3DEXPERIENCE PLATFORMU BULUT GÜVENLİĞİ VE GİZLİLİK

White Paper

İÇİNDEKİLER

GİRİŞ

FELSEFEMİZ

Bulut bilişim, iş yapma şeklimizde bir paradigma değişikliğini temsil eder. Kuruluşlar, bulut imkanlarının hızı ve basitliğinin yanı sıra uzman sağlayıcıların bakım, BT ve güvenlik hizmetlerinden faydalanmak için uygulamalar kullanmakta, verileri yönetmekte ve operasyonları buluta kaydırmaktadır.

Dassault Systèmes, 2012 yılında **3D**EXPERIENCE® platformunun kurulmasından bu yana bulut tabanlı hizmetler sunmaktadır. Müşterilerimizin güvenli, esnek ve ölçeklenebilir bulut kaynaklarından yararlanmasını sağlayan tam bulut tabanlı bir ekosistem olan **3D**EXPERIENCE Cloud platformunu oluşturduk. Müşterilerimizi çözümlerimizin her alanında güven ve güvenilirlik ile desteklemeyi misyonumuz haline getirdik.

Risk yönetimi yaklaşımımız çok yönlü ve proaktif olup en iyi uygulamalara dayanır ve operasyonlarımızdaki güvenlik tehditlerini öngörmek üzere tasarlanmıştır. ISO/IEC 27001:2017 ve ISO/IEC 27701:2019 sertifikalı, rutin denetime tabi olan bir Bilgi Güvenliği ve Gizlilik Yönetim Sistemi (ISPMS) kullanıyoruz. ISPMS'miz gizlilik, bütünlük, kullanılabilirlik ve sorumluluk gibi temel değerlere dayanmaktadır.

Bu White Paper, Dassault Systèmes'in müşterilerin uygulamalara, veri depolama alanına ve ölçeklenebilir bilgi işlem kaynaklarına eriştiği bulut tabanlı platformumuz olan **3D**EXPERIENCE için güvenlik ve uyumluluk yaklaşımını özetlemektedir. Bu White Paper'da bulut güvenliği, gizlilik ve uyumluluk uygulamalarımızın temel yönlerini ele alıyoruz.

BİLGİ GÜVENLİĞİ VE GİZLİLİK MİSYON BİLDİRİMİZ

Dassault Systèmes Bilgi Güvenliği ve Gizlilik Misyon Bildirimi aşağıdadır:[1].

3DEXPERIENCE platformu Hizmet olarak Yazılım (SaaS) için bilgi güvenliği ile ilgili riske maruz kalma durumunu yönetmek ve kişisel olarak tanımlanabilir bilgileri (PII) korumanın yanı sıra bilgilerin gizliliği, bütünlüğü ve kullanılabilirliği ile aşağıdakilerin korunmasını sürekli olarak geliştirme:

- PII dahil olmak üzere müşteri fikri mülkiyet ve kullanıcı verileri
- Dassault Systèmes'in itibarı ve fikri mülkiyeti
- Bulut kullanılabilirliği ve esnekliği
- Geçerli siber güvenlik ve veri koruma düzenlemelerine ve standartlarına uygunluk

Bu misyon bildirimi, çalışanlar için belgelenmiş bilgi olarak ve ilgili taraflar için talep üzerine sunulmuştur.

SORUMLULUK REDDİ

Bu içerik, Mart 2022 itibarıyla **3D**EXPERIENCE Cloud platformunun güvenlik, gizlilik, kalite ve uyumluluk uygulamalarını temsil etmektedir. Burada belirtilen uygulamalarımızın içeriği, tamamen Dassault Systèmes'in takdirine bağlı olarak değişebilir. Bu belgede kullanılan "biz" ve "bizim" ifadeleri, özel olarak Dassault Systèmes'e atıfta bulunmaktadır.

1. Bu, ISO 27001 Bilgi Güvenliği ve Gizlilik Politikası'na karşılık gelir.

DASSAULT SYSTÈMES: GÜVENLİK VE GİZLİLİK ODAKLI BİR ORGANİZASYON

3DEXPERIENCE PLATFORMU SAAS SİBER GÜVENLİK VE GİZLİLİK YÖNETİMİ

Dassault Systèmes Ar-Ge, **3DEXPERIENCE** platformu SaaS için SGS International Certification Services (SGS-ICS) tarafından ISO/IEC 27001:2017 ve ISO/IEC 27701:2019 sertifikalı, merkezi olarak kontrol edilen bir Bilgi Güvenliği ve Gizlilik Yönetim Sistemi (ISPMS) kullanmaktadır. Sertifikasyonun kapsamı şunları içerir:

1. Tasarım, geliştirme, teslimat, dağıtım, bulut operasyonları ve **3DEXPERIENCE** platformu SaaS desteği.

2. Dassault Systèmes aşağıdaki görevleri gördüğünde veri gizliliği yönetimi:

a. **3DEXPERIENCE** platformu SaaS bağlamında sağlanan kişisel verilerin işlenmesi için denetleyici.

b. Bir müşterinin kontrolü altında **3DEXPERIENCE** platformu SaaS içinde işlenen PII için işlemci.

