USE CASE • PHARMA & LIFE SCIENCE INDUSTRY

Securing complex R&D ecosystems

Global pharmaceutical groups operate across multi-cloud platforms, distributed research entities and external partners. As these ecosystems expand, exposure signals multiply across environments. Security teams see more findings but struggle to understand **which exposures can actually propagate toward critical R&D systems.** For CISO teams, the challenge is no longer discovering vulnerabilities. It is identifying which exposures create real attack paths toward sensitive research assets.

CISO CHALLENGE

Fragmented visibility across cloud platforms, research systems and third-party partners creates **blind spots and prioritisation noise**.

Security teams detect more issues, but lack the context needed to **determine what truly threatens** critical R&D environments.

PANOP OPERATIONAL RESPONSE

- Attack surface mapping of R&D environments, identifies exposed lab systems, cloud research platforms
- Validation of exploitable vulnerabilities, prioritizes real risks to clinical trials or manufacturing
- Protection of sensitive datasets → continuous monitoring of data leaks and access paths
- Third-party risk visibility → CROs, biotech partners, supply chain exposures
- Automated remediation orchestration via existing SOC, ITSM and CI/CD workflows

Panop connects **exposure signals to business impact,** allowing security teams to prioritise what truly matters.

OPERATIONAL IMPACT

- Unknown external assets brought back into scope across cloud environments
- Attack paths toward critical R&D systems identified earlier
- Exposure prioritisation driven by propagation risk and business context
- Exposure-to-remediation cycles reduced from weeks to days in critical scenarios
- Faster cross-team decision making between security, cloud and engineering teams

With Panop, identify which exposures can actually **reach your critical R&D systems** and **act on them first**.