NIS2 COMPLIANT CYBER SECURITY

SECURE DEVELOPMENT LIFE CYCLE PROCESS

Honeywell has developed a robust system for considering security at the outset of product conception and during development, as well as responding to potential vulnerabilities in existing products. This system, Honeywell's Secure Software Development Lifecycle (SSDLC) initiative, has evolved and grown even more robust over the past few years.

Honeywell takes product security seriously. Our products go through a robust and comprehensive penetration testing regimen. In some cases, additional independent security testing is conducted. The criteria for this additional testing as well as which products or offerings are selected for this are closely held proprietary information.

We have a robust and comprehensive Secure Development Life Cycle (SDLC) based on best practices and industry standards that includes the following:

- Security Risk Assessment based on the threat environment faced by a particular product or offering as well as the technical features and customer needs
- Security Requirements and security controls based on industry standards and guidelines such as BSIMM, ISA/IEC 99/62443, ISO 27001, PCI DSS, GDPR, OWASP, applicable local laws and regulations, and others depending on the product or offering and the Security Risk Assessment
- Privacy Impact Assessments
- Threat Modeling
- Secure by Design, Privacy by Design and Secure Coding standards and practices
- Static Application Security Testing (SAST, also known as source code scanning) to enforce secure design and coding practices. We scan for OWASP Top 10 and SANS Top 25 vulnerabilities as well as for language-specific quality measures. Current SAST tools include SonarQube and Coverity depending on product and language needs.
- Binary scanning to identify open source usage and potential vulnerabilities.
- A formal Risk Management Policy that requires specific mitigation timelines based on severity
- Review and approval of cybersecurity by senior leadership prior to product shipment
- Lifecycle support and customer notification for security updates.

An audit team of Honeywell performs checks to ensure that security deliverables required under Honeywell's Secure Development Life Cycle processes are completed.

Honeywell completes training programs for its employees on the company's security process and on specific cybersecurity concerns and solutions.

All software engineers in Honeywell receive formal training on the Secure Development Life Cycle process and general cyber/product security topics.

NETWORK AND INFORMATION SECURITY DIRECTIVE 2 (NIS2)

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)

The EU cybersecurity requirements introduced in 2016 by NIS Directive were updated and strengthened by the NIS2 Directive that came into force in 2023. In the light of increased digitalization with growing cyber-attacks and an evolving overall cybersecurity threat landscape, EU has introduced more stringent supervisory measures with incident response capacities and stricter enforcement requirements by expanding them to new sectors and entities.

By 17 October 2024, all EU member countries must adopt and publish the measures necessary to comply with the NIS2 Directive and they shall apply those measures from 18 October 2024.

Honeywell

HONEYWELL CYBERSECURITY REPORTING POLICY

The goal of our Product Security Incident Response Team (PSIRT) is to minimize customers' risk associated with security vulnerabilities by providing timely information, guidance and remediation of vulnerabilities in our products, including software and applications, hardware and devices, services and solutions. This team manages the receipt, investigation, internal coordination, remediation and disclosure of security vulnerability information related to Honeywell products.

PSIRT coordinates the response and disclosure of all externally identified product vulnerabilities.

REPORTING A POTENTIAL SECURITY VULNERABILITY

We welcome reports from independent researchers, industry organizations, vendors and customers concerned with product security. To find out more information on how to report a potential vulnerability, please visit the Vulnerability Reporting webpage at https://www.honeywell.com/us/en/product-security#vulnerability-reporting

COORDINATED VULNERABILITY DISCLOSURE (CVD)

We strive to follow Coordinated Vulnerability Disclosure (CVD). This process allows independent reporters who discover a vulnerability contact Honeywell directly and allow us the opportunity to investigate and remediate the vulnerability before the reporter discloses the information to the public.

The PSIRT will coordinate with the reporter throughout the vulnerability investigation and will provide them with updates on progress as appropriate. With their agreement, the PSIRT may recognize the reporter on our acknowledgments for finding a valid product vulnerability and privately reporting the issue. After an update or mitigation information is publicly released by Honeywell, the reporter is welcome to discuss the vulnerability publicly.

Following the CVD allows us to protect our customers and at the same time coordinate public disclosures and appropriately acknowledge the reporter for their finding. If a reported vulnerability involves a vendor product, the PSIRT will notify the vendor directly, coordinate with the reporter or engage a third-party coordination center.

Please refer to https://www.honeywell.com/us/en/product-security for further information.

KEY CYBERSECURE COMMERCIAL SECURITY OFFERINGS

PRO-WATCH® ECOSYSTEM

INTEGRATED SECURITY PLATFORM

- Highest security thanks to cryptographic co-processor
- TLS 1.2 encryption
- Point to point encryption with OSDPv2
- Dual authentication and Biometrics
- Audit and compliance reporting
- Transparent mode access control
- Traceability of IT assets

MB-SECURE PRO ECOSYSTEM*

MB-SECURE PRO, ACS PRO, WINMAG INTEGRATED INTRUSION AND ACCESS CONTROL

- Highest security thanks to cryptographic co-processor
- AES 128-bit encryption
- Encrypted Ethernet connection
- TLS 1.2 encryption and 2-fold authentication
- IT room security with dual authentication

MAXPRO® CLOUD ECOSYSTEM

INCLUDING MAXPRO® ACCESS & MAXPRO® INTRUSION INTEGRATED VIDEO, INTRUSION AND ACCESS CONTROL

- Software as a Service (SaaS) managed by Azure
- All data encrypted with TLS1.2 AES256 bit between host and server
- 2-factor authentication
- Point to point encryption with OSDP V2
- Audit and compliance recording
- Dual authentication for data rooms (card + pin)

VIDEO SURVEILLANCE

35, 60 AND 70 SERIES IP CAMERAS 35 SERIES AND MAXPRO® NVRS

- Highest security thanks to cryptographic co-processor
- Built-in FIPS/TPM certificated encryption chipsets
- All encrypted communications (HTTPS) with Web and Mobile Clients
- Point to point encryption of the video stream for perimeter protection

**Currently available in DACH & Eastern Europe and soon in other European countries.*

For more information
hwll.co/securityuk
https://buildings.honeywell.com

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

HCS-FY-NIS2-A4-UK-31may2024

Honeywell
COMMERCIAL SECURITY