler, 2024 yılında yürürlüğe giren UNECE Düzenlemesi No. 155 (R-155) ve No. 156 (R-156) gibi düzenlemelere ve uyumluluk son tarihlerine uyum sağlamaktadır. Buna paralel olarak standart kuruluşları ve endüstri grupları, tedarikçilerin uyumluluğu sağlamasına ve siber güvenlik risklerini azaltmasına yardımcı olmak için en iyi uygulamalar geliştirmektedir.



Otomotiv sektöründe siber güvenliğe hız verin:
Her virajda güveni tesis etmek için yol gösterici rehberiniz

Güven ve uyumluluğu tesis etmeye yönelik beş temel araç

Otomotiv sektöründe kapsamlı siber güvenlik uzmanlığına sahip, küresel çapta tanınan bir lider kuruluş olarak, uyumluluk ve güven için kapsamlı en iyi uygulama çözümlerini hayata geçirmenize yardımcı oluyoruz. Küresel düzenlemelere uyumluluğu sağlama, dijital riski azaltma ve güven oluşturma çabalarınıza eğitim, denetim ve akredite sertifikasyon hizmetlerimizle destek oluyoruz.



Sonraki iki sayfada, kuruluşunuzun en iyi uygulamaları anlamasına ve benimsemesine yardımcı olmak için kullanması gereken beş temel standardı ve değerlendirme şemasını paylaşıyoruz. Bunlar sektörünüz için geçerli standartların sadece bir alt kümesini temsil etmektedir.

Üst düzey yöneticilerin %68,5'i otomotiv tedarik zincirinde standartların etkileri ve işletmeler için ne anlama geldikleri konusunda daha fazla anlayışa ihtiyaç olduğunu düşünüyor.³

Güven ve uyumluluğu tesis etmeye yönelik beş temel araç

1

Bilgi Güvenliği Yönetim Sistemleri (ISO/IEC 27001)

Bilgi güvenliği yönetimi alanında dünya çapında kabul gören ve güvenilen bir standart. Yapay zeka, makine öğrenimi ve otomasyonun sorumlu ve güvenli kullanımına kapı açan temel bilgi güvenliği yönetim sistemleri standardıdır.

