CYBERSÉCURITÉ CONFORME SRI2

CYCLE DE VIE DU DEVELOPPEMENT DE LA SECURITE (SECURE DEVELOPMENT LIFE CYCLE)

Honeywell a mis en place un processus rigoureux de sécurisation de ses produits de la conception au développement, ainsi que de réponse aux vulnérabilités potentielles des produits existants. Ce processus, le Cycle de développement logiciel sécurisé, ou 'Secure Software Development Lifecycle' (SSDLC), a été développé il y a quelques années et est en constante évolution afin de devenir de plus en plus robuste.

Honeywell prend la sécurité de ses produits très au sérieux. Nos produits sont soumis à une série de tentatives d'intrusion solide et exhaustive. Dans certains cas, des essais complémentaires sont effectués par des instances indépendantes. Les critères appliqués pendant ces essais complémentaires, ainsi que les produits ou solutions concernés sont des données propriétaires sauvegardées scrupuleusement.

Notre Cycle de vie du développemnt de la sécurité (Secure Development Life Cycle, SDLC) solide et exhaustif. Il a été défini sur la base des meilleures pratiques et normes en vigueur dans l'industrie, telles que:

- Évaluation des risques de sécurité (Security Risk Assessment) sur la base de menaces émanant de l'environnement auquel un produit ou solution est confronté, ainsi que des caractéristiques techniques et des besoins clients
- Exigences (Security Requirements) et contrôles de sécurité émanant des normes et directives reconnues dans l'industrie, telles que BSIMM, ISA:CEI 99/62443, ISO 27001, PCI DSS, RGPD, OWASP, de lois et réglementations locales et d'autres éléments en fonction du produit, l'offre et les risques de sécurité encourus
- Evaluations d'impact sur la vie privée (Privacy Impact Assessments)
- Modélisation des menaces (Threat Modeling)
- Normes et pratiques de codage sécurisé, telles que Secure by Design (sécurisé dès la conception), Privacy by Design (protection de la vie privée dès la conception) et Secure Coding (codage sécurisé)
- Tests de sécurité des applications statiques (SAST), également connus sous le nom d'Analyse du code source, pour appliquer des pratiques de conception et de codage sécurisées. Nous recherchons les vulnérabilités de sécurité incluses dans le rapport OWASP Top 10 sur les vulnérabilités des applications Web et dans le rapport des 25 erreurs logicielles les plus dangereuses selon l'institut SANS - SANS Top 25, ainsi dans la liste d'indicateurs de qualité spécifiques à la langue. Les outils SAST actuels incluent l'analyse de code statique (SonarQube) et l'analyse d'analyse de couverture de code statique (Coverity) en fonction des besoins du produit et du langage
- Analyse binaire pour identifier l'utilisation de logiciels open source et les vulnérabilités potentielles
- Politique formelle de gestion des risques qui nécessite des calendriers d'atténuation spécifiques en fonction du degré de risque
- Examen de la cybersécurité et approbation par la haute direction avant expédition du produit
- Support du cycle de vie des produits et notification aux clients des mises à jour de sécurité

L'équipe d'audit d'Honeywell effectue des audits pour s'assurer que les tâches de sécurité requises par les processus du Cycle de vie du développement de la sécurité ont été accomplies.

Honeywell organise des formations pour ses employés au sujet du processus de sécurité de l'entreprise et des problèmes et solutions spécifiques en matière de cybersécurité.

Tous les ingénieurs IT chez Honeywell sont formés sur le Cycle de vie de développement sécurisé et des problèmes de cybersécurité et de sécurité des produits.

DIRECTIVE NIS2 (SRI2), NETWORK AND INFORMATION SECURITY DIRECTIVE 2

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures visant à atteindre un niveau commun élevé de cybersécurité dans l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972 et abrogeant la directive (UE) 2016/1148 (directive NIS2)

Les exigences de l'UE en matière de cybersécurité introduites en 2016 dans le cadre de la directive SRI (NIS) ont été mises à jour et renforcées par la directive SRI2 (NIS2), entrée en vigueur en 2023. À la lumière d'une numérisation accrue, la croissance des cyberattaques et un paysage global des menaces de cybersécurité en évolution, l'UE a introduit davantage de mesures de surveillance plus strictes pour garantir la capacité de réponse aux incidents et des exigences d'application plus fortes en les étendant à de nouveaux secteurs et entités.

D'ici le 17 octobre 2024, tous les États membres de l'UE doivent adopter et publier les mesures nécessaires pour se conformer à la directive SRI2 (NIS2) et commencer à appliquer ces mesures à partir du 18 octobre 2024.

Honeywell

POLITIQUE DE REPORTING SUR LA CYBERSECURITE D'HONEYWELL

L'objectif de notre équipe Réponse aux incidents de sécurité des produits (Product Security Incident Response Team, PSIRT) est de limiter les risques liés aux vulnérabilités pour nos clients en fournissant en temps opportun des informations, conseils et mesures correctives sur les vulnérabilités de nos logiciels et applications, matériel et appareils, services et solutions en temps et en heure. Cette équipe gère la réception, l'enquête, la coordination interne, la correction et la divulgation des vulnérabilités des solutions Honeywell.