ISPMS'miz Dassault Systèmes Ar-Ge Yönetim Kurulu tarafından yönetilir ve yönetim incelemesine tabidir. **3DEXPERIENCE** platformunda çalışan ve SGS-ICS onaylı ISO 9001:2015 sertifikasına sahip, köklü bir Kalite Yönetim Sistemi (QMS) üzerine kurulmuştur.

QMS ve ISPMS, Güvenli Yazılım Geliştirme Yaşam Döngüsü (Secure SDLC) yöntemine dayanan birçok temel ve destekleyici süreci paylaşmaktadır. ISPMS ayrıca bilgi güvenliği ve veri korumasına odaklanan ek risk tabanlı süreçler de içerir.

Tüm ISPMS süreçleri ve kontrolleri, Dassault Systèmes Ar-Ge **3DEXPERIENCE** Uyumluluk Denetimi programı tarafından uyumluluk ve etkinlik açısından sürekli olarak değerlendirilmektedir. Sonuç olarak ortaya çıkan düzeltici eylemler ve sürekli iyileştirmeler **3DEXPERIENCE** platformunda takip edilir.

Denetim kriterleri ISO 9001, ISO 27001 ve ISO 27701 yönetim sistemi ve kontrol gereksinimlerine dayanmaktadır. Dassault Systèmes hem PII denetleyicisi hem de PII işlemcisi rolünde hareket ettiğinden tüm ISO 27001 Ek A kontrolleri ve ISO 27701 Ek A ve B kontrolleri, yönetim sisteminin kapsamına dahil edilmiştir (bkz. Veri Koruma ve Gizlilik, s. 11).

ISPMS, **3DEXPERIENCE** platformu Bilgi Güvenliği ve Gizlilik Misyonu Bildirimi (Politika Bildirimi) ve yıllık hedefler ile desteklenmektedir. Hedefler, operasyonel ekipler tarafından izlenen ölçülebilir hedefler ve Temel Performans Göstergeleri (KPI'lar) sağlar. Siber güvenlik ve veri koruma hedefleri, Dassault Systèmes yıllık planlama sürecinin bir parçası olarak uygunluk açısından düzenli aralıklarla gözden geçirilir.

GÜVENLİK, GİZLİLİK VE UYUMLULUK PERSONELİMİZ

Ar-Ge Yönetim Kurulu

Dassault Systèmes Ar-Ge Yönetim Kurulu, veri koruma gereksinimleri ve gizliliği için Dassault Systèmes Genel Danışmanının desteğiyle **3DEXPERIENCE** Bilgi Güvenliği ve Gizlilik Yönetim sisteminin (ISPMS) etkinliğinden nihai olarak sorumludur. AR-Ge Yönetim Kurulu, ISPMS'ye ve müşteri beklentilerine olan bağlılığını aşağıdakiler dahil olmak üzere çeşitli yollarla aktif olarak göstermektedir:

- Bilgi Güvenliği ve Gizlilik Politikasının ve yıllık hedeflerin kuruluşun stratejik yönüyle uyumlu olmasını sağlamak;
- ISPMS gerekliliklerinin kuruluşun iş süreçlerine entegrasyonunu sağlamak;
- ISPMS için gerekli kaynakların mevcut olmasını sağlamak;
- ISPMS'nin önemini bildirmek;
- ISPMS'nin amaçlanan sonuçlara ulaşmasını sağlamak;
- Kişileri ISPMS'nin etkinliğine katkıda bulunmak üzere yönlendirmek ve desteklemek;
- ISPMS süreçlerinin ve operasyonlarının sürekli iyileştirilmesini teşvik etmek.

Siber Güvenlik, Veri Gizliliği ve Uyumluluk Ekipleri

Dassault Systèmes, her bir pozisyon veya rolle ilişkili misyonu, açıklamayı, teslim edilecek öğeleri, KPI'ları, rol profilini ve becerileri tanımlayan bir kurumsal rol modelini sürdürmektedir.

Bilgi Güvenliği Başkanları (CISO) ve güvenlik liderlerinden oluşan bir ekip, Dassault Systèmes Bilgi Güvenliği Programı'nı uygulamaktan genel olarak sorumludur. Bu ekip; küresel düzeyde bilgi güvenliği politikalarını, standartlarını, kılavuzlarını ve prosedürlerini oluşturmaktan, sürdürmekten ve uygulamaktan sorumludur.

Dassault Systèmes Ar-Ge Siber Güvenlik ve Veri Gizliliği Bölümü, **3DEXPERIENCE** ISPMS'sinin ISO 27001 ve ISO 27701 gerekliliklerine uygun olarak planlanmasını, uygulanmasını, sürdürülmesini ve sürekli olarak geliştirilmesini sağlamaktan sorumludur. Bu bölüm, ISPMS'ye uygunluğu ve ISPMS'nin etkinliğini izlemenin yanı sıra bunu standart yönetim toplantılarının bir parçası olarak üst düzey yönetime bildirmekten sorumludur.

Grup Veri Koruma Görevlisi (DPO); en iyi uygulamaları, sorumluluğu ve Dassault Systèmes'in sürdürülebilir büyümesini sağlamak için Dassault Systèmes'e PII koruması konusunda bilgi verir ve tavsiyelerde bulunur. Grup DPO'su, veri korumasını denetleme makamlarının ayrıcalıklı muhatabıdır ve Dassault Systèmes Genel Danışmanına ISPMS'nin uygunluğu ve etkinliği hakkında raporlar sunar.

