DASSAULT SYSTEMES

PLATE-FORME 3DEXPERIENCE SÉCURITÉ DU CLOUD ET CONFIDENTIALITÉ

Livre blanc

TABLE DES MATIÈRES

INTRODUCTION

NOTRE PHILOSOPHIE

Le cloud computing représente un changement de paradigme dans la façon dont nous travaillons. Les entreprises exécutent des applications, gèrent des données et transfèrent leurs opérations vers le cloud pour tirer parti de la rapidité et de la simplicité du déploiement cloud. Elles bénéficient également de l'efficacité opérationnelle de fournisseurs spécialisés en matière de maintenance, de services informatiques et de sécurité.

Dassault Systèmes fournit des services basés sur le cloud depuis la création de la plate-forme **3D**EXPERIENCE® en 2012. Nous avons créé un écosystème complet basé sur le cloud, la plate-forme **3D**EXPERIENCE sur le cloud, qui permet à nos clients de bénéficier de ressources cloud sécurisées, flexibles et évolutives. Nous nous sommes donné pour mission d'aider nos clients en leur faisant confiance et en leur garantissant la fiabilité de tous les aspects de nos solutions.

Notre approche de la gestion des risques est à la fois polyvalente et proactive, basée sur les meilleures pratiques et conçue pour anticiper les menaces de sécurité dans l'ensemble de nos opérations. Nous utilisons un système de gestion de la sécurité et de la confidentialité des informations (ISPMS) certifié ISO/IEC 27001:2017 et ISO/IEC 27701:2019 et soumis à des audits de routine. Notre ISPMS repose sur les valeurs fondamentales de confidentialité, d'intégrité, de disponibilité et de responsabilité.

Ce livre blanc décrit l'approche de Dassault Systèmes en matière de sécurité et de conformité pour **3D**EXPERIENCE, notre plate-forme basée sur le cloud, qui permet aux clients d'accéder à des applications, à un stockage des données et à des ressources informatiques évolutives. Dans ce livre blanc, nous allons aborder les principaux aspects de nos pratiques en matière de sécurité, de confidentialité et de conformité dans le cloud.

NOTRE ÉNONCÉ DE MISSION SUR LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES INFORMATIONS

L'Énoncé de mission de Dassault Systèmes en matière de sécurité et de confidentialité des informations est le suivant[1] :

Gérer l'exposition aux risques liés à la sécurité des informations et protéger les informations personnelles identifiables (PII) pour le logiciel en tant que service (SaaS) de la plate-forme **3D**EXPERIENCE, et améliorer en permanence la confidentialité, l'intégrité et la disponibilité des informations ainsi que la protection des éléments suivants :

- Propriété intellectuelle et données utilisateur du client, informations personnelles identifiables incluses
- Réputation et propriété intellectuelle de Dassault Systèmes
- Disponibilité et résilience du Cloud
- Conformité aux réglementations et normes en vigueur en matière de cybersécurité et de protection des données

Cet énoncé de mission est disponible pour nos collaborateurs sous forme d'informations documentées et pour les parties intéressées sur demande.

AVIS DE NON-RESPONSABILITÉ

Ce contenu représente les pratiques de sécurité, de confidentialité, de qualité et de conformité de la plate-forme **3D**EXPERIENCE sur le cloud en mars 2022. Le contenu de nos pratiques énoncé dans les présentes est susceptible d'être modifié à la seule discrétion de Dassault Systèmes. Les termes « Nous » et « Notre » utilisés dans ce document font spécifiquement référence à Dassault Systèmes.

1. Cela correspond à la politique ISO 27001 relative à la sécurité et à la confidentialité des informations.

DASSAULT SYSTÈMES : UNE ORGANISATION AXÉE SUR LA SÉCURITÉ ET LA CONFIDENTIALITÉ

CYBERSÉCURITÉ ET GOUVERNANCE DE LA CONFIDENTIALITÉ DU SAAS DE LA PLATE-FORME 3DEXPERIENCE

Dassault Systèmes R&D exploite un système de gestion de la confidentialité et de la sécurité des informations (ISPMS) contrôlé de manière centralisée pour le SaaS de la plate-forme **3D**EXPERIENCE, certifié ISO/IEC 27001:2017 et ISO/IEC 27701:2019 par SGS International Certification Services (SGS-ICS). Le champ d'application de la certification comprend :

1. La conception, le développement, la livraison, le déploiement, les opérations cloud et la prise en charge du SaaS de la plate-forme **3D**EXPERIENCE.

