NIS2 Compliant Cyber Security

SECURE DEVELOPMENT LIFE CYCLE PROCESS

LenelS2 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, LenelS2's Secure Software Development Lifecycle (SSDLC) initiative, has evolved and grown even more robust over the past few years.

LenelS2 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 LenelS2 performs checks to ensure that security deliverables required under LenelS2's Secure Development Life Cycle processes are completed.

LenelS2 completes training programs for its employees on the company's security process and on specific cybersecurity concerns and solutions.

All software engineers in LenelS2 receive formal training on the Secure Development Life Cycle process and general cyber/product security topics.

The LenelS2 Professional Services Team offers comprehensive solutions to help customers identify and mitigate risks, supporting business continuity and readiness for NIS2 compliance. For more information about our service offerings, please contact the LenelS2 Services team at services.lenel.com or contact your local Sales Representative.

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. There is an 18 months enforcement deadline after the transposition deadline of 17 October 2024.

LenelS2 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 LenelS2 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 LenelS2 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 LenelS2, 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.

NIS2 COMPLIANT CYBER SECURITY

Elements™ Cloud-based Access Control Solution

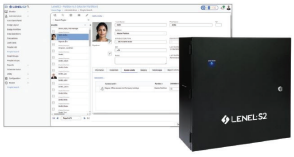
- Continuously updated, dynamically scalable, software as a service built on the Microsoft Azure platform
- Encrypted communication from browser through reader (TLS 1.2+, OSDP/SC)
- Multi-factor authentication and single sign-on support via OIDC (OpenID Connect)
- Sync people and groups with identity providers via SCIM (System for Cross-domain Identity Management)
- Lockdown profiles with configurable override access
- Role-based access control with option to disable integrator access

OnGuard® Cloud

- Single tenant, software as a service built in Amazon Web Services (AWS)
  - Leverages the power and security of both the OnGuard system and AWS
- Secure IKEv2 tunnel for connectivity between customer and cloud. Supports up to AES 256 encryption.
- Support for TLS 1.2+ when connecting to the OnGuard system through web console or AppStream
- Multi-factor authentication and single sign-on support via OIDC (OpenID Connect)
- Full system redundancy

OnGuard® Access Control System

- MS SQL server transparent data encryption with service principal authentication support
- Multi-factor authentication and single sign-on support via OIDC (OpenID Connect)
- UI and API capabilities for controller user credentials and certificate rotation
- Fully customizable industry standard password policies for OnGuard users
- Encrypted communication from browser through reader (TLS 1.2+, OSDP/SC)
- Digitally signed files via CA-issued certificate backed by Azure HSM



NetBox™ Access Control System

- Manufactured as an appliance and network devices, with no end-user access to operating system
- Multi-factor authentication and single sign-on support via OIDC (OpenID Connect) and Cisco Duo
- Encrypted communication from browser through reader (TLS 1.2+, OSDP/SC)
- Fully customizable industry standard password policies
- Role based control of operator and administrator functions
- Encryption of credential information stored on LenelS2 Network Nodes

LENEL·S2

LenelS2.com

(866) 788-5095

Specifications subject to change without notice.