Ar-Ge Uyum ve Risk ekibi, Dassault Systèmes'in iç süreçlere ve ISO 9001, ISO 27001 ve ISO 27701 gibi endüstri sertifikalarına uygunluğunu değerlendirmek için bir iç uyumluluk denetim programı yürütmektedir. Denetim bulguları ve ilgili düzeltici ve önleyici eylem planları (CAPA'lar) platformda yönetilir.

Grup İç Denetim ekibi, Dassault Systèmes İç Kontrol Değerlendirmesi (ICE) çerçevesine uyumu ve bu çerçevenin etkinliğini kurumsal düzeyde bir iç denetim programı aracılığıyla tanımlar ve değerlendirir. İç Kontrol Çerçevesi, Genel Kontroller ve Bilgi Teknolojileri Genel Kontrollerinin (ITGC) kurulması ve doğrulanması yoluyla risklerin azaltılmasına yardımcı olur.

TÜM ÇALIŞANLAR İÇİN İŞE ALIM VE EĞİTİM

Dassault Systèmes'e katılan çalışanlar; davranış kurallarımıza, BT tüzüğüne ve veri koruma politikalarımıza uymayı kabul etmelidir. Tüm yeni çalışanlar, aşağıdakiler de dahil olmak üzere güvenlik ve gizliliğe yönelik zorunlu etik ve uyumluluk eğitimini alır:

- Veri güvenliğine yönelik tehditleri önleme.
- Temiz masa politikasıyla fiziksel verilerin ve iş istasyonlarının güvenliğini sağlama.
- Kişisel verilerin korunması ve gizliliği.
- Etik iş davranışı; yolsuzlukla mücadele ve rekabet hukuku ilkeleri.
- Olay yönetimi; potansiyel tehditleri tanıma ve raporlama.

Kuruluş genelinde güvenlik ve gizlilik bilincini sürekli olarak destekliyoruz.

UZAKTAN ÇALIŞIRKEN GÜVENLİK

Dassault Systèmes çalışanları uzaktan çalışırken verilerine, uygulamalarına ve platformun yardımcı programlarına yalnızca bir VPN üzerinden erişebilir. Bu hem şirket hem de kişisel cihazlar için geçerlidir. Sadece VPN erişimi olan kayıtlı ve onaylanmış kişisel cihazlara izin verilir.

BULUT GÜVENLİĞİ ORTAKLARIMIZ

Operasyonlarımız genelinde güvenlik ve uyumluluk sağlamak için 3DS Outscale dahil olmak üzere bulut altyapısı (IaaS) sağlayıcılarımızla yakın bir şekilde çalışırız. IaaS sağlayıcılarımızın diğer kriterlerin yanı sıra ISO 27001 sertifikalı olmasını şart koşarız.

GÜVENLİK STANDARTLARIMIZ

Siber güvenlik yaklaşımımız en saygın endüstri standartlarına dayanmaktadır. Bağımsız siber güvenlik uzmanları, yazılım sağlayıcıları için küresel standartlar oluşturmak üzere aktif olarak iş birliği yapmaktadır. OWASP, NIST ve ISO/IEC, siber güvenlik ve gizlilik ekiplerimize riskler ile güvenlik açıklarını azaltmak için en iyi uygulamalar, gereksinimler, kontroller, testler ve diğer araçlarla rehberlik eden üç uzman kuruluştur.

OWASP: OPEN WEB APPLICATION SECURITY PROJECT[1]

OWASP, kuruluşların son derece güvenli uygulamalar geliştirip bunları sürdürmelerini sağlamak için çalışmaktadır. OWASP Vakfı; en son araştırmalar, yaygın olarak kullanılan çerçeveler ve uygulama güvenliği ile ilgili önemli bilgiler için önde gelen kaynaktır.

Küresel ittifakların yardımıyla OWASP, şunları sağlar:

- Uygulama güvenliği araçları, standartları ve yöntemleri
- Güvenli kod geliştirme, güvenlik kodu incelemeleri ve uygulama güvenliği testi için kaynaklar
- Standart güvenlik kontrolleri ve kütüphaneleri

OWASP'ın başlıca yayınları şunları içerir:

- En Büyük 10 Web Uygulaması Güvenliği Riski
- Güvenli Kodlama Uygulamaları
- Kod İnceleme Kılavuzu
- Uygulama Güvenliği Doğrulama Standardı

NIST: ULUSAL STANDARTLAR VE TEKNOLOJİ ENSTİTÜSÜ[2]

NIST, önemli ölçüm çözümlerinin yanı sıra elektronik, yazılım ve diğer teknolojilerdeki tarafsız standartlar için önde gelen bir kaynaktır. NIST Special Publication (SP) 800-53 bilgi sistemleri ve kuruluşları için güvenlik kontrollerini ve gizlilik kontrollerini tanımlar.

NIST SP 800-53; organizasyonel operasyonları ve varlıkları, bireyleri ve diğer oluşumları "düşmanca saldırılar, insan hataları, doğal afetler, yapısal arızalar, yabancı istihbarat kuruluşları ve gizlilik riskleri dahil olmak üzere çeşitli tehdit ve risklerden" korumak için tasarlanmıştır. Bu kontroller, hem işlevsellik hem de güvence açısından güvenlik ve gizliliği ele alır.