2. La gestion de la confidentialité des données lorsque Dassault Systèmes agit en tant que :

a. responsable du traitement des données à caractère personnel fournies dans le cadre du SaaS de la plate-forme **3D**EXPERIENCE.

b. sous-traitant des PII sous le contrôle d'un client et traitées dans le SaaS de la plate-forme **3D**EXPERIENCE.

Notre ISPMS est administré et soumis à l'examen de la direction par le Comité exécutif R&D de Dassault Systèmes. Il repose sur un système de gestion de la qualité (QMS) bien établi, géré sur la plate-forme **3D**EXPERIENCE et certifié ISO 9001:2015 par SGS-ICS.

Le QMS et l'ISPMS partagent de nombreux processus fondamentaux et de support reposant sur une méthodologie de cycle de développement sécurisé des logiciels (SDLC sécurisé). L'ISPMS inclut également des processus supplémentaires reposant sur les risques, axés sur la sécurité des informations et la protection des données.

La conformité et l'efficacité de tous les processus et contrôles de l'ISPMS sont continuellement évaluées par le programme d'audit de conformité de **3D**EXPERIENCE de Dassault Systèmes R&D. Les actions correctives et les améliorations continues qui en résultent sont suivies dans la plate-forme **3D**EXPERIENCE.

Les critères d'audit reposent sur le système de gestion et les exigences de contrôle des normes ISO 9001, ISO 27001 et ISO 27701. Tous les contrôles des normes ISO 27001 Annexe A et ISO 27701 Annexe A et B sont inclus dans le champ d'application du système de gestion, car Dassault Systèmes agit à la fois en tant que responsable du traitement des PII et sous-traitant des PII (voir Protection et confidentialité des données, p.11).

L'ISPMS est soutenu par l'énoncé de mission en matière de sécurité et de confidentialité des informations (Énoncé de politique) et les objectifs annuels de la plate-forme **3D**EXPERIENCE. Les objectifs sont mesurables et fournissent des indicateurs clés de performance (KPI) surveillés par les équipes opérationnelles. Les objectifs en matière de cybersécurité et de protection des données sont régulièrement examinés pour vérifier leur adéquation dans le cadre du processus de planification annuelle de Dassault Systèmes.

NOTRE PERSONNEL EN CHARGE DE LA SÉCURITÉ, DE LA CONFIDENTIALITÉ ET DE LA CONFORMITÉ

Comité exécutif R&D

Le Comité exécutif R&D de Dassault Systèmes est en dernier ressort responsable de l'efficacité du système de gestion de la sécurité et de la confidentialité des informations (ISPMS) de **3D**EXPERIENCE avec le soutien de l'avocat-conseil de Dassault Systèmes pour les exigences en matière de protection des données et de confidentialité. Le Comité exécutif R&D démontre activement son engagement envers l'ISPMS et les attentes des clients par divers moyens, notamment :

- en s'assurant que la politique de sécurité et de confidentialité des informations et les objectifs annuels sont compatibles avec l'orientation stratégique de l'entreprise ;
- en assurant l'intégration des exigences de l'ISPMS dans les processus métier de l'entreprise ;
- en s'assurant que les ressources nécessaires à l'ISPMS sont disponibles ;
- en communiquant l'importance de l'ISPMS ;
- en s'assurant que l'ISPMS atteint les résultats escomptés ;
- en dirigeant et soutenant les personnes pour contribuer à l'efficacité de l'ISPMS ;
- en promouvant l'amélioration continue des processus et des opérations de L'ISPMS.

Équipes de cybersécurité, de confidentialité des données et de conformité

Dassault Systèmes gère un modèle de rôle d'entreprise qui définit la mission, la description, les livrables, les KPI, le profil de rôle et les compétences associées à chaque poste ou rôle.

Une équipe de responsables de la sécurité des systèmes d'information (CISO) et de responsables de la sécurité est chargée de la mise en œuvre du programme de sécurité des informations de Dassault Systèmes. Elle est chargée d'établir, de maintenir et d'appliquer les politiques, normes, directives et procédures de sécurité des informations à l'échelle mondiale.

Les services Cybersécurité et Confidentialité des données de Dassault Systèmes R&D sont responsables de la planification, de la mise en œuvre, de la maintenance et de l'amélioration continue de l'ISPMS de **3D**EXPERIENCE, conformément aux exigences des normes ISO 27001 et ISO 27701. Ils sont chargés de surveiller la conformité et l'efficacité de l'ISPMS et de faire des rapports à ce sujet à la direction dans le cadre des réunions de gouvernance standard.

