PILLAR P2 | Weeks 1-8 - first detection-as-code shipped by week 3 | EX - Cyber Security

Adversarial Defence Mesh

XDR - SOAR - Identity Graph - AI Red Team

AI red-team agents, identity-graph SOC, posture-as-code.

MTTR (P1 INCIDENTS)	DETECTION COVERAGE (MITRE)	FALSE-POSITIVE RATE
71%	+ 3.4	62%

MANIFESTO

Why this pillar exists

Reseller SOCs sell tickets. We ship a defence mesh that learns: continuous AI red-team agents, identity-graph SOC, posture-as-code in CI, breach-rehearsal drills with measurable MTTR. Security that compounds, not catalogues.

KPIS

Outcomes we contract to

- MTTR (P1 incidents): 71%
- Detection coverage (MITRE): + 3.4
- False-positive rate: 62%

DELIVERABLES

Everything that ships

> Identity-graph SOC
Unified identity, device and workload graph powering correlation and blast-radius scoring.

> Detection-as-code library
Sigma + custom rules under git, CI tests, drift alerts.

> AI red-team agents
Continuous adversarial simulation across email, identity, app and cloud surfaces.

> Posture-as-code controls
Terraform-bound CIS / NCSC controls, drift detection, auto-remediation.

> Regulator dossier (DORA / NIS2)
Auto-generated evidence pack: ICT register, incident reporting, third-party risk.

POD COMPOSITION

Who shows up

- Security Principal (CISSP / CCSP)
- Detection Engineer
- AI Red-Team Lead
- GRC + Audit Lead

TIMELINE

Weeks 1-8 - first detection-as-code shipped by week 3

1. **Weeks 1-2 - Identity-graph baseline**
   Onboard IdPs, EDR, SaaS audit logs into the graph; map crown jewels.
2. **Weeks 3-5 - Detection-as-code + SOAR**
   Ship rule library, runbooks, auto-remediation; CI gates on every change.
3. **Weeks 5-8 - AI red-team continuous**
   Continuous adversarial drills, MTTR scorecard, regulator dossier signed off.

FLAGSHIP PODS

Squads we drop in

- SOC-as-Code Pod
- AI Red-Team Pod
- DORA / NIS2 Readiness Pod
- Identity-Graph Pod

PARTNERS

Hyperscalers & ISVs we orchestrate

Microsoft Defender - CrowdStrike - Wiz - Splunk - Sentinel - Okta - 1Password

FAQS

What buyers actually ask

Q. Do you replace our SIEM / EDR?
A. Usually no - we orchestrate Defender, CrowdStrike, Wiz, Splunk or Sentinel. The mesh is the brain, your tools are the limbs.

Q. How is this different from an MSSP?
A. We are SLA'd on MTTR and detection coverage, not ticket volume. Detections live in your git repo, not our portal.

Q. DORA / NIS2 ready?
A. Yes - the regulator dossier is shipped on day one and updated continuously, including third-party ICT risk and 24-hour incident reporting.

Q. What about AI-specific threats?
A. Prompt-injection, model-exfil and agent-abuse detections ship in the standard library, with red-team coverage on

every release.

Commission Adversarial Defence Mesh

Outcome-priced. Sovereign by default. Refund-backed if the contracted KPI isn't hit.

Reply to this PDF: alfaxprienz.com/stack/adversarial-defence-mesh#commission