CINDER

Cinder Security Report

demo-tenant.onmicrosoft.com

Scan completed 2026-06-12 22:42

ABOUT THIS REPORT

Cinder focuses on Microsoft 365 identity and access security — a critical component of NIS2, GDPR and cyber-insurance readiness. However, NIS2 also includes broader organisational and operational requirements such as incident response governance, business continuity, supplier risk management, staff awareness training and physical security. Cinder should be considered one part of a broader compliance and cybersecurity strategy.

Health score

12 / 100

Critical

5 findings captured in this scan. Score deducts 25 for each critical, 10 for each high, 4 for each medium, 1 for each low. Floor 0.

Executive summary

Severity	Findings	Share
CRITICAL	2	40%
HIGH	2	40%
MEDIUM	1	20%
LOW	0	0%
INFO	0	0%

Findings

CINDER

Cinder Security Report

demo-tenant.onmicrosoft.com

Scan completed 2026-06-12 22:42

CRITICAL

Global Administrator alice.admin@demo-tenant.onmicrosoft.com has no MFA registered

A password-only Global Administrator account is a one-credential path to full tenant compromise — including reading mail, resetting other users' passwords, and creating persistent backdoors.

Admin accounts | ~10 min | NIS2-21.2.d | NIS2-21.2.j | GDPR-32

CRITICAL

Legacy authentication is not blocked tenant-wide

Legacy IMAP, POP, and SMTP AUTH endpoints bypass every modern MFA control. As long as they're reachable, a leaked password is enough to access mail — even on accounts that have MFA registered.

Conditional Access | ~15 min | NIS2-21.2.d | NIS2-21.2.j | GDPR-32

HIGH

8 Global Administrators detected — Microsoft recommends fewer than 5

Every additional Global Administrator increases the blast radius of a single credential compromise. Most of the named admins haven't used the role in over 30 days.

Admin accounts | ~30 min | NIS2-21.2.i | GDPR-32

HIGH

Third-party app 'Slack Web API' has Mail.Read consented at the tenant level

An OAuth app with Mail.Read can read every mailbox in the tenant. If the publisher is breached or the integration is decommissioned without revoking consent, that access persists indefinitely.

App consents | ~15 min | NIS2-21.2.e | GDPR-32

MEDIUM

Client secret for application 'HR Webhook' expires in 12 days

An expired secret quietly breaks the integration; rotating under pressure usually means a rushed change with weak documentation. Surface the rotation now and schedule it on a planned change window.

App consents | ~20 min | NIS2-21.2.i