Un délégué à la protection des données du groupe (DPO) informe et conseille Dassault Systèmes sur la protection des informations personnelles identifiables afin de garantir les meilleures pratiques ainsi que la responsabilité et la croissance durable de Dassault Systèmes. Le DPO du Groupe est l'interlocuteur privilégié des autorités de contrôle de la protection des données et rend compte de la conformité et de l'efficacité de l'ISPMS à l'avocat-conseil de Dassault Systèmes.

Une équipe R&D Conformité et Risque gère un programme d'audit de conformité interne pour évaluer la conformité de Dassault Systèmes aux processus internes et aux certifications du secteur telles que ISO 9001, ISO 27001 et ISO 27701. Les résultats de l'audit et les plans d'action corrective et préventive (CAPA) correspondants sont gérés dans la plate-forme.

Une équipe d'audit interne du groupe définit et évalue la conformité et l'efficacité du cadre d'évaluation du contrôle interne (ICE) de Dassault Systèmes par le biais d'un programme d'audit interne à l'échelle de l'entreprise. Le cadre de contrôle interne permet d'atténuer les risques en établissant et en vérifiant les contrôles généraux et les contrôles généraux des technologies de l'information (ITGC).

INTÉGRATION ET FORMATION POUR TOUS LES EMPLOYÉS

Les collaborateurs qui rejoignent Dassault Systèmes doivent accepter de respecter notre code de conduite, notre charte informatique et nos politiques de protection des données. Tous les nouveaux collaborateurs suivent une formation obligatoire sur l'éthique et la conformité en matière de sécurité et de confidentialité, qui couvre notamment :

- La prévention des menaces pour la sécurité des données.
- La sécurisation des données physiques et des postes de travail ; la politique de rangement du bureau.
- La protection et la confidentialité des données personnelles.
- La conduite éthique des affaires ; les principes de lutte contre la corruption et de droit de la concurrence.
- La gestion des incidents ; l'identification et le signalement des menaces potentielles.

Nous promouvons en permanence la sensibilisation à la sécurité et à la confidentialité dans l'ensemble de l'entreprise.

SÉCURITÉ DANS LE TÉLÉTRAVAIL

Lorsqu'ils travaillent à distance, les collaborateurs de Dassault Systèmes peuvent accéder à leurs données, applications et utilitaires de plate-forme uniquement via un VPN. Cela s'applique aussi bien aux appareils professionnels qu'aux appareils personnels. Seuls les appareils personnels enregistrés et approuvés disposant d'un accès VPN sont autorisés.

NOS PARTENAIRES EN MATIÈRE DE SÉCURITÉ DANS LE CLOUD

Nous travaillons en étroite collaboration avec nos fournisseurs d'infrastructure cloud (IaaS), notamment 3DS Outscale, pour garantir la sécurité et la conformité de nos opérations. Nous exigeons de nos fournisseurs IaaS qu'ils soient certifiés ISO 27001, entre autres critères.

NOS NORMES DE SÉCURITÉ

Notre approche de la cybersécurité repose sur les normes les plus respectées du secteur. Des experts indépendants en cybersécurité collaborent activement pour établir des normes mondiales pour les fournisseurs de logiciels. L'OWASP, le NIST et l'ISO/IEC sont trois organismes d'experts qui guident nos équipes de cybersécurité et de confidentialité à travers les meilleures pratiques, exigences, contrôles, tests et autres outils de réduction des risques et d'atténuation des vulnérabilités.

OWASP : PROJET OUVERT DE SÉCURITÉ DES APPLICATIONS WEB[1]

L'OWASP a pour objectif de permettre aux organisations de développer et de maintenir des applications hautement sécurisées. La fondation OWASP est la principale source de recherche de pointe, de cadres prédominants et d'informations essentielles relatives à la sécurité des applications.

Avec l'aide d'alliances mondiales, l'OWASP fournit :

- Des outils, normes et méthodologies de sécurité des applications
- Des ressources pour le développement de code sécurisé, des examens de code de sécurité et des tests de sécurité des applications
- Des bibliothèques et contrôles de sécurité standard

Les principales publications de l'OWASP comprennent :

- Les 10 principaux risques liés à la sécurité des applications Web
- Les pratiques de codage sécurisé
- Le guide de révision du code
- La norme de vérification de la sécurité des applications

NIST : NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY[2]

Le NIST est la principale source de solutions de mesures critiques et de normes équitables en matière d'électronique, de logiciels et d'autres technologies. La publication spéciale (SP) 800-53 du NIST définit les contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations.