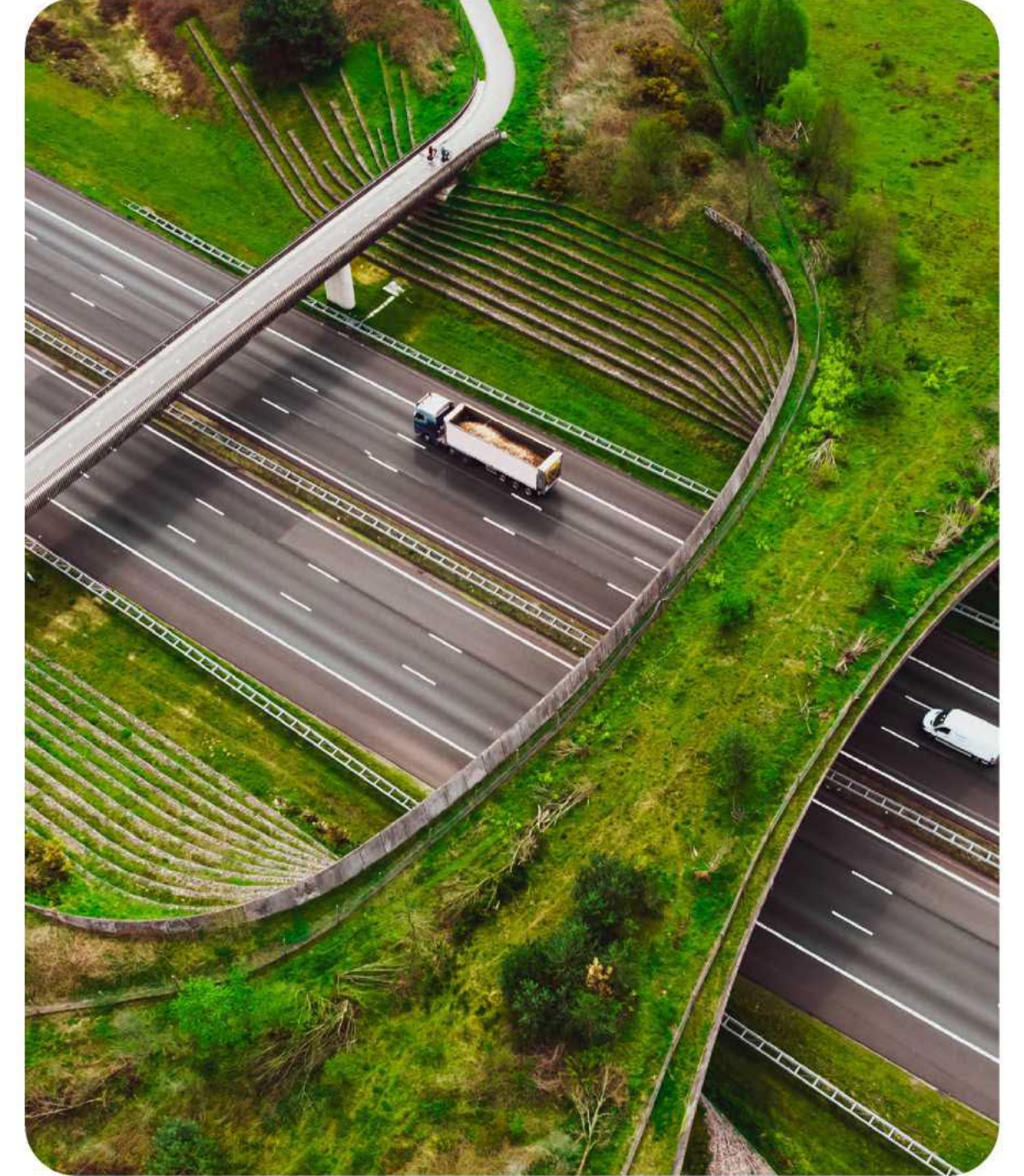
Daha fazla bilgi edinin

2

TISAX Değerlendirmesi

Otomotiv sektörü için otomotiv sektörü tarafından geliştirilen bu bilgi güvenliği değerlendirme şeması ISO/IEC 27001 gerekliliklerini temel almaktadır. Üç temel alanda bilgi güvenliğini bir araya getirmekte ve OEM'lerden tüm kademelerdeki tedarikçilere kadar tedarik zinciri ortakları arasında güvenli bilgi alışverişine imkan sağlamaktadır.

Daha fazla bilgi edinin



Güven ve uyumluluđu tesis etmeye yönelik beş temel araç

3

Araç Siber Güvenlik Gereksinimleri (ISO/SAE 21434)

Bu standart, tüm bileşenler ve arabirimler de dahil olmak üzere, karayolu taşıtlarındaki elektrikli ve elektronik (E/E) sistemlerin tüm yaşam döngüsü boyunca siber güvenlik risk yönetimine ilişkin gereklilikleri belirtir. Standardın etkili bir şekilde uygulanması, UNECE düzenlemeleri R-155 (siber güvenlik yönetim sisteminin uygulanması) ve R-156'nın (yazılım güncelleme yönetim sisteminin uygulanması) gerekliliklerini karşılamanıza yardımcı olur.

Daha fazla bilgi edinin

4

ENX Araç Siber Güvenliğı (VCS) Denetim Şeması

2024'te yayınlanan bu şema, karayolu taşıtları için E/E sistemleri geliştiren, üreten veya sürdüren otomotiv tedarikçilerini desteklemektedir. ISO/SAE 21434 ve UNECE R-155 kapsamında siber güvenlik mühendisliğinin denetimine ilişkin yönergeleri (ISO/PAS 5112) uygulayarak standartlaştırılmış Siber Güvenlik Yönetim Sistemi (CSMS) denetimleri sağlar. Başarılı bir denetim, tedarik zinciri ortakları arasında güven ve iş birliğinin temelini oluşturur.

Daha fazla bilgi edinin

5

Güvenli Dijital Uygulamalar için BSI Kitemark™ Sertifikasyonu

Bu BSI Kitemark™ sertifikasyonu, kuruluşunuzun bir araca gömülü olan veya uzaktan bağlanan dijital uygulamalarını titiz ve bağımsız testlerden geçirdiğini kanıtlar. OWASP (Açık Web Uygulaması Güvenlik Projesi), web uygulamaları için ASVS (Uygulama Güvenliğı Doğrulama Standardı) ve MASVS (Mobil Uygulama Güvenliğı Doğrulama Standardı) gibi sektör standartlarını karşılayan sağlam kontroller sağlayarak güven yaratır.

Daha fazla bilgi edinin



Otomotiv sektöründe siber güvenliğe hız verin:
Her virajda güveni tesis etmek için yol gösterici rehberiniz

Sağlam bir siber güvenlik ekosistemi oluşturmak

Tedarik zinciri ve ürün yaşam döngüsündeki rolünüzle ilgili standartları, çerçeveleri ve çözümleri keşfetmek için bir sonraki sayfada yer alan grafiğimizi kullanın. Bu grafik, bu kılavuzda özetlenen beş en iyi uygulamayı ve ilgili ek standartları bir araya getirerek dijital güveni artırmak için kapsamlı bir araç seti oluşturmanıza yardımcı olur.

