KRATOS / CYBER RESILIENCE SERIES



TECHNICAL WHITE PAPER

Understand exposure. Prioritise improvement.

A practical approach to website security assessment, evidence-led remediation and verification.

INSIDE THIS PAPER

Scope / Assessment process / Coverage / Data handling / Reporting / Service boundaries

Version 1.0 | 20 November 2026

KRATOS product family | Prepared by UKIYOAI PRIVATE LIMITED

info@ukiyoai.de | www.ukiyoai.de

01 / The business problem

Security evidence helps teams make better decisions; a scan result is not a protection guarantee.

Why a website deserves a recurring security review

A company website often handles enquiries, account sessions and integrations with other business services. Its configuration and software can change between reviews. SecureShield is designed to make supported external weaknesses visible and turn findings into an ordered improvement plan.

What SecureShield contributes

The service combines an agreed assessment scope, supported automated checks, contextual review where commissioned, reporting and a defined route to remediation and retesting. The value lies in evidence and follow-through: which asset was checked, what was observed, why it matters and what should happen next.

Confidentiality	Identify relevant transport, exposure and access weaknesses; approved fixes can help reduce opportunities for unauthorised disclosure.
Integrity	Review supported configuration and application indicators; prioritise corrections that help preserve trusted website behaviour.
Availability	Identify relevant exposure and maintenance concerns. Resilient hosting, DDoS protection and backups require their own controls and scope.

Assessment is one part of protection

SecureShield does not itself provide a universal attack-blocking layer. Risk reduction depends on addressing valid findings and maintaining complementary access, hosting and recovery controls.

Who this paper is for

Business owners, website managers, developers and procurement teams evaluating a repeatable website assessment service. It explains the reference service model; the signed engagement defines actual assets, methods and delivery commitments.

02 / Assessment-to-improvement process

Figure 1. A controlled cycle from permission to evidence and validated change.



Authorisation comes before technical assessment

Business-email confirmation can help verify a requester, but is not proof of domain ownership by itself. Use suitable evidence such as a domain-control token or documented authority. Provider-managed and third-party assets require appropriate permission. Never infer authorisation for additional hosts from a submitted URL.

Operate within explicit limits

Limit crawl depth, request volume, target origin and test windows. Prevent private-network and metadata access, validate redirects and apply rate limits. Intrusive testing, exploitation or authenticated access belongs in a separately authorised scope.

Continuous improvement, not a one-off badge

After remediation, record the rescan result and remaining risks. Repeat scheduled reviews and consider additional testing after material releases or changes. A passed check describes the evidence at that time, not future security.

03 / Baseline and deeper testing

Separate the public evaluation from recurring assessment and commissioned manual VAPT.

Public evaluation	Observed evaluation design: one declared HTTPS origin; up to ten public pages, sixty requests and three minutes; 12 baseline configuration checks. This is not a penetration test.
Recurring assessment	Available methods, frequency, authenticated coverage and retesting are agreed per package and implemented tooling. Only supported, applicable checks can be reported as completed.
Manual VAPT	Vulnerability Assessment and Penetration Testing uses a signed scope for deeper investigation, including selected access controls, inputs and business workflows. It is separately commissioned.
Remediation	Guidance can accompany findings. Configuration or code changes need agreed responsibility, access, approval, rollback and effort limits. Assessment does not imply automatic repairs.

How to interpret common indicators

Missing security headers may weaken defence in depth without proving an exploitable application flaw. A visible software version is not by itself evidence of an exploitable vulnerability. Certificate and TLS observations concern the connection, not every aspect of data storage or access. Context and validation determine priority.

Broader coverage must be evidenced

A proposed catalogue of 60 assessment topics is described on the next page. It is a scoping menu, not proof that every test is implemented, applicable or included. The evaluation currently presents a smaller baseline.

Methodology context

OWASP WSTG provides structured guidance for web application testing, including identity, authentication, authorisation and session testing [1]. SecureShield may use relevant guidance within an agreed scope; no OWASP certification or complete WSTG coverage is claimed.