La norme SP 800-53 du NIST est conçue pour protéger les opérations et les actifs de l'entreprise, les individus et d'autres entités contre « un ensemble diversifié de menaces et de risques, y compris les attaques hostiles, les erreurs humaines, les catastrophes naturelles, les défaillances structurelles, les entités de renseignement étrangères et les risques en matière de confidentialité ». Ces contrôles abordent la sécurité et la confidentialité du point de vue des fonctionnalités et de l'assurance.

ISO/IEC : ORGANISATION INTERNATIONALE DE NORMALISATION ET COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE[3]

L'ISO/IEC est un comité technique conjoint qui s'efforce de promouvoir les normes en matière de technologies informatiques et de la communication. Notre ISPMS pour la plate-forme **3D**EXPERIENCE est certifié ISO/IEC 27001:2017 et ISO/IEC 27701:2019, tandis que notre QMS est certifié ISO 9001:2015, tous deux par SGS-ICS (voir la section Cybersécurité et gouvernance de la confidentialité du Saas de la plate-forme **3D**EXPERIENCE, p. 4).

La norme ISO 9001 spécifie les exigences d'un système de gestion de la qualité lorsqu'une organisation :

a. doit démontrer sa capacité à fournir constamment des produits et services répondant aux exigences du client ainsi qu'aux exigences légales et réglementaires, et

b. vise à améliorer la satisfaction des clients grâce à l'application efficace du système, y compris des processus d'amélioration du système et de l'assurance de la conformité aux exigences du client ainsi qu'aux exigences légales et réglementaires applicables.

Notre système de gestion de la qualité (QMS) est ancré dans les processus utilisés pour la conception, le développement, la livraison, le déploiement, les opérations cloud et la prise en charge de la plate-forme **3D**EXPERIENCE. Bon nombre de nos pratiques de sécurité des applications sont intégrées à notre système de gestion de la qualité.

La norme ISO/IEC 27001 spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la maintenance et à l'amélioration continue d'un système de gestion de la sécurité des informations (ISMS). L'annexe A de la norme ISO/IEC 27001 expose les contrôles attendus pour tout ce qui va de la sécurisation des services applicatifs sur les réseaux publics à la protection des transactions de sécurité des applications, en passant par l'application d'une politique de développement sécurisée, la restriction des modifications apportées aux packages logiciels, l'application des principes d'ingénierie des systèmes sécurisés, etc.

La norme ISO/IEC 27701 spécifie les exigences et fournit des directives pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue d'un système de gestion des informations de confidentialité (PIMS) sous la forme d'une extension des normes ISO/IEC 27001 et ISO/IEC 27002 pour la gestion de la confidentialité dans le contexte de l'organisation. Cette norme fournit des conseils aux responsables du traitement et aux sous-traitants qui assument la responsabilité du traitement des PII. L'annexe A spécifie les objectifs et les contrôles pour les responsables du traitement des PII et l'Annexe B spécifie les objectifs et contrôles pour les sous-traitants des PII.

1. Pour en savoir plus : www.owasp.org
2. Pour en savoir plus : csrc.nist.gov
3. Pour en savoir plus : iso.org/isoiec-27001-information-security

FONCTIONS DE SÉCURITÉ CLÉS

AUTHENTIFICATION ET AUTORISATION

Le mécanisme d'authentification et d'autorisation de la plate-forme **3D**EXPERIENCE sur le cloud est le **3D** Passport, un identifiant de connexion personnalisé qui permet aux utilisateurs d'accéder en toute sécurité à tous leurs rôles, applications et services. Les administrateurs appliquent des politiques d'authentification utilisateur comme la force ou l'expiration des mots de passe, et configurent des répétitions pour détecter les tentatives de déverrouillage de mots de passe utilisant la force brute.

Fonctionnalités du 3D Passport

Confidentialité des données

Chaque utilisateur de nos solutions en ligne a accès à la politique de confidentialité de Dassault Systèmes et est tenu de l'accepter lors de la création de son **3D** Passport. Les utilisateurs peuvent exercer leurs droits conformément aux politiques et processus de Dassault Systèmes en soumettant une demande via un formulaire en ligne.

Une entreprise peut, en outre, présenter aux utilisateurs sa propre politique de confidentialité à accepter. Dans ce cas, l'administrateur de la plate-forme téléchargera sa propre Politique de confidentialité par le biais du tableau de bord Platform Management (Gestion de la plate-forme).

Authentification unique (SSO)

En échangeant les données d'authentification et d'autorisation dans un format standard, le **3D** Passport fournit une expérience d'identification transparente sur l'ensemble des applications de la plate-forme **3D**EXPERIENCE sur le cloud.