L'équipe PSIRT coordonne la réponse et la divulgation de toutes les vulnérabilités des produits identifiées en externe.

SIGNALER UN RISQUE POTENTIEL DE SÉCURITÉ

Nous acceptons les signalements de chercheurs indépendants, d'organisations industrielles, de fournisseurs et de clients intéressés par la sécurité des produits. Pour plus d'informations sur le signalement d'une vulnérabilité potentielle, visitez la page Web de Signalement de vulnérabilité (Vulnerability Reporting) à l'adresse https://www.honeywell.com/us/en/product-security#vulnerability-reporting

DIVULGATION COORDONNÉE DES VULNÉRABILITÉS (CVD)

Chez Honeywell, nous suivons un processus de Divulgation coordonnée des risques de sécurité potentiels (CVD). Il permet aux déclarants indépendants qui découvrent une vulnérabilité de contacter Honeywell directement, ce qui nous donne la possibilité d'enquêter sur la vulnérabilité et la corriger avant que le déclarant ne divulgue l'information publiquement.

L'équipe PSIRT coordonne les activités du déclarant tout au long de l'enquête de vulnérabilité et, le cas échéant, fournit des mises à jour sur l'avancement. PSIRT peut reconnaître le déclarant pour avoir trouvé une vulnérabilité de produit valide et signalé le problème en privé et, avec l'autorisation du déclarant, peut inclure ces informations dans l'onglet « Remerciements » sur son site Web. Une fois qu'Honeywell a publié une mise à jour ou une correction, le déclarant peut discuter publiquement de la vulnérabilité.

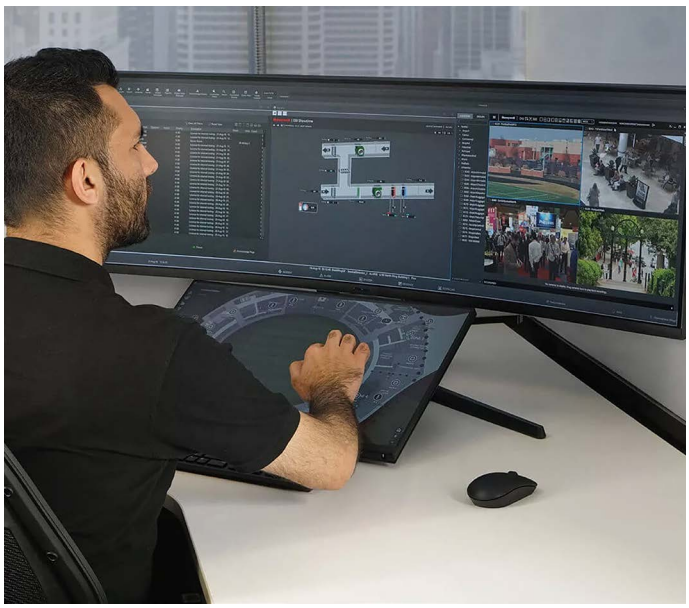
Suivre le processus CVD nous permet de protéger nos clients tout en coordonnant la divulgation publique et de reconnaître correctement les déclarants pour les menaces signalées. Si la vulnérabilité signalée affecte le produit d'un fournisseur, la PSIRT en informe directement le fournisseur concerné, se coordonne avec le déclarant ou engage un centre de coordination externe.

Pour plus d'informations :
https://www.honeywell.com/us/en/product-security

SOLUTIONS VIDÉOSURVEILLANCE, CONTRÔLE D'ACCÈS ET ANTI-INTRUSION

Le portefeuille produits d'Honeywell propose des fonctionnalités qui peuvent aider les entreprises à renforcer la cybersécurité et leur conformité à la directive SRI2 (NIS2), telles que:

- La sécurisation optimale grâce aux coprocesseurs cryptographiques
- Chipsets de chiffrement FIPS/TPM certifiés intégrés
- Types de cryptage : TLS 1.2, AES 128/256 bits, chiffrement de bout en bout OSDP v2, cryptage point à point du flux vidéo pour une protection périmétrique
- Connexion Ethernet cryptée & toutes les communications cryptées (HTTPS) avec les clients Web et mobiles
- Authentification multifacteur et biométrie pour la sécurité informatique, des données et des salles techniques
- Rapportage d'audit et conformité
- Contrôle d'accès en mode transparent
- Traçabilité des ressources informatiques



Honeywell Commercial Security
Building 5, Carlton Park
King Edward Avenue, Narborough,
Leicester LE19 0LF
Tel: +44(0)1163500714
Honeywell.com

Pour plus d'informations
hwll.co/securityuk
https://buildings.honeywell.com

HCS-FY-NIS2-A4-FR-short-28aug2024

Honeywell
COMMERCIAL SECURITY