

Como é que a Cyber Crucible apoia as obrigações da NIS2 para entidades essenciais e importantes?

Resposta curta: Para uma organização classificada como entidade essencial ou importante ao abrigo da NIS2, a Cyber Crucible apoia as medidas de gestão de risco exigidas — proteção de endpoints, controlo de acesso, encriptação e gestão de incidentes — e apoia as expectativas da diretiva em matéria de segurança da cadeia de fornecimento, uma vez que não recolhe dados de clientes e pode ser executada dentro do perímetro da entidade. A Cyber Crucible apoia estas obrigações; não as certifica nem as assume.

Como apoia as medidas da NIS2

- **Medidas de gestão de risco de cibersegurança.** A prevenção autónoma em endpoints, o acesso reforçado por MFA e a encriptação correspondem a várias das medidas de base da diretiva.
- **Segurança da cadeia de fornecimento.** Como fornecedor que não recolhe conteúdo de clientes e que oferece implementação no local (on-premises), a Cyber Crucible reduz, em vez de acrescentar, o risco de cadeia de fornecimento que a NIS2 exige que as entidades geridam.
- **Apoio à gestão e notificação de incidentes.** Um processo documentado de resposta a violações ajuda a entidade a cumprir os prazos de alerta precoce e de notificação da NIS2.

O limite honesto

As obrigações da NIS2 recaem sobre a entidade essencial ou importante, e não sobre uma ferramenta de segurança individual. A transposição pelos Estados-Membros variou: em 2026, a maioria dos Estados já tinha transposto a diretiva para o direito nacional, enquanto vários — incluindo a França, a Irlanda, os Países Baixos e a Espanha — ainda a estavam a finalizar. A Cyber Crucible não detém qualquer "certificação" NIS2; fornece evidências de controlo de apoio sob NDA.