CASE STUDY

KION Group

From Manual to Automated Continuous Monitoring

How KION Group gained real-time visibility into supplier cybersecurity posture with SecurityScorecard

Using the SecurityScorecard platform and MAX Program, KION Group moved from manual approach for vendor cybersecurity management to automated continuous monitoring of thousands of critical suppliers, enabling informed decisions on supplier awards and supporting key certification goals like ISO27001 and TISAX.

> SecurityScorecard gave us insights we simply didn't have before. The MAX program has greatly helped us track supplier security, reduce risk, and strengthen our compliance position through ISO27001 and TISAX certifications.
>
> **Jakub Watemborski**
> Director Global Supplier Risk and Capacity Management
> KION Group

Use Case

- Cyber Due Diligence
- Third Party Risk Management
- Vendor Risk Monitoring

About KION Group

Based in Germany, KION Group is one of the world's leading providers of industrial trucks and supply chain solutions. With operations across more than 100 countries and a portfolio of globally recognized brands such as Linde, Dematic, and Still, the company supports intelligent material handling and intralogistics solutions across industries.

SecurityScorecard.com
info@securityscorecard.com

Key Benefits

Once KION Group started working with SecurityScorecard, they:

1. **Gained ongoing visibility into the Information Security maturity and vulnerabilities of business-critical suppliers**
2. **Integrated cyber risk scores into vendor KPI frameworks, supporting procurement decisions**
3. **Supported ISO27001 and TISAX certi ications across several business units**
4. **Reduced risk exposure and improved supplier accountability through SSC's MAX Program, our managed service for Supply Chain Detection and Response (SCDR)**

The Challenge

KION Group had established a manual process to obtain visibility into the cybersecurity posture of its suppliers. However, the company struggled to obtain quickly and efficiently actionable intelligence on vendor vulnerabilities and risk exposure, making it difficult to assess and mitigate third-party cyber risks on regular basis. Once risks were assessed, setting up improvement measures was quite manual and a high-effort task.

This gap created potential downstream risk to its operations, supply chain, and compliance programs.

The Solution

KION implemented SecurityScorecard's platform and MAX Program to gain real-time, continuous insight into the security maturity of its most critical vendors. Instead of relying on one-off assessments or manual reviews, the company now uses SecurityScorecard ratings and MAX evaluations as key performance indicators in supplier decision-making.

The platform is primarily used by the supplier risk management and information security teams, who track progress toward remediation on a weekly and monthly basis. The risk assessment outcomes are considered by wide procurement teams in their sourcing and strategic decisions. SecurityScorecard has become a core internal tool for evaluating vendor risk and ensuring accountability.

The Results

A measurable shift in visibility and control

Today, the company can track real-time changes in vendor ratings and take action based on verified intelligence. This continuous monitoring has helped prevent potential vendor-related incidents and improved overall cyber resilience.

Certifications supported

SecurityScorecard contributed to achieve TISAX and ISO27001 certifications at several locations, highlighting the platform's effectiveness in elevating compliance readiness and supporting audit requirements.

Supplier performance now tied to security

By incorporating SSC scores and MAX Program outcomes into its supplier award process, KION has added a meaningful security metric into vendor evaluation. This has helped align procurement decisions with cybersecurity risk posture and driven vendors to proactively improve.

Looking to the Future

KION sees significant potential in further scaling the MAX Program and expanding the use of questionnaires and real-time alerts to deepen vendor engagement and reduce risk. The company is evaluating ways to broaden adoption internally and drive a stronger culture of cyber accountability across its supplier ecosystem.