Cybersecurity Assessment Service

Optimize Your Organization's Cybersecurity Posture

Cybersecurity threats continue to evolve and grow

LenelS2 works hand in hand with businesses across a variety of industries to systematically identify and remediate existing cybersecurity vulnerabilities while also strengthening businesses' cybersecurity posture against potential future threats by leveraging leading-edge standards and technologies.

Using contemporary cybersecurity frameworks and tools, **the LenelS2 Cybersecurity Assessment** reveals actionable vulnerabilities across your physical access control system's operational and network implementation and provides you with the tools and guidance to address those vulnerabilities. The impact of the LenelS2 Cybersecurity Assessment is enhanced by the use of the Honeywell Cyber Insights monitoring software, which proactively monitors your entire system for new areas of vulnerability.

The Problem:

Cybersecurity risks and exposure

Existing Vulnerabilities:

Your network design, hardware and firmware configurations, and associated operating practices can inadvertently create certain attack vectors and/or vulnerabilities that may not have been fully accounted for in the deployment of your organization's access control solution. Many of these vulnerabilities fall into the category of Operational Technology (OT) systems. Do you know where your current cybersecurity vulnerabilities may be lurking on your system? Are your panels exposed to the outside world? Are you using encryption in all possible communications?

Future Vulnerabilities:

New exploits are always in the works based on vulnerabilities that are not yet public, which means no system is ever completely risk-free. Hence, your ability to quickly identify and address unexpected activity is often critical. LenelS2 can help you to evaluate potentially effective frameworks and techniques for monitoring your system. We can also assist in providing continuous network monitoring to detect potential threats early and help clients maintain a secure environment as an additional service.

The Solution:

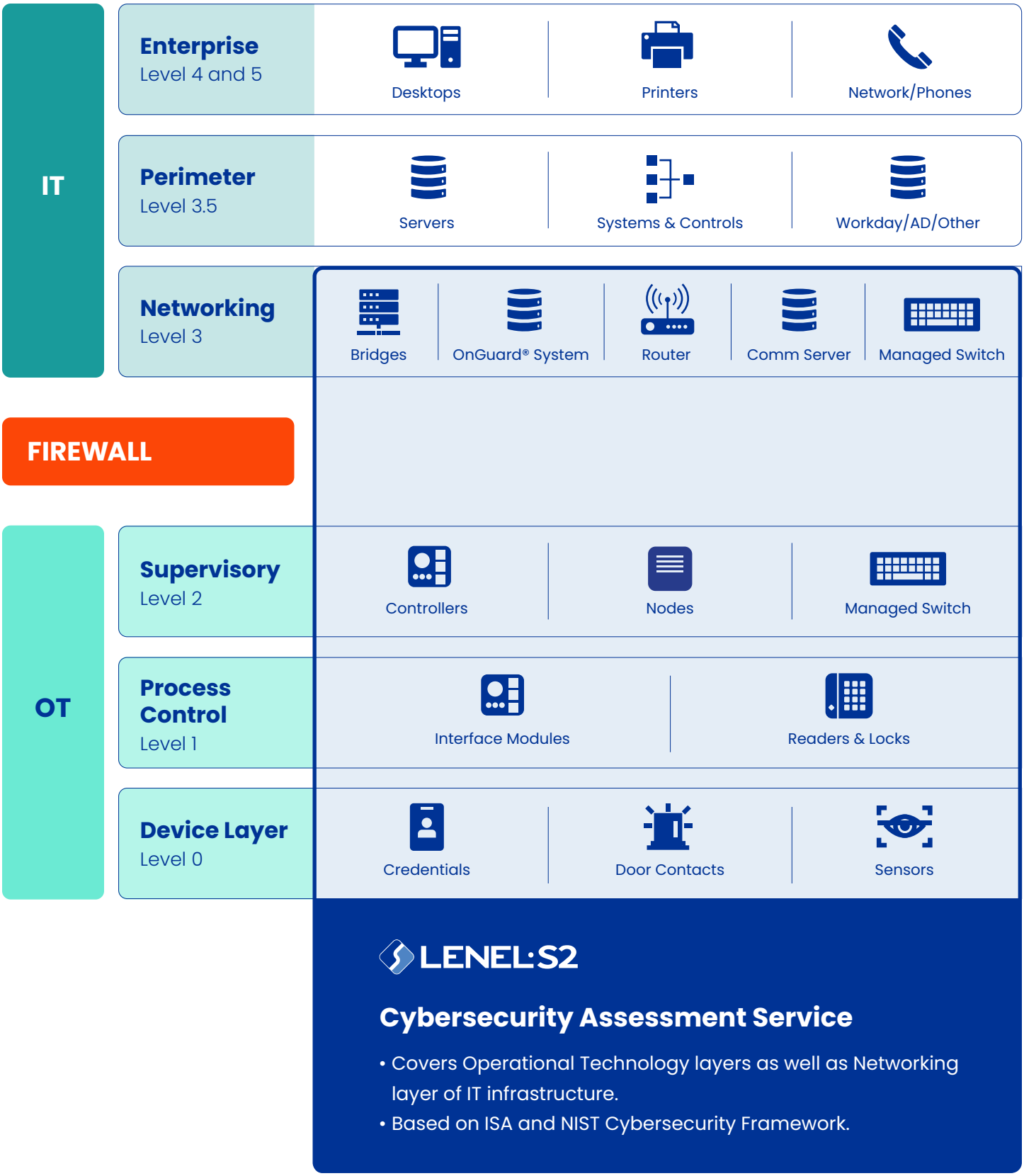
LenelS2 Cybersecurity Assessment Service