Authentification multifactorielle (MFA)

Un niveau de sécurité supérieur peut être atteint grâce à l'exploitation des fonctionnalités MFA sur la plate-forme. Par exemple, une fois l'authentification à facteurs multiples configurée, l'utilisateur peut se servir d'une application mobile pour générer un code à saisir en plus du mot de passe afin d'accroître la sécurité.

CONTRÔLE D'ACCÈS

Le contrôle d'accès détermine qui peut accéder aux ressources, les afficher ou les utiliser dans notre environnement de cloud computing. Ces autorisations permettent de sécuriser les données clients, ainsi que de prendre en charge les processus de conformité et de certification client réalisables au sein de la plate-forme **3D**EXPERIENCE sur le cloud.

CHIFFREMENT

Les données en transit sont sécurisées à l'aide d'un protocole de chiffrement HTTPS/TLS de bout en bout pour protéger leur intégrité et leur confidentialité.

HAUTE DISPONIBILITÉ ET ANTI-DDOS

Tous les services sont protégés par un service de proxy d'équilibrage de charge haute disponibilité et hautes performances qui s'intègre aux mécanismes de liste noire et anti-DDoS (déni de service distribué).

SÉCURITÉ OPÉRATIONNELLE

NOTRE ACTIVITÉ CLOUD

Nos solutions sur le cloud sont conçues et exploitées sur une structure à trois couches. Nous identifions et surveillons les menaces et nous les atténuons sur chaque couche en utilisant les normes du secteur pour prendre en compte et hiérarchiser les risques.

Logiciel en tant que service (SaaS)

La couche la plus élevée est la couche logicielle en tant que service (SaaS) ou couche applicative. C'est là que les utilisateurs de la plate-forme **3D**EXPERIENCE sur le cloud accèdent à leurs applications et les utilisent.

Plate-forme en tant que service (PaaS)

La couche intermédiaire est la couche PaaS (plate-forme en tant que service) ou la couche plate-forme. C'est là que la plate-forme **3D**EXPERIENCE est construite et exploitée. Cette couche nous permet de gérer en toute sécurité nos relations avec nos fournisseurs d'infrastructure et de stocker les bases de données avec lesquelles notre couche SaaS interagit.

Notre équipe PaaS détermine la configuration, le système d'exploitation, la structure et les ressources virtuelles qui composent la plate-forme **3D**EXPERIENCE sur le cloud et détermine la façon dont nous recevons les informations de nos fournisseurs d'infrastructure cloud.

Les stratégies d'atténuation des risques critiques pour nos couches SaaS et PaaS comprennent l'authentification, le contrôle d'accès basé sur les rôles, le chiffrement, la surveillance et l'audit, les DAST et SAST, le renforcement du middleware, le renforcement du serveur et la vérification SSL/TLS.

Infrastructure en tant que service (IaaS)

L'infrastructure en tant que service (IaaS) ou la couche d'infrastructure est l'emplacement où se trouvent nos ressources de cloud computing. Elles offrent des fonctions de virtualisation et assurent la maintenance des sauvegardes et des services de reprise après sinistre.

Cette couche offre une évolutivité à Dassault Systèmes et à nos clients, avec une puissance de traitement et un stockage supplémentaires disponibles à la demande.

Nos principaux fournisseurs de cloud sont 3DS Outscale, une société du groupe Dassault Systèmes, et Amazon Web Services.

LE MODÈLE DE RESPONSABILITÉ PARTAGÉE

Dans un modèle de cloud computing, les fournisseurs et les utilisateurs du cloud ont la responsabilité partagée d'assurer le plus haut niveau de sécurité et de conformité pour les services en ligne. Chaque partie est responsable des différents aspects de la sécurité du cloud :

- Le fournisseur du cloud est responsable de la sécurité de l'infrastructure cloud.
- Le fournisseur de plate-forme (Dassault Systèmes) est responsable de la configuration, de la gestion et du fonctionnement de la sécurité.
- Le client est responsable de la sécurité au niveau de la couche applicative, notamment de la gestion administrateur/locataire.
- Nous suivons les meilleures pratiques en matière de sécurité pour renforcer et exploiter l'environnement cloud, conformément aux meilleures pratiques de nos fournisseurs de cloud, en plus des directives de la CSA (Cloud Security Alliance) et du NIST.

Pour plus d'informations, reportez-vous aux meilleures pratiques d'Outscale.

SLA (ACCORD DE NIVEAU DE SERVICE) DE DISPONIBILITÉ

Notre objectif est de garantir la disponibilité de nos services en ligne pendant au moins 99,5 % du temps au cours duquel les services en ligne ne sont pas soumis à (i) une interruption de service planifiée ou (ii) une interruption résultant de la demande du client.