ISO/IEC: ULUSLARARASI STANDARDİZASYON TEŞKİLATI VE ULUSLARARASI ELEKTROTEKNİK KOMİSYONU[3]

ISO/IEC; BT ve iletişim teknolojisindeki standartları teşvik etmek için çalışan ortak bir teknik komitedir. **3D**EXPERIENCE platformu SaaS için ISPMS'miz ISO/IEC 27001:2017 ve ISO/IEC 27701:2019 sertifikalı, QMS'miz ise ISO 9001:2015 sertifikalıdır ve her ikisi de SGS-ICS tarafından onaylanmıştır (bkz. "**3D**EXPERIENCE platformu SaaS Siber Güvenlik ve Gizlilik Yönetimi", s. 4).

ISO 9001, bir kuruluşta aşağıdaki durumlar geçerli olduğunda kalite yönetim sistemi için gereklilikleri belirtir:

a. müşterinin gereksinimlerinin yanı sıra geçerli yasal ve düzenleyici gereksinimleri karşılayan ürün ve hizmetleri sürekli olarak sunabilmesi gerektiğinde ve

b. sistemin iyileştirilmesine yönelik süreçler ve müşterinin gereksinimlerinin yanı sıra geçerli yasal ve düzenleyici gereksinimlere uygunluğun güvencesi dahil olmak üzere sistemin etkin bir şekilde uygulanması yoluyla müşteri memnuniyetini artırmayı amaçladığında.

Kalite Yönetim Sistemimiz (QMS); tasarım, geliştirme, teslimat, dağıtım, bulut operasyonları için kullanılan süreçlere dayanmakta ve **3D**EXPERIENCE platformunu desteklemektedir. Uygulama güvenliği uygulamalarımızın çoğu QMS'mize gömülüdür.

ISO/IEC 27001; Bilgi Güvenliği Yönetim Sisteminin (ISMS) oluşturulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereklilikleri belirtir. ISO/IEC 27001 Ek A; kamu ağlarında uygulama hizmetlerinin güvenceye alınması, uygulama güvenliği işlemlerinin korunması, güvenli bir geliştirme politikasının uygulanması, yazılım paketlerindeki değişikliklerin kısıtlanması, güvenli sistem mühendisliği ilkelerine uyulması gibi beklenen her türlü kontrolleri belirtir.

ISO/IEC 27701, gereklilikleri belirler ve kuruluş bağlamında gizlilik yönetimi için ISO/IEC 27001 ve ISO/IEC 27002'ye bir uzantı olarak bir Gizlilik Bilgi Yönetim Sistemi'nin (PIMS) oluşturulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için rehberlik sağlar. Bu standart, PII işlemesi için sorumluluk ve sorumluluk sahibi PII denetleyicileri ve PII işlemcileri için rehberlik sağlar. Ek A, PII denetleyicileri için kontrol hedeflerini ve kontrollerini belirtir. Ek B, PII işlemcileri için kontrol hedeflerini ve kontrollerini belirtir.

1. Daha fazla bilgi için: www.owasp.org
2. Daha fazla bilgi için: csrc.nist.gov
3. Daha fazla bilgi için: iso.org/isoiec-27001-information-security

TEMEL GÜVENLİK ÖZELLİKLERİ

KİMLİK DOĞRULAMA VE YETKİLENDİRME

3DEXPERIENCE Cloud platformunun kimlik doğrulama ve yetkilendirme mekanizması **3D** Passport, kullanıcıların tüm rollerine, uygulamalarına ve hizmetlerine güvenli erişim sağlayan kişiselleştirilmiş bir giriştir. Yöneticiler, parola gücü ve son kullanım tarihi gibi kullanıcı kimlik doğrulaması ilkelerini düzenleyip parolaları kırmaya yönelik deneme yanılma saldırısı girişimlerini tespit etmek için belirli modeller yapılandırır.

3D Passport Özellikleri

Veri Gizliliği

Çevrimiçi çözümlerimizin tüm kullanıcıları Dassault Systèmes Gizlilik Politikasına erişebilir ve **3D** Passport'larını oluştururken bunu kabul etmeleri gerekir. Kullanıcılar, haklarını Dassault Systèmes politikaları ve süreçlerine uygun şekilde bir web formu aracılığıyla talep göndererek kullanabilir.

Buna ek olarak şirketler, onay için kullanıcılarına kendi Gizlilik Politikalarını da sunabilir. Bu durumda platform yöneticisi kendi Gizlilik Politikasını, Platform Yönetimi panosundan yüklemelidir.

Tek Oturum Açma (SSO)

3D Passport, doğrulama ve yetkilendirme verisi alışverişini standart bir biçimde gerçekleştirerek **3D**EXPERIENCE Cloud platformundaki uygulamalarda sorunsuz tek oturum açma deneyimi sağlar.

Çok Faktörlü Kimlik Doğrulama (MFA)

Platformda MFA özelliklerinden yararlanılarak daha yüksek bir güvenlik seviyesi elde edilebilir. Örneğin, MFA bir yönetici tarafından yapılandırıldığında, kullanıcı ek güvenlik için parolanın yanında girilecek bir kod oluşturmak üzere bir mobil uygulama kullanabilir.