LenelS2 Cybersecurity Assessment Service helps customers identify, evaluate, and mitigate current and potential cybersecurity risks with their organization's access control systems and network.

The Cybersecurity Assessment prioritizes risk identification, enables compliance, and highlights gaps for enhanced security measures. Armed with a comprehensive understanding of your security posture, your organization can proactively manage risks and better protect against financial loss, legal consequences, and brand damage.

LenelS2 will conduct a thorough cybersecurity assessment across up to three sites, inclusive of the primary or central server. Throughout the assessment process, LenelS2 will focus on opportunities for system and hardware hardening, vulnerability assessments, and network security analysis in alignment with IEC 62443 and NIST SP 800-53 standards. As an outcome of the project, LenelS2 will identify gaps and deliver enhancement recommendations for bridging the disparity between your current practices and contemporary cybersecurity standards.

Where does LenelS2 bring value?



LENEL·S2

Cybersecurity Assessment Service

- Covers Operational Technology layers as well as Networking layer of IT infrastructure.
- Based on ISA and NIST Cybersecurity Framework.

What's included:

Current-State Gap Analysis

LenelS2 will map your organization's existing cybersecurity practices against IEC 62443 and NIST SP 800-53 standards through comprehensive questionnaires. Further, LenelS2 will identify gaps and deliver enhancement recommendations for bridging the disparity between current practices and standard requirements.

Site-Specific Analyses

- **Central Server Assessment:** LenelS2 will perform an in-depth security assessment of the central server's configuration and management of network connections and other essential security tasks. Further, LenelS2 will conduct vulnerability scanning and intrusion detection analysis and then will provide server hardening strategies based on assessment findings.
- **Satellite Sites Assessment:** LenelS2 will evaluate the security posture of satellite sites, with a focus on local server, hardware, and endpoint configurations. Additionally, LenelS2 will inspect remote connection protocols and firewall rules for inter-site communications.

System Hardening Evaluations

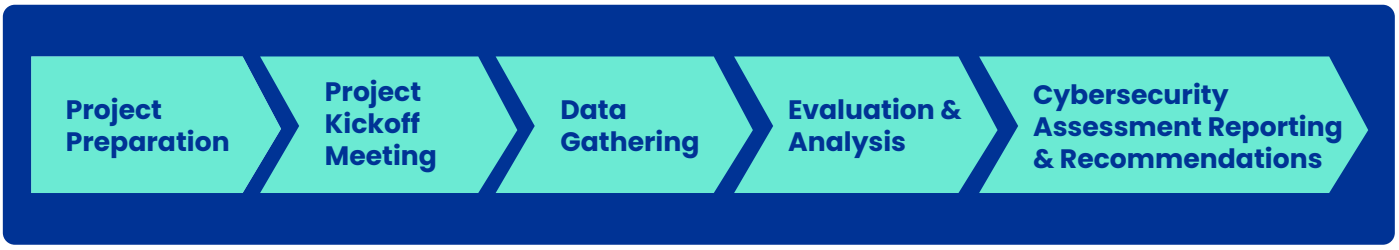
- **Panels:** LenelS2 will review the firmware version of installed panels for vulnerabilities and recommend patches where needed. LenelS2 will also identify opportunities to refine access controls to limit permissions and prevent unauthorized access.
- **OnGuard Hosts:** LenelS2 will assess and audit each site's OnGuard host following the same structured approach. Further, we will review application file systems to remove redundant services, thereby enhancing security.
- **Card Readers:** LenelS2 will inspect card reader systems and recommend security measures to prevent tampering.
- **Applications:** LenelS2 will optimize database roles and permissions to enforce the principle of least privilege. Further, LenelS2 will validate application configurations against OnGuard's hardening guidelines.