Pour plus d'informations, veuillez consulter notre Contrat de niveau de service pour les services en ligne.

GESTION DES VULNÉRABILITÉS

Dans le cadre de nos mesures de surveillance et d'atténuation continues des vulnérabilités, nous appliquons une évaluation complète des risques pour identifier, analyser et évaluer les risques et sélectionner des contrôles de traitement des risques basés sur les normes NIST SP 800-53, ISO/IEC 27001 et ISO/IEC 27701.

Nous utilisons un système de gestion des vulnérabilités multicouche reposant sur les meilleures pratiques du NIST, combinant des systèmes externes et internes pour identifier, tester et contrôler les vulnérabilités. Notre utilisation des scanneurs de réseau et de vulnérabilité représente une part importante de notre système de gestion des vulnérabilités. Si une vulnérabilité devant être corrigée est identifiée, elle est consignée et hiérarchisée en fonction de sa gravité, puis suivie jusqu'à ce qu'elle soit corrigée.

Nous utilisons des tests d'analyse de code statique (SAST), des tests d'analyse dynamique (DAST) ainsi que des tests de pénétration manuels intensifs en plus de contrôles reposant sur les meilleures pratiques de l'OWASP pour ajouter en permanence de nouvelles mesures de sécurité contre les menaces potentielles.

Méthodes de détection des menaces

Nos méthodes de détection des menaces comprennent les éléments suivants :

Prévention des programmes malveillants

Nous interdisons l'utilisation de logiciels non autorisés et formons nos collaborateurs à l'utilisation acceptable de l'équipement. Nous avons mis en place des contrôles techniques pour identifier les programmes malveillants et nous menons une formation de sensibilisation des collaborateurs. En outre, nous avons mis en place des procédures pour garantir une réponse efficace et rapide en cas d'incident lié à un programme malveillant.

Surveillance

Nous surveillons l'efficacité des contrôles et les événements de sécurité sur toutes les couches du cloud, y compris le middleware, le réseau, l'accès au système d'exploitation et le système d'exploitation. La surveillance automatisée fournit des données en temps réel sur les performances opérationnelles et fonctionnelles.

Gestion des incidents

Nous utilisons une approche systématique pour identifier, classer, enregistrer et communiquer les incidents de sécurité et de confidentialité. Tous les incidents sont évalués par le point de contact en fonction de notre échelle de classification et traités par le biais de nos processus établis de gestion des incidents et de violation des données.

Gestion des vulnérabilités de la couche applicative

L'exécution de SaaS et PaaS sécurisés dans le cloud nécessite une identification et une atténuation continues des vulnérabilités, communes aux technologies de l'information et de la communication. Dans le cadre de notre cycle de développement sécurisé des logiciels (SDLC sécurisé), nous avons intégré plusieurs mesures clés pour identifier les vulnérabilités logicielles et valider nos contrôles de sécurité existants. Ces mesures comprennent des analyses statiques et dynamiques à différentes étapes du développement, ainsi que des tests de pénétration manuels approfondis.

Tests de sécurité des applications statiques (SAST)

Les SAST évaluent automatiquement le code source pendant le processus de développement afin de résoudre les problèmes avant que le code ne passe à la phase suivante du SDLC sécurisé. Nous travaillons avec un fournisseur de SAST leader auprès de Gartner.

Tests de sécurité des applications dynamiques (DAST)

Les DAST évaluent automatiquement la plate-forme via le front-end pour détecter les faiblesses architecturales et les vulnérabilités de sécurité potentielles. Nos DAST sont réalisés à l'aide d'outils de sécurité de pointe.

Test de pénétration manuel

Des professionnels de la sécurité tiers autorisés simulent manuellement des attaques sur la plate-forme **3D**EXPERIENCE sur le cloud ou sur un ensemble spécifique d'applications pour confirmer leur stratégie de sécurité.

Tests d'ingénierie de la qualité interfonctionnelle

Nos équipes d'ingénierie de la qualité indépendantes contribuent au processus de vérification de la sécurité en exécutant régulièrement des scénarios de menaces. Leur connaissance approfondie des produits et leur maîtrise rigoureuse des concepts clés de la sécurité constituent une couche supplémentaire de vérification et de validation de la sécurité.

Middleware, réseau et gestion des vulnérabilités du système d'exploitation

Nous utilisons plusieurs contrôles de vulnérabilité et des analyses accrédités pour identifier les ressources Internet, à l'aide d'un scanneur de vulnérabilité leader auprès de Gartner pour identifier rapidement et efficacement les défauts potentiels de notre réseau et de nos ressources.