ERİŞİM KONTROLÜ

Erişim kontrolü, bulut bilişim ortamımızdaki kaynaklara kimlerin erişebileceğini, görüntüleyebileceğini veya kullanabileceğini düzenler. Bu yetkiler, müşteri verilerinin güvenliğini sağlamanın yanı sıra **3D**EXPERIENCE Cloud platformunda elde edilebilecek müşteri uyumluluğu ve sertifika süreçlerini desteklemektedir.

ŞİFRELEME

Aktarılan veriler, bütünlüğü ve gizliliği korumak için uçtan uca bir HTTPS/TLS şifreleme protokolü kullanılarak güvence altına alınır.

YÜKSEK DÜZEY KULLANILABİLİRLİK VE ANTİ-DDOS

Tüm hizmetler, anti-DDoS (dağıtık hizmet aksatma) saldırısı ve kara liste mekanizmaları ile entegre olan yüksek kullanılabilirlik, yüksek performans, yük dengeleme proxy hizmeti ile korunmaktadır.

OPERASYONEL GÜVENLİK

BULUT OPERASYONLARIMIZ

Bulut çözümlerimiz üç katmanlı bir yapı üzerine kuruludur ve bu şekilde işletilir. Riskleri göz önünde bulundurmak ve önceliklendirmek için endüstri standartlarını kullanarak tehditleri belirleyip izler ve her katmanda riskleri azaltırız.

Hizmet Olarak Yazılım (SaaS)

En yüksek katmanda Hizmet Olarak Yazılım (SaaS) veya uygulama katmanı bulunur. Bu **3D**EXPERIENCE Cloud platformu kullanıcılarının uygulamalarına eriştiği ve kullandığı yerdir.

Hizmet Olarak Platform (PaaS)

Orta katman, Hizmet Olarak Platform (PaaS) veya platform katmanıdır. **3D**EXPERIENCE platformumuzun kurulduğu ve çalıştırıldığı yerdir. Bu katman, altyapı sağlayıcılarımızla olan ilişkimizi güvenli bir şekilde yönetmemize ve SaaS katmanımızın etkileşime girdiği veritabanlarını saklamamıza olanak tanır.

PaaS ekibimiz, **3D**EXPERIENCE Cloud platformunu oluşturan yapılandırma, işletim sistemi, yapı ve sanal kaynakları belirlemenin yanı sıra bulut altyapı sağlayıcılarımızdan nasıl bilgi aldığımızı belirler.

SaaS ve PaaS katmanlarımız için önemli risk azaltma stratejileri arasında kimlik doğrulama, rol tabanlı erişim kontrolü, şifreleme, izleme ve denetim, DAST ve SAST, ara yazılım sertleştirme, sunucu sertleştirme ve SSL/TLS kontrolleri bulunur.

Hizmet Olarak Altyapı (IaaS)

Hizmet Olarak Altyapı (IaaS) veya altyapı katmanı, bulut bilgi işlem kaynaklarımızın bulunduğu katmandır. Sanallaştırma yetenekleri sağlayıp yedeklemeleri ve Acil Durum Kurtarma Hizmetlerini sürdürür.

Bu katman, Dassault Systèmes ve müşterilerimiz için ölçeklenebilirliğin yanı sıra talep üzerine ek işlem gücü ve depolama olanağı sunar.

Birincil bulut sağlayıcılarımız, bir Dassault Systèmes Group şirketi olan 3DS Outscale ve Amazon Web Services'dir.

PAYLAŞILAN SORUMLULUK MODELİ

Bulut bilişim modelinde bulut sağlayıcıları ve bulut kullanıcıları, çevrimiçi hizmetler için en yüksek düzeyde güvenlik ve uyumluluk sağlamak üzere ortak bir sorumluluğa sahiptir. Her bir taraf bulut güvenliğinin farklı yönlerinden sorumludur:

- Bulut sağlayıcısı, bulut altyapısının güvenliğinden sorumludur.
- Platform sağlayıcısı (Dassault Systèmes); güvenlik yapılandırması, yönetimi ve işletimden sorumludur.
- Müşteri, yönetici/kiracı yönetimi de dahil olmak üzere uygulama katmanındaki güvenlikten sorumludur.
- Bulut ortamını güçlendirmek ve işletmek için en iyi güvenlik uygulamalarını, CSA (Cloud Security Alliance) ve NIST yönergelerine ek olarak bulut sağlayıcılarımızın en iyi uygulamalarına uygun olarak takip ediyoruz.

Daha fazla bilgi için lütfen Outscale En İyi Uygulamalar bölümüne bakın.

KULLANILABİLİRLİK SLA'SI (SERVICE LEVEL AGREEMENT)

Hedefimiz, çevrimiçi hizmetlerimizin (i) Planlanan Hizmet Kesintisi veya (ii) bir Müşterinin talebinin sonucu olan bir kesinti altında olmadığı zamanın en az %99,5'inde çevrimiçi hizmetlerimizin kullanılabilirliğini sağlamaktır.

Daha fazla bilgi için lütfen Çevrimiçi Hizmetler İçin Service Level Agreement'a bakın.