Network Security Analysis

- **Network Scan Analysis:** Leveraging our Honeywell Cyber Insights monitoring software, LenelS2 will perform network scans to identify vulnerabilities within the infrastructure. From there, we will prioritize vulnerabilities for remediation based on severity and potential network impact. Finally, LenelS2 will analyze network segmentation and recommend improvements for enhanced security.
- **Documentation and Reporting:** LenelS2 will compile all the findings and recommendations into a clear and concise report. The report will include an executive summary, along with detailed findings as well as advised remediation steps and a suggested timeline.

The process and deliverables

The LenelS2 Cybersecurity Assessment follows a proven model to evaluate your overall access control system, cybersecurity posture, and areas for improvement. Read on for the process:



1

Project Preparation:

LenelS2 delivers site preparation guidelines; client prepares for assessment as per guidelines.

2

Project Kickoff Meeting:

LenelS2 hosts a kickoff meeting, including project teams and sponsors; date and time for the on-site visit is set.

3

Data Gathering:

LenelS2 takes a holistic approach to evaluating your organization, collecting data for each of these areas:

- OnGuard host hardening assessment
- OnGuard application advanced hardening assessment
- Panel & reader hardening assessment
- Network segregation assessment using GrassMarlin
- Network vulnerability scan using Nessus®
- Physical inspection for threat detection
- Installation of Honeywell Cyber Insights monitoring software

4

Evaluation & Analysis:

LenelS2 will review each of the following carefully, analyzing and synthesizing what has been learned and documenting the analyses:

- Review of output from script logs from server and application
- Mapping of ISA-level assessment to controls
- Creating a visual representation of the network segregation
- Assessing host vulnerabilities based on Nessus scan

5

Cybersecurity Assessment Reporting & Recommendations:

LenelS2 will prepare a detailed report, curated and delivered by LenelS2 cybersecurity, product, and industry experts, to include:

- **Executive summary:** providing a dashboard of findings that includes the number and severity of cybersecurity vulnerabilities found as well as the organization's and team's strengths and weaknesses, with respect to protecting against cybersecurity threats.
- **Detailed individual reporting on each activity and finding:** diving into each of the areas of vulnerability found to qualify and quantify their magnitude and impact on your cybersecurity posture.
- **Top cybersecurity priorities & recommendations:** identifying the areas of greatest vulnerability as well as the actions and investments that will yield the greatest level of protection.

Next steps:

- After the initial three-month Honeywell Cyber Insights demonstration period, you have the option to fully integrate the cybersecurity monitoring tool, thereby providing proactive vulnerability warnings and insights as a cornerstone of your cybersecurity arsenal.

- Additionally, the complete Cybersecurity Assessment is recommended every two years to ensure the utmost levels of cybersecurity protection. Consult with your LenelS2 sales representative to schedule regular Assessments.

Honeywell Cyber Insights:

Protecting operations in an ever-changing threat landscape

As potential cyber threats increase with more specific attacks on OT, **companies that can best identify threats and vulnerabilities earlier can reduce the likelihood of an unplanned shutdown or safety incident caused by a malicious actor.** Knowing your site's current cybersecurity posture is vital to reducing cyber risk.

Honeywell Cyber Insights is designed to be used in OT environments to provide crucial information on your site's assets, vulnerabilities, and threats, to give your OT cybersecurity team the insights needed to better protect operations. Honeywell Cyber Insights is designed to be a readily accessible resource, with up-to-date information empowering you to focus on improving a facility's overall cybersecurity posture.

Why Honeywell Cyber Insights?

- Know what's connected to your network
- Detect threats faster and better manage vulnerabilities to limit remediation costs and impact to your business
- Get better visibility of an OT system's cybersecurity status
- An on-premises solution keeps data within your control

Delivered as part of the LenelS2 Cybersecurity Assessment, Honeywell Cyber Insights real-time monitoring is included for three months; please contact your LenelS2 sales representative for a quote for an annual Honeywell Cyber Insights service subscription.

Why LenelS2 Cybersecurity Assessment Service?

- Tailored for LenelS2 access control solutions
- Network scan and segmentation analysis
- Identifies security risks
- Evaluates risks
- Recommends mitigation strategy and steps
- Easy to understand Executive Summary, supported by detailed reports.

How does your company benefit?

- Identify and highlight vulnerabilities
- Prevent costly incidents
- Safeguard sensitive information
- Build trust within and outside the organization
- Contribute toward a resilient disaster recovery plan

Why LenelS2?

- Number one access control company globally (Omdia)
- Live and breathe access control
- Cybersecurity experts
- Security-first mindset from corporate down
- SIA validated cybersecurity training

Getting started

Contact your LenelS2 sales representative or value-added reseller to get started.

LenelS2.com • (866) 788-5095