GESTION DES CORRECTIFS

Nous appliquons régulièrement des mises à jour logicielles, y compris des correctifs fonctionnels et de sécurité. Des interruptions de service planifiées se produisent régulièrement, comme indiqué dans notre SLA. En outre, nos processus de gestion des correctifs et des incidents tiennent compte des correctifs de sécurité d'urgence qui peuvent être appliqués en quelques heures, ce qui entraîne parfois des interruptions de service imprévues.

SURVEILLANCE DE LA SÉCURITÉ ET GESTION DES INCIDENTS

Notre système complet de surveillance de la sécurité et de gestion des incidents identifie les menaces de sécurité, les analyse et y répond en temps réel. Nous adoptons une approche en deux volets pour identifier et corriger les vulnérabilités et pour réagir rapidement aux incidents de sécurité.

Surveillance de la sécurité

Les journaux et les événements sont collectés et analysés de manière centralisée via notre solution SIEM (Security, Incident and Event Management) et surveillés 24 h sur 24 et 7 j sur 7 par notre centre des opérations de sécurité (SOC) dédié. Notre plate-forme SIEM collecte les données de manière centralisée et utilise un moteur de corrélation avancé pour identifier de manière proactive les événements relatifs à la sécurité, en analysant d'importants volumes de données de journaux de sécurité pour identifier les tentatives d'activité malveillante.

Notre service de surveillance et de supervision de la plate-forme **3D**EXPERIENCE sur le cloud comprend des dizaines d'indicateurs sur les couches cloud pour surveiller les fonctionnalités, les performances et la sécurité.

Processus de réponse aux incidents

Notre équipe SOC surveille et évalue en permanence les risques identifiés par notre solution SIEM en fonction de la nature des incidents. Nous traitons immédiatement les incidents sur la base de notre évaluation des risques, en suivant notre procédure de gestion des incidents conformément aux directives SP 800-61 du NIST. Celle-ci comprend les principales phases de confinement, d'éradication, de récupération et de notification.

Dans le cadre de notre processus de gestion des correctifs, les correctifs d'urgence sont effectués en quelques heures (voir Gestion des correctifs).

PLANS DE REPRISE D'ACTIVITÉ (BCP) ET PLANS DE REPRISE APRÈS INCIDENT (DRP)

Les plans de reprise d'activité (BCP) et les plans de reprise après incident (DRP) sont essentiels à toute mise à disposition de logiciels basés sur le cloud. Notre plan de reprise d'activité vise à restaurer les services informatiques, les services logiciels, les connexions et les données à leur pleine fonctionnalité en cas de perte de données. Notre DRP traite des procédures visant à limiter ou à annuler les pertes en cas d'événements majeurs.

Nous suivons les meilleures pratiques du secteur en matière de BCP/DRP, notamment :

1. Maintenir un plan cohérent pour la sauvegarde et la restauration des données clients et s'assurer que tous les composants du plan sont accessibles en cas de sinistre majeur.

2. Conserver des copies des données critiques en dehors de notre région de production, à l'écart de notre datacenter principal.

3. Maintenir notre BCP/DRP à jour et nous assurer qu'il prend en compte les changements dans l'environnement de production.

4. Exercer notre BCP/DRP tous les ans.

5. Tirer parti des fonctions de virtualisation, telles que les systèmes d'équilibrage de charge et de basculement, pour limiter au maximum les interruptions de service.

Nous visons une durée maximale d'interruption admissible (RTO) et une perte de données maximale admissible (RPO) ambitieuses afin d'assurer la continuité des activités de nos clients dans tous les scénarios.

Sauvegarde et récupération des données

Conformément à notre Contrat de niveau de service, nous garantissons des sauvegardes quotidiennes des données des clients et des utilisateurs, qui sont conservées conformément au SLA. Nous effectuons continuellement des sauvegardes à chaud et à froid afin de limiter les interruptions de service tout en optimisant la protection des données.

Les données clients de la plate-forme **3D**EXPERIENCE sur le cloud restent disponibles pour être récupérées pendant une période définie, comme spécifié dans le SLA.

Pour plus d'informations, veuillez consulter notre Contrat de niveau de service pour les services en ligne.

PROTECTION ET CONFIDENTIALITÉ DES DONNÉES

Nos solutions cloud sont conçues dans le respect de la confidentialité de nos clients et utilisateurs. Nous respectons des normes strictes pour nous assurer que toutes les PII sont stockées et traitées en toute sécurité, conformément aux lois et normes pertinentes telles que le Règlement général européen sur la protection des données 2016/679 (RGPD).

