CIBERSEGURIDAD CUMPLE CON NIS2

PROCESO DE DESARROLLO DE PRODUCTOS SEGURO

Honeywell ha desarrollado un sistema integral que incorpora la seguridad desde la etapa inicial de la concepción de un producto y durante todo su desarrollo, además de abordar posibles vulnerabilidades en productos existentes. Este sistema, conocido como la iniciativa "Secure Development Life Cycle" (SDLC) de Honeywell, se ha vuelto aún más robusto en los últimos años.

Honeywell se compromete con la seguridad de los productos. Nuestros productos pasan por pruebas exhaustivas y rigurosas. Y en determinados casos, se realizan pruebas de seguridad adicionales independientes. Los criterios para estas pruebas adicionales, así como los productos u ofertas específicos seleccionados, son información confidencial y propia. El "Secure Development Life Cycle" (SDLC) representa un proceso sólido e integral basado en las mejores prácticas y estándares de la industria que incluye lo siguiente:

- Evaluación de Riesgos de Seguridad basado en el entorno de amenazas al que se enfrenta un producto u oferta en particular, así como en las características técnicas y las necesidades del cliente.
- Requisitos de Seguridad y controles de seguridad basados en estándares y directrices de la industria tales como BSIMM, ISA/IEC 99/62443, ISO 27001, PCI DSS, GDPR, OWASP, leyes y regulaciones locales aplicables, entre otros, dependiendo del producto o la oferta y la Evaluación de Riesgos de Seguridad.
- Evaluaciones de Impacto en la Privacidad.
- Análisis de amenzas.
- Estándares y prácticas de "Seguro por Diseño", "Privacidad por Diseño" y codificación segura.
- Pruebas de Seguridad de Aplicaciones Estáticas (SAST, también conocidas como escaneo de código fuente) para imponer prácticas de diseño y codificación seguros. Realizamos escaneos en búsqueda de vulnerabilidades del OWASP Top 10 y SANS Top 25, así como de medidas de calidad específicas del idioma. Las herramientas SAST actuales incluyen SonarQube y Coverity dependiendo de las necesidades del producto y el idioma.
- Escaneo binario para identificar el uso de código abierto y posibles vulnerabilidades.
- Una Política de Gestión de Riesgos formal que requiere plazos específicos de mitigación basados en la severidad.
- Revisión y aprobación de ciberseguridad por parte de la alta dirección antes del lanzamiento del producto.
- Soporte durante el ciclo de vida del producto y notificación al cliente de actualizaciones de seguridad.

Un equipo de auditoría de Honeywell realiza verificaciones para asegurar que se cumplen los requisitos de seguridad incluidos en el proceso "Secure Development Life Cycle" (SDLC) de Honeywell.

Honeywell realiza programas de formación para sus empleados sobre el proceso de seguridad de la empresa y sobre preocupaciones y soluciones específicas de ciberseguridad.

Todos los ingenieros de software en Honeywell reciben formaciones sobre el "SDLC" y sobre temas generales de ciberseguridad y seguridad de productos.

DIRECTIVA DE SEGURIDAD DE REDES Y SISTEMAS DE INFORMACIÓN 2 (NIS2)

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre las medidas para un alto nivel común de ciberseguridad en toda la Unión, que modifica el Reglamento (UE) Nº 910/2014 y la Directiva (UE) 2018/1972, y deroga la Directiva (UE) 2016/1148.

Las normas de ciberseguridad de la UE introducidas en 2016 por la Directiva NIS fueron actualizadas y reforzadas por la Directiva NIS2, que entró en vigor en 2023. Debido al aumento de la digitalización, los crecientes ciberataques y un panorama general de amenazas de ciberseguridad en aumento, la UE ha introducido medidas de supervisión más estrictas con capacidad de respuesta a incidentes y requisitos de cumplimiento más rigurosos, ampliándolos a nuevos sectores y entidades.

El 17 de octubre de 2024, todos los países miembros de la UE deben adoptar y publicar las medidas necesarias para cumplir con la Directiva NIS2 y deberán aplicar dichas medidas a partir del 18 de octubre de 2024.

Honeywell

POLÍTICA DE INFORMES DE CIBERSEGURIDAD DE HONEYWELL

El objetivo de nuestro Equipo de Respuesta a Incidentes de Seguridad de Productos (PSIRT) es minimizar el riesgo de los clientes asociado con las vulnerabilidades de seguridad, proporcionando información oportuna, orientación y solución de las vulnerabilidades en nuestros productos, incluyendo software, aplicaciones, hardware, dispositivos, servicios y soluciones. Este equipo gestiona la recepción, investigación, coordinación interna, solución y divulgación de la información sobre vulnerabilidades de seguridad relacionadas con los productos de Honeywell.

