CYBEREINFORCE

COMPLIANCE & AUDIT EVIDENCE

One control that maps to five frameworks at once.

Browser-layer URL enforcement is one of the few controls auditors can see working in real time: a block event, timestamped, tied to a device and a threat indicator. Cybereinforce turns that into standing evidence across ISO 27001, NIS2, NIST CSF 2.0, DORA and SOC 2 — without a separate compliance project.

ISO 27001

A.5.9 A.5.23 A.8.7 A.8.15 A.8.20

Asset inventory, cloud service security, anti-malware, logging, and network security controls — directly evidenced by enforced browser policy and block logs.

NIS2

Art. 21(2)

Risk-management measures for incident handling and supply-chain security — deterministic URL blocking is a concrete technical control for both.

NIST CSF 2.0

PR.PS-05 DE.CM-01 DE.CM-09

Prevents execution of unauthorized/malicious content and continuously monitors network and endpoint activity for adverse events.

DORA

Art. 9

ICT risk-management protection and prevention measures — deterministic, auditable URL-level protection for financial entities.

SOC 2

CC6.1 CC7.3

Logical access security and incident detection criteria — satisfied by enforced access controls and evidenced detection events.

What an auditor actually sees

EVIDENCE ARTIFACT	WHAT IT DEMONSTRATES	FRAMEWORKS IT SUPPORTS
Enforced IOC policy	A defined, active technical control blocking known-bad URLs/domains	ISO 27001 A.8.7 / A.8.20 · NIST PR.PS-05
Per-device block event	Timestamped, attributable detection of an adverse event	NIST DE.CM-01 / DE.CM-09 · SOC 2 CC7.3
Sentinel-ingested telemetry	Centralized, tamper-evident logging tied to incident response	ISO 27001 A.8.15 · DORA Art. 9 · NIS2 Art. 21(2)
Scoped device-group policy	Least-privilege enforcement across managed and partner devices	ISO 27001 A.5.9 / A.5.23 · SOC 2 CC6.1

Why this matters to auditors

Detection alone doesn't satisfy a control. Enforcement does.

Most Microsoft-stack environments can show that a threat was *identified*. Fewer can show it was *blocked*, on which device, at which URL, at what time — the specific evidence ISO 27001, DORA and SOC 2 auditors ask for when testing a control rather than reading a policy document.

Cybereinforce closes that gap at the browser, where the block actually happens, and pushes the event straight into Microsoft Sentinel alongside your existing incident evidence.

Platform certification

- **ISO/IEC 27001 certified** SaaS operations for the Cybereinforce platform itself.
- Data residency aligned to your selected region.
- Audit-ready exports for every enforcement and telemetry event.
- Retention configurable per plan tier, up to 365 days.

Preparing for an ISO 27001, NIS2, DORA or SOC 2 audit?

We'll map your current Defender/Sentinel setup to the controls above in a 30-minute session.

Book a compliance review →