Responsable du traitement

Les responsables du traitement, tels que définis dans le RGPD, doivent déterminer les politiques et procédures de traitement des données personnelles, y compris la durée de conservation du stockage, la conformité à la minimisation des PII et le traitement des demandes des personnes concernées. Dassault Systèmes agit en tant que responsable du traitement lors du traitement des PII liées à ses processus métiers internes et à ses systèmes d'information.

Un client des solutions SaaS de Dassault Systèmes est responsable de la gestion des PII conservées dans la solution et agit donc en tant que responsable du traitement.

Le RGPD et d'autres lois sur la protection des données visent à renforcer les droits fondamentaux des résidents de leur législation en élargissant les droits sur la confidentialité et en donnant aux individus le contrôle sur leurs PII. En tant qu'entreprise internationale, Dassault Systèmes se conforme au RGPD, ainsi qu'aux autres lois sur la protection des données dans les législations où Dassault Systèmes exerce ses activités. Le RGPD et les autres lois spécifiques à chaque pays sont référencés dans la politique de confidentialité de Dassault Systèmes disponible sur 3ds.com.

Pour la plate-forme **3D**EXPERIENCE sur le cloud, Dassault Systèmes joue le rôle de responsable du traitement des éléments suivants :

- **3D** Passport, à l'exception des offres de cloud privé
- **3D** Passport créé par une personne via 3ds.com
- Communautés publiques **3D**EXPERIENCE disponibles sur les plates-formes publiques de Dassault Systèmes
- Support client de Dassault Systèmes
- **3D**EXPERIENCE Marketplace

Outre le RGPD, d'autres lois et réglementations locales sur la protection des données sont contrôlées par les responsables régionaux de la protection des données de Dassault Systèmes et sont appliquées par le biais de procédures et processus locaux.

Le **3D** Passport est le profil d'authentification créé pour un utilisateur. Le traitement des PII dans un **3D** Passport est sous la responsabilité de Dassault Systèmes. Les PII associées au **3D** Passport sont stockées en Europe, avec quelques exceptions spécifiques en raison d'exigences réglementaires.

Sous-traitant

Lorsque Dassault Systèmes propose des offres basées sur le cloud, telles que la plate-forme **3D**EXPERIENCE sur le cloud, Dassault Systèmes agit en tant que sous-traitant des PII dont on lui a confié le traitement et le stockage. À cette fin, Dassault Systèmes traite les PII conformément à l'accord contractuel signé entre les parties.

Dassault Systèmes agit en tant que sous-traitant, tel que défini dans le RGPD, pour les éléments suivants :

- Offres cloud de Dassault Systèmes (privées et publiques) fournies aux clients et partenaires commerciaux
- **3D** Passport pour les offres de Cloud privé

Lorsque Dassault Systèmes agit en tant que sous-traitant, les données de la plate-forme seront stockées par un fournisseur IaaS tiers (par exemple, 3DS Outscale ou Amazon Web Services), dans un centre de données local.

CONCLUSION

Dassault Systèmes place la sécurité et la confidentialité au cœur de ses opérations. Nos mesures de cybersécurité et de protection des données reposent sur les normes les plus fiables du secteur et sont systématiquement appliquées par le biais de formations, d'exigences de conception, de contrôles de sécurité, de mesures de confidentialité ainsi que d'audits et de tests tiers. Nous améliorons continuellement nos mesures de sécurité et de confidentialité dans un esprit d'innovation et d'excellence, en nous assurant de soutenir nos clients de la meilleure façon possible.

Au service de 11 industries, la plate-forme **3D**EXPERIENCE® dynamise nos applications de marque et propose une vaste gamme de solutions industrielles.

Dassault Systèmes, l'entreprise de la **3D**EXPERIENCE, est un « accélérateur de progrès humain ». Elle propose aux entreprises et aux particuliers des environnements virtuels collaboratifs qui leur permettent d'imaginer des innovations plus durables. En développant un jumeau virtuel du monde réel, grâce à la plateforme **3D**EXPERIENCE et à ses applications, Dassault Systèmes donne à ses clients les moyens de repousser les limites de l'innovation, de l'apprentissage et de la production.

Les 20 000 collaborateurs de Dassault Systèmes travaillent à créer de la valeur pour nos 270 000 clients de toutes tailles, dans toutes les industries, dans plus de 140 pays. Pour plus d'informations, visitez notre site **www.3ds.com/fr.**

3DEXPERIENCE®

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

Europe/Moyen-Orient/Afrique
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

Amériques
Dassault Systèmes
175 Wyman Street
Waltham, MA 02451
Etats-Unis

Asie-Pacifique
Dassault Systèmes K.K.
ThinkPark Tower,
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Japon