El PSIRT coordina la respuesta y divulgación de todas las vulnerabilidades de productos identificadas externamente.

CÓMO INFORMAR SOBRE UNA POTENCIAL VULNERABILIDAD DE SEGURIDAD

Estamos abiertos a recibir informes de investigadores independientes, organizaciones de la industria, proveedores y clientes preocupados por la seguridad de los productos. Para obtener más información sobre cómo informar de una posible vulnerabilidad, visite la página web sobre cómo reportar una vulnerabilidad en https://www.honeywell.com/us/en/product-security#vulnerabilityreporting

PROCESO DE DIVULGACIÓN COORDINADA DE VULNERABILIDADES

Este proceso permite que las fuentes de información independientes que descubran una vulnerabilidad se pongan en contacto directamente con Honeywell y nos den la oportunidad de investigar y remediar la vulnerabilidad antes de que el informante divulgue la información al público.

El PSIRT (Equipo de Respuesta a Incidentes de Seguridad de Productos) coordinará con el informante durante toda la investigación de la vulnerabilidad y le proporcionará actualizaciones sobre el progreso según corresponda. Con su consentimiento, el PSIRT puede reconocer al informante en nuestros agradecimientos por encontrar una vulnerabilidad válida en el producto y reportar el problema de manera privada. Después de que Honeywell publique una actualización o información de mitigación, el informante podrá discutir públicamente la vulnerabilidad.

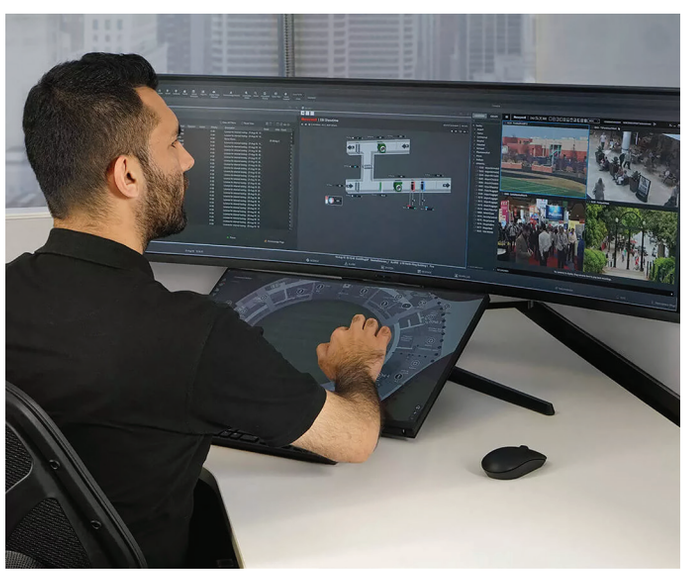
Seguir el Proceso de Divulagción de Vulnaverabilidades nos permite proteger a nuestros clientes y, al mismo tiempo, coordinar las divulgaciones públicas y reconocer adecuadamente al informante por su hallazgo. Si una vulnerabilidad reportada involucra un producto de un proveedor, el PSIRT notificará directamente al proveedor, coordinará con el informante o involucrará a un centro de coordinación de terceros.

Para más información, por favor consulte: https://www.honeywell.com/us/en/product-security

SOLUCIONES DE VIDEO, ACCESOS E INTRUSIÓN DE HONEYWELL COMMERCIAL SECURITY

Las diferentes gamas de productos de Honeywell Commercial Security ofrecen múltiples características y funcionalidades que pueden ayudar a las organizaciones a mejorar su ciberseguridad y facilitar el cumplimiento con la Directiva NIS2, tales como:

- Máxima seguridad gracias a coprocesadores criptográficos
- Chipsets de cifrado integrados con certificación FIPS/TPM
- Tipos de cifrado: TLS 1.2, AES 128/256 bits, cifrado punto a punto con OSDP v2, cifrado punto a punto del flujo de vídeo para protección perimetral
- Conexión Ethernet cifrada y comunicaciones cifradas (HTTPS) con clientes web y App móviles
- Autenticación multifactor y biometría para seguridad de TI, salas técnicas y de almacenamiento de datos
- Informes de auditoría y cumplimiento
- Lectores de control de accesos en modo transparente
- Trazabilidad de activos de TI



Para más información
hwll.co/securityes
https://buildings.honeywell.com

Honeywell Commercial Security
Calle María de Portugal 3-5
28050 - Madrid
España
Tel: +34 902 667 800
Honeywell.com

HBA-SEC-NIS2-FLY-ES-ES-V2-July24-C

Honeywell
COMMERCIAL SECURITY