

Cybersecurity

Turn security concerns into prioritized work.

PHANTOM - assessment and audit-readiness service line

Understand the security of your identities, devices and critical services, then implement a practical improvement plan with ownership and evidence. Start with a bounded readiness assessment or a targeted remediation project.

GOOD FIT Leadership teams that need a defensible starting point, and technical teams that need help closing specific control gaps.

Scope

Readiness assessment - Review agreed configuration and evidence across identity, endpoints, critical applications, backup and operating procedures. Active exploitation requires its own written scope.

Risk and remediation - Describe the business consequence, affected boundary, observed evidence and a practical corrective action. Separate verified findings from questions that need further testing.

Control implementation - Scope changes to MFA, privileged access, endpoint settings, logging, segmentation or recovery. Use a pilot, acceptance checks and rollback.

Continuing oversight - Set a review cadence and evidence owners. Human SOC triage, incident response and regulatory programs are explicit service lines.

WHAT YOU RECEIVE

- Evidence-based assessment report
- Prioritized risk and remediation register
- Implementation and rollback plan
- Acceptance results for the agreed changes
- Leadership readout with decisions and dependencies

CUSTOMER RESPONSIBILITIES

- Authorize the exact assets and methods.
- Provide appropriate read-only access and existing policies.
- Approve changes and identify risk/reporting authority.

ACCEPTANCE CHECKS

- The report identifies the evidence and limits behind each conclusion.
- Approved and blocked identity paths behave as intended.
- Logging and alert routing work for a controlled event.
- Open findings have a named owner and next action.

SCOPE BOUNDARIES

- Guaranteed prevention or a regulatory certification
- Unscoped penetration testing or red-team activity
- Incident forensics and legal reporting unless contracted
- Third-party platform charges and emergency response retainers

DELIVERY FLOW

SCOPE / REVIEW / IMPROVE / VALIDATE