

# Detection & Escalation: Consistency in Federated Organisations

A practical view for cyber and risk leaders in federated environments

## The problems we see in federated organisations

In federated organisations, security risks are often detected and escalated inconsistently across entities. While individual teams or providers may respond effectively at a local level, group cyber and risk teams often lack timely, reliable visibility when incidents span entities or impact group-level risk.

- Detection rules differ between entities and providers
- Escalation paths behave differently depending on who sees the alert
- Group visibility often occurs after an incident, not before



## Why this happens in federated environments

- Different entities use different detection rules
- SOC delivery is split between internal teams and MSPs
- Risk ownership sits at group level, but detection operates locally
- Policies exist, but detection behaviour doesn't reflect them

## What effective group-level detection looks like

### Before:

- Risks detected differently by entity
- Escalation depends on who receives the alert
- Group teams rely on reports or post-incident reviews

### After:

- The same risks are detected across all entities
- Escalation paths are clear and consistent
- Group-level risks are visible as they emerge

## How organisations address this (without replacing existing arrangements)

We help organisations validate and uplift their existing SOC and SIEM arrangements so that the same risks are detected, escalated and acted on consistently across the group, regardless of whether delivery sits with internal teams, MSPs or a combination of both.

- Validate which risks must be detected consistently across entities
- Align detection use cases and escalation paths to those risks
- Test whether this works in real scenarios, not just on paper