04 / Reference coverage catalogue

60 scoping topics / 12 domains / not an automatic subscription inclusion list

Exposure	Asset inventory; public services; admin interfaces; information leakage; dangling DNS.
Configuration	Known vulnerable software; unsupported components; default settings; browser headers; unnecessary methods.
Authentication	Password policy; MFA; account enumeration; login throttling; account recovery.
Authorisation	Cross-user access; privilege boundaries; object-level API access; admin functions; tenant separation.
Sessions	Cookie attributes; session rotation; logout invalidation; timeouts; CSRF controls.
Input handling	Query injection; script injection; command injection; path traversal; server-side request forgery.
APIs	Endpoint inventory; schema validation; rate limits; token scopes; excessive data exposure.
Business workflows	Workflow bypass; transaction integrity; replay; upload controls; download access.
Data & crypto	TLS settings; certificates; exposed sensitive data; at-rest encryption review; key handling.
Network access	Segmentation; remote access; firewall exposure; insecure protocols; lateral-movement paths.
Cloud posture	Cloud permissions; public storage; security groups; workload isolation; audit logging.
Detection & recovery	Security-event coverage; alert routing; backup access; restore-test evidence; recovery runbooks.

Five topics per domain = 60 reference topics. Network, cloud, at-rest data, authenticated controls and recovery evidence need separately agreed access and scope. Never mark an unperformed topic as passed.

05 / Data protection and reporting

Keep evidence useful, minimised and restricted to authorised recipients.

Protect the assessment data

Collect only the business and technical information needed for the service. Restrict report access, encrypt transport and stored reports, and redact credentials, tokens and unnecessary personal data from evidence. Use separate scanner and management privileges. Set retention and deletion rules before production use.

Make the report traceable

Include the exact target, assessment window, accepted scope, method / tool version, authorisation reference and completed-check list. For each finding provide a description, redacted evidence, confidence, severity rationale, affected asset, recommended action and retest status. Record partial results and unavailable evidence explicitly.

Monthly view	Changes since the previous period; findings by severity; remediation progress; overdue actions; retest results; limitations.
Check states	Passed; finding; inconclusive; not applicable; not tested. Only evidence-backed outcomes are conclusive.
Management measures	Critical findings outstanding, validated closure rate and time to act. A closure rate is not an attack-prevention percentage.
Customer actions	Provide authority, approve scope, identify contacts, review priorities and authorise changes; maintain hosting, access and backups.

Illustrative example - not a customer result

A configuration review flags missing framing restrictions. The owner checks whether embedding is needed, approves an appropriate policy and tests it. A rescan verifies the response setting; this does not prove every application attack is prevented.

06 / Service boundary and next steps

Choose the engagement that matches your website, risk and assurance requirements.

Current evaluation versus reference service

The assessment page previously reviewed for this project is labelled evaluation edition, with browser-based reports, 12 baseline checks and email delivery / email verification disabled. It states that no automatic fixes are made. This paper does not announce those features as enabled or certify the evaluation for production use. Confirm the release and scope before submitting data.

What must be agreed

Specify included hosts, environments, access levels, scan limits, reporting frequency, review depth, remediation allowance, retest windows, support hours, data processing, retention and escalation. Full manual penetration testing, infrastructure reviews and major repairs require explicit scope. Commercial terms and availability are provided separately.

Combine the products where useful

SecureShield focuses on assessment and verification. SecureFortress addresses commissioned enterprise protection controls. SecureRevive addresses commissioned backup and recovery services. Buying one does not automatically include the others.

Technical sources and reading guide

References support the general security practices discussed here. They do not certify, endorse or verify KRATOS product implementation. Architecture and service choices remain engagement-specific.

[1] OWASP Web Security Testing Guide v4.2

https://wstg.owasp.org/v4.2/4-Web_Application_Security_Testing/

[2] NIST Cybersecurity Framework 2.0

https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20

Service assurance

No percentage of attacks prevented is claimed. Services reduce risk but cannot eliminate it. No guarantee of finding every vulnerability, uninterrupted operation or complete data recovery is made. Contracted work is performed with reasonable skill and care; responsibilities and liability follow the signed agreement and applicable law.

Discuss your scope: info@ukiyoai.de | www.ukiyoai.de