

Capability overview

Know your exposure. Strengthen your defence.

Quellium helps organisations understand attack paths, harden critical systems and turn security requirements into practical, verifiable improvements. Clear findings. Controlled change. Evidence you can use.

OUR EXPERTISE

01 AD attack path mapping

Map identity relationships and excessive privileges. Prioritise routes to critical assets and validate agreed remediation.

02 Security hardening

Review identity, endpoint and network configurations. Plan controlled improvements and verify the resulting baseline.

03 NIST SP 800-171 readiness

Scope requirements, assess gaps and organise implementation evidence against the revision applicable to your obligations.

04 Network monitoring

Improve telemetry, tune alerts and define escalation. Coverage hours and response responsibilities are agreed per engagement.

05 DNS security & resilience

Assess architecture and protective DNS policy. Validate filtering, resolution and failover, with useful operational visibility.

FOUNDER EXPERIENCE

5 years

Cybersecurity experience in a defence-contractor environment.

A background that informs careful scoping, documented decisions and practical verification.

Defined scope.
Controlled change.
Verified outcomes.

HOW WE DELIVER

01 Scope

Agree priorities, systems and success criteria.

02 Assess

Identify exposure and prioritise findings.

03 Strengthen

Implement agreed improvements with care.

04 Verify

Validate changes and hand over evidence.

Let's discuss your security priorities.

admin@quellium.com

quellium.com

Readiness support does not constitute certification or a guarantee of compliance.

Reference standards: NIST SP 800-171 Rev. 3 / NIST SP 800-171A Rev. 3