GÜVENLİK AÇIĞI YÖNETİMİ

Güvenlik açıklarını sürekli izleme ve azaltma önlemlerimizin kapsamında riskleri tanımlamak, analiz edip değerlendirmek ve NIST SP 800-53, ISO/IEC 27001 ve ISO/IEC 27701'e dayalı risk giderme kontrollerini seçmek için kapsamlı risk değerlendirmesi uyguluyoruz.

Güvenlik açıklarını tanımlamak, test etmek ve kontrol etmek için harici ve şirket içi sistemleri birleştiren, NIST en iyi uygulamalarına dayanan çok katmanlı bir güvenlik açığı yönetim sistemi kullanıyoruz. Güvenlik açığı yönetim sistemimizin önemli bir kısmı ağ ve güvenlik açığı tarayıcılarını kullanmamızdır. İyileştirme gerektiren bir güvenlik açığı tespit edilirse önem derecesine göre günlüğe kaydedilir ve önceliklendirilir, ardından düzeltilene kadar izlenir.

Potansiyel tehditlere karşı sürekli yeni güvenlik önlemleri eklemek için OWASP en iyi uygulamalarına dayanan kontrollere ek olarak statik kod analizi (SAST), dinamik analiz (DAST) ve yoğun manuel penetrasyon testleri kullanıyoruz.

Tehdit Algılama Yöntemleri

Tehdit algılama yöntemlerimiz şunları içerir:

Kötü Amaçlı Yazılımları Önleme

Yetkisiz yazılım kullanımını yasaklıyor ve çalışanları ekipmanın kabul edilebilir kullanımı konusunda eğitiyoruz. Kötü amaçlı kodu tanımlamak için teknik kontrollerimiz bulunur ve çalışan farkındalığı eğitimi veririz. Buna ek olarak kötü amaçlı yazılım olayı durumunda etkili ve hızlı bir yanıt sağlamak için prosedürler oluşturduk.

İzleme

Ara yazılım, ağ, işletim sistemi erişimi ve işletim sistemi dahil olmak üzere tüm bulut katmanlarında kontrol etkinliği ve güvenlik olaylarını izliyoruz. Otomatik izleme, operasyonel ve işlevsel performans hakkında gerçek zamanlı veriler sağlar.

Olay Yönetimi

Güvenlik ve gizlilik olaylarını tanımlamak, sınıflandırmak, kaydetmek ve iletmek için sistematik bir yaklaşım kullanıyoruz. Tüm olaylar, sınıflandırma ölçeğimize göre temas noktası açısından değerlendirilip yerleşik olay yönetimi ve veri ihlali süreçlerimiz aracılığıyla ele alınır.

Uygulama Katmanında Güvenlik Açığı Yönetimi

Güvenli bulut SaaS ve PaaS katmanlarını çalıştırmak, Bilgi ve İletişim Teknolojileri arasında yaygın olan güvenlik açıklarının sürekli olarak tanımlanmasını ve azaltılmasını gerektirir. Güvenli Yazılım Geliştirme Yaşam Döngüsü'nün (Secure SDLC) bir parçası olarak, yazılım güvenlik açıklarını tanımlamak ve mevcut güvenlik kontrollerimizi doğrulamak için birkaç ana önlemi entegre ettik. Bu önlemler, çeşitli geliştirme aşamalarında statik ve dinamik taramaların yanı sıra kapsamlı manuel penetrasyon testlerini içerir.

Statik Uygulama Güvenlik Testi (SAST)

SAST, kodun güvenli SDLC'nin bir sonraki aşamasına geçmesinden önce sorunları düzeltmek için geliştirme işleminde kaynak kodu otomatik olarak değerlendirir. Gartner'ın önde gelen SAST sağlayıcısı ile çalışıyoruz.

Dinamik Uygulama Güvenliği Testi (DAST)

DAST, platformu mimari zayıflıklar ve potansiyel güvenlik açıkları için ön uçtan otomatik olarak değerlendirir. DAST'ımız önde gelen endüstri güvenlik araçları kullanılarak gerçekleştirilir.

Manuel Penetrasyon Testi

Yetkili üçüncü taraf güvenlik uzmanları, güvenlik duruşlarını doğrulamak için **3D**EXPERIENCE Cloud platformuna veya belirli bir uygulama setine yönelik saldırıları manuel olarak simüle eder.

İşlevler Arası Kalite Mühendisliği Testi

Bağımsız Kalite Mühendisliği ekiplerimiz, rutin olarak tehdit senaryoları çalıştırarak güvenlik doğrulama sürecine katkıda bulunur. Kapsamlı ürün bilgisi ve temel güvenlik kavramlarına güçlü bir şekilde hakim olmaları, ekstra bir güvenlik doğrulama ve onaylama katmanı olarak hizmet eder.

Ara Katman Yazılımı, Ağ ve İşletim Sistemi Güvenlik Açığı Yönetimi

Ağımızdaki ve varlıklarımızdaki potansiyel kusurları hızlı ve verimli bir şekilde tespit etmek için Gartner'ın önde gelen güvenlik açığı tarayıcısını kullanarak internete bakan varlıkları tanımlamak üzere birden fazla güvenlik açığı kontrolü ve kimlik bilgileri taraması kullanıyoruz.

