Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada

T: +1 514.332.4000

Communiqué de presse

Le *Cyber Resilience Act* européen relève le niveau d'exigence pour les fournisseurs de technologies de sécurité physique

Genetec liste cinq questions que les responsables de la sécurité devraient poser à leur fournisseur pour évaluer la sécurité des produits, la transparence et la prise en charge tout au long du cycle de vie.

Londres, le 9 septembre 2026 — Genetec Inc. ("Genetec"), le leader mondial des logiciels de sécurité physique d'entreprise, publie aujourd'hui des recommandations pour aider les responsables de la sécurité physique à évaluer la manière dont les fournisseurs de technologies conçoivent, maintiennent et assurent le support des produits connectés, alors que le règlement européen sur la cyber-résilience (*Cyber Resilience Act*, ou CRA) renforce les exigences de cybersécurité tout au long du cycle de vie des produits.

Le CRA définit des exigences de cybersécurité pour les produits comportant des éléments numériques et commercialisés dans l'Union européenne. Il accorde une plus grande importance au développement de produits sécurisés, à la gestion des vulnérabilités, à la transparence en matière de cybersécurité et à la continuité du support tout au long du cycle de vie des produits. Bien qu'il s'applique principalement aux fabricants, ce règlement aura également des répercussions sur les organisations qui distribuent, installent, achètent et exploitent des appareils connectés.

« *Le règlement sur la cyber-résilience conforte bon nombre des principes de sécurité dès la conception et de gestion du cycle de vie que Genetec défend depuis des années* », déclare Mathieu Chevalier, architecte principal de sécurité chez Genetec Inc. « *En relevant le niveau d'exigence en matière de sécurité des produits et de transparence, le CRA offre aux acheteurs une base claire pour évaluer les fournisseurs de technologies et la cyber-résilience de leurs produits à long terme.* »

Avec l'entrée en application, le 11 septembre, des obligations de signalement des vulnérabilités prévues par le CRA, les organisations s'appuieront de plus en plus sur les fournisseurs de technologies pour répondre aux nouvelles exigences de cybersécurité et de traitement des

vulnérabilités. Pour évaluer le niveau de préparation des fournisseurs qu'elles envisagent de retenir, Genetec encourage les organisations à leur poser cinq questions clés :

Pendant combien de temps le produit bénéficiera-t-il de mises à jour de sécurité et d'un support ?

Le CRA souligne l'importance de maintenir la sécurité d'un produit tout au long de son cycle de vie. Les responsables de la sécurité doivent savoir pendant combien de temps le fournisseur proposera des mises à jour, comment il traitera les vulnérabilités et quel accompagnement il offrira lorsque les produits arriveront en fin de vie. Le CRA impose aux fabricants de fournir des mises à jour de sécurité et d'assurer le traitement des vulnérabilités pendant au moins cinq ans. Le support à long terme constitue donc un critère important dans l'évaluation des produits.

La cybersécurité a-t-elle été intégrée au produit dès sa conception ?

Les principes de sécurité dès la conception (*Secured by Design*) et de sécurité par défaut (*Secure by Default*) sont au cœur du CRA. Demandez au fournisseur d'expliquer comment il intègre la cybersécurité à la conception, au développement et aux tests de ses produits, ainsi qu'à toutes les étapes de leur cycle de vie.

Comment le fournisseur identifie-t-il, divulgue-t-il et traite-t-il les vulnérabilités ?

Aucun logiciel n'est à l'abri des vulnérabilités. La manière dont un fournisseur y répond est un indicateur fort de son engagement en matière de cybersécurité. Recherchez un programme de gestion des vulnérabilités bien établi, comprenant des tests de sécurité réguliers, une politique de divulgation des vulnérabilités coordonnée, des mesures correctives basées sur les risques et appliquées sans retard injustifié, une distribution sécurisée des mises à jour de sécurité et des avis clairs sur les vulnérabilités corrigées.

Le fournisseur fait-il preuve de transparence sur ses propres pratiques de cybersécurité ?

La cybersécurité est une responsabilité partagée. Les fournisseurs responsables expliquent comment ils développent, testent et maintiennent leurs produits, et donnent aux clients et aux intégrateurs des consignes claires pour les déployer de manière sécurisée. Demandez au fournisseur comment il teste et réévalue

régulièrement la sécurité de ses produits, communique sur les vulnérabilités et les mises à jour de sécurité, et fournit des recommandations de renforcement de la sécurité des systèmes.

Comment le fournisseur vous aidera-t-il à maintenir votre cyber-résilience sur le long terme ?

La cybersécurité d'un produit ne s'arrête pas à son installation. Il est essentiel de collaborer avec des partenaires technologiques de confiance. Les organisations doivent évaluer la manière dont le fournisseur détermine et communique la durée de support du produit, traite les vulnérabilités, fournit les mises à jour de sécurité, assure un fonctionnement sécurisé du produit et gère sa fin de vie. Elles doivent également lui demander quels éléments il peut fournir pour démontrer que le produit respecte les exigences de cybersécurité applicables tout au long de son cycle de vie.

« *Les organisations les mieux préparées à gérer les cybermenaces de demain abordent la cybersécurité comme un partenariat continu, et non comme une décision d'achat ponctuelle* », conclut Mathieu Chevalier. « *Le CRA contribue à renforcer cette approche en définissant des exigences communes en matière de transparence, de gestion rigoureuse des vulnérabilités et de support des produits à long terme, au bénéfice des fabricants, des intégrateurs et des organisations qui dépendent de systèmes de sécurité physique connectés.* »

Depuis plus de 25 ans, Genetec applique des pratiques de développement cybersécurisé à ses technologies de sécurité physique. L'entreprise développe des solutions reposant sur une architecture ouverte et place la cybersécurité au cœur de leur conception, intégrant le chiffrement, la gestion des identités et des accès, la surveillance continue et la gestion des vulnérabilités, ainsi que des recommandations pour aider les clients à préserver la résilience de leurs systèmes dans la durée.

Pour plus d'informations sur les bonnes pratiques de cybersécurité appliquées aux systèmes de sécurité physique, rendez-vous sur https://www.genetec.com/fr/confiance-cybersecurite

--fin--

À propos de Genetec

Genetec Inc. est une entreprise technologique internationale qui transforme le secteur de la sécurité physique depuis plus de 25 ans. Le portefeuille de solutions de la société permet aux entreprises, aux gouvernements et aux communautés du monde entier de sécuriser les personnes et les biens, tout en améliorant l'efficacité opérationnelle et en garantissant le respect de la vie privée.

Genetec fournit les meilleurs produits au monde pour la gestion vidéo, le contrôle d'accès et la RAPI, tous basés sur une architecture ouverte et conçus avec la cybersécurité au cœur de leur développement. Le portefeuille de la société comprend également des solutions de détection d'intrusion, d'interphonie et de gestion des preuves numériques.

Genetec, dont le siège social est situé à Montréal, au Canada, compte plus de 42 500 clients, qu'elle accompagne via un vaste réseau de partenaires distributeurs et de consultants certifiés dans plus de 159 pays.

Pour plus d'informations sur Genetec, rendez-vous sur : www.genetec.com/fr

Contact presse :

Royaume-Uni
Anna Short
Phoenix Communications
genetec@phoenix-comms.co.uk
+44 (0) 774 791 7235