ARICOMA

MICROSOFT PURVIEW DATA LOSS PREVENTION

Ochrana citlivých dat napříč Microsoft 365

Pomůžeme zákazníkovi nastavit praktický model prevence úniku dat: od prvotní analýzy a klasifikace, přes návrh DLP politik až po pilotní nasazení, monitoring a předání provozního modelu.

Cíl řešení: Identifikovat, klasifikovat a chránit citlivé informace v e-mailech, dokumentech, Teams a na koncových zařízeních - bez zbytečného omezení produktivity uživatelů.

✔ Ochrana citlivých dat

Prevence nechtěného sdílení osobních, finančních a obchodních informací.

✔ Soulad s požadavky

Podpora GDPR, NIS2, ISO 27001 a interních bezpečnostních pravidel.

✔ Přehled o práci s daty

Viditelnost toho, kde se citlivá data nacházejí a jak jsou sdílena.

✔ Rychlejší reakce

Centrální monitoring, alerty a podklady pro řešení bezpečnostních událostí.

✔ Bezpečná spolupráce

Kontrolované sdílení informací uvnitř organizace i s externími partnery.

✔ Využití investic do M365

Maximalizace hodnoty Microsoft 365 a Purview bez dalšího samostatného DLP nástroje.

Rozsah služby

1 Discovery	Audit M365 prostředí, compliance pravidel, vlastníků dat a prioritních use-case scénářů.
2 Klasifikace dat	Definice datových kategorií, Sensitive Information Types, klasifikátorů a Sensitivity Labels.
3 DLP politiky	Návrh 5-7 politik pro Exchange, SharePoint, OneDrive, Teams a pilotní skupinu.
4 Endpoint DLP	Onboarding a test scénářů: USB, tisk, clipboard, síťová úložiště a cloud upload.
5 Monitoring & optimalizace	Audit mode, vyhodnocení událostí, snížení false positives a proces výjimek.

Typické scénáře