USE CASE • DEFENSE & AEROSPACE

Protecting sensitive programs and strategic defense assets

Defense and aerospace organizations operate across highly segmented environments combining engineering platforms, classified networks, industrial partners and complex supply chains. As these ecosystems expand across contractors, suppliers and digital infrastructures, exposure signals multiply across environments. Security teams detect more findings but struggle to understand **which exposures can propagate toward sensitive defense programs and strategic assets.** For CISO teams, the challenge is no longer discovering vulnerabilities. It is identifying **which exposures create real attack paths toward classified systems, engineering environments and mission-critical infrastructures.**

CISO CHALLENGE

Fragmented visibility across internal systems, industrial partners and supply chain environments creates blind spots and prioritisation noise.

Security teams detect more issues but lack the context needed to determine **what truly threatens sensitive programs, defense intellectual property and mission-critical infrastructures.**

PANOP OPERATIONAL RESPONSE

- Deep asset visibility across classified/unclassified systems
- Supply chain exposure validation ,dentifies weakest contractor links
- Mission-critical risk prioritization, focuses on systems impacting operations
- Correlation of exposure data, threat intelligence and operational context
- Automated remediation orchestration through existing SOC, ITSM and CI/CD workflows

Panop **connects exposure signals to operational risk,** enabling security teams to prioritise the threats that truly impact defense programs and strategic assets.

OPERATIONAL IMPACT

- Previously unknown external assets brought back into scope across defense ecosystems
- Attack paths toward classified environments and engineering systems identified earlier
- Exposure prioritisation driven by propagation risk and program criticality
- Exposure-to-remediation cycles reduced from weeks to days in critical scenarios
- Faster coordination between security, engineering and industrial partner teams

With Panop, identify which exposures **can reach your most sensitive defense** programs and **act on them first**.