SAMPLE

Security summary for Kymora Logistics

2 November 2026. Covers the last 30 days. Generated from the console's records. Prepared by Kymora Logistics. Made with Vardion.

Overview

A critical account takeover path is open at vpn.example.com: staff credentials exposed in a breach, with no second factor enforced. Signing in with a stolen password is one of the most common ways ransomware groups get in. This is the priority this week. 2 weaknesses rated high or critical are open on systems reachable from the internet. The number of open findings fell over the past 30 days, with 16 findings closed and 8 opened. The exposure score for systems reachable from the internet is 4.1 out of 10, in the low range (below 5).

Key figures

4.1 / 10	10	2	0.9 / 10	49.4%
Risk from the internet	Open internet findings	High or critical	Internal network risk	EAK gap analysis

EAK compliance is measured with the gap analysis of Greece's National Cybersecurity Authority (EAK).

Movement in the period

There was no material change in the exposure score over the past 30 days (3.9 to 4.1). By contrast, version 1 is now the approved Statement of Applicability.

Risks

In the last continuity test, 1 function took longer to recover than its objective allows. In a real outage the function would be down for longer than the organisation has said it can tolerate. One system accounts for 41% of the risk on its own. The internal network scores 0.9 on its own scale, with 2 findings open and none rated high or critical.

Governance, risk and compliance

Against the EAK controls, compliance stands at 49.4%, which the authority's method rates as high risk. The authority uses this analysis when it supervises the organisation. The loss scenarios estimate the expected cost of cyber incidents at €183,900 a year, and at least €693,000 in 1 year out of 10.

The expected loss sums 2 loss scenarios. The method is in the console under Risk.

Recommended actions

1. This week: Reset the credentials on finance@example.com, revoke its active sessions and confirm multi-factor authentication is enforced on vpn.example.com. This closes 1 finding and brings the exposure score to 1.6.
2. Within 30 days: Record a treatment or an acceptance for the risk above appetite.
3. This quarter: Turn the largest EAK gaps into actions with an owner and a date.

Decisions for the board

- Set the security budget against the expected loss of €183,900 a year.
- Decide whether to fund treatment of the risk above appetite or to accept it.
- Acknowledge this quarter's security figures, as part of the oversight NIS2 Article 20 gives the management body.

About this summary

The figures are the console's records on 2 November 2026. Each statement can be checked on its page in the console.