YAMA YÖNETİMİ

Fonksiyonel ve güvenlikle ilgili yamalar dahil olmak üzere yazılım güncellemelerini rutin olarak uyguluyoruz. Planlanan servis kesintileri SLA'mızda belirtildiği gibi düzenli olarak gerçekleşir. Ek olarak yama yönetimi ve olay yönetimi süreçlerimiz, zaman zaman planlanmamış hizmet kesintileri gerektiren ve saatler içinde uygulanabilen acil durum güvenlik yamalarını dikkate alır.

GÜVENLİK İZLEME VE OLAY YÖNETİMİ

Kapsamlı güvenlik izleme ve olay yönetim sistemimiz, güvenlik tehditlerini gerçek zamanlı olarak tanımlar, analiz eder ve bunlara yanıt verir. Bir yandan güvenlik açıklarını tanımlayıp düzeltmek ve güvenlik olaylarına hızlı bir şekilde yanıt vermek için iki yönlü bir yaklaşım benimsiyoruz.

Güvenlik İzleme

Günlükler ve etkinlikler SIEM (Güvenlik, Olay ve Olay Yönetimi) çözümümüz aracılığıyla merkezi olarak toplanıp analiz edilir ve özel SOC (Güvenlik Operasyonları Merkezi) ekibimiz tarafından 7/24 izlenir. SIEM platformumuz, verileri merkezi olarak toplar ve güvenlik olaylarını proaktif olarak tanımlamak için gelişmiş bir korelasyon motoru kullanır. Böylece büyük hacimli güvenlik günlüğü verilerini analiz ederek kötü amaçlı etkinlik girişimlerini tespit eder.

3DEXPERIENCE Cloud platformu denetim ve izleme hizmetimiz; işlevsellik, performans ve güvenliği izlemek için bulut katmanlarında düzinelerce gösterge içerir.

Olay Müdahale Süreçleri

SOC ekibimiz, SIEM çözümümüzün belirlediği riskleri olayın niteliğine göre sürekli olarak izler ve değerlendirir. NIST SP 800-61 yönergelerine uygun olay yönetimi prosedürümüzü takip ederek ve risk değerlendirmemize dayanarak olayları hemen ele alırız. Bu; çevreleme, yok etme, kurtarma ve bildirim gibi ana aşamaları içerir.

Yama yönetim sürecimizin bir parçası olarak, acil durum yamaları saatler içinde yapılır (bkz. Yama Yönetimi).

İŞ KURTARMA PLANLARI (BCP) VE ACİL DURUM KURTARMA PLANLARI (DRP)

İş Kurtarma planları (BCP) ve Acil Durum Kurtarma planları (DRP), herhangi bir bulut tabanlı yazılım tedariki için kritik öneme sahiptir. BCP'miz; bilgi işlem hizmetlerini, yazılım hizmetlerini, bağlantıları ve verileri bir kayıp durumunda tam işlevselliğe geri getirme planlarını ele alır. DRP'miz, büyük olaylar söz konusu olduğunda kayıpları sınırlamaya veya tersine çevirmeye yönelik prosedürleri ele alır.

BCP/DRP için aşağıdakiler de dahil olmak üzere sektördeki en iyi uygulamaları takip ediyoruz:

1. Müşteri verilerinin yedeklenmesi ve kurtarılması için tutarlı bir plan sürdürmek ve büyük bir felaket durumunda tüm plan bileşenlerinin erişilebilir olmasını sağlamak.

2. Kritik verilerin kopyalarını üretim bölgemiz dışında, birincil veri merkezimizden uzakta tutmak.

3. BCP/DRP'mizi güncel tutmak ve üretim ortamındaki değişiklikleri dikkate almak.

4. BCP/DRP'yi yıllık olarak kullanmak.

5. Minimum hizmet kesintisi sağlamak için yük dengeleme ve yük devretme sistemleri gibi sanallaştırma özelliklerinden yararlanmak.

Müşterilerimizin tüm senaryolarda iş sürekliliğini sağlamak için agresif bir Kurtarma Süresi Hedefi (RTO) ve Kurtarma Noktası Hedefi (RPO) doğrultusunda çalışıyoruz.

Veri Yedekleme ve Alma

Service Level Agreement'ımıza uygun olarak, SLA'ya göre tutulan müşteri ve kullanıcı verilerinin günlük yedeklemelerini sağlıyoruz. Veri korumasını en üst düzeye çıkarırken arıza süresini en aza indirmek için sürekli sıcak ve soğuk yedeklemeler gerçekleştiriyoruz.

3DEXPERIENCE Cloud platformu müşteri verileri, SLA'da belirtildiği gibi belirli bir süre boyunca alınabilir.

Daha fazla bilgi için lütfen Çevrimiçi Hizmetler İçin Service Level Agreement'ımıza bakın.

VERİ KORUMASI VE GİZLİLİK

Bulut çözümlerimiz, müşterilerimizin ve kullanıcılarımızın gizliliğine saygı duyarak oluşturulmuştur. Tüm PII'lerin güvenli bir şekilde depolanmasını ve işlenmesini sağlamak için 2016/679 Avrupa Genel Veri Koruma Yönetmeliği (GDPR) gibi ilgili yasa ve standartlara uygun olarak yüksek standartları takip ediyoruz.

