MetaCache — Security Consultation Guide & Checklist

Comprehensive security assessments and threat intelligence investigations

Updated: September 5, 2025

1. Who this is for

For founders, CISOs, and legal/ops teams who need:

- **Targeted threat investigations** to unmask adversaries and stop active abuse
- **Comprehensive security audits** across web, mobile, network, and cloud infrastructure

2. What we do — two pillars

Threat Intelligence & Investigations

Scope: Identify actors; map infrastructure (dark web, Censys/Shodan); social graph pivots; credential/leak analysis; malware/app reverse engineering where relevant.

Outcomes: Adversary dossier, infrastructure map, IOC list, risk narrative, takedown/defence guidance.

Comprehensive Security Audits

Scope: Web/mobile/network/cloud; authN/Z; business-logic abuse; APIs; misconfigurations; hardening.

Alignment: OWASP ASVS/MASVS, CIS, cloud best practices.

Deliverables: Evidence-backed findings with PoCs, risk scoring, prioritized fixes, `retest included`.

3. How an engagement works

Discovery & Scope → Define objectives, boundaries, and success criteria

Threat Recon & Profiling → OSINT gathering and adversary identification

Automated Baselines → Vulnerability scanning and configuration analysis

Manual Deep Dive → Expert analysis and exploitation validation

Evidence & Validation → Document findings with proof-of-concept

Report, Fix Support & Retest → Deliverables, remediation guidance, and validation

4. What we need from you

- **Authorization:** ROE/SOW with clear engagement boundaries
- **Context and artefacts:** Background information, samples, indicators
- **Access:** Test accounts, logs, read-only cloud roles
- **Assets list:** Complete inventory of in-scope systems
- **Constraints:** Data sensitivity, blackout windows, compliance requirements

5. What you receive

- **Executive summary** with risk heatmap
- **Adversary dossier** and IOC list (CSV/STIX format)
- **Evidence pack:** Screenshots, PCAPs, PoCs, infrastructure maps
- **Prioritized remediation plan** with owners and effort estimates
- **Retest report** and attestation letter after successful remediation

6. Indicative timelines (typical)

7. Evidence handling & confidentiality

6. Indicative timelines (typical)

- **Investigations:** 3–10 days depending on scope/evidence
- **Security audits:** 5–14 days depending on asset count/depth
- **Critical issues** flagged within 24 hours during testing windows

7. Evidence handling & confidentiality

- NDA/MSA/SOW standard
- Segmented workspaces
- Encryption at rest/in transit
- Least-privilege access
- Data purge on sign-off

8. Commercial notes

- Fixed-scope proposals with transparent pricing
- Time-boxed retest window included
- Change orders for scope expansion
- Milestones for discovery/testing/reporting phases
- No public attribution without explicit client consent

9. Pre-engagement questionnaire

Please provide responses to these questions to help us scope your engagement effectively:

1. **Trigger:** What prompted this security assessment or investigation?
2. **Objectives:** What are your success criteria and key concerns?
3. **Assets in scope:** Which systems, applications, or domains should we examine?
4. **Data handling:** Any PII, secrets, or sensitive data considerations?
5. **Prior work:** Previous audits, incidents, or security assessments?
6. **Available artefacts:** Suspicious emails, malware samples, URLs, wallet IDs, logs?
7. **Change windows:** When can testing occur without business impact?
8. **Required outcomes:** Report format, attestation letters, legal support needed?
9. **Stakeholders:** Who are the key contacts and decision makers?
10. **On-call contact:** Emergency contact during testing windows?
11. **Access provision:** What tooling, accounts, or access can you provide?
12. **Timeline constraints:** Hard deadlines or preferred delivery dates?

Additional context: Any other information that would help us understand your specific situation?

Contact

hello@metacache.in

Book a consultation: Include 2–3 preferred slots and a brief overview of your objectives.