Otomotiv sektörü şirketleri bir sorun olduğunun farkındalar ancak şu anda bu konuda ne yapacaklarını bilemiyorlar.⁴



Otomotiv Siber Güvenlik Ekosistemi

Ürün Yaşam Döngüsü	Tasarım ve Yapım				İşletme ve Bakım			Yeniden Kullanma ve Geri Dönüşüm	
Tedarik zinciri	Kademe 3 Parça/donanım/ yazılım tedarikçisi	Kademe 2 Bileşen tedarikçisi	Kademe 1 Sistem tedarikçisi	OEM Otomobil üreticisi	Geliştirici Gömülü Yazılım, SaaS	İşlemci Veri depolama ve işleme	Geliştirici Yazılım güncellemesi	İşlemci Fabrika ayarlarına sıfırlama/veri silme	Geri dönüşümcü Geri kazanım ve yeniden kullanım
Ürünler	Çipler	PCB'ler	SatNav, ALKS, EMS	Araç kullanıcı uygulamaları ve Bayi araçları	Gömülü yazılım uygulamaları	Bulut depolama	Düzeltilme paketleri, sürümler, güvenlik güncellemeleri	Araçtaki, uygulamalardaki ve buluttaki veriler	Çipler, PCB'ler, sistemler, değerli malzemeler
Düzenlemeler	<<< UN R155 >>>				>>> UN 156 >>>			GDPR	>>>
OEM Aşağı Akış	<<< ISO/IEC 27001, TISAX ve ENX VCS için OEM aşağı akış gereksinimleri >>>								>>>
Tedarikçi hedefleri	<<< Düzenlemelere ve müşteri gereksinimlerine uyumluluk OEM'lerden ve müşterilerden gelen istenmeyen kontrolleri ortadan kaldırın Teknolojik ilerleme için sağlam bir platform oluşturun Siber risklere (kötü amaçlı yazılım) ve yetkisiz erişime (hack) karşı önlem alın >>>								>>>
BSI Çözümleri	<<< Aşağıdakileri destekleyen standartlar, eğitimler, değerlendirmeler ve sertifikasyonlar: ISO/IEC 27001 - Bilgi Güvenliği Yönetimi ISO/SAE 21434 - Araç Siber Güvenlik Yönetimi TISAX Değerlendirmesi ve ENX VCS Denetim Şeması >>>								>>>
	ISO/IEC 24089- Taşıtlar için Yazılım Güncellemesi Güvenli Dijital Uygulamalar için BSI Kitemark™				ISO/IEC 24089- Taşıtlar için Yazılım Güncellemesi Güvenli Dijital Uygulamalar için BSI Kitemark™	ISO/IEC 27017 - Bulut Hizmetleri için Bilgi Güvenliği ISO/IEC 27018 - Genel Bulutlarda Kişiyi Tanımlamak için Kullanılabilen Bilgiler (PII)	ISO/IEC 24089- Taşıtlar için Yazılım Güncellemesi Güvenli Dijital Uygulamalar için BSI Kitemark™	ISO/IEC 27017 - Bulut Hizmetleri için Bilgi Güvenliği ISO/IEC 27018 - Genel Bulutlarda Kişiyi Tanımlamak için Kullanılabilen Bilgiler (PII)	
Faydalar	<<<				Tüketiciler, tedarik zinciri ortakları ve düzenleyiciler nezdinde paydaş güvenini tesis etme				>>>



Otomotiv sektöründe siber güvenliğe hız verin:
Her virajda güveni tesis etmek için yol gösterici rehberiniz

Güvenli bir dijital geleceğe adım atmak

Bu kılavuzda paylaştığımız yaklaşım, siber güvenliğe yönelik sağlam bir yaşam döngüsü yaklaşımı oluşturmanıza yardımcı olabilir ve yaklaşım:

- 1** Dijital riskleri aktif olarak öngörmenizi ve azaltmanızı sağlar.
- 2** Tedarik zinciri ortaklarıyla iş birliğini güçlendirmenize yardımcı olur.
- 3** Düzenlemelere ve OEM zorunluluklarına uyumluluğu gösterir.
- 4** Yapay zeka, makine öğrenimi ve otomasyon teknolojilerinin benimsenmesini hızlandırır.

Olumlu etki yaratmak ve işlerinizi daha hızlı büyütmek için olmazsa olmaz bir gereklilik olarak değişen dijital risklere önlem almanıza yardımcı olacaktır.



//

Otomotiv siber güvenliği pazarı büyüklüğünün 2030 yılına kadar **9,7 milyar ABD dolarına** ulaşması beklenmektedir.⁵

//



İş ortağınız ilerlemeye devam ediyor

Standartlarımız, eğitimlerimiz,
denetimlerimiz ve belgelendirme
hizmetlerimiz hakkında daha fazla bilgi
edinmek için web sitemizi ziyaret edin