Denetleyici

GDPR'de tanımlandığı üzere denetleyicilerin; depolama saklama süresinin belirlenmesi, PII'nin en aza indirilmesine uyum ve veri sahiplerinin talepleriyle ilgilenmek de dahil olmak üzere kişisel verilerin işlenmesine ilişkin politika ve prosedürleri belirlemeleri gerekir. Dassault Systèmes, şirket içi iş süreçleri ve bilgi sistemleriyle ilgili PII'yi işlerken denetleyici rolünü üstlenir.

Dassault Systèmes SaaS çözümlerinin müşterisi, çözümde tutulan PII'nin ele alınmasından sorumludur ve bu nedenle denetleyici rolünde hareket eder.

GDPR ve diğer veri koruma yasaları, gizlilik haklarını genişleterek ve bireylere PII'leri üzerinde kontrol sağlayarak sakinlerinin temel haklarını güçlendirmeyi amaçlamaktadır. Küresel bir şirket olarak Dassault Systèmes, GDPR'ye ve Dassault Systèmes'in işini yürüttüğü diğer veri koruma yasalarına uyum sağlar. GDPR ve diğer ülkeye özgü yasalar için 3ds.com adresinde bulunan Dassault Systèmes Gizlilik Politikasında referans sağlanmıştır.

3DEXPERIENCE Cloud platformu için Dassault Systèmes, aşağıdakilerle ilgili olarak denetleyici rolünü üstlenir:

- Özel bulut teklifleri hariç **3D** Passport
- 3ds.com aracılığıyla bir kişi tarafından oluşturulan **3D** Passport
- Dassault Systèmes genel platformlarında mevcut **3D**EXPERIENCE genel toplulukları
- Dassault Systèmes Müşteri Desteği
- **3D**EXPERIENCE Marketplace

GDPR'ye ek olarak diğer yerel veri koruma yasaları ve düzenlemeleri, bölgesel tabanlı Dassault Systèmes Veri Koruma Görevlileri tarafından izlenip yerel süreçler ve prosedürler tarafından uygulanır.

3D Passport, kullanıcı başına oluşturulan kimlik doğrulama profilidir. **3D** Passport dahilinde PII'nin işlenmesi Dassault Systèmes'in sorumluluğundadır. **3D** Passport ile ilişkili PII, yasal gereklilikler nedeniyle bazı özel istisnalar dışında Avrupa'da saklanır.

İşleyen

Dassault Systèmes, **3D**EXPERIENCE Cloud platformu gibi bulut tabanlı teklifler sunduğunda işlenmesi ve saklanması istenen PII için bir işleyen olarak hareket eder. Dassault Systèmes, PII'yi taraflar arasında imzalanan sözleşmeye göre işler.

Dassault Systèmes, GDPR'de tanımlandığı üzere aşağıdakiler için işlemci rolünde hareket eder:

- Müşterilere ve iş ortaklarına sağlanan Dassault Systèmes Bulut teklifleri (özel ve herkese açık)
- Özel Bulut teklifleri için **3D** Passport

İşleyen olarak hareket ederken, platform verileri bir üçüncü taraf IaaS sağlayıcısı (örneğin, 3DS Outscale veya Amazon Web Services) tarafından yerel bir veri merkezinde depolanır.

SONUÇ

Dassault Systèmes, güvenlik ve gizliliği operasyonlarının merkezinde konumlandırır. Siber güvenlik ve veri koruma önlemlerimiz en saygın endüstri standartlarına dayanmaktadır. Ayrıca eğitim, tasarım gereksinimleri, güvenlik kontrolleri, gizlilik önlemleri ve üçüncü taraf denetimleri ve testleri yoluyla sistematik olarak uygulanmaktadır. Güvenlik ve gizlilik önlemlerimizi yenilik ve mükemmellik ruhu içinde sürekli olarak geliştirerek müşterilerimizi mümkün olan en iyi şekilde destekliyoruz.

3DEXPERIENCE® platformumuz marka uygulamalarımızı desteklemekte, 11 sektöre hizmet vermekte ve zengin bir endüstri çözümü deneyimleri portföyü sunmaktadır.

3DEXPERIENCE Şirketi Dassault Systèmes, insani ilerlemeyi hızlandıran ve kolaylaştıran bir aracıdır. İşletmelere ve kişilere, sürdürülebilir yenilikler hayal etmeleri için iş birliğine dayalı sanal ortamlar sunmaktayız. Müşterilerimiz **3D**EXPERIENCE platformumuz ve uygulamalarımızla gerçek dünyanın "sanal deneyim ikizlerini" oluşturarak yenilik, öğrenme ve üretimin sınırlarını zorlar.

Dassault Systèmes'in 20.000 çalışanı, 140'tan fazla ülkede tüm sektörlerde her ölçekteki 270.000'den fazla müşteriye değer katar. Daha fazla bilgi için **www.3ds.com/tr-tr** adresini ziyaret edin.

3DEXPERIENCE®

DASSAULT SYSTEMES | The **3D**EXPERIENCE® Company

Avrupa/Orta Doğu/Afrika
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

Kuzey ve Güney Amerika
Dassault Systèmes
175 Wyman Street
Waltham, MA 02451
USA

Asya/Pasifik
Dassault Systèmes K.K.
ThinkPark Tower,
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Japan