UKIYOAI SecureShield

Find weaknesses. Prioritise action.



VAPT with a defined 60-checkpoint coverage model.

See where an attacker could exploit weaknesses, understand the business impact and direct effort towards the most important fixes.

USP: EVIDENCE THAT LEADS TO ACTION

A proposed baseline of 60 defined checkpoints across 12 domains, combining automated assessment, manual validation and authorised penetration testing. Findings link technical exposure to remediation priorities.

HOW THIS HELPS PROTECT YOUR BUSINESS

Testing identifies weaknesses; remediation reduces exposure; retesting checks whether agreed fixes work. SecureShield itself is not a firewall or a continuous blocking service.

THE CLIENT OUTCOME

An evidence-led risk picture, a prioritised remediation backlog and a clearer basis for technical and management decisions.

SERVICE DESIGN NOTE

This brochure describes the proposed offer. Applicable assets, delivery capabilities and inclusions are confirmed during scoping. No service guarantees prevention of every attack or complete data recovery.

BOOK A VAPT SCOPING CALL

info@ukiyoai.de | www.ukiyoai.de | Book a consultation

Scope, deliverables, licences, availability, service levels and fees are agreed in writing.

What will be checked?

60 proposed baseline checkpoints / 12 domains / 5 checkpoints per domain

01 External exposure	01 Asset and subdomain inventory; 02 Exposed ports and services; 03 Administrative interfaces; 04 Information leakage; 05 Dangling DNS / takeover exposure
02 Configuration & patching	06 Known vulnerable software; 07 Unsupported components; 08 Default configurations; 09 HTTP security headers; 10 Unnecessary services / methods
03 Identity & authentication	11 Password policy; 12 MFA coverage / bypass resistance; 13 Account enumeration; 14 Login throttling; 15 Account recovery flows
04 Authorisation	16 Horizontal access controls; 17 Vertical privilege boundaries; 18 Object-level API permissions; 19 Administrative function access; 20 Tenant separation
05 Session management	21 Cookie security attributes; 22 Session rotation; 23 Logout invalidation; 24 Idle / absolute timeouts; 25 CSRF protections
06 Input & execution	26 SQL / query injection; 27 Cross-site scripting; 28 Command injection; 29 Path traversal / file inclusion; 30 Server-side request forgery
07 API security	31 Endpoint inventory; 32 Request / schema validation; 33 Rate limiting / resource abuse; 34 Token validation / scopes; 35 Excessive data exposure
08 Business logic & files	36 Workflow bypass; 37 Transaction tampering; 38 Replay / duplicate actions; 39 File upload restrictions; 40 File download authorisation
09 Data & cryptography	41 TLS configuration; 42 Certificate validity / trust; 43 Sensitive data exposure; 44 Encryption-at-rest configuration; 45 Secrets and key handling
10 Network & remote access	46 Segmentation controls; 47 Remote access configuration; 48 Firewall rule exposure; 49 Insecure network protocols; 50 Lateral movement paths
11 Cloud & platform	51 Cloud identity permissions; 52 Public storage exposure; 53 Security group configuration; 54 Workload isolation; 55 Cloud audit logging
12 Detection & resilience	56 Security event coverage; 57 Alert routing evidence; 58 Backup access separation; 59 Restore-test evidence; 60 Recovery runbook readiness

COUNTING RULE

60 is UKIYOAI's proposed baseline, not an OWASP-mandated count. Only applicable checks run; unavailable checks and exclusions are recorded. Additional tests depend on assets, access and risk. Resilience checks include evidence review, not destructive testing.

info@ukiyoai.de | www.ukiyoai.de | Book a consultation

Scope, deliverables, licences, availability, service levels and fees are agreed in writing.

From findings to verified fixes

A defined engagement that supports technical and business decisions

01 / SCOPE & AUTHORISE

Agree assets, environments, access, test windows, exclusions, escalation contacts and permitted techniques. Third-party assets need appropriate permission.

02 / ASSESS & VALIDATE

Use automated checks and manual investigation. Validate selected attack paths only within written rules of engagement; intrusive tests need explicit agreement.

03 / REPORT & PRIORITISE

Provide evidence, affected assets, severity, business context and remediation recommendations. Escalate critical findings using agreed contacts.

04 / REMEDIATE & RETEST

The client or an agreed delivery team implements fixes. A scoped retest records closed, partially resolved and open findings.

DELIVERABLES

Executive summary; technical report; checkpoint coverage and exclusions; remediation backlog; stakeholder readout; retest report where commissioned.

EXAMPLE: AN OVER-EXPOSED CUSTOMER API

A test identifies an authorisation weakness. The delivery team fixes the permission checks; retesting validates the scoped correction. Related weaknesses may require wider design changes.

WHAT TO AGREE BEFORE STARTING

Asset and application counts; authenticated or unauthenticated testing; assessment depth; severity method; report handling; timelines; retest scope and responsibilities.

TECHNICAL REFERENCES / No certification or endorsement implied

OWASP Web Security Testing Guide v4.2

TURN SECURITY FINDINGS INTO A CLEAR ACTION PLAN

info@ukiyoai.de | www.ukiyoai.de | Book a consultation

Scope, deliverables, licences, availability, service levels and fees are agreed in writing.

UKIYO KRATOS

SecureShield | Website assessment

Your next step starts here.

Generate your first report free, read the methodology, or choose an optional monthly plan. These links open the live portal and website.

Start free website assessment

Read the detailed white paper

Subscribe: USD or INR monthly plan

Visit the SecureShield product website

Monthly plan: US$21 or INR 1,961.18 per website, including applicable taxes. The selected currency and amount are fixed for renewal. Fixes are separately quoted. Generate your free report before subscribing.

Current portal scope: 12 bounded public-page checks. One free assessment per website. Email delivery is off. The preceding three original brochure pages describe a broader proposed VAPT service, separately scoped and agreed. Historical product names remain in those pages.

Updated 20 November 2026 | info